(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
27. August 2015 (27.08.2015)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2015/124317 A1

(51) Internationale Patentklassifikation:
H04W 4/00 (2009.01) *H04W 8/20* (2009.01)
H04W 8/18 (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2015/000402

(22) Internationales Anmeldedatum:
20. Februar 2015 (20.02.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 002 603.5
24. Februar 2014 (24.02.2014) DE

(71) Anmelder: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstraße 159, 81677 München (DE).

(72) Erfinder: **INDERST, Bernhard**; Klenzestr. 60, 80469 München (DE). **BESCHNIDT, Tobias**; Kürnbergstr. 5, 81369 München (DE). **SUMMERER, Alexander**; Mitterfeldring 56, 85586 Poing (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) Title: METHOD FOR REMOTELY MANAGING A DATA ELEMENT STORED ON A SECURITY ELEMENT

(54) Bezeichnung : VERFAHREN ZUM ENTFERNTEN VERWALTEN EINES AUF EINEM SICHERHEITSELEMENT GESPEICHERTEN DATENELEMENTS

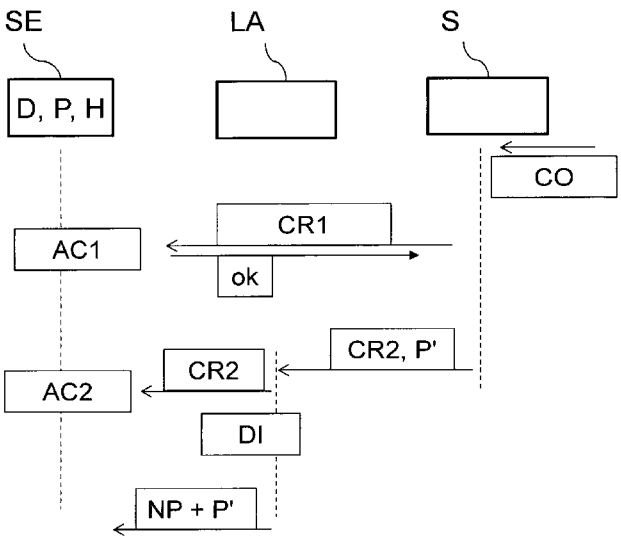

Fig. 1

(57) Abstract: The invention relates to a method for remotely managing a data element (D) stored on a security element (SE), wherein a change request for the data element (D) originating at least partially from a server (S) is transferred to the security element (SE), whereupon the data element (D) stored in the security element is changed in the security element (SE), wherein the change comprises a first changing memory access (AC1) and a second changing memory access (AC2) to the security element (SE). The first memory access (AC1) and the second memory access (AC2) occur in partial steps of the change that are decoupled from each other, wherein a first partial step comprises the transfer of a first partial change request (CR1) from the change request to the security element (SE) by the server (S) and the first memory access (AC1) and wherein a second partial step comprises the transfer of a second partial change request (CR2) from the change request to the security element (SE) and the second memory access (AC2).

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2015/124317 A1

Die Erfindung betrifft ein Verfahren zum entfernten Verwalten eines auf einem Sicherheitselement (SE) gespeicherten Datenelements (D), bei dem eine Änderungsanforderung für das Datenelement (D), welche zumindest zum Teil von einem Server (S) stammt, an das Sicherheitselement (SE) übermittelt wird, woraufhin in dem Sicherheitselement (SE) das darin gespeicherte Datenelement (D) geändert wird, wobei die Änderung einen ersten ändernden Speicherzugriff (AC1) und einen zweiten ändernden Speicherzugriff (AC2) auf das Sicherheitselement (SE) umfasst. Der erste Speicherzugriff (AC1) und der zweite Speicherzugriff (AC2) erfolgen in voneinander entkoppelten Teilschritten der Änderung, wobei ein erster Teilschritt das Übermitteln einer ersten Teiländerungsanforderung (CR1) aus der Änderungsanforderung von dem Server (S) zu dem Sicherheitselement (SE) sowie den ersten Speicherzugriff (AC1) umfasst und wobei ein zweiter Teilschritt das Übermitteln einer zweiten Teiländerungsanforderung (CR2) aus der Änderungsanforderung zu dem Sicherheitselement (SE) und den zweiten Speicherzugriff (AC2) umfasst.

Verfahren zum entfernten Verwalten eines auf einem Sicherheitselement gespeicherten Datenelements

Die Erfindung betrifft ein Verfahren und ein System zum entfernten Verwalten eines auf einem Sicherheitselement gespeicherten Datenelements.

Sicherheitselemente können für unterschiedliche Zwecke zur sicheren Speicherung von Datenelementen eingesetzt werden. Oftmals sind auf Sicherheitselementen Benutzeridentifikationsdaten, wie z.B. ein Passwort oder eine PIN, hinterlegt. Ein Benutzer kann dabei durch Eingabe des Passworts oder der PIN, vorzugsweise über ein mit dem Sicherheitselement verbundenes Endgerät, Funktionen des Sicherheitselements autorisieren.

