



(10) **DE 10 2014 014 078 A1** 2016.03.24

(12)

Offenlegungsschrift

(21) Aktenzeichen: **10 2014 014 078.4**

(22) Anmeldetag: **23.09.2014**

(43) Offenlegungstag: **24.03.2016**

(51) Int Cl.: **H04W 48/08 (2009.01)**
H04W 8/18 (2009.01)

(71) Anmelder:

Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:

**Ahrens, Carsten, 81929 München, DE; Müller,
Bernd, 81825 München, DE; Dinger, Jens, 81827
München, DE; Morawietz, Andreas, 81377
München, DE; Huber, Ulrich, 81475 München, DE**

(56) Ermittelter Stand der Technik:

US 2014 / 0 057 558 A1

US 2014 / 0 066 011 A1

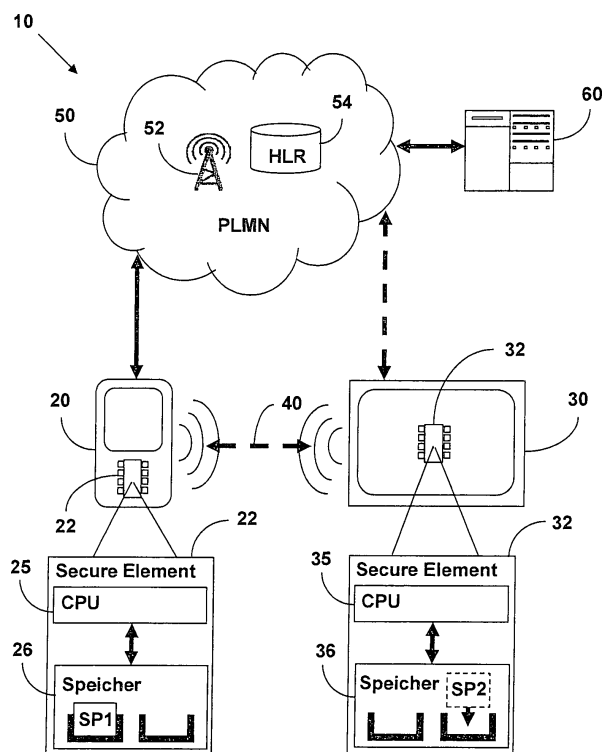
US 2014 / 0 206 313 A1

Rechercheantrag gemäß § 43 Abs. 1 Satz 1 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Vorrichtungen zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät**

(57) Zusammenfassung: Es werden ein Verfahren und ein System zum Bereitstellen eines Subskriptionsprofils (SP2) auf einem mobilen Endgerät (30) zur Kommunikation über ein Mobilfunknetzwerk bereitgestellt. Dabei umfasst das Verfahren die folgenden Schritte: das Einbuchen eines ersten mobilen Endgeräts (20) mit einem ersten Subskriptionsprofil (SP1) in ein Mobilfunknetzwerk (50); das Herunterladen eines zweiten Subskriptionsprofils (SP2) über das Mobilfunknetzwerk (50) auf das erste mobile Endgerät (20); und das Weiterleiten des zweiten Subskriptionsprofils (SP2) vom ersten mobilen Endgerät (20) über einen Kommunikationskanal (40) an ein zweites mobiles Endgerät (30).



Beschreibung**Gebiet der Erfindung**

[0001] Die Erfindung betrifft die Kommunikation über Mobilfunknetze im Allgemeinen und insbesondere Verfahren und Vorrichtungen zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät zur Kommunikation über ein Mobilfunknetz.

Hintergrund der Erfindung

[0002] Das Kommunizieren mittels eines mobilen Endgeräts, beispielsweise mittels eines Mobiltelefons, über ein Mobilfunknetzwerk (auch als PLMN [Public Land Mobile Network] bezeichnet), das von einem Netzbetreiber (auch als MNO [Mobile Network Operator] bezeichnet) betrieben wird, erfordert in der Regel, dass das mobile Endgerät mit einem Sicherheitselement bzw. Teilnehmeridentifikationsmodul, beispielsweise in Form einer SIM-Karte, zur sicheren Aufnahme von Subskriptionsberechtigungsdaten ("Subscription Credentials") ausgestattet ist, die in der Regel Teil eines Subskriptionsprofils sind und den Benutzer des mobilen Endgeräts gegenüber dem Mobilfunknetzwerk eindeutig identifizieren und authentisieren. Derartige Subskriptionsberechtigungsdaten, beispielsweise eine IMSI (International Mobile Subscriber Identity) und ein Authentisierungsschlüssel K_i , sind in der Vergangenheit üblicherweise im Rahmen einer sogenannten "Personalisierung" in der sicheren Umgebung des Sicherheitselementherstellers auf dem Sicherheitselement hinterlegt worden.

[0003] Während in der Vergangenheit die große Mehrzahl von Sicherheitselementen in Form von SIM-Karten in einem mobilen Endgerät einfach ausgetauscht werden konnte, gibt es seit einiger Zeit mehr und mehr Sicherheitselemente, die fest in einem mobilen Endgerät verbaut werden. Ein solches fest in einem mobilen Endgerät verbauten Sicherheitselement, das dem Fachmann insbesondere unter dem Begriff "Embedded SIM" oder "Embedded UICC (eUICC)" bekannt ist, kann in der Regel nicht mehr in einer sicheren Umgebung beim Hersteller des Sicherheitselements personalisiert werden, da insbesondere das Einsatzgebiet des Sicherheitselements nicht im Voraus bekannt ist.

