(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
7. August 2014 (07.08.2014)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2014/117939 A1

(51) Internationale Patentklassifikation:
H04W 12/06 (2009.01) *H04W 88/06* (2009.01)
H04L 29/06 (2006.01) *H04W 4/12* (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2014/000246

(22) Internationales Anmeldedatum:
29. Januar 2014 (29.01.2014)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102013001733.5 31. Januar 2013 (31.01.2013) DE

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

(72) Erfinder: **SUMMERER, Alexander**; Mitterfeldring 56, 85586 Poing (DE). **BRANDL, Denny**; Jäger-Schöttl-Str. 12, 85635 Höhenkirchen (DE). **INDERST, Bernhard**; Klenzestr. 60, 80469 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, LT, 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, 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,

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD FOR ACCESSING A SERVICE OF A SERVER USING AN APPLICATION OF A TERMINAL

(54) **Bezeichnung** : VERFAHREN ZUM ZUGRIFF AUF EINEN DIENST EINES SERVERS ÜBER EINE APPLIKATION EINES ENDGERÄTS

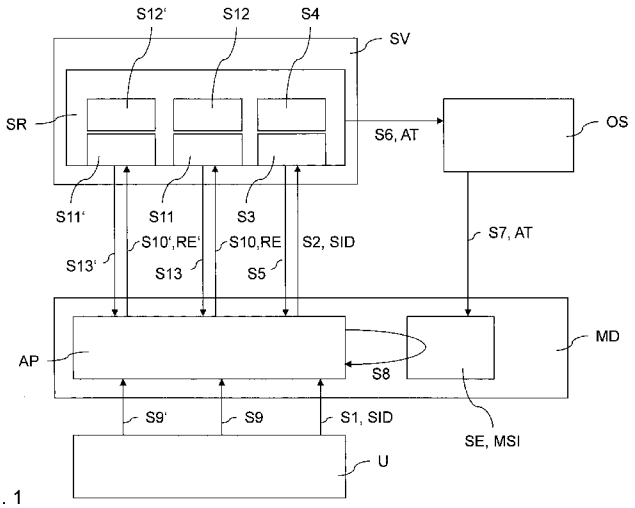

Fig. 1

(57) **Abstract**: The invention relates to a method for accessing a service (SR) of a server (SV) using an application (AP) of a terminal (MD), wherein the terminal (MD) has an associated security element (SE) with which the terminal (MD) can communicate and the security element (SE) contains a subscriber identification (MSI) of a mobile radio subscriber in a mobile radio network. The application (AP) of the terminal (MD) uses a first channel of an IP-based nework to transmit an identification (SID, TN) to the service (SR) of the server (SV) on the basis of IP-based transmission. In the event that the service (SR) is able to successfully verify the identification (SID, TN), an authentication token (AT) is transmitted from the service (SR) to the security element (SE) in encrypted form using a second channel of the mobile radio network on the basis of transmission that differs from the first channel. Next, the application (AP) is automatically provided with the authentication token (AT) transmitted to the security element (SE). Finally, the application (AP) accesses the service (SR) by means of encrypted communication via the first channel, wherein the application (AP) automatically provides requests (RE, RE') that are transmitted from the application (AP) to the service (SR) in the course of the encrypted communication with the provided authentication token (AT), with requests (RE, RE') being processed further by the service (SR) only in the event of successful verification of the authentication token (AT).

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2014/117939 A1

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)*

Die Erfindung betrifft ein Verfahren zum Zugriff auf einen Dienst (SR) eines Servers (SV) über eine Applikation (AP) eines Endgeräts (MD), wobei dem Endgerät (MD) ein Sicherheitselement (SE) zugeordnet ist, mit dem das Endgerät (MD) kommunizieren kann, und das Sicherheitselement (SE) eine Teilnehmeridentifikation (MSI) eines Mobilfunkteilnehmers in einem Mobilfunknetz enthält. Die Applikation (AP) des Endgeräts (MD) übermittelt über einen ersten Kanal eines IP-basierten Netzes basierend auf einer IP-basierten Übertragung eine Identifikation (SID, TN) an den Dienst (SR) des Servers (SV). Im Falle, dass der Dienst (SR) die Identifikation (SID, TN) erfolgreich verifizieren kann, wird ein Authentisierungstoken (AT) von dem Dienst (SR) über einen zweiten Kanal des Mobilfunknetzes basierend auf einer sich vom ersten Kanal unterscheidenden Übertragung verschlüsselt an das Sicherheitselement (SE) übermittelt. Anschließend wird der Applikation (AP) automatisch der an das Sicherheitselement (SE) übermittelte Authentisierungstoken (AT) bereitgestellt. Schließlich greift die Applikation (AP) auf den Dienst (SR) mittels einer verschlüsselten Kommunikation über den ersten Kanal zu, wobei die Applikation (AP) Anfragen (RE, RE'), welche im Rahmen der verschlüsselten Kommunikation von der Applikation (AP) an den Dienst (SR) übermittelt werden, automatisch mit dem bereitgestellten Authentisierungstoken (AT) versieht, wobei Anfragen (RE, RE') durch den Dienst (SR) nur bei erfolgreicher Verifikation des Authentisierungstokens (AT) weiterverarbeitet werden.

Verfahren zum Zugriff auf einen Dienst eines Servers über eine Applikation eines Endgeräts

Die Erfindung betrifft ein Verfahren zum Zugriff auf einen Dienst eines Servers über eine Applikation eines Endgeräts. Ferner betrifft die Erfindung ein entsprechendes System zum Zugriff auf einen Dienst.

Aus dem Stand der Technik sind Authentisierungs-Verfahren für Zugriffe auf Server bekannt, welche auf Authentisierungstoken beruhen. Eine Applikation, welche sich im Besitz eines solchen Authentisierungstokens befindet, kann sich über diesen Token Zugriff zu einem Dienst bzw. einer Ressource verschaffen. Bekannte Token-basierte Authentisierungs-Verfahren sind die Protokolle OAuth 1.0 bzw. OAuth 2.0.

In den Authentisierungs-Protokollen OAuth 1.0 bzw. OAuth 2.0 wird der Austausch der Authentisierungstoken rein über IP-basierte Übertragungstechnologie zwischen Applikation und Dienst ausgetauscht. Um dabei eine ausreichende Sicherheit gegenüber Zugriffen unautorisierter Applikationen zu gewährleisten, wird in der Regel eine Benutzerauthentisierung durchgeführt, welche jedoch Benutzerinteraktionen, z.B. die Eingabe von Benutzernamen und Passwort, erfordern.

Aufgabe der Erfindung ist es, ein Verfahren zum Zugriff auf einen Dienst eines Servers über eine Applikation zu schaffen, welches gegenüber Angriffen unbefugter Dritter gut geschützt ist und dabei wenige bzw. gegebenenfalls keine Benutzerinteraktionen zur Authentisierung erfordert.

Diese Aufgabe wird durch das Verfahren gemäß Patentanspruch 1 bzw. das System gemäß Patentanspruch 12 gelöst. Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen definiert.

