(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. Mai 2007 (10.05.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/051787 A1

(51) Internationale Patentklassifikation:
H04Q 7/38 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2006/067955

(22) Internationales Anmeldedatum:
31. Oktober 2006 (31.10.2006)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2005 052717.5
4. November 2005 (04.11.2005) DE
10 2006 009726.2 2. März 2006 (02.03.2006) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **FALK, Rainer** [DE/DE]; Hollerner Str. 23 A, 85386 Eching (DE). **GÜNTHER, Christian** [DE/DE]; Hauptstr. 110 A, 85579 Neubiberg (DE). **KRÖSELBERG, Dirk** [DE/DE]; Pestalozzistr. 27, 80469 München (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

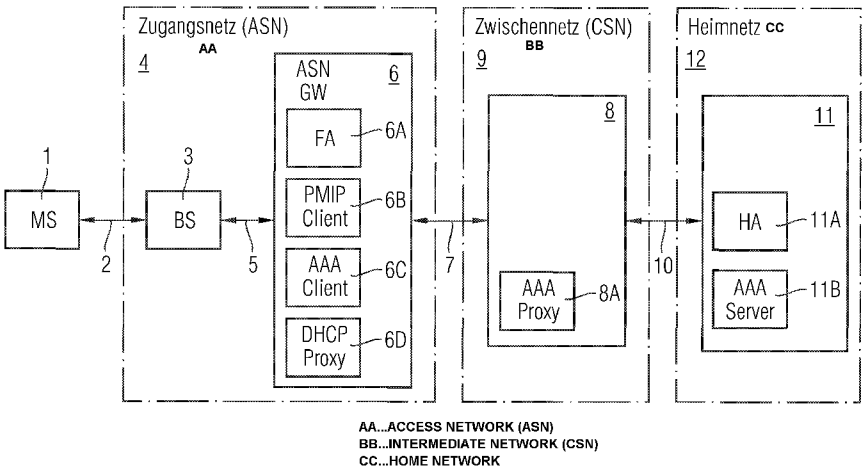
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND SERVER FOR PROVIDING A MOBILE KEY

(54) Bezeichnung: VERFAHREN UND SERVER ZUM BEREITSTELLEN EINES MOBILITÄTSSCHLÜSSELS



(57) Abstract: The invention relates to a method and authentication server for providing a mobile key. According to said method, upon receipt of an authentication message (access authentication) that is transmitted when a subscriber logs on to the network, the authentication server (11B) extracts a subscriber identification (T-ID) contained in said message and generates a corresponding mobile key (MIP_KEY), which is stored together with the respective extracted subscriber identification (T_ID). Upon subsequent receipt of a key request message (key request) that is transmitted when a subscriber registers, the authentication server (11B) extracts a mobile identification (MIP_ID) of the subscriber contained in said message and searches for an identical mobile identification (MIP_ID'), which can be derived in accordance with a configurable derivation function (AF) from a subscriber identification (T_ID') that is stored in the authentication server (11B). Once a derived mobile identification (MIP_ID') that is identical or can be uniquely assigned to the extracted mobile identification (MIP_ID) has been found, the authentication server (11B) provides the stored corresponding mobile key (MIP_KEY) that has been generated, to cryptographically protect the mobile signalling messages of the registered subscriber.

[Fortsetzung auf der nächsten Seite]

WO 2007/051787 A1

EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Verfahren und Authentisierungsserver zum Bereitstellen eines Mobilitätsschlüssels, wobei der Authentisierungsserver (11B) bei Empfang einer während einer Netzanmeldung eines Teilnehmers übertragenen Authentisierungsnachricht (access authentication) eine darin enthaltene Teilnehmeridentität (T_ID) des Teilnehmers extrahiert und einen zugehörigen Mobilitätsschlüssel (MIP_KEY) generiert, der zusammen mit der jeweils extrahierten Teilnehmeridentität (T_ID) gespeichert wird, wobei der Authentisierungsserver (11B) bei einem späteren Empfang einer während einer Registrierung eines Teilnehmers übertragenen Schlüsselanfragenachricht (Key-Request) eine darin enthaltene Mobilitätsidentität (MIP_ID) des Teilnehmers extrahiert und nach einer identischen Mobilitätsidentität (MIP_ID') sucht, die gemäß einer konfigurierbaren Ableitungsfunktion (AF) aus einer der in dem Authentisierungsserver (11B) gespeicherten Teilnehmeridentitäten (T_ID') ableitbar ist, und wobei der Authentisierungsserver (11B) bei Auffinden einer abgeleiteten Mobilitätsidentität (MIP_ID'), die identisch bzw. eindeutig zuordenbar zu der extrahierten Mobilitätsidentität (MIP_ID) ist, den gespeicherten zugehörigen generierten Mobilitätsschlüssel (MIP_KEY) zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten des registrierten Teilnehmers bereitstellt.

Beschreibung

Verfahren und Server zum Bereitstellen eines Mobilitäts-schlüssels.

Die Erfindung betrifft ein Verfahren und einen Authentisierungs-Server zum Bereitstellen eines eindeutig zuordbaren Mobilitätsschlüssels zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten für einen Heimagenten eines Mobilfunknetzes, insbesondere für anonyme Teilnehmer.

Das Internet mit dem TCP/IP-Protokoll bietet eine Plattform für die Entwicklung höherer Protokolle für den mobilen Bereich. Da die Internet-Protokolle weit verbreitet sind, kann mit entsprechenden Protokollerweiterungen für mobile Umgebungen ein großer Anwenderkreis erschlossen werden. Die herkömmlichen Internet-Protokolle sind jedoch ursprünglich nicht für den mobilen Einsatz konzipiert. In der Paketvermittlung des herkömmlichen Internets werden die Pakete zwischen stationären Rechnern ausgetauscht, die weder ihre Netzwerkadresse ändern noch zwischen verschiedenen Subnetzen wandern. Bei Funknetzen mit mobilen Rechnern, werden mobile Rechner MS häufig in verschiedene Netzwerke eingebunden. Das DHCP (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weitere Konfigurationsparameter an einen Rechner in einem Netzwerk. Ein Rechner, der in ein Netzwerk eingebunden wird, bekommt automatisch eine freie IP-Adresse durch das DHCP-Protokoll zugewiesen. Hat ein mobiler Rechner DHCP installiert, muss er lediglich in Rechweite eines lokalen Netzwerkes kommen, das die Konfiguration über das DHCP-Protokoll unterstützt. Bei dem DHCP-Protokoll ist eine dynamische Adressvergabe möglich, d.h. eine freie IP-Adresse wird automatisch für eine bestimmte Zeit zugeteilt. Nach Ablauf dieser Zeit muss die Anfrage durch den mobilen Rechner entweder erneut gestellt werden oder die IP-Adresse kann anderweitig vergeben werden.

Mit DHCP kann ein mobiler Rechner ohne manuelle Konfiguration in ein Netzwerk eingebunden werden. Als Voraussetzung muss lediglich ein DHCP-Server zur Verfügung stehen. Ein mobiler Rechner kann so Dienste des lokalen Netzwerkes benutzen und beispielsweise zentral abgelegte Dateien benutzen. Bietet ein mobiler Rechner jedoch selbst Dienste an, kann ein potentieller Dienstnutzer den mobilen Rechner nicht auffinden, da sich dessen IP-Adresse in jedem Netzwerk, in das der mobile Rechner eingebunden wird, ändert. Das gleiche geschieht, wenn sich eine IP-Adresse während einer bestehenden TCP-Verbindung ändert. Dies führt zum Abbruch der Verbindung. Daher bekommt bei Mobile-IP ein mobiler Rechner eine IP-Adresse zugewiesen, die er auch in einem anderen Netzwerk behält. Bei herkömmlichem IP-Netzwechsel ist es nötig, die IP Adressen-Einstellungen entsprechend anzupassen. Eine ständige Anpassung von IP- und Routing-Konfigurationen auf dem Endgerät ist jedoch manuell fast unmöglich. Bei den herkömmlichen automatischen Konfigurationsmechanismen wird die bestehende Verbindung bei einem Wechsel der IP-Adresse unterbrochen. Das MIP-Protokoll (RFC 2002, RFC 2977, RFC3344, RFC3846, RFC3957, RFC3775, RFC3776, RFC4285) unterstützt die Mobilität von mobilen Endgeräten. Bei den herkömmlichen IP-Protokollen muss das mobile Endgerät jedes Mal seine IP-Adresse anpassen, wenn es das IP-Subnetz wechselt, damit die an das mobile Endgerät adressierten Datenpakete richtig geroutet werden. Um eine bestehende TCP-Verbindung aufrecht zu erhalten, muss das mobile Endgerät seine IP-Adresse beibehalten, da ein Adressenwechsel zu einer Unterbrechung der Verbindung führt. Das MIP-Protokoll hebt diesen Konflikt auf, indem es einem mobilen Endgerät bzw. einem Mobile Node (MN) erlaubt, zwei IP-Adressen zu besitzen. Das MIP-Protokoll ermöglicht eine transparente Verbindung zwischen den beiden Adressen, nämlich einer permanenten Home-Adresse und einer zweiten temporären Care-Of-Adresse. Die Care-Of-Adresse ist die IP-Adresse, unter der das mobile Endgerät aktuell erreichbar ist.

Ein Heimagent (Home Agent) ist ein Stellvertreter des mobilen Endgerätes, solange sich das mobile Endgerät nicht in dem ur-

sprünglichen Heimnetz aufhält. Der Heimagent ist ständig über den aktuellen Aufenthaltsort des mobilen Rechners informiert. Der Heimagent stellt üblicherweise eine Komponente eines Routers im Heimnetz des mobilen Endgerätes dar. Wenn das mobile Endgerät sich außerhalb des Heimnetzes befindet, stellt der Heimagent eine Funktion bereit, damit sich das mobile Endgerät anmelden kann. Dann leitet der Heimagent die an das mobile Endgerät adressierten Datenpakete in das aktuelle Subnetz des mobilen Endgerätes weiter.

Ein Fremdagent (Foreign Agent) befindet sich in dem Subnetz, in dem sich das mobile Endgerät bewegt. Der Fremdagent leitet eingehende Datenpakete an das mobile Endgerät bzw. an den mobilen Rechner weiter. Der Fremdagent befindet sich in einem sogenannten Fremdnetz (Visited Network). Der Fremdagent stellt ebenfalls üblicherweise eine Komponente eines Routers dar. Der Fremdagent routet alle administrativen Mobile-Datenpakete zwischen dem mobilen Endgerät und dessen Heimagenten. Der Fremdagent entpackt die von dem Heimagent gesendeten, getunnelten IP-Datenpakete und leitet deren Daten an das mobile Endgerät weiter.

Die Heimadresse des mobilen Endgerätes ist die Adresse, unter der das mobile Endgerät permanent erreichbar ist. Die Heimadresse hat dasselbe Adressenpräfix wie der Heimagent. Die Care-Of-Adresse ist diejenige IP-Adresse, die das mobile Endgerät in dem fremden Netz verwendet.

Der Heimagent pflegt eine sogenannte Mobilitätsanbindungstabelle (MBT: Mobility Binding Table). Die Einträge in dieser Tabelle dienen dazu, die beiden Adressen, d.h. die Heimadresse und die Care-Of-Adresse, eines mobilen Endgeräts einander zuzuordnen und die Datenpakete entsprechend umzuleiten. Die MBT-Tabelle enthält Einträge über die Heimadresse, die Care-Of-Adresse und eine Angabe über die Zeitspanne, in der diese Zuordnung gültig ist (Life Time). Figur 1 zeigt ein Beispiel für eine Mobilitätsanbindungstabelle nach dem Stand der Technik.