Aus dem Stand der Technik sind Verfahren zum entfernten Verwalten von Datenelementen und insbesondere PINs auf einem Sicherheitselement bekannt. In dem Dokument WO 2007/036341 A1 wird ein Verfahren zum Entsperren einer mittels einer Zugangskennung eines Benutzers gesperrten Mobilfunkkarte beschrieben, bei dem nach erfolgter Authentisierung des Benutzers gegenüber einer Serviceeinrichtung automatisch ein Zugang für den Benutzer auf der Mobilfunkkarte eingerichtet wird. Dies kann dadurch erfolgen, dass dem Benutzer eine gültige oder neue Zugangskennung mitgeteilt wird oder der Benutzer zur Eingabe einer neuen Zugangskennung aufgefordert wird.

Herkömmliche Verfahren zum entfernten Verwalten von Datenelementen auf einem Sicherheitselement weisen den Nachteil auf, dass nur bestimmte Informationen der Datenelemente zentral durch einen Server geändert werden können. Ferner besteht ein Sicherheitsrisiko, da zur Verwaltung der Datenelemente Kommunikationskanäle zwischen dem Sicherheitselement und

dem Server verwendet werden, welche durch Angriffe Dritter abgehört werden können.

Aufgabe der Erfindung ist es, ein einfaches und sicheres Verfahren bzw. System zum entfernten Verwalten eines auf einem Sicherheitselement gespeicherten Datenelements zu schaffen.

Diese Aufgabe wird durch den Gegenstand der unabhängigen Ansprüche gelöst. Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen definiert.

Im Rahmen des erfindungsgemäßen Verfahrens wird eine Änderungsanforderung für das zu ändernde Datenelement, welche zumindest zum Teil von einem Server stammt, an das Sicherheitselement übermittelt, woraufhin in dem Sicherheitselement das darin gespeicherte Datenelement geändert wird. Die Änderung umfasst einen ersten ändernden Speicherzugriff und einen zweiten ändernden Speicherzugriff auf das Sicherheitselement.

Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass der erste Speicherzugriff und der zweite Speicherzugriff in voneinander entkoppelten Teilschritten der Änderung des Datenelements erfolgen. Ein erster Teilschritt umfasst dabei das Übermitteln einer ersten Teiländerungsanforderung aus der Änderungsanforderung von dem Server zu dem Sicherheitselement sowie den ersten ändernden Speicherzugriff, wohingegen ein zweiter Teilschritt das Übermitteln einer zweiten Teiländerungsanforderung aus der Änderungsanforderung zu dem Sicherheitselement und den zweiten Speicherzugriff umfasst. Im Unterschied zur Übermittlung der ersten Teiländerungsanforderung muss die zweite Teiländerungsanforderung nicht zwangsläufig von dem Server stammen.

Das erfindungsgemäße Verfahren weist den Vorteil auf, dass durch die Aufteilung der Speicherzugriffe in voneinander entkoppelte Teilschritte die Sicherheit des Verfahrens erhöht wird und flexibel verschiedene Informationen des Datenelements unabhängig voneinander geändert werden können.

Die Entkopplung der soeben beschriebenen Teilschritte kann im erfindungsgemäßen Verfahren auf verschiedene Weise realisiert werden. In einer Variante wird die Entkopplung dadurch erreicht, dass der erste Teilschritt zu einem anderen Zeitpunkt als der zweite Teilschritt ausgeführt wird. Ebenso kann der erste Teilschritt einen anderen Verbindungstyp zum Übermitteln der ersten Teiländerungsanforderung nutzen als der zweite Teilschritt zum Übermitteln der zweiten Teiländerungsanforderung. Ferner kann der erste Teilschritt eine andere lokale Applikation (d.h. eine Software-Applikation bzw. einen Software-Agenten) auf einem mit dem Sicherheitselement kommunizierenden Endgerät als der zweite Teilschritt nutzen. Bei dem Endgerät handelt es sich insbesondere um ein mobiles Endgerät, wie z.B. ein Mobiltelefon. Das Sicherheitselement kann z.B. in das Endgerät eingesetzt sein oder auch integraler Bestandteil des Endgeräts sein. Die lokale Applikation läuft dabei nicht direkt auf dem Sicherheitselement, sondern auf dem Endgerät. Nichtsdestotrotz kann zusätzlich zur Verarbeitung der Teiländerungsanforderungen auch eine Applikation bzw. ein Applet auf dem Sicherheitselement laufen.

Zur Entkopplung des ersten und zweiten Teilschritts kann der erste Teilschritt auch eine andere Rückmeldung zur Bestätigung des ersten Speicherzugriffs ausgeben als der zweite Teilschritt zur Bestätigung des zweiten Speicherzugriffs. Ebenso kann nur der erste oder zweite Teilschritt (d.h. nicht

beide Teilschritte) eine Rückmeldung zur Bestätigung des ersten bzw. zweiten Speicherzugriffs ausgeben.

In einer weiteren bevorzugten Variante der Erfindung wird die erste Teiländerungsanforderung direkt ohne Zwischenschaltung einer lokalen Applikation auf einem mit dem Sicherheitselement kommunizierenden Endgerät von dem Server an das Sicherheitselement übermittelt. Die direkte Kommunikation zwischen Sicherheitselement und Server schließt nicht aus, dass auf dem Sicherheitselement eine Applikation bzw. ein Applet zum Verarbeiten der Teiländerungsanforderungen läuft.