Das erfindungsgemäße Verfahren dient zum Zugriff auf einen Dienst eines Servers über eine Applikation eines Endgeräts, wobei dem Endgerät ein Sicherheitselement zugeordnet ist, mit dem das Endgerät kommunizieren kann. Das Sicherheitselement enthält dabei eine Teilnehmeridentifikation eines Mobilfunkteilnehmers in einem Mobilfunknetz. Das Endgerät hat Zugriff auf eine Mobilfunk-Schnittstelle und kann je nach Ausgestaltung ein tragbares Mobilfunkgerät, wie z.B. ein Mobiltelefon, Smart-Phone, Tablet-PC oder ein tragbarer Computer, sein. Ebenfalls kann das Endgerät auch ein stationäres Gerät, wie z.B. ein Desktop-Computer, sein.

Das Sicherheitselement ist vorzugsweise ein Hardwaresicherheitselement. Das Sicherheitselement ist je nach Anwendungsfall eine UICC-Karte bzw. SIM/USIM-Karte (UICC = Universal Integrated Circuit Card, USIM = Universal Subscriber Identity Module). Diese Karten können in das entsprechende Endgerät eingesetzt werden, ebenso könnten andere tragbare Datenträger wie USB-Token, sichere Massenspeicherkarte oder RFID-Transponder als Sicherheitselement dienen. Gegebenenfalls kann das Sicherheitselement auch ein fest in dem Endgerät verbautes Element sein (Sicherheitsmodul), insbesondere in der Form einer sog. embedded UICC-Karte bzw. embedded SIM/USIM-Karte, aber auch als NFC-Modul oder TPM-Modul. Die Zuordnung des Endgeräts zu dem Sicherheitselement kann somit durch Einsetzen des Sicherheitselements in das Endgerät bzw. durch den festen Einbau des Sicherheitselements in dem Endgerät erreicht werden. Ebenso kann eine solche Zuordnung auch über eine andere Kopplung zwischen Endgerät und Sicherheitselement gewährleistet werden, z.B. indem ein Mobilfunk-Stick

oder ein anderes Gerät, welches das Sicherheitselement enthält, drahtgebunden (z.B. über USB) oder drahtlos (z.B. über Bluetooth) mit dem Endgerät verbunden wird.

Das im erfindungsgemäßen Verfahren verwendete Mobilfunknetz kann auf beliebigen Technologien beruhen, z.B. kann es sich um ein GSM-Netz (GSM = Global System for Mobile Communications) oder um ein 3G-Netz bzw. auch um ein LTE-Netz (LTE = Long Term Evolution) handeln.

In dem erfindungsgemäßen Verfahren übermittelt die Applikation des Endgeräts in einem Schritt a) über einen ersten Kanal eines IP-basierten Netzes basierend auf einer IP-basierten Übertragung (IP = Internet Protocol) eine Identifikation an den Dienst des Servers. In einer besonders bevorzugten Variante wird die Identifikation dabei verschlüsselt über den ersten Kanal übertragen, z.B. unter Verwendung des TLS-Protokolls (TLS = Transport Layer Security). In einem Schritt b) des erfindungsgemäßen Verfahrens wird im Falle, dass der Dienst die Identifikation erfolgreich verifizieren kann, ein Authentisierungstoken von dem Dienst über einen zweiten Kanal des Mobilfunknetzes basierend auf einer sich vom ersten Kanal unterscheidenden Übertragung (d.h. mittels einer anderen Art der Übertragung) verschlüsselt an das Sicherheitselement übermittelt. Der zweite Kanal beruht somit auf einer Übertragungstechnologie, welche nicht auf dem Internet-Protokoll beruht. Die Verifikation der entsprechenden Identifikation kann je nach Ausgestaltung unterschiedlich erfolgen, wobei bei nicht erfolgreicher Identifikation das Verfahren abgebrochen wird. In einer bevorzugten Variante sind eine oder mehrere vorbestimmte Identifikationen in dem Server hinterlegt, wobei im Falle, dass die über den ersten Kanal empfangene Identifikation mit einer der vorbestimmten Identifikationen übereinstimmt, die Identifikation erfolgreich verifiziert wird. Der Begriff des Authentisierungstokens ist hier und im

Folgenden weit zu verstehen und kann beliebige Arten von Authentisierungsdaten basierend auf beliebigen Datenformaten umfassen.

In einem Schritt c) wird der Applikation automatisch (d.h. ohne eine Benutzerinteraktion) der an das Sicherheitselement übermittelte Authentisierungstoken bereitgestellt. Schließlich greift die Applikation in einem Schritt d) mittels einer verschlüsselten Kommunikation über den ersten (IP-basierten) Kanal auf den Dienst zu, wobei die Applikation Anfragen, welche im Rahmen der verschlüsselten Kommunikation von der Applikation an den Dienst übermittelt werden, automatisch (d.h. ohne Benutzerinteraktion) mit dem bereitgestellten Authentisierungstoken versieht. Dabei werden Anfragen durch den Dienst nur bei erfolgreicher Verifikation des Authentisierungstokens weiterverarbeitet. Die Verifikation des Authentisierungstokens erfolgt insbesondere derart, dass der Authentisierungstoken mit dem in Schritt b) übermittelten und noch im Server gespeicherten Authentisierungstoken verglichen wird, wobei nur bei Übereinstimmung der Token die Verifikation erfolgreich ist. Die in Schritt d) verwendete verschlüsselte Kommunikation beruht vorzugsweise auf dem bereits oben erwähnten TLS-Protokoll. Im Rahmen der verschlüsselten Kommunikation wird ferner insbesondere das HTTP-Protokoll verwendet (HTTP = Hypertext Tranfer Protocol).

Das erfindungsgemäße Verfahren weist den Vorteil auf, dass durch die Verwendung von zwei Kanälen zur Datenübertragung, nämlich einem ersten Kanal zum verschlüsselten Zugriff auf den Dienst und einem zweiten Kanal zur Übermittlung eines Authentisierungstokens, die Sicherheit gegenüber Angriffen Dritter erhöht wird. Dabei wird ferner die Anzahl der erforderlichen Benutzereingaben im Rahmen einer Authentisierung reduziert. Insbesondere wird der Authentisierungstoken automatisch von der Applikation

verarbeitet, ohne dass Authentisierungsdaten manuell eingegeben werden müssen.

In einer Ausführungsform des erfindungsgemäßen Verfahrens wird die in Schritt a) übermittelte Identifikation vorab einem Benutzer des Endgeräts mitgeteilt, wobei diese Mitteilung insbesondere über den Dienst erfolgt, auf den zugegriffen werden soll. Dabei gibt der Benutzer in Schritt a) die Identifikation an dem Endgerät über eine Benutzerschnittstelle ein, woraufhin die Applikation die eingegebene Identifikation über den ersten Kanal an den Dienst übermittelt. Die Mitteilung der Identifikation an den Benutzer kann dabei z.B. durch das Aussenden einer E-Mail bzw. einer Text-SMS erfolgen.

