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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2019 (24.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/017883 A1

(51) International Patent Classification:
G06F 21/62 (2013.01) *H04L 9/14* (2006.01)

(21) International Application Number:
PCT/US2017/042412

(22) International Filing Date:
17 July 2017 (17.07.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventors: **SCHIFFMAN, Joshua S**; HP Inc., Long Down Ave, Stoke Gifford, Bristol, Bristol BS34 8QZ (GB). **MATHER, Luke T.**; 9 Whatley Road, Bristol, Bristol BS8 2PS (GB). **MOHMAN, Christopher C**; 11445 Compaq Center Dr W, Houston, Texas 77070 (US).

(74) Agent: **BURROWS, Sarah** et al.; HP Inc, 3390 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

(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, 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.

(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).

Declarations under Rule 4.17:
— *as to the identity of the inventor (Rule 4.17(i))*

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

(54) Title: AUTHENTICATION OF ENTITLEMENT CERTIFICATES

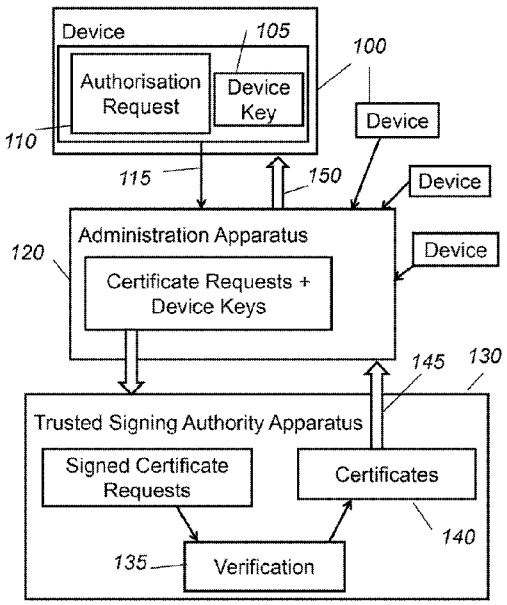


Figure 1

(57) Abstract: A method for providing a set of certificates encoding authorisations, the method comprising processing respective ones of multiple authorisation requests at a trusted signing authority apparatus to verify respective digital signatures applied to the requests, the multiple authorisation requests received over a first communication link between the trusted signing authority apparatus and an administration apparatus, validating one or more authorisation request parameters of respective ones of the authorisation requests, generating a certificate encoding an authorisation at the trusted signing authority apparatus and transmitting the generated certificate to the administration apparatus or a requesting apparatus over a second communication fink.

WO 2019/017883 A1

AUTHENTICATION OF ENTITLEMENT CERTIFICATES

BACKGROUND

[0001] In a device to device (D2D) computing environment such as a smart office or home, users or administrators can authorise a set of actions that devices can perform based on user or device policy that dictates the actions such authorisations confer. A service provider device can contact a signing authority to authorise and produce an authentication certificate. The service provider device can access a policy decision point using, for example, an online connection to an infrastructure portal to use authorisation encoding.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Various features of certain examples will be apparent from the detailed description which follows, taken in conjunction with the accompanying drawings, which together illustrate, by way of example only, a number of features, and wherein:

[0003] Figure 1 shows an apparatus for providing a set of certificates that encode authorisations according to an example;

[0004] Figure 2 shows a flow chart of a method for providing a set of certificates that encode authorisations according to an example; and

[0005] Figure 3 shows an apparatus according to an example.

DETAILED DESCRIPTION

[0006] In the following description, for purposes of explanation, numerous specific details of certain examples are set forth. Reference in the specification to "an example" or similar language means that a particular feature, structure, or characteristic described in connection with the example is included in at least that one example, but not necessarily in other examples.

[0007] According to an example, there is provided a method for an entitlement signing workflow to enable an administration device to collect multiple authorisation requests from devices wishing to use certain services or perform certain actions. That is, the administration device can collect multiple requests from devices wishing to obtain permission or authorization to use certain services or perform certain actions. Accordingly, certificates that encode these authorizations can be provided. The requesting device need not have a persistent connection to an infrastructure as the certificate that encodes the permissions for the device can be requested and delivered by way of an administration apparatus that can act as an effective broker between the requesting device and a trusted certificate generating apparatus.

