



- | | |
|---|---|
| (51) International Patent Classification:
<i>G06F 21/33</i> (2013.01) | (72) Inventors: FRIELINGSDORF, Matthias ; Königswinterer Straße 258, 53227 Bonn (DE). SCHENK, Volker ; In den Herbstbenden 17, 53881 Euskirchen (DE). |
| (21) International Application Number:
PCT/EP2017/065931 | (74) Agent: SCHWÖBEL, Thilo et al.; Kutzenberger Wolff & Partner, Theodor-Heuss-Ring 23, 50668 Köln (DE). |
| (22) International Filing Date:
27 June 2017 (27.06.2017) | (81) Designated States (<i>unless otherwise indicated, for every kind of national protection available</i>): 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW. |
| (25) Filing Language:
English | |
| (26) Publication Language:
English | |
| (30) Priority Data:
16179012.6 12 July 2016 (12.07.2016) EP | |
| (71) Applicant: DEUTSCHE TELEKOM AG [DE/DE];
Friedrich-Ebert-Allee 140, 53113 Bonn (DE). | |

(54) Title: METHOD FOR PROVIDING AN ENHANCED LEVEL OF AUTHENTICATION RELATED TO A SECURE SOFTWARE CLIENT APPLICATION PROVIDED BY AN APPLICATION DISTRIBUTION ENTITY IN ORDER TO BE TRANSMITTED TO A CLIENT COMPUTING DEVICE; SYSTEM, APPLICATION DISTRIBUTION ENTITY, SOFTWARE CLIENT APPLICATION, AND CLIENT COMPUTING DEVICE FOR PROVIDING AN ENHANCED LEVEL OF AUTHENTICATION RELATED TO A SECURE SOFTWARE CLIENT APPLICATION, PROGRAM AND COMPUTER PROGRAM PRODUCT

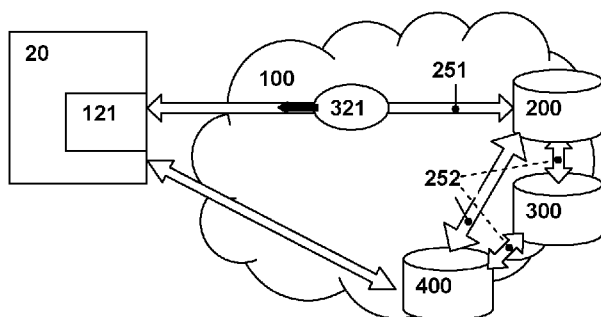


Fig. 1

(57) Abstract: The invention relates to a method for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device, wherein a first secure communication channel is established - in view of transmitting an instance of the software client application to the client computing device - between the client computing device and the application distribution entity, and wherein a second secure communication channel is established between the application distribution entity and a third party server entity, wherein the method comprises the following steps: - in a first step, an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data - provided by the software client application instance upon it being executed by the client computing device - to the third party server entity, the asymmetric pair of cryptographic keys comprising a specific private cryptographic key and a specific public cryptographic key, - in a second step, subsequent to the first step, - the software client application instance as well as the specific private cryptographic key, or - the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key, is transmitted to the client computing device using the

(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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

Method for providing an enhanced level of authentication related to a secure software client application provided by an application distribution entity in order to be transmitted to a client computing device; system, application distribution entity, software client application, and client computing device for providing an enhanced
5 **level of authentication related to a secure software client application, program and computer program product**

BACKGROUND

[0001] The present invention relates to a method for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device, wherein a first secure communication channel is established – in view of transmitting an instance of the software client application to the client computing device – between the client computing device and the application distribution entity, and wherein a second secure communication channel is established between the application distribution entity and a third party server entity.

[0002] The present invention further relates to a system for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device, the system comprising the client computing device, the application distribution entity and a third party server entity.

25 **[0003]** Additionally, the invention relates to an application distribution entity for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device.

30 **[0004]** Furthermore, the invention relates to a software client application instance for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted,

using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device.

[0005] Additionally, the present invention relates to a client computing device for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device.

[0006] Furthermore, the invention relates to a program comprising a computer readable program code and to a computer program product for providing an enhanced level of authentication related to a secure software client application provided by an application distribution entity.

[0007] Today, software – or applications or apps – to be used by client devices (such as desktop computers, or mobile computers such as tablets, mobile phones or the like) is often distributed using download stores or application stores. It is known to provide application stores such that the downloaded software is at least adapted to the client device class, i.e. a different version of the software could be downloaded dependent on whether the requesting client device is, e.g., a phone device or a tablet device.

[0008] However, it becomes more and more important – especially with respect to the development of the internet of things or mobile devices handling sensitive data – that data provided by client devices can be trusted. Since such data are typically provided by software client applications, the software client applications need to be trusted, hence the software client application need to be authenticated.

SUMMARY

[0009] An object of the present invention is to provide a cost effective and comparatively fast solution, especially an automated solution, for providing an enhanced level of authentication related to a secure software client application that is provided by an application distribution entity and transmitted to a client computing device, and/or for providing an enhanced level of authentication related to data generated or provided by such a secure software client application.

[0010] The object of the present invention is achieved by a method for providing an enhanced level of authentication related to a secure software client application that is

provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device, wherein a first secure communication channel is established – in view of transmitting an instance of the software client application to the client computing device – between the client computing device and the application distribution entity, and wherein a second secure communication channel is established between the application distribution entity and a third party server entity,

wherein the method comprises the following steps:

- 10 -- in a first step, an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance upon it being executed by the client computing device – to the third party server entity, the asymmetric pair of cryptographic keys comprising a specific private cryptographic key and a specific public cryptographic key,
- 15 -- in a second step, subsequent to the first step,
 - the software client application instance as well as the specific private cryptographic key, or
 - the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key,
- 20 is transmitted to the client computing device using the first secure communication channel, and
- the specific public cryptographic key is transmitted to the third party server entity using the second secure communication channel.

[0011] According to the present invention, it is thereby advantageously possible that a software client application can be authenticated – i.e. provided with an enhanced level of authentication related to the software client application – (and thereby rendered more secure compared to a non-authenticated software client application) in an automated manner by means of the application distribution entity transmitting, to the client computing device, at least either (i.e. according to a first variant of the present invention) the software client application instance as well as the specific private cryptographic key using the first secure communication channel, or (i.e. according to a second variant of the present invention) the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key using the first secure communication channel, wherein in both the first and second variant according to the present invention, the specific private cryptographic key and the specific public cryptographic key are generated as an asymmetric pair of cryptographic keys, wherein

this pair of cryptographic keys is generated in view of subsequently (i.e. after the software client application instance being transmitted to the client computing device) allowing for an authenticated transmission of data – provided or generated by the software client application instance upon it being executed by the client computing device – to the third party server entity.

According to the present invention, the specific public cryptographic key is transmitted to the third party server entity using the second secure communication channel; this transmission (of the specific public cryptographic key to the third party server entity) either occurs (as a separate transmission) prior to or during or after the transmission of at least either the software client application instance as well as the specific private cryptographic key (first variant according to the present invention), or the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key (second variant according to the present invention).