Der Fremdagent (FA) enthält eine Besucherliste bzw. Visitor List (VL: Visitor List), die Informationen über die mobilen Endgeräte enthält, die sich gerade in dem IP-Netz des Fremdagenten befinden. Figur 2 zeigt ein Beispiel für eine derartige Besucherliste nach dem Stand der Technik.

Damit ein mobiler Rechner in ein Netz eingebunden werden kann, muss er zunächst in Erfahrung bringen, ob er sich in seinem Heim- oder einem Fremdnetz befindet. Zusätzlich muss das mobile Endgerät in Erfahrung bringen, welcher Rechner in dem Subnetz der Heim- bzw. der Fremdagent ist. Diese Informationen werden durch sogenanntes Agent Discovery ermittelt.

Durch die nachfolgende Registrierung kann das mobile Endgerät seinen aktuellen Standort seinem Heimagenten mitteilen. Hierzu sendet der mobile Rechner bzw. das mobile Endgerät dem Heimagenten die aktuelle Care-Of-Adresse zu. Zur Registrierung sendet der mobile Rechner einen Registration-Request bzw. eine Registrierungsanforderung an den Heimagenten. Der Heimagent (HA) trägt die Care-Of-Adresse in seine Liste ein und antwortet mit einem Registration Reply bzw. einer Registrierungsantwort. Hierbei besteht allerdings ein Sicherheitsproblem. Da prinzipiell jeder Rechner an einen Heimagenten eine Registrierungsanforderung schicken kann, könnte man auf einfache Weise einem Heimagenten vorspiegeln, ein Rechner habe sich in ein anderes Netzwerk bewegt. So könnte ein fremder Rechner alle Datenpakete eines mobilen Rechners bzw. mobilen Endgerätes übernehmen, ohne dass ein Sender davon erfährt. Um dies zu verhindern, verfügen der mobile Rechner und der Heimagent über gemeinsame geheime Schlüssel. Kehrt ein mobiler Rechner in sein Heimatnetzwerk zurück, deregistriert er sich beim Heimagenten, da der mobile Rechner nunmehr alle Datenpakete selbst entgegennehmen kann. Ein mobiles Funknetz muss unter Anderem folgende Sicherheitseigenschaften aufweisen. Informationen dürfen nur für gewünschte Kommunikationspartner zugänglich gemacht werden, d.h. nicht gewünschte Mithörer dürfen keinen Zugriff auf übertragene Daten erhalten. Das mo-

bile Funknetz muss also die Eigenschaft der Vertraulichkeit (Confidentiality) aufweisen. Daneben muss Authentizität gegeben sein. Die Authentizität (Authenticity) erlaubt es einem Kommunikationspartner zweifelsfrei festzustellen, ob eine Kommunikation tatsächlich zu einem gewünschten Kommunikationspartner aufgebaut wurde oder ob sich eine fremde Partei als Kommunikationspartner ausgibt. Authentifizierungen können pro Nachricht oder pro Verbindung durchgeführt werden. Wird auf Basis von Verbindungen authentifiziert, wird nur einmal zu Anfang einer Sitzung (Session) der Kommunikationspartner identifiziert. Man geht dann für den weiteren Verlauf der Sitzung davon aus, dass die folgenden Nachrichten weiterhin von dem entsprechenden Sender stammen. Selbst wenn die Identität eines Kommunikationspartners feststeht, d.h. der Kommunikationspartner authentifiziert ist, kann der Fall auftreten, dass dieser Kommunikationspartner nicht auf alle Ressourcen zugreifen darf bzw. nicht alle Dienste über das Netzwerk benutzen darf. Eine entsprechende Autorisation setzt in diesem Fall eine vorhergehende Authentifizierung des Kommunikationspartners voraus.

Bei mobilen Datennetzen müssen Nachrichten längere Strecken über Luftschnittstellen zurücklegen und sind somit für potentielle Angreifer leicht erreichbar. Bei mobilen und drahtlosen Datennetzen spielen daher Sicherheitsaspekte eine besondere Rolle. Ein wesentliches Mittel zur Erhöhung der Sicherheit in Datennetzwerken stellen Verschlüsselungstechniken dar. Durch die Verschlüsselung ist es möglich, Daten über unsichere Kommunikationswege, beispielsweise über Luftschnittstellen übertragen, ohne dass unbefugte Dritte Zugriff auf die Daten erlangen. Zum Verschlüsseln werden die Daten, d.h. der sogenannte Klartext mit Hilfe eines Verschlüsselungsalgorithmus in Chiffre-Text transformiert. Der verschlüsselte Text kann über den unsicheren Datenübertragungskanal transportiert und anschließend entschlüsselt bzw. dechiffriert werden.

Als eine vielversprechende drahtlose Zugangstechnologie wird WiMax (Worldwide Interoperability for Microwave Access) als neuer Standard vorgeschlagen, der für die Funkübertragung IEEE 802.16 verwendet. Mit WiMax sollen mit Sendestationen ein Bereich von bis zu 50km mit Datenraten von über 100 Mbit pro Sekunde versorgt werden.

Figur 3 zeigt ein Referenzmodel für ein WiMax-Funknetzwerk. Ein mobiles Endgerät MS befindet sich im Bereich eines Zugangsnetzwerkes (ASN: Access Serving Network). Das Zugangsnetz ASN ist über mindestens ein besuchtes Netz (Visited Connectivity Service Network VCSN) bzw. Zwischennetz mit einem Heimnetz HCSN (Home Connectivity Service Network) verbunden. Die verschiedenen Netzwerke sind über Schnittstellen bzw. Referenzpunkte R miteinander verbunden. Der Heimagent HA der Mobilstation MS befindet sich in dem Heimnetz HCSN oder in einem der besuchten Netze VCSN.

WiMax unterstützt zwei Realisierungsvarianten von Mobile IP, sogenanntes Client MIP (CMIP), bei dem die Mobilstation selbst die MIP-Clientfunktion realisiert, und Proxy-MIP (PMIP), bei dem die MIP-Client-Funktion durch das WiMax-Zugangsnetz realisiert ist. Die dazu im ASN vorgesehene Funktionalität wird als Proxy Mobile Node (PMN) oder als PMIP-Client bezeichnet. Dadurch kann MIP auch mit Mobilstationen verwendet werden, die selbst kein MIP unterstützen.

Figur 4 zeigt den Verbindungsaufbau bei Proxy-MIP, wenn sich der Heimagent in dem besuchten Netzwerk befindet nach dem Stand der Technik.

Nach Aufbau einer Funkverbindung zwischen dem mobilen Endgerät und einer Basisstation erfolgt zunächst eine Zugangsauthentisierung. Die Funktion der Authentisierung, der Autorisation und der Buchhaltung erfolgt mittels sogenannter AAA-Servern (AAA: Authentication Authorization and Accounting). Zwischen dem mobilen Endgerät MS und dem AAA-Server des Heimnetzes (HAAA) werden Authentisierungsnachrichten ausgetauscht

mittels der die Adresse des Heimagenten und ein Authentisierungsschlüssel gewonnen werden. Der Authentisierungsserver im Heimnetz enthält die Profildaten des Teilnehmers. Der AAA-Server erhält eine Authentisierungsanfragenachricht, die eine Teilnehmeridentität des mobilen Endgerätes enthält. Der AAA-Server generiert nach erfolgreicher Zugangsauthentisierung einen MSK-Schlüssel (MSK: Master Session Key) zum Schutz der Datenübertragungsstrecke zwischen dem mobilen Endgerät MS und der Basisstation des Zugangsnetzwerkes ASN. Dieser MSK-Schlüssel wird von dem AAA-Server des Heimnetzes über das Zwischennetz CSN an das Zugangsnetzwerk ASN übertragen.

Nach der Zugangsauthentisierung wird, wie in Figur 4 zu sehen, der DHCP-Proxy-Server im Zugangsnetzwerk ASN konfiguriert. Falls die IP-Adresse und Host-Konfiguration bereits in der AAA-Antwortnachricht enthalten ist, wird die gesamte Information in den DHCP-Proxy-Server heruntergeladen.

Nach erfolgreicher Authentisierung und Autorisierung sendet die Mobilstation bzw. das mobile Endgerät MS eine DHCP Discovery Nachricht und es erfolgt eine IP-Adressenzuweisung.

Falls das Zugangsnetzwerk ASN sowohl PMIP als auch CMIP Mobilität unterstützt, informiert der Fremdagent die ASN-Handover Funktion, indem es eine R3-Mobilitätskontextnachricht sendet. Bei Netzwerken, die nur PMIP unterstützen kann hierauf verzichtet werden. Nachdem die Heimadresse ausgelesen worden ist, wird diese an den PMIP-Client weitergeleitet.

Anschließend erfolgt eine MIP-Registrierung. Bei der Registrierung wird der Heimagent über den aktuellen Standort des mobilen Endgerätes informiert. Zur Registrierung sendet der mobile Rechner die Registrierungsanforderung an den Heimagenten, die die aktuelle Care-Of-Adresse enthält. Der Heimagent trägt die Care-Of-Adresse in eine von ihm verwaltete Liste ein und antwortet mit einer Registrierungsantwort (Registration Reply). Da prinzipiell jeder Rechner an einen Heimagenten Registrierungsanforderungen schicken kann, könnte auf

einfache Weise einem Heimagenten vorgespielt werden, ein Rechner habe sich in ein anderes Netzwerk bewegt. Um dies zu verhindern verfügen sowohl der mobile Rechner als auch der Heimagent über einen gemeinsamen geheimen Schlüssel, nämlich einen MIP-Schlüssel. Falls der Heim-Agent (HA) den MIP-Schlüssel nicht kennt, richtet er ihn ein, wozu er mit einem Heim-AAA-Server kommuniziert.

Nach Abschluss des in Figur 4 dargestellten Verbindungsaufbaus hat das mobile Endgerät eine Heimadresse erhalten und ist bei dem Heimatagenten registriert.

Der herkömmliche Verbindungsaufbau erfolgt im Wesentlichen in drei Schritten, nämlich der Zugangsauthentisierung des Teilnehmers, einer anschließenden IP-Adressenzuweisung und schließlich einer MIP-Registrierung. Bei der Zugangsauthentisierung meldet sich der Teilnehmer beim Mobilnetz an. Hierzu wird bei einer herkömmlichen Netzwerkanmeldung zunächst eine Funkverbindung zwischen dem mobilen Endgerät MS und dem Zugangnetz ASN aufgebaut, wobei ein Authentisierungsserver H-AAA zur Authentisierung des Teilnehmers mindestens eine Authentisierungsnachricht von dem Teilnehmerendgerät über einen Authentisierungs-Client des Zugangsnetzes empfängt. Diese Authentisierungsnachricht (Access Authentication) enthält unter Anderem eine äußere Teilnehmeridentität bzw. einen Netzwerk-Access-Identifier (NAI). Durch diese äußere NAI ist der Authentisierungsserver H-AAA des Teilnehmers bestimmbar. Bei erfolgreicher Authentisierung benachrichtigt der Authentisierungs-Server H-AAA den Authentisierungs-Client des Zugangsnetzes hierüber, sodass dieses eine gesicherte Funkverbindung zu dem Teilnehmerendgerät einrichtet.

