(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 012 941 B3** 2017.04.06

(12) # Patentschrift

(21) Aktenzeichen: **10 2015 012 941.4**
(22) Anmeldetag: **07.10.2015**
(43) Offenlegungstag: **–**
(45) Veröffentlichungstag der Patenterteilung: **06.04.2017**

(51) Int Cl.: ***H04W 12/12*** (2009.01)
H04W 12/04 (2009.01)
G06F 21/88 (2013.01)
G06F 21/62 (2013.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Nitsch, Nils, 85570 Markt Schwaben, DE; Huber, Ulrich, 81475 München, DE

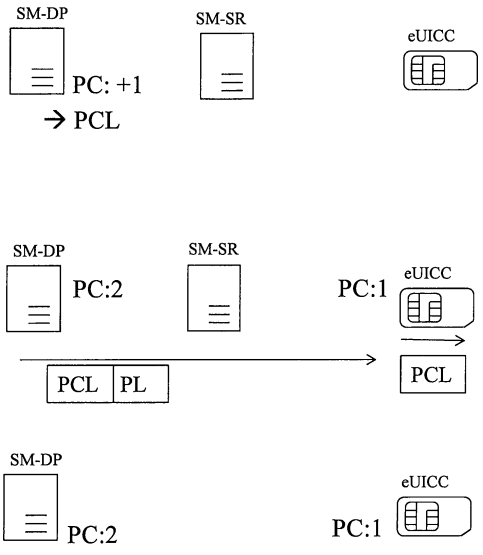
(56) Ermittelter Stand der Technik:

US 2006 / 0 090 077 A1
US 2012 / 0 190 354 A1
US 2013 / 0 129 086 A1

12FAST.13 - Embedded SIM Remote Provisioning Architecture, 17 December 2013, GSMA

SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, 13 October 2014, GSMA

(54) Bezeichnung: **Verfahren zum Laden eines Profils unter Verwendung eines Ladepakets**



(57) Zusammenfassung: Die Erfindung schafft ein Lade-Paket und ein Verfahren zum Laden eines Profils für eine Mobilfunk-Subskription (Subskription-Profils) in ein Teilnehmeridentitätsmodul zum Laden eines Profils. Mit einem Profil-Lade-Zähler wird überprüft, ob eine zulässige Anzahl von Malen, die das Profil in das Teilnehmeridentitätsmodul geladen werden darf, noch unterschritten ist.

Beschreibung

Gebiet der Erfindung

[0001] Die Erfindung betrifft ein Verfahren zum Laden eines Profils für eine Subskription (Subskriptions-Profils) in ein Teilnehmeridentitätsmodul unter Verwendung eines Ladepakets.

Stand der Technik

[0002] Mobile Endgeräte werden mittels Teilnehmeridentitätsmodulen, auch Secure Elements genannt, sicher in Funknetzwerken betrieben. Als mobile Endgeräte können insbesondere Mobilfunk-Endgeräte, wie z. B. Smartphones, sowie M2M-Endgeräte vorgesehen sein.

[0003] Im Rahmen des Einrichten eines Teilnehmeridentitätsmoduls muss ein Subskriptions-Profil in das Teilnehmeridentitätsmodul geladen werden. Änderungswünsche am Subskriptions-Profil (oder auch kurz nur Profil) erfordern das Bereitstellen eines geänderten Subskriptions-Profils. Bei Plug-In-SIM-Karten für Mobilfunk-Endgeräte kann die Änderung durch Austausch der SIM-Karte durchgeführt werden. Alternativ wird ein neues Subskriptions-Profil in das Teilnehmeridentitätsmodul geladen, was besonders für festeingelötete Teilnehmeridentitätsmodule (z. B. eUICC im Mobilfunkbereich oder festeingelötetes M2M-Modul) durchgeführt wird, die nicht ohne Weiteres ausgetauscht werden können. Das Verwalten von Subskriptionen, insbesondere durch Herunterladen von Subskriptions-Profilen und begleitenden Daten in ein Teilnehmeridentitätsmodul, wird im Allgemeinen auch als Subscription Management bezeichnet.