[0012] By means of using the first secure communication channel between the application distribution entity and the client computing device, and the second secure communication channel between the application distribution entity and the third party server entity, it is advantageously possible according to the present invention to securely (i.e. in a protected manner) transmit the specific private cryptographic key to the client computing device, and the specific public cryptographic key to the third party server entity, ensuring confidentiality of the specific private cryptographic key and integrity of the specific public cryptographic key during transmission.

[0013] According to the present invention, it is advantageously possible to provide a cryptographically strong authentication of the client computing device and/or of the software client application instance: For each software client application instance that is executed on the client computing device and for which the method according to the present invention is used, a client certificate or client secret is present, on the client computing device and/or within the software client application instance, by means of which a mutual authentication of the communication channel between the software client application instance (and/or the respective client computing device), on the one hand, and the third party server entity (especially by means of conventionally used server certificates), on the other hand, is possible. Thereby, it is advantageously possible according to the present invention to provide an enhanced level of authentication concerning the communication (i.e. the data exchanged or transmitted) between the software client application instances of the client computing device and the third party server entity, especially relating to data generated or provided by such a secure software client application, such as, e.g., medical data, bank relating data or the like.

[0014] According to the present invention, it is advantageously possible to provide secure software client applications, i.e. software client applications that can be trusted, by means of requiring an authentication step to be performed. Furthermore, data exchanged between especially the software client application instance and the third party server entity should preferably be transmitted in a protected manner, especially regarding confidentiality and/or integrity and/or originality and/or non-repudiation.

[0015] According to the present invention, the third party server entity corresponds, e.g., to an application server, i.e. providing the server component of the software client application (instance) on the client computing device.

10 **[0016]** In conventionally known systems, different methods exist in order to improve the security of the communication between software client applications on client computing devices on the one hand, and server entities (or third party server entities) on the other hand (or between different software client applications, especially on different client computing devices): The most common approach consists in using TLS (Transport Layer Security) by means of using server certificates, i.e. the servers are authenticated towards the software client applications. However, typically the software client applications do not have a certificate typically used with a version of the TLS protocol family and, thus, the respective servers are typically not able to authenticate the software client applications in an easy and intuitive (for a user of the software client application) manner, in a comparatively cheap and/or comparatively fast manner, without requiring user interaction (or, at least, without requiring extensive user interaction) and especially automatically. Known authentication techniques involve, e.g., using a separate channel, transmission of data per snail mail, the use of credentials (such as, e.g., user name and password), other authentication techniques such as the use of OAuth-tokens; however, 25 such techniques typically require a registration process step of the user, hence (perhaps unintuitive) user interaction. An alternative consists in transmitting a secret as part of the software client application. However, conventionally such secrets are typically not individual to each software client application instance; this means that two client computing devices, having the same software client application (while, of course, having 30 different instances of the (same) software client application), would have the same secret – hence, an attacker able to retrieve that secret (common to all such instances of the software client application) would be able to eavesdrop on the communication between the software client application instances and the respective server, and could also make the respective server believe being a software client application instance of that kind 35 (impersonation).

[0017] According to the present invention, a pair of cryptographic keys is generated, and the (specific) private cryptographic key transmitted using a secure communication channel (i.e. the first secure communication channel) between the application distribution entity and the software client application instance (i.e. the client computing device). This 5 secure communication channel is typically provided by the application distribution entity, i.e. typically by the application store or app store. According to the present invention, it is advantageously possible to combine the distribution of the software client application instance (to a specific client computing device) with a specific pair of cryptographic keys (and hence the distribution or transmission of the specific private cryptographic key). This 10 provides the possibility to at least implicitly bind the pair of cryptographic keys to the software client application instance. This binding of the pair of cryptographic keys to the software client application instance also ensures that multiple requests to provide or to issue a client certificate do not result in providing a plurality of pairs of cryptographic key: typically, the application distribution entity ensures that each client computing device is 15 able to download each software client application only once (of course, the download of updates is normally allowed).

[0018] As a consequence, the client, i.e. the software client application instance within the client computing device, is equipped with an application-specific client certificate providing the possibility of a cryptographically strong authentication of the client 20 with regard to the third party server entity (and vice versa using the server certificate), e.g. by means of using TLS with mutual authentication. However, the method according to the present invention is independent from which specific protocol is used and which secure communication channel is used; other protocols than TLS, and also the use of a VPN (Virtual Private Network) channel is possible. According to the present invention, 25 besides the authentication of the third party server (by means of server certificates), also the cryptographically strong authentication of the client (i.e. the software client application instance and/or the client computing device) is possible. Thereby, it is possible that a request (or transmitted data) received at the third party server entity is able to be unequivocally assigned to a specific software client application instance (and hence 30 typically a person), or – especially in case of anonymous usage – that at least no fabricated data are received. An example of the latter situation might refer to a software client application that anonymously collects medical data, e.g. for a medical survey: Without an authentication of the data provided by the different software client application instances (of the different client computing devices of the participants of the survey), the 35 reception of fabricated or manipulated data at the third party server entity (potentially leading to false results) cannot be excluded.

[0019] Additionally, the use of a client certificate that is individual to the software client application instance limits the motivation of an attacker and also the potential damage: In case that an attacker is able to successfully retrieve the specific private cryptographic key, the use, according to the present invention, of an instance-specific client certificate (i.e. specific to each software client application instance) also means that the attacker is only able use this specific client certificate, i.e. with respect to this specific software client application instance; in order to use another software client application instance, the corresponding other client certificate would need to be retrieved.

[0020] According to the present invention, due to the fact that the generation of the pair of cryptographic keys is typically performed on a backend side (typically either at the application distribution entity or at the third party server entity, or at a trusted entity), the developer of the software client application (or the operator of the application distribution entity) is able to use a comparatively high cryptographic quality of the generated cryptographic keys; typically, at a backend side, more resources, especially concerning processing power, high-quality random number generators, etc., are available.

[0021] Furthermore according to the present invention, it is possible to newly transmit a (different) client certificate with each update of the software client application instance; especially in case of any doubts that any (previously transmitted) client certificates might be compromised.

[0022] According to an embodiment of the present invention, in a third step, prior to the first step, a unique identity information is assigned to the software client application instance, the identity information being specific to the software client application instance or to the combination of the software client application instance and the client computing device,

wherein during the second step,

- the identity information is additionally transmitted to the client computing device using the first secure communication channel, and furthermore
- the identity information or the mutual assignment of the specific public cryptographic key to the identity information is transmitted to the third party server entity using the second secure communication channel.

[0023] By means of using a unique identity information that is assigned to the software client application instance, it is advantageously possible, according to the present invention, to identify each software client application instance distributed by the application distribution entity. Hence, according to a third variant of the present invention, the identity information is additionally transmitted to the client computing device using the

first secure communication channel (i.e. the identity information is transmitted additionally to the software client application instance as well as the specific private cryptographic key. Furthermore, according to a fourth variant of the present invention, the identity information is additionally transmitted to the client computing device using the first secure
5 communication channel (i.e. the identity information is transmitted additionally to the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key). According to both the third and fourth variant of the present invention, at least one of the identity information and the mutual assignment of the specific public cryptographic key to the identity information is (or are) transmitted to
10 the third party server entity using the second secure communication channel.

