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

(10) **DE 603 20 511 T2** 2009.07.23

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 424 868 B1**
(21) Deutsches Aktenzeichen: **603 20 511.9**
(96) Europäisches Aktenzeichen: **03 257 087.1**
(96) Europäischer Anmeldetag: **11.11.2003**
(97) Erstveröffentlichung durch das EPA: **02.06.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **23.04.2008**
(47) Veröffentlichungstag im Patentblatt: **23.07.2009**

(51) Int Cl.[8]: ***H04W 12/06*** (2009.01)
H04W 24/02 (2009.01)
H04W 4/16 (2009.01)

(30) Unionspriorität:
0227777 **28.11.2002** **GB**

(73) Patentinhaber:
Nokia Siemens Networks Oy, Nokia, FI

(74) Vertreter:
Becker, Kurig, Straus, 80336 München

(72) Erfinder:
Tuomi, Jukka, 33730 Tampere, FI; Takamaki, Timo, 33960 Pirkkala, FI

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR

(54) Bezeichnung: **Verfahren, Vorrichtung und System zur Behandlung von einem Authentifizierungsfehler von einem zwischen einem GSM-Netz und einem WLAN-Netz umherstreifenden Teilnehmer**

Beschreibung

[0001] Die Erfindung bezieht sich auf das Ausführen einer Authentifizierung in einem Kommunikationssystem.

[0002] In vielen Kommunikationssystemen, beispielsweise Telefonsystemen, werden Benutzer authentifiziert, bevor ihnen Zugang zu den Ressourcen gewährt wird. Die Ressourcen könnten beispielsweise Datensende- und/oder Datenempfangsdienste, Zugang zu einem Netz oder zu Daten oder Zugang zu Konfigurationsoptionen sein.

[0003] Fig. 1 zeigt ein solches System. Fig. 1 ist ein schematisches Diagramm eines GSM-Kommunikationssystems (Global System for Mobile Communications). Nur die relevanten Teile des Systems sind in Fig. 1 gezeigt. Das in Fig. 1 gezeigte System umfasst ein GSM-Netz, mit dem ein Endgerät **1** kommunizieren kann. Das Netz umfasst ein Heimatregister (HLR) **3**, ein Besucherregister (VLR) **4** und einen Authentifizierungsserver (AS) **5**. Das System umfasst auch ein drahtloses lokales Netz (WLAN) **7**. Das Endgerät kann sowohl im GSM-Netz als auch im WLAN kommunizieren.

[0004] Das HLR und das VLR liefern zusammen Einrichtungen, die primär für eine Ruflenkung und ein Roaming verwendet werden. Das HLR speichert ein Benutzerprofil für jeden Teilnehmer des Netzes **1**, einschließlich von Verwaltungsinformation für den Teilnehmer. Es kann auch Information speichern, die den aktuellen Standort des Endgeräts, das von diesem Teilnehmer verwendet wird, definiert. Der aktuelle Standort des Endgeräts wird typischerweise in Form der Signalisieradresse des VLR, die mit der Mobilstation verknüpft ist, vorgehalten. Wenn das Endgerät im Netz **1** arbeitet, so wird das dann die Adresse des VLR **4** sein. Wenn das Endgerät sich in ein anderes Netz bewegt, dann ist dies die Adresse des VLR dieses Netzes. Es gibt logisch ein einziges HLR in jedem GSM-Netz, obwohl es als eine verteilte Datenbank implementiert sein kann. Das VLR speichert ausgewählte Verwaltungsinformation vom HLR, die für die Rufsteuerung und das Vorsehen von Diensten notwendig ist, für jedes Endgerät, das sich aktuell im geographischen Gebiet befindet, für das das VLR verantwortlicht ist.

[0005] Der Authentifizierungsserver wird verwendet, um ein Endgerät zu authentifizieren, wenn Dienste an es geliefert werden sollen. Ein Weg, auf dem dies erfolgt, ist der folgende. Das Endgerät **2** umfasst ein Teilnehmeridentitätsmodul (SIM) **6**, das einen geheimen Authentifizierungsschlüssel speichert und das eine Authentifizierungsfunktion ausführen kann, die als Operanden diesen Schlüssel und Daten verwendet, die an das SIM vom Endgerät geliefert werden. Das Ergebnis der Funktion wird an das Endgerät zurückgegeben. Der geheime Schlüssel wird auch im Benutzerprofil für den Teilnehmer gespeichert, das in seinem HLR vorgehalten wird. Wenn der Teilnehmer authentifiziert werden soll, werden diesem Endgerät Abfragedaten durch die Einheit geliefert, die wünscht, dass er authentifiziert werden soll. Die Abfragedaten werden an das SIM gegeben, das die Authentifizierungsfunktion aus den Abfragedaten und dem gespeicherten geheimen Schlüssel berechnet. Das Ergebnis dieser Funktion wird an das Netz zurückgegeben, beispielsweise an die Einheit, die wünscht, dass der Teilnehmer authentifiziert wird. Das Ergebnis kann dann zusammen mit den Abfragedaten an den Authentifizierungsserver **5** gegeben werden, der den geheimen Schlüssel für den Teilnehmer vom HLR des Teilnehmers abruft und die Authentifizierungsfunktion dieses Schlüssels und der Abfragedaten berechnet. Wenn das Ergebnis dieser Berechnung zum Ergebnis passt, das an den Authentifizierungsserver geliefert wird, dann gibt der Authentifizierungsserver eine Nachricht an die Einheit zurück, die wünscht, dass der Teilnehmer authentifiziert wird, um anzugeben, dass der Teilnehmer authentifiziert worden ist. Ansonsten ist der Teilnehmer nicht authentifiziert. Ein erweitertes Authentifizierungsprotokoll (Extensible Authentication Protocol, EAP) kann für diesen Zweck verwendet werden.