[0004] Die technischen Spezifikationen [1] 12 FAST.13 – Embedded SIM Remote Provisioning Architecture 17 December 2013”, GSMA, und [2] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0,13 October 2014, GSMA, beschreiben das Herunterladen und Installieren eines Subskription-Profils in ein eUICC. Gemäß [1] 12FAST.13 sind am Laden eines Subskription-Profils in ein Teilnehmeridentitätsmodul eine Subscription Management Data Preparation SM-SP und ein Subscription Management Secure Router SM-SR beteiligt. Die Subscription Management Data Preparation SM-SP verfügt über Teilnehmeridentitätsmodul-spezifische Information und erzeugt hiermit ausgehend vom Subskriptions-Profil ein in das Teilnehmeridentitätsmodul zu ladendes Lade-Paket. Das Lade-Paket umfasst eine für das Teilnehmeridentitätsmodul spezifische verschlüsselte Lade-Sequenz, die dem Subskription-Profil entspricht, und ausgehend von der sich das Subskription-Profil im Teilnehmeridentitätsmodul implementieren lässt. Die Subscription Management Data Preparation SM-SP stellt das Lade-Paket an den Subscription Management Secure Router SM-SR bereit, der das Lade-Paket in das Teilnehmeridentitätsmodul lädt. Durch Implementierungsvorgänge im Teilnehmeridentitätsmodul, die im Zusammenhang mit der Erfindung nicht von Bedeutung sind und deshalb nicht weiter betrachtet werden, wird das Subskriptions-Profil schließlich im Teilnehmeridentitätsmodul implementiert. [2] SGP 02, Kap. 3 beschreibt den protokollarischen Ablauf beim Herunterladen und Installieren eines Subskriptions-Profils in ein eUICC. Die Subscription Management Data Preparation SM-SP wird im Folgenden deutsch Daten-Aufbereitungsserver SM-DP genannt, der Subscription Management Secure Router SM-SR deutsch Sicherheits-Router SM-SR.

[0005] Um ein Laden des Lade-Pakets in mehrere unterschiedliche Teilnehmeridentitätsmodule zu verhindern, also um ein Klonen eines Subskriptions-Profils zur Nutzung in mehreren Teilnehmeridentitätsmodulen zu verhindern, ist die im Lade-Paket enthaltene Lade-Sequenz Teilnehmeridentitätsmodulspezifisch verschlüsselt.

[0006] Durch diese Maßnahme kann allerdings nicht verhindert werden, dass ein Lade-Paket mehrmals in ein und dasselbe Teilnehmeridentitätsmodul geladen und dort installiert wird. Warum diese auf den ersten Blick harmlose Maßnahme, ein Lade-Paket mehrmals in ein und dasselbe Teilnehmeridentitätsmodul zu laden, problematisch sein kann, wird nachfolgend aufgezeigt. Nutzungsverträge für Subskription-Profile können durch den Netzbetreiber zeitlich befristet sein. Um die zeitliche Befristung durchzusetzen, kann vorgesehen sein, dass anlässlich des Vertragsablaufs der Netzbetreiber das im Teilnehmeridentitätsmodul implementierte Subskriptions-Profil per Remote-Zugriff im Teilnehmeridentitätsmodul deaktiviert. Ein Nutzer könnte versuchen, die zeitliche Befristung des Nutzungsvertrags auszuhebeln, indem er nach der Remote-Deaktivierung erneut beantragt, das Lade-Paket solle in das Teilnehmeridentitätsmodul geladen werden, unter der Vorgabe, er hätte das Profil noch gar nicht erhalten.

[0007] Das Dokument US 2013/0 129 086 A1 aus dem Stand der Technik offenbart ein Verfahren zum Laden von Software von einem Software-Provider in einen sicheren Prozessor eines sicheren Geräts, bei welchem aus in einem Speicher des Geräts gespeicherten personalisierten Einheitsdaten ein Schlüssel abgeleitet wird, beim Gerät die Software vom Software-Provider empfangen wird und die Software mit dem abgeleiteten Schlüssel verschlüsselt wird. Sukzessive können aus den personalisierten Einheitsdaten weitere Schlüssel abgeleitet werden, mit denen weitere empfangene Software verschlüsselt werden kann.

[0008] Das Dokument US 2006/0 090 077 A1 aus dem Stand der Technik offenbart ein Verfahren zum autorisierten Transfer von Software in ein Embedded System, bei welchem ein Teil von heruntergeladener Software mittels eines Passworts geschützt wird. Das Passwort ist erzeugt aus einem Hardware-Identifier des eines Service Tool zum Softwareladen oder des Embedded System, sowie einem Software-Identifier von einem noch in das Embedded System zu ladender Software-Teil erzeugt worden ist. Das Service Tool lädt den Software-Teil nur dann in das Embedded System wenn das Passwort als gültig verifiziert wird.