[0024] According to a further embodiment of the present invention, prior to or during the first step, a unique identity information is assigned to the software client application instance,

the identity information especially being specific to the software client application instance
15 or to the combination of the software client application instance and the client computing device,

wherein in a fourth step, subsequent to the first step and prior to the second step, a trusted entity, having a further private cryptographic key, is used as certification authority such that a combination of, on the one hand, the identity information of the software client
20 application instance, and, on the other hand, the specific public cryptographic key, is cryptographically signed using the further private cryptographic key of the trusted entity and thereby a client application certificate information obtained, the client application certificate information being specific to the software client application instance, wherein during the second step,

25 -- the client application certificate information is additionally transmitted to the client computing device using the first secure communication channel, and furthermore
-- at least one out of the group comprising the identity information, the mutual assignment of the specific public cryptographic key to the identity information, and the client application certificate information is transmitted to the third party server entity using
30 the second secure communication channel.

[0025] By means of using the unique identity information that is assigned to the software client application instance and by using a client application certificate information, it is advantageously possible, according to the present invention, to both identify each software client application instance distributed by the application distribution
35 entity and furthermore to achieve a higher level of authentication as the client application certificate information is obtained using a cryptographic signature operation (typically

performed on a piece of data, such as both the identity information and the specific public cryptographic key itself or the result of a hashing operation performed on the identity information and the specific public cryptographic key (i.e. applying a hash operation to the combination of the identity information and the specific public cryptographic key)) using
5 the further private cryptographic key to produce a digital signature of the combination of the identity information and the specific public cryptographic key, i.e. the client application certificate information; this means that thereafter, it is possible to verify this signature (i.e. the client application certificate information) by performing a cryptographic operation with the specific public key on the signature obtained (i.e. the client application certificate
10 information) with the (further) public cryptographic key of the trusted entity (and, if applicable, applying the hashing operation prior to this decryption operation). The further private cryptographic key is the private cryptographic key of the trusted entity used as certification authority, i.e. the trusted entity generates the client application certificate information. Hence, according to a fifth variant of the present invention, the client
15 application certificate information is additionally transmitted to the client computing device using the first secure communication channel (i.e. the client application certificate information is transmitted additionally to the software client application instance as well as the specific private cryptographic key. Furthermore, according to a sixth variant of the present invention, the client application certificate information is additionally transmitted to
20 the client computing device using the first secure communication channel (i.e. the client application certificate information is transmitted additionally to the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key). According to both the fifth and sixth variant of the present invention, at least one out of the group comprising the identity information, the mutual
25 assignment of the specific public cryptographic key to the identity information, and the client application certificate information is (or are) transmitted to the third party server entity using the second secure communication channel.

[0026] According to a further sub-variant of the first, second, third, fourth, fifth or sixth variant, a server certificate is additionally transmitted to the client computing device, using
30 the first secure communication channel.

[0027] According to a further embodiment of the present invention, at least one out of the following (but in any case comprising the specific private cryptographic key):
-- the specific private cryptographic key,
-- the specific public cryptographic key,
35 -- the identity information,
-- the client application certificate information,

- a server certificate,
(i.e. additional pieces of information) is transmitted to the client computing device, using the first secure communication channel,
- either separately from the software client application instance,
- 5 -- or while transmitting the software client application instance, especially as a part of an application instance package, comprising additionally (to the additional pieces of information) the software client application instance.

[0028] Thereby, it is advantageously possible according to the present invention that different possibilities can be used for transmitting the whole of the software client application instance on the one hand, and the additional pieces of information (such as the specific private and/or public cryptographic key, the identity information, the client application certificate information and/or the server certificate) on the other hand, to the client computing device using the first secure communication channel. According to the present invention, at least the additional pieces of information provide for an individualization of the software client application instance (i.e. as related to the specific client computing device and/or as related to a specific user of the client computing device). The software client application instance itself (i.e. without the additional pieces of information) might be (but does not need to be) provided in an un-individualized manner, i.e. being related to an information content representing, e.g., code executable on the client computing device, such code being, if applicable (but not necessarily), specific to the device class of the client computing device but not (individually) specific to the client computing device itself, i.e. individually to the client computing device. If the software client application instance (itself) is provided in an un-individualized manner, then the additional pieces of information provide for an individualization of the whole of the software client application instance on the one hand, and the additional pieces of information on the other hand. The whole of the software client application instance and the additional pieces of information is also called application instance package. The additional pieces of information are transmitted to the client computing device either separately from the software client application instance (e.g. as separate “files” or transmission content representing or being able to represent “files”; e.g. the software client application instance could be transmitted initially, and the (or part of the) additional pieces of information transmitted in a subsequent step or in a plurality of subsequent steps) or while transmitting the software client application instance (especially as part of the application instance package, e.g. representing one individualized “file”).

35 **[0029]** According to still a further embodiment of the present invention, in a fifth step, subsequent to the second step, client application data, generated by and/or involving the

software client application instance are transmitted, from the client computing device, to the third party server entity and/or to a further client computing device and/or to a further software client application instance.

[0030] According to a further embodiment of the present invention, in a sixth step, subsequent to the second step, the software client application instance together with at least the specific private cryptographic key is used to securely communicate with the application distribution entity and/or with the trusted entity and/or with the third party server entity and/or with a further client computing device and/or with a further software client application instance.

10 **[0031]** Thereby, it is advantageously possible to subsequently use the inventive concept of (initially) transmitting – using the first secure communication channel – at least the specific private cryptographic key to the client computing device (or to the software client application instance) in a trusted and secured manner. If the confidentiality and integrity of this transmission of at least the specific private cryptographic key, using the
15 first secure communication channel, can be relied on, any data generated and/or transmitted by the software client application instance (and received by the third party server entity and/or any other server entity or device (such as a further client computing device and/or a further software client application instance)) can be authenticated and hence its confidentiality, integrity and/or plausibility verified.

20 **[0032]** According to a further embodiment of the present invention, in the fourth step, the client application certificate information is

- generated by the trusted entity and transmitted to the application distribution entity, or
- generated by the application distribution entity, wherein especially the trusted entity is part of the application distribution entity.

25 **[0033]** According to a further embodiment of the present invention, the unique identity information is an anonymous information or a pseudonymous information or an information identifying the user of the software client application instance, and wherein – in case of the unique identity information being anonymous information – especially the unique identity information is independent from an identification of either the software
30 client application instance and/or the software client application and/or the client computing device and/or the user of the client computing device (as in this case otherwise that data might be misused to break the intended anonymity).

[0034] According to a further embodiment of the present invention, the application distribution entity is an application store, wherein especially the trusted entity is identical to the third party server entity.