In einer besonders bevorzugten Ausführungsform liest die Applikation in Schritt a) eine im Sicherheitselement hinterlegte Rufnummer aus, über welche der Mobilfunkteilnehmer kontaktiert werden kann, wobei die in Schritt a) übermittelte Identifikation die ausgelesene Rufnummer ist. In diesem Fall muss die entsprechende Identifikation nicht mehr manuell durch einen Benutzer eingegeben werden.

In einer besonders bevorzugten Variante des erfindungsgemäßen Verfahrens wird der Authentisierungstoken in Schritt b) über eine SMS (SMS = Short Message Service) verschlüsselt an das Sicherheitselement übermittelt. Zur verschlüsselten Übermittlung der SMS können an sich bekannte Technologien, wie z.B. der Standard GSM 03.48, eingesetzt werden. Vorzugsweise erfolgt die Übermittlung des Authentisierungstokens an das Sicherheitselement in Schritt b) unter Zwischenschaltung eines sog. OTA-Servers (OTA = Over The Air), mit dem in an sich bekannter Weise Informationen über ein Mobilfunknetz an entsprechende Sicherheitselemente und insbesondere eine

SIM/USIM-Karte bzw. eine embedded SIM/USIM-Karte übertragen werden können.

In einer weiteren Variante des erfindungsgemäßen Verfahrens erfolgt die automatische Bereitstellung des Authentisierungstokens in Schritt c) über ein Polling der Applikation nach dem Authentisierungstoken auf dem Sicherheitselement. Unter dem an sich bekannten Begriff des Pollings wird eine zyklische Abfrage verstanden, über welche die Applikation die Information erhält, dass ein entsprechender Authentisierungstoken auf dem Sicherheitselement verfügbar ist.

In einer weiteren Variante werden der Empfang des Authentisierungstokens im Sicherheitselement und das Bereitstellen dieses Authentisierungstokens für die Applikation mit Hilfe eines Programms und insbesondere eines Java-Applets auf dem Sicherheitselement durchgeführt. In einer weiteren bevorzugten Ausführungsform kommuniziert das Sicherheitselement bzw. das Programm über eine sog. Secure-Element-API (API = Application Programming Interface) mit der Applikation. Solche APIs sind an sich aus dem Stand der Technik bekannt (z.B. Open Mobile API oder JSR177). Diese APIs ermöglichen Zugriffsschutz-Mechanismen, so dass nur eine autorisierte Applikation den Authentisierungstoken aus dem Sicherheitselement auslesen kann.

In einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens kann die Übermittlung von Anfragen in Schritt d) zumindest teilweise durch einen Benutzer über eine Benutzerschnittstelle des Endgeräts ausgelöst werden. Hierdurch kann die Ausführung der Applikation in geeigneter Weise über einen Benutzer gesteuert werden.

Der Authentisierungstoken ist vorzugsweise nur für eine definierte Zeit zur Verwendung mit einem Dienst gültig. Der Authentisierungstoken wird von dem Dienst also zur Verifikation akzeptiert, wenn er innerhalb der definierten Zeitdauer verwendet wird. Nach Ablauf der Zeitdauer wird der Authentisierungstoken von dem Dienst jedoch nicht mehr akzeptiert. Der Server kann einen übermittelten (und zur Verifikation gespeicherten) Authentisierungstoken nach Ablauf der definierten Zeit beispielsweise löschen oder als abgelaufen markieren.

In einer bevorzugten Ausgestaltung kann der übertragene (erste) Authentisierungstoken auch als zweite Identifikation (Session-ID) für eine zweite Kommunikation mit dem Dienst oder einem anderen Dienst dienen, für welche dann - analog zum bereits beschriebenen Vorgehen - ein zweiter Authentisierungstoken übertragen wird.

Das erfindungsgemäße Verfahren kann zum Zugriff auf beliebige Arten von Diensten verwendet werden. Insbesondere können im Rahmen des Zugriffs auf den Dienst in Schritt d) eine oder mehrere kryptographische Schlüssel oder ein oder mehrere Zertifikate durch den Dienst auf dem Endgerät hinterlegt bzw. erneuert werden.

Zudem ist eine Session-ID unabhängig von der Art des ersten Kommunikationskanals. Die Session-ID kann somit für unterschiedliche erste Kommunikationskanäle zwischen der Applikation und dem einen Dienst verwendet werden.

Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein System zum Zugriff auf einen Dienst eines Servers über eine Applikation eines Endgeräts, wobei dem Endgerät ein Sicherheitselement zugeordnet ist,

mit dem das Endgerät kommunizieren kann, und das Sicherheitselement eine Teilnehmeridentifikation eines Mobilfunkteilnehmers in einem Mobilfunknetz enthält. Die Applikation, das Sicherheitselement und der Dienst sind dabei derart ausgestaltet, dass das erfindungsgemäße Verfahren bzw. ein oder mehrere bevorzugte Varianten des erfindungsgemäßen Verfahrens durchführbar sind.

Die Erfindung betrifft darüber hinaus einen Server mit einem darauf hinterlegten Dienst, wobei der Dienst zur Verwendung in dem erfindungsgemäßen Verfahren bzw. einer oder mehrerer bevorzugten Varianten des erfindungsgemäßen Verfahrens eingerichtet ist. Das heißt, der Dienst ist zur Durchführung der durch ihn durchgeführten Schritte gemäß Anspruch 1 bzw. entsprechender abhängiger Ansprüche eingerichtet. Mit anderen Worten ist der Dienst derart ausgestaltet, dass er einem Dienst des oben beschriebenen erfindungsgemäßen Systems entspricht.

Die Erfindung umfasst ferner ein Endgerät mit darauf hinterlegter Applikation und zugeordnetem Sicherheitselement, wobei die Applikation und das Sicherheitselement zur Verwendung in dem erfindungsgemäßen Verfahren bzw. einer oder mehrerer bevorzugter Varianten des erfindungsgemäßen Verfahrens eingerichtet sind. Das heißt, die Applikation und das Sicherheitselement sind zur Durchführung der von ihnen ausgeführten Schritte gemäß Anspruch 1 bzw. entsprechender abhängiger Ansprüche eingerichtet. Mit anderen Worten entsprechen die Applikation und das Sicherheitselement der Applikation und dem Sicherheitselement in dem oben beschriebenen erfindungsgemäßen System.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der beigefügten Figuren detailliert beschrieben.

Es zeigen:

Fig. 1 eine schematische Darstellung einer ersten Ausführungsform des erfindungsgemäßen Verfahrens, und

Fig. 2 eine schematische Darstellung einer zweiten Ausführungsform des erfindungsgemäßen Verfahrens.

In der Ausführungsform der Fig. 1 ist ein Verfahren zum Zugriff einer Applikation AP, bei der es sich um eine beliebige Consumer-Applikation handelt, auf einen Dienst SR eines Servers SV gezeigt. Die Applikation AP ist dabei auf einem Mobilfunkgerät MD eines Benutzers U hinterlegt. Dieses Mobilfunkgerät ermöglicht eine Kommunikation in einem Mobilfunknetz. Hierfür ist im Mobilfunkgerät ein Sicherheitselement SE in der Form einer SIM/USIM-Karte mit entsprechender IMSI-Teilnehmeridentifikation MSI eines Mobilfunkteilnehmers (IMSI = International Mobile Subscribe Identity) und zugeordneter Rufnummer vorgesehen.

