

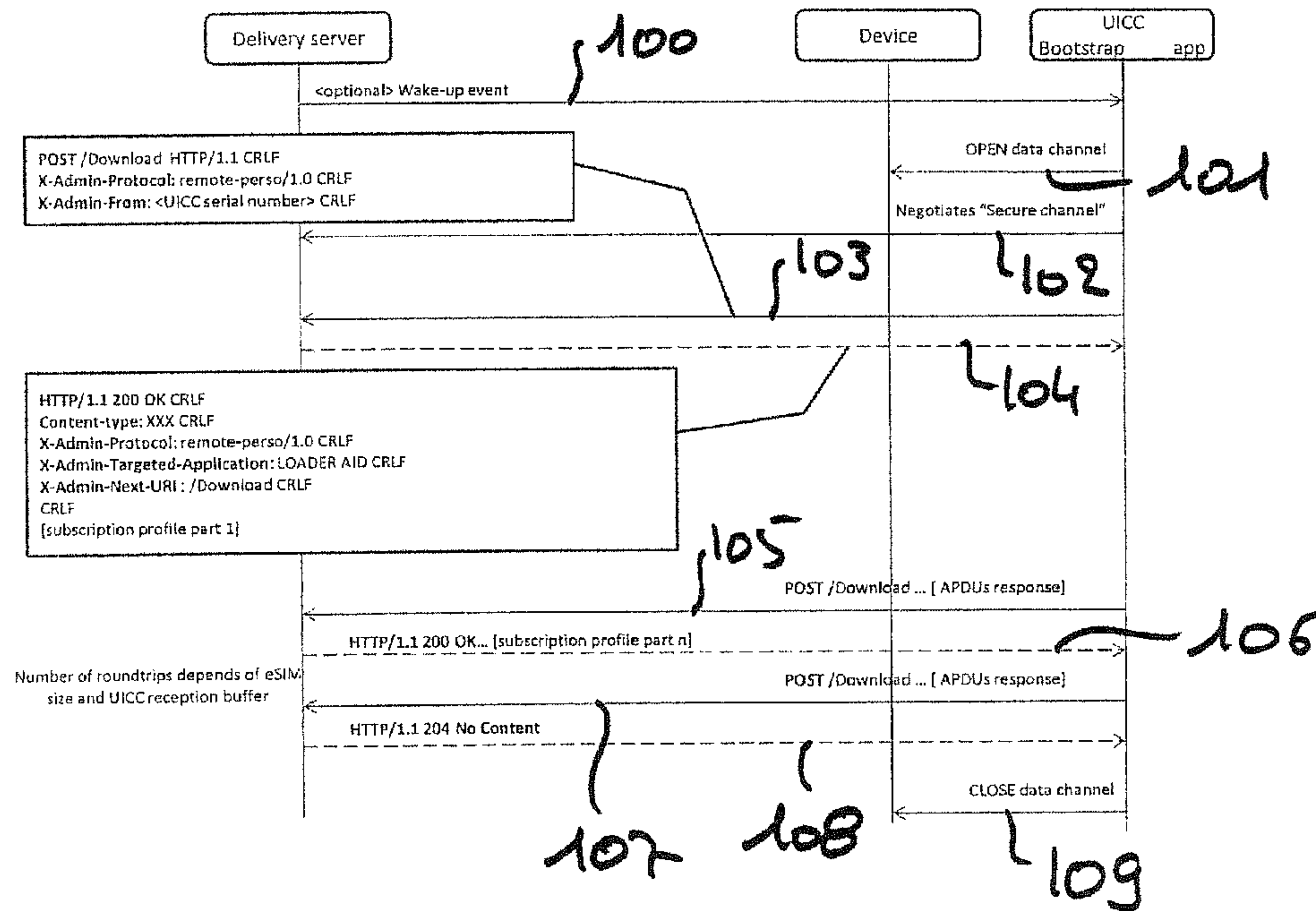


(86) Date de dépôt PCT/PCT Filing Date: 2011/12/02
 (87) Date publication PCT/PCT Publication Date: 2012/06/14
 (85) Entrée phase nationale/National Entry: 2013/06/03
 (86) N° demande PCT/PCT Application No.: EP 2011/071675
 (87) N° publication PCT/PCT Publication No.: 2012/076425
 (30) Priorité/Priority: 2010/12/06 (EP10306359.0)

