(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 2019/017920 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 21/46* (2013.01)

(21) International Application Number:
PCT/US2017/042641

(22) International Filing Date:
18 July 2017 (18.07.2017)

(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).

(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).

(54) Title: RENDERING APPARATUS IDENTITIES

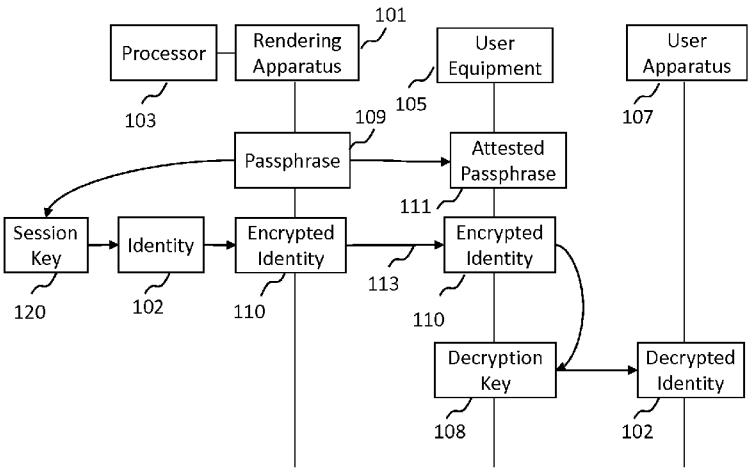

Figure 1

(57) Abstract: A method for registering the identity of a rendering apparatus, the method comprising generating a passphrase using a processor of the rendering apparatus, attesting to the validity of the passphrase at user equipment or submitting the passphrase to the user equipment, encrypting a rendering apparatus identity using a cryptographic session key agreed on the basis of the passphrase, and transferring the rendering apparatus identity from the user equipment to a user apparatus

WO 2019/017920 A1

[Continued on next page]

Declarations under Rule 4.17:

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

Published:

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

RENDERING APPARATUS IDENTITIES

BACKGROUND

[0001] An IT department can manage the identities of rendering apparatus, such as 2D and 3D printers for example, and a pull-print process exists in which a user's print job is held on a server or a user's workstation and released by the user at a printing device. Users manually enrol identities of rendering apparatus onto a workstation.

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 is a schematic representation of a method for registering the identity of a rendering apparatus according to an example;

[0004] Figure 2 is a flow chart of a method according to an example; and

[0005] Figure 3 is a schematic representation of a system 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] In, for example, a non-enterprise or infrastructure print environment or a traditional IP-based network, users may not have a way to bind the observation

of a physical rendering apparatus, such as a 2D or 3D printer, with cryptographic key material used to communicate securely with it. Also, in such an environment, users may not have an automated method for discovering a printer identity and having it available at their printing device (workstation or laptop for example). Collecting a name or IP address of a printer may not be sufficient to ensure that the printer the workstation connects to is the same one that the user found because such identifiers may not be bound to the physical printer.

[0008] According to an example, there is provided a method of using a passphrase to establish a shared key that can be deployed over a peer-to-peer or networking transport protocol to transfer an identity and address of a rendering apparatus, such as a printer, to user equipment, such as a mobile device. A user can then securely enrol that render apparatus at their workstation with a minimum of effort and with the assurance that the identity matches the physical printer they observed.

[0009] In an example, a password authenticated key exchange (PAKE) can be performed between a rendering apparatus and user equipment to agree a temporary shared key. The key can be used to transport an identity of the rendering appratus (such as a certificate, or a public key and associated metadata for example) to user equipment (UE). The UE can then transport the identity and enrol it back at the user's workstation. That is, in an example, the UE can configure parameters used for communicating with a rendering apparatus. This can include setting records in an OS, displaying UI elements, and verifying the apparatus identity.

[0010] Use of the PAKE authenticates the identity with the physical rendering appratus, as the user confirms that a passphrase displayed on the apparatus is the same as one they observe on the UE.

[0011] Figure 1 is a schematic representation of a method for registering the identity of a rendering apparatus according to an example. A passphrase 109 is generated using a processor 103 of a rendering apparatus 101. The passphrase may be an alphanumeric sequence, a sequence of letters or words or other text.

[0012] The validity of the passphrase is attested to 111 at user equipment 105 or the passphrase is submitted to user equipment 105. For example, a user may manually input the passphrase at the user equipment 105 or provide a confirmation that a passphrase provided and displayed by the user equipment 105 matches the passphrase 109, which may be displayed on a display of the rendering appratus 101.

[0013] A rendering apparatus identity 102 is encrypted using a cryptographic session key 120 agreed on the basis of the passphrase 109 to provide an encrypted rendering apparatus identity 110. The rendering apparatus identity 110 is transferred from the user equipment to a user apparatus 107, such as a workstation after having been transferred 113 from the rendering apparatus 101 to the user equipment 105. That is, the user can transport the encrypted identity to their workstation. It can be decrypted 108 using the user equipment, which has the shared session key, and the decrypted identity 102 can be transferred from the user equipment 105 to the rendering apparatus 107.