Die Applikation AP kann über eine geeignete Schnittstelle mittels einer IP-basierten Datenübertragung auf den Dienst SR zugreifen. Bei diesem Dienst handelt es sich um eine sog. Service-Provider-Applikation, über welche die Applikation AP auf dem Mobilfunkgerät MD Daten beziehen kann oder Aktionen ausführen kann. Der Dienst SR wird somit durch einen Service-Provider angeboten, wobei dieser Anbieter nicht zwangsläufig mit dem Betreiber des Servers SV übereinstimmen muss. Die Applikation AP kann beispielsweise auf einen Dienst zur Bereitstellung von Schlüsseln zugreifen, wobei die Schlüssel im Server SV hinterlegt sind. Ebenso kann mit einem entsprechenden Dienst des Servers SV ein Zertifikat für die Applikation AP

ausgestellt werden. Wurde z.B. ein neuer Schlüssel durch die Applikation AP generiert, kann diese durch den Zugriff auf den Dienst ein Zertifikat für den neuen Schlüssel anfordern. Ein weiteres Beispiel eines Diensts ist die Erneuerung eines bestehenden Zertifikats für eine Applikation.

Der in Fig. 1 schematisch angedeutete Benutzer U ist eine menschliche Person, die die Applikation AP auf dem Mobilfunkgerät MD bedient, um hierdurch auf den Dienst SR des Servers SV zuzugreifen. In der Regel ist diese Person auch gleichzeitig der Besitzer des Mobilfunkgeräts. Das Mobilfunkgerät kann ein Mobiltelefon oder ein Smartphone sein. Das Mobilfunkgerät kann gegebenenfalls auch ein Tablet-Computer, tragbarer Computer bzw. Laptop mit darin eingesetztem bzw. integriertem Sicherheitselement sein. Ebenso kann das Mobilfunkgerät ein stationärer Desktop-Computer bzw. PC sein.

Das Sicherheitselement SE kann je nach Ausführungsform unterschiedlich realisiert sein. Insbesondere kann es sich um eine austauschbare SIM/USIM-Karte handeln, die reversibel in das Mobilfunkgerät eingesetzt ist (tragbarer Datenträger). Ebenso kann das Sicherheitselement eine sog. embedded SIM/USIM-Karte sein, welche fest in dem Mobilfunkgerät integriert ist (Sicherheitsmodul). Zur Zuordnung eines Sicherheitselements zu einem entsprechenden Mobilfunkgerät ist es gegebenenfalls auch nicht erforderlich, dass sich das Sicherheitselement in dem Mobilfunkgerät befindet. Insbesondere kann das Sicherheitselement auch in einem Mobilfunk-Stick zum Aufbau einer Mobilfunkverbindung eingesetzt sein, wobei der Stick wiederum mit einem Endgerät (z.B. über USB) verbunden ist. Das Endgerät zusammen mit dem Stick stellt dann das Mobilfunkgerät dar. Ebenso kann das Sicherheitselement einem Endgerät über ein weiteres Mobilfunkgerät zugeordnet sein, welches über eine entsprechende Schnittstelle und insbesondere draht-

los (z.B. über Bluetooth) mit dem Endgerät kommuniziert. Das Mobilfunkgerät MD der Fig. 1 entspricht in diesem Fall der Kombination aus Endgerät und weiterem Mobilfunkgerät.

Die Applikation AP kann im Rahmen des erfindungsgemäßen Verfahrens auf das Sicherheitselement SE zugreifen. Hierbei können an sich bekannte Technologien verwendet werden, z.B. kann der Zugriff über eine sog. Secure-Element-API (API = Application Programming Interface) erfolgen. Beispiele für solche Secure-Element-APIs sind Open Mobile API unter dem Betriebssystem Android oder JSR177 für Blackberry-Phones. Eine Secure-Element-API ermöglicht einen Transfer von sog. APDUs gemäß dem Standard ISO 7816-4 (APDU = Application Protocol Data Unit). APDUs werden typischerweise für den Datentransfer zwischen einem Sicherheitselement und einem Terminal bzw. mobilen Gerät verwendet. Die Kommunikation zwischen Applikation und Sicherheitselement sowie der weiter unten beschriebene Empfang eines Authentisierungstokens wird auf dem Sicherheitselement vorzugsweise über ein spezielles Java-Applet geregelt.

Im Rahmen des Verfahrens der Fig. 1 gibt der Benutzer U in einem Schritt S1 zunächst eine Identifikation in der Form einer sog. Session-ID SID ein, wobei dem Benutzer diese Identifikation vorab über einen geeigneten Übertragungsweg (z.B. per Text-SMS oder E-Mail) mitgeteilt wurde. Die entsprechende Mitteilung mit der darin enthaltenen Indentifikation wird in der hier beschriebenen Ausführungsform von dem Server SV an das Mobilfunkgerät MD übermittelt und kann dort dem Benutzer U angezeigt werden. Nach Eingabe der Identifikation SID wird diese von der Applikation AP in einem Schritt S2 an den Dienst SR übermittelt. Hierfür wird einer IP-basierte Datenübertragung über einen entsprechenden ersten Kanal, z.B. über eine LAN- bzw. WLAN-Schnittstelle des Mobilfunkgeräts, genutzt. Ebenso kann die

Datenübertragung unter Zwischenschaltung der entsprechenden Mobilfunkschnittstelle des Mobilfunkgeräts erfolgen. Die Übertragung der Identifikation SID erfolgt zur Vermeidung von Manipulationen verschlüsselt, z.B. über das TLS-Protokoll. Über den IP-basierten ersten Kanal wird somit eine Verbindung der Applikation AP zu dem Server SV über das Internet hergestellt. Dieser Kanal wird auch bei der weiteren direkten Kommunikation zwischen Applikation AP und Dienst SR verwendet.

Die in Schritt S2 von dem Dienst SR empfangene Identifikation SID wird in Schritt S3 von dem Dienst SR dahingehend überprüft, ob sie dem Dienst bekannt ist. Hierzu kann gegebenenfalls eine Datenbank mit entsprechenden zulässigen Identifikationen in dem Server SV hinterlegt sein. Ist die Identifikation SID im Server bekannt, wird in einem nächsten Schritt S4 ein sog. Authentisierungstoken AT generiert, der entsprechende Authentisierungsdaten enthält und in einem späteren Stadium des Verfahrens zur Autorisierung der Applikation AP gegenüber dem Dienst SR genutzt wird. Im Rahmen eines Schritts S5 wird ferner eine Statusmeldung an die Applikation AP gegeben, mit der dieser mitgeteilt wird, ob die Identifikation SID erfolgreich identifiziert werden konnte oder nicht. Im letzteren Fall wird das Verfahren gestoppt, da die Applikation AP keine Berechtigung zum Zugriff auf den Dienst SR hat.

