

(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
21. Januar 2016 (21.01.2016)



(10) Internationale Veröffentlichungsnummer
WO 2016/008581 A1

(51) Internationale Patentklassifikation:
H04W 4/00 (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2015/001441

(22) Internationales Anmeldedatum:
13. Juli 2015 (13.07.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102014010698.5 18. Juli 2014 (18.07.2014) DE

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

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

Erklärungen gemäß Regel 4.17:

— hinsichtlich der Berechtigung des Anmelders, ein Patent zu
beantragen und zu erhalten (Regel 4.17 Ziffer ii)

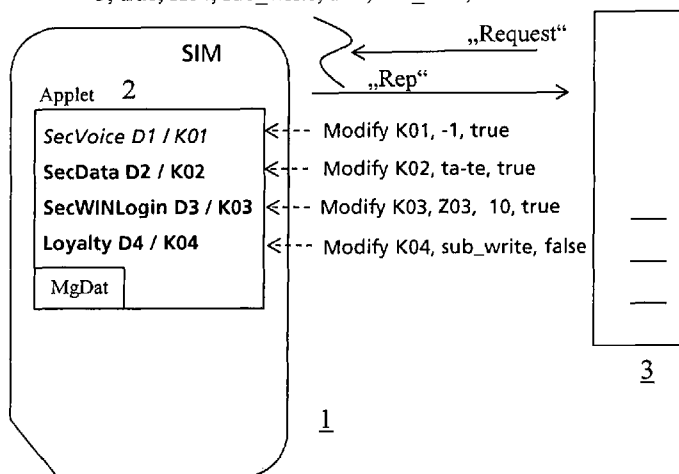
Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz
3)

(54) Title: PARTICIPANT IDENTITY MODULE HAVING A NUMBER OF SERVICES

(54) Bezeichnung : TEILNEHMERIDENTITÄTSMODUL MIT MEHREREN DIENSTEN

Rep: 4, true, K01, 0, false, K02, 0, false, K03, Z03,
5, true, K04, sub_write, true, sub_read, true



(57) Abstract: The invention relates to a participant
identity module (1) which is inserted or which can be
inserted into a mobile end device, and which has a
subscription and a number of services, which services
can have an activated and a deactivated status. The
services are implemented in a single applet (2) in the
participant identity module. The number of services are
individually manageably designed, wherein the applet
has a respective service management key for each service
that is individually manageably designed, said service
management key being designed in such a way that it can
have an activated and a deactivated status, corresponding
to an activated or deactivated status of each service. The
status of each service management key can be switched
between the activated and the deactivated status using a
management command directed at the service
management key, such that the service corresponding to
the service management key is activated or deactivated.

(57) Zusammenfassung: Die Erfindung schafft ein
Teilnehmeridentitätsmodul (1), eingesetzt oder einsetzbar
in ein mobiles Endgerät, mit einer Subskription und mit
mehreren Diensten, die einen aktivierten und einen
deaktivierten Status haben können.

[Fortsetzung auf der nächsten Seite]

Fig. 1

WO 2016/008581 A1



Die Dienste sind in einem einzigen Applet (2) im Teilnehmeridentitätsmodul implementiert. Die mehreren Dienste sind einzeln verwaltbar gestaltet, wobei das Applet für jeden Dienst, der einzeln verwaltbar gestaltet ist, einen eigenen Dienst- Verwaltungs-Schlüssel aufweist, der so gestaltet sind, dass er einen aktivierten und einen deaktivierten Status haben kann, der einem aktivierten bzw deaktivierten Status des jeweiligen Dienstes entspricht. Der Status des jeweiligen Dienst- Verwaltungs-Schlüssels ist mittels eines an den Dienst- Verwaltungs-Schlüssel gerichteten Verwaltungs-Kommandos zwischen dem aktivierten und dem deaktivierten Status schaltbar, so dass der dem Dienst- Verwaltungs-Schlüssel entsprechende Dienst aktiviert bzw. deaktiviert wird.

Teilnehmeridentitätsmodul mit mehreren Diensten

Die Erfindung betrifft ein Teilnehmeridentitätsmodul mit mehreren Diensten, die zusätzlich zu einer implementierten oder noch zu implementierenden Subskription zur Nutzung eines Endgeräts in einem Mobilfunknetz im Teilnehmeridentitätsmodul implementiert sind.