[0004] Somit besteht ein Bedarf nach verbesserten Verfahren und Vorrichtungen zum Personalisieren eines mobilen Endgeräts, d. h. zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät, insbesondere dem Sicherheitselement davon.

Zusammenfassung der Erfindung

[0005] Die vorstehende Aufgabe wird gemäß der vorliegenden Erfindung durch den jeweiligen Gegen-

stand der unabhängigen Ansprüche gelöst. Bevorzugte Ausgestaltungen der Erfindung werden in den abhängigen Ansprüchen definiert.

[0006] Gemäß einem ersten Aspekt der Erfindung wird ein Verfahren zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät zur Kommunikation über ein Mobilfunknetzwerk bereitgestellt. Dabei umfasst das Verfahren die folgenden Schritte: das Einbuchen eines ersten mobilen Endgeräts mit einem ersten Subskriptionsprofil in ein Mobilfunknetzwerk; das Herunterladen eines zweiten Subskriptionsprofils über das Mobilfunknetzwerk auf das erste mobile Endgerät; und das Weiterleiten des zweiten Subskriptionsprofils vom ersten mobilen Endgerät über einen Kommunikationskanal an ein zweites mobiles Endgerät.

[0007] Vorzugsweise umfasst das Verfahren nach dem Schritt des Weiterleitens des zweiten Subskriptionsprofils vom ersten mobilen Endgerät über den Kommunikationskanal an das zweite mobile Endgerät den weiteren Schritt des Einbuchens des zweiten mobilen Endgeräts mit dem zweiten Subskriptionsprofil in ein Mobilfunknetzwerk.

[0008] Gemäß bevorzugter Ausführungsformen der Erfindung ist das Mobilfunknetzwerk, in das sich das zweite mobile Endgerät mit dem zweiten Subskriptionsprofil einbucht, das Mobilfunknetzwerk, über das das zweite Subskriptionsprofil auf das erste mobile Endgerät heruntergeladen worden ist.

[0009] Vorzugsweise ist der Kommunikationskanal zwischen dem ersten mobilen Endgerät und dem zweiten mobilen Endgerät ein NFC-Kommunikationskanal, ein WiFi-Kommunikationskanal, ein Bluetooth-Kommunikationskanal, ein optischer Kommunikationskanal und/oder ein akustischer Kommunikationskanal.

[0010] Gemäß bevorzugter Ausführungsformen der Erfindung wird das zweite Subskriptionsprofil von einem Server über das Mobilfunknetzwerk auf das erste mobile Endgerät heruntergeladen.

[0011] Vorzugsweise ist der logische Kommunikationskanal zwischen dem Server und dem zweiten mobilen Endgerät kryptographisch gesichert.

[0012] Gemäß bevorzugter Ausführungsformen der Erfindung ist der logische Kommunikationskanal zwischen dem Server und dem zweiten mobilen Endgerät dadurch kryptographisch gesichert, dass das zweite Subskriptionsprofil vom Server mit einem Schlüssel verschlüsselt wird, der auf dem Server in Verbindung mit einem Identifier des zweiten mobilen Endgeräts und/oder eines Sicherheitselements des zweiten mobilen Endgeräts hinterlegt ist.

[0013] Gemäß einem zweiten Aspekt der Erfindung wird ein System zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät zur Kommunikation über ein Mobilfunknetzwerk bereitgestellt. Dabei umfasst das System: ein erstes mobiles Endgerät, das dazu ausgestaltet ist, sich mit einem ersten Subskriptionsprofil in ein Mobilfunknetzwerk einzubuchen; einen Server zum Herunterladen eines zweiten Subskriptionsprofils über das Mobilfunknetzwerk auf das erste mobile Endgerät; und ein zweites mobiles Endgerät, das dazu ausgestaltet ist, dass das zweite Subskriptionsprofil vom ersten mobilen Endgerät über einen Kommunikationskanal an das zweite mobile Endgerät weitergeleitet wird.

[0014] Wie der Fachmann erkennt, lassen sich die vorstehend beschriebenen bevorzugten Ausgestaltungen sowohl im Rahmen des ersten Aspekts der Erfindung, d. h. im Rahmen des Verfahrens zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät zur Kommunikation über ein Mobilfunknetzwerk, als auch im Rahmen des zweiten Aspekts der Erfindung, d. h. im Rahmen eines Systems zum Bereitstellen eines Subskriptionsprofils auf einem mobilen Endgerät zur Kommunikation über ein Mobilfunknetzwerk, vorteilhaft implementieren.

[0015] Weitere Merkmale, Vorteile und Aufgaben der Erfindung gehen aus der folgenden detaillierten Beschreibung mehrerer Ausführungsbeispiele und Ausführungsalternativen hervor. Es wird auf die Zeichnungen verwiesen, in denen zeigen:

[0016] Fig. 1 eine schematische Darstellung eines Kommunikationssystems mit einem Mobilfunksystem in Kommunikation mit einem ersten mobilen Endgerät und einem zweiten mobilen Endgerät, die unterschiedliche Aspekte der vorliegenden Erfindung illustriert, und

[0017] Fig. 2 eine schematische Darstellung eines bevorzugten Ablaufs beim Bereitstellen eines Subskriptionsprofils auf dem zweiten mobilen Endgerät von Fig. 1.