Nach der Generierung des Authentisierungstokens AT in Schritt S4 wird dieser Token in Schritt S6 an einen OTA-Server OS übermittelt. Solche Server sind aus dem Stand der Technik bekannt und ermöglichen eine Übertragung von Informationen Over-The-Air über ein Mobilfunknetz. Demzufolge überträgt der OTA-Server OS in einem Schritt S7 basierend auf einer Mobilfunkübertragung den Token AT an das Sicherheitselement SE des Mobilfunkgeräts MD. Der hierfür verwendete zweite Kanal ist dabei nicht IP-basiert und

verwendet somit eine andere Übertragungstechnologie als der erste Kanal. In der hier beschriebenen Ausführungsform erfolgt die Übertragung mittels einer Textnachricht basierend auf einer verschlüsselten SMS, wobei vorzugsweise der Standard GSM 03.48 verwendet wird. Dabei ist die zur Übermittlung der SMS verwendete Telefonnummer im Dienst SR bekannt und mit der Session-Identifikation SID verknüpft.

Nach dem Versenden der Identifikation SID in Schritt S2 führt die Applikation AP ein sog. Polling (d.h. eine zyklische Abfrage) über eine Secure-Element-API durch, wobei im Rahmen des Pollings nach einem an das Sicherheitselement SE übermittelten Authentisierungstoken AT gesucht wird. Sobald der Authentisierungstoken AT von dem Sicherheitselement SE empfangen wurde, wird dieser in Schritt S8 von der Applikation AP bezogen. Dieser Authentisierungstoken wird dann zur Authentisierung der Applikation AP im Rahmen der nachfolgenden Kommunikation mit dem Dienst SR über den ersten IP-basierten Kanal genutzt. In der hier beschriebenen Ausführungsform erfolgt die darauffolgende Kommunikation mit Hilfe von sog. HTTP-Anfragen, welche die Applikation AP an den Dienst SR richtet, um hierdurch entsprechende Aktionen auszulösen. Eine HTTP-Anfrage, welche auf dem an sich bekannten Hypertext-Transfer-Protokoll beruht, ist dabei ein konkreter HTTP-Übertragungsbefehl. Insbesondere können mit dem Befehl „HTTP GET" Daten von einem HTTP-Server angefordert werden. Demgegenüber können mit dem Befehl HTTP POST Daten von einem HTTP-Server an eine Applikation übermittelt werden. Der Server SV hat somit unter anderem auch die Funktionalität eines HTTP-Servers.

In Schritt S9 wird über eine Benutzereingabe an einer Benutzerschnittstelle des Mobilfunkgeräts MD (oder automatisiert, insbesondere nach Benutzervorgabe) eine entsprechende Aktion zur Durchführung durch den Dienst SV

ausgelöst. Basierend auf der Benutzereingabe wird dann in Schritt S10 eine HTTP-Anfrage RE über den ersten Kanal an den Dienst SR gerichtet. Dabei wird automatisiert durch die Applikation AP der Authentisierungstoken AT in die HTTP-Anfrage als Attribut eingefügt. In Schritt S11 wird dann von dem Dienst SR überprüft, ob der empfangene Token dem in Schritt S4 ausgesendeten Token entspricht. Ist dies der Fall, ist die Applikation AP erfolgreich authentisiert bzw. autorisiert, so dass die entsprechende Aktion, die über den HTTP-Befehl RE angefordert wurde, in Schritt S12 ausgeführt wird. Sollte in Schritt S12 keine Übereinstimmung der Tokens festgestellt werden, wird das Verfahren abgebrochen. In beiden Fällen wird in Schritt S13 eine Antwort an die Applikation AP von dem Dienst SR zurückgegeben. Bei erfolgreicher Authentisierung in Schritt S11 wird als Antwort das Ergebnis der angeforderten Aktion, z.B. ein angeforderter Schlüssel bzw. ein angefordertes Zertifikat, an die Applikation AP gegeben. Bei nicht erfolgreicher Authentisierung wird demgegenüber eine Abbruchmeldung an die Applikation AP übermittelt.

In der Ausführungsform der Fig. 1 ist beispielhaft die Ausführung einer weiteren Aktion über entsprechende Schritte S9', S10', ..., S13' dargestellt. Diese Schritte entsprechen den Schritten S9 bis S13, die oben beschrieben wurden. Das heißt, es wird wiederum über den Schritt S9' durch den Benutzer (oder automatisiert) eine Aktion ausgelöst, welche zum Aussenden einer HTTP-Anfrage RE' führt, die den Authentisierungstoken AT als Attribut enthält. Es wird dann eine Überprüfung des Tokens in Schritt S11' durchgeführt sowie bei erfolgreicher Authentisierung die Aktion S12' ausgeführt, welche in Schritt S13' zum Zurücksenden einer Antwort führt. Je nach Ausgestaltung der Applikation können auch weitere Aktionen zum Zugriff auf den Dienst ausgelöst werden.

In dem soeben beschriebenen Zugriff auf den Dienst SR wird basierend auf der IP-basierten Kommunikation über den ersten Kanal immer verschlüsselt kommuniziert. Zur Verschlüsselung wird in einer besonders bevorzugten Ausführungsform das an sich bekannte TLS-Protokoll eingesetzt. Mit diesem Protokoll wird der Server authentisiert und werden die entsprechenden Anfragen RE bzw. RE' und die darauf basierenden Antworten verschlüsselt. Hierdurch wird sichergestellt, dass der Authentisierungstoken nicht von Dritten durch Abhören des ersten Kanals ausgelesen werden kann.

Fig. 2 zeigt eine schematische Darstellung einer Abwandlung der Ausführungsform der Fig. 1. Das Verfahren der Fig. 2 entspricht größtenteils dem Verfahren der Fig. 1. Es werden somit nur noch die Unterschiede zwischen den beiden Verfahren beschrieben. Im Unterschied zu Fig. 1 wird im Verfahren der Fig. 2 als Identifikation in Schritt S2 keine Session-ID SID übertragen, sondern stattdessen die Rufnummer bzw. Telefonnummer TN des Mobilfunkteilnehmers, die in dem Sicherheitselement SE hinterlegt ist. Der Start der Applikation AP durch den Benutzer U in Schritt S1 erfolgt dabei ohne die Eingabe einer Session-ID. Anschließend wird dann automatisiert durch die Applikation AP die Telefonnummer TN aus dem Sicherheitselement SE ausgelesen und verschlüsselt (insbesondere mit dem TLS-Protokoll) über den ersten IP-basierten Kanal an den Dienst SR des Servers SV übertragen. Der Dienst SR verifiziert anschließend die Telefonnummer, z.B. indem er die Telefonnummer mit zulässigen Telefonnummern aus einer Benutzerdatenbank vergleicht. Bei erfolgreicher Verifikation läuft das Verfahren analog wie in Fig. 1 beschrieben ab, d.h. ein Authentisierungstoken AT wird über einen zweiten Kanal mittels SMS verschlüsselt an das Sicherheitselement SE übermittelt und anschließend zur Autorisierung entsprechender Anfragen im Rahmen des Zugriffs auf den Dienst genutzt. Zwecks Vermeidung von Wiederholungen werden die entsprechenden Verfahrensschritte nicht nochmals

im Detail beschrieben. Diesbezüglich wird vielmehr auf die obigen Ausführungen zu Fig. 1 verwiesen.