Nach erfolgter IP-Adressenzuweisung wird schließlich die mobile IP-Registrierung durchgeführt. Hierzu empfängt der Heimagent HA eine Registrierungsanfragenachricht, die eine Teilnehmeridentität beinhaltet, und richtet eine Schlüsselanfrage an den Authentisierungsserver. Nach Empfang einer Schlüsselanfragenachricht (key request) für einen Mobilitätsschlüssel

durch den Authentisierungsserver stellt der Authentisierungsserver einen mobilen Schlüssel für den Heimagenten des Teilnehmers zur Verfügung, wenn für die in der Schlüsselanfragenachricht enthaltene Teilnehmeridentität ein zugehöriger Mobilitätsschlüssel in dem Authentisierungsserver gespeichert ist.

Bei einem herkömmlichen Mobilnetz (standard mobile IP) ist der Mobilitätsschlüssel, der zu kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten dient, im Authentisierungsserver H-AAA des Heimnetzes vorkonfiguriert, d. h. für jeden Teilnehmer ist jeweils für seine Teilnehmeridentität ein zugehöriger Mobilitätsschlüssel in dem Authentisierungsserver H-AAA des Heimnetzes gespeichert.

Bei neuartigen Mobilfunknetzen, wie beispielsweise WiMax, wird allerdings bei der Netzwerkanmeldung der Mobilitätsschlüssel im Authentisierungsserver H-AAA erzeugt und gespeichert, d. h. der Mobilitätsschlüssel ist nicht vorkonfiguriert. Wenn bei einem derartigen Mobilfunknetz der Heimagent eines Teilnehmers eine Schlüsselanfragenachricht mit einer darin enthaltenen Teilnehmeridentität an den Authentisierungsserver des Heimnetzes richtet, kann der Authentisierungsserver die in der Schlüsselanfragenachricht enthaltene Teilnehmeridentität nicht zuordnen und kann somit keinen entsprechenden Mobilitätsschlüssel bereitstellen.

Es ist daher die Aufgabe der vorliegenden Erfindung, ein Verfahren und einen Authentisierungsserver zu schaffen, die stets einen Mobilitätsschlüssel für einen sich registrierenden Teilnehmer bereitstellen.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den im Patentanspruch 1 angegebenen Merkmalen und durch einen Authentisierungsserver mit den im Patentanspruch 24 angegebenen Merkmalen gelöst.

Die Erfindung schafft ein Verfahren zum Bereitstellen mindestens eines Mobilitätsschlüssels zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten,
wobei bei einer Netzanmeldung eines Teilnehmers der Mobilitätsschlüssel generiert wird und
wobei eine spätere Registrierung des Teilnehmers bei einem Heimagenten mittels einer Mobilitätsidentität des Teilnehmers erfolgt, die dem generierten Mobilitätsschlüssel in einem Authentisierungsserver eindeutig zugeordnet wird.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird bei der Netzanmeldung mindestens eine Authentisierungsnachricht, welche eine äußere Teilnehmeridentität des Teilnehmers enthält, von dem Authentisierungsserver empfangen.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens befindet sich der Authentisierungsserver in dem Heimnetz des Teilnehmers.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens generiert der Authentisierungsserver des Heimnetzes nach Empfang der Authentisierungsnachricht mindestens einen Mobilitätsschlüssel für den Teilnehmer und speichert diesen zusammen mit der in der Authentisierungsnachricht enthaltenen äußeren Teilnehmeridentität ab.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens speichert der Authentisierungsserver des Heimnetzes zusätzlich eine Sitzungsidentität des Teilnehmers zu dem generierten Mobilitätsschlüssel und zu der äußeren Teilnehmeridentität des Teilnehmers ab.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens sendet der Teilnehmer bei einer Registrierung bei dem Heimagenten eine Registrierungsanfragenachricht (MIP RRQ), welche eine Teilnehmeridentität des Teilnehmers enthält, an den Heimagenten.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird eine Mobilitätsidentität von der in der Registrierungsanfragenachricht enthaltenen Teilnehmeridentität gemäß einer beliebigen konfigurierbaren Ableitungsfunktion abgeleitet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird eine Mobilitätsidentität von der in der Registrierungsanfragenachricht enthaltenen Teilnehmeridentität und von einer Sitzungsidentität (Session ID) des Teilnehmers gemäß einer konfigurierbaren Ableitungsfunktion abgeleitet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die Sitzungsidentität durch eine Abrechnungsidentität (CUI: chargeable user ID) des Teilnehmers gebildet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die äußere Teilnehmeridentität durch einen Netzwerkzugriffsidentifizierer NAI (network access identifier) gebildet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die äußere Teilnehmeridentität durch einen anonymen Netzwerkzugriffsidentifizierer NAI gebildet.

Bei einer alternativen Ausführungsform des erfindungsgemäßen Verfahrens wird die äußere Teilnehmeridentität durch einen sitzungsspezifisch gewählten pseudonymen Netzwerkzugriffsidentifizierer NAI gebildet.

Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens wird die äußere Teilnehmeridentität durch einen Hash-Funktionswert einer Mobilitätsidentität gebildet.

Bei einer weiteren bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die Mobilitätsidentität (MIP ID)

durch einen Hash-Funktionswert einer äußeren Teilnehmeridentität gebildet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens stellt der Authentisierungsserver dem Heimagenten bei Empfang einer Schlüsselanfragenachricht (key request), welche eine Mobilitätsidentität enthält, denjenigen generierten Mobilitätsschlüssel bereit, der zu derjenigen äußeren Teilnehmeridentität abgespeichert ist, aus der eine identische Mobilitätsidentität gemäß einer vorgegebenen konfigurierbaren Ableitungsfunktion ableitbar ist.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens stellt der Authentisierungsserver dem Heimagenten bei Empfang einer Schlüsselanfragenachricht (key request), welche eine Mobilitätsidentität enthält, denjenigen generierten Mobilitätsschlüssel bereit, der zu derjenigen äußeren Teilnehmeridentität abgespeichert ist, aus der eine Identität gemäß einer ersten vorgegebenen konfigurierbaren Ableitungsfunktion ableitbar ist, die identisch ist zu einer gemäß einer zweiten vorgegebenen konfigurierbaren Ableitungsfunktion aus der Mobilitätsidentität abgeleiteten Identität.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens stellt der Authentisierungsserver dem Heimagenten bei Empfang einer Schlüsselanfragenachricht (key request), welche eine Mobilitätsidentität enthält, denjenigen generierten Mobilitätsschlüssel bereit, der zu derjenigen äußeren Teilnehmeridentität abgespeichert ist, die aus der Mobilitätsidentität gemäß einer vorgegebenen konfigurierbaren Ableitungsfunktion ableitbar ist.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die Teilnehmeridentität durch ein mobiles Teilnehmerendgerät oder durch einen PMIP-Client eines Zugangsnetzes gebildet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die generierte Teilnehmeridentität von einem Authentisierungs-Client oder einem Fremdagenten FA eines Zugangsnetzes (ASN) modifiziert.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens werden die Authentisierungsnachrichten jeweils durch ein Datenpaket gebildet, dessen Verwaltungsdaten eine äußere Teilnehmeridentität enthalten.Ein Authentisierungsnachrichtendatenpaket weist vorzugsweise Nutzdaten auf, die eine teilnehmerspezifische innere Teilnehmeridentität enthalten.

Dabei wird die innere Teilnehmeridentität vorzugsweise durch einen eindeutigen Teilnehmernamen gebildet.

Bei einer alternativen Ausführungsform wird die innere Teilnehmeridentität durch eine Telefonnummer gebildet.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens enthält die äußere Teilnehmeridentität eine Adresse zum Routen des Datenpakets zu dem Authentisierungsserver des Heimnetzes.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die Registrierungsanfragenachricht durch ein Datenpaket gebildet, das unter Anderem die äußere Teilnehmeridentität und eine dem Teilnehmer zugewiesene aktuelle Care-of-Adresse enthält.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird die Schlüsselanfragenachricht (key request) durch ein Datenpaket gebildet, dessen Verwaltungsdaten eine Mobilitätsidentität (MIP_ID) enthalten, die vorzugsweise gemäß einer vorgegebenen Abteilungsfunktion (AF) durch den Heimagenten aus der übertragenen Teilnehmeridentität abgeleitet wird.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird das Zugangsnetz durch ein WiMax-Netz gebildet.

Bei einer Ausführungsform des erfindungsgemäßen Verfahrens werden die Authentisierungsnachrichten nach einem Radius-Datenübertragungsprotokoll übertragen.

Bei einer alternativen Ausführungsform des erfindungsgemäßen Verfahrens werden die Authentisierungsnachrichten nach einem Diameter-Datenübertragungsprotokoll übertragen.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird ein Zwischennetz durch ein WiMax-Zwischennetz CSN gebildet.

Bei einer ersten Ausführungsform des erfindungsgemäßen Verfahrens ist das Heimnetz ein 3GPP-Netz.

Bei einer alternativen Ausführungsform des erfindungsgemäßen Verfahrens wird das Heimnetz durch ein Netz gebildet, welches eine AAA-Infrastruktur für WLAN-Teilnehmer bereitstellt (WLAN-Netz).

Die Erfindung schafft ferner einen Authentisierungsserver zum Bereitstellen eines Mobilitätsschlüssels,
wobei der Authentisierungsserver bei Empfang einer während einer Netzanmeldung eines Teilnehmers übertragenen Authentisierungsnachricht (access authentication) eine darin enthaltene Teilnehmeridentität (T-ID) des Teilnehmers extrahiert und einen zugehörigen Mobilitätsschlüssel (MIP_KEY) generiert, der zusammen mit der jeweils extrahierten Teilnehmeridentität (T_ID) gespeichert wird,
wobei der Authentisierungsserver bei einem späteren Empfang einer während einer Registrierung eines Teilnehmers übertragenen Schlüsselanfragenachricht (Key-Request) eine darin enthaltene Mobilitätsidentität (MIP_ID) des Teilnehmers extrahiert und nach einer identischen oder eindeutig zuordenbaren

Mobilitätsidentität (MIP_ID') sucht, die gemäß einer konfigurierbaren Ableitungsfunktion (AF) aus einer der in dem Authentisierungsserver gespeicherten Teilnehmeridentitäten (T_ID') ableitbar ist, und
wobei der Authentisierungsserver bei Auffinden einer abgeleiteten Mobilitätsidentität (MIP_ID'), die identisch oder eindeutig zuordenbar zu der extrahierten Mobilitätsidentität (MIP_ID) ist, den gespeicherten zugehörigen generierten Mobilitätsschlüssel (MIP_KEY) zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten des registrierten Teilnehmers bereitstellt.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Authentisierungsservers wird die Teilnehmeridentität durch eine in den Verwaltungsdaten der Authentisierungsnachricht enthaltene äußere Teilnehmeridentität NAI gebildet, die zum Routen der Authentisierungsnachricht zu dem Authentisierungsserver vorgesehen ist.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Authentisierungsservers befindet sich dieser in einem Heimnetz des Teilnehmers.

Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird der Mobilitätsschlüssel zusätzlich einem PMIP-Client des Zugangsnetzes (ASN) bereitgestellt.