[0035] Furthermore, the present invention relates to a system for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device, the system comprising the client computing device, the application distribution entity and a third party server entity,

wherein the system is configured such that a first secure communication channel is established – in view of transmitting an instance of the software client application to the client computing device – between the client computing device and the application distribution entity, and wherein a second secure communication channel is established between the application distribution entity and the third party server entity,

wherein the system is furthermore configured such that:

- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance upon it being executed by the client computing device – to the third party server entity, the asymmetric pair of cryptographic keys comprising a specific private cryptographic key and a specific public cryptographic key,

- either the software client application instance as well as the specific private cryptographic key, or the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key, is transmitted to the client computing device using the first secure communication channel,

and the specific public cryptographic key is transmitted to the third party server entity using the second secure communication channel.

[0036] By means of such a system, it is advantageously possible according to the present invention to securely (i.e. in a protected manner) transmit the secret of the specific private cryptographic key to the client computing device, and the specific public cryptographic key to the third party server entity.

[0037] Additionally, the present invention relates to an application distribution entity for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software

code of the software client application being executed by the client computing device, wherein the application distribution entity is configured such that a first secure communication channel is established – in view of transmitting an instance of the software client application to the client computing device – between the client computing
5 device and the application distribution entity, and wherein a second secure communication channel is established between the application distribution entity and a third party server entity,

wherein the application distribution entity is furthermore configured such that:

- an asymmetric pair of cryptographic keys is generated in view of subsequently
10 allowing for an authenticated transmission of data – provided by the software client application instance upon it being executed by the client computing device – to the third party server entity, the asymmetric pair of cryptographic keys comprising a specific private cryptographic key and a specific public cryptographic key,
- either the software client application instance as well as the specific private
15 cryptographic key, or the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key, is transmitted to the client computing device using the first secure communication channel, and the specific public cryptographic key is transmitted to the third party server entity using the second secure communication channel.

20 **[0038]** By means of such an application distribution entity, it is advantageously possible according to the present invention to securely (i.e. in a protected manner) transmit the secret of the specific private cryptographic key to the client computing device, and the specific public cryptographic key to the third party server entity.

[0039] Furthermore, the present invention relates to a software client application
25 instance for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software code of the software client application being executed by the client computing device,

30 wherein the software client application instance is configured such that a first secure communication channel is established – in view of transmitting an instance of the software client application to the client computing device – between the client computing device and the application distribution entity, and wherein a second secure communication channel is established between the application distribution entity and a
35 third party server entity,

wherein the software client application instance is furthermore configured such that:

-- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance upon it being executed by the client computing device – to the third party server entity, the asymmetric pair of cryptographic keys comprising a specific
5 private cryptographic key and a specific public cryptographic key,
-- either the software client application instance as well as the specific private cryptographic key, or the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key, is transmitted to the client computing device using the first secure communication channel,
10 and the specific public cryptographic key is transmitted to the third party server entity using the second secure communication channel.

[0040] By means of such a software client application instance, it is advantageously possible according to the present invention to securely (i.e. in a protected manner) transmit the secret of the specific private cryptographic key to the client computing
15 device, and the specific public cryptographic key to the third party server entity.

[0041] Additionally, the present invention relates to a client computing device for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity, in order to be transmitted, using a telecommunications network, to a client computing device in view of software
20 code of the software client application being executed by the client computing device, wherein the client computing device is configured such that a first secure communication channel is established – in view of transmitting an instance of the software client application to the client computing device – between the client computing device and the application distribution entity, and wherein a second secure communication channel is
25 established between the application distribution entity and a third party server entity, wherein the client computing device is furthermore configured such that:
-- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance upon it being executed by the client computing device – to the third
30 party server entity, the asymmetric pair of cryptographic keys comprising a specific private cryptographic key and a specific public cryptographic key,
-- either the software client application instance as well as the specific private cryptographic key, or the software client application instance as well as the specific private cryptographic key and the specific public cryptographic key, is transmitted to the
35 client computing device using the first secure communication channel,

and the specific public cryptographic key is transmitted to the third party server entity using the second secure communication channel.

[0042] By means of such a client computing device, it is advantageously possible according to the present invention to securely (i.e. in a protected manner) transmit the
5 secret of the specific private cryptographic key to the client computing device, and the specific public cryptographic key to the third party server entity.

[0043] Furthermore, the present invention relates to a program comprising a computer readable program code which, when executed on a computer or on a client computing device or as part of a software client application instance or on an application
10 distribution entity or on a trusted entity, or in part on a client computing device and/or in part as part of a software client application instance and/or in part on an application distribution entity and/or in part on a trusted entity, causes the computer and/or the client computing device and/or the software client application instance and/or the application distribution entity and/or the trusted entity to perform an inventive method.

15 **[0044]** Still additionally, the present invention relates to computer program product for providing an enhanced level of authentication related to a secure software client application provided by an application distribution entity, the computer program product comprising a computer program stored on a storage medium, the computer program comprising program code which, when executed on a computer or on a client computing
20 device or as part of a software client application instance or on an application distribution entity or on a trusted entity, or in part on a client computing device and/or in part as part of a software client application instance and/or in part on an application distribution entity and/or in part on a trusted entity, causes the computer and/or the client computing device and/or the software client application instance and/or the application distribution entity
25 and/or the trusted entity to perform an inventive method.

[0045] These and other characteristics, features and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, which illustrate, by way of example, the principles of the invention. The description is given for the sake of example only, without
30 limiting the scope of the invention. The reference figures quoted below refer to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0046] Figure 1 schematically illustrates an exemplary system and situation according to the present invention where a mobile communication network – with a user
5 equipment connected to the mobile communication network – is connected to an application distribution entity, and the application distribution entity is able to exchange information with a trusted entity and/or with a third party server entity.

[0047] Figure 2 schematically illustrates a communication diagram related to a first example of the invention.

10 **[0048]** Figure 3 schematically illustrates a communication diagram related to further examples of the invention.

DETAILED DESCRIPTION

[0049] The present invention will be described with respect to particular
15 embodiments and with reference to certain drawings but the invention is not limited thereto but only by the claims. The drawings described are only schematic and are non-limiting. In the drawings, the size of some of the elements may be exaggerated and not drawn on scale for illustrative purposes.

[0050] Where an indefinite or definite article is used when referring to a singular
20 noun, e.g. “a”, “an”, “the”, this includes a plural of that noun unless something else is specifically stated.

[0051] Furthermore, the terms first, second, third and the like in the description and in the claims are used for distinguishing between similar elements and not necessarily for describing a sequential or chronological order. It is to be understood that the terms so
25 used are interchangeable under appropriate circumstances and that the embodiments of the invention described herein are capable of operation in other sequences than described or illustrated herein.

[0052] In Figure 1, a system for realizing the present invention is schematically shown, the system comprising a telecommunications network 100, especially a mobile
30 communication network 100, and especially a public land mobile network 100. The

telecommunications network 100 is connected to a user equipment 20 that is also referred to as a client computing device 20. The system furthermore also comprises an application distribution entity 200, a trusted entity 300, and a third party server entity 400.