[0006] Die konventionelle Sequenz der Signalisierung des AS, um Teilnehmerprofilinformation von einem HLR zu erhalten, ist folgende:

A. Der AS überträgt eine MAP_SEND_AUTHENTICATION_INFO-Nachricht (MAP_SENDE_AUTHENTIFIZIERUNGS_INFO-Nachricht) an das HLR.

B. Das HLR antwortet mit einer MAP_SEND_AUTHENTICATION_INFO_ACK-Bestätigungsnachricht (MAP_SENDE_AUTHENTIFZIERUNGS_INFO_ACK-Bestätigungsnachricht).

C. Der AS überträgt eine MAP_RESTORE_DATE-Nachricht (MAP_WIEDERHERSTELLUNGS_DATEN-Nachricht) an das HLR.

D. Das HLR antwortet mit einer MAP_INSERT_SUBSCRIBER_DATA-Nachricht (MAP_EINSCHUB_TEILNEHMER_DATEN-Nachricht), die die Teilnehmerdaten an den AS liefert.

[0007] Ein Beispiel einer Situation, bei der eine Authentifizierung verwendet werden kann, ist die Authentifizierung eines Endgeräts, um helfen zu bestimmen, ob ihm Zugang zu einem drahtlosen lokalen Netz (WLAN) (**7** in Fig. 1) gegeben werden soll. Wenn diese Form der Authentifizierung in Gebrauch ist, wenn ein Teilnehmer versucht, auf das WLAN zuzugreifen, so authentifiziert die Einheit, die den Zugang zum WLAN steuert, die Identität des Teilnehmers mittels des AS des GSM-Netzes. Dies erfordert,

dass der AS das Teilnehmerbenutzerprofil von seinem HLR abruft. Sogar wenn das Endgerät in beiden Netzen arbeiten kann, kann es sein, dass das Endgerät sich nicht in Kommunikation oder Verbindung mit dem GSM-Netz befindet, wenn es versucht, auf das GSM-Netz zuzugreifen: es könnte sich außerhalb des Bereichs des GSM-Netzes befinden oder sein GSM-Sende-Empfänger könnte ausgeschaltet sein.

[0008] In obigem Szenarium wird das GSM-Netz verwendet, um die Authentifizierung eines Endgeräts zu unterstützen, das versucht, Zugang zu einem anderen Netz zu bekommen. Die Kreuznetzauthentifizierung (cross-network authentication) dieses Typs stellt eine etwas andere Situation dar als sie vorausgesehen wurde, als die HLRs des GSM zuerst entwickelt wurden. Bevor die Kreuznetzauthentifizierung dieses Typs verbreitet vorausgesehen wurde, konnte angenommen werden, dass das Endgerät, das zu authentifizieren ist, mit dem GSM-Netz verbunden sein würde. Dies ist jedoch nicht notwendigerweise der Fall. Somit kann vorausgesehen werden, dass Probleme auftreten können beim Erhalten des Teilnehmerprofils von einem HLR, um eine Authentifizierung in diesem Szenarium auszuführen.

[0009] Beispielsweise hat der Anmelder entdeckt, dass HLRs, die von mindestens einem Hersteller hergestellt werden, kein Teilnehmerprofil in Erwiderung auf eine MAP_RESTORE_DATA-Nachricht zurückgeben, es sei denn, dass sie einen Datensatz der Adresse eines VLR für den Teilnehmer speichern, und dass solche HLRs ihre Datensätze des VLR, die mit einem Teilnehmer verbunden sind, nach einer Dauer von ungefähr drei Tagen löschen. Somit kann es mit diesen HLRs, wenn das Endgerät mit dem GSM-Netz in den Tagen vor der Zeit, zu der es versucht, einen Zugang zum WLAN zu erhalten, nicht kommuniziert hat, sein, dass ihm keine VLR zugewiesen ist, und dass somit das HLR das Teilnehmerprofil in Erwiderung auf eine MAP_RESTORE_DATE-Nachricht (MAP_WIEDERHERSTELLUNGS_DATEN-Nachricht) nicht zurückgibt. In diesem Fall würde der AS es nicht authentifizieren können. Einige andere HLRs können so antworten, wie es der AS erfordert, aber sie weisen dies nicht als Standardkonfiguration auf. Es kann sein, dass solche HLRs rekonfiguriert werden müssen, um zu gewährleisten, dass sie das Teilnehmerprofil an den AS liefern.

[0010] Einige HLRs implementieren einen Mechanismus, wodurch ein Teilnehmerkonto aktiviert wird, nachdem die erste GSM-Standortaktualisierung stattfindet. Dies würde ein Problem verursachen, wenn eine SIM-Karte nur für einen WLAN-Authentifizierung verwendet werden würde, das heißt, wenn der Endbenutzer ein SIM für normale GSM-Sprachdienste verwendet und ein anderes für den WLAN-Datenzugang. In diesem Fall würde der Netzbetreiber sich vom Normalfall unterscheidende Instruktionen spezifizieren müssen, wenn die WLAN-SIM-Karte (nur Daten) geliefert wird. Wenn man dem normalen SIM-Karten-Verteilungsverfahren folgt, bei dem die Teilnahme automatisch durch den Endbenutzer aktualisiert wird, wenn er die erste Standortaktualisierung initiiert, würde die Nur-Daten-SIM-Karte nicht aktiviert werden. Das Aktivieren des Daten-SIM würde es erforderlich machen, dass irgend jemand eine Standortaktualisierung unter Verwendung dieses SIM ausführt, bevor es an den Endbenutzer gegeben würde, was einen zusätzlichen Schritt bei der SIM-Karten-Verteilung und einen möglichen Grund für Fehler darstellen würde.