[0018] Fig. 1 zeigt eine schematische Darstellung der Komponenten eines Kommunikationssystems **10** sowie einige der Kommunikationsverbindungen zwischen diesen Komponenten, die unterschiedliche Aspekte der vorliegenden Erfindung illustriert. Obgleich in der nachstehenden detaillierten Beschreibung auf ein "mobiles" Endgerät Bezug genommen wird, wird der Fachmann erkennen, dass die vorliegende Erfindung vorteilhaft im Zusammenhang mit jeder Art von Endgerät implementiert werden kann, das dazu ausgestaltet ist, über ein mobiles oder zelluläres Kommunikationsnetzwerk zu kommunizieren, also auch mit Endgeräten, deren Standort sich praktisch nicht ändert. Mit anderen Worten: das hierin verwendete Attribut "mobil" bezieht sich auf die Fä-

higkeit des Endgeräts über ein mobiles oder zelluläres Kommunikationsnetzwerk zu kommunizieren.

[0019] In Fig. 1 sind beispielhaft ein erstes mobiles Endgerät **20** und ein zweites mobiles Endgerät **30** dargestellt. Vorzugsweise verfügen das erste mobile Endgerät **20** und das zweite mobile Endgerät **30** jeweils über ein Sicherheitselement ("Secure Element") **22** bzw. **32** zum sicheren Speichern und Verarbeiten von Daten, die beispielsweise das erste mobile Endgerät **20** und das zweite mobile Endgerät **30** in einem Mobilfunknetz eindeutig identifizieren.

[0020] Wie dies in Fig. 1 angedeutet ist, handelt es sich bei dem ersten mobilen Endgerät **20** vorzugsweise um ein Smartphone und bei dem zweiten mobilen Endgerät **30** um einen Tablet-Computer. Der Fachmann wird jedoch erkennen, dass das erste mobile Endgerät **20** und das zweite mobile Endgerät **30** gemäß der vorliegenden Erfindung ebenfalls in Form von anderen Vorrichtungen implementiert werden können, die dazu eingerichtet sind, über ein Mobilfunknetzwerk zu kommunizieren, wie beispielsweise ein Notebook, ein TV-System, eine Set-Top-Box, ein Verkaufsautomat, ein Kraftfahrzeug, eine Überwachungskamera, eine Sensorvorrichtung und dergleichen.

[0021] Gemäß bevorzugter Ausführungsformen der Erfindung sind das Sicherheitselement **22** und das Sicherheitselement **32** als eine eUICC (embedded Universal Integrated Circuit Card) mit einer darauf implementierten SIM-Applikation ausgestaltet, d. h. als ein Sicherheitselement, das fester Bestandteil des ersten mobilen Endgeräts **20** bzw. des zweiten mobilen Endgeräts **30** ist und in einem Mobilfunknetzwerk für die eindeutige und sichere Identifizierung des Benutzers bzw. Teilnehmers und für die Bereitstellung unterschiedlicher Funktionen und Mehrwertdienste verwendet wird. Alternativ können das Sicherheitselement **22** und/oder das Sicherheitselement **32** als eine UICC (Universal Integrated Circuit Card) oder SIM-Karte (Subscriber Identity Module) ausgestaltet sein, die dem Fachmann als eine der zurzeit am häufigsten verwendeten Formen eines Sicherheitselements bekannt ist. Der Fachmann wird jedoch erkennen, dass andere Arten von Sicherheitselementen, die je nach Generation und Typ des zugrunde liegenden Mobilfunkstandards als USIM, R-UIM, ISIM und dergleichen bezeichnet werden, ebenfalls von der vorliegenden Erfindung umfasst werden.

[0022] Gemäß weiterer bevorzugter Ausführungsformen der Erfindung können das Sicherheitselement **22** und/oder das Sicherheitselement **32** als eine Kombination aus Hard- und Softwarekomponenten in einem vertrauenswürdigen Teil eines Betriebssystems einer zentralen Prozessoreinheit des ersten mobilen Endgeräts **30** bzw. des zweiten mobilen Endgeräts **30** ausgebildet sein, die dem Fachmann auch als gesi-

cherte Laufzeitumgebung ("Trusted Execution Environment"; TEE) bekannt ist. Das Sicherheitselement **22** und/oder das Sicherheitselement **32** können dann beispielsweise innerhalb einer solchen gesicherten Laufzeitumgebung des ersten mobilen Endgeräts **20** bzw. des zweiten mobilen Endgeräts **30** in Form von darin ablaufenden Programmen, sogenannten Trustlets® ausgebildet sein.

[0023] Das erste mobile Endgerät **20** und das zweite mobile Endgerät **30** sind dazu ausgestaltet, über die Luftschnittstelle mit einem Mobilfunknetzwerk **50** (auch kurz als "Mobilfunknetz" oder als "Public Land Mobile Network" [PLMN] bezeichnet) zu kommunizieren. Hierzu verfügen das erste mobile Endgerät **20** und das zweite mobile Endgerät **30** in der Regel jeweils über eine geeignet ausgestaltete Antenne (in **Fig. 1** nicht dargestellt) zum Senden und Empfangen von Radiowellen.

