(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
20. März 2014 (20.03.2014)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2014/040724 A1

(51) Internationale Patentklassifikation:
G06F 21/74 (2013.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/002720

(22) Internationales Anmeldedatum:
10. September 2013 (10.09.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 017 915.4
11. September 2012 (11.09.2012) DE

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

(72) Erfinder: **DIETZE, Claus**; Frühlingsweg 5, 82395 Obersöchering (DE). **GALKA, Gero**; Sollach 17a, 83626 Valley (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, 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.

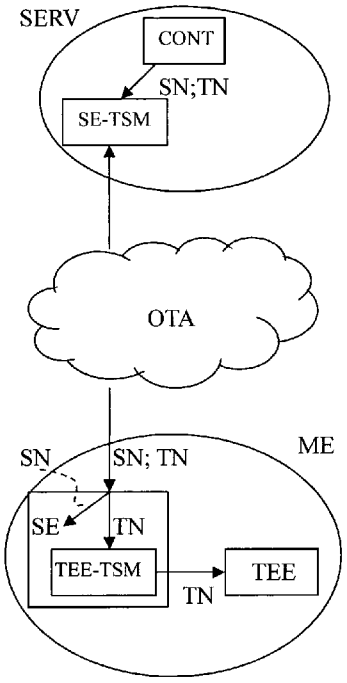
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE,

[Fortsetzung auf der nächsten Seite]

WO 2014/040724 A1

(54) **Title**: CONTENT MANAGEMENT FOR MOBILE STATION WITH RUNTIME ENVIRONMENT

(54) **Bezeichnung** : INHALTEVERWALTUNG FÜR MOBILSTATION MIT LAUFZEITUMGEBUNG



(57) **Abstract**: The invention relates to a mobile station comprising a mobile terminal (ME) with a secure runtime environment (TEE) and comprising a removable or securely implemented security element (SE). The security element (SE) is equipped with a terminal transmission server (TEE-TSM) which is designed to transmit terminal messages to the secure runtime environment (TEE), said messages being receivable by the secure runtime environment (TEE). The terminal messages are transmitted to the security element (SE) by means of a trusted service manager (SE-TSM) which is provided for the security element (SE), whereby greater efficiency with constant security is ensured.

(57) **Zusammenfassung**: Die Erfindung schafft eine Mobilstation umfassend ein mobiles Endgerät (ME)mit einer gesicherten Laufzeitumgebung (TEE) und ein entfernbares oder festimplementiertes Sicherheitselement (SE), mit einem im Sicherheitselement (SE) eingerichteten Endgerät- Sendeserver (TEE-TSM), der dazu eingerichtet ist, an die gesicherte Laufzeitumgebung (TEE) Endgerät-Nachrichten zu senden, die von der gesicherten Laufzeitumgebung (TEE) empfangen werden können. Die Endgeräte-Nachrichten werden durch ein Trusted Service Manager (SE-TSM), der für das Sicherheitselement (SE) vorgesehen ist, an das Sicherheitselement (SE) gesendet, wodurch höhere Effizient bei bleibender Sicherheit gewährleistet wird.

Fig. 3

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)*

INHALTEVERWALTUNG FÜR MOBILSTATION MIT LAUFZEITUMGEBUNG

Die Erfindung betrifft eine Mobilstation, umfassend ein mobiles Endgerät mit einer gesicherten Laufzeitumgebung und ein entfernbares oder festimplementiertes Sicherheitselement, einen Verwaltungsserver und ein Inhalteverwaltungs-System (Content Managment System) für die gesicherte Ausführungsumgebung.

Mobilstationen umfassen im GSM- und UMTS-System und ähnlichen Mobilfunksystemen ein mobiles Endgerät, z.B. Mobiltelefon oder Smartphone, und ein entfernbares oder festimplementiertes Sicherheitselement. Im Sicherheitselement sind Verbindungsdaten, z.B. IMSI (International Mobile Subscriber Identity), Schlüssel und Algorithmen zum Betreiben einer Verbindung im Mobilfunknetz implementiert. Im GSM- bzw. UMTS-System ist als entfernbares Sicherheitselement die SIM-Karte bzw. USIM-Karte bekannt (SIM = Subscriber Identity Module, USIM = Universal SIM). Als festimplementiertes Sicherheitselement ist die eUICC (embedded Universal Integrated Circuit Card) bekannt, die ein fest eingelötetes Bauelement ist. Die Kommunikation mit dem Sicherheitselement ist durch Normen der Organisation ETSI (European Telecommunications Standards Institute) standardisiert.