Zur Nutzung eines mobilen Endgeräts wie Smartphones oder Mobiltelefons in einem Mobilfunknetzwerk eines Netzbetreibers enthält das Endgerät ein Teilnehmeridentitätsmodul mit einer Subskription. Die Subskription ist durch einen Datensatz gebildet, der den Aufbau, Betrieb und Abbau einer Verbindung des Endgeräts im Mobilfunknetzwerk ermöglicht, und umfasst beispielsweise einen kryptographischen Authentisierungs-Schlüssel Ki und eine International Mobile Subscriber Identity IMSI. Das Teilnehmeridentitätsmodul kann entweder als entfernbare Plug-In SIM-Karte (SIM = Subscriber Identity Module) oder USIM-Karte (Universal SIM) oder UICC (Universal Integrated Circuit Card) gestaltet sein, oder alternativ als festeingelötete eUICC (embedded UICC) oder eSIM oder eUSIM.

In zunehmendem Maß werden in das Teilnehmeridentitätsmodul, zusätzlich zum eigentlichen Grund-Dienst Sprachverbindung (Telefonie) und ggf. Datenverbindung, zusätzliche Dienste implementiert, wie beispielsweise Dienste für Verschlüsselung von Sprachverbindungen oder Datenverbindungen, Zahlungsverkehr, Loyalty (d.h. Bonuspunkte-Programme), Login zu Daten- und Rechenressourcen und dergleichen.

Die zusätzlichen Dienste sind durch im Teilnehmeridentitätsmodul implementierte Applets implementiert. Mit an das Applet eines Diensts gerichteten Applet-Lifecycle-Kommandos lässt sich der Dienst ansteuern und verwalten. Beispielsweise lässt sich mit den Applet-Lifecycle-Kommandos ein Dienst Löschen, Sperren oder Entsperren.

Bei einem gemäß [1] GPCS 2.1.1., „Global Platform Card Specification, Version 2.1.1, March 2003“, eingerichteten Teilnehmeridentitätsmodul lässt sich beispielsweise mittels des in Kapitel 9.2 beschriebenen DELETE-Kommandos ein Applet löschen. Gemäß [1] GPCS 2.1.1, Kapitel 6.7.1 Application Locking, lässt sich mit dem Lifecycle-Kommando SET STATUS LOCKED ein Applet in den gesperrten Zustand versetzen, und analog auch wieder entsperren.

Damit jeder Dienst einzeln ansteuerbar und verwaltbar ist (z.B. mittels DELETE gemäß [1] GPCS 2.1.1), ist in derzeit verwirklichten Implementierungen für jeden Dienst ein eigenes Applet implementiert. Diese Implementierungsart ist speicherintensiv. Die denkbare Alternative, alle Dienste in einem einzigen Applet zu verwirklichen hat den Nachteil, dass mit einem Applet-Lifecycle-Kommando nur das Applet als Ganzes ansteuerbar und verwaltbar ist, nicht jedoch selektiv ein einzelner Dienst.

Der Erfindung liegt die Aufgabe zu Grunde, ein Teilnehmeridentitätsmodul mit mehreren Diensten zu schaffen, die speichersparend implementiert sind und bei dem zugleich die Dienste einzeln verwaltbar sind.

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

Das erfindungsgemäße Teilnehmeridentitätsmodul (z.B. Plug-In (U)SIM-Karte, oder alternativ festeingelötetes oder anderweitig embedded Secure Element) nach Anspruch 1 ist eingesetzt oder einsetzbar in ein mobiles Endgerät, z.B. Smartphone, Mobiltelefon oder dergleichen. Im Teilnehmeridentitätsmodul implementiert oder noch zu implementieren ist eine Subskription

zur Nutzung des mobilen Endgeräts in einem Mobilfunknetz. Weiter sind im Teilnehmeridentitätsmodul mehrere von der Subskription i.W. unabhängige Dienste implementiert. Die Dienste können einen aktivierten Status haben, in dem sie funktionsfähig sind, und einen deaktivierten Status, in dem sie nicht
5 funktionsfähig sind und erst aktiviert werden müssen, damit sie funktionsfähig sind.