[0011] Die EP 1,209,935 offenbart ein Verfahren einer gefälschten Detektion, bei dem Daten, die sich auf nicht erfolgreiche Authentifizierungsversuche beziehen, in eine Authentifizierungsmisslingensnachricht eingeschlossen werden, die von der bedienenden Umgebung zurück zur Heimatumgebung gesendet wird, die im Heimatregister gespeichert und dann an betrügerische Detektionssysteme für eine Verarbeitung gegeben wird.

[0012] Die US-6,285,882 offenbart ein Verfahren für das Registrieren eines Teilnehmers, bei dem, wenn eine vorbestimmte Anzahl von Teilnehmerverifizierungen ausgeführt worden ist, ein Teilnehmerverifizierungsverfahren angefordert wird.

[0013] Die WO 01/15463 offenbart ein Verfahren für das Handhaben von Teilnehmerdaten, bei dem ein Teilnehmerprofil, das in einer Einheit eines Besuchsnetzes gespeichert ist, durch das Senden von Modifikationen von einer Heimatnetzeinheit an die Einheit des Besuchsnetzes aktualisiert wird. Es besteht somit ein Bedürfnis nach einem verbesserten Verfahren zur Ausführung einer Authentifizierung und insbesondere für das Erhalten der Benutzerprofildaten.

[0014] Gemäß der vorliegenden Erfindung wird ein Verfahren für das Ausführen einer Authentifizierung in einem Kommunikationssystem, das einen Authentifizierungsserver (AS) und einen Benutzerprofilspeicher, der Benutzerprofile für die Benutzer des Kommunikationssystems speichert, umfasst, geliefert, wobei das Verfahren die Übertragung einer Anforderung bezüglich eines Benutzerprofils eines Benutzers vom Authentifizierungsserver an den Benutzerprofilspeicher umfasst, wobei der Benutzerprofilspeicher so ausgebildet ist, dass er an den Authentifizierungsserver eine Fehlernachricht in Erwiderung auf diese Anforderung zurück gibt, wenn sich der Benutzer während einer längeren Zeit nicht in Kommunikation mit dem Netz befindet, von dem das Benutzerprofil einen Teil darstellt, Empfangen einer Antwort auf die Anforderung am AS, Bestimmen ob die Antwort einen Fehler angibt, und wenn die Antwort einen Fehler angibt, Übertragen einer Nachricht vom Authentifizie-

rungsserver an den Benutzerprofilspeicher eines Type, die den Benutzerprofilspeicher veranlasst, ein Standortaktualisierungsverfahren bezüglich des Benutzers auszuführen.

[0015] Gemäß einem zweiten Aspekt der vorliegenden Erfindung wird ein Authentifizierungsserver für das Ausführen einer Authentifizierung in einem Kommunikationssystem geliefert, der einen Benutzerprofilspeicher, der Benutzerprofile für die Benutzer des Kommunikationssystems speichert, umfasst, wobei der Benutzerprofilspeicher so ausgelegt ist, dass er an den Authentifizierungsserver eine Fehlernachricht in Erwiderung auf diese Anforderung zurück gibt, wenn sich der Benutzer während längerer Zeit nicht in Kommunikation mit dem Netz befindet, von dem das Benutzerprofil einen Teil darstellt, wobei der Authentifizierungsserver ausgelegt ist, um eine Authentifizierung auszuführen, folgendes zu tun: Übertragen einer Anforderung bezüglich des Benutzerprofils eines Benutzers vom Authentifizierungsserver an den Benutzerprofilspeicher; Empfangen einer Antwort auf die Anforderung am Authentifizierungsserver; Bestimmen, ob die Antwort einen Fehler angibt; und wenn die Antwort einen Fehler angibt, Übertragen einer Nachricht vom Authentifizierungsserver an den Benutzerprofilspeicher eines Typs, der den Benutzerprofilspeicher veranlasst, ein Standortaktualisierungsverfahren bezüglich des Benutzers auszuführen.

[0016] Gemäß einem dritten Aspekt der vorliegenden Erfindung wird ein Kommunikationssystem geliefert, das umfasst: einen Benutzerprofilspeicher, der Benutzerprofile für die Benutzer des Kommunikationssystems speichert, wobei der Benutzerprofilspeicher so ausgelegt ist, dass er an den Authentifizierungsserver eine Fehlernachricht in Erwiderung auf diese Anforderung zurück gibt, wenn sich der Benutzer längere Zeit nicht in Kommunikation mit dem Netz befunden hat, von dem das Benutzerprofil einen Teil darstellt; und einen Authentifizierungsserver (AS) für das Ausführen einer Authentifizierung im Kommunikationssystem, wobei dieser ausgelegt ist, um die Authentifizierung auszuführen, folgendes zu tun: Übertragen einer Anforderung vom Authentifizierungsserver an den Benutzerprofilspeicher bezüglich des Benutzerprofils eines Benutzers; Empfangen einer Antwort auf die Anforderung an dem AS; Bestimmen, ob die Antwort einen Fehler angibt; und wenn die Antwort einen Fehler angibt, Übertragen einer Nachricht vom Authentifizierungsserver an den Benutzerprofilspeicher eines Typs, die den Benutzerprofilspeicher veranlasst, ein Standortaktualisierungsverfahren in Bezug auf den Benutzer auszuführen.