In mobilen Endgeräten sind gesicherte Laufzeitumgebungen TEEs (TEE = trusted execution environment) bekannt, bei denen auf Software-Ebene eine Trennung zwischen Ausführungsumgebungen unterschiedlicher Sicherheitsniveaus erzeugt wird. Sicherheitskritische Daten und Programme sind unter Verwaltung der gesicherten Laufzeitumgebung gespeichert. Die übrigen Daten und Programme sind in einer daneben existierenden normalen Laufzeitumgebung gespeichert. Die auch „Normal Zone" oder „Normal World" genannte unsichere Laufzeitumgebung ist durch ein Normalbetriebssystem (z.B. Android, Windows Phone, Symbian) gesteuert. Die auch „Trustzone" oder „Trusted World" oder „Secure World" oder „Trusted Exe-

cution Environment TEE" genannte gesicherte oder vertrauenswürdige Laufzeitumgebung ist durch ein Sicherheitsbetriebssystem gesteuert.

Insbesondere sicherheitskritische Applikationen und manche Peripherie-Funktionen (z.B. Tastaturtreiber) werden durch das Sicherheitsbetriebssystem auf sichere Weise gesteuert. Applikationen unter dem Sicherheitsbetriebssystem werden auch als Trusted Applications (z.B. Global Platform) oder teilweise als Trustlets (eingetragene Marke) bezeichnet, in assoziativer Anlehnung an die Begriffe „Trust" (Vertrauen) und „Applet".

So beschreibt z.B. das Dokument „Global Platform Device Technology: TEE System Architecture, Version 0.4, Public Review Draft October 2011, Document Reference: GPD_SPE_009" ein mobiles Endgerät mit einer normalen oder unsicheren Ausführungsumgebung „Rich Execution Environment (REE)" und einer sicheren Ausführungsumgebung „Trusted Execution Environment (TEE)" (vgl. Kapitel 1).

Mobilfunknetzbetreiber haben zur Verwaltung der Inhalte (sogenannte Contents; z.B. Daten, Programme) im Sicherheitselement eine ausgereifte Serverinfrastruktur. Diese ermöglicht es ihnen, Nachrichten nach ETSI-Standard, in denen die Inhalte enthalten sind, auf kryptographisch gesicherte Weise von einem Inhalteserver (Content Server) über das Mobilfunknetz (OTA, over-the-air) in das Sicherheitselement zu laden.

Zur Verwaltung der Inhalte in der gesicherten Laufzeitumgebung eines mobilen Endgeräts ist ebenfalls eine kryptographisch absicherbare Infrastruktur erforderlich. Herkömmlicherweise werden die Inhalte von gesicherten Laufzeitumgebungen, z.B. solchen nach Global Platform, durch einen sogenannten Trusted Service Manager verwaltet.

Durch die höheren Sicherheitsanforderungen der gesicherten Laufzeitumgebung im Vergleich zur normalen Laufzeitumgebung reicht die Infrastruktur zur Verwaltung der Inhalte eines herkömmlichen mobilen Endgeräts nicht aus. Die Serverinfrastruktur zur Inhalte-Verwaltung des Sicherheitselements ist nicht direkt zur Inhalte-Verwaltung der gesicherten Laufzeitumgebung geeignet. Denn die Kommunikation zwischen dem Sicherheitselement und einem Server erfolgt mittels Nachrichten gemäß ETSI Standard. Nachrichten an die gesicherte Laufzeitumgebung müssen anderen Vorgaben, z.B. denen der Global Platform Organisation genügen. Ein Trusted Service Manager ist in der Lage, solche Global Platform konforme Nachrichten auf sichere Weise an die gesicherte Laufzeitumgebung zu übermitteln. Der Betrieb einer zusätzlichen sicheren Serverinfrastruktur für die Verwaltung der Inhalte der gesicherten Laufzeitumgebung bedeutet für den Mobilfunknetzbetreiber einen großen organisatorischen und finanziellen Aufwand.