[0008] Therefore, according to an example, authorisation rights or permissions can be encoded in a certificate. The requests for authorisation are tied to an identity of a device through a digital signature. This is done by signing the request with the private key of a device's public key pair. It can then be forwarded from the administration device to a signing authority in a single set.

[0009] In an example, the signed requests and their contents, which can be authorisation request parameters defining the scope of an authorisation request, can be authenticated and certificates encoding one or more permissions generated for the devices. The certificates can be transmitted to the devices using a different communication path to the one used to deliver the requests to the signing authority (which itself need not be secure as a result of the initial request signing). For example, a request can be made using a low energy radio frequency communication protocol, and delivery of a certificate can be by made using a different radio frequency communication protocol such as WiFi for example. Alternatively, either or both of the request and delivery pathways can use other wireless and/or hardwired communication protocols or methods, near field communication and so on.

[0010] In an example, an authorisation request parameter can provide an indication of the device's desired entitlement to use a service. For example, a parameter can indicate whether read and/or write access to a service is requested, or if a device requests access to or use of a particular node in a network and so on.

[0011] Devices that wish to generate authorisation signing requests (ASR), for use in a protocol using access control under a trusted third-party authority can leverage their pre-existing authenticated identity to sign their requests. These requests can be transferred using any means (manually, over peer-to-peer networks, or over an infrastructure LAN or WLAN connection for example) to a signing authority. The authority can produce signed entitlements and these can be returned to the requesting devices.

[0012] The disclosed method for provisioning devices with certificates means that a device does not have to have an online connection to an infrastructure portal. The methods are suitable even when a device, or a set of many devices, require signed entitlements and are not in a position to directly connect to a signing authority.

[0013] The method can be used in scenarios where a service provider device does not have persistent access to a policy decision point, since the device can still benefit from authorization encoding. The process of generating the certificates encoding permissions uses an administration apparatus as an intermediary to enable a device to indirectly make contact with a signing authority.

[0014] In an example, an authorized administrator's device can be used to collect requests from devices and forward the requests to a signing authority. Certificates encoding the permissions that were requested by the device can be generated by the signing authority, and the resulting certificates can then be returned to the requesting devices over a channel, which may or may not be the same as the channel over which the requests were initially communicated.

[0015] Figure 1 is a schematic representation of an apparatus for providing a set of certificates encoding one or more authorisations or permissions according to an example. Devices 100 have pre-existing identity certificates that have been signed by a trusted third-party authority. The certificates contains a unique verification key or device key 105 associated with a corresponding signing key. When a device wishes to request an authorisation 110, it generates an authorisation request and signs the request with its private signing key. Thus, the request can no longer be modified without detection by the authority. This

allows the request to be transported 115 via an administration apparatus 120 to a trusted signing authority 130 using any means since no security requirements need to be placed on the transport mechanism. The requests can take any route from the requesting device to the authority.

[0016] When the authority 130 receives a request it verifies 135 the correctness of the signature as well as whether the authorisation(s) requested are acceptable. For example, the authority 130 can determine whether a requested authorisation accords with a set of allowable permissions for the device that may be preconfigured at the authority 130 and which may be periodically updated.

[0017] If both checks pass, the authority generates a certificate 140 encoding the or each requested authorisation. This certificate can be transported 145, 150 via the administration apparatus 120 back to the requesting device 100 using any transport method.

[0018] Upon receiving the certificate, the requesting device verifies the authority's signature within the certificate and whether the authorisations signed were those requested. If all checks pass, the device has been successfully provisioned with authorisations.

[0019] Figure 2 shows a flow chart of a method for providing a set of certificates according to an example. At block 200 the trusted signing authority apparatus receives a request for authorisation to use or access a service or apparatus (e.g. a printer or network node) via the administration apparatus from the one or more devices. At block 210 the authority verifies the digital signatures applied to the requests. At block 220 one or more request parameters are validated. At block 230 the authority generates the certificates encoding the authorisations for each respective request from the one or more devices. At block 240 the certificates are transmitted via the administration apparatus back to the one or more devices that made the respective requests.

[0020] In an example, the method for providing a set of certificates encoding authorisations uses an administrator device provisioned with authorisations that allow it to read and write to a security policy held by a participating device.