[0053] According to the present invention, a software client application instance 121 is transmitted to the client computing device 20, i.e. after this transmission, the client computing device 20 comprises the software client application instance 121. According to a preferred embodiment of the present invention, a client application certificate information 321 is transmitted to the client computing device 20; this specifically represented in Figure 1.

10 **[0054]** According to the present invention, the communication between the client computing device 20 and the third party server entity 400 is to be secured by means of not only relying on the use of a (comparatively high level) server certificate but also using a kind of (comparatively high level) client certificate. According to the present invention, the third party server entity 400 corresponds, e.g., to an application server, i.e. providing
15 the server component of the software client application (instance) on the client computing device 20.

[0055] In Figure 2 a communication diagram relating to a first example of the present invention is schematically represented. The communication diagram involves the client computing device 20, the application distribution entity 200, the trusted entity 300 and the
20 third party server entity 400. In a first processing step 201, a request is transmitted from the client computing device 20 to the application distribution entity 200 to transmit a software client application, i.e. to install the software client application on the client computing device 20. The application distribution entity 200 typically distributes a multitude of different software client applications to a multitude of different client
25 computing devices, e.g. as an app store or the like. Hence, an instance of the software client application, i.e. a software client application instance, is able to be provided by the application distribution entity 200. In a second processing step 202, the application distribution entity 200 requests, from the trusted entity 300, to generate a pair of cryptographic keys, comprising a specific private cryptographic key 222 and a specific
30 public cryptographic key 223. After the trusted entity 300 has generated the pair of cryptographic keys 222, 223 (corresponding to the first step of the inventive method), these are transmitted to the application distribution entity 200 in a third processing step 203. In a fourth processing step 204, the software client application instance 121 and the specific private cryptographic key 222 is transmitted to the client computing device 20,
35 especially as an application instance package 121', and in a fifth processing step 205, the

specific public cryptographic key 223 is transmitted to the third party server entity 400 (thereby realizing the second step of the inventive method).

[0056] In Figure 3 a communication diagram relating to further examples of the invention is schematically shown. The communication diagram again involves the client 5 computing device 20, the application distribution entity 200, the trusted entity 300 and the third party server entity 400. Again, in a first processing step 201, a request is transmitted from the client computing device 20 to the application distribution entity 200 to transmit a software client application, i.e. to install the software client application on the client computing device 20. Again, an instance of the software client application, i.e. a software 10 client application instance, is able to be provided by the application distribution entity 200. In a third step of the inventive method, which can be prior to the first step, a unique identity information 221 is generated and/or assigned to an instance of the software client application to be transmitted to the requesting client computing device 20. The identity information 221 is specific to the software client application instance 121 or to the 15 combination of the software client application instance 121 and the client computing device 20. Again, in a second processing step 202, the application distribution entity 200 requests, from the trusted entity 300, to generate a pair of cryptographic keys, comprising a specific private cryptographic key 222 and a specific public cryptographic key 223, and typically transmits the identity information 221 to the trusted entity 300. In a fourth step of 20 the inventive method, subsequent to the first step and prior to the second step, the trusted entity 300, having a further private cryptographic key 322, is used as certification authority such that a combination of, on the one hand, the identity information 221 of the software client application instance 121, and, on the other hand, the specific public cryptographic key 223, is cryptographically signed using the further private cryptographic 25 key 322 of the trusted entity 300 and thereby a client application certificate information 321 obtained, wherein the client application certificate information 321 is specific to the software client application instance 121. Optionally, a server certificate 423 of the third party server entity 400 is transmitted to the trusted entity 300. After the trusted entity 300 has generated the pair of cryptographic keys 222, 223 (corresponding to the first step of 30 the inventive method) and the client application certificate information 321, these are transmitted to the application distribution entity 200 in a third processing step 203. Likewise also with regard to Figure 3, in a fourth processing step 204,

- the software client application instance 121 and the specific private cryptographic key 222, or
- 35 -- the software client application instance 121 and the identity information 221 and the specific private cryptographic key 222, or

-- the software client application instance 121 and the client application certificate information 321 and the specific private cryptographic key 222, or

-- the software client application instance 121 and the client application certificate information 321 and the specific private cryptographic key 222 and the server certificate 5 423, or

-- the software client application instance 121 and the client application certificate information 321 and the identity information 221 and the specific private cryptographic key 222 and the server certificate 423,

is (or are) transmitted to the client computing device 20, especially as an application 10 instance package 121', and in a fifth processing step 205,

-- the specific public cryptographic key 223, or

-- the client application certificate information 321, or

-- the identity information 221 and the specific public cryptographic key 223, or

-- the specific public cryptographic key 223 and the client application certificate 15 information 321, or

-- the identity information 221 and the specific public cryptographic key 223 and the client application certificate information 321

is (or are) transmitted to the third party server entity 400 (thereby realizing the second step of the inventive method).

20 **[0057]** Both in case of Figure 2 as in case of Figure 3, after having performed the second step, a data transmission path is available between the client computing device 20 and the third party server entity 400 such that especially data transmitted from the client computing device 20 towards the third party server entity 400 are able to be authenticated by the third party server entity 400 and such that the integrity of such data 25 transmitted is protected during the transmission. This is represented in both figures by means of a dashed arrow on the bottom part of the communication diagram. According to the present invention, it is additionally possible to encrypt such data exchanged between the client computing device 20 and the third party server entity 400.

[0058] According to the present invention, it is especially advantageous that for the 30 transmission of the specific private cryptographic key 222 the first secure communication channel is used, i.e. the secure communication channel that is also used, by the application distribution entity 200, to distribute the software client applications (i.e. the software client application instances). Thereby, it is possible that the integrity and confidentiality of the data transmitted can be assured. Additionally, mechanisms of the 35 application distribution entity 200 (i.e. of the app store), can assure that only one copy of an app (i.e. one software client application instance) can be downloaded to any client

computing device, and, hence, also to the client computing device 20; thereby it is advantageously possible that the application distribution entity 200 prevents an attacker from using a valid client certificate that could potentially be non-manually (i.e. by a robot) requested and used in a manipulated software client application instance.

5 **[0059]** As mentioned above, an additional step according to the method of the present invention might consist of transmitting the server certificate 423 to the client computing device 20 that the software client application instance 121 might use to perform a better or more secure verification or authentication of the server side, e.g. by means of storing the server certificate, and, during verification in the context of the TLS
10 connection setup, only allowing this server certificate as a valid certificate (in an analogous manner to a certificate pinning process or protocol).

[0060] The specific implementation of the method according to the present invention might encompass to also modify the operating system of the client computing device 20, e.g. in order optimally support the steps or processing steps according to the present
15 invention and/or according to the inventive method, e.g., by means of the app installer (i.e. a component of the operating system of the client computing device 20, used to install new software client application instances) storing the additional pieces of information (i.e. the application certificate, i.e. especially the specific private cryptographic key 222, and/or the specific public cryptographic key 223 and/or the identity information
20 221 and/or the client application certificate information 321 and/or the server certificate 423 (without the private key of the server certificate 423)) at an appropriate location within the client computing device 20, e.g. private keys in an iOS keychain and/or by means of using the Android API (application programming interface) of the keychain.