[0009] Das Dokument US 2012/0 190 354 A1 (Gemalto SA) aus dem Stand der Technik offenbart ein Verfahren zum Management von Secure Elements wie z. B. UICCs (wahlweise festinstalliert oder nicht in ein Terminal) mit eingebetteten SIM-Applikationen. Insbesondere offenbart das Dokument ein Verfahren zum Übertragen einer SIM-Applikation von einem ersten Terminal an ein zweites Terminal. Der Zugriff auf die SIM-Applikation im ersten Terminal ist mittels eines PIN Code gesichert. Die SIM-Applikation wird vom ersten Terminal an einen entfernten Ort übertragen, zusammen mit dem PIN-Code und einem Fern-Lade-Code. Der Nutzer des zweiten Terminals wird aufgefordert, den Fern-Lade-Code einzugeben. Stimmt der eingegebene Fern-Lade-Code mit dem abgespeicherten überein, wird die Installation der SIM-Applikation in ein Secure Element des zweiten Terminals autorisiert.

Zusammenfassung der Erfindung

[0010] Der Erfindung liegt die Aufgabe zu Grunde, ein Verfahren zum Laden eines Profils für eine Mobilfunk-Subskription (Subskriptions-Profils) in ein Teilnehmeridentitätsmodul zu schaffen, bei welchem ein Aushebeln von Nutzungsbeschränkungen, insbesondere zeitlichen Befristungen, erschwert oder vorzugsweise verhindert ist. Insbesondere soll ein mehrmaliges Laden eines Subskriptions-Profils in ein Teilnehmeridentitätsmodul verhindert werden.

[0011] Die Aufgabe wird gelöst durch ein Verfahren nach Anspruch 1. Vorteilhafte Ausgestaltungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0012] Das erfindungsgemäße Verfahren verwendet ein Lade-Paket. Dieses ist eingerichtet zum Laden eines Profils für eine Subskription in ein Teilnehmeridentitätsmodul und umfasst eine Lade-Sequenz, durch deren Implementieren im Teilnehmeridentitätsmodul das Profil im Teilnehmeridentitätsmodul angelegt wird. Das Lade-Paket umfasst eine Profil-Lade-Zähler-Sequenz. Diese ist ausgehend von einem Zählerstand eines bei einem Daten-Aufbereitungsserver geführten Profil-Lade-Zähler erstellt, der anlässlich eines Übertragens des Lade-Pakets vom Daten-Aufbereitungsserver an das Teilnehmeridentitätsmodul verändert, insbesondere hochgezählt, wird. Weiter ist die Profil-Lade-Zähler-Sequenz eingerichtet, in das Teilnehmeridentitätsmodul einen Profil-Lade-Zähler mit dem erstellten Zählerstand zu laden. Die Profil-Lade-Zähler-Sequenz für den Zähler wird vor der Lade-Sequenz für das Profil in das Teilnehmeridentitätsmodul geladen, also aus dem übermittelten Lade-Paket extrahiert.

[0013] Falls im Teilnehmeridentitätsmodul kein implementierter Profil-Lade-Zähler vorhanden ist, wird der Profil-Lade-Zähler im Teilnehmeridentitätsmodul mit einem Zählerstand implementiert, der eine zulässige Anzahl von Malen festlegt, welche das Lade-Paket in das Teilnehmeridentitätsmodul geladen werden darf. Falls im Teilnehmeridentitätsmodul bereits ein implementierter Profil-Lade-Zähler vorhanden ist, wird dessen Zählerstand daraufhin überprüft, ob gemäß dem Zählerstand im Teilnehmeridentitätsmodul eine zulässige Anzahl von Malen, welche das Lade-Paket bereits in das Teilnehmeridentitätsmodul geladen oder/und implementiert worden ist, noch unterschritten ist. Das Laden oder/und Implementieren der Lade-Sequenz, also letztlich des Profils, wird nur höchstens zugelassen, falls die zulässige Anzahl noch unterschritten ist, und andernfalls wird das Laden oder/und Implementieren der Lade-Sequenz (PL) verhindert.

[0014] Durch den im Lade-Paket selbst angelegten Lade-Zähler wird die Möglichkeit eröffnet, die Zulässigkeit des Profil-Lade-Vorgangs an Hand des Lade-Pakets selbst zu überprüfen. Bei erstmaligem Laden eines Profils wird im Teilnehmeridentitätsmodul der Profil-Lade-Zähler angelegt und mit der zulässigen Höchstzahl (Anzahl) Implementier-Vorgänge für dasselbe Profil angelegt. Bei jedem weiteren Laden desselben Profils wird beim Daten-Aufbereitungs-Server der Profil-Lade-Zähler um einen Zählschritt verändert (hochgezählt; alternativ auch heruntergezählt, je nach Art der Verwirklichung im Detail). Wird dabei, anlässlich eines Profil-Lade-Vorgangs, die im Teilnehmeridentitätsmodul implementierte Höchstzahl für den Zählerstand überschritten, wird bei diesem Profil-Lade-Vorgang das Lade-Paket nicht aus dem Lade-Paket extrahiert (also nicht heraus geladen) und folglich nicht im Teilnehmeridentitätsmodul implementiert, oder zwar extrahiert (geladen) aber nicht implementiert.