Das Verfahren zeichnet sich dadurch aus, dass die Dienste in einem einzigen Applet im Teilnehmeridentitätsmodul implementiert sind. Die mehreren
10 Dienste sind dabei jedoch einzeln verwaltbar gestaltet. Das Applet hat hierzu für jeden Dienst, der einzeln verwaltbar gestaltet ist, einen eigenen Dienst-Verwaltungs-Schlüssel, der so gestaltet ist, dass er einen aktivierten und einen deaktivierten Status haben kann, der einem aktivierten bzw. deaktivierten Status des jeweiligen Dienstes entspricht. Der Status des jeweiligen
15 Dienst-Verwaltungs-Schlüssels ist mit einem an den Dienst-Verwaltungs-Schlüssel gerichteten Verwaltungs-Kommando zwischen dem aktivierten und dem deaktivierten Status schaltbar. Hierdurch wird der dem Dienst-Verwaltungs-Schlüssel entsprechende Dienst aktiviert bzw. deaktiviert.

20 Da die mehreren Dienste in einem einzigen Applet eingerichtet sind, ist der Verwaltungsdatenbereich (auch Metadaten genannt) des Applets nur ein einziges Mal erforderlich. Somit lässt sich auch hier Speicherplatz sparen. Andererseits ist durch die (de)aktivierbaren Dienst-Verwaltungs-Schlüssel ein Mechanismus zur feingranularen Verwaltung der Dienste innerhalb des
25 Applet geschaffen, wie er herkömmlicherweise nur erreicht wird, indem für jeden Dienst eine eigene Applet-Instanz im Teilnehmeridentitätsmodul implementiert wird.

Daher ist gemäß Anspruch 1 ein Teilnehmeridentitätsmodul geschaffen, das beide Anforderungen der speichersparenden Implementierung und der Einzel-Verwaltbarkeit der einzelnen Dienste erfüllt.

- 5 Das Verwaltungs-Kommando ist wahlweise mit einem oder mehrere Parametern parametrisiert. Als Parameter ist bzw. sind wahlweise einer oder mehrere der folgenden vorgesehen. Ein Aktivierungs-Zeitraum oder Deaktivierungs-Zeitraum, für welchen der Dienst-Verwaltungs-Schlüssel in den aktivierten bzw. deaktivierten Status geschaltet wird. Nach Ablauf des Zeit-
- 10 raums fällt der Dienst-Verwaltungs-Schlüssel ohne weiteres Zutun in den Status vor dem Schalten zurück (z.B. deaktivierter Status; alternativ auch möglich: aktivierter Status). Eine Anzahl oder Höchstzahl von möglichen Aktivierungen des Dienst-Verwaltungs-Schlüssels, d.h. wie oft oder wie oft höchstens der Dienst-Verwaltungs-Schlüssels aktiviert werden kann. Eine
- 15 Anzahl oder Höchstzahl von möglichen Anwendungen des Dienstes. Wurde der Dienst-Verwaltungs-Schlüssel die mögliche Anzahl Male verwendet, wird ohne weiteres Zutun der Dienst-Verwaltungs-Schlüssel und damit der Dienst deaktiviert. Für einen Dienst-Verwaltungs-Schlüssel können Gültigkeits-Zeitraum und zulässige Anzahl oder Höchstzahl von Anwendungen
- 20 auch gleichzeitig vorgesehen sein. Weiter kann als Parameter eine Unterfunktionalität eines Dienstes angegeben sein.

Falls als Parameter eine zulässige Anzahl Anwendungen vorgesehen ist, hat das Teilnehmeridentitätsmodul wahlweise zudem einen Schlüsselzähler, die

25 die Anzahl bereits erfolgter oder noch zulässiger Anwendungen des Schlüssels mitverfolgt. Wahlweise lässt sich durch ein Verwaltungs-Kommando, mit dem eine neue zulässige Anzahl festgelegt wird, zudem auch der Schlüsselzähler entsprechend ändern.

Wahlweise verursacht der Empfang des Verwaltungs-Kommando beim Teilnehmeridentitätsmodul, dass der Status des Applets geprüft wird, z.B. ob das Applet selbst aktiviert oder deaktiviert ist. Nur falls das Applet im Status aktiviert ist, werden weiter Dienst-Verwaltungs-Schlüssel und damit
5 Dienste aktiviert. Bei deaktiviertem Applet wird die Aktivierung von Dienst-Verwaltungs-Schlüsseln und Diensten beispielsweise abgebrochen.