PATENT CLAIMS

1. Method for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity (200), in order to be transmitted, using a telecommunications network (100), to a client computing device (20) in view of software code of the software client application being executed by the client computing device (20), wherein a first secure communication channel (251) is established – in view of transmitting an instance (121) of the software client application to the client computing device (20) – between the client computing device (20) and the application distribution entity (200), and wherein a second secure communication channel (252) is established between the application distribution entity (200) and a third party server entity (400), wherein the method comprises the following steps:
- in a first step, an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance (121) upon it being executed by the client computing device (20) – to the third party server entity (400), the asymmetric pair of cryptographic keys comprising a specific private cryptographic key (222) and a specific public cryptographic key (223),
 - in a second step, subsequent to the first step,
 - the software client application instance (121) as well as the specific private cryptographic key (222), or
 - the software client application instance (121) as well as the specific private cryptographic key (222) and the specific public cryptographic key (223),is transmitted to the client computing device (20) using the first secure communication channel (251), and the specific public cryptographic key (223) is transmitted to the third party server entity (400) using the second secure communication channel (252).
2. Method according to claim 1, wherein in a third step, which can be prior to the first step, a unique identity information (221) is assigned to the software client application instance (121), the identity information (221) being specific to the software client application instance (121) or to the combination of the software client application instance (121) and the client computing device (20), wherein during the second step,

-- the identity information (221) is additionally transmitted to the client computing device (20) using the first secure communication channel (251), and furthermore
-- the identity information (221) or the mutual assignment of the specific public cryptographic key (223) to the identity information (221) is transmitted to the third party server entity (400) using the second secure communication channel (252).

3. Method according to claim 1, wherein prior to or during the first step, a unique identity information (221) is assigned to the software client application instance (121),
the identity information (221) especially being specific to the software client application instance (121) or to the combination of the software client application instance (121) and the client computing device (20),
and wherein in a fourth step, subsequent to the first step and prior to the second step, a trusted entity (300), having a further private cryptographic key (322), is used as certification authority such that a combination of, on the one hand, the identity information (221) of the software client application instance (121), and, on the other hand, the specific public cryptographic key (223), is cryptographically signed using the further private cryptographic key (322) of the trusted entity (300) and thereby a client application certificate information (321) obtained, the client application certificate information (321) being specific to the software client application instance (121),
and wherein during the second step,
-- the client application certificate information (321) is additionally transmitted to the client computing device (20) using the first secure communication channel (251), and furthermore
-- at least one out of the group comprising the identity information (221), the mutual assignment of the specific public cryptographic key (223) to the identity information (221), and the client application certificate information (321) is transmitted to the third party server entity (400) using the second secure communication channel (252).

4. Method according to one of the preceding claims, wherein at least one out of the following:
-- the specific private cryptographic key (222),
-- the specific public cryptographic key (223),
-- the identity information (221),
-- the client application certificate information (321),

- a server certificate (423),
is transmitted to the client computing device (20), using the first secure communication channel (251),
-- either separately from the software client application instance (121),
5 -- or while transmitting the software client application instance (121), especially as a part of an application instance package (121'), comprising additionally the software client application instance (121).
5. Method according to one of the preceding claims, wherein in a fifth step,
10 subsequent to the second step, client application data, generated by and/or involving the software client application instance (121) are transmitted, from the client computing device (20), to the third party server entity (400) and/or to a further client computing device (50) and/or to a further software client application instance (151).
- 15 6. Method according to one of the preceding claims, wherein in a sixth step, subsequent to the second step, the software client application instance (121) together with at least the specific private cryptographic key (222) is used to securely communicate with the application distribution entity (200) and/or with the
20 trusted entity (300) and/or with the third party server entity (400) and/or with a further client computing device (50) and/or with a further software client application instance (151).
7. Method according to one of the preceding claims, wherein in the fourth step, the
25 client application certificate information (321) is
-- generated by the trusted entity (300) and transmitted to the application distribution entity (200), or
-- generated by the application distribution entity (200), wherein especially the trusted entity (300) is part of the application distribution entity (200).
- 30 8. Method according to one of the preceding claims, wherein the unique identity information (221) is an anonymous information or a pseudonymous information or an information identifying the user of the software client application instance (121), and wherein – in case of the unique identity information (221) being
35 anonymous information – especially the unique identity information (221) is independent from an identification of either the software client application instance (121) and/or the software client application and/or the client computing device (20)

and/or the user of the client computing device (20).

9. Method according to one of the preceding claims, wherein the application distribution entity (200) is an application store, wherein especially the trusted
5 entity is identical to the third party server entity (400).
10. System for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity (200), in order to be transmitted, using a telecommunications network (100), to a
10 client computing device (20) in view of software code of the software client application being executed by the client computing device (20), the system comprising the client computing device (20), the application distribution entity (200) and a third party server entity (400), wherein the system is configured such that a first secure communication channel (251) is established – in view of transmitting an instance (121) of the software
15 client application to the client computing device (20) – between the client computing device (20) and the application distribution entity (200), and wherein a second secure communication channel (252) is established between the application distribution entity (200) and the third party server entity (400), wherein the system is furthermore configured such that:
20 -- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance (121) upon it being executed by the client computing device (20) – to the third party server entity (400), the asymmetric pair of
25 cryptographic keys comprising a specific private cryptographic key (222) and a specific public cryptographic key (223),
-- either the software client application instance (121) as well as the specific private cryptographic key (222), or the software client application instance (121) as well as the specific private cryptographic key (222) and the specific public
30 cryptographic key (223), is transmitted to the client computing device (20) using the first secure communication channel (251), and the specific public cryptographic key (223) is transmitted to the third party server entity (400) using the second secure communication channel (252).
- 35 11. Application distribution entity (200) for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity (200), in order to be transmitted, using a

telecommunications network (100), to a client computing device (20) in view of software code of the software client application being executed by the client computing device (20),

wherein the application distribution entity (200) is configured such that a first
5 secure communication channel (251) is established – in view of transmitting an instance (121) of the software client application to the client computing device (20) – between the client computing device (20) and the application distribution entity (200), and wherein a second secure communication channel (252) is established between the application distribution entity (200) and a third party server entity
10 (400),

wherein the application distribution entity (200) is furthermore configured such that:

-- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software
15 client application instance (121) upon it being executed by the client computing device (20) – to the third party server entity (400), the asymmetric pair of cryptographic keys comprising a specific private cryptographic key (222) and a specific public cryptographic key (223),

-- either the software client application instance (121) as well as the specific
20 private cryptographic key (222), or the software client application instance (121) as well as the specific private cryptographic key (222) and the specific public cryptographic key (223), is transmitted to the client computing device (20) using the first secure communication channel (251), and the specific public cryptographic key (223) is transmitted to the third party server entity (400) using
25 the second secure communication channel (252).