(51) Cl.Int./Int.Cl. *H04W 8/20* (2009.01),
G06F 21/00 (2013.01), *H04L 29/06* (2006.01)
 (71) Demandeur/Applicant:
GEMALTO SA, FR
 (72) Inventeurs/Inventors:
BERARD, XAVIER, FR;
GACHON, DENIS, FR
 (74) Agent: ROBIC

(54) Titre : PROCÉDE POUR ACHEMINER A DISTANCE UN PROFIL D'ABONNEMENT COMPLET A UN UICC SUR IP
 (54) Title: METHOD FOR REMOTELY DELIVERING A FULL SUBSCRIPTION PROFILE TO A UICC OVER IP

FIG. 1



(57) **Abrégé/Abstract:**

The invention proposes a method consisting in: - opening (102), at the request of the UICC (101), a data channel between the terminal and the server; - performing a mutual authentication between the UICC and the server by using the bootstrap credentials; - requesting (105, 107), from the UICC to the server, the delivery of a subscription profile by using the unique serial number; - if a subscription profile exists for the UICC, downloading (106, 108) the subscription profile to the UICC.



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau(10) International Publication Number
WO 2012/076425 A1(43) International Publication Date
14 June 2012 (14.06.2012)

(51) International Patent Classification:

H04W 8/20 (2009.01) *H04L 29/06* (2006.01)
G06F 21/00 (2006.01)

(21) International Application Number:

PCT/EP2011/071675

(22) International Filing Date:

2 December 2011 (02.12.2011)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10306359.0 6 December 2010 (06.12.2010) EP

(71) Applicant (for all designated States except US):

GEMALTO SA [FR/FR]; 6 rue de la Verrerie, F-92190
Meudon (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BERARD, Xavier**
[FR/FR]; 18, Route du stade, F-13950 Cadolive (FR).
GACHON, Denis [FR/FR]; Lot Rivière de Peyruis, F-
83640 Saint Zacharie (FR).

(81) Designated States (unless otherwise indicated, for every

kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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) Designated States (unless otherwise indicated, for every