Der Erfindung liegt die Aufgabe zu Grunde, eine Mobilstation mit einer gesicherten Laufzeitumgebung bereitzustellen, die eine effiziente und zugleich sichere Verwaltung der Inhalte (Daten, Programme) der gesicherten Laufzeitumgebung ermöglicht. Zudem soll ein dazu passender Verwaltungsserver für Mobilstationen angegeben werden.

Aus EP 1 510 012 B1 ist eine Mobilstation mit einem entfernbaren Sicherheitselement in Form einer SIM-Karte bekannt. In der SIM-Karte sind neben den herkömmlichen Verbindungsdaten (IMSI) zum Betreiben einer Verbindung im Mobilfunknetz zusätzlich auch Verbindungsdaten (IP-Adresse) zum Betreiben einer Verbindung in einem IP-Netz gespeichert. In der SIM-Karte ist zudem ein Server implementiert, der eine über das Mobilfunknetz bestehende Verbindung zu einer IP-Verbindung umleitet.

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

Die erfindungsgemäße Mobilstation umfasst ein Endgerät (z.B. Smartphone, Mobiltelefon oder dergleichen) mit einer gesicherten Laufzeitumgebung, sowie ein entfernbares oder festimplementiertes Sicherheitselement (z.B. SIM-Karte, UICC, eUICC etc.). Im Sicherheitselement ist eine Sicherheitselement-Empfangseinrichtung zum Empfangen von an das Sicherheitselement gesandten Sicherheitselement-Nachrichten eingerichtet. Sicherheitselement-Nachrichten sind dazu vorgesehen, Inhalte in das Sicherheitselement einzubringen, beispielsweise Daten, Programme oder Aktualisierungen für im Sicherheitselement bereits vorhandene Daten oder Programme, dabei insbesondere auch Daten und Programme betreffend die Subskription, d.h. das Vertragsverhältnis, um mit der Mobilstation Mobilfunkverbindungen über ein Mobilnetz eines Mobilnetzbetreibers zu betreiben. In der gesicherten Laufzeitumgebung ist eine Endgerät-Empfangseinrichtung zum Empfangen von an die gesicherte Laufzeitumgebung des Endgeräts gesandten Endgerät-Nachrichten eingerichtet. Endgerät-Nachrichten sind dazu vorgesehen, Inhalte wie Daten, Programme und Aktualisierungen zu Daten und Programmen in die gesicherte Laufzeitumgebung zu laden. Als Programme sind beispielsweise Anwendungen wie Zahlungsverkehrsapplikationen vorgesehen.

Die Mobilstation zeichnet sich aus durch einen im Sicherheitselement eingerichteten Endgerät-Sendeserver, der dazu eingerichtet ist, an die gesicherte Laufzeitumgebung Endgerät-Nachrichten zu senden, die von der gesicherten Laufzeitumgebung empfangen werden können.

Auf diese Weise können Inhalte für die gesicherte Laufzeitumgebung an das Sicherheitselement gesendet werden. Der im Sicherheitselement eingerichtete Endgerät-Sendeserver sendet die Inhalte an die gesicherte Laufzeitumgebung weiter. Folglich kann ein Netzbetreiber die Serverinfrastruktur verwenden, die zur Verwaltung des Sicherheitselements eingerichtet ist, um auch die gesicherte Laufzeitumgebung zu verwalten. Insbesondere kann zur Verwaltung der Inhalte der gesicherten Laufzeitumgebung ein Verwaltungsserver verwendet werden, der eigentlich zur Verwaltung der Inhalte des Sicherheitselements vorgesehen ist, und der hierzu nur geringfügig erweitert werden muss. Ein solcher Verwaltungsserver ist in Anspruch 3 angegeben. Die erforderliche Weiterleitung der Kommunikation an die gesicherte Laufzeitumgebung wird nicht durch einen externen Server des Netzbetreibers durchgeführt, sondern durch den im Sicherheitselement implementierten karteninteren (bzw. eUICC-internen etc.) Server. Der Netzbetreiber ist hierdurch entlastet. Da sowohl die Kommunikation zwischen dem externen (zB beim Netzbetreiber betriebenen) Server und dem Sicherheitselement als auch die Kommunikation zwischen dem Sicherheitselement und der gesicherten Laufzeitumgebung sicher sind, ist die erfindungsgemäße Lösung zudem ohne Sicherheitsverluste gegenüber einer Lösung mit einer gesonderten externen Serverinfrastruktur für die gesicherte Laufzeitumgebung.