In einer weiteren, besonders bevorzugten Ausführungsform wird auch die zweite Teiländerungsanforderung von dem Server an das Sicherheitselement übermittelt. Vorzugsweise erfolgt die Übermittlung der zweiten Teiländerungsanforderung unter Zwischenschaltung einer lokalen Applikation auf einem mit dem Sicherheitselement kommunizierenden Endgerät. Alternativ oder zusätzlich kann die Übermittlung der zweiten Teiländerungsanforderung auch ohne Beteiligung des Servers von einer lokalen Applikation auf einem mit dem Sicherheitselement kommunizierenden Endgerät übermittelt werden.

In einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens umfasst die erste Teiländerungsanforderung eine Änderungsanweisung und spezifiziert den zu ändernden Dateninhalt des Datenelements. Analog kann die zweite Teiländerungsanforderung eine Änderungsanweisung umfassen und den zu ändernden Dateninhalt des Datenelements spezifizieren. Hierdurch können die Teiländerungsanforderungen einfach voneinander unterschieden werden.

In einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens weist die erste Teiländerungsanforderung ein größeres oder ein kleineres Datenvolumen als die zweite Teiländerungsanforderung auf. Auf diese Weise wird eine asymmetrische Aufteilung des Datenvolumens bewirkt. Zum Beispiel kann ein minimaler Dateninhalt in der ersten oder zweiten Teiländerungsanforderung enthalten sein, wohingegen mit der anderen Teiländerungsanforderung ein größeres Datenvolumen übermittelt wird.

In einer weiteren bevorzugten Ausführungsform umfasst das zu ändernde Datenelement sowohl Verwaltungsdaten (insbesondere einen Header) als auch Nutzdaten, d.h. den eigentlichen Dateninhalt. Vorzugsweise umfassen die Nutzdaten vertrauliche Informationen und insbesondere Benutzeridentifikationsdaten, z.B. ein vom Benutzer einzugebendes Passwort zur Freischaltung einer oder mehrerer Funktionen des Sicherheitselements. Der Begriff des Passworts ist dabei weit zu verstehen und kann beliebige Zeichenfolge umfassen. Insbesondere fällt unter dem Begriff des Passworts auch eine PIN. Das erfindungsgemäße Verfahren eignet sich somit im Speziellen auch zur Verwaltung von Passwörtern zum Schutz von Funktionen des Sicherheitselements.

In einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens spezifiziert die erste Teiländerungsanforderung einen ersten Speicherzugriff zur Invalidierung der oben genannten Benutzeridentifikationsdaten. Hierdurch wird sichergestellt, dass aktuelle Benutzeridentifikationsdaten nicht mehr verwendet werden können und im Rahmen der erfindungsgemäßen Verwaltung durch neue Benutzeridentifikationsdaten ersetzt werden müssen.

In einer weiteren bevorzugten Ausführungsform spezifizieren die Verwaltungsdaten eine oder mehrere Vorgaben für die Struktur und/oder Verwen-

dung der Benutzeridentifikationsdaten. Solche Vorgaben können insbesondere eine oder mehrere der folgenden Vorgaben umfassen:

- eine minimale Länge und/oder eine maximale Länge für die Benutzeridentifikationsdaten;
- einen Fehlbedienungszähler, der angibt, wie oft Benutzeridentifikationsdaten durch einen Benutzer falsch eingegeben werden dürfen;
- kodierte Informationen über den Aufbau der Benutzeridentifikationsdaten, z.B. ob die Daten alphanumerisch und/oder numerisch sein müssen oder dürfen und/oder ob die Daten eine bestimmte Anzahl von Sonderzeichen und/oder Großbuchstaben umfassen müssen und/oder ob die Daten eine Mindestanzahl von unterschiedlichen Zeichen umfassen müssen und/oder ob die Daten nur eine maximale Anzahl von gleichen Zeichen hintereinander umfassen dürfen;
- eine Lebensdauer der Benutzeridentifikationsdaten für eine bestimmte Maximalanzahl von Zugriffen auf das Sicherheitselement.

In einer besonders bevorzugten Ausführungsform spezifiziert die erste und/oder zweite Teiländerungsanforderung einen ersten bzw. zweiten Speicherzugriff zum Ändern zumindest eines Teils der Verwaltungsdaten, wobei die Änderung vorzugsweise kleiner als 1 Byte ist.

In einer weiteren bevorzugten Variante spezifiziert die zweite Teiländerungsanforderung einen zweiten Speicherzugriff zum Ändern der Benutzeridentifikationsdaten und/oder von einer oder mehreren Vorgaben für die Struktur und/oder Verwendung der Benutzeridentifikationsdaten.

Das erfindungsgemäße Verfahren kann in Kombination mit beliebigen Sicherheitselementen zum Einsatz kommen. Das Sicherheitselement kann ein Hardwaresicherheitsmodul, welches reversibel (SIM-Karte) oder fest (em-

bedded SIM, TPM-Modul) in ein Endgerät eingesetzt ist, oder ein Softwaresicherheitsmodul (virtuelle SIM in TEE) sein. Ein Sicherheitselement kann dabei eine oder mehrere folgende Komponenten umfassen:
eine SIM/ USIM-Karte (SIM = Subscriber Identity Modul, USIM = Universal Subscriber Identity Modul), eine MikroSD-Karte, einen USB-Token (USB = Universal Serial Bus), eine Chipkarte, ein RFID-Modul (RFID = Radio Frequency Identification), ein TPM-Modul (TPM = Trusted Platform Modul), ein NFC-Modul (NFC = Near Field Communication), ein embedded SIM-Modul, eine TEE-Umgebung (TEE = Trusted Execution Environment im Sinne der GlobalPlatform Spezifikation).

Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein System zum entfernten Verwalten eines auf einem Sicherheitselement gespeicherten Datenelements, wobei das System zur Durchführung des erfindungsgemäßen Verfahrens bzw. einer oder mehrerer bevorzugter Varianten des erfindungsgemäßen Verfahrens ausgestaltet ist. Das System umfasst dabei den im erfindungsgemäßen Verfahren verwendeten Server sowie auch das entsprechende Sicherheitselement. Bei der Realisierung von bevorzugten Varianten kann das System ferner die oben beschriebene lokale Applikation auf einem mit dem Sicherheitselement kommunizierenden Endgerät beinhalten, sofern die entsprechende Ausführungsform eine lokale Applikation verwendet.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend anhand der beigefügten Figur 1 detailliert beschrieben. Diese Figur zeigt in schematischer Darstellung den Ablauf einer Variante des erfindungsgemäßen Verfahrens.

Das erfindungsgemäße Verfahren wird beispielhaft anhand eines Sicherheitselements in der Form eines SIM-Moduls erläutert. Dieses Modul ist eine

Karte, die in ein Mobilfunkgerät eingesetzt ist. Gegebenenfalls kann das SIM-Modul auch ein sog. embedded SIM-Element sein, welches integraler Bestandteil des Mobilfunkgeräts ist. Die Erfindung ist jedoch nicht auf SIM-Module beschränkt, sondern kann auch für beliebige andere Sicherheitselemente eingesetzt werden, wobei Beispiele solcher Sicherheitselemente im Vorangegangenen genannt wurden.

Ziel des nachfolgend beschriebenen Verfahren ist es, die in dem Sicherheitselement hinterlegte PIN über einen entfernten Servers zu verwalten und dabei durch Kommunikation des SIM-Moduls mit dem Server die PIN sowie entsprechende Vorgaben für die Struktur bzw. Verwendung der PIN zu ändern. Die PIN ist dabei ein Code, der vertraulich ist und durch den Benutzer des Mobilfunkgeräts bei Bedarf über eine entsprechende Benutzerschnittstelle am Gerät eingegeben werden kann, um z.B. das SIM-Modul als Ganzes freizuschalten oder ggf. auch nur bestimmte kryptographische Schlüssel zu aktivieren. Mit anderen Worten können in dem SIM-Modul ggf. auch mehrere PINs für unterschiedliche kryptographische Schlüssel hinterlegt sein, welche alle über einen entfernten Server verwaltet werden.

In dem in Fig. 1 gezeigten Ablaufdiagramm bezeichnet das Bezugszeichen SE das Sicherheitselement in der Form des SIM-Moduls, das Bezugszeichen S einen entfernt vom Sicherheitsmodul angeordneten Server, der zur Verwaltung der Daten des Moduls dient, sowie das Bezugszeichen LA einen lokalen Agenten, d.h. eine Software-Applikation, die auf dem Mobilfunkgerät hinterlegt ist, in dem sich das Sicherheitselement SE befindet. Gemäß Fig. 1 erhält der Server S zunächst ein Kommando CO, das ihn anweist, ein Datenelement auf dem Sicherheitselement SE zu verändern. Dieses Datenelement ist in Fig. 1 mit D bezeichnet und umfasst Verwaltungsdaten in der Form eines Headers H sowie Nutzdaten P, die den eigentlichen Dateninhalt betreffen. Diese

Nutzdaten stellen in der Ausführungsform der Fig. 1 eine entsprechende PIN für das SIM-Modul dar. Der Header H umfasst die oben erwähnten Vorgaben für die Struktur bzw. Verwendung der PIN.

Das Kommando CO kann z.B. durch den Benutzer des SIM-Moduls bzw. des Mobilfunkgeräts ausgelöst werden, vorzugsweise über eine Telefon-App, ein Webportal oder einen Anruf des Benutzers bei einem Call-Center. Dabei wird jeweils eine Sicherheitsabfrage des Servers beim Benutzer zur Authentisierung durchgeführt. Ggf. kann der Server S auch von sich aus eine Änderung der PIN auslösen, wenn sich beispielsweise die Regeln für die Struktur der PIN (z.B. fünfstellige PIN anstatt vierstellige PIN) geändert haben. In der hier beschriebenen Ausführungsform der Erfindung wird zum einen die in dem Sicherheitselement SE hinterlegte PIN zurückgesetzt und zum anderen die Vorgabe für eine neue festzulegende PIN dahingehend verändert, dass die PIN anstatt von vier Stellen fünf Stellen umfassen muss.