These administrator devices can be mobile devices, such as phones and tablets, and can communicate with targets using a protocol such as Bluetooth Low Energy for example, which is a low energy radio frequency communication protocol. The mobile devices may not always have an infrastructure connection available to an administrator portal. Accordingly, using pre-existing authenticated device identities, these devices can generate temporary requests offline. These requests can be collected by, for example, an administrator and transported on foot to an infrastructure connected portal. This portal can then complete the remainder of the process.

[0021] According to an example, the method enables a set of requests to be collated and delivered to a signing authority in a single batch. Thus, only one member of an IT department, for example, may need to walk to an infrastructure connected machine. This is useful in a whole raft of office-of-the-future use cases. It enables a low-effort and seamless workflow for generating and authenticating short-lived entitlements for use in device administration, access and authorization protocols. The method also allows for any transport protocol or method to be used to generate an entitlement signing request and a corresponding certificate. This includes a sneakernet approach (that is, the transfer of electronic information by physically moving media comprising the information, such as magnetic tape, flash drives or external hard drives and so on, from one device to another), which in turn enables a bulk collection and collation of requests that can be ferried to an authority in one go.

[0022] The method is suitable for deployment over a variety of different transport protocols, ranging from full infrastructure communication protocols, to peer-to-peer protocols, to manual transport on a physical device.

[0023] Examples in the present disclosure can be provided as methods, systems or machine-readable instructions. Such machine-readable instructions may be included on a computer readable storage medium (including but not limited to disc storage, CD-ROM, optical storage, etc.) having computer readable program codes therein or thereon.

[0024] The present disclosure is described with reference to flow charts and/or block diagrams of the method, devices and systems according to examples of

the present disclosure. Although the flow diagrams described above show a specific order of execution, the order of execution may differ from that which is depicted. Blocks described in relation to one flow chart may be combined with those of another flow chart. In some examples, some blocks of the flow diagrams may not be necessary and/or additional blocks may be added. It shall be understood that each flow and/or block in the flow charts and/or block diagrams, as well as combinations of the flows and/or diagrams in the flow charts and/or block diagrams can be realized by machine readable instructions.

[0025] The machine-readable instructions may, for example, be executed by a device, an administration apparatus, a trusted signing authority apparatus, a general-purpose computer, a special purpose computer, an embedded processor or processors of other programmable data processing devices to realize the functions described in the description and diagrams. In particular, a processor or processing apparatus may execute the machine-readable instructions. Thus, modules of the administration apparatus or trusted signing authority apparatus may be implemented by a processor executing machine readable instructions stored in a memory, or a processor operating in accordance with instructions embedded in logic circuitry. The term 'processor' is to be interpreted broadly to include a CPU, processing unit, ASIC, logic unit, or programmable gate set etc. The methods and modules may all be performed by a single processor or divided amongst several processors.

[0026] Such machine-readable instructions may also be stored in a computer readable storage that can guide the computer or other programmable data processing devices to operate in a specific mode.

[0027] For example, the instructions may be provided on a non-transitory computer readable storage medium encoded with instructions, executable by a processor.

[0028] Figure 3 shows an example of an apparatus comprising a processor 350 associated with a memory 352. The memory 352 comprises computer readable instructions 354 which are executable by the processor 350. The instructions 354 comprise:

Instructions to receive requests;

Instruction to verify digital signatures applied to the requests by the devices;

Instructions to validate one or more request parameter(s);

Instructions to generate certificates; and

Instructions to transmit certificates.

[0029] Such machine-readable instructions may also be loaded onto a computer or other programmable data processing devices, so that the computer or other programmable data processing devices perform a series of operations to produce computer-implemented processing, thus the instructions executed on the computer or other programmable devices provide an operation for realizing functions specified by flow(s) in the flow charts and/or block(s) in the block diagrams.

[0030] Further, the teachings herein may be implemented in the form of a computer software product, the computer software product being stored in a storage medium and comprising a plurality of instructions for making a computer device implement the methods recited in the examples of the present disclosure.

[0031] While the method, apparatus and related aspects have been described with reference to certain examples, various modifications, changes, omissions, and substitutions can be made without departing from the spirit of the present disclosure. In particular, a feature or block from one example may be combined with or substituted by a feature/block of another example.