Die im Vorangegangenen beschriebenen Ausführungsformen der Erfindung weisen eine Reihe von Vorteilen auf. Insbesondere werden im Rahmen des Zugriffs auf einen Dienst durch eine Applikation zwei verschiedene Übertragungstechnologien über einen ersten Kanal eines IP-basierten Netzes sowie einen zweiten, davon unterschiedlichen Kanal eines Mobilfunknetzes genutzt. Für die direkte Kommunikation der Applikation mit dem Dienst wird dabei der erste Kanal und zur Übermittlung des Authentisierungstokens der zweite Kanal verwendet. Demzufolge werden Angriffe unbefugter Dritter erschwert, denn ein Angreifer benötigt Zugriff zu beiden Netzwerken, um entsprechende Protokoll-Daten aufzuzeichnen und zu analysieren, um sich hierdurch Zugriff auf den Dienst zu verschaffen.

Mit dem erfindungsgemäßen Verfahren wird ferner sichergestellt, dass der Authentisierungstoken stets verschlüsselt übertragen wird. Zudem wird sichergestellt, dass der Authentisierungstoken nur zu authentisierten Kommunikationspartnern übertragen wird. Hierfür kann in speziellen Ausführungsformen eine verschlüsselte SMS und das TSL-Protokoll genutzt werden. Darüber hinaus kann durch typische Zugriffsschutz-Mechanismen einer Secure-Element-API (z.B. GP SE Access Control) bei der Kommunikation zwischen Applikation und Sicherheitselement sichergestellt werden, dass nur autorisierte Applikationen den Authentisierungstoken aus dem Sicherheitselement auslesen können.

Ein weiterer Vorteil des erfindungsgemäßen Verfahrens besteht darin, dass die Authentisierung der Applikation automatisch abläuft, was durch das automatische Bereitstellen des Authentisierungstokens sowie die automati-

sche Einbindung des Authentisierungstokens in entsprechende Anfragen an den Dienst realisiert wird. Demzufolge ist es im Rahmen der Authentisierung nicht mehr erforderlich, dass manuell durch einen Benutzer Eingaben vorgenommen werden müssen, wie dies oftmals bei herkömmlichen Authentisierungs-Protokollen der Fall ist.

Patentansprüche

1. Verfahren zum Zugriff auf einen Dienst (SR) eines Servers (SV) über eine Applikation (AP) eines Endgeräts (MD), wobei dem Endgerät (MD) ein Sicherheitselement (SE) zugeordnet ist, mit dem das Endgerät (MD) kommunizieren kann, und das Sicherheitselement (SE) eine Teilnehmeridentifikation (MSI) eines Mobilfunkteilnehmers in einem Mobilfunknetz enthält, wobei

   a) die Applikation (AP) des Endgeräts (MD) über einen ersten Kanal eines IP-basierten Netzes basierend auf einer IP-basierten Übertragung eine Identifikation (SID, TN) an den Dienst (SR) des Servers (SV) übermittelt;

   b) im Falle, dass der Dienst (SR) die Identifikation (SID, TN) erfolgreich verifizieren kann, ein Authentisierungstoken (AT) von dem Dienst (SR) über einen zweiten Kanal des Mobilfunknetzes basierend auf einer sich vom ersten Kanal unterscheidenden Übertragung verschlüsselt an das Sicherheitselement (SE) übermittelt wird;

   c) der Applikation (AP) automatisch der an das Sicherheitselement (SE) übermittelte Authentisierungstoken (AT) bereitgestellt wird;

   d) die Applikation (AP) auf den Dienst (SR) mittels einer verschlüsselten Kommunikation über den ersten Kanal zugreift, wobei die Applikation (AP) Anfragen (RE, RE'), welche im Rahmen der verschlüsselten Kommunikation von der Applikation (AP) an den Dienst (SR) übermittelt werden, automatisch mit dem bereitgestellten Authentisierungstoken (AT) versieht, wobei Anfragen (RE, RE') durch den Dienst (SR) nur bei erfolgreicher Verifikation des Authentisierungstokens (AT) weiterverarbeitet werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die in Schritt a) übermittelte Identifikation (SID) vorab einem Benutzer (U) des Endgeräts (MD) durch den Dienst (SR) mitgeteilt wird, wobei in Schritt a) nach einer Eingabe der mitgeteilten Identifikation (SID) durch den Benutzer mittels einer Benutzerschnittstelle des Endgeräts (MD) die Applikation (AP) die Identifikation (SID) über den ersten Kanal an den Dienst (SR) übermittelt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Applikation (AP) in Schritt a) eine im Sicherheitselement (SE) hinterlegte Rufnummer (TN) ausliest, über welche der Mobilfunkteilnehmer im Mobilfunknetz kontaktiert werden kann, wobei die in Schritt a) übermittelte Identifikation die ausgelesene Rufnummer (TN) ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Authentisierungstoken (AT) in Schritt b) über eine SMS an das Sicherheitselement (SE) übermittelt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Authentisierungstoken (AT) in Schritt b) unter Zwischenschaltung eines OTA-Servers (OS) an das Sicherheitselement (SE) übermittelt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die automatische Bereitstellung des Authentisierungstokens (AT) in Schritt c) über ein Polling der Applikation (AP) nach dem Authentisierungstoken (AT) auf dem Sicherheitselement (SE) erfolgt.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Empfang des Authentisierungstokens (AT) im Sicherheitselement (SE) und das Bereitstellen des Authentisierungstokens (AT) für die Applikation (AP) mit Hilfe eines Programms und insbesondere eines Java-Applets auf dem Sicherheitselement (SE) durchgeführt wird und/oder dass das Sicherheitselement (SE) über eine Secure-Element-API mit der Applikation (AP) kommuniziert.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Verschlüsselung der Kommunikation über den ersten Kanal in Schritt d) basierend auf dem TLS-Protokoll erfolgt.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Übermittlung von Anfragen (RE, RE') in Schritt d) zumindest teilweise durch einen Benutzer (U) über eine Benutzerschnittstelle des Endgeräts (MD) ausgelöst werden kann.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im Rahmen des Zugriffs auf den Dienst in Schritt d) eine oder mehrere kryptographische Schlüssel und/oder eine oder mehrere Zertifikate durch den Dienst (SR) auf dem Endgerät hinterlegt und/oder erneuert werden.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Verfahren mittels eines Sicherheitselements (SE) durchgeführt wird, der als tragbarer Datenträger in dem Endgerät (MD) eingesetzt oder als Sicherheitsmodul in dem Endgerät (MD) fest integriert ist.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Authentisierungstoken (AT) nur für eine definierte Zeit zur Verwendung in dem Schritt d gültig ist.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Identifikation (SID, TN) für unterschiedliche erste Kanäle zwischen der Applikation (AP) und dem Dienst (SR) einsetzbar ist.