Als Dienst ist/sind wahlweise einer oder mehrere der folgenden vorgesehen. Ein Sprachverschlüsselungs-Dienst zur Verschlüsselung von im Mobilfunk-
10 netz übertragenen Sprachdaten. Ein Datenverschlüsselungs-Dienst zur Verschlüsselung von im Mobilfunknetz übertragenden Daten, die keine Sprachdaten sind. Ein Zugriffs-Dienst, d.h. ein Login-Dienst, für Daten- oder/und Rechenressourcen eines Computersystems. Ein Loyalty-Dienst (Bonuspunkte-Programm-Dienst) zur Verwaltung von Bonuspunkten. Ein Ticketing-
15 Dienst zur Verwaltung von elektronischen Tickets für ein Verkehrsmittelsystem (=Transitsystem) oder für ein Eintrittskartensystem.

Der Dienst-Verwaltungs-Schlüssel ist wahlweise als privater oder öffentlicher, vorzugsweise privater, Schlüssel eines PKI-Schlüsselpaars gestaltet.
20

Das Teilnehmeridentitätsmodul ist wahlweise weiter dazu eingerichtet, gemäß dem Secure Channel Protocol SCP gemäß Global Platform Card Specification, insbesondere Version 2.1.1, March 2003, oder Nachfolgeversion, zu kommunizieren. Das Verwaltungs-Kommando ist in diesem Fall wahlweise
25 als ein zusätzliches Lifecycle-Kommando gestaltet, und kann strukturell ähnlich wie die bereits vorhandenen Lifecycle-Kommandos für Karten und Applets gestaltet sein. Im Unterschied zu bekannten Lifecycle-Kommandos wird durch das erfindungsgemäße Verwaltungs-Kommando eine Unterstruktur innerhalb eines Applets beeinflusst. Durch die Parametrisierung des Verwal-

tungs-Kommandos mit Parametern wird eine noch feinere Unterstruktur innerhalb des Applets geschaffen, die sich selektiv verwalten, steuern und beeinflussen lässt.

- 5 Wahlweise ist das Verwaltungs-Kommando zum Versenden über das Mobilfunknetz gestaltet, wahlweise zum Versenden in einer gesicherten Form, so dass ein Nutzer des Endgeräts keinen Zugriff auf das Verwaltungs-Kommando hat, insbesondere als durch das Teilnehmeridentitätsmodul interpretierbares Steuer-Kommando, insbesondere in einer verschlüsselten
- 10 binären Kurznachrichtendienst-Nachricht wie z.B. einer binären SMS gemäß dem SCP-Protokoll. Eine binäre SMS ist verschlüsselt und durch das Teilnehmeridentitätsmodul interpretierbar. Andererseits ist eine binäre SMS für einen Nutzer des Endgeräts, in dem das Teilnehmeridentitätsmodul betrieben wird, nicht sichtbar und wegen der Ende-zu-Ende-Verschlüsselung vom
- 15 Sender bis in das Teilnehmeridentitätsmodul auch nicht interpretierbar. Somit kann das Teilnehmeridentitätsmodul das in der binären SMS enthaltenen Verwaltungs-Kommando aus der binären SMS extrahieren und ausführen. Ein Nutzer kann hingegen das Verwaltungs-Kommando nicht manipulieren.
- 20 Bei einem erfindungsgemäßen Verfahren zum Aktivieren eines Dienstes in einem erfindungsgemäßen Teilnehmeridentitätsmodul werden folgende Schritte durchgeführt. Von einem Server wird an das Teilnehmeridentitätsmodul ein Verwaltungs-Kommando für einen oder mehrere der Dienst-Verwaltungs-Schlüssel gesendet. Im Teilnehmeridentitätsmodul wird das
- 25 Verwaltungs-Kommando ausgewertet und der Status des jeweiligen Dienst-Verwaltungs-Schlüssels entsprechend dem Verwaltungs-Kommando geschaltet. Hierdurch wird der jeweilige Dienst entsprechend dem Verwaltungs-Kommando aktiviert bzw. deaktiviert.