[0032] The word "comprising" does not exclude the presence of elements other than those listed in a claim, "a" or "an" does not exclude a plurality, and a single processor or other unit may fulfil the functions of several units recited in the claims.

[0033] The features of any dependent claim may be combined with the features of any of the independent claims or other dependent claims.

CLAIMS

1. A method for providing a set of certificates encoding authorisations, the method comprising:

processing respective ones of multiple authorisation requests at a trusted signing authority apparatus to verify respective digital signatures applied to the requests, the multiple authorisation requests received over a first communication link between the trusted signing authority apparatus and an administration apparatus;

validating one or more authorisation request parameters of respective ones of the authorisation requests;

generating a certificate encoding an authorisation at the trusted signing authority apparatus; and

transmitting the generated certificate to the administration apparatus or a requesting apparatus over a second communication link.

2. A method as claimed in claim 1, wherein an authorisation request parameter comprises an indication of a device's desired entitlement to use a service.

3. A method as claimed in claim 1, wherein processing respective ones of multiple authorisation requests at the trusted signing authority apparatus to verify respective digital signatures applied to the requests further comprises verifying a digital signature of an authorisation request applied to the authorisation using a private key of a device public key pair.

4. A method as claimed in claim 1, further comprising signing an identity certificate for a device.

5. A method as claimed in claim 1, further comprising collating a set of generated certificates for transmission to the administration apparatus.

6. An administration apparatus to:

receive an authorisation request from a device;

collate the authorisation request with multiple other such requests from respective other devices to form a set of authorisation requests; and

transmit the set of authorisation requests to a trusted signing authority apparatus.

7. An administration apparatus as claimed in claim 6, wherein the administration apparatus is provisioned with authorisation read and write to a security policy of a device.

8. An administration apparatus as claimed in claim 6, the administration apparatus to receive a certificate encoding an authorisation from the trusted signing authority apparatus; and

transmit the certificate to the device.

9. A device comprising a processor to:

generate an authorisation request for a certificate encoding an authorisation; and

transmit the authorisation request to an administration device.

10. A device as claimed in claim 9, the processor to:

apply a digital signature to the authorisation request using a private key of a device public key pair.

11. A device as claimed in claim 9, the device to:

receive a certificate encoding an authorisation.

12. A device as claimed in claim 11, the device to receive the certificate from the administration apparatus or a trusted signing authority apparatus.

13. A machine-readable storage medium encoded with instructions for providing a set of certificates encoding authorisations, the instructions

executable by a processor of a trusted signing authority apparatus to cause the apparatus to:

process respective ones of multiple authorisation requests to verify respective digital signatures applied to the requests, the multiple authorisation requests received over a first communication link between the trusted signing authority apparatus and an administration apparatus;

validate one or more authorisation request parameters of respective ones of the authorisation requests;

generate a certificate encoding an authorisation; and

transmit the generated certificate to the administration apparatus or a requesting apparatus over a second communication link.

14. A machine-readable storage medium encoded with instructions as claimed in claim 13, comprising instructions further executable to:

verify a digital signature of an authorisation request applied to the authorisation request using a private key of a device public key pair.

15. A machine-readable storage medium encoded with instructions as claimed in claim 13, comprising instructions further executable to:

collate a set of generated certificates for transmission to the administration apparatus.