[0024] Nachstehend werden bevorzugte Ausführungsformen der Erfindung im Zusammenhang mit einem Mobilfunknetzwerk **50** gemäß dem GSM-Standard ("Global Standard for Mobile Communications") beschrieben, der in einer Vielzahl von ETSI-Spezifikationen spezifiziert ist. Der Fachmann wird jedoch erkennen, dass die vorliegende Erfindung auch im Zusammenhang mit anderen Mobilfunknetzen vorteilhaft eingesetzt werden kann. Derartige Netze umfassen Mobilfunknetze der dritten Generation (3GPP), wie UMTS (Universal Mobile Telecommunications System), Mobilfunknetze der vierten Generation (4G), wie LTE (Long Term Evolution), sowie andere Mobilfunknetze, wie CDMA und dergleichen.

[0025] Wie dies dem Fachmann bekannt ist, umfasst ein gemäß dem GSM-Standard aufgebautes Mobilfunknetz bzw. PLMN im Allgemeinen ein BSS ("Base Station Subsystem"), das aus einer Vielzahl von BTS ("Base Transceiver Station") besteht, die jeweilige Funkzellen des PLMN definieren und mit einem BSC ("Base Station Controller") verbunden sind. Üblicherweise handelt es sich bei dem BSC um einen einer Vielzahl von BSC, die mit einem gemeinsamen MSC ("Mobile Switching Center") kommunizieren. Häufig ist eine lokale Datenbank, die VLR ("Visitor Location Register") genannt wird, Teil des MSC, um Informationen über die Mobilfunkteilnehmer vorzuhalten, die sich momentan in den Funkzellen befinden, die von einem MSC versorgt werden (d. h. der von einem MSC abgedeckte Bereich). Das MSC stellt im Wesentlichen dieselbe Funktionalität wie eine Vermittlungsstelle im Festnetz (publicswitched telephone network; PSTN) bereit und steht in Kommunikation mit einem HLR ("Home Location Register"), bei dem es sich um die primäre Datenbank des PLMN handelt, in der Informationen zur Anmeldung bzw. Authentisierung der Mobilfunkteilnehmer gespeichert sind. Hierzu hat das HLR üblicherweise Zugriff auf ein AUC ("Authentication Center"). Wie dies dem Fach-

mann bekannt ist, können die Kommunikationsverbindungen zwischen den vorstehend beschriebenen Komponenten eines PLMNs auf proprietären und/oder offenen Standards basieren. Die verwendeten Protokolle können beispielsweise SS7- oder IP-basiert sein. Wie die Netzwerkkomponenten als separate oder zusammengefasste Einheiten ausgebildet sind und wie die Schnittstellen zwischen diesen Komponenten ausgebildet sind, ist Sache des MNO, so dass die vorstehende Beschreibung lediglich als beispielhaft zu verstehen ist.

[0026] Der Fachmann wird erkennen, dass, obgleich die vorstehend beschriebenen Funktionseinheiten eines herkömmlichen Mobilfunknetzes gemäß dem GSM-Standard in anderen oder zukünftigen Mobilfunkstandards andere Namen aufweisen können, die zugrundeliegenden Prinzipien im Wesentlichen gleich sind und diese daher von der Erfindung ebenfalls umfasst werden. Der Übersichtlichkeit halber sind von den vorstehend beschriebenen Komponenten eines Mobilfunknetzes lediglich die folgenden in der schematischen Darstellung von **Fig. 1** gezeigt: ein beispielhaftes BTS **52** sowie ein HLR **54** für das Mobilfunknetz **50**.

[0027] Wie sich dies **Fig. 1** entnehmen lässt, steht das Mobilfunknetz **50** zumindest zeitweise in Kommunikation mit einem Hintergrundsystem **60**, vorzugsweise in Form eines geeignet ausgestalteten "Subscription Management" Servers (SM Server), wie dies nachstehend im Detail beschrieben wird.

[0028] Wie sich dies den jeweils vergrößerten Ansichten der Sicherheitselemente **22** und **32** in **Fig. 1** entnehmen lässt, umfassen diese vorzugsweise jeweils eine zentrale Verarbeitungseinheit bzw. einen zentralen Prozessor ("central processing unit"; CPU) **25** bzw. **35**. Vorzugsweise ist der Prozessor **25** bzw. **35** derart ausgestattet, dass Applikationen auf dem Prozessor **25** bzw. **35** ausgeführt werden können, die vorzugsweise zumindest einige der Features zum Bereitstellen eines Subskriptionsprofils auf dem zweiten mobilen Endgerät **30** bereitstellen, wie dies nachstehend im Zusammenhang mit **Fig. 2** detailliert beschrieben wird. Derartige Applikationen sind vorzugsweise in Form von Java Applets implementiert.

[0029] Das Sicherheitselement **22** und das Sicherheitselement **32** umfassen vorzugsweise ferner jeweils eine Speichereinheit **26** bzw. **36**, die vorzugsweise als eine nicht-flüchtige, wiederbeschreibbare Speichereinheit, z. B. in Form eines Flash-Speichers, implementiert ist. Dabei ist die Speichereinheit **26** bzw. **36** dazu ausgestaltet, wenigstens ein Subskriptionsprofil aufzunehmen, beispielsweise die Subskriptionsprofile SP1 bzw. SP2, wie dies in **Fig. 1** schematisch angedeutet ist.