Nach der Generierung des Kommandos CO sendet der Server S eine erste Teiländerungsanforderung CR1 an das Sicherheitselement SE. Diese erste Teiländerungsanforderung dient zur Spezifikation der Ungültigkeit der aktuellen PIN und wird vom entfernten Server über einen sog. OTA-Kanal (OTA = Over the Air) an das Sicherheitselement direkt (d.h. ohne Zwischenschaltung des lokalen Agenten LA) übermittelt. Zum Schutz der ersten Teiländerungsanforderung wird in der hier beschriebenen Ausführungsform das sichere SCP-Protokoll der GlobalPlatform Card Spezifikation 2.1.1 verwendet (SCP = Secure Channel Protocol).

Die erste Teiländerungsanforderung CR1 stellt in der hier beschriebenen Variante eine binäre SMS dar, die nach Übermittlung über den OTA-Kanal an das Sicherheitselement SE dort einen ersten Speicherzugriff AC1 auf das Si-

cherheitselement auslöst, der die aktuelle PIN invalidiert, indem der Header H des Datenelements D auf einen Status gesetzt wird, der die Ungültigkeit der PIN anzeigt. Die durch die PIN gesicherten Funktionen, primär kryptographische Funktionen und/oder eine Anwendung, sind daraufhin gesperrt und nicht mehr benutzbar.

Nach Durchführung des ersten Speicherzugriffs wird von dem Sicherheitselement SE eine Bestätigung („ok") an den Server S gesendet. Zu diesem Zeitpunkt ist ein erster Teilschritt zum Ändern des Datenelements D basierend auf der ersten Teiländerungsanforderung abgeschlossen. Entkoppelt von diesem Teilschritt erfolgt über einen separaten Kanal die Durchführung eines zweiten Teilschritts, bei dem mittels einer zweiten Teiländerungsanforderung die Vorgabe für die PIN dahingehend geändert wird, dass die PIN mindestens fünf Stellen umfassen muss. Hierzu wird die zweite Teiländerungsanforderung CR2 an das Sicherheitselement SE übermittelt. Zur Entkopplung des zweiten Teilschritts von dem ersten Teilschritt wird die zweite Teiländerungsanforderung vorzugsweise über einen anderen als den oben beschriebenen OTA-Kanal an das Sicherheitselement übertragen. Zum Beispiel kann die Übertragung über eine (sichere) Internetverbindung bzw. HTTP-basiert durch die Zwischenschaltung des lokalen Agenten LA erfolgen, wie in Fig. 1 angedeutet ist. Nichtsdestotrotz kann ggf. auch der oben beschriebene OTA-Kanal zur Übermittlung der zweiten Teiländerungsanforderung eingesetzt werden. In diesem Fall kann die Entkopplung des ersten und zweiten Teilschritts lediglich dadurch sichergestellt werden, dass die beiden Teilschritte zu unterschiedlichen Zeitpunkten durchgeführt werden.

Gemäß Fig. 1 wird im Rahmen des zweiten Teilschritts die zweite Änderungsanforderung CR2 zunächst zusammen mit einer PUK an den lokalen Agenten LA übermittelt. Die aus dem Stand der Technik bekannte PUK stellt

eine vertrauliche Information des Sicherheitselements SE dar, welche dazu benötigt wird, eine Änderung einer PIN veranlassen zu können. Die zweite Teiländerungsanforderung CR2 enthält eine Kennung, dass es sich hierbei um ein PIN-Reset-Kommando handelt, wobei sich das Kommando je nach Ausführungsform lediglich auf einen Schlüssel in dem Sicherheitselement oder auch auf das ganze Sicherheitselement beziehen kann. Darüber hinaus enthält die zweite Teiländerungsanforderung nunmehr die neue Vorgabe für die Struktur bzw. Verwendung der PIN, d.h. es wird festgelegt, dass die PIN eine Länge von mindestens fünf Stellen aufweisen muss.

Ggf. kann die zweite Teiländerungsanforderung auch noch weitere Vorgaben für die PIN und deren Verwendung enthalten, welche bei Bedarf auch gegenüber den ursprünglichen Vorgaben für die PIN verändert sein können. Entsprechende Vorgaben können neben einer minimalen PIN-Länge auch eine maximale PIN-Länge spezifizieren sowie einen Fehlbedienungszähler, der anzeigt, wie oft eine PIN durch einen Benutzer falsch eingegeben werden darf, bevor das Sicherheitselement gesperrt wird. Die Vorgaben können ferner kodierte Informationen über die Güte der PIN betreffen. Beispielsweise kann spezifiziert werden, ob die PIN numerische und/oder alphanumerische Zeichen umfassen darf bzw. muss. Ferner können die Vorgaben festlegen, ob die PIN eine bestimmte Anzahl von Sonderzeichen oder Großbuchstaben umfassen muss bzw. inwieweit die PIN eine bestimmte Mindestanzahl von unterschiedlichen Zeichen beinhalten muss. Ferner kann durch die Vorgaben festgelegt werden, wie viele gleiche Zeichen in der PIN maximal hintereinander folgen dürfen. Ggf. kann durch die Vorgaben auch die Lebensdauer der PIN für eine maximale Anzahl von Zugriffen auf das Sicherheitselement spezifiziert werden.