[0017] Vorzugsweise ist diese Nachricht von einem Typ, der den Benutzerprofilspeicher veranlasst, die Standortaktualisierung auszuführen und nachfolgend das Benutzerprofil des Benutzers an den Authentifizierungsserver zu übertragen.

[0018] Der Benutzerprofilspeicher ist geeigneterweise ein Benutzerprofilspeicher eines GSM-Netzes. Der Benutzerprofilspeicher ist vorzugsweise ein Heimatregister (HLR).

[0019] Der Benutzerprofilspeicher ist geeignet um: in einigen Fällen an den Authentifizierungsserver das Benutzerprofil des Benutzers in Erwiderung auf die Anforderung nach dem Benutzerprofil des Benutzers zurück zu geben, und in anderen Fällen eine Fehlernachricht in Erwiderung auf diese Anforderung an den Authentifizierungsserver zurück zu geben. Diese anderen Umstände umfassen vorzugsweise den Fall, dass sich der Benutzer für eine längere Zeit, beispielsweise ein oder zwei Tage oder mehr, nicht in Kommunikation mit dem Netz befindet, von dem der Benutzerprofilspeicher ein Teil ist. Der Benutzerprofilspeicher kann so ausgelegt sein, dass er an den Authentifizierungsserver das Benutzerprofil des Benutzers in Erwiderung auf diese Anforderung nur dann zurück gibt, wenn er einen Standort für den Benutzer speichert, und dass die anderen Umstände den Fall einschließen, dass der Benutzerprofilspeicher jeglichen Standort des Benutzers aus seinem Datenspeicher gelöscht hat.

[0020] Die Anforderung ist vorzugsweise eine Nachricht gemäß dem MAP-Protokoll (Mobile Application Part, mobiler Anwendungsteil), am besten eine MAP_RESTORE_DATA-Nachricht (MAP_WIEDERHERSTELLUNGS_DATEN-Nachricht).

[0021] Die Nachricht des Typs, der den Benutzerprofilspeicher veranlasst, ein Standortaktualisierungsverfahren in Bezug auf den Benutzer auszuführen, ist vorzugsweise eine Nachricht gemäß dem MAP-Protokoll, am besten eine MAP_UPDATE_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_STANDORT-Nachricht) oder eine MAP_UPDATE_GPRS_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_GPRS_STANDORT-Nachricht).

[0022] Das Verfahren kann umfassen: Empfangen des Benutzerprofils des Benutzers vom Benutzerprofilspeicher am Authentifizierungsserver; und Authentifizieren von Berechtigungen des Benutzers mittels des empfangenen Benutzerprofils; wobei wenn die Berechtigungen korrekt authentifiziert werden, dem Benutzer Zugang zu einer Ressource gewährt wird, und ansonsten dem Benutzer der Zugang zur Ressource verwehrt wird. Die Ressource umfasst geeigneterweise einen Zugang zu einem anderen Netz als demjenigen, von dem der Benutzerprofilspeicher einen Teil darstellt. Das Netz, das ein anderes als das

ist, von dem der Benutzerprofilspeicher einen Teil darstellt, kann beispielsweise ein drahtlose lokales Netz sein.

[0023] Der Benutzer ist vorzugsweise ein Teilnehmer, am besten ein Teilnehmer des Netzes, von dem der Benutzerprofilspeicher einen Teil darstellt. Der Benutzer/Teilnehmer kann mittels eines Endgeräts auf das Netz zugreifen. Vorzugsweise kann das Endgerät eine drahtlose Kommunikation (beispielsweise eine Funkkommunikation) mit dem Netz ausführen. Das Endgerät kann eine Mobilstation sein. Das Endgerät kann ein Mobiltelefon oder eine mobile Datenvorrichtung sein. Das Endgerät kann mit einer Benutzeridentitätseinheit, beispielsweise einem SIM oder USIM (UMTS-SIM (Universal Mobile Telephone System), das Daten einschließt, mittels denen das Endgerät am Authentifizierungsverfahren teilnehmen kann, kommunizieren (und es vorzugsweise enthalten). Das Endgerät kann vorzugsweise in Netzen von mindestens zwei unterschiedlichen Typen kommunizieren. Eines dieser Netze ist vorzugsweise das Netz, von dem der Benutzerprofilspeicher einen Teil darstellt. Das andere ist vorzugsweise die Ressource, zu der ein Zugang gesucht wird.

[0024] Das Authentifizierungsverfahren umfasst vorzugsweise folgende Schritte: der Benutzer sucht Zugang zu einer Ressource zu erhalten; das Endgerät, das vom Benutzer verwendet wird, bildet Authentifizierungsdaten, die mittels des Benutzerprofils des Benutzers authentifiziert werden können und überträgt diese Daten direkt oder indirekt an den Authentifizierungsserver; der Authentifizierungsserver authentifiziert die Authentifizierungsdaten (vorzugsweise in der oben beschriebenen Art); und dem Benutzer wird entsprechend Zugang zur Ressource gewährt oder verwehrt.

[0025] Die vorliegende Erfindung wird nun beispielhaft unter Bezug auf die begleitenden Zeichnungen beschrieben.

[0026] In den Zeichnungen:

[0027] Fig. 1 ist ein schematisches Teildiagramm eines GSM-Kommunikationsnetzes; und

[0028] Fig. 2 zeigt die Signalisierung während der Authentifizierung gemäß einer Ausführungsform der vorliegenden Erfindung.