Wahlweise wird ein Teilnehmeridentitätsmodul mit einem Applet mit mehreren Diensten bereitgestellt, die für Dienst-Verwaltungs-Schlüssel eingerichtet sind, die aber die Dienst-Verwaltungs-Schlüssel noch nicht enthalten. Um die Dienste zu aktivieren oder zumindest aktivierbar zu machen, werden
5 den Dienst-Verwaltungs-Schlüssel für die Dienste in das Applet geladen. Wahlweise werden die Dienste bereits durch das Laden der Dienst-Verwaltungs-Schlüssel aktiviert. Alternativ können die Dienst-Verwaltungs-Schlüssel und damit die Dienste durch ein nachfolgend an das Teilnehmeridentitätsmodul gesendetes Verwaltungs-Kommando aktiviert werden.

10

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

Fig. 1 eine SIM-Karte mit einem Applet mit mehreren Diensten, gemäß einer
15 Ausführungsform der Erfindung.

Fig. 1 zeigt, als ein beispielhaftes Teilnehmeridentitätsmodul 1, eine SIM-Karte 1 mit einem Applet 2 mit mehreren Diensten D1, D2, D3, D4, gemäß einer Ausführungsform der Erfindung. D1 ist ein Dienst zur Sprachverschlüsselung für Sprachverbindungen im Mobilfunknetz. D2 ist ein D1 ist
20 ein Dienst zur Datenverschlüsselung für Datenverbindungen im Mobilfunknetz. D3 ist ein Dienst für Zugang (Login) zu Daten- und Rechenressourcen an einem Computer. D4 ist ein Loyalty-Dienst, d.h. ein Bonuspunkt-Dienst. Die vier Dienste D1, D2, D3, D4 sind in einem einzigen Applet 2 implementiert, das nur einen einzigen Verwaltungsbereich MgDat hat, der für alle vier
25 Dienste bereitsteht.

Die SIM-Karte 1 aus Fig. 1 ist zur Verarbeitung von Secure Channel Kommandos gemäß [1] GPCS 2.1.1, „Global Platform Card Specification, Version

2.1.1, March 2003" eingerichtet, die ein Server 3 über einen OTA Kanal an die SIM-Karte 1 sendet (OTA = over the air). Mit Statuskommandos kann der Server 3 zunächst den Status des Applets 2 und der Dienste D1, D2, D3, D4 abrufen. Mit einer Status-Anfrage „Request“ an das Applet 2 ruft der Server
5 3 alle Schlüssel des Applets 2 einschließlich des Status des jeweiligen Schlüssels (z.B. aktiviert oder deaktiviert) ab. Falls in der SIM-Karte Zertifikate zu den Schlüsseln abgespeichert sind, werden die Zertifikate und ihre Stati ebenfalls abgerufen. Die SIM-Karte aus Fig. 1 sendet auf die Status-Anfrage hin z.B. folgende Antwort „Rep“ an den Server 3: <4, true, K01, 0, false, K02,
10 0, false, K03, Z03, 5, true, K04, sub_write, true, sub_read, true>. Die Antwort bedeutet Folgendes. Das Applet 2 enthält 4 Schlüssel (für 4 Dienste), das Applet ist in aktiviertem Zustand („true“). Der erste Schlüssel K01 hat die ID01, lässt eine Anzahl von 0 (Null) Nutzungen zu und ist deaktiviert („false“). Der zweite Schlüssel K02 hat die ID02, lässt eine Anzahl von 0 (Null)
15 Nutzungen zu und ist deaktiviert („false“). Der dritte Schlüssel K03 hat die ID03, ein Zertifikat Z03 mit ID03, lässt fünf Nutzungen zu und ist aktiviert („true“). Im Zertifikat Z03 kann insbesondere auch ein maximaler Gültigkeitszeitraum des Schlüssels abgelegt sein, so dass die höchstens fünf Nutzungen nur höchstens innerhalb des Gültigkeitszeitraums erfolgen können.
20 Der vierte Schlüssel K04 hat die ID04, die Unterfunktionalität Punkte zu schreiben „sub_write“ ist aktiviert („true“), die Unterfunktionalität Punkte zu lesen „sub_read“ ist ebenfalls aktiviert („true“).