12. Software client application instance (121) for providing an enhanced level of authentication related to a secure software client application that is provided, by an application distribution entity (200), in order to be transmitted, using a
30 telecommunications network (100), to a client computing device (20) in view of software code of the software client application being executed by the client computing device (20),

wherein the software client application instance (121) is configured such that a first secure communication channel (251) is established – in view of transmitting
35 an instance (121) of the software client application to the client computing device (20) – between the client computing device (20) and the application distribution entity (200), and wherein a second secure communication channel (252) is

established between the application distribution entity (200) and a third party server entity (400),

wherein the software client application instance (121) is furthermore configured such that:

- 5 -- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance (121) upon it being executed by the client computing device (20) – to the third party server entity (400), the asymmetric pair of cryptographic keys comprising a specific private cryptographic key (222) and a
- 10 specific public cryptographic key (223),
- either the software client application instance (121) as well as the specific private cryptographic key (222), or the software client application instance (121) as well as the specific private cryptographic key (222) and the specific public cryptographic key (223), is transmitted to the client computing device (20) using
- 15 the first secure communication channel (251), and the specific public cryptographic key (223) is transmitted to the third party server entity (400) using the second secure communication channel (252).

13. Client computing device (20) for providing an enhanced level of authentication
- 20 related to a secure software client application that is provided, by an application distribution entity (200), in order to be transmitted, using a telecommunications network (100), to a client computing device (20) in view of software code of the software client application being executed by the client computing device (20), wherein the client computing device (20) is configured such that a first secure
- 25 communication channel (251) is established – in view of transmitting an instance (121) of the software client application to the client computing device (20) – between the client computing device (20) and the application distribution entity (200), and wherein a second secure communication channel (252) is established between the application distribution entity (200) and a third party server entity
- 30 (400),
- wherein the client computing device (20) is furthermore configured such that:
- an asymmetric pair of cryptographic keys is generated in view of subsequently allowing for an authenticated transmission of data – provided by the software client application instance (121) upon it being executed by the client computing
- 35 device (20) – to the third party server entity (400), the asymmetric pair of cryptographic keys comprising a specific private cryptographic key (222) and a specific public cryptographic key (223),

-- either the software client application instance (121) as well as the specific private cryptographic key (222), or the software client application instance (121) as well as the specific private cryptographic key (222) and the specific public cryptographic key (223), is transmitted to the client computing device (20) using the first secure communication channel (251), and the specific public cryptographic key (223) is transmitted to the third party server entity (400) using the second secure communication channel (252).

14. Program comprising a computer readable program code which, when executed on a computer or on a client computing device (20) or as part of a software client application instance (121) or on an application distribution entity (200) or on a trusted entity (300), or in part on a client computing device (20) and/or in part as part of a software client application instance (121) and/or in part on an application distribution entity (200) and/or in part on a trusted entity (300), causes the computer and/or the client computing device (20) and/or the software client application instance (121) and/or the application distribution entity (200) and/or the trusted entity (300) to perform a method according one of claims 1 to 9.

15. Computer program product for providing an enhanced level of authentication related to a secure software client application provided by an application distribution entity (200), the computer program product comprising a computer program stored on a storage medium, the computer program comprising program code which, when executed on a computer or on a client computing device (20) or as part of a software client application instance (121) or on an application distribution entity (200) or on a trusted entity (300), or in part on a client computing device (20) and/or in part as part of a software client application instance (121) and/or in part on an application distribution entity (200) and/or in part on a trusted entity (300), causes the computer and/or the client computing device (20) and/or the software client application instance (121) and/or the application distribution entity (200) and/or the trusted entity (300) to perform a method according one of claims 1 to 9.