[0029] Das vorliegende System kann in einem System implementiert werden, das schematisch dasselbe ist, wie das, das in Fig. 1 gezeigt ist. Beim Beschreiben des aktuellen Systems werden äquivalente Komponenten des Systems wie in Fig. 1 angegeben. Im aktuellen System ist jedoch die Funktion des AS von der eines konventionellen AS adaptiert.

[0030] Wie oben angegeben ist, können Probleme auftreten, wenn ein AS ein Teilnehmerprofil von einem HLR bestimmen muss, sich das HLR aber in einem solchen Zustand befindet, dass es kein Profil für den in Frage stehenden Teilnehmer zurück gibt. Ein Weg dies anzusprechen besteht darin, den AS so zu konfigurieren, dass er eine Standortaktualisierung für den Teilnehmer initiiert, wenn die Anforderung nach einem Teilnehmerprofil nicht akzeptabel ist. Dies wird unten detaillierter beschrieben.

[0031] Um zu rekapitulieren, so stellt sich die konventionelle Sequenz der Signalisierung des AS, um eine Teilnehmerprofilinformation von einem HLR zu erhalten, folgendermaßen dar:

A. Der AS überträgt eine MAP_SEND_AUTHENTICATION_INFO-Nachricht (MAP_SENDE_AUTHENTIFIZIERUNGS_INFO-Nachricht) an das HLR.

B. Das HLR antwortet mit einer MAP_SEND_AUTHENTICATION_INFO_ACK-Bestätigungsnachricht (MAP_SENDE_AUTHENTIFZIERUNGS_INFO_ACK-Bestätigungsnachricht).

C. Der AS überträgt eine MAP_RESTORE_DATE-Nachricht (MAP_WIEDERHERSTELLUNGS_DATEN-Nachricht) an das HLR.

D. Das HLR antwortet mit einer MAP_INSERT_SUBSCRIBER_DATA-Nachricht (MAP_EINSCHUB_TEILNEHMER_DATEN-Nachricht), die die Teilnehmerdaten an den AS liefert.

[0032] Wenn sich das HLR in einem solchen Zustand befindet, dass es kein Profil für den in Frage stehenden Teilnehmer zurückgeben wird, so gibt es eine Fehlernachricht in der Stufe D zurück.

[0033] Der AS des aktuellen Systems ist so konfiguriert, dass wenn er versucht, ein Benutzerprofil von einem HLR zu erhalten, er eine Fehlernachricht in Erwiderung auf die Nachricht, die er in Stufe C sendet, empfängt, dann eine Standortaktualisierung für den in Frage stehenden Teilnehmer initiiert. Es wird dann vom HLR erwartet, dass es eine Standortaktualisierung für den Teilnehmer ausführt und das Benutzerprofil des Teilnehmers zurück gibt. Somit finden die folgenden zusätzlichen Schritte statt, nachdem im Schritt D ein Fehler zurückgegeben wurde:

E. Der AS überträgt eine MAP_UPDATE_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_STANDORT-Nachricht) an das HLR.

F. Das HLR führt eine Standortaktualisierung für den Teilnehmer aus und antwortet dem AS mit einer MAP_INSERT_SUBSCRIBER_DATA-Nachricht (MAP_EINSCHUB_TEILNEHMER_DATEN-Nachricht), die die Teilnehmerdaten an den AS liefert.

[0034] Es kann erwartet werden, dass der AS, der eine MAP_UPDATE_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_STANDORT-Nachricht) an das HLR überträgt, Probleme für die Verbindung des Teilnehmers im GSM-Netz verursachen wird. Der AS überträgt jedoch die MAP_UPDATE_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_STANDORT-Nachricht), wenn ein Fehler im Schritt D empfangen wird. Der Grund hinter diesem Fehlersignal ist der, dass das HLR die VLR-Adresse für den Teilnehmer gelöscht hat, da der Teilnehmer nicht mit dem GSM-Netz verbunden worden ist. Somit wird, wenn die Schritte E und F unternommen werden, erwartet, dass der Teilnehmer nicht wirklich mit dem GSM-Netz verbunden ist.

[0035] Die Signalisierschritte in dem Fall, dass ein Fehler im Schritt D empfangen wird, sind in Fig. 2 dargestellt. Diese Figur zeigt auch die Signalisierung zwischen dem AS **5** und der WLAN-Zugangszone **7** (Schritte X und Y). Diese Signalisierung kann das RADIUS-Protokoll verwenden. Schritt X ist die Anforderung von der WLAN-Zugangszone für die Authentifizierung des Teilnehmers. Dies kann die Authentifizierungsdaten und die Abfragedaten, von denen sie abgeleitet wurde, zusammen mit einer Identifikation des Teilnehmers einschließen. Schritt Y ist die Nachricht, die der WLAN-Zugangszone angibt, ob auf der Basis des Ergebnisses der Authentifizierung der Zugang zu gestatten oder zu verneinen ist.

[0036] Das oben beschriebene Verfahren kann es ermöglichen, dass ein GSM-Teilnehmerprofil zuverlässig für eine Authentifizierung des Zugangs zu Diensten verwendet werden kann, wenn der Teilnehmer/das Endgerät nicht mit dem GSM-Netz verbunden ist. Solche Dienste können der Zugang zu einem anderen Netz als dem GSM-Netz sein. GSM-Netze sollten so verstanden werden, dass sie Netze einschließen, die auf abgeleiteten Standards von GSM basieren.