Im Weiteren werden bevorzugte Ausführungsformen des erfindungsgemäßen Verfahrens und des erfindungsgemäßen Authentisierungsservers unter Bezugnahme auf die beigefügten Figuren zur Erläuterung erfindungswesentlicher Merkmale beschrieben.

Es zeigen:

Figur 1 ein Beispiel für eine Mobilitätsanbindungstabelle nach dem Stand der Technik;

Figur 2 ein Beispiel für eine Besucherliste nach dem Stand der Technik;

Figur 3 eine Referenznetzwerkstruktur für ein WiMax-Funknetz;

Figur 4 einen Verbindungsaufbau bei einem herkömmlichen WiMax-Netz nach dem Stand der Technik;

Figur 5 eine Netzstruktur gemäß einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens;

Figur 6 ein Ablaufdiagramm zur Erläuterung der Funktionsweise des erfindungsgemäßen Verfahrens;

Figur 7 ein weiteres Ablaufdiagramm zur Erläuterung der Funktionsweise des erfindungsgemäßen Verfahrens;

Figur 8 eine Tabelle zur Erläuterung der Funktionsweise des erfindungsgemäßen Verfahrens;

Figur 9 Datenstrukturen verschiedener bei dem erfindungsgemäßen Verfahren eingesetzter Datenpakete;

Figur 10 ein Diagramm zur Erläuterung des erfindungsgemäßen Verfahrens.

Wie man aus Figur 5 erkennen kann ist ein mobiles Endgerät 1 über eine drahtlose Schnittstelle 2 mit einer Basisstation 3 eines Zugangsnetzes 4 verbunden. Bei dem mobilen Endgerät 1 handelt es sich um ein beliebiges mobiles Endgerät, beispielsweise einen Laptop, einen PDA, ein Mobiltelefon, oder ein sonstiges mobiles Endgerät. Die Basisstation 3 des Zugangsnetzes 4 ist über eine Datenübertragungsleitung 5 mit einem Zugangsnetzwerk-Gateway 6 verbunden. In dem Zugangs-Gateway-Rechner 6 sind vorzugsweise weitere Funktionalitäten integriert, insbesondere ein Fremdagent 6A, ein PMIP-Client 6B, ein AAA-Client-Server 6C und ein DHCP-Proxy-Server 6D.

Der Fremdagent 6A ist ein Router, der Routing-Dienste für das mobile Endgerät 1 zur Verfügung stellt. Die an das mobile Endgerät 1 gerichteten Datenpakete werden getunnelt übertragen und von dem Fremdagenten 6A entpackt.

Das Gateway 6 des Zugangsnetzes 4 ist über eine Schnittstelle 7 mit einem Rechner 8 eines Zwischennetzes 9 verbunden. Der Rechner 8 enthält vorzugsweise einen AAA-Proxy-Server. Ein Heimagent 11A befindet sich in einem Heimnetz 12 innerhalb eines Rechners 11 und ist der Stellvertreter des mobilen Endgerätes 1. Der Heimagent 11A ist ständig über den aktuellen Aufenthaltsort des mobilen Rechners 1 informiert. Datenpakete für das mobile Endgerät 1 werden zunächst an den Heimagenten 11A übertragen und von dem Heimagenten 11A aus getunnelt an den Fremdagenten 6A weitergeleitet. Umgekehrt können Datenpakete, die von dem mobilen Endgerät 1 ausgesendet werden, direkt an den jeweiligen Kommunikationspartner gesendet werden. Die Datenpakete des mobilen Endgerätes 1 enthalten dabei die Heimadresse als Absenderadresse. Die Heimadresse hat dasselbe Adresspräfix, d.h. Netzadresse und Subnetzadresse, wie der Heimagent 11A. Datenpakete, die an die Heimadresse des mobilen Endgerätes 1 gesendet werden, werden von dem Heimagenten 11A abgefangen und getunnelt von dem Heimagenten 11A an die Care-of-Adresse des mobilen Endgerätes 1 übertragen und schließlich an dem Endpunkt des Tunnels, d.h. durch den Fremdagenten 6A oder das mobile Endgerät 1 selbst empfangen.

Der Rechner 8 des Zwischennetzes 9 ist über eine weitere Schnittstelle 10 mit einem Authentisierungsserver 11B des Heimnetzes 12 verbunden. Bei dem Heimnetz 12 handelt es sich beispielsweise um ein 3GPP-Netz für UMTS. Bei einer alternativen Ausführungsform handelt sich bei dem Server 11B um einen Authentisierungsserver eines WLAN-Netzes.

Figur 6 zeigt ein Ablaufdiagramm zur Erläuterung einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens. Der Authentisierungsserver 11A, welcher sich vorzugsweise in einem Heimnetz 12 des Teilnehmers befindet, überwacht in einem

Schritt S1 ständig bzw. in regelmäßigen Zeitabständen, ob er eine Authentisierungsanfragenachricht (access authentication) empfängt.

Die Datenstruktur einer derartigen Authentisierungsnachricht ist in Figur 9A dargestellt. Bei einer bevorzugten Ausführungsform werden die Authentisierungsnachrichten durch Datenpakete gebildet, wobei die Verwaltungsdaten jeweils eine äußere Teilnehmeridentität NAI enthalten und die Nutzdaten vorzugsweise einen innere Teilnehmeridentität beinhalten. Die äußere Teilnehmeridentität NAI wird zum Routen des Datenpaketes zu dem Authentisierungsserver 11B des Heimnetzes 12 verwendet. Bei der äußeren Teilnehmeridentität handelt es sich vorzugsweise um einen sogenannten Netzwerkzugriffsidentifizierer NAI (network access identifier). Bei dem Netzwerkzugriffsidentifizierer NAI kann es sich beispielsweise um eine anonyme Teilnehmeridentität handeln (z. B. "Guest") oder um eine vom Teilnehmer gewählte pseudonyme Teilnehmeridentität (z. B. "Superman" oder "1274O3L"). Auch ein spezifischer Benutzername (user name) kann als äußere Teilnehmeridentität in der Authentisierungsnachricht enthalten sein. Bei einer möglichen Ausführungsform wird die äußere Teilnehmeridentität durch einen kryptographischen Hash-Funktionswert H(r) gebildet, wobei r beispielsweise eine Zufallszahl oder eine zufällig gewählte Zeichenkette ist.

Die in den Nutzdaten der Authentisierungsnachricht enthaltene innere Teilnehmeridentität, wie sie in Figur 9A dargestellt ist, wird beispielsweise durch einen eindeutigen Teilnehmernamen (user name) oder durch eine Telefonnummer (IMSI, International Mobile Subscriber Identity; oder MSISDN Mobile Station international PSTN/ISDN number) gebildet.

Empfängt der Authentisierungsserver 11B eine Authentisierungsnachricht, wie sie in Figur 9A dargestellt ist, extrahiert er im Schritt S2 die darin enthaltene äußere Teilnehmeridentität NAI.

Anschließend generiert der Authentisierungsserver 11B im Schritt S3 einen Mobilitätsschlüssel (MIP key). Das Generieren des Mobilitätsschlüssels kann in beliebiger Weise erfolgen. Beispielsweise wird der Mobilitätsschlüssel als Zufallszahl generiert.

Bei einer alternativen Ausführungsform wird der Mobilitätsschlüssel im Rahmen der Netzzugangsauthentisierung unter Verwendung eines kryptographischen Schlüsselvereinbarungsprotokolls eingerichtet. Bekannte kryptographische Schlüsselvereinbarungsprotokolle sind beispielsweise EAP-SIM, EAP-AKA und EAP-TLS.

Bei einer alternativen Ausführungsform wird der Mobilitätsschlüssel aus der extrahierten äußeren Teilnehmeridentität entsprechend einer beliebigen Ableitungsfunktion AF abgeleitet.

In einem Schritt S4 speichert der Authentisierungsserver 11B die extrahierte Teilnehmeridentität NAI zusammen mit dem zugehörigen generierten Mobilitätsschlüssel (MIP_key) ab. Der in Figur 6 dargestellte Ablauf erfolgt während der Netzwerkanmeldung bzw. Authentisierung des Teilnehmers.

Figur 8 zeigt schematisch die nach dem Vorgang in Figur 6 in dem Authentisierungsserver 11B abgespeicherten Informationen. Der Authentisierungsserver 11B speichert intern die extrahierte äußere Teilnehmeridentität NAI und jeweils dazu einen generierten Mobilitätsschlüssel MIP key.

Bei einer bevorzugten Ausführungsform wird zusätzlich zu der äußeren Teilnehmeridentität NAI eine Sitzungsidentität (session ID) des Teilnehmers gespeichert, wobei es sich beispielsweise um eine Abrechnungsidentität zur Abrechnung von Kosten CUI (chargeable user ID) des Teilnehmers handeln kann. Diese chargeable user ID wird dem Radius-Client (network access server) von dem Authentisierungsserver im Rahmen der Netzwerkanmeldung übermittelt. Die chargeable user ID CUI

bzw. Abrechnungsidentität, die vorzugsweise als sitzungsspezifische Identität des Teilnehmers eingesetzt wird, wird in dem mobile IP request und in einem Radius access request von dem Fremdagenten 6A an den Authentisierungsserver 11B eingetragen. Der Eintrag erfolgt durch den Fremdagenten 6A bzw. PMN (PMIP client) und nicht durch den Client-Server der Mobile Station MS, da dieser die chargeable user ID nicht kennt. Dies ist bei PMIP möglich, da der registration request bzw. die Registrierungsanfragenachricht bei PMIP nicht vom Client-Server gesendet wird. Der Authentisierungsserver 11B verwaltet den Zustandsdatensatz für die chargeable user ID und den zugeordneten MIP-Schlüssel, um bei einer Anfrage durch den Heimagenten 11A den passenden Mobilitätsschlüssel zu liefern. Das Vorsehen einer Sitzungs-ID bzw. -CUI ist bei dem erfindungsgemäßen Verfahren optional.

Nach der Zugangsauthentisierung und der anschließenden IP-Adressenzuweisung erfolgt zu einem späteren Zeitpunkt die MIP-Registrierung des Teilnehmers. Hierzu sendet der Teilnehmer bei seiner Registrierung bei einem Heimagenten 11A eine Registrierungsanfragenachricht (MIP RRQ), welche eine Teilnehmeridentität des Teilnehmers enthält. Die Struktur einer derartigen Registrierungsanfragenachricht ist in Figur 9 dargestellt. Die Registrierungsanfragenachricht besteht dabei vorzugsweise aus einem Datenpaket, das unter Anderem eine Teilnehmeridentität NAI und die aktuelle Care-of-Adresse des Teilnehmers beinhaltet. Der Heimagent 11A des Teilnehmers empfängt die Registrierungsanfragenachricht und leitet aus der Teilnehmeridentität gemäß einer konfigurierbaren Ableitungsfunktion AF eine Mobilitätsidentität des sich registrierenden Teilnehmers ab.

Bei einer alternativen Ausführungsform wird die Mobilitätsidentität des Teilnehmers aus der in der Registrierungsanfragenachricht enthaltenen Teilnehmeridentität NAI und einer Sitzungsidentität des Teilnehmers gemäß einer weiteren konfigurierbaren Ableitungsfunktion AF abgeleitet. Bei den Ablei-

tungsfunktionen AF kann es sich um beliebige Funktionen handeln.