Somit ist gemäß Anspruch 1 eine Mobilstation mit einer gesicherten Laufzeitumgebung geschaffen, die eine effiziente und zugleich sichere Verwaltung der Inhalte der gesicherten Laufzeitumgebung ermöglicht.

Als Endgerät-Sendeserver ist beispielsweise ein sogenannter Trusted Service Manager vorgesehen. Erfindungsgemäß ist der Trusted Service Manager für die gesicherte Laufzeitumgebung im Sicherheitselement (z.B. SIM-Karte, UICC, eUICC, etc.) implementiert.

Wahlweise sind das Sicherheitselement und die Sicherheitselement-Nachrichten gemäß ETSI spezifiziert und die gesicherte Laufzeitumgebung und die Endgerät-Nachrichten gemäß Global Platform spezifiziert.

Ein erfindungsgemäßer Verwaltungsserver ist zur Verwaltung der Inhalte von Mobilstationen eingerichtet. Die Mobilstation umfasst jeweils ein mobiles Endgerät mit einer gesicherten Laufzeitumgebung und ein entfernbares oder festimplementiertes Sicherheitselement. Der Verwaltungsserver umfasst einen herkömmlichen Sicherheitselement-Sendeserver, der dazu eingerichtet ist, an das Sicherheitselement Sicherheitselement-Nachrichten zu senden, die von dem Sicherheitselement empfangen und ausgewertet werden können. Der Verwaltungsserver zeichnet sich dadurch aus, dass er weiter dazu eingerichtet ist, Endgerät-Nachrichten, die von der gesicherten Laufzeitumgebung des Endgeräts empfangen werden können, entgegenzunehmen und an einen im Sicherheitselement eingerichteten Endgerät-Sendeserver weiterzuleiten. Die Kommunikation mit der gesicherten Laufzeitumgebung wird schließlich durch den im Sicherheitselement vorgesehenen und in Anspruch 1 angegebenen Endgerät-Sendeserver durchgeführt. Der Verwaltungsserver selbst muss dagegen nicht in der Lage sein, direkt mit der gesicherten Laufzeitumgebung zu kommunizieren. Folglich hat der Betreiber des Verwaltungsservers, z.B. ein Mobilfunk-Netzbetreiber, einen vergleichsweise geringen Aufwand.

Ein erfindungsgemäßes Inhalte-Verwaltungssystem umfasst mindestens eine Mobilstation sowie einen Verwaltungsserver wie oben beschrieben.

Das Inhalte-Verwaltungssystem umfasst wahlweise weiter einen Inhalteserver (Content Server), durch den Inhalte, insbesondere Daten oder/und Pro-

gramme, zum Speichern in die gesicherte Laufzeitumgebung eines mobilen Endgeräts an den Sicherheitselement-Sendeserver bereitstellbar sind. Der Inhalteserver für Inhalte für die gesicherte Laufzeitumgebung kann wahlweise getrennt vorgesehen sein von einem Inhalteserver für Inhalte für das Sicherheitselement. Alternativ kann für Inhalte für Sicherheitselement und Laufzeitumgebung ein gemeinsamer/kombinierter Inhalteserver vorgesehen sein. Der Inhalteserver kann vom selben Betreiber betrieben werden wie der Verwaltungsserver oder alternativ von einem anderen Betreiber.