Mit einem Verwaltungs-Kommando „Modify“ (Pseudo-Code für verändern)
25 kann der Server 3 den Status des Applets 2 und der Dienste ändern. Mit dem Verwaltungs-Kommando <Modify K01, -1, true> wird z.B. der Status des Dienstes D1 aktiviert (auf „true“ gesetzt), mit unbegrenzter Gültigkeitsdauer (Parameter Gültigkeitszeitraum hat den Wert -1). Mit dem Verwaltungs-Kommando <Modify K02, ta-te, true> wird der Status des Dienstes D2 akti-

viert (auf „true“ gesetzt), mit Gültigkeitsdauer beginnend am Datum/Zeitpunkt ta und endend am Datum/Zeitpunkt te (Parameter Gültigkeitszeitraum hat den Wert ta-te), z.B. hexadezimal 34929478582AE6-34929478582F08. Mit dem Verwaltungs-Kommando <Modify K03, Z03, 10, true> wird der Status des bereits aktivierten Dienstes D3 beibehalten („true“), und der Gültigkeitsdauer von 5 auf 10 Anwendungen erhöht (Parameter Gültigkeit von Wert 5 auf 10 geändert). Mit <Modify K04, sub_write, false> wird die Unterfunktionalität Punkte schreiben des Loyalty-Dienstes 4 deaktiviert (neuer Status „false“). Die andere Unterfunktionalität Punkte lesen sub_read des Loyalty-Dienstes 4 bleibt unverändert in aktiviertem Status.

Zitierte Literatur

15

[1] GPCS 2.1.1, „Global Platform Card Specification, Version 2.1.1, March 2003“

Patentansprüche

1. Teilnehmeridentitätsmodul (1), eingesetzt oder einsetzbar in ein mobiles Endgerät, mit einer im Teilnehmeridentitätsmodul (1) implementierten oder
5 noch zu implementierenden Subskription zur Nutzung des mobilen Endgeräts in einem Mobilfunknetz, und mit mehreren im Teilnehmeridentitätsmodul (1) implementierten Diensten (D1, D2, D3, D4), die so gestaltet sind, dass sie einen aktivierten und einen deaktivierten Status haben können,
dadurch gekennzeichnet, dass
- 10 die Dienste (D1, D2, D3, D4) in einem einzigen Applet (2) im Teilnehmeridentitätsmodul (1) implementiert sind und
die mehreren Dienste (D1, D2, D3, D4) einzeln verwaltbar gestaltet sind, wobei das Applet (2) für jeden Dienst, der einzeln verwaltbar gestaltet ist, einen eigenen Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) aufweist, der so
15 gestaltet ist, dass er einen aktivierten und einen deaktivierten Status haben kann, der einem aktivierten bzw deaktivierten Status des jeweiligen Dienstes entspricht, wobei der Status des jeweiligen Dienst-Verwaltungs-Schlüssels (K01, K02, K03, K04) mittels eines an den Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) gerichteten Verwaltungs-Kommandos zwischen dem
20 aktivierten und dem deaktivierten Status schaltbar ist, so dass der dem Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) entsprechende Dienst (D1, D2, D3, D4) aktiviert bzw. deaktiviert wird.
2. Teilnehmeridentitätsmodul (1) nach Anspruch 1, wobei das Verwaltungs-
- 25 Kommando mit einem oder mehreren Parametern parametrisiert ist, wobei als Parameter einer oder mehrere der folgenden vorgesehen ist/sind:
- ein Aktivierungs-Zeitraum oder Deaktivierungs-Zeitraum, für welchen der Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) in den aktivierten bzw. deaktivierten Status geschaltet wird;
 - 30 - eine Anzahl oder Höchstzahl von möglichen Aktivierungen des Dienst-Verwaltungs-Schlüssels (K01, K02, K03, K04);

- eine Anzahl oder Höchstzahl von möglichen Aktivierungen des Dienstes (D1, D2, D3, D4);
- eine Unterfunktionalität des Dienstes (D1, D2, D3, D4).

- 5 3. Teilnehmeridentitätsmodul (1) nach Anspruch 1 oder 2, wobei als Dienst einer oder mehrere der folgenden vorgesehen ist bzw. sind:
- ein Sprachverschlüsselungs-Dienst (D1) zur Verschlüsselung von im Mobilfunknetz übertragenen Sprachdaten;
 - ein Datenverschlüsselungs-Dienst (D2) zur Verschlüsselung von im Mobil-
 - 10 funknetz übertragenden Daten, die keine Sprachdaten sind;
 - ein Zugriffs-Dienst (D3) für Daten- oder/und Rechenressourcen eines Computersystems;
 - ein Loyalty-Dienst (D4) zur Verwaltung von Bonuspunkten;
 - ein Ticketing-Dienst zur Verwaltung von elektronischen Tickets für ein
 - 15 Verkehrsmittelsystem (Transitsystem) oder Eintrittskartensystem.