[0037] Die spezifische Nachrichten, die verwendet werden, könnten gegenüber solchen, wie sie oben beschrieben wurden, variieren. Statt einer MAP_UPDATE_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_STANDORT-Nachricht), wie sie in Schritt **5** verwendet wird, könnte eine MAP_UPDATE_GPRS_LOCATION-Nachricht (MAP_AKTUALISIERUNGS_GPRS_STANDORT-Nachricht) verwendet werden. Sie veranlasst auch das HLR, eine Standortaktualisierung für den Teilnehmer auszuführen und muss vom HLR mit einer MAP_INSERT_SUBSCRIBER_DATA-Nachricht (MAP_EINSCHUB_TEILNEHMER_DATEN-Nachricht) beantwortet werden.

[0038] Es sollte angemerkt werden, dass die Signalisierung, die oben ausgeführt wurde, das MAP-Protokoll verwendet. Obwohl andere Signalisierungsprotokolls verwendet werden könnten, ist das MAP-Protokoll vorteilhaft.

[0039] Der Authentifizierungsserver kann Teil des Netzes sein, von dem das HLR einen Teil darstellt (wie in Fig. 1 dargestellt) oder Teil eines anderen Netzes oder es kann sich um eine unabhängige Funktion handeln. Der Authentifizierungsserver kann als eine einzelne Einheit vorgesehen werden, oder er kann als eine Funktion, die zwischen zwei oder mehr physikalischen Einheiten und/oder Standorten verteilt ist, ausgebildet sein.

Patentansprüche

1. Verfahren zum Durchführen einer Authentifizierung in einem Kommunikationssystem (**1**, **7**), umfassend einen Authentifizierungsserver (AS) (**5**), und einen Benutzerprofilspeicher (**3**), der Benutzerprofile für Benutzer des Kommunikationssystems speichert, wobei das Verfahren umfasst:
Übertragen einer Anforderung bezüglich des Benutzerprofils eines Benutzers (C) von dem Authentifizierungsserver an den Benutzerprofilspeicher, wobei der Benutzerprofilspeicher so ausgelegt ist, dass er in Reaktion auf die Anforderung eine Fehlernachricht (D) an den Authentifizierungsserver zurückgibt, wenn der Benutzer für längere Zeit nicht in Kommunikation mit dem Netz stand, von dem das Benutzerprofil ein Teil ist;
Empfangen einer Antwort auf die Anforderung an dem AS;
Bestimmen, ob die Antwort einen Fehler anzeigt; und
dadurch gekennzeichnet, dass
falls die Antwort einen Fehler anzeigt, Übertragen einer Nachricht von dem Authentifizierungsserver an den Benutzerprofilspeicher, die solcher Art ist, dass sie den Benutzerprofilspeicher dazu veranlasst, einen Standortaktualisierungsvorgang bezüglich des Benutzers (E) durchzuführen.

2. Verfahren nach Anspruch 1, wobei die Nachricht solcher Art ist, dass sie den Benutzerprofilspeicher dazu veranlasst, die Standortaktualisierung durchzuführen und anschließend das Benutzerprofil des Benutzers an den Authentifizierungsserver zu übertragen.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Benutzerprofilspeicher ein Benutzerprofilspeicher eines GSM-Netzes ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Benutzerprofilspeicher ein Standortverzeichnis (HLR) ist.

5. Verfahren nach einem der Ansprüche 1 bis 4, wobei der Benutzerprofilspeicher so ausgelegt ist, dass er an den Authentifizierungsserver eine Fehler-

nachricht in Reaktion auf die Anforderung zurückgibt, wenn der Benutzer einen Tag oder länger nicht in Kommunikation mit dem Netzwerk stand, von dem das Benutzerprofil ein Teil ist.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Anforderung eine Nachricht gemäß dem MAP-Protokoll ist.

7. Verfahren nach Anspruch 6, wobei die Anforderung eine MAP_RESTORE_DATA-Nachricht ist.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht, die solcher Art ist, dass sie den Benutzerprofilspeicher veranlasst, einen Standortaktualisierungsvorgang bezüglich des Benutzers durchzuführen, eine Nachricht gemäß dem MAP-Protokoll ist.

9. Verfahren nach dem Anspruch 8, wobei die Nachricht, die solcher Art ist, dass sie den Benutzerprofilspeicher veranlasst, einen Standortaktualisierungsvorgang bezüglich des Benutzers durchzuführen, eine MAP_UPDATE_LOCATION- oder eine MAP_UPDATE_GPRS_LOCATION-Nachricht ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, weiter umfassend:
Empfangen des Benutzerprofils des Benutzers von dem Benutzerprofilspeicher an dem Authentifizierungsserver; und
Authentifizieren von Berechtigungen des Benutzers mittels des empfangenen Benutzerprofils; und wobei
falls die Berechtigungen korrekt authentifiziert werden, dem Benutzer Zugang zu einer Ressource gewährt wird, und andernfalls dem Benutzer der Zugang zu der Ressource verwehrt wird.

11. Verfahren nach Anspruch 10, wobei die Ressource Zugang zu einem anderen Netz (**7**) als dem, von dem der Benutzerprofilspeicher ein Teil ist, einschließt.

12. Verfahren nach Anspruch 11, wobei das andere Netz als das, zu dem der Benutzerprofilspeicher gehört, ein drahtloses lokales Netz ist.