[0030] In der schematischen Darstellung von **Fig. 1** ist das Subskriptionsprofil SP1 bereits in die Speichereinheit **26** des Sicherheitselements **22** des ersten mobilen Endgeräts **20** eingebracht, was insbesondere bedeutet, dass beispielsweise die CPU **25** des Sicherheitselements **22** auf das Subskriptionsprofil SP1 zugreifen kann. Vorzugsweise enthält das Subskriptionsprofil SP1 Daten, die es dem Sicherheitselement **22** und dem ersten mobilen Endgerät **20** ermöglichen, sich in das Mobilfunknetz **50** einzubuchen und über dieses zu kommunizieren, d. h. Daten, wie Subskriptionsberechtigungsdaten ("Subscription Credentials"), einen MNO-spezifischen Authentisierungsalgorithmus und/oder dergleichen.

[0031] In der schematischen Darstellung von **Fig. 1** ist die Speichereinheit **36** des Sicherheitselements **32** des zweiten mobilen Endgeräts **30** zur Aufnahme des Subskriptionsprofils SP2 bereit, was nachstehend unter weiterer Bezugnahme auf **Fig. 2** im Detail beschrieben wird. Vorzugsweise enthält das Subskriptionsprofil SP2 Daten, die es dem Sicherheitselement **32** und dem zweiten mobilen Endgerät **30** ermöglichen, sich in das Mobilfunknetz **50** einzubuchen und über dieses zu kommunizieren, d. h. Daten, wie Subskriptionsberechtigungsdaten ("Subscription Credentials"), einen MNO-spezifischen Authentisierungsalgorithmus und/oder dergleichen. Alternativ kann das Subskriptionsprofil SP2 Daten enthalten, die es dem Sicherheitselement **32** und dem zweiten mobilen Endgerät **30** ermöglichen, sich in anderes Mobilfunknetz als das Mobilfunknetz **50** einzubuchen, beispielsweise in das Mobilfunknetz eines anderen Mobilfunknetzbetreibers.

[0032] **Fig. 2** zeigt einen erfindungsgemäß bevorzugten Ablauf beim Bereitstellen des Subskriptionsprofils SP2 auf dem zweiten mobilen Endgerät **30**.

[0033] In Schritt S1 von **Fig. 2** bucht sich das erste mobile Endgerät **20** mit dem bestehenden Subskriptionsprofil SP1 in das Mobilfunknetz **50** ein. Dies erfolgt im Rahmen eines Authentisierungsvorgangs unter Verwendung der Subskriptionsberechtigungsdaten, die Teil des Subskriptionsprofils SP1 sind, wie beispielsweise eine IMSI und/oder ein Authentisierungsschlüssel K_i .

[0034] Nachdem sich das erste mobile Endgerät **20** erfolgreich in das Mobilfunknetz **50** eingebucht hat und über dieses kommunizieren kann, fragt das erste mobile Endgerät **20** in Schritt S2 von **Fig. 2** über das Mobilfunknetz **50** beim SM-Server **60** ein Subskriptionsprofil SP2 für das zweite mobile Endgerät **30** an. Erfindungsgemäß ist denkbar, dass mittels einer auf dem ersten mobilen Endgerät **20** laufenden Applikation mit einer graphischen Benutzeroberfläche ein Benutzer diesen Vorgang anstoßen kann und insbesondere das Subskriptionsprofil S2 für das zweite mobile Endgerät **30** auswählen kann.

[0035] Auf diese Anfrage hin lädt der SM-Server **60** in Schritt S3 von **Fig. 2** das vom Benutzer für das zweite mobile Endgerät **30** ausgewählte Subskriptionsprofil SP2 über das Mobilfunknetz **50** auf das erste mobile Endgerät **20**. Dabei kann der SM-Server **60** dem ersten mobilen Endgerät **20** vertrauen, da sich dies gegenüber dem Mobilfunknetz **50** authentifiziert hat.

[0036] In Schritt S4 von **Fig. 2** wird ein Kommunikationskanal **40** zwischen dem ersten mobilen Endgerät **20** und dem zweiten mobilen Endgerät **30** ausgebildet. Da dem Benutzer in der Regel sowohl das erste mobile Endgerät **20** als auch das zweite mobile Endgerät **30** zur Verfügung stehen und er die beiden Endgeräte **20**, **30** zusammenführen kann, kann es sich bei dem Kommunikationskanal **40** um einen Kommunikationskanal mit kurzer Reichweite handeln. Vorzugsweise handelt es sich bei diesem Kommunikationskanal **40** um einen NFC-Kanal, Bluetooth-Kanal, WiFi-Kanal oder dergleichen. Alternativ ist auch ein Kommunikationskanal **40** in Form einer optischen oder einer akustischen Datenübertragung zwischen dem ersten mobilen Endgerät **20** und dem zweiten mobilen Endgerät **30** denkbar. Beispielsweise können die Daten auf einem Display des ersten mobilen Endgeräts **20** dargestellt werden, z. B. in Form eines QR-Codes, und mittels einer Kamera des zweiten mobilen Endgeräts **30** erfasst werden.

[0037] Nachdem in Schritt S4 von **Fig. 2** der Kommunikationskanal zwischen dem ersten mobilen Endgerät **20** und dem zweiten mobilen Endgerät **30** ausgebildet worden ist, wird in Schritt S5 von **Fig. 2** das Subskriptionsprofil SP2 vom ersten mobilen Endgerät **20** über den Kommunikationskanal **40** an das zweite mobile Endgerät **30** übertragen.