Ein erfindungsgemäßes Verfahren zum Speichern eines Inhalts, insbesondere von Daten oder/und eines Programms, in die gesicherte Laufzeitumgebung des mobilen Endgeräts zeichnet sich dadurch aus, dass
- der Inhalt von einem außerhalb der Mobilstation vorgesehenen Inhalteserver (Content Server) an einen außerhalb der Mobilstation vorgesehenen Sicherheitselement-Sendeserver bereitgestellt wird,
- der Inhalt in einer Sicherheitselement-Nachricht vom Sicherheitselement-Sendeserver an einen im Sicherheitselement eingerichteten Endgerät-Sendeserver gesendet wird und
- der Inhalt in einer Endgerät-Nachricht vom Endgerät-Sendeserver an die gesicherte Laufzeitumgebung gesendet wird.

Als Inhalte können insbesondere Daten oder/und Programmcode wie Treiber, Applikationen oder/und Aktualisierungen dafür vorgesehen sein.

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

Fig. 1 ein herkömmliches Laden von Inhalten in eine Mobilstation;
Fig. 2 ein herkömmliches Laden von Inhalten in eine Mobilstation;

Fig. 3 ein Laden von Inhalten in eine Mobilstation, gemäß einer Ausführungsform der Erfindung.

Fig. 1 und Fig. 2 zeigen das herkömmliche Laden von Inhalten in eine Mobilstation, die ein mobiles Endgerät ME mit einer gesicherten Laufzeitumgebung TEE und ein Sicherheitselement SE umfasst. Inhalte (Daten, Programmcode, Treiber, Applikationen, Aktualisierungen zu den genannten Inhalten etc.) CONT für die gesicherte Laufzeitumgebung TEE werden durch einen TEE Inhalte Server TEE CONT an einen Trusted Service Manager TEE TSM gemäß Global Platform bereitgestellt und durch den TEE TSM in die gesicherte Laufzeitumgebung TEE des Endgeräts ME geladen. Inhalte (Daten, Programmcode, Treiber, Applikationen, Aktualisierungen zu den genannten Inhalten etc.) CONT für das Sicherheitselement SE werden durch einen SE Inhalte Server SE CONT an einen Sicherheitselement Trusted Service Manager SE TSM (Sicherheitselement-Sendeserver) gemäß ETSI bereitgestellt und durch den SE TSM in das Sicherheitselement geladen. Wie in Fig. 2 gezeigt ist, werden die Inhalte für das Sicherheitselement SE in ETSI konformen Sicherheitselement-Nachrichten SN übermittelt. Inhalte für die gesicherte Laufzeitumgebung TEE werden in Global Platform konformen Endgerät-Nachrichten TN übermittelt. Der herkömmliche Sicherheitselement Trusted Service Manger SE TSM kann nur ETSI konforme Nachrichten verarbeiten. Der herkömmliche Trusted Service Manager für die gesicherte Laufzeitumgebung TEE TSM kann nur Nachrichten gemäß Global Platform verarbeiten.

Gemäß Fig. 1 und Fig. 2 werden somit herkömmlicherweise Inhalte für Endgerät ME und Sicherheitselement SE durch separate Server-Infrastrukturen bereitgestellt und geladen.

Fig. 3 zeigt ein Laden von Inhalten in eine Mobilstation, gemäß einer Ausführungsform der Erfindung. Inhalte für das Sicherheitselement SE werden wie in Fig. 1, 2 auf herkömmliche Weise in das Sicherheitselement SE geladen. Inhalte für die gesicherte Laufzeitumgebung TEE werden, in dieser Hinsicht wie herkömmlich, in Global Platform konformen Endgerät-Nachrichten TN gesendet. Im Unterschied zum Stand der Technik werden diese Endgerät-Nachrichten TE durch den Trusted Service Manager SE TSM, der für das Sicherheitselement SE vorgesehen ist, (Sicherheitselement-Sendeserver) an das Sicherheitselement SE gesendet. Der im Sicherheitselement SE implementierte TEE Trusted Service Manager TEE TSM, der für die gesicherte Laufzeitumgebung TEE vorgesehen ist, (Endgerät-Sendeserver) erkennt die Endgerät-Nachrichten TN als solche und leitet sie an die gesicherte Laufzeitumgebung TEE des Endgeräts ME weiter. Daher ist beim in Fig. 3 skizzierten System die Verwaltung der gesicherten Laufzeitumgebung TEE von einem herkömmlichen externen TEE TSM Server in das erweiterte Sicherheitselement SE verlagert. Im Sicherheitselement SE wird die Verwaltung des TEE genauer durch den kartenintern integrierten TEE TSM Server durchgeführt.