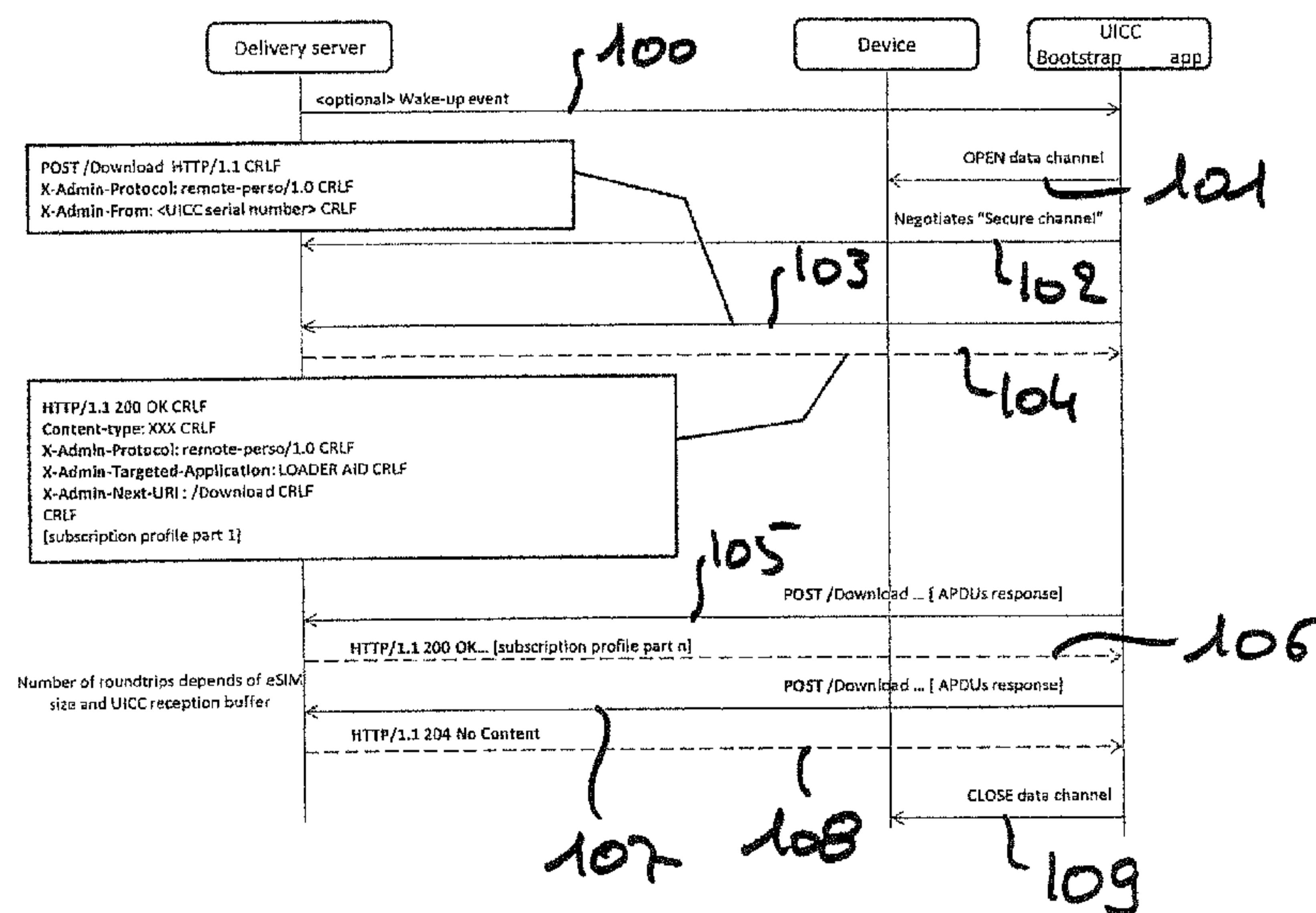
kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD FOR REMOTELY DELIVERING A FULL SUBSCRIPTION PROFILE TO A UICC OVER IP

FIG. 1



(57) Abstract: The invention proposes a method consisting in: - opening (102), at the request of the UICC (101), a data channel between the terminal and the server; - performing a mutual authentication between the UICC and the server by using the bootstrap credentials; - requesting (105, 107), from the UICC to the server, the delivery of a subscription profile by using the unique serial number; - if a subscription profile exists for the UICC, downloading (106, 108) the subscription profile to the UICC.

Method for remotely delivering a full subscription profile to a UICC over IP

The present invention concerns a method for remotely delivering a full subscription profile to a UICC over IP.

5 In the domain of telecommunications, secure elements, like UICCs (Universal Integrated Circuit Card) embedding Sim applications, are installed, fixedly or not, in terminals, like for example mobile phones. In some cases, the terminals are constituted by machines that communicate with other machines for M2M (Machine to Machine) applications.

10 A UICC can be in the format of a smart card, or may be in any other format such as for example but not limited to a packaged chip as described in PCT/SE2008/050380, or any other format. It can be used in mobile terminals in GSM and UMTS networks for instance. The UICC ensures network authentication, integrity and security of all kinds of personal data.

15 In a GSM network, the UICC contains mainly a SIM application and in a UMTS network it is the USIM application. A UICC may contain several other applications, making it possible for the same smart card to give access to both GSM and UMTS networks, and also provide storage of a phone book and other applications. It is also possible to access a GSM network using an USIM application and it is possible to access UMTS networks using a SIM application with mobile terminals prepared for this. With the UMTS release 5 and later stage network like LTE, a new application, the IP multimedia Services Identity Module (ISIM) is required for services in the
20 IMS (IP Multimedia Subsystem). The telephone book is a separate application and not part of either subscription information module.