[0038] Daraufhin kann sich in Schritt S6 von **Fig. 2** das zweite mobile Endgerät bzw. dessen Sicherheitselement **32** mit dem Subskriptionsprofil SP2 und den darin enthaltenen Subskriptionsberechtigungsdaten, wie beispielsweise eine IMSI und/oder ein Authentisierungsschlüssel K_i , in das Mobilfunknetz **50** einbuchten. Wie bereits oben erwähnt, wird von der Erfindung ebenfalls der Fall erfasst, dass die Subskriptionsberechtigungsdaten des Subskriptionsprofils SP2 den Zugang zu einem anderen Mobilfunknetz ermöglichen, beispielsweise das Mobilfunknetz eines anderen Mobilfunknetzbetreibers.

[0039] Falls sich das mobile Endgerät **30** in Schritt S6 erfolgreich in das Mobilfunknetz **50** eingebucht hat, kann in Schritt S7 von **Fig. 2** das zweite mobile Endgerät **30** über das Mobilfunknetz **50** eine entsprechende Bestätigung an den SM-Server **60** senden.

[0040] Wie der Fachmann erkennen wird, ist es zur Erzielung der durch die vorliegende Erfindung bereitgestellten Vorteile nicht erforderlich, dass die Schritt-

te von **Fig. 2** in der dort dargestellten Reihenfolge erfolgen. Beispielsweise ist es im Rahmen der Erfindung denkbar, dass der Schritt S4 zum Ausbilden des Kommunikationskanals **40** zwischen dem ersten mobilen Endgerät **20** und dem zweiten mobilen Endgerät **30** bereits vor dem Herunterladen des Subskriptionsprofils SP2 auf das erste mobile Endgerät **20** erfolgt.

[0041] Die Schritte S3 bis S5 von **Fig. 2** zum Herunterladen des Subskriptionsprofils vom SM-Server **60** über das Mobilfunknetz **50** auf das erste mobile Endgerät **20** und vom ersten mobilen Endgerät **20** über den Kommunikationskanal **40** auf das zweite mobile Endgerät **30** können als ein logischer Kommunikationskanal zwischen dem SM-Server **60** und dem zweiten mobilen Endgerät **30** betrachtet werden, bei dem das erste mobile Endgerät **20** lediglich zum Weiterleiten der Daten dient. Vorzugsweise ist der logische Kommunikationskanal zwischen dem SM-Server **60** und dem zweiten mobilen Endgerät **30** kryptographisch gesichert.

[0042] Die kryptographische Sicherung des logischen Kommunikationskanals zwischen dem SM-Server **60** und dem zweiten mobilen Endgerät **30** kann beispielsweise dadurch erreicht werden, dass vorzugsweise auf dem Sicherheitselement **32** des zweiten mobilen Endgeräts **30** ein geheimer Schlüssel hinterlegt ist, der ebenfalls auf dem SM-Server **60** in Verbindung mit einem Identifier des zweiten mobilen Endgeräts **30** bzw. des Sicherheitselements **32**, z. B. einer Chip-ID, hinterlegt ist. In diesem Fall würde sich das zweite mobile Endgerät **30** in einem zusätzlichen, nicht in **Fig. 2** dargestellten Schritt gegenüber dem SM-Server **60** identifizieren und der SM-Server **60** das Subskriptionsprofil SP2 mit dem diesem Identifier zugeordneten Schlüssel verschlüsseln. Wie der Fachmann erkennen wird, kann in diesem Fall der Kommunikationskanal **40** zwischen dem ersten mobilen Endgerät **20** und dem zweiten mobilen Endgerät **30** bereits zu einem früheren Zeitpunkt ausgebildet werden, um dem ersten mobilen Endgerät **20** den Identifier, beispielsweise eine Chip-ID der Sicherheitselements **32** des zweiten mobilen Endgeräts **30** mitzuteilen. Hierbei ist vorstellbar, dass das erste mobile Endgerät **20** den Identifier des zweiten mobilen Endgeräts **30** bzw. des Sicherheitselements **32** im Rahmen der Anfrage des zweiten Subskriptionsprofils SP2 über das Mobilfunknetzwerk **50** beim SM-Server **60** (siehe Schritt S2 von **Fig. 2**).

Patentansprüche

1. Verfahren zum Bereitstellen eines Subskriptionsprofils (SP2) auf einem mobilen Endgerät (**30**) zur Kommunikation über ein Mobilfunknetzwerk, wobei das Verfahren die folgenden Schritte umfasst: das Einbuchen eines ersten mobilen Endgeräts (**20**) mit einem ersten Subskriptionsprofil (SP1) in ein Mobilfunknetzwerk (**50**);

das Herunterladen eines zweiten Subskriptionsprofils (SP2) über das Mobilfunknetzwerk (**50**) auf das erste mobile Endgerät (**20**); und das Weiterleiten des zweiten Subskriptionsprofils (SP2) vom ersten mobilen Endgerät (**20**) über einen Kommunikationskanal (**40**) an ein zweites mobiles Endgerät (**30**).

2. Verfahren nach Anspruch 1, wobei das Verfahren nach dem Schritt des Weiterleitens des zweiten Subskriptionsprofils (SP2) vom ersten mobilen Endgerät (**20**) über den Kommunikationskanal (**40**) an das zweite mobile Endgerät (**30**) den weiteren Schritt des Einbuchen des zweiten mobilen Endgeräts (**30**) mit dem zweiten Subskriptionsprofil (SP2) in ein Mobilfunknetzwerk umfasst.