Patentansprüche

1. Mobilstation, umfassend ein mobiles Endgerät (ME) mit einer gesicherten Laufzeitumgebung (TEE) und ein entfernbares oder festimplementiertes Sicherheitselement (SE),
wobei im Sicherheitselement (SE) eine Sicherheitselement-Empfangseinrichtung zum Empfangen von an das Sicherheitselement gesandten Sicherheitselement-Nachrichten (SN) eingerichtet ist,
und wobei in der gesicherten Laufzeitumgebung (TEE) des Endgeräts (ME) eine Endgerät-Empfangseinrichtung zum Empfangen von an die gesicherte Laufzeitumgebung (TEE) des Endgeräts (ME) gesandten Endgerät-Nachrichten (TN) eingerichtet ist,
gekennzeichnet durch
einen im Sicherheitselement (SE) eingerichteten Endgerät-Sendeserver (TEE-TSM), der dazu eingerichtet ist, an die gesicherte Laufzeitumgebung (TEE) Endgerät-Nachrichten (TN) zu senden, die von der gesicherten Laufzeitumgebung (TEE) empfangen werden können.

2. Mobilstation nach Anspruch 1, wobei das Sicherheitselement (SE) und die Sicherheitselement-Nachrichten (SN) gemäß ETSI spezifiziert sind und die gesicherte Laufzeitumgebung (TEE) und die Endgerät-Nachrichten (TN) gemäß Global Platform spezifiziert sind.

3. Verwaltungsserver (SERV) für Mobilstationen, die jeweilige Mobilstation umfassend ein mobiles Endgerät (ME) mit einer gesicherten Laufzeitumgebung (TEE) und ein entfernbares oder festimplementiertes Sicherheitselement (SE),
wobei der Verwaltungsserver (SERV) einen Sicherheitselement-Sendeserver (SE-TSM) umfasst, der dazu eingerichtet ist, an das Sicherheitselement (SE) Sicherheitselement-Nachrichten (SN) zu senden, die von dem Sicherheitselement (SE) empfangen werden können,

dadurch gekennzeichnet, dass
der Verwaltungsserver (SERV) dazu eingerichtet ist, Endgeräte-Nachrichten (TE), die von der gesicherten Laufzeitumgebung (TEE) des Endgeräts (ME) empfangen werden können, entgegenzunehmen und an einen im Sicherheitselement (SE) eingerichteten Endgerät-Sendeserver (TEE-TSM) weiterzuleiten.

4. Inhalte-Verwaltungssystem, umfassend mindestens eine Mobilstation nach Anspruch 1 oder 2 und einen Verwaltungsserver (SERV) nach Anspruch 3.

5. Inhalte-Verwaltungssystem nach Anspruch 4, weiter umfassend einen Inhalteserver (CONT), durch den Inhalte, insbesondere Daten oder/und Programme, zum Speichern in die gesicherte Laufzeitumgebung (TEE) eines mobilen Endgeräts (ME) an den Sicherheitselement-Sendeserver (SE-TSM) bereitstellbar sind.

6. Verfahren, für eine Mobilstation umfassend ein mobiles Endgerät (ME) mit einer gesicherten Laufzeitumgebung (TEE) und ein entfernbares oder festimplementiertes Sicherheitselement (SE), zum Speichern eines Inhalts, insbesondere von Daten oder/und eines Programms, in die gesicherte Laufzeitumgebung (TEE) des mobilen Endgeräts (ME),
dadurch gekennzeichnet, dass bei dem Verfahren
- der Inhalt von einem außerhalb der Mobilstation vorgesehenen Inhalteserver (CONT) an einen außerhalb der Mobilstation vorgesehenen Sicherheitselement-Sendeserver (SE-TSM) bereitgestellt wird,
- der Inhalt in einer Sicherheitselement-Nachricht (SN) vom Sicherheitselement-Sendeserver (SE-TSM) an einen im Sicherheitselement (SE) eingerichteten Endgerät-Sendeserver (ME-TSM) gesendet wird und

- der Inhalt in einer Endgerät-Nachricht (TN) vom Endgerät-Sendeserver (ME-TSM) an die gesicherte Laufzeitumgebung (TEE) gesendet wird.