[0015] Wahlweise stellt das Teilnehmeridentitätsmodul einen Profil-Lade-Zähler bereit, der einem einzelnen Profil zugeordnet ist.

[0016] Wahlweise, stellt das Teilnehmeridentitätsmodul, alternativ oder zusätzlich, einen globalen Profil-Lade-Zähler bereit, der alle Profil-Ladevorgänge zählt, insbesondere auch für unterschiedliche Profile.

[0017] Somit ist gemäß Anspruch 1 ein Verfahren geschaffen, bei welchem ein Aushebeln von Nutzungsbeschränkungen, verhindert ist.

[0018] Das Überprüfen des Zählerstandes erfolgt wahlweise, indem der Zählerstand des im Teilnehmeridentitätsmodul implementierten Profil-Lade-Zählers mit dem Zählerstand aus dem Lade-Paket verglichen wird.

[0019] Wahlweise ist im Lade-Paket die Profil-Lade-Zähler-Sequenz der Lade-Sequenz vorangestellt, so dass das Teilnehmeridentitätsmodul die Profil-Lade-Zähler-Sequenz vor der Lade-Sequenz aus dem Lade-Paket heraus laden oder extrahieren muss.

[0020] Ein erfindungsgeeigneter Daten-Aufbereitungs-Server ist eingerichtet, ein zum Übertragen an ein Teilnehmeridentitätsmodul bereitgestelltes Lade-Paket zu erstellen.

[0021] Wahlweise verschlüsselt der Daten-Aufbereitungs-Server das erstellte Lade-Paket mit einem für das Teilnehmeridentitätsmodul spezifischen Schlüssel und überträgt das verschlüsselte Lade-Paket an das Teilnehmeridentitätsmodul. Im Teilnehmeridentitätsmodul wird das Lade-Paket entschlüsselt.

Kurze Beschreibung der Zeichnungen

[0022] Im Folgenden wird die Erfindung an Hand von Ausführungsbeispielen und unter Bezugnahme auf die Zeichnungen näher erläutert, in der zeigen:

[0023] Fig. 1 ein Schaubild zum erstmaligen Laden eines Lade-Pakets von einem Daten-Aufbereitungsserver über einen Sicherheits-Router in ein Teilnehmeridentitätsmodul, gemäß einer Ausführungsform der Erfindung;

[0024] Fig. 2 ein zu **Fig.** 1 analoges Schaubild für den Versuch des Sicherheits-Routers, das Lade-Paket ein zweites Mal in das Teilnehmeridentitätsmodul zu laden.

Detaillierte Beschreibung von Ausführungsbeispielen

[0025] Fig. 1 zeigt ein Schaubild zum erstmaligen Laden eines Lade-Pakets von einem Daten-Aufbereitungsserver SM-DP in ein Teilnehmeridentitätsmodul eUICC, gemäß einer Ausführungsform der Erfindung. Das Lade-Paket umfasst eine Lade-Sequenz PL zum Implementieren eines Subskriptionsprofil P und eine Profil-Lade-Zähler-Sequenz PCL zum Implementieren eines Profil-Lade-Zählers PC, jeweils im Teilnehmeridentitätsmodul eUICC. In einem Schritt (a) erstellt der Daten-Aufbereitungsserver SM-DP das Lade-Paket aus einer Lade-Sequenz PL und einer Profil-Lade-Zähler-Sequenz PCL. Die Lade-Sequenz PL wird ausgehend von zu ladenden Profildaten P erzeugt. Die Profil-Lade-Zähler-Sequenz PCL wird ausgehend vom Zählerstand eines Profil-Lade-Zählers PC erstellt, der um einen Zählschritt hochgezählt wird, im vorliegenden Fall des erstmaligen Ladens auf den Zählerstand eins. Aus Lade-Sequenz PL und einer Profil-Lade-Zähler-Sequenz PCL wird das Lade-Paket erstellt und mit einem für das Teilnehmeridentitätsmodul eUICC spezifischen Schlüssel verschlüsselt. (b) Das verschlüsselte Lade-Paket wird vom Datenaufbereitungs-Server SM-DP über einen Sicherheits-Router SM-SR an das Teilnehmeridentitätsmodul eUICC übermittelt. Das Teilnehmeridentitätsmodul eUICC entschlüsselt das Lade-Paket. Im Lade-Paket ist die Profil-Lade-Zähler-Sequenz PCL der Lade-Sequenz PL für das Profil P vorangestellt. Daher kann das Teilnehmeridentitätsmodul eUICC nur zuerst die Profil-Lade-Zähler-Sequenz PCL aus dem entschlüsselten Lade-Paket heraus in das Teilnehmeridentitätsmodul laden. In einem Schritt (c) wird daraufhin im Teilnehmeridentitätsmodul festgestellt, dass dort noch kein Profil-Lade-Zähler PC implementiert ist und der Profil-Lade-Zähler wird im Teilnehmeridentitätsmodul eUICC neu implementiert, einschließlich des Zählerstandes, hier also eins, was hier zugleich die höchstens zulässige Anzahl von Malen ist, die das Profil im Teilnehmeridentitätsmodul eUICC implementiert werden darf. In einem Schritt (d) lädt das Teilnehmeridentitätsmodul eUICC nun die Lade-Sequenz PL für das Profil aus dem Lade-Paket heraus in das Teilnehmeridentitätsmodul eUICC und implementiert im Teilnehmeridentitätsmodul eUICC das Profil P ausgehend von der geladenen Lade-Sequenz PL.