4. Teilnehmeridentitätsmodul (1) nach einem der Ansprüche 1 bis 3, wobei der Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) als privater oder öffentlicher, vorzugsweise privater, Schlüssel eines PKI-Schlüsselpaars gestaltet ist.
- 20

5. Teilnehmeridentitätsmodul (1) nach einem der Ansprüche 1 bis 4, das dazu eingerichtet ist, gemäß dem Secure Channel Protocol SCP gemäß Global Platform Card Specification, insbesondere Version 2.1.1, March 2003, oder
- 25 Nachfolgeversion, zu kommunizieren, insbesondere verschlüsselt zu kommunizieren.

6. Teilnehmeridentitätsmodul (1) nach einem der Ansprüche 1 bis 5, wobei das Verwaltungs-Kommando zum Versenden über das Mobilfunknetz ge-

staltet ist, insbesondere in einer verschlüsselten binären Kurznachrichtendienst-Nachricht (binären SMS).

7. Teilnehmeridentitätsmodul (1) nach einem der Ansprüche 1 bis 6, wobei
5 das Teilnehmeridentitätsmodul (1) und das Verwaltungs-Kommando weiter so eingerichtet sind, dass

- durch den Empfang des Verwaltungs-Kommando beim Teilnehmeridentitätsmodul (1) verursacht wird, dass ein Applet-Status des Applets geprüft wird, wobei der Applet-Status entweder aktiviert oder deaktiviert sein kann,

10 und

- nur falls das Applet den Applet-Status aktiviert hat, zugelassen wird, dass Dienst-Verwaltungs-Schlüssel und damit Dienste aktiviert werden.

8. Verfahren zum Aktivieren eines Dienstes (D1, D2, D3, D4) in einem Teil-
15 nehmeridentitätsmodul (1) nach einem der Ansprüche 1 bis 7, wobei

- von einem Server (3) an das Teilnehmeridentitätsmodul (1) ein Verwaltungs-Kommando für einen oder mehrere der Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) gesendet wird,

- im Teilnehmeridentitätsmodul (1) das Verwaltungs-Kommando ausgewertet wird und der Status des jeweiligen Dienst-Verwaltungs-Schlüssels (K01, K02, K03, K04) entsprechend dem Verwaltungs-Kommando geschaltet wird, so dass der jeweilige Dienst entsprechend dem Verwaltungs-Kommando
20 aktiviert bzw. deaktiviert wird.

25 9. Verfahren zum Aktivieren, oder zum Versetzen in einen aktivierbaren Zustand, eines Dienstes (D1, D2, D3, D4) in einem Teilnehmeridentitätsmodul (1) nach einem der Ansprüche 1 bis 7, wobei

- von einem Server (3) an das Teilnehmeridentitätsmodul (1) ein oder mehrere Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) gesendet wird bzw.

werden,

- der bzw. die Dienst-Verwaltungs-Schlüssel (K01, K02, K03, K04) im Teilnehmeridentitätsmodul (1) implementiert wird/werden,

- so dass der Dienst (D1, D2, D3, D4) aktiviert wird oder in einen aktivierba-

5 ren Zustand versetzt wird.