7. Verfahren nach Anspruch 6, wobei das Sicherheitselement (SE) und die Sicherheitselement-Nachrichten (SN) gemäß ETSI spezifiziert sind und die gesicherte Laufzeitumgebung (TEE) und die Endgerät-Nachrichten (TN) gemäß Global Platform spezifiziert sind.

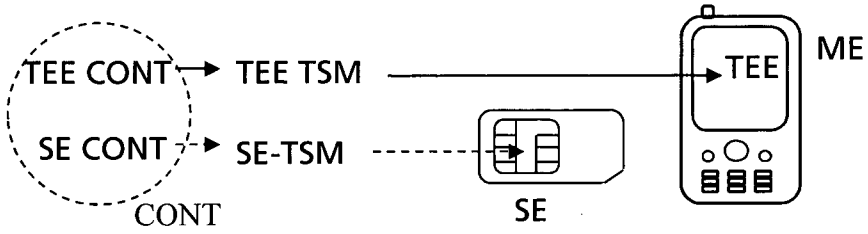

TEE CONT
TEE TSM
SE CONT
SE-TSM
CONT
SE
TEE
ME

Fig. 1

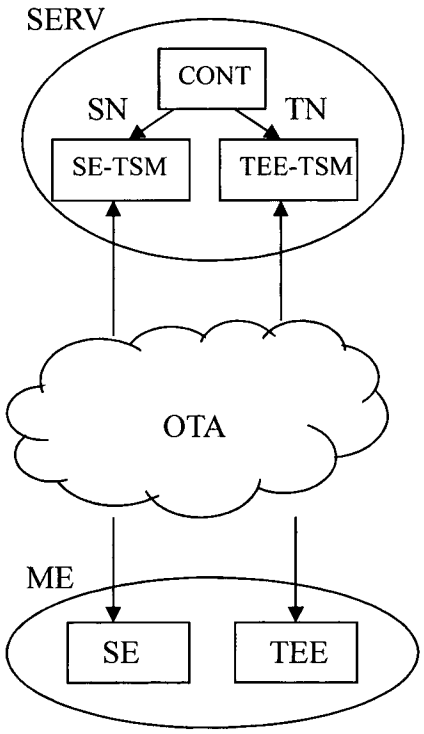

SERV
CONT
SN
TN
SE-TSM
TEE-TSM
OTA
ME
SE
TEE

Fig. 2

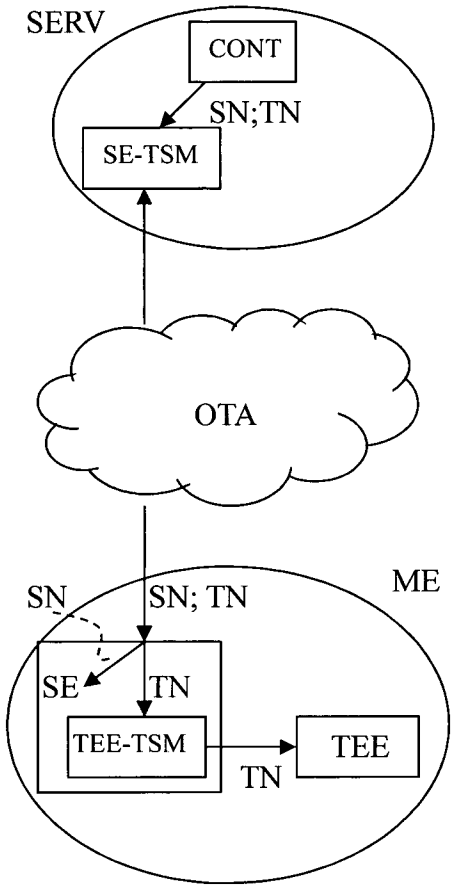


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/002720

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/74 H04L29/06
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)
G06F 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/027743 A2 (VODAFONE PLC [GB]; BELROSE CAROLINE [GB]; BONE NICHOLAS [GB]) 5 March 2009 (2009-03-05)	1,2
Y	page 7, line 1 - page 9, line 8	4-7
A	page 12, line 19 - page 13, line 20 page 14, line 17 - page 16, line 2; claims 1,16,23,33-36; figures 1,22	3