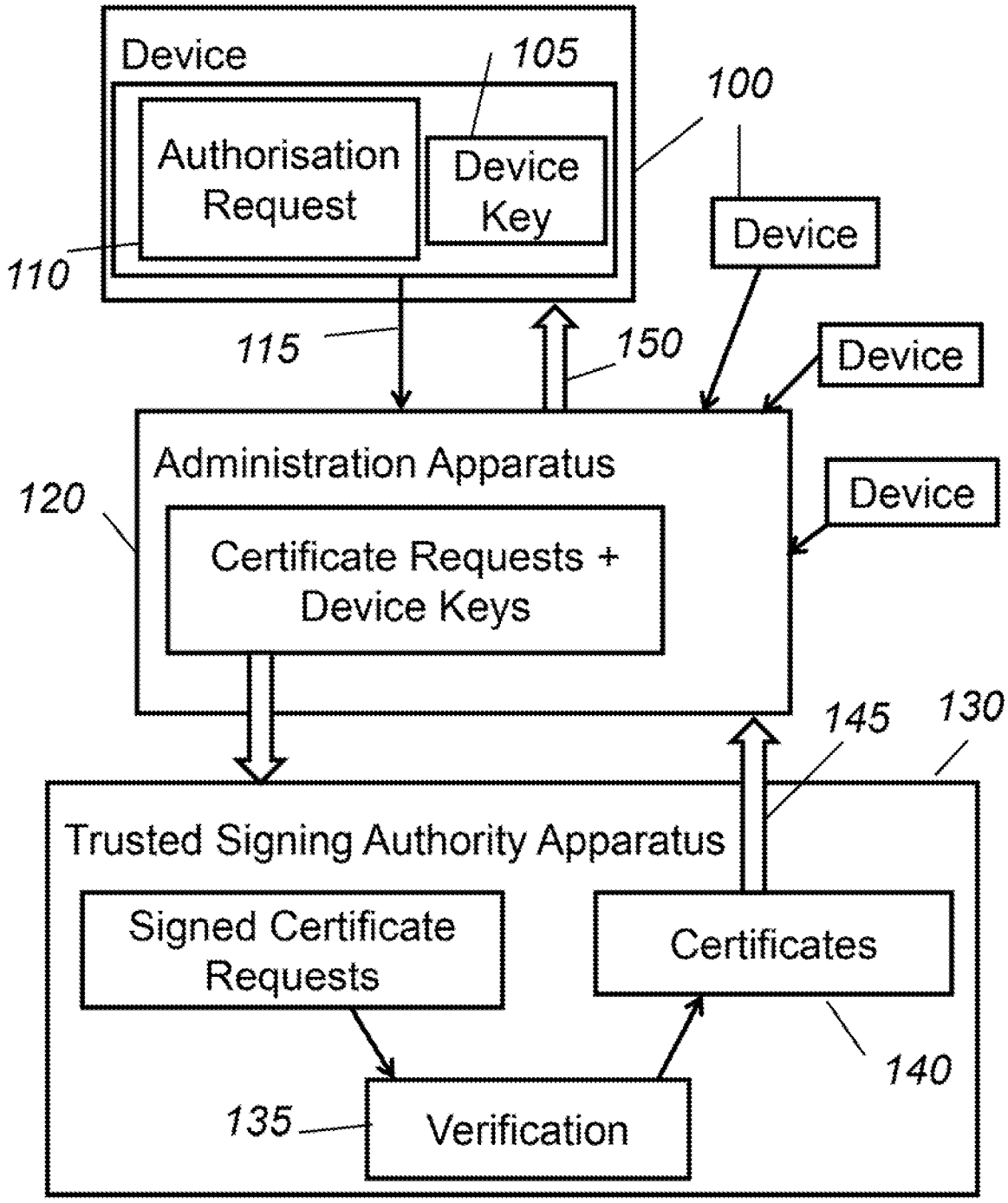

Device
105
100
Authorisation Request
Device Key
110
Device
115
150
Device
Administration Apparatus
Device
120
Certificate Requests + Device Keys
145
130
Trusted Signing Authority Apparatus
Signed Certificate Requests
Certificates
140
135
Verification