Nach Empfang der zweiten Teiländerungsanforderung CR2 und der PUK P' im lokalen Agenten LA wird im Rahmen des zweiten Teilschritts die Änderung der PIN angestoßen. Dies kann sofort oder bei der nächsten Benutzung des Sicherheitselements bzw. des entsprechenden, über die PIN geschützten Schlüssels (z.B. Anfordern einer kryptographischen Operation) erfolgen. Dabei wird das SIM-Toolkit des SIM-Moduls oder eine ähnliche Software-Instanz auf dem Mobilfunkgerät antriggert, woraufhin die zweite Teiländerungsanforderung CR2 (ohne PUK) an das Sicherheitselement SE übermittelt wird. Anschließend wird mittels eines zweiten Speicherzugriffs AC2 auf das Sicherheitselement SE der Header H des Datenelements D entsprechend der neuen Vorgaben aus der zweiten Teiländerungsanforderung CR2 geändert.

Im Rahmen des zweiten Teilschritts wird ferner an dem Display des Mobilfunkgeräts ein Dialog ausgelöst, der in FIG. 1 mit DI bezeichnet ist. Dabei wird der Benutzer dazu aufgefordert, eine neue fünfstellige PIN für das SIM-Modul einzugeben. Nach erfolgter Eingabe wird die neue mit NP bezeichnete PIN zusammen mit der PUK P' an das Sicherheitselement SE übermittelt. Das SIM-Toolkit oder eine entsprechende Software-Instanz löst dann eine sog. APDU aus (APDU = Application Protocol Data Unit), die ein Setzen der neuen PIN bedeutet. Dabei wird die PUK dahingehend überprüft, ob sie dem Sicherheitselement zugeordnet ist. Nur in diesem Fall wird die alte PIN durch die neue PIN ersetzt. Die Speicherung der neuen PIN kann als ein Bestandteil des zweiten Speicherzugriffs AC2 zum Ändern der Nutzdaten P des Datenelements D aufgefasst werden.

Es ist darauf hinzuweisen, dass somit auch zwei Regeln eingehalten werden. Die PUK wird gesichert übertragen, insbesondere ohne dass der Benutzer sie zu Gesicht bekommt. Die PIN wird vom Benutzer vergeben und nicht über das Netz übertragen. Die PUK ist ein weiteres auf dem Sicherheitselement

gespeichertes Datenelement, welches der PIN P, in der Regel über einen im Header H enthaltenen Verweis und/oder eine Zugriffsbedingung zugeordnet ist.

Die im Vorangegangenen beschriebene Ausführungsform des erfindungsgemäßen Verfahrens weist eine Reihe von Vorteilen auf. Insbesondere wird eine entfernte Verwaltung der PIN eines Sicherheitselements erreicht, ohne dass durch den Benutzer eine Serviceeinrichtung aufgesucht werden muss. Dabei wird die Sicherheit der entfernten Verwaltung dadurch erhöht, dass die entsprechenden Änderung der PIN bzw. der Verwaltungsdaten der PIN in einem zweistufigen Verfahren durchgeführt wird. Insbesondere können neben der eigentlichen PIN auch entsprechende Vorgaben für die PIN geändert werden.

Patentansprüche

1. Verfahren zum entfernten Verwalten eines auf einem Sicherheitselement (SE) gespeicherten Datenelements (D), bei dem eine Änderungsanforderung für das Datenelement (D), welche zumindest zum Teil von einem Server (S) stammt, an das Sicherheitselement (SE) übermittelt wird, woraufhin in dem Sicherheitselement (SE) das darin gespeicherte Datenelement (D) geändert wird, wobei die Änderung einen ersten ändernden Speicherzugriff (AC1) und einen zweiten ändernden Speicherzugriff (AC2) auf das Sicherheitselement (SE) umfasst,
dadurch gekennzeichnet, dass
der erste Speicherzugriff (AC1) und der zweite Speicherzugriff (AC2) in voneinander entkoppelten Teilschritten der Änderung erfolgen, wobei ein erster Teilschritt das Übermitteln einer ersten Teiländerungsanforderung (CR1) aus der Änderungsanforderung von dem Server (S) zu dem Sicherheitselement (SE) sowie den ersten Speicherzugriff (AC1) umfasst und wobei ein zweiter Teilschritt das Übermitteln einer zweiten Teiländerungsanforderung (CR2) aus der Änderungsanforderung zu dem Sicherheitselement (SE) und den zweiten Speicherzugriff (AC2) umfasst.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Teilschritte dadurch voneinander entkoppelt sind, dass:
   - der erste Teilschritt zu einem anderen Zeitpunkt als der zweite Teilschritt ausgeführt wird, und/oder
   - der erste Teilschritt einen anderen Verbindungstyp zum Übermitteln der ersten Teiländerungsanforderung (CR1) nutzt als der zwei-

te Teilschritt zum Übermitteln der zweiten Teiländerungsanforderung (CR2), und/oder