[0026] Fig. 2 zeigt ein zu **Fig.** 1 analoges Schaubild für den Versuch des Daten-Aufbereitungsservers SM-DP, das Lade-Paket ein zweites Mal in das Teilnehmeridentitätsmodul eUICC zu laden. Der Daten-Aufbereitungsserver SM-DP beginnt mit dem Erstellen des Lade-Pakets und stellt die Profil-Lade-Sequenz bereit. (a) Hierfür zählt der Daten-Aufbereitungsserver SM-DP den Zählerstand des Profil-Lade-Zählers PC um einen Zählschritt hoch von eins auf zwei und erstellt auf Grundlage dieses Zählerstandes die Profil-Lade-Zähler-Sequenz PCL. Der Daten-Aufbereitungsserver SM-DP konkateniert die Profil-Lade-Sequenz PL und die Profil-Lade-Zähler-Sequenz PCL in das Lade-Paket und verschlüsselt das Lade-Paket mit dem für das Teilnehmeridentitätsmodul eUICC spezifischem Schlüssel. (b) Das verschlüsselte Lade-Paket wird vom Datenaufbereitungs-Server SM-DP über einen Sicherheits-Router SM-SR an das Teilnehmeridentitätsmodul eUICC übermittelt. Das Teilnehmeridentitätsmodul eUICC entschlüsselt das Lade-Paket und extrahiert die Profil-Lade-Zähler-Sequenz PCL, mit Zählerstand zwei. (c) Das Teilnehmeridentitätsmodul eUICC stellt fest, dass es schon einen implementierten Profil-Lade-Zähler PC hat und prüft den Zählerstand aus dem Lade-Paket, also

zwei, gegenüber dem Zählerstand des im Teilnehmeridentitätsmodul eUICC implementierten Profil-Lade-Zählers PC, also eins. Somit übersteigt der Zählerstand die zulässige Anzahl Implementierungs-Vorgänge des Profils P. In einem Schritt (d) wird folglich verhindert, dass die Lade-Sequenz PL ein zweites Mal in das Teilnehmeridentitätsmodul eUICC extrahiert (geladen) und implementiert wird.

[0027] Wahlweise sind bei dem Verfahren weiter Maßnahmen vorgesehen, um zu verhindern, dass eine unberechtigte Datenquelle ein Lade-Paket an das Teilnehmeridentitätsmodul sendet. Wahlweise wird dadurch verhindert, dass ein Lade-Paket zwischengespeichert und unverändert wieder in das Teilnehmeridentitätsmodul eingespielt wird.

[0028] Wahlweise wird hierbei durch den Daten-Aufbereitungs-Server dem, ggf. verschlüsselten, Lade-Paket ein für den Daten-Aufbereitungs-Server spezifisches Verifizierungs-Token beigefügt, welches nach dem Übermitteln des Lade-Pakets an das Teilnehmeridentitätsmodul beim Teilnehmeridentitätsmodul verifiziert wird. Das Lade-Paket wird nur bei erfolgreicher Verifizierung des Verifizierungs-Token beim Teilnehmeridentitätsmodul akzeptiert. Andernfalls wird die Profil-Zähler-Lade-Sequenz oder/und die Lade-Sequenz aus dem Lade-Paket nicht geladen oder/und nicht implementiert.