Figure 1

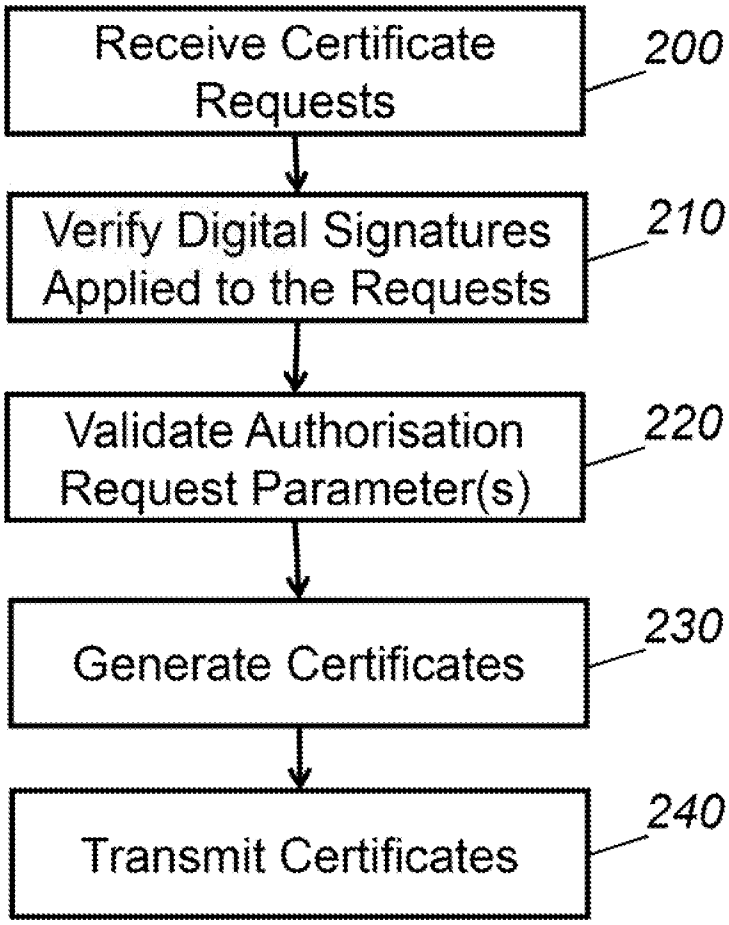


Figure 2

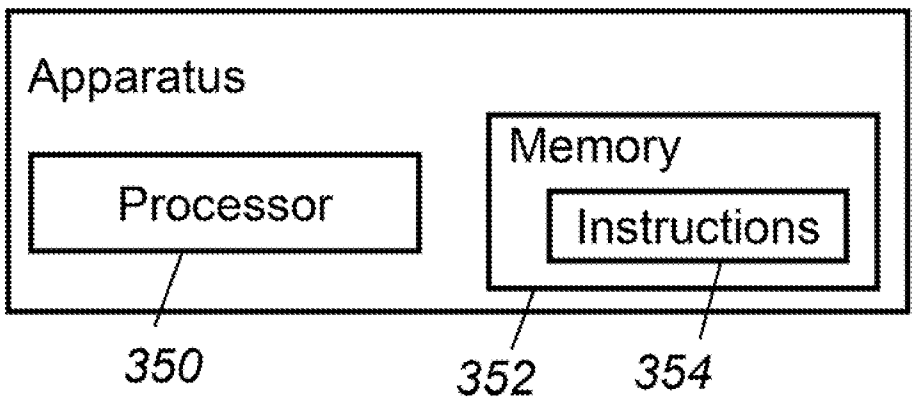


Figure 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2017/042412

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 *(2013.01)*
H04L 9/14 *(2006.01)*

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 1/00-1/32, 15/00-17/50; H04N 9/00-9/38, 13/00-13/04, 19/00-21/858; H04L 7/00-9/38, 12/00-12/955, 25/00-29/14; H04H 60/00-60/98; H04W 4/00-12/12, 40/00-48/20, 60/00-60/06, 68/00-68/12, 74/00-84/22, 92/00-99/00; H04B 1/00-1/76; H04J 3/00-3/26

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)

PatSearch (RUPTO internal), USPTO, PAJ, Esp@cenet, DWPI, EAPATIS, PATENTSCOPE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/0247055 A1 (MICROSOFT CORPORATION) 06.10.2011, abstract, [0004], [0013], [0015], [0019]-[0022], [0024], [0026], [0029]-[0033], [0035], [0038]-[0040]	1-15
A	US 2010/150353 A1 (INTERNATIONAL BUSINESS MACHINES) 17.06.2010	1-15
A	US 2004/025022 A1 (YACH DAVID P. et al.) 05.02.2004	1-15
A	US 2014/164764 A1 (RAWLLIN INTERNATIONAL INC.) 12.06.2014	1-15
A	RU 2522024 C2 (ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ЛАБОРАТОРИЯ ЭЛАНДИС») 10.07.2014	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 document but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 March 2018 (22.03.2018)	05 April 2018 (05.04.2018)

Name and mailing address of the ISA/RU:
Federal Institute of Industrial Property,
Berezhkovskaya nab., 30-1, Moscow, G-59,
GSP-3, Russia, 125993
Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37

Authorized officer

V. Zhakovich

Telephone No. 8 499 240 25 91