- der erste Teilschritt eine andere lokale Applikation (LA) auf einem mit dem Sicherheitselement (SE) kommunizierenden Endgerät als der zweite Teilschritt nutzt, und/oder
- der erste Teilschritt eine andere Rückmeldung zur Bestätigung des ersten Speicherzugriffs (AC1) ausgibt als der zweite Teilschritt zur Bestätigung des zweiten Speicherzugriffs (AC2) oder nur der erste oder zweite Teilschritt eine Rückmeldung zur Bestätigung des ersten bzw. zweiten Speicherzugriffs (AC1, AC2) ausgibt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die erste Teiländerungsanforderung (CR1) direkt ohne Zwischenschaltung einer lokalen Applikation (LA) auf einem mit dem Sicherheitselement (SE) kommunizierenden Endgerät von dem Server (S) an das Sicherheitselement (SE) übermittelt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweite Teiländerungsanforderung (CR2) von dem Server (S), vorzugsweise unter Zwischenschaltung einer lokalen Applikation (LA) auf einem mit dem Sicherheitselement (SE) kommunizierenden Endgerät, an das Sicherheitselement (SE) übermittelt wird und/oder ohne Beteiligung des Servers (S) von einer lokalen Applikation (LA) auf einem mit dem Sicherheitselement (SE) kommunizierenden Endgerät an das Sicherheitselement (SE) übermittelt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erste Teiländerungsanforderung (CR1) eine Änderungsanweisung umfasst und den zu ändernden Dateninhalt des

Datenelements (D) spezifiziert und/oder die zweite Teiländerungsanforderung (CR2) eine Änderungsanweisung umfasst und den zu ändernden Dateninhalt des Datenelements (D) spezifiziert.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erste Teiländerungsanforderung (CR1) ein größeres oder kleineres Datenvolumen als die zweite Teiländerungsanforderung (CR2) aufweist.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das zu ändernde Datenelement (D) Verwaltungsdaten (H) und Nutzdaten (P) umfasst.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass die Nutzdaten (P) vertrauliche Informationen und insbesondere Benutzeridentifikationsdaten, vorzugsweise ein vom Benutzer einzugebendes Passwort zur Freischaltung einer oder mehrerer Funktionen des Sicherheitselements (SE), umfassen.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die erste Teiländerungsanforderung (CR1) einen ersten Speicherzugriff zur Invalidierung der Benutzeridentifikationsdaten spezifiziert.

10. Verfahren nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, dass die Verwaltungsdaten (H) eine oder mehrere Vorgaben für die Struktur und/oder Verwendung von Benutzeridentifikationsdaten spezifizieren.

11. Verfahren nach einem der Ansprüche 7 bis 10, dadurch gekennzeichnet, dass die erste und/oder zweite Teiländerungsanforderung (CR2) einen ersten bzw. zweiten Speicherzugriff zum Ändern zumindest eines Teils der Verwaltungsdaten (H) spezifiziert.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die zweite Teiländerungsanforderung (CR2) einen zweiten Speicherzugriff zum Ändern von Benutzeridentifikationsdaten und/oder von einer oder mehreren Vorgaben für die Struktur und/oder Verwendung der Benutzeridentifikationsdaten spezifiziert.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Sicherheitselement eine SIM/USIM-Karte und/oder eine MikroSD-Karte und/oder einen USB-Token und/oder eine Chipkarte und/oder ein RFID-Modul und/oder ein TPM-Modul und/oder ein NFC-Modul und/oder ein embedded SIM-Modul und/oder eine TEE-Umgebung umfasst.

14. System zum entfernten Verwalten eines auf einem Sicherheitselement (SE) gespeicherten Datenelements (D), wobei das System zur Durchführung eines Verfahrens eingerichtet ist, bei dem eine Änderungsanforderung für das Datenelement (D), welche zumindest zum Teil von einem Server (S) stammt, an das Sicherheitselement (SE) übermittelt wird, woraufhin in dem Sicherheitselement (SE) das darin gespeicherte Datenelement (D) geändert wird, wobei die Änderung einen ersten ändernden Speicherzugriff (AC1) und einen zweiten ändernden Speicherzugriff (AC2) auf das Sicherheitselement (SE) umfasst,
dadurch gekennzeichnet, dass

der erste Speicherzugriff (AC1) und der zweite Speicherzugriff (AC2) in voneinander entkoppelten Teilschritten der Änderung erfolgen, wobei ein erster Teilschritt das Übermitteln einer ersten Teiländerungsanforderung (CR1) aus der Änderungsanforderung von dem Server (S) zu dem Sicherheitselement (SE) sowie den ersten Speicherzugriff (AC1) umfasst und wobei ein zweiter Teilschritt das Übermitteln einer zweiten Teiländerungsanforderung (CR2) aus der Änderungsanforderung zu dem Sicherheitselement (SE) und den zweiten Speicherzugriff (AC2) umfasst.

15. System nach Anspruch 14, dadurch gekennzeichnet, dass das System zur Durchführung eines Verfahrens nach einem der Ansprüche 2 bis 13 eingerichtet ist.