[0029] Wahlweise ist als Verifizierungs-Token eine Prüfsumme vorgesehen, insbesondere Message Authentication Code MAC, oder alternativ ein Zertifikat.

Zitierter Stand der Technik

[1] 12FAST.13 – Embedded SIM Remote Provisioning Architecture 17 December 2013, GSMA
[2] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, 13 October 2014, GSMA

Patentansprüche

1. Verfahren zum Laden eines Lade-Pakets von einem Daten-Aufbereitungs-Server (SM-DP) in ein Teilnehmeridentitätsmodul (eUICC), das Lade-Paket umfassend eine Lade-Sequenz (PL), durch deren Implementieren im Teilnehmeridentitätsmodul (eUICC) das Profil (P) im Teilnehmeridentitätsmodul (eUICC) angelegt wird, und umfassend eine Profil-Lade-Zähler-Sequenz (PCL); das Verfahren umfassend die Schritte:
– bei einem Daten-Aufbereitungsserver (SM-DP):
– Erstellen der Lade-Sequenz (PL) für das Profil (P);
– Verändern, insbesondere Hochzählen, eines Zählerstandes eines Profil-Lade-Zähler (PC) für das Profil und Erstellen der Profil-Lade-Zähler-Sequenz (PCL) ausgehend vom veränderten Zählerstand;
– Erstellen eines Lade-Pakets umfassend die erstellte Lade-Sequenz (PL) und der Profil-Lade-Zähler-Sequenz (PCL);
– Übertragen des Lade-Pakets umfassend die Lade-Sequenz (PL) und die Profil-Lade-Zähler-Sequenz (PCL) vom Daten-Aufbereitungs-Server (SM-DP) an das Teilnehmeridentitätsmodul (eUICC);
– vor dem Laden der Lade-Sequenz (PL) aus dem Lade-Paket, Laden der Profil-Lade-Zähler-Sequenz (PCL) aus dem Lade-Paket in das Teilnehmeridentitätsmodul (eUICC);
– falls im Teilnehmeridentitätsmodul kein implementierter Profil-Lade-Zähler (PC) vorhanden ist, ausgehend von der Profil-Lade-Zähler-Sequenz (PCL) Implementieren des Profil-Lade-Zählers (PC) im Teilnehmeridentitätsmodul mit einem Zählerstand, der eine zulässige Anzahl von Malen festlegt, welche das Lade-Paket (PL) in das Teilnehmeridentitätsmodul geladen werden darf;
– oder falls im Teilnehmeridentitätsmodul bereits ein implementierter Profil-Lade-Zähler (PC) vorhanden ist, Überprüfen von dessen Zählerstand daraufhin, ob gemäß dem Zählerstand eine zulässige Anzahl von Malen, welche das Lade-Paket (PL) bereits in das Teilnehmeridentitätsmodul geladen oder/und implementiert worden ist, noch unterschritten ist, und falls die zulässige Anzahl noch unterschritten ist Laden oder/und Implementieren der Lade-Sequenz (PL), und andernfalls Verhindern des Ladens oder/und Implementierens der Lade-Sequenz (PL).

2. Verfahren nach Anspruch 1, wobei das Überprüfen des Zählerstandes dadurch durchgeführt wird, dass, der Zählerstand des im Teilnehmeridentitätsmodul implementierten Profil-Lade-Zählers (PC) mit dem Zählerstand aus dem Lade-Paket als Vergleichs-Zählerstand verglichen wird.

3. Verfahren nach Anspruch 2, wobei das Lade-Paket vom Daten-Aufbereitungs-Server (SM-DP) über einen Sicherheits-Router (SM-SR) an das Teilnehmeridentitätsmodul (eUICC) übertragen wird, wobei der Sicherheits-Router (SM-SR) keine Zugriffsmöglichkeit auf den Profil-Lade-Zähler (PC) hat.

4. Verfahren nach einem der Ansprüche 2 bis 3, wobei:
das Verfahren den weiteren Schritt des Verschlüsselns des erstellten Lade-Pakets mit einem für das Teilnehmeridentitätsmodul (eUICC) spezifischen Schlüssel umfasst;
das Übertragen des Lade-Pakets als Übertragen des verschlüsselten Lade-Pakets gestaltet ist; und
das Verfahren im Teilnehmeridentitätsmodul (eUICC) den Schritt des Entschlüsselns des verschlüsselten Lade-Pakets umfasst.