Der Heimagent 11A sendet eine Schlüsselanfragenachricht (Key_request) an den Authentisierungsserver 11B. Der Authentisierungsserver 11B überwacht, wie in Figur 7 zu sehen, ständig, ob er eine Schlüsselanfragenachricht empfängt. Die Datenstruktur einer derartigen Schlüsselanfragenachricht ist beispielsweise in Figur 9C dargestellt. Die Schlüsselanfragenachricht wird vorzugsweise durch ein Datenpaket gebildet, das als äußere Teilnehmeridentität NAI die von dem Heimagenten 11A aus der Registrierungsanfragenachricht extrahierte Mobilitätsidentität enthält. D Das Datenpaket ist als Schlüsselanfragenachricht (key request) gekennzeichnet.

Der Authentisierungsserver 11A extrahiert im Schritt S6 die in der Schlüsselanfragenachricht enthaltene Mobilitätsidentität (MIP_ID).

Anschließend sucht der Authentisierungsserver 11B in einem Schritt S7 nach einem Teilnehmer, der eine identische bzw. eindeutig zuordenbare Mobilitätsidentität aufweist, die gemäß der vorgegebenen Ableitungsfunktion AF aus einer in dem Authentisierungsserver 11B im Schritt S4 gespeicherten Teilnehmeridentität ableitbar ist. Hierzu leitet der Authentisierungsserver 11B für jede von ihm gespeicherte Teilnehmeridentität gemäß der vorgegebenen Ableitungsfunktion eine entsprechende Mobilitätsidentität MIP_ID ab und vergleicht diese mit der extrahierten Mobilitätsidentität MIP_ID. Sobald der Authentisierungsserver 11B einen Teilnehmer findet, dessen abgeleitete Mobilitätsidentität MIP_ID mit der extrahierten Mobilitätsidentität MIP_ID identisch bzw. eindeutig zuordenbar ist, stellt er dem Heimagenten 11A den dazu gespeicherten Mobilitätsschlüssel (MIP key) zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten des registrierten Teilnehmers zur Verfügung.

Die in den Figuren 6, 7 dargestellten Abläufe lassen sich wie folgt zusammenfassen. Als erstes wird während der Netzanmeldung des Teilnehmers ein generierter Mobilitätsschlüssel MIP_KEY zusammen mit der äußeren Teilnehmeridentität NAI durch den Authentisierungsserver 11B gespeichert.

```
Extract NAI from Access Authentication Message
Generate MIP_Key
Store (NAI, MIP_Key)
```

Anschließend wird während der MIP-Registrierung des Teilnehmers durch den Authentisierungsserver 11B ein eindeutig zugeordneter Mobilitätsschlüssel (MIP_KEY) bereitgestellt.

```
Extract MIP_ID from Key Request Message
For all NAI MIP_ID‘ = function (NAI)
IF MIP_ID‘ = MIP_ID THEN OUTPUT MIP_KEY
```

Bei einer alternativen Ausführungsform leitet der Authentisierungsserver 11B, anstatt dem in Fig. 7 dargestellten Schritt S7, aus der gespeicherten Teilnehmeridentität unter Verwendung einer ersten Ableitungsfunktion und aus der Mobilitätsidentität unter Verwendung einer zweiten Ableitungsfunktion jeweils eine Identität ab und vergleicht diese. Sobald der Authentisierungsserver 11B einen Teilnehmer findet, dessen aus der Mobilitätsidentität MIP_ID abgeleitete Identität mit der aus der extrahierten Mobilitätsidentität MIP_ID abgeleiteten Identität identisch ist, stellt er dem Heimagenten 11A den dazu gespeicherten Mobilitätsschlüssel (MIP key) zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten des registrierten Teilnehmers zur Verfügung.

```
Extract MIP_ID from Key Request Message
For all NAI MIP_ID‘ = function1 (NAI)
IF MIP_ID‘ = function2 (MIP_ID) THEN OUTPUT MIP_KEY
```

Bei einer weiteren alternativen Ausführungsform stellt der Authentisierungsserver 11B, anstatt dem in Fig. 7 dargestellten Schritt S7, denjenigen Mobilitätsschlüssel bereit, der zu derjenigen äußeren Teilnehmeridentität abgespeichert ist, die aus der Mobilitätsidentität gemäß einer vorgegebenen konfigurierbaren Ableitungsfunktion ableitbar ist.

```
Extract MIP_ID from Key Request Message
For all NAI MIP_ID‘ = NAI
IF MIP_ID‘ = function (MIP_ID) THEN OUTPUT MIP_KEY
```

Das erfindungsgemäße Verfahren eignet sich insbesondere bei WiMax-Mobilfunknetzen.

Figur 10 zeigt ein Diagramm zur Erläuterung des Verbindungsaufbaus für Client-MIP in dem erfindungsgemäßen Verfahren.

Die Teilnehmeridentität des Teilnehmers wird bei einer Ausführungsform des erfindungsgemäßen Verfahrens durch das mobile Teilnehmerendgerät 1 oder durch einen PMIP-Client des Zugangsnetzes 4 gebildet. Die generierte Teilnehmeridentität kann durch einen Authentisierungs-Client 6C oder durch einen Fremdagenten des Zugangsnetzes 4 modifiziert werden.

Patentansprüche

1. Verfahren zum Bereitstellen mindestens eines Mobilitätsschlüssels (MIP_KEY) zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten,
wobei bei einer Netzanmeldung eines Teilnehmers der Mobilitätsschlüssel (MIP_KEY) generiert wird und
wobei eine spätere Registrierung des Teilnehmers bei einem Heimagenten (11A) mittels einer Mobilitätsidentität (MIP_ID) des Teilnehmers erfolgt, die dem generierten Mobilitätsschlüssel (MIP_KEY) in einem Authentisierungsserver (11B) eindeutig zugeordnet wird.

2. Verfahren nach Anspruch 1,
wobei bei der Netzanmeldung mindestens eine Authentisierungsnachricht (Access Authentication), welche eine äußere Teilnehmeridentität des Teilnehmers enthält, von dem Authentisierungsserver empfangen wird.

3. Verfahren nach Anspruch 2,
wobei der Authentisierungsserver (11B) nach Empfang der Authentisierungsnachricht (Access Authentication) mindestens einen Mobilitätsschlüssel (MIP_KEY) für den Teilnehmer generiert und zusammen mit der in der Authentisierungsnachricht enthaltenen äußeren Teilnehmeridentität speichert.

4. Verfahren nach Anspruch 3,
wobei der Authentisierungsserver (11B) zusätzlich eine Sitzungsidentität (CUI) des Teilnehmers zu dem generierten Mobilitätsschlüssel (MIP_KEY) und zu der äußeren Teilnehmeridentität des Teilnehmers speichert.

5. Verfahren nach Anspruch 1,
wobei der Teilnehmer bei der Registrierung bei dem Heimagenten (11A) eine Registrierungsanfragenachricht (MIP RRQ), welche die Teilnehmeridentität des Teilnehmers enthält, an den Heimagenten (11A) sendet.

6. Verfahren nach Anspruch 5,
wobei eine Mobilitätsidentität des Teilnehmers von der in der Registrierungsanfragenachricht (MIP RRQ) enthaltenen Teilnehmeridentität gemäß einer konfigurierbaren Ableitungsfunktion (AF) abgeleitet wird.

7. Verfahren nach Anspruch 5,
wobei eine Mobilitätsidentität des Teilnehmers von einer in der Registrierungsanfragenachricht (MIP_RRQ) enthaltene Teilnehmeridentität und von einer Sitzungsidentität (CUI) des Teilnehmers gemäß einer konfigurierbaren Ableitungsfunktion (AF) abgeleitet wird.

8. Verfahren nach Anspruch 4,
wobei die Sitzungsidentität durch eine Abrechnungsidentität (CUI) des Teilnehmers gebildet wird.

9. Verfahren nach Anspruch 2,
wobei die äußere Teilnehmeridentität durch einen Netzwerkzugriffsidentifizierer NAI (Network Access Identifier) gebildet wird.

10. Verfahren nach Anspruch 2,
wobei die äußere Teilnehmeridentität durch einen anonymen Netzwerkzugriffsidentifizierer NAI gebildet wird.

11 Verfahren nach Anspruch 2,
wobei die äußere Teilnehmeridentität durch einen sitzungsspezifisch gewählten pseudonymen Netzwerkzugriffsidentifizierer NAI gebildet wird.

12. Verfahren nach Anspruch 2,
wobei die äußere Teilnehmeridentität durch einen Hash-Funktionswert einer Mobilitätsidentität gebildet wird.

13. Verfahren nach Anspruch 1,
wobei die Mobilitätsidentität (MIP_ID) durch einen Hash-Funktionswert einer äußeren Teilnehmeridentität gebildet wird.

14. Verfahren nach Anspruch 2,
wobei der Authentisierungsserver (11B) dem Heimagenten (11A) bei Empfang einer Schlüsselanfragenachricht (key request), welche eine Mobilitätsidentität (MIP_ID) enthält, denjenigen generierten Mobilitätsschlüssel (MIP_KEY) bereitstellt, der zu derjenigen äußeren Teilnehmeridentität (NAI) abgespeichert ist, aus der eine identische Mobilitätsidentität (MIP_ID') gemäß einer vorgegebenen konfigurierbaren Ableitungsfunktion (AF) ableitbar ist.

15. Verfahren nach Anspruch 1,
wobei die Teilnehmeridentität durch ein mobiles Teilnehmerendgerät (1) oder durch einen PMIP-Client (6B) eines Zugangsnetzes (4) gebildet wird.

16. Verfahren nach Anspruch 1,
wobei die generierte Teilnehmeridentität von einem Authentisierungsclient (6C) oder einem Fremdagenten (6A) eines Zugangsnetzes (4) modifiziert wird.

17. Verfahren nach Anspruch 2,
wobei die Authentisierungsnachricht (Access Authentication) durch ein Datenpaket gebildet wird dessen Verwaltungsdaten die äußere Teilnehmeridentität enthalten und dessen Nutzdaten eine teilnehmerspezifische innere Teilnehmeridentität enthalten.

18. Verfahren nach Anspruch 16,
wobei die innere Teilnehmeridentität durch einen eindeutigen Teilnehmernamen gebildet wird.

19. Verfahren nach Anspruch 16,
wobei die innere Teilnehmeridentität durch eine vorgegebenen Telefonnummer gebildet wird.

20. Verfahren nach Anspruch 16,
wobei die äußere Teilnehmeridentität eine Adresse zum Routen des Datenpaketes zu dem Authentisierungsserver (11B) bildet.

21. Verfahren nach Anspruch 5,
wobei die Registrierungsanfragenachricht (MIP_RRQ) durch ein Datenpaket gebildet wird, das die äußere Teilnehmeridentität enthält und das eine dem Teilnehmer zugewiesene aktuelle Care-of-Adresse enthält.

22. Verfahren nach Anspruch 13,
wobei die Schlüsselanfragenachricht (key request) durch ein Datenpaket gebildet wird dessen Verwaltungsdaten die Mobilitätsidentität (MIP_ID) enthalten.