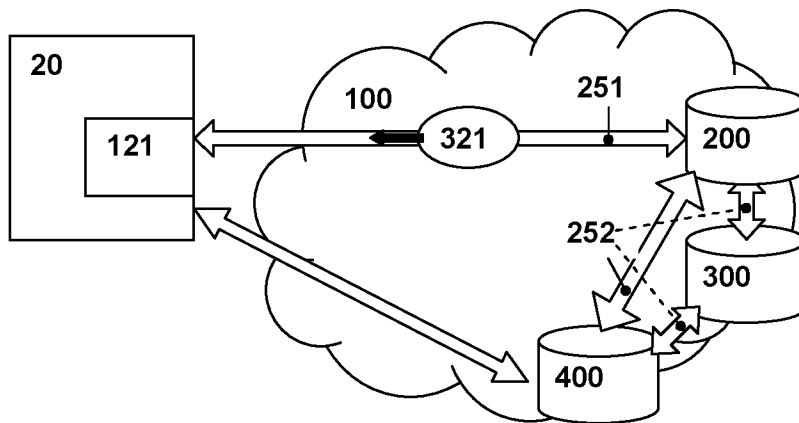


Fig. 1

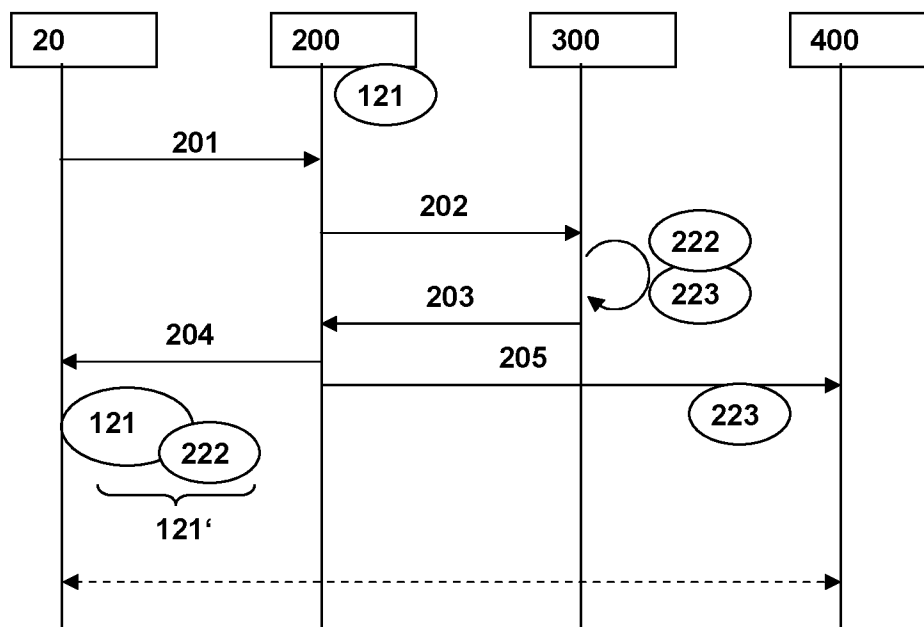


Fig. 2

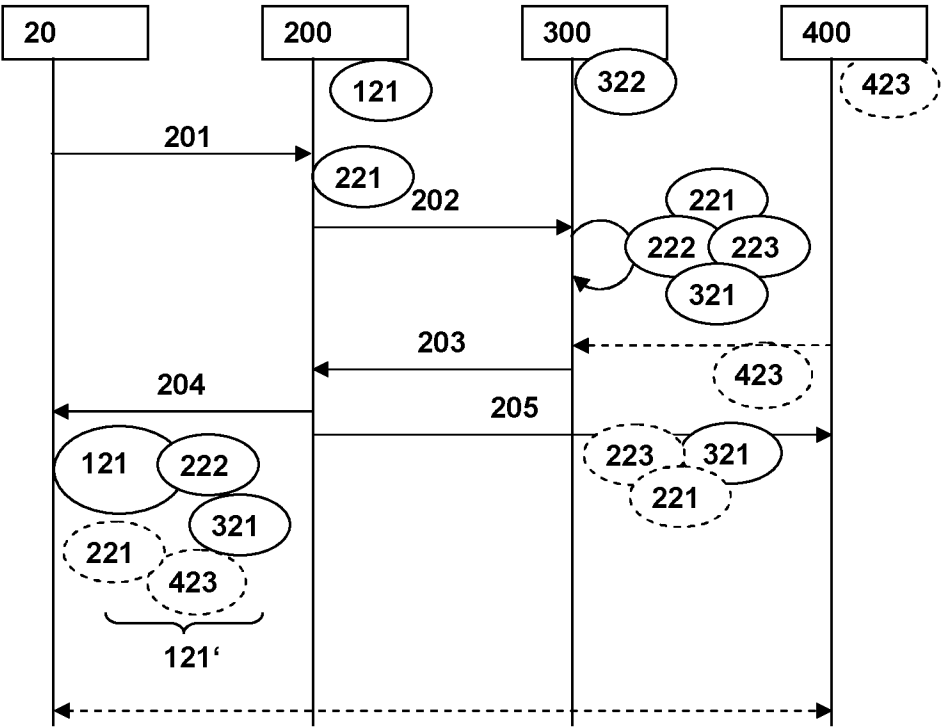


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/065931

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/33
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

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 8 312 518 B1 (EZELL JOEL M [US] ET AL) 13 November 2012 (2012-11-13) column 6 - column 12	1-15
X	US 2005/154889 A1 (ASHLEY PAUL A [AU] ET AL) 14 July 2005 (2005-07-14) paragraph [0016] - paragraph [0054]	1-15
X	WO 2016/019106 A1 (NOK NOK LABS INC [US]) 4 February 2016 (2016-02-04) paragraph [0020] - paragraph [0070]	1-15
X	US 2006/195689 A1 (BLECKEN CARSTEN [US] ET AL) 31 August 2006 (2006-08-31) paragraph [0031] - paragraph [0059]	1-15
	----- -/-	



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

8 September 2017

Date of mailing of the international search report

22/09/2017

Name and mailing address of the ISA/

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

Authorized officer

Jascou, Adrian

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/065931

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 748 528 B1 (GREENFIELD JONATHAN SCOTT [US]) 8 June 2004 (2004-06-08) column 5 - column 9 -----	1-15
X	US 2006/075242 A1 (AISSI SELIM [US] ET AL) 6 April 2006 (2006-04-06) abstract; figure 2 -----	1-15
X	US 2005/027871 A1 (BRADLEY WILLIAM [US] ET AL) 3 February 2005 (2005-02-03) abstract; figure 3 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/065931

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8312518	B1	13-11-2012	NONE
US 2005154889	A1	14-07-2005	AT 367025 T 15-08-2007 CN 1906886 A 31-01-2007 DE 602005001613 T2 10-04-2008 EP 1714422 A1 25-10-2006 JP 4600851 B2 22-12-2010 JP 2007518324 A 05-07-2007 KR 20060123465 A 01-12-2006 US 2005154889 A1 14-07-2005 WO 2005069531 A1 28-07-2005
WO 2016019106	A1	04-02-2016	CN 106664208 A 10-05-2017 EP 3175578 A1 07-06-2017 KR 20170041729 A 17-04-2017 US 2016219043 A1 28-07-2016 WO 2016019106 A1 04-02-2016
US 2006195689	A1	31-08-2006	EP 1859564 A2 28-11-2007 JP 2008532419 A 14-08-2008 US 2006195689 A1 31-08-2006 WO 2006093561 A2 08-09-2006
US 6748528	B1	08-06-2004	NONE
US 2006075242	A1	06-04-2006	CN 101032126 A 05-09-2007 DE 112005002362 T5 30-08-2007 GB 2433003 A 06-06-2007 JP 4792037 B2 12-10-2011 JP 2008515357 A 08-05-2008 KR 20070046966 A 03-05-2007 US 2006075242 A1 06-04-2006 US 2016192198 A1 30-06-2016 WO 2006039616 A1 13-04-2006
US 2005027871	A1	03-02-2005	AU 2004264582 A1 24-02-2005 AU 2010212301 A1 02-09-2010 BR PI0410999 A 04-07-2006 CA 2528428 A1 24-02-2005 CA 2776354 A1 24-02-2005 CN 1860761 A 08-11-2006 CN 103001923 A 27-03-2013 EA 200501896 A1 30-06-2006 EA 200700510 A1 28-12-2007 EP 1629363 A2 01-03-2006 EP 2270622 A2 05-01-2011 EP 2280524 A2 02-02-2011 IL 172366 A 31-01-2013 IL 223027 A 29-01-2015 JP 5059577 B2 24-10-2012 JP 5242915 B2 24-07-2013 JP 5731679 B2 10-06-2015 JP 2007526526 A 13-09-2007 JP 2008140399 A 19-06-2008 JP 2012053913 A 15-03-2012 JP 2014146345 A 14-08-2014 KR 20060054192 A 22-05-2006 KR 20080058459 A 25-06-2008

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/065931

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		KR 20100058634 A	03-06-2010
		KR 20100136533 A	28-12-2010
		SG 155065 A1	30-09-2009
		US 9466054 B1	11-10-2016
		US 2005027871 A1	03-02-2005
		US 2007283423 A1	06-12-2007
		US 2008056500 A1	06-03-2008
		US 2008133731 A1	05-06-2008
		US 2008140835 A1	12-06-2008
		US 2008285757 A1	20-11-2008
		US 2008298591 A1	04-12-2008
		US 2008301430 A1	04-12-2008
		US 2009094453 A1	09-04-2009
		US 2010005513 A1	07-01-2010
		US 2010017606 A1	21-01-2010
		US 2010067699 A1	18-03-2010
		US 2010070774 A1	18-03-2010
		US 2010131412 A1	27-05-2010
		US 2010241849 A1	23-09-2010
		US 2010250927 A1	30-09-2010
		US 2010313038 A1	09-12-2010
		US 2012042389 A1	16-02-2012
		US 2012159642 A1	21-06-2012
		US 2012159643 A1	21-06-2012
		US 2017163645 A1	08-06-2017
		WO 2005017654 A2	24-02-2005