5. Verfahren nach einem der Ansprüche 2 bis 4, wobei durch den Daten-Aufbereitungs-Server (SM-DP) dem, ggf. verschlüsselten, Lade-Paket ein für

den Daten-Aufbereitungs-Server (SM-DP) spezifisches Verifizierungs-Token beigefügt wird, welches nach dem Übermitteln des Lade-Pakets an das Teilnehmeridentitätsmodul (eUICC) beim Teilnehmeridentitätsmodul (eUICC) verifiziert wird, und wobei das Lade-Paket nur bei erfolgreicher Verifizierung des Verifizierungs-Token beim Teilnehmeridentitätsmodul (eUICC) akzeptiert wird, und andernfalls die Profil-Zähler-Lade-Sequenz (PCL) oder/und die Lade-Sequenz aus dem Lade-Paket nicht geladen oder/und nicht implementiert wird.

6. Verfahren nach Anspruch 5, wobei als Verifizierungs-Token eine Prüfsumme, insbesondere Message Authentication Code (MAC), oder ein Zertifikat vorgesehen ist.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

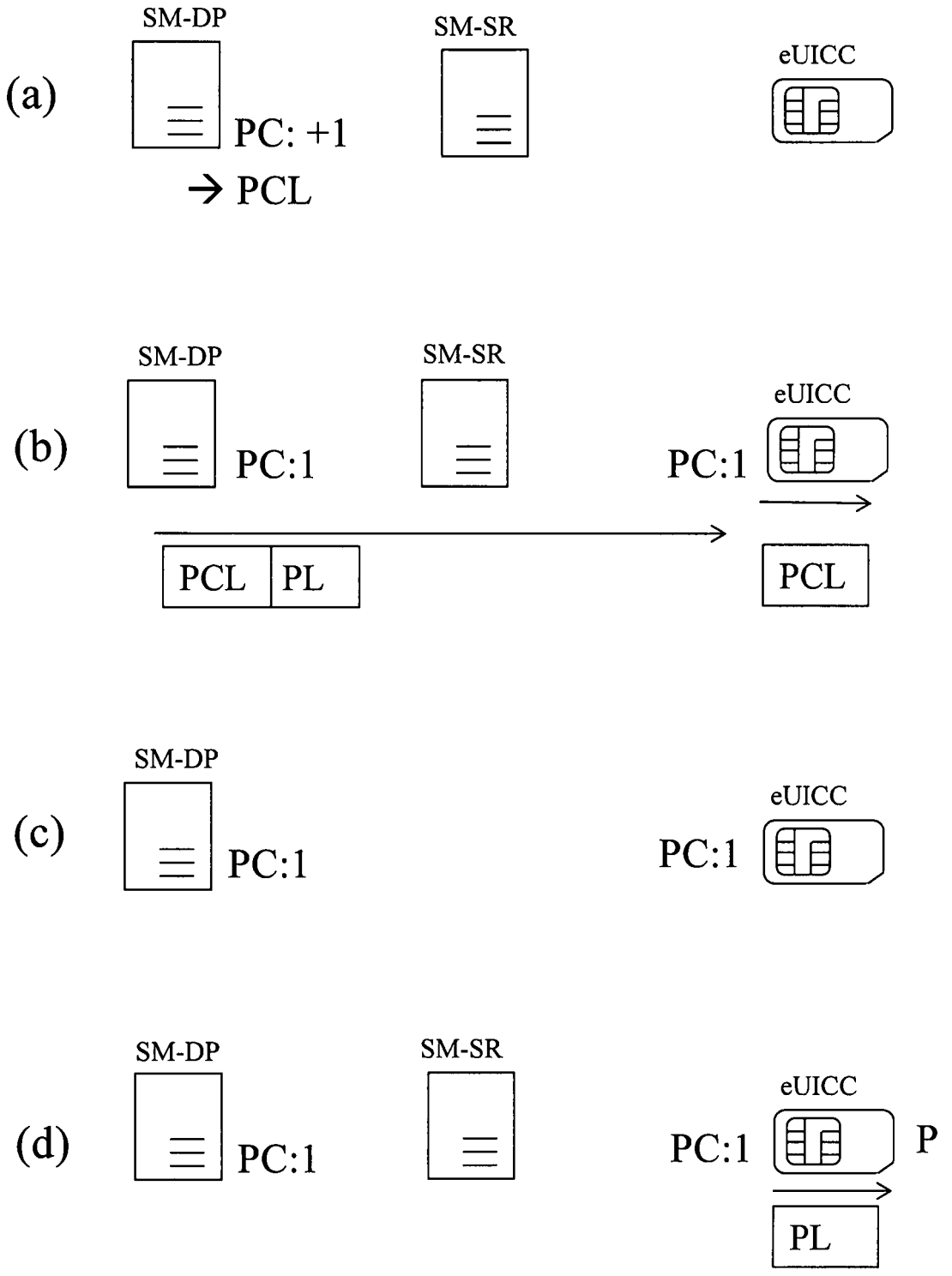


Fig. 1

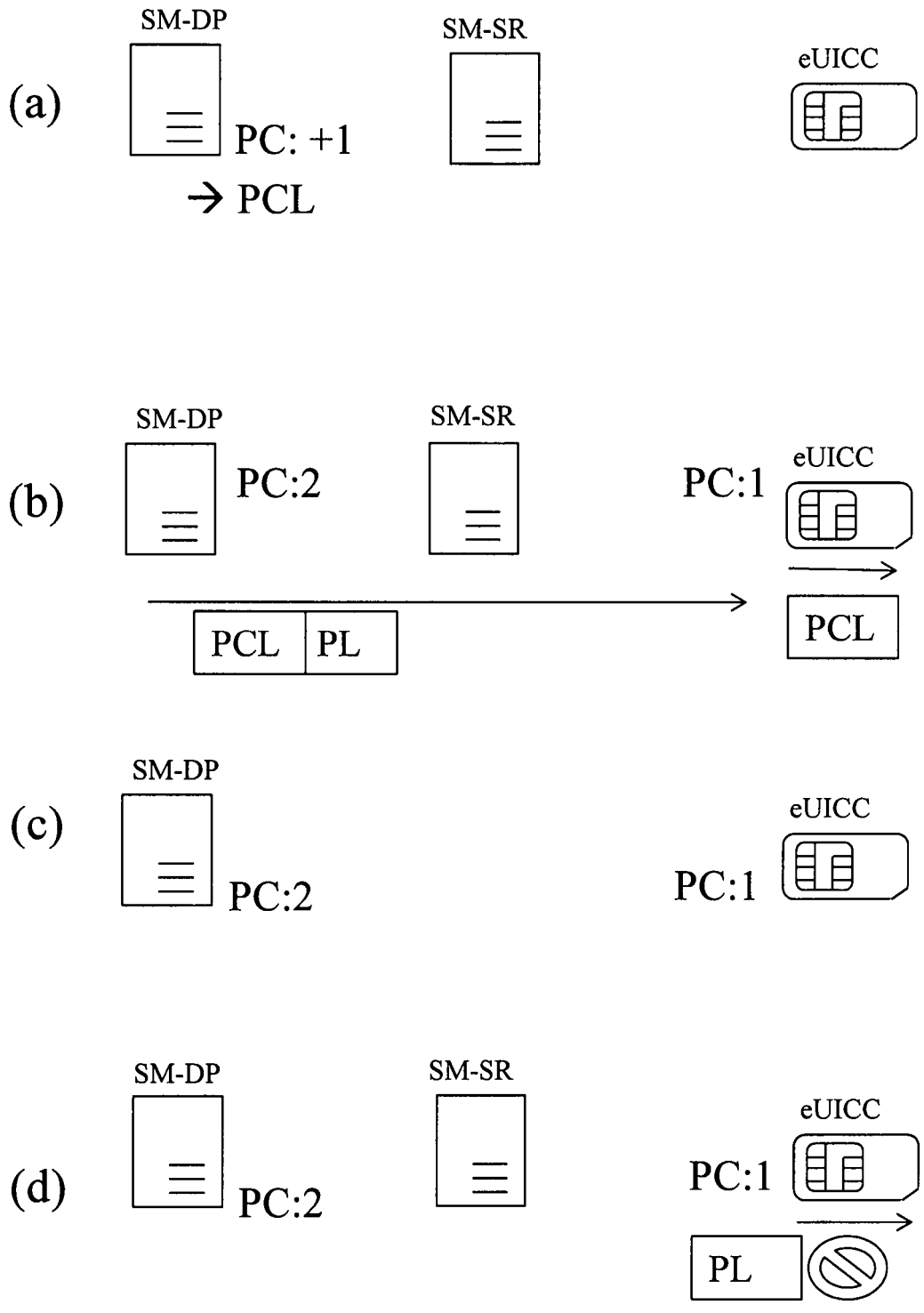

(a)
SM-DP
PC: +1
→ PCL
SM-SR
eUICC
(b)
SM-DP
PC:2
SM-SR
PC:1
eUICC
PCL
PL
PCL
(c)
SM-DP
PC:2
eUICC
PC:1
(d)
SM-DP
PC:2
SM-SR
eUICC
PC:1
PL

Fig. 2