23. Verfahren nach Anspruch 14 oder 15,
wobei das Zugangsnetz (4) durch ein Wimax-Netz gebildet wird.

24. Authentisierungsserver zum Bereitstellen eines Mobilitätsschlüssels,
(a) wobei der Authentisierungsserver (11B) bei Empfang einer während einer Netzanmeldung eines Teilnehmers übertragenen Authentisierungsnachricht (access authentication) eine darin enthaltene Teilnehmeridentität (T-ID) des Teilnehmers extrahiert und einen zugehörigen Mobilitätsschlüssel (MIP_KEY) generiert, der zusammen mit der jeweils extrahierten Teilnehmeridentität (T_ID) gespeichert wird,
(b) wobei der Authentisierungsserver (11B) bei einem späteren Empfang einer während einer Registrierung eines Teilnehmers übertragenen Schlüsselanfragenachricht (Key-Request) eine darin enthaltene Mobilitätsidentität (MIP_ID) des Teilnehmers extrahiert und nach einer Mobilitätsidentität (MIP_ID‘) sucht, die gemäß einer konfigurierbaren Ableitungsfunktion

(AF) aus einer der in dem Authentisierungsserver (11B) gespeicherten Teilnehmeridentitäten (T_ID') ableitbar ist, und

(c) wobei der Authentisierungsserver (11B) bei Auffinden einer abgeleiteten Mobilitätsidentität (MIP_ID'), die zu der extrahierten Mobilitätsidentität (MIP_ID) zuordenbar ist, den gespeicherten zugehörigen generierten Mobilitätsschlüssel (MIP_KEY) zur kryptographischen Sicherung von Mobilitätssignalisierungsnachrichten des registrierten Teilnehmers bereitstellt.

25. Authentisierungsserver nach Anspruch 24,
wobei die Teilnehmeridentität (T_ID) eine in Verwaltungsdaten der Authentisierungsnachricht enthaltene äußere Teilnehmeridentität (NAI) ist, die zum Routen der Authentisierungsnachricht zu dem Authentisierungsserver vorgesehen ist.

26. Authentisierungsserver nach Anspruch 24,
wobei der Authentisierungsserver in einem Heimnetz des Teilnehmers vorgesehen ist.

FIG 1
Stand der Technik

Mobilitätsanbindungstabelle

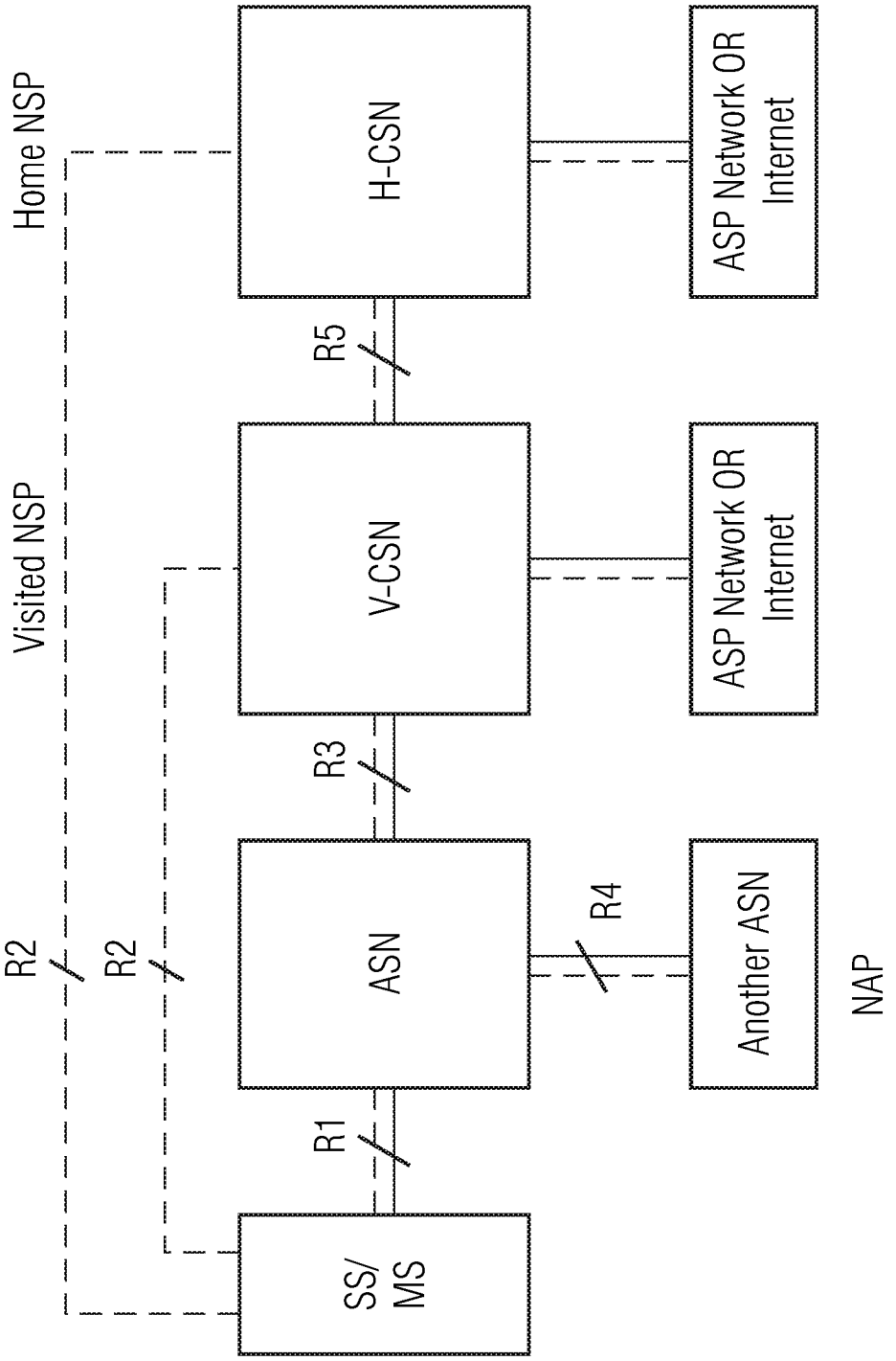
Home Address	Care-of-Address	Lifetime (ms)
131.192.180.42	129.142.23.42	100
213.123.24.140	172.23.142.49	150
...	...	...

FIG 2
Stand der Technik

Besucherliste

Home Address	Home Agent Address	Media Address	Lifetime
131.192.180.42	129.142.23.42	08-00-46-26-75-6A	100
213.123.24.140	172.23.142.49	00-02-B3-77-43-00	150
...	...	...	...