3. Verfahren nach Anspruch 2, wobei das Mobilfunknetzwerk, in das sich das zweite mobile Endgerät (**30**) mit dem zweiten Subskriptionsprofil (SP2) einbucht, das Mobilfunknetzwerk (**50**), über das das zweite Subskriptionsprofil (SP2) auf das erste mobile Endgerät (**20**) heruntergeladen worden ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Kommunikationskanal (**40**) zwischen dem ersten mobilen Endgerät (**20**) und dem zweiten mobilen Endgerät (**30**) ein NFC-Kommunikationskanal, ein WiFi-Kommunikationskanal, ein Bluetooth-Kommunikationskanal, ein optischer Kommunikationskanal und/oder ein akustischer Kommunikationskanal ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei das zweite Subskriptionsprofil (SP2) von einem Server (**60**) über das Mobilfunknetzwerk (**50**) auf das erste mobile Endgerät (**20**) heruntergeladen wird.

6. Verfahren nach Anspruch 5, wobei der logische Kommunikationskanal zwischen dem Server (**60**) und dem zweiten mobilen Endgerät (**30**) kryptographisch gesichert ist.

7. Verfahren nach Anspruch 6, wobei der logische Kommunikationskanal zwischen dem Server (**60**) und dem zweiten mobilen Endgerät (**30**) dadurch kryptographisch gesichert ist, dass das zweite Subskriptionsprofil (SP2) vom Server (**60**) mit einem Schlüssel verschlüsselt wird, der auf dem Server in Verbindung mit einem Identifier des zweiten mobilen Endgeräts (**30**) und/oder eines Sicherheitselements (**32**) des zweiten mobilen Endgeräts (**30**) hinterlegt ist.

8. Sicherheitselement (**32**), wobei dem Sicherheitselement (**32**) mittels des Verfahrens nach einem der Ansprüche 1 bis 7 ein Subskriptionsprofil (SP2) bereitgestellt worden ist.

9. Mobiles Endgerät (**30**) mit einem Sicherheitselement (**34**) nach Anspruch 8.

10. System zum Bereitstellen eines Subskriptionsprofils (SP2) auf einem mobilen Endgerät (**30**) zur Kommunikation über ein Mobilfunknetzwerk, wobei das System umfasst:

ein erstes mobiles Endgerät (**20**), das dazu ausgestaltet ist, sich mit einem ersten Subskriptionsprofil (SP1) in ein Mobilfunknetzwerk (**50**) einzubuchen;
einen Server zum Herunterladen eines zweiten Subskriptionsprofils (SP2) über das Mobilfunknetzwerk (**50**) auf das erste mobile Endgerät (**20**); und
ein zweites mobiles Endgerät, das dazu ausgestaltet ist, dass das zweite Subskriptionsprofil (SP2) vom ersten mobilen Endgerät (**20**) über einen Kommunikationskanal (**40**) an das zweite mobile Endgerät (**30**) weitergeleitet wird.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