1/1

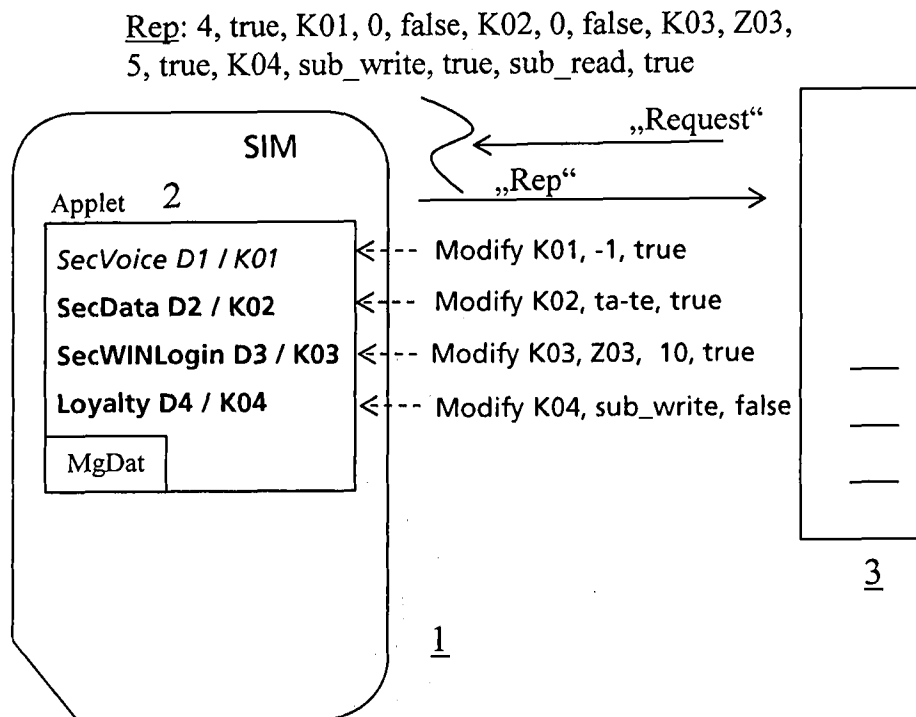


Fig. 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/001441

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/00
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.
A	"Digital cellular telecommunications system (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2 (3GPP TS 03.48 version 8.9.0 Release 1999); ETSI TS 101 181", IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. 3-T3;SMG9, no. V8.9.0, 1 June 2005 (2005-06-01), XP014030428, ISSN: 0000-0001 paragraph 9	1-9
A	EP 2 048 900 A2 (SAGEM ORGA GMBH [DE]) 15 April 2009 (2009-04-15) paragraph [0030] - paragraph [0032] figure 1 ----- -/-	1-9



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

30 September 2015

Date of mailing of the international search report

09/10/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Rabe, Marcus

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/001441

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 605 202 A1 (RESEARCH IN MOTION LTD [CA]) 19 June 2013 (2013-06-19) paragraph [0038] - paragraph [0040] -----	1-9
A	"Global Platform Card Specification 2.1.1", INTERNET CITATION, March 2003 (2003-03), XP002461434, Retrieved from the Internet: URL:www.globalplatform.org [retrieved on 2007-12-06] cited in the application paragraph 6 paragraph 9 -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2015/001441

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2048900	A2	15-04-2009	AT 536058 T 15-12-2011
		EP 2048900 A2	15-04-2009
		EP 2403275 A1	04-01-2012
		WO 2009047309 A2	16-04-2009

EP 2605202	A1	19-06-2013	CA 2788051 A1 15-06-2013
		EP 2605202 A1	19-06-2013
		US 2013160134 A1	20-06-2013

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

INV. H04W4/00

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.
A	"Digital cellular telecommunications system (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2 (3GPP TS 03.48 version 8.9.0 Release 1999); ETSI TS 101 181", IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, Bd. 3-T3;SMG9, Nr. V8.9.0, 1. Juni 2005 (2005-06-01), XP014030428, ISSN: 0000-0001 paragraph 9	1-9
A	EP 2 048 900 A2 (SAGEM ORGA GMBH [DE]) 15. April 2009 (2009-04-15) Absatz [0030] - Absatz [0032] Abbildung 1 ----- -/-	1-9



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

30. September 2015

Absendedatum des internationalen Recherchenberichts

09/10/2015

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Rabe, Marcus

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 2 605 202 A1 (RESEARCH IN MOTION LTD [CA]) 19. Juni 2013 (2013-06-19) Absatz [0038] - Absatz [0040] -----	1-9
A	"Global Platform Card Specification 2.1.1", INTERNET CITATION, März 2003 (2003-03), XP002461434, Gefunden im Internet: URL:www.globalplatform.org [gefunden am 2007-12-06] in der Anmeldung erwähnt paragraph 6 paragraph 9 -----	1-9

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2015/001441

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2048900	A2	15-04-2009	AT 536058 T 15-12-2011
		EP 2048900 A2	15-04-2009
		EP 2403275 A1	04-01-2012
		WO 2009047309 A2	16-04-2009

EP 2605202	A1	19-06-2013	CA 2788051 A1 15-06-2013
		EP 2605202 A1	19-06-2013
		US 2013160134 A1	20-06-2013