FIG 3
Stand der Technik



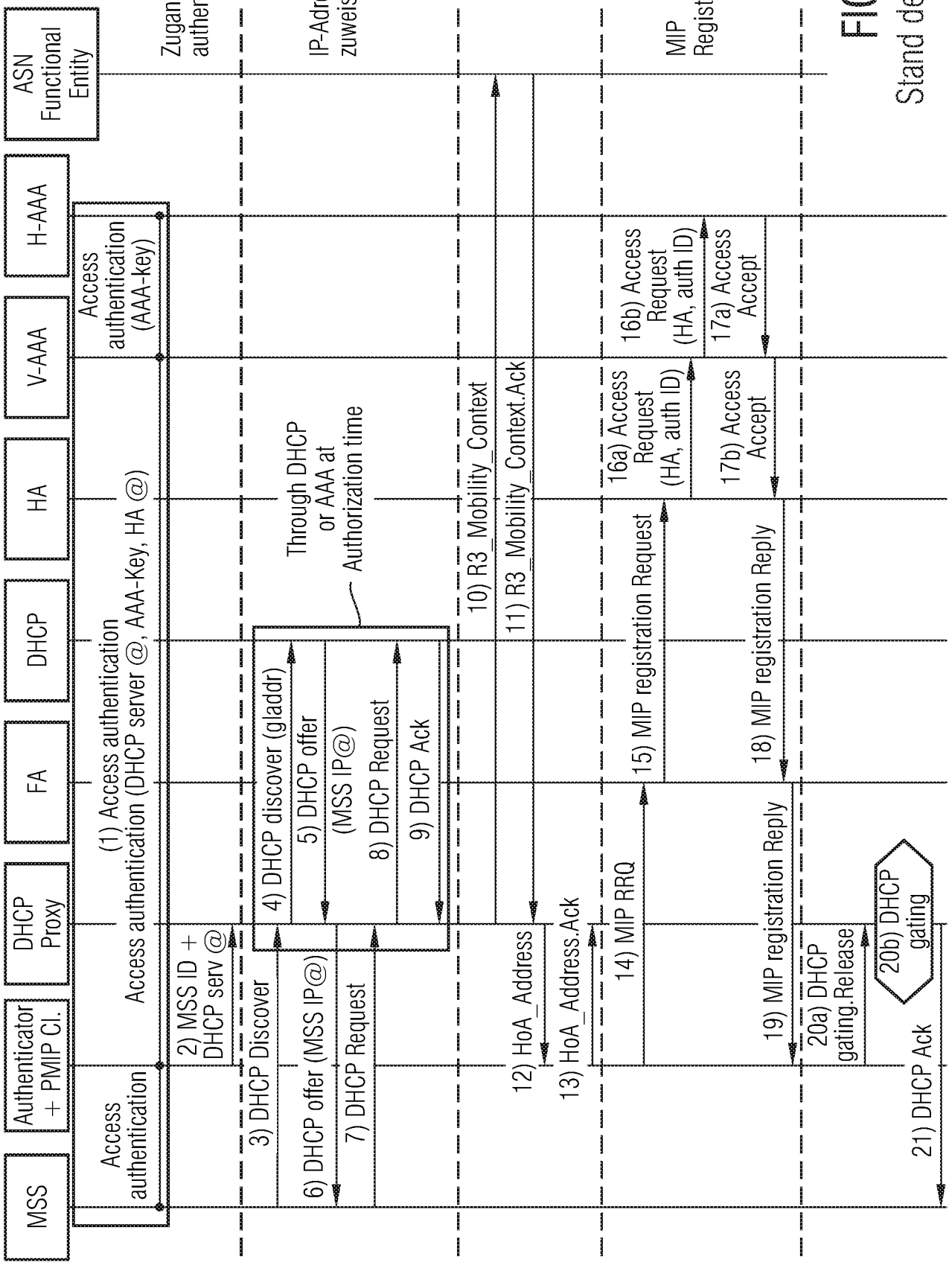


FIG 4
Stand der Technik

FIG 5

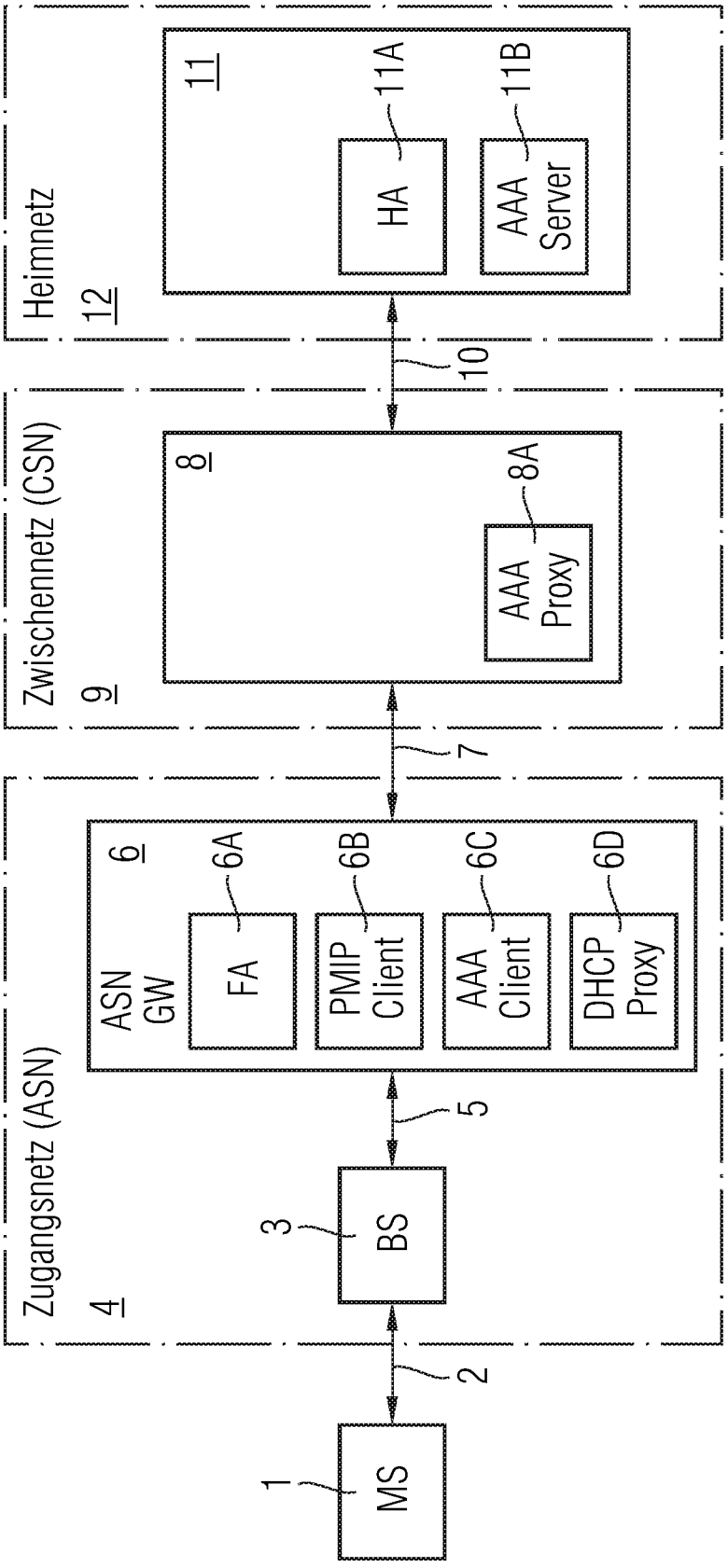

Heimnetz
12
11
11A
HA
11B
AAA Server
10
Zwischennetz (CSN)
9
8
8A
AAA Proxy
7
Zugangsnetz (ASN)
4
ASN GW
6
6A
FA
6B
PMIP Client
6C
AAA Client
6D
DHCP Proxy
5
3
BS
2
1
MS

FIG 6

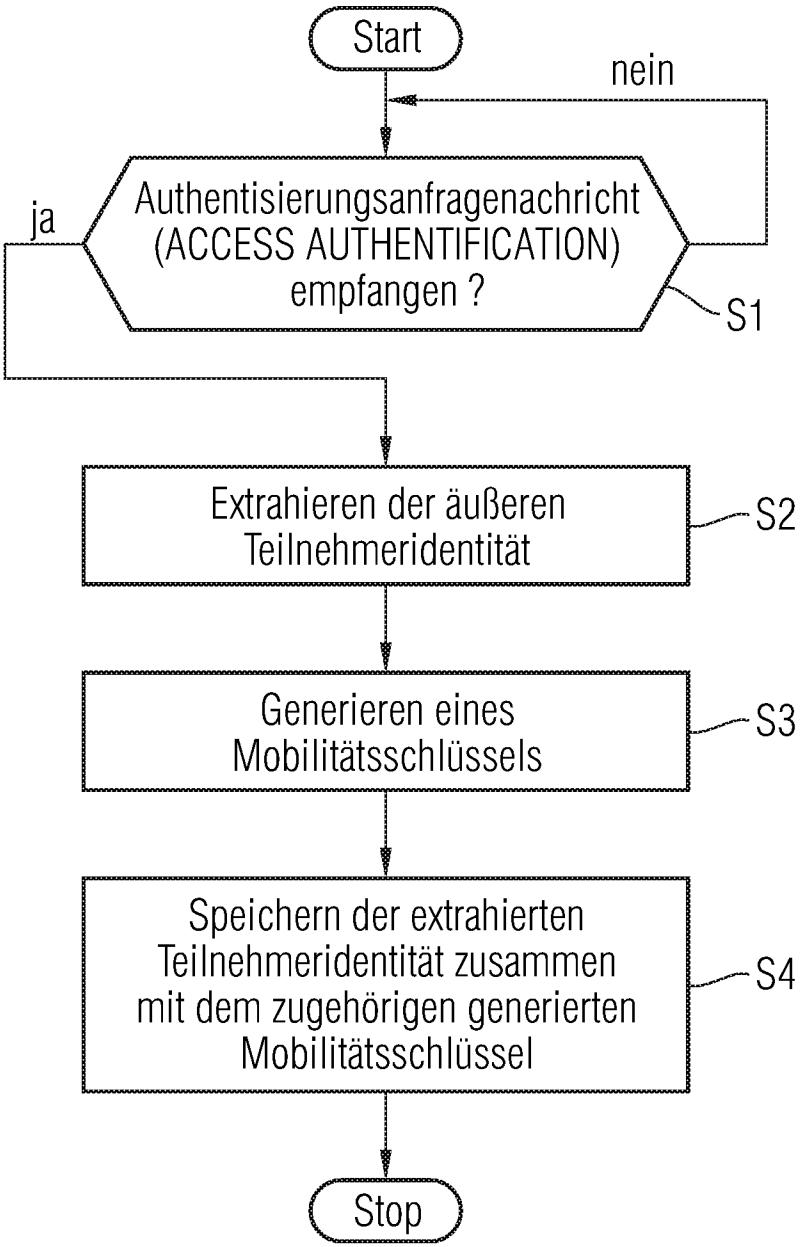

Start
nein
Authentisierungsanfragenachricht (ACCESS AUTHENTIFICATION) empfangen ?
S1
ja
Extrahieren der äußeren Teilnehmeridentität
S2
Generieren eines Mobilitätsschlüssels
S3
Speichern der extrahierten Teilnehmeridentität zusammen mit dem zugehörigen generierten Mobilitätsschlüssel
S4
Stop

FIG 7

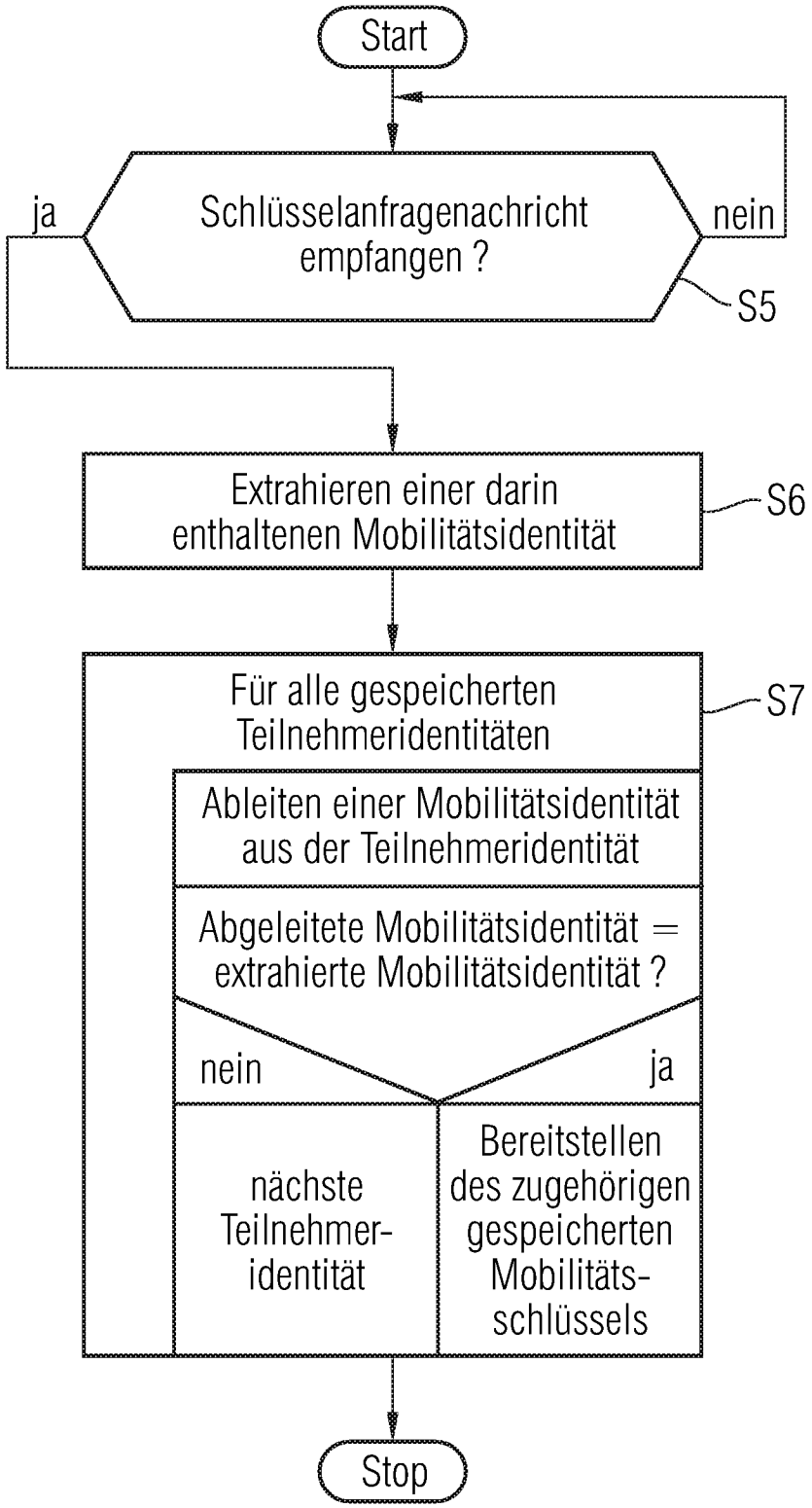

Start
Schlüsselanfragenachricht empfangen ?
ja
nein
S5
Extrahieren einer darin enthaltenen Mobilitätsidentität
S6
Für alle gespeicherten Teilnehmeridentitäten
S7
Ableiten einer Mobilitätsidentität aus der Teilnehmeridentität
Abgeleitete Mobilitätsidentität = extrahierte Mobilitätsidentität ?
nein
ja
nächste Teilnehmer-identität
Bereitstellen des zugehörigen gespeicherten Mobilitäts-schlüssels
Stop