25 In a CDMA network, the UICC contains a CSIM application, in addition to 3GPP USIM and SIM applications. A card with all three features is called a removable user identity card, or R-UIM. Thus, the R-UIM card can be inserted into CDMA, GSM, or UMTS handsets, and will work in all three cases.

In 2G networks, the SIM card and SIM application were bound together, so that "SIM card" could mean the physical card, or any physical card with the SIM application.

30 The UICC smart card consists of a CPU, ROM, RAM, EEPROM and I/O circuits. Early versions consisted of the whole full-size (85 × 54 mm, ISO/IEC 7810 ID-1) smart card. Soon the race for smaller telephones called for a smaller version of the card.

Since the card slot is standardized, a subscriber can easily move their wireless account and phone number from one handset to another. This will also transfer their phone book and text messages. Similarly, usually a subscriber can change carriers by inserting a new carrier's UICC card into their existing handset. However, it is not always possible because some carriers

(e.g. in U.S.) SIM-LOCK the phones that they sell, thus preventing competitor carriers' cards being used.

The integration of the ETSI framework and the Application management framework of Global Platform is standardized in the UICC configuration.

5 UICCs are standardized by 3GPP and ETSI.

A UICC can normally be removed from a mobile terminal, for example when the user wants to change his mobile terminal. After having inserted his UICC in his new terminal, the user will still have access to his applications, contacts and credentials (network operator).

10 It is also known to solder or weld the UICC in a terminal, in order to get it dependent of this terminal. This is done in M2M (Machine to Machine) applications. The same objective is reached when a chip (a secure element) containing the SIM or USIM applications and files is contained in the terminal. The chip is for example soldered to the mother-board of the terminal or machine and constitutes an e-UICC.

15 Some of the further disclosed inventions apply to such soldered UICCs or to such chips containing the same applications than the chips comprised in UICCs. A parallel can be done for UICCs that are not totally linked to devices but that are removable with difficulty because they are not intended to be removed, located in terminals that are distant or deeply integrated in machines. A special form factor of the UICC (very small for example and therefore not easy to handle) can also be a reason to consider it as in fact integrated in a terminal. The same applies
20 when a UICC is integrated in a machine that is not intended to be opened.

In the next description, welded UICCs or chips containing or designed to contain the same applications than UICCs will generally be called embedded UICCs or embedded secure elements (in contrast to removable UICCs or removable secure elements). This will also apply to UICCs or secure elements that are removable with difficulty.

25 The present invention concerns a method for remotely delivering a full subscription profile to a UICC over IP. More precisely, the invention concerns the delivery of a full subscription profile (including File System, Security Domains, Applications (STK, USIM, ISM,...), unique data like Ki, applicative keys,...) to a UICC embedded in a device using an HTTP transport OTI or OTA.

30 The invention proposes to solve the following problem. Once a UICC is attached to a receiving device, for instance soldered, or simply not physically removable because of the device form factor, or because not economically viable (distance,...), or when the device has to be commercialized without any attachment to a particular subscription (in order to give to the

end-user the possibility to choose separately the device and the subscription), it is no longer possible to personalize the UICC at manufacturing stage with subscription profile.

The invention proposes a way to perform the personalization of a UICC remotely, in a very secure way, when the UICC is already deployed on the market without low expectations regarding device functionalities (IP connectivity only). The MNO profile has to be downloaded via OTA or OTI since the UICC is already in the field.

The invention proposes to use the HTTP protocol in order to personalize remotely a UICC.

More precisely, the invention proposes a method for remotely delivering a full subscription profile to a UICC over IP, the UICC being installed in a terminal able to provide an IP connectivity to a remote server and give access to the UICC. The UICC is pre-personalised with a unique serial number and with a bootstrap application and bootstrap credentials allowing establishing a secure transport channel with the remote server. The remote server hosts a stock of subscription profiles and acts as a web server. According to the invention, the method consists in:

- opening, at the request of the UICC, a data channel between the terminal and the server;
- performing a mutual authentication between the UICC and the server by using the bootstrap credentials;
- requesting, from the UICC to the server, the delivery of a subscription profile by using the unique serial number;
- if a subscription profile exists for the UICC, downloading the subscription profile to the UICC.