14. System zum Zugriff auf einen Dienst (SR) eines Servers (SV) über eine Applikation (AP) eines Endgeräts (MD), wobei dem Endgerät (MD) ein Sicherheitselement (SE) zugeordnet ist, mit dem das Endgerät (MD) kommunizieren kann, und das Sicherheitselement (SE) eine Teilnehmeridentifikation (MSI) eines Mobilfunkteilnehmers in einem Mobilfunknetz enthält, wobei die Applikation (AP), das Sicherheitselement (SE) und der Dienst (SR) derart ausgestaltet sind, dass ein Verfahren durchführbar ist, bei dem

a) die Applikation (AP) des Endgeräts (MD) über einen ersten Kanal eines IP-basierten Netzes basierend auf einer IP-basierten Übertragung eine Identifikation (SID, TN) an den Dienst (SR) des Servers (SV) übermittelt;

b) im Falle, dass der Dienst (SR) die Identifikation (SID, TN) erfolgreich verifizieren kann, ein Authentisierungstoken (AT) von dem Dienst (SR) über einen zweiten Kanal des Mobilfunknetzes basierend auf einer sich vom ersten Kanal unterscheidenden Übertragung verschlüsselt an das Sicherheitselement (SE) übermittelt wird;

c) der Applikation (AP) automatisch der an das Sicherheitselement (SE) übermittelte Authentisierungstoken (AT) bereitgestellt wird;

d) die Applikation (AP) auf den Dienst (SR) mittels einer verschlüsselten Kommunikation über den ersten Kanal zugreift, wobei die Applikation (AP) Anfragen (RE, RE'), welche im Rahmen der verschlüsselten Kommunikation von der Applikation (AP) an den Dienst (SR) übermittelt werden, automatisch mit dem bereitgestellten Authentisierungstoken (AT) versieht, wobei Anfragen (RE, RE') durch den Dienst (SR) nur bei erfolgreicher Verifikation des Authentisierungstokens (AT) weiterverarbeitet werden.

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

16. Server (SV) mit einem darauf hinterlegtem Dienst (SR), dadurch gekennzeichnet, dass der Dienst (SR) zur Verwendung in einem Verfahren nach einem der Ansprüche 1 bis 13 eingerichtet ist.

17. Endgerät mit einer darauf hinterlegten Applikation (AP) und einem zugeordneten Sicherheitselement (SE), dadurch gekennzeichnet, dass die Applikation (AP) und das Sicherheitselement (SE) zur Verwendung in einem Verfahren nach einem der Ansprüche 1 bis 13 eingerichtet sind.

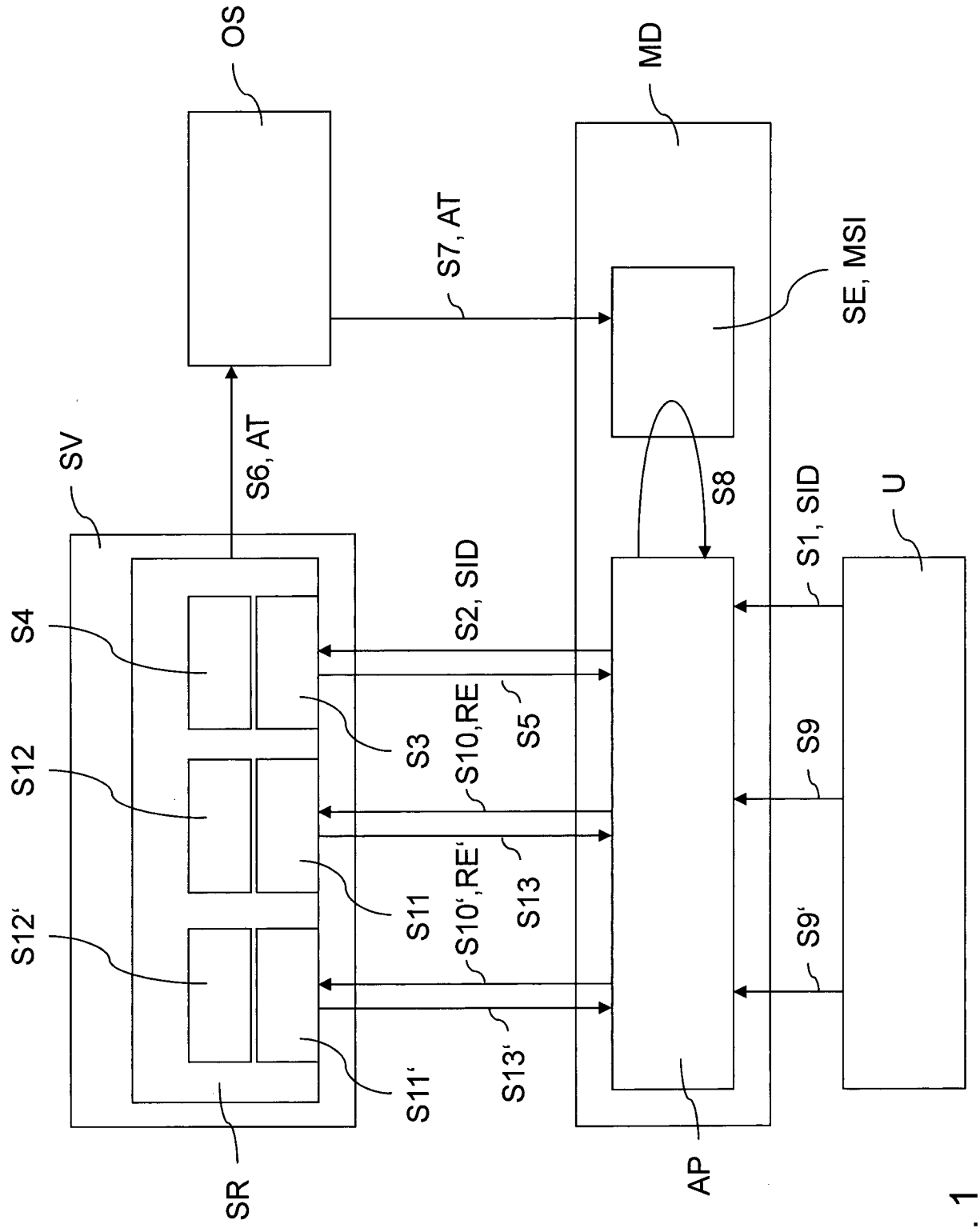
OS
MD
S7, AT
SE, MSI
SV
S6, AT
S8
U
S1, SID
S4
S2, SID
S12
S3
S10,RE
S5
S9
S12'
S11
S10',RE'
S13
S9'
S11'
S13'
SR
AP