13. Authentifizierungsserver (AS) (**5**) zum Durchführen einer Authentifizierung in einem Kommunikationssystem (**1**, **7**), umfassend einen Benutzerprofilspeicher (**3**), der Benutzerprofile für Benutzer des Kommunikationssystems speichert, wobei der Benutzerprofilspeicher so ausgelegt ist, dass er an den Authentifizierungsserver in Reaktion auf eine Anforderung bezüglich des Benutzerprofils eines Benutzers eine Fehlermeldung (D) zurückgibt, wenn der Benutzer für längere Zeit nicht in Kommunikation mit dem Netz stand, von dem das Benutzerprofil ein Teil ist, wobei der Authentifizierungsserver, um eine Authentifizierung durchzuführen, eingerichtet ist zum:
Übertragen einer Anforderung bezüglich des Benutzerprofils eines Benutzers
(C) von dem Authentifizierungsserver an den Benutzerprofilspeicher;
Empfangen einer Antwort auf die Anforderung an dem AS;
Bestimmen, ob die Antwort einen Fehler anzeigt; und
dadurch gekennzeichnet, dass
falls die Antwort einen Fehler anzeigt, der Authentifizierungsserver eingerichtet ist, eine Nachricht solcher Art von dem Authentifizierungsserver an den Benutzerprofilspeicher zu übertragen, die den Benutzerprofilspeicher dazu veranlasst, einen Standortaktualisierungsvorgang bezüglich des Benutzers (E) durchzuführen.

14. Kommunikationssystem (**1**, **7**), umfassend:
einen Benutzerprofilspeicher, der Benutzerprofile für Benutzer des Kommunikationssystems speichert, wobei der Benutzerprofilspeicher (**3**) so ausgelegt ist, dass er an den Authentifizierungsserver in Reaktion auf eine Anforderung bezüglich des Benutzerprofils eines Benutzers eine Fehlermeldung (D) zurückgibt, wenn der Benutzer für längere Zeit nicht in Kommunikation mit dem Netz stand, von dem das Benutzerprofil ein Teil ist; und
einen Authentifizierungsserver (AS) (**5**) zum Durchführen einer Authentifizierung in dem Kommunikationssystem, der, um die Authentifizierung durchzuführen, eingerichtet ist zum:
Übertragen einer Anforderung bezüglich des Benutzerprofils eines Benutzers
(C) von dem Authentifizierungsserver an den Benutzerprofilspeicher;
Empfangen einer Antwort auf die Anforderung an dem AS;
Bestimmen, ob die Antwort einen Fehler anzeigt; und
dadurch gekennzeichnet, dass
falls die Antwort einen Fehler anzeigt, der Authentifizierungsserver eingerichtet ist, eine Nachricht solcher Art von dem Authentifizierungsserver an den Benutzerprofilspeicher zu übertragen, die den Benutzerprofilspeicher dazu veranlasst, einen Standortaktualisierungsvorgang bezüglich des Benutzers (E) durchzuführen.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