Preferably, the http communication protocol is used between the UICC and the remote server.

Advantageously, the UICC and the terminal communicate over a BIP channel.

The present invention will be better understood by reading the following description in relation to figure 7 that describes the overall overflow of an embodiment of the invention.

This invention requires:

- a UICC pre-personalised with a unique serial number and with a bootstrap application, bootstrap credentials allowing to establish a secure transport channel with a remote server entity;
- a remote Delivery server which role is to host and deliver a stock of subscription profiles and acting as a simple web server;

- a device (terminal) able to provide an IP connectivity to the remote server and give access to the UICC, for instance through a BIP interface. The connectivity may be provided by any of these methods for instance: wired, WIFI, OTA through a pre-loaded UICC subscription which role is to only provide initial data connection.

5 The diagram of figure 1 presents the overall flow.

At the beginning of the sequence we assume that the subscription profile for the UICC has been determined and reserved in the Delivery server.

10 - At step 100, optionally, the Delivery Server may send to the UICC a wake-up event to triggers UICC connection. This may also be achieved simply by the UICC itself at power on, or by a periodic connection.

- At step 101, the UICC requests the device to open a data channel. At this stage the UICC may provide connectivity information. A preferred method would be a BIP OPEN CHANNEL command.

15 - At step 102, the UICC negotiates the opening of a secure channel with the Delivery Server using its pre-loaded credentials. A preferred method would be the establishment of a SCP 81 (PSK-TLS) channel as defined in Global Platform. During this step, a mutual authentication occurs between the UICC and the Delivery server and the integrity of the exchanged data can be verified.

20 - At step 103, the UICC sends a first HTTP POST request to the delivery server using a pre-defined (or configurable) URL, requesting the delivery of the subscription profile. This request shall at least comprise the UICC serial number. The POST request in the diagram is given as example.

25 - The Delivery Server then checks if a subscription profile is available for this UICC. If yes, at step 104, the Delivery server returns an HTTP 200 OK response with the subscription profile as body of the answer. In case no subscription profile is available for this UICC a 204 No content response shall be returned.

- The UICC then receives the HTTP response and executes the loading of the subscription profile. At step 105, the UICC sends a second HTTP POST request on the URL given as NEXT-URI in the server response. This POST shall include loading execution status.

30 - In case the UICC is not able to receive in a single answer the whole subscription profile, it may be required to perform several round-trips between UICC and delivery server (steps 106 and 107).

- The sequence shall end when the whole subscription profile has been delivered. In that case the last Delivery Server HTTP response shall indicate a 204 No content (step 108).

- At step 109, the UICC closes the data channel established with the device.

This method may also be applicable to an UICC not physically attached to the device (removable UICC).

5 HTTP protocol is preferably used for communicating with the delivery server, and BIP protocol for the communications between the UICC and the device.

Claims

1. Method for remotely delivering a full subscription profile to a UICC over IP, said UICC being installed in a terminal able to provide an IP connectivity to a remote server and give access to said UICC, said UICC being pre-personalised with a unique serial number and with a bootstrap application and bootstrap credentials allowing to establish a secure transport channel with said remote server, said remote server hosting a stock of subscription profiles and acting as a web server, said method consisting in:
- opening, at the request of said UICC, a data channel between said terminal and said server;
 - performing a mutual authentication between said UICC and said server by using said bootstrap credentials;
 - requesting, from said UICC to said server, the delivery of a subscription profile by using said unique serial number;
 - if a subscription profile exists for said UICC, downloading said subscription profile to said UICC.
2. Method according to claim 1, wherein http communication protocol is used between said UICC and said remote server.
3. Method according to any of the claims 1 or 2, wherein said UICC and said terminal communicate over a BIP channel.