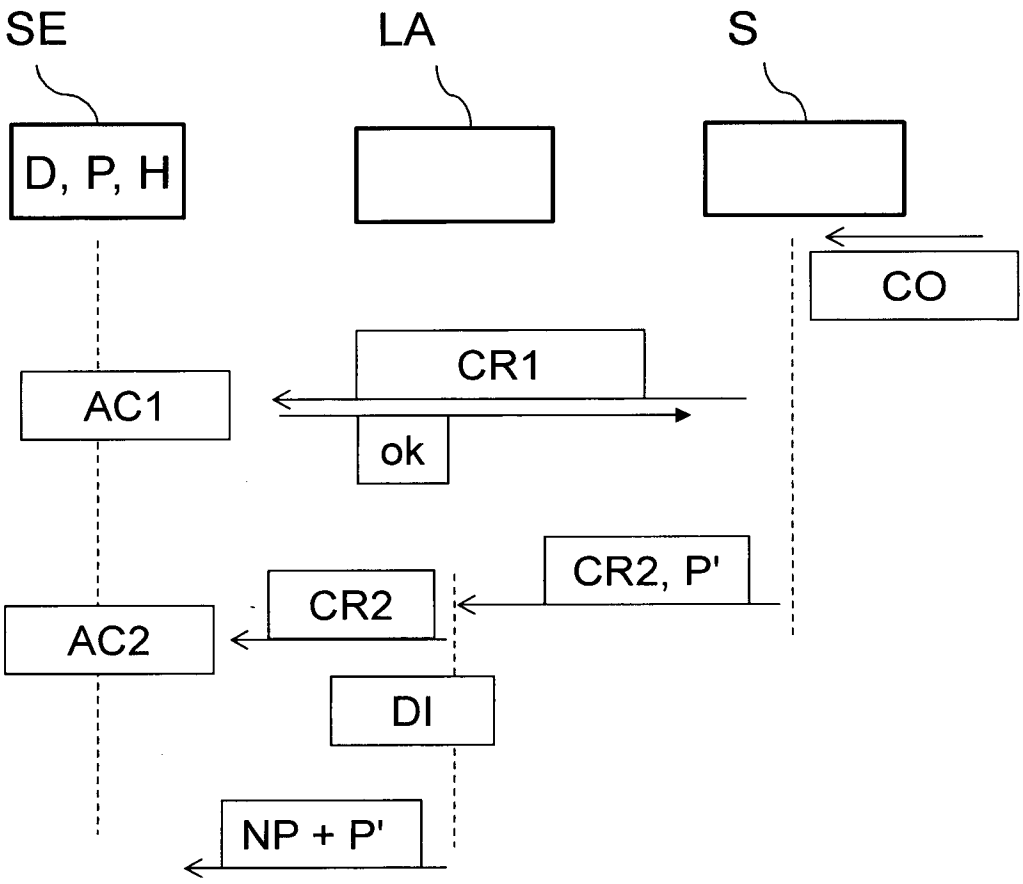

Fig. 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/000402

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/00 H04W8/18 H04W8/20
ADD.

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)
H04W

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 practicable, search terms used)
EPO-Internal, 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	US 2013/303122 A1 (LI LI [US] ET AL) 14 November 2013 (2013-11-14) page 5 - page 7; figures 4,5	1-15
A	WO 2009/091588 A2 (MICE GROUP HOLDINGS LTD E [CN]; CHAN YUEN WAH EVA; FUNG HENRY [US]) 23 July 2009 (2009-07-23) paragraph [00274] - paragraph [00275]; figure 20	1-15
A	EP 2 590 383 A1 (RESEARCH IN MOTION LTD [CA]) 8 May 2013 (2013-05-08) column 1 - column 6	1-15

☐ Further documents are listed in the continuation of Box C.

☒ 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 application or patent 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
27 April 2015	08/05/2015

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, Fax: (+31-70) 340-3016	Jardak, Christine

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/000402

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013303122 A1	14-11-2013	CN 104396289 A	04-03-2015
		DE 112013002437 T5	22-01-2015
		TW 201408110 A	16-02-2014
		US 2013303122 A1	14-11-2013
		US 2014349617 A1	27-11-2014
		WO 2013169484 A1	14-11-2013
WO 2009091588 A2	23-07-2009	US 2009198618 A1	06-08-2009
		WO 2009091588 A2	23-07-2009
EP 2590383 A1	08-05-2013	EP 2590383 A1	08-05-2013
		EP 2590384 A1	08-05-2013
		US 2013109308 A1	02-05-2013
		US 2013111598 A1	02-05-2013

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2015/000402

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04W4/00 H04W8/18 H04W8/20
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04W

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, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2013/303122 A1 (LI LI [US] ET AL) 14. November 2013 (2013-11-14) Seite 5 - Seite 7; Abbildungen 4,5	1-15
A	WO 2009/091588 A2 (MICE GROUP HOLDINGS LTD E [CN]; CHAN YUEN WAH EVA; FUNG HENRY [US]) 23. Juli 2009 (2009-07-23) Absatz [00274] - Absatz [00275]; Abbildung 20	1-15
A	EP 2 590 383 A1 (RESEARCH IN MOTION LTD [CA]) 8. Mai 2013 (2013-05-08) Spalte 1 - Spalte 6	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ 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" frühere Anmeldung oder Patent, die bzw. 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 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
27. April 2015	08/05/2015

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Jardak, Christine

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2015/000402

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2013303122 A1	14-11-2013	CN 104396289 A	04-03-2015
		DE 112013002437 T5	22-01-2015
		TW 201408110 A	16-02-2014
		US 2013303122 A1	14-11-2013
		US 2014349617 A1	27-11-2014
		WO 2013169484 A1	14-11-2013
WO 2009091588 A2	23-07-2009	US 2009198618 A1	06-08-2009
		WO 2009091588 A2	23-07-2009
EP 2590383 A1	08-05-2013	EP 2590383 A1	08-05-2013
		EP 2590384 A1	08-05-2013
		US 2013109308 A1	02-05-2013
		US 2013111598 A1	02-05-2013