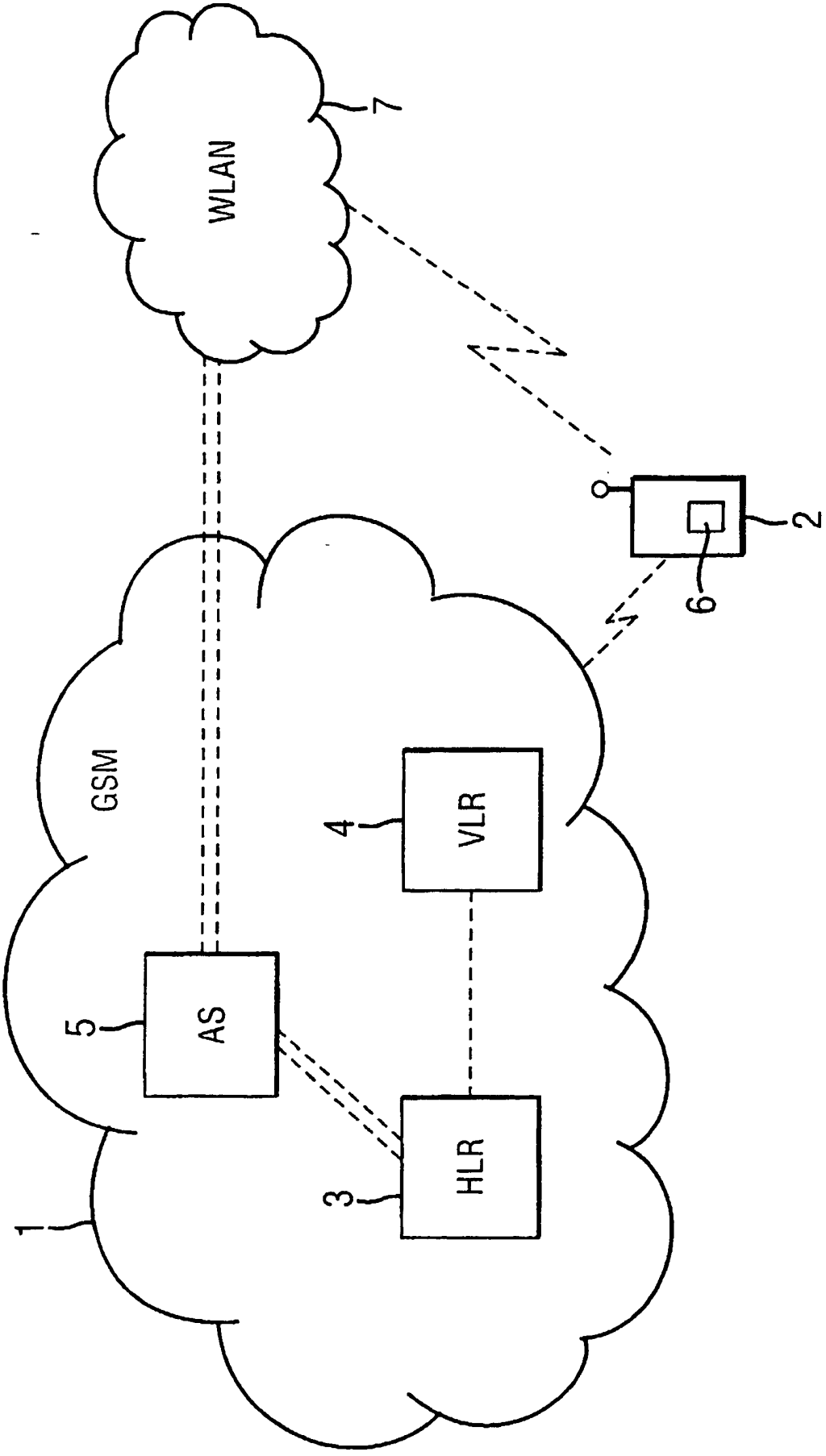
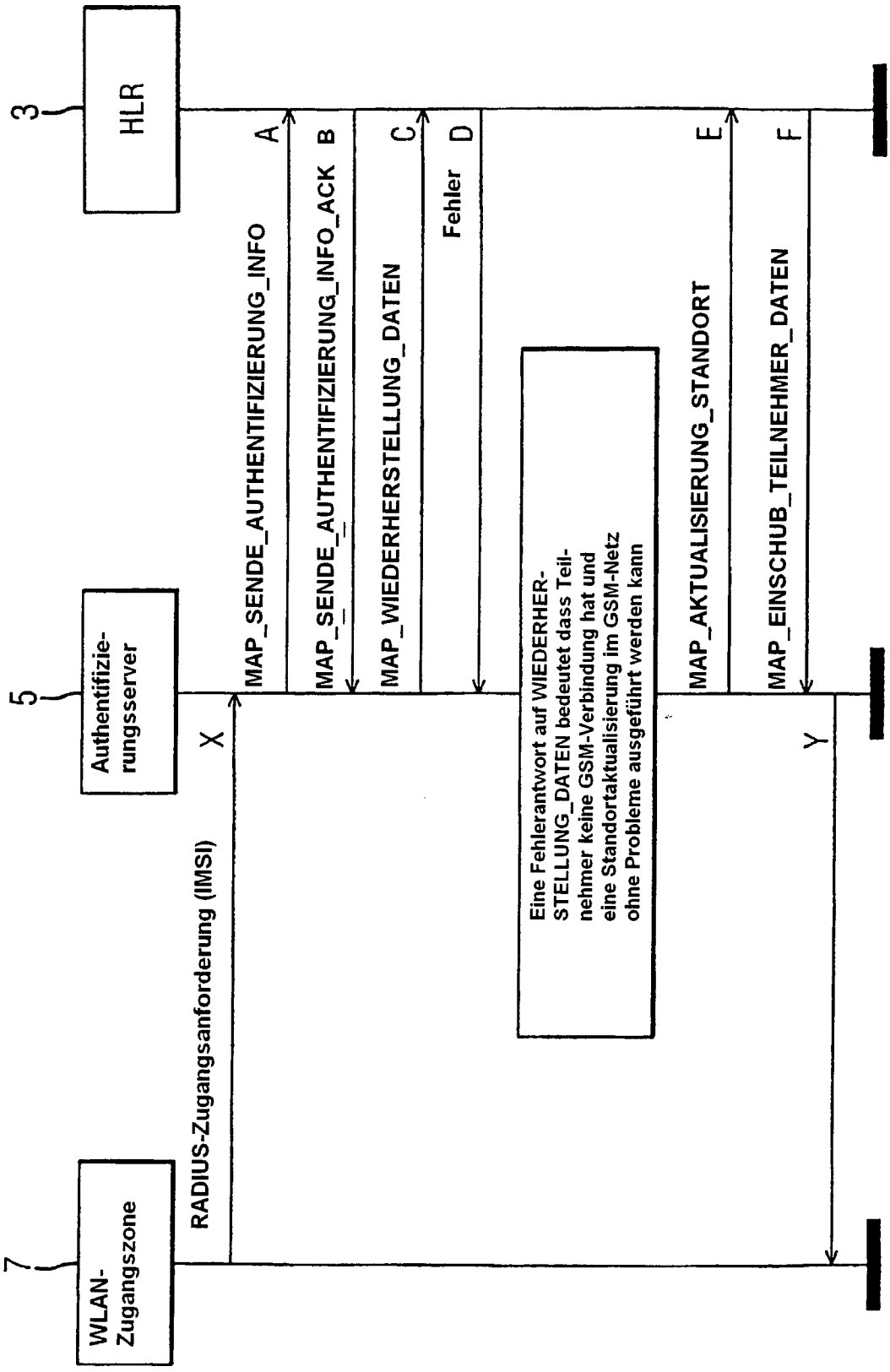


FIG. 2


3
HLR
5
Authentifizierungsserver
7
WLAN-Zugangszone
MAP_SENDE_AUTHENTIFIZIERUNG_INFO
A
MAP_SENDE_AUTHENTIFIZIERUNG_INFO_ACK
B
MAP_WIEDERHERSTELLUNG_DATEN
C
Fehler
D
MAP_AKTUALISIERUNG_STANDORT
E
MAP_EINSCHUB_TEILNEHMER_DATEN
F
RADIUS-Zugangsanforderung (IMSI)
X
Y
Eine Fehlerantwort auf WIEDERHERSTELLUNG_DATEN bedeutet dass Teilnehmer keine GSM-Verbindung hat und eine Standortaktualisierung im GSM-Netz ohne Probleme ausgeführt werden kann