X	EP 2 291 015 A1 (GEMALTO SA [FR]) 2 March 2011 (2011-03-02)	3
Y	paragraph [0023] - paragraph [0027]	4-7
A	paragraph [0097] - paragraph [0109] paragraph [0133] - paragraph [0146]; claims 1-10; figures 1,2	1,2

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] 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
19 November 2013	28/11/2013

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	Schwibinger, Hans

3

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	NN: "The Trusted Execution Environment, White Paper", GlobalPlatform inc. , 28 February 2011 (2011-02-28), XP002716538, Retrieved from the Internet: URL:http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf [retrieved on 2013-11-11] page 10, line 1 - page 15, line 3 page 21, line 1 - line 23; figures 1-3 -----	1-7
A	EP 1 890 228 A2 (GIESECKE & DEVRIENT GMBH [DE]) 20 February 2008 (2008-02-20) paragraph [0030] - paragraph [0031] paragraph [0043] - paragraph [0044]; claim 2; figures 1,3,4,12,18,19 -----	1-7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/002720

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009027743 A2	05-03-2009	EP 2198382 A2	23-06-2010
		GB 2453518 A	15-04-2009
		US 2011003580 A1	06-01-2011
		WO 2009027743 A2	05-03-2009
EP 2291015 A1	02-03-2011	CN 102577454 A	11-07-2012
		EP 2291015 A1	02-03-2011
		EP 2474178 A1	11-07-2012
		US 2012164981 A1	28-06-2012
		WO 2011023819 A1	03-03-2011
EP 1890228 A2	20-02-2008	DE 102006038876 A1	21-02-2008
		EP 1890228 A2	20-02-2008

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/002720

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/74 H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F 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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2009/027743 A2 (VODAFONE PLC [GB]; BELROSE CAROLINE [GB]; BONE NICHOLAS [GB]) 5. März 2009 (2009-03-05)	1,2
Y	Seite 7, Zeile 1 - Seite 9, Zeile 8	4-7
A	Seite 12, Zeile 19 - Seite 13, Zeile 20 Seite 14, Zeile 17 - Seite 16, Zeile 2; Ansprüche 1,16,23,33-36; Abbildungen 1,22	3
X	EP 2 291 015 A1 (GEMALTO SA [FR]) 2. März 2011 (2011-03-02)	3
Y	Absatz [0023] - Absatz [0027]	4-7
A	Absatz [0097] - Absatz [0109] Absatz [0133] - Absatz [0146]; Ansprüche 1-10; Abbildungen 1,2	1,2

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] 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
19. November 2013	28/11/2013

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	Schwibinger, Hans

3

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	NN: "The Trusted Execution Environment, White Paper", GlobalPlatform inc. , 28. Februar 2011 (2011-02-28), XP002716538, Gefunden im Internet: URL:http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf [gefunden am 2013-11-11] Seite 10, Zeile 1 - Seite 15, Zeile 3 Seite 21, Zeile 1 - Zeile 23; Abbildungen 1-3 -----	1-7
A	EP 1 890 228 A2 (GIESECKE & DEVRIENT GMBH [DE]) 20. Februar 2008 (2008-02-20) Absatz [0030] - Absatz [0031] Absatz [0043] - Absatz [0044]; Anspruch 2; Abbildungen 1,3,4,12,18,19 -----	1-7

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/002720

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2009027743 A2	05-03-2009	EP 2198382 A2	23-06-2010
		GB 2453518 A	15-04-2009
		US 2011003580 A1	06-01-2011
		WO 2009027743 A2	05-03-2009
EP 2291015 A1	02-03-2011	CN 102577454 A	11-07-2012
		EP 2291015 A1	02-03-2011
		EP 2474178 A1	11-07-2012
		US 2012164981 A1	28-06-2012
		WO 2011023819 A1	03-03-2011
EP 1890228 A2	20-02-2008	DE 102006038876 A1	21-02-2008
		EP 1890228 A2	20-02-2008