Fig. 1

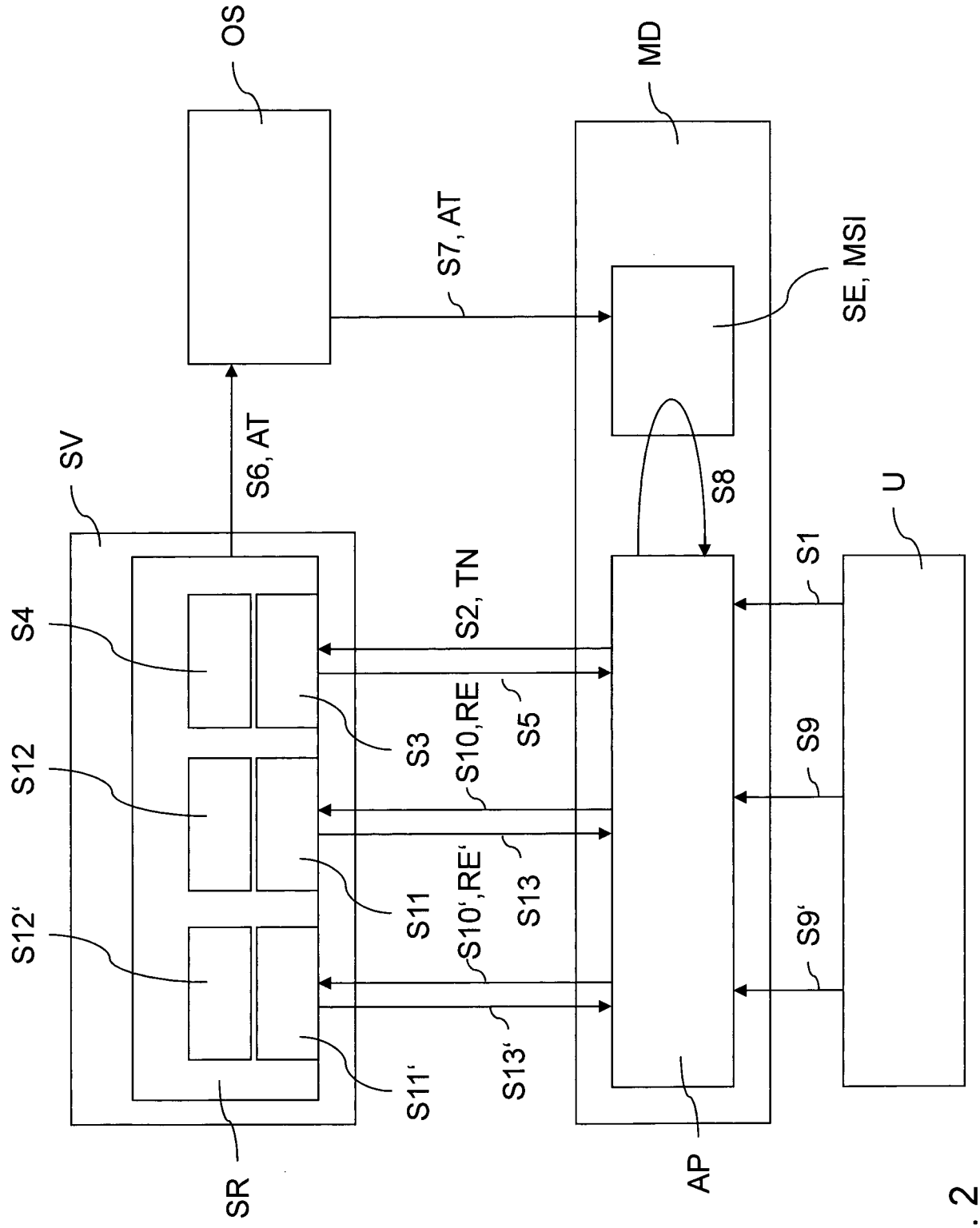
OS
MD
S7, AT
SE, MSI
SV
S6, AT
S8
U
S4
S2, TN
S1
S12
S3
S10,RE
S5
S9
S11
S10',RE'
S13
S12'
S9'
S11'
S13'
SR
AP

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/000246

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06
ADD. H04L29/06 H04W88/06 H04W4/12

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 H04L

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, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 624 360 A1 (MICROSOFT CORP [US]) 8 February 2006 (2006-02-08) paragraphs [0021] - [0022], [0025], [0027] - [0037]; figure 3	1-17
X	EP 1 422 960 A1 (MICROSOFT CORP [US]) 26 May 2004 (2004-05-26) paragraphs [0031] - [0035] figures 2,3	1-17
X,P	EP 2 651 097 A1 (VODAFONE HOLDING GMBH [DE]) 16 October 2013 (2013-10-16) paragraphs [0019], [0020] - [0028], [0031], [0034] - [0038] figure 1	1,3,6-8, 11-14, 16,17

☐ 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
17 April 2014	08/05/2014

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	Ghomrasseni, Z

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/000246

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1624360 A1	08-02-2006	CN 1717111 A	04-01-2006
		EP 1624360 A1	08-02-2006
		JP 2006048653 A	16-02-2006
		KR 20060049718 A	19-05-2006
		US 2006002556 A1	05-01-2006
EP 1422960 A1	26-05-2004	AT 433632 T	15-06-2009
		CN 1503597 A	09-06-2004
		EP 1422960 A1	26-05-2004
		HK 1066676 A1	12-02-2010
		JP 4031751 B2	09-01-2008
		JP 2004173282 A	17-06-2004
		KR 20040044348 A	28-05-2004
		TW I335187 B	21-12-2010
		US 2004203599 A1	14-10-2004
		US 2006030296 A1	09-02-2006
EP 2651097 A1	16-10-2013	DE 102012103106 A1	17-10-2013
		EP 2651097 A1	16-10-2013
		US 2013276080 A1	17-10-2013

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2014/000246

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04W12/06
ADD. H04L29/06 H04W88/06 H04W4/12

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04W H04L

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, COMPENDEX, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 1 624 360 A1 (MICROSOFT CORP [US]) 8. Februar 2006 (2006-02-08) Absätze [0021] - [0022], [0025], [0027] - [0037]; Abbildung 3	1-17
X	EP 1 422 960 A1 (MICROSOFT CORP [US]) 26. Mai 2004 (2004-05-26) Absätze [0031] - [0035] Abbildungen 2,3	1-17
X,P	EP 2 651 097 A1 (VODAFONE HOLDING GMBH [DE]) 16. Oktober 2013 (2013-10-16) Absätze [0019], [0020] - [0028], [0031], [0034] - [0038] Abbildung 1	1,3,6-8, 11-14, 16,17

☐ 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
17. April 2014	08/05/2014

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	Ghomrasseni, Z

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2014/000246

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1624360 A1	08-02-2006	CN 1717111 A	04-01-2006
		EP 1624360 A1	08-02-2006
		JP 2006048653 A	16-02-2006
		KR 20060049718 A	19-05-2006
		US 2006002556 A1	05-01-2006
EP 1422960 A1	26-05-2004	AT 433632 T	15-06-2009
		CN 1503597 A	09-06-2004
		EP 1422960 A1	26-05-2004
		HK 1066676 A1	12-02-2010
		JP 4031751 B2	09-01-2008
		JP 2004173282 A	17-06-2004
		KR 20040044348 A	28-05-2004
		TW I335187 B	21-12-2010
		US 2004203599 A1	14-10-2004
		US 2006030296 A1	09-02-2006
EP 2651097 A1	16-10-2013	DE 102012103106 A1	17-10-2013
		EP 2651097 A1	16-10-2013
		US 2013276080 A1	17-10-2013