FIG 8

FIG 9A

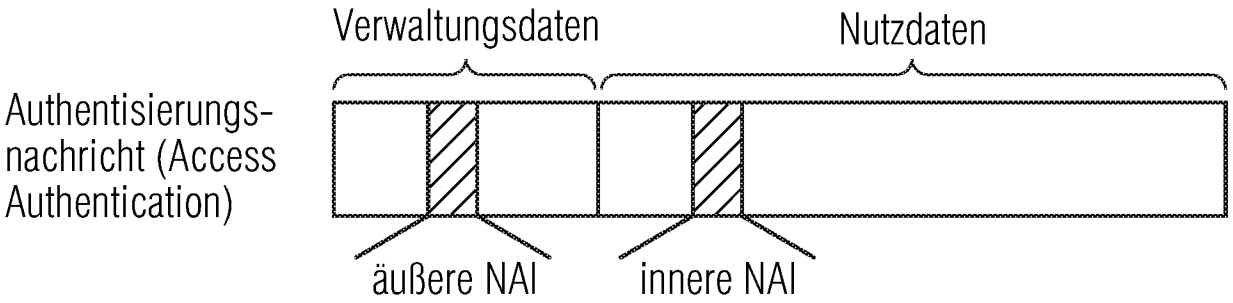


FIG 9B

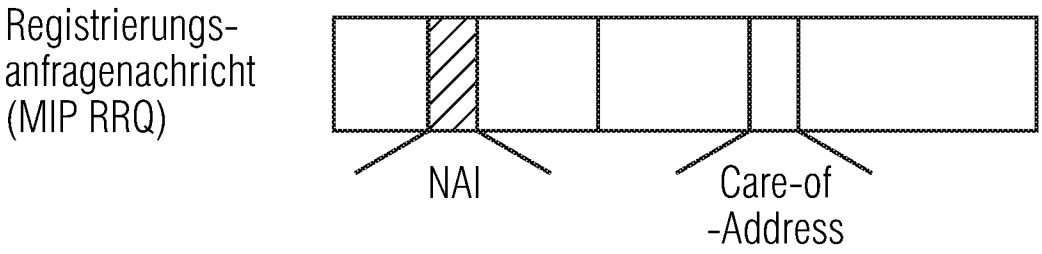


FIG 9C

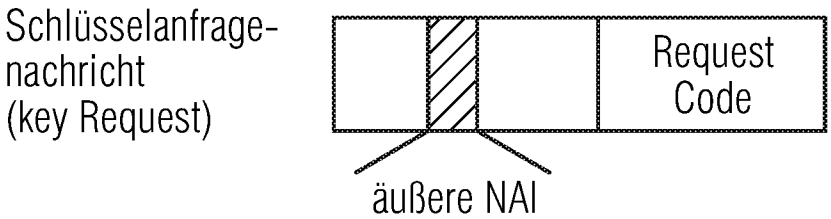
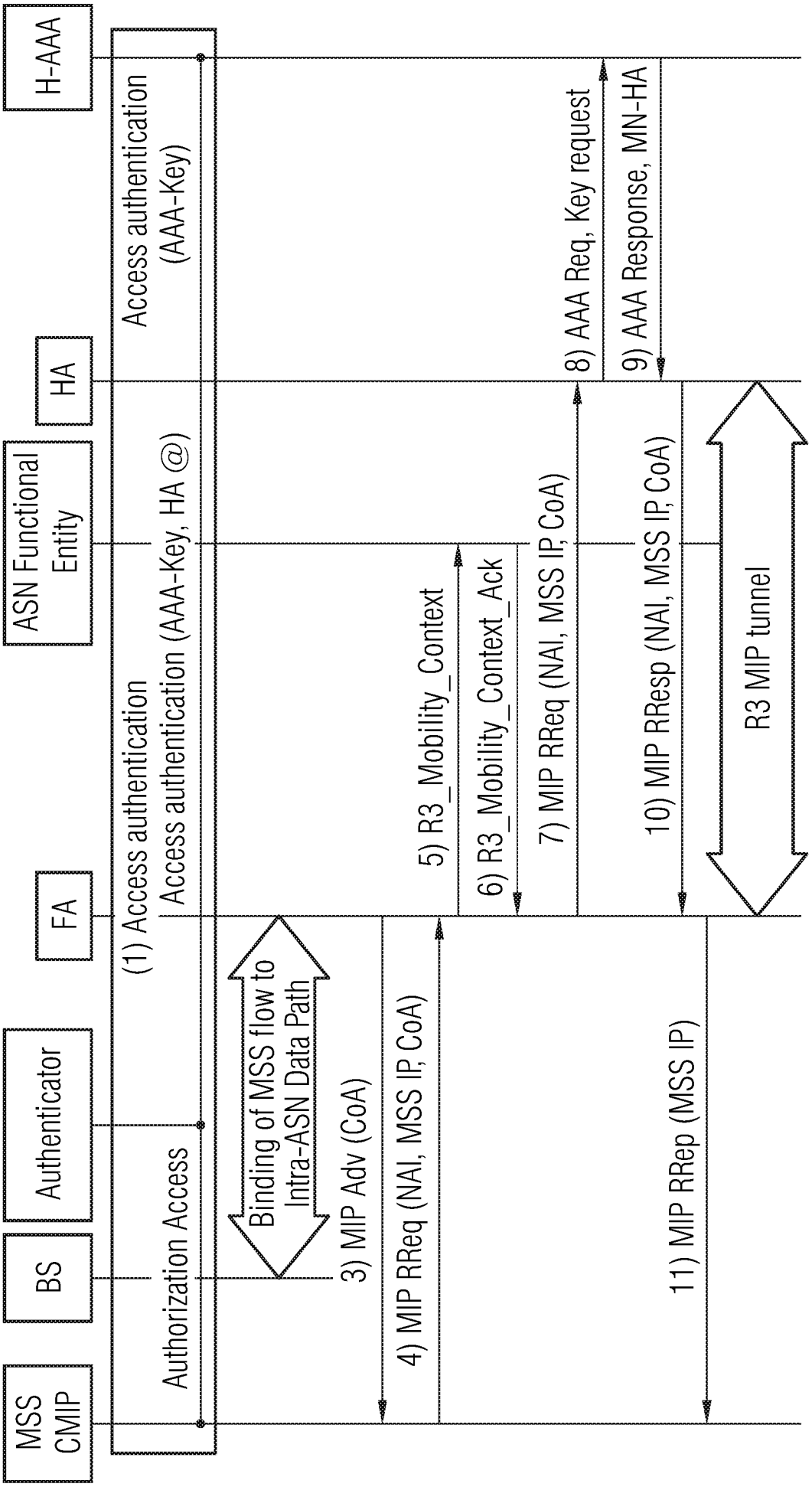


FIG 10


MSS CMIP
BS
Authenticator
FA
ASN Functional Entity
HA
H-AAA
(1) Access authentication
Access authentication (AAA-Key, HA @)
Access authentication (AAA-Key)
Authorization Access
Binding of MSS flow to Intra-ASN Data Path
3) MIP Adv (CoA)
4) MIP RReq (NAI, MSS IP, CoA)
5) R3_Mobility_Context
6) R3_Mobility_Context_Ack
7) MIP RReq (NAI, MSS IP, CoA)
8) AAA Req, Key request
9) AAA Response, MN-HA
10) MIP RResp (NAI, MSS IP, CoA)
11) MIP RRep (MSS IP)
R3 MIP tunnel

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/067955

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/068418 A (NOKIA CORP [FI]; FACCIN STEFANO [US]; LE FRANCK [US]) 6 September 2002 (2002-09-06)	1,5,6, 13,15, 16, 18-22, 24,26
Y	page 1, line 3 - line 24	2-4, 7-12,17, 25
	page 2, line 21 - line 25	
A	page 4, line 8 - line 15	14,23
	page 5, line 1 - line 10	
	page 5, line 29 - page 6, line 28	

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 February 2007	06/03/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Heinrich, Dietmar

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/067955

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"3rd Generation Partnership Project; Technical SPecification Group Services and System Aspects; 3GPP system to WIreless Local Area Network (WLAN) interworking; System description (Release 6)" 3GPP TS 23.234 V6.6.0 (2005-09) TECHNICAL SPECIFICATION, [Online] 1 September 2005 (2005-09-01), pages 1-80, XP002421430 Retrieved from the Internet: URL:http://3gpp.org> [retrieved on 2007-02-21]	2-4, 9-12,17, 25
A	page 8, line 1 - line 13 page 9, line 25 - page 10, line 30 page 11, line 50 - page 12, line 16 page 15, line 26 - page 16, line 8 page 20, line 14 - line 32 page 25, line 1 - line 21 page 29, line 11 - page 30, line 30 page 39, line 1 - page 41, line 27	1,24
Y	ADRANGI INTEL A LIOR BRIDGEWATER SYSTEMS J KORHONEN TELIASONERA J LOUGHNEY NOKIA F: "Chargeable User Identity" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. radext, no. 6, 12 October 2005 (2005-10-12), XP015042642 ISSN: 0000-0004 page 1, line 24 - page 2, line 1 page 3, line 1 - line 29 page 5, line 30 - page 6, line 9	7,8
A	MADJID NAKHJIRI NARAYANAN VENKITARAMAN MOTOROLA LABS: "EAP based Proxy Mobile IP key bootstrapping for WiMAX" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, January 2005 (2005-01), XP015044434 ISSN: 0000-0004 the whole document	1-26

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/067955

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02068418 A	06-09-2002	AU 2002258068 A1	12-09-2002
		US 2002120844 A1	29-08-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2006/067955

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04Q7/38

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L H04Q

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 02/068418 A (NOKIA CORP [FI]; FACCIN STEFANO [US]; LE FRANCK [US]) 6. September 2002 (2002-09-06)	1,5,6, 13,15, 16, 18-22, 24,26
Y	Seite 1, Zeile 3 - Zeile 24	2-4, 7-12,17, 25
A	Seite 2, Zeile 21 - Zeile 25 Seite 4, Zeile 8 - Zeile 15 Seite 5, Zeile 1 - Zeile 10 Seite 5, Zeile 29 - Seite 6, Zeile 28	14,23

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
22. Februar 2007	06/03/2007

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Heinrich, Dietmar

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	"3rd Generation Partnership Project; Technical SPecification Group Services and System Aspects; 3GPP system to WIreless Local Area Network (WLAN) interworking; System description (Release 6)" 3GPP TS 23.234 V6.6.0 (2005-09) TECHNICAL SPECIFICATION, [Online] 1. September 2005 (2005-09-01), Seiten 1-80, XP002421430 Gefunden im Internet: URL:http://3gpp.org> [gefunden am 2007-02-21]	2-4, 9-12,17, 25
A	Seite 8, Zeile 1 - Zeile 13 Seite 9, Zeile 25 - Seite 10, Zeile 30 Seite 11, Zeile 50 - Seite 12, Zeile 16 Seite 15, Zeile 26 - Seite 16, Zeile 8 Seite 20, Zeile 14 - Zeile 32 Seite 25, Zeile 1 - Zeile 21 Seite 29, Zeile 11 - Seite 30, Zeile 30 Seite 39, Zeile 1 - Seite 41, Zeile 27	1,24
Y	ADRANGI INTEL A LIOR BRIDGEWATER SYSTEMS J KORHONEN TELIASONERA J LOUGHNEY NOKIA F: "Chargeable User Identity" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, Bd. radext, Nr. 6, 12. Oktober 2005 (2005-10-12), XP015042642 ISSN: 0000-0004 Seite 1, Zeile 24 - Seite 2, Zeile 1 Seite 3, Zeile 1 - Zeile 29 Seite 5, Zeile 30 - Seite 6, Zeile 9	7,8
A	MADJID NAKHJIRI NARAYANAN VENKITARAMAN MOTOROLA LABS: "EAP based Proxy Mobile IP key bootstrapping for WiMAX" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, Januar 2005 (2005-01), XP015044434 ISSN: 0000-0004 das ganze Dokument	1-26

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2006/067955

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 02068418 A	06-09-2002	AU 2002258068 A1	12-09-2002
		US 2002120844 A1	29-08-2002