FIG. 1

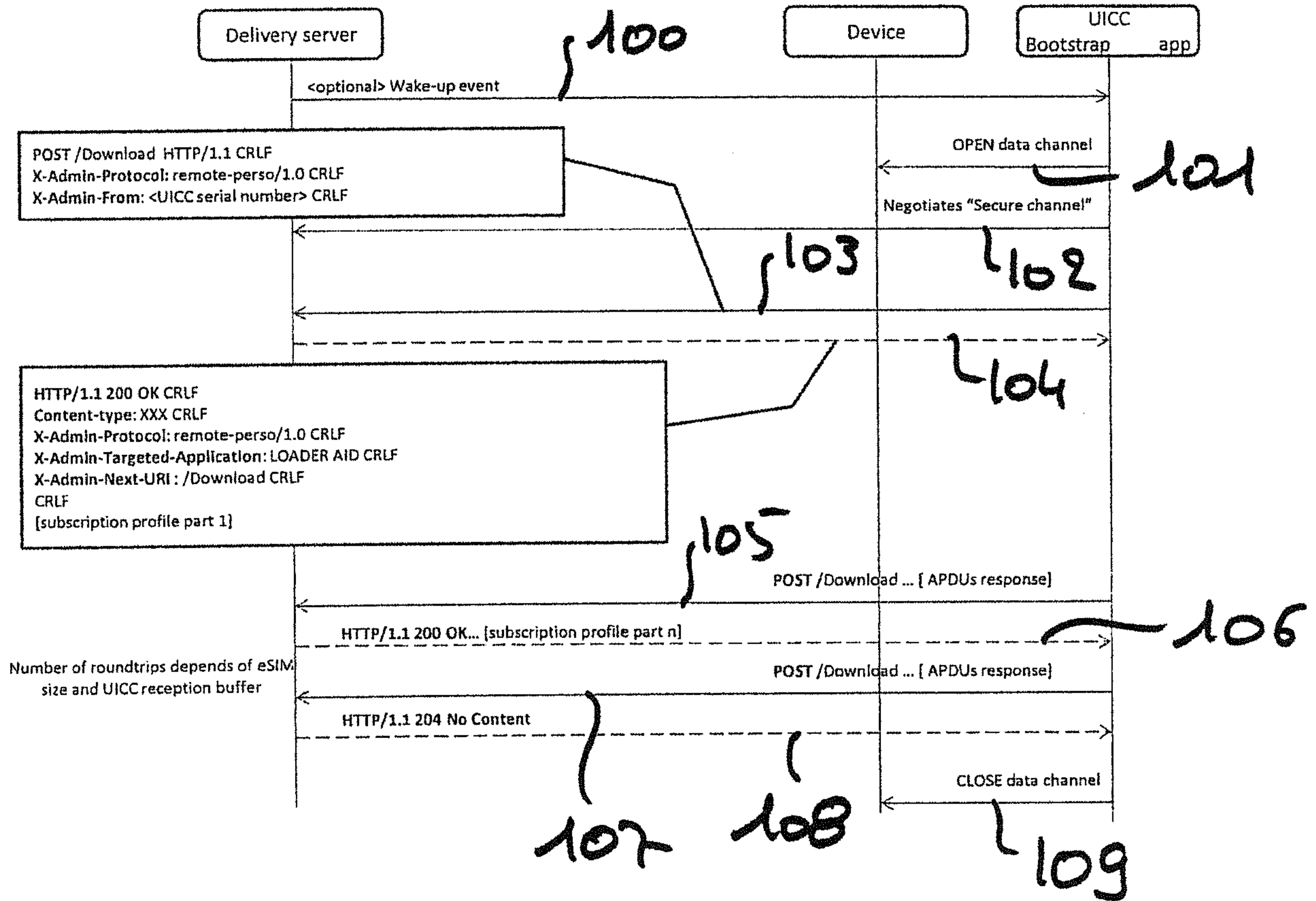


FIG. 1