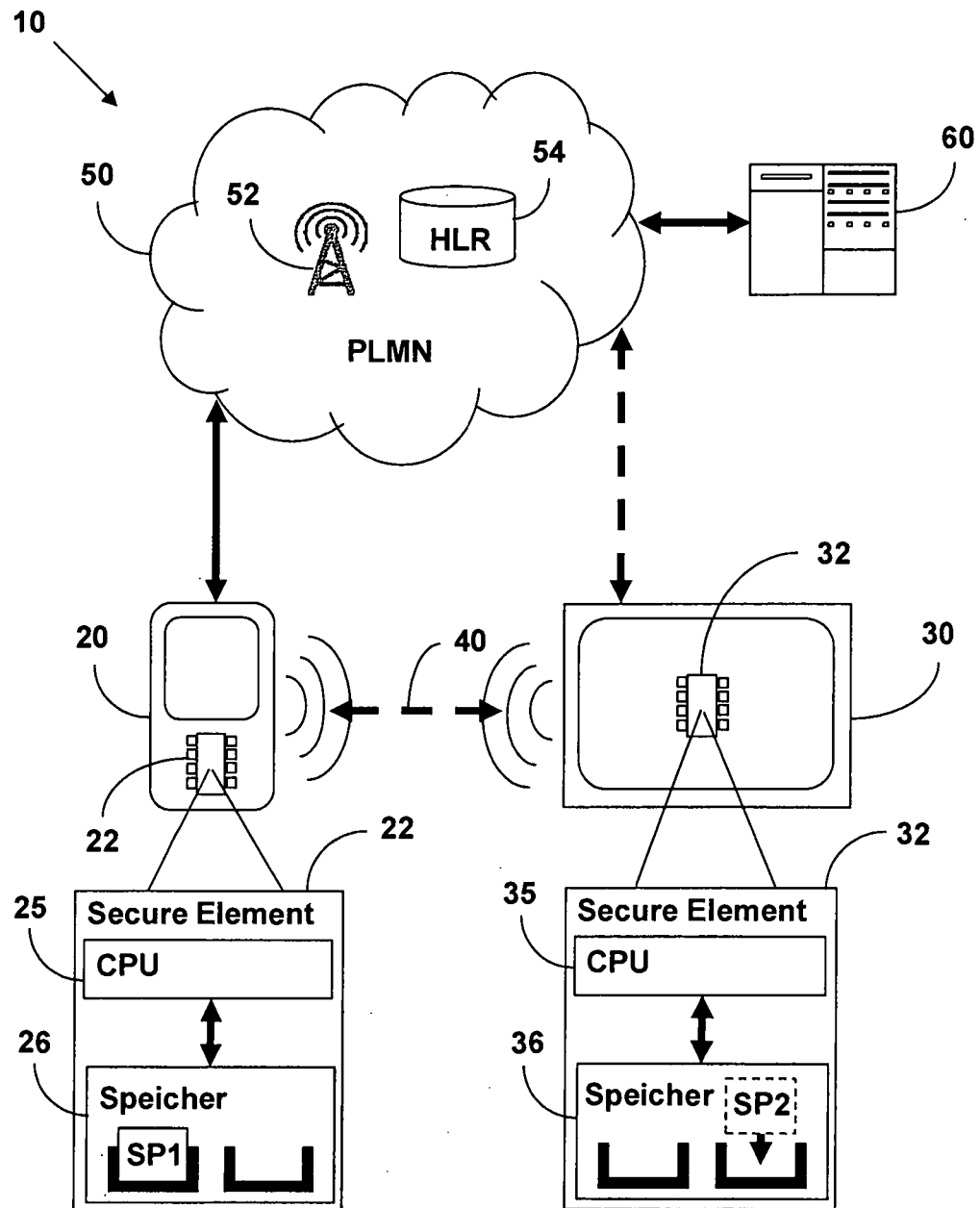


Fig. 1

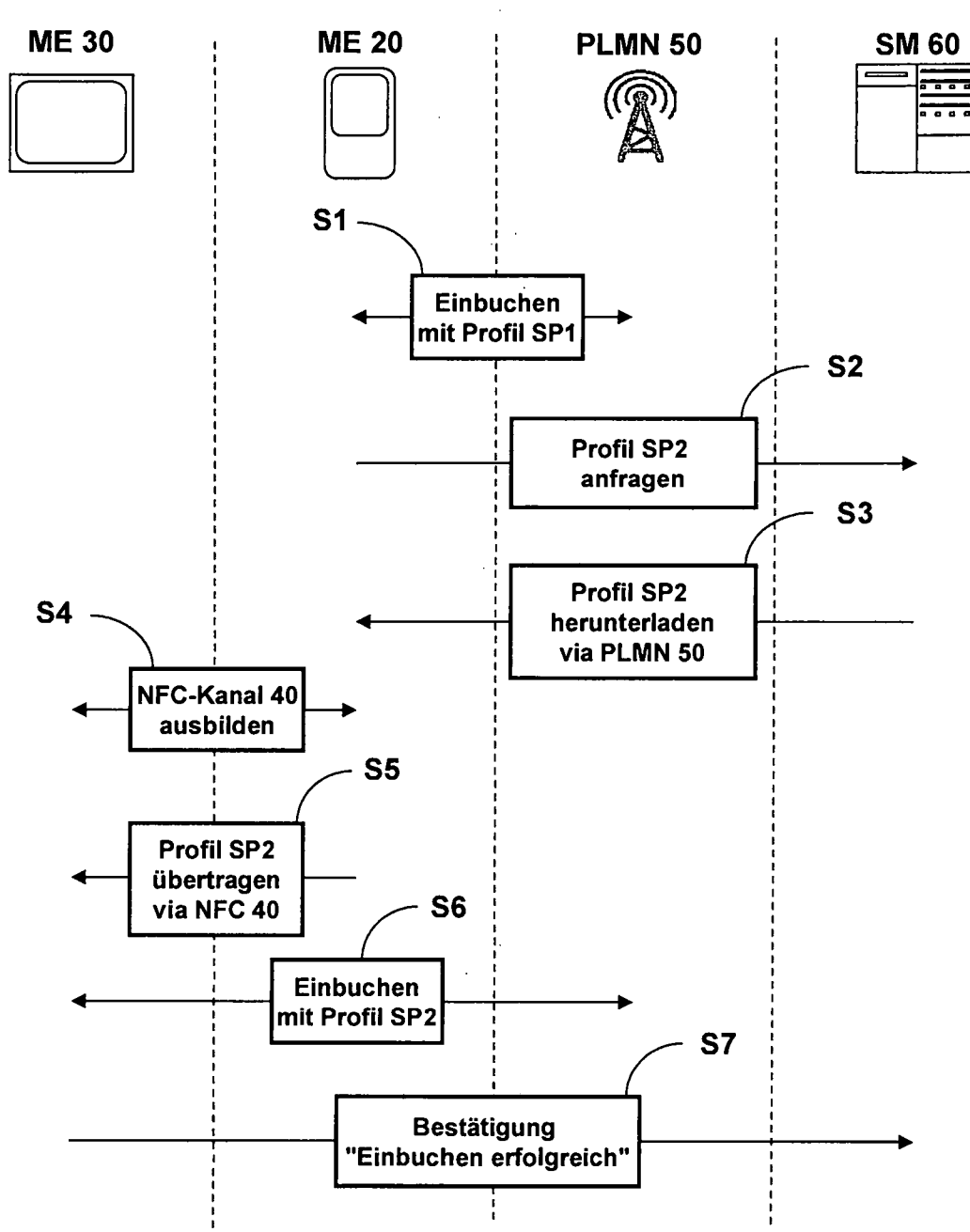


Fig. 2