[0014] Figure 2 is a flow chart of a method according to an example. When the user wishes to enrol a printer identity at their workstation, they can perform the following steps:

[0015] In block 201, a user carries their mobile device to a printer. The user presses a button on the printer in block 203 or sends a request from their mobile device to the printer to request it to initiate a PAKE in block 203. In block 205, the printer generates a human-readable passphrase 206 and shows the password using an on-device display. In block 207, the user enters the same passphrase (or confirms that a passphrase displayed on its device is the same, depending on the particular PAKE used).

[0016] In block 209, a session key 210 is generated on the basis of the passphrase. The key may be generated using a PAKE process, such as SPAKE2 for example). In block 211, the freshly derived session 210 key is used to encrypt the printer's identity material 212 (certificate or public key and

metadata for example) to provide an encrypted version of the identity 214 which is transferred to the mobile device in block 213.

[0017] An example of the transport process is for the mobile device and printer to exchange random information to produce a session key S. The printer then encrypts the identity I using an authenticated encryption scheme like AES-GCM. This produces an encrypted identity C and an associated integrity tag, T. The printer sends C+T to the mobile device, which then validates T and decrypts C using S.

[0018] When the user returns to their workstation, they can initiate the transfer of the identity material 214 from the mobile device to their workstation in block 215. The workstation can then validate the printer's identity (e.g., certificate) against a trust CA certificate and the user can assess other attributes about the printer that are present in the identity. An example would be information about the location and capabilities of the printer. If the user is satisfied with these attributes, they can then instruct the workstation to complete the printer enrolment process. The printer is now authenticated for use from user's workstation. The PAKE can be used over any transport protocol – peer-to-peer or infrastructure.

[0019] Figure 3 is a schematic representation of a system according to an example. A rendering apparatus 301, such as a printer for example, comprises a processor 303 and a memory 305. Memory 305 stores data representing a passphrase 307 that has been agreed between the rendering apparatus 301 (or configured by a user or administrator for example) and user equipment 309. Rendering apparatus further comprises a display 306.

[0020] User equipment 309 comprises a processor 311 and a memory 313. Memory 313 can store data representing the passphrase 307 that has been agreed between the rendering apparatus 301 and user equipment 309 as noted above. User equipment 309 further comprises an input device 317 and a display 319.

[0021] As described above, the validity of the passphrase 307 is attested to at user equipment 309. In an example, this can be by the passphrase 307 being

displayed on display 306 of rendering apparatus 301 for a user. The user can then confirm whether the displayed passphrase 307 matches the passphrase that can be displayed using display 319 of user equipment 309. The mutual display of the passphrase can be triggered automatically as the user equipment approaches the vicinity of the apparatus 301 (e.g. user equipment 309 may poll rendering apparatus 301 or vice versa), or may be triggered by the user selecting an appropriate function of the rendering apparatus 301.

[0022] In an example, the validity of the passphrase 307 can be attested to at user equipment 309 by submitting the passphrase 307 to the user equipment 309. For example, the rendering apparatus 301 can display the passphrase 307 using display 306. A user can use input device 317 to input the passphrase to the user equipment 309 where the processor 311 can verify that the passphrase matches with one stored in memory 313 for example.

[0023] The passphrase, once validated, can be used as part of a PAKE protocol to generate a session key 320 than can be used to encrypt an identity 321 of the rendering apparatus 301 to generate an encrypted rendering apparatus identity 323. User equipment 309 can then be transported to a workstation or device 315 where the encrypted rendering apparatus identity 323 can be decrypted using session key 320 and transferred to the workstation or device 315 to enable the rendering apparatus to be enrolled.

[0024] There are several additional approaches for delivering the printer identity to the user. Delivery of a temporary key can be accomplished through visual media such as a QR code on the rendering device's LCD or through a rendering of the key in physical space (e.g., a paper print out or a 3D rendering). The user could then capture this rendering with a camera (e.g., on a mobile phone) and translate the code into a key. The code would also contain information that would be used to contact the apparatus such as the IP address or the name of a WiFi direct network.

[0025] As an alternative to the temporary key, the apparatus could generate a one-time use password to access a private WiFi Direct network. This would enable the user's mobile device to contact the apparatus directly and obtain the identity.

[0026] The SPAKE2 key exchange algorithm can be implemented on printer and mobile application (Android; iOS) software. The communication between the printer and mobile device can use any transport protocol without security. In an example, the user equipment (mobile device) can use a pre-existing Bluetooth classic pairing with their workstation to transfer the identity and register it with their desktop software.

[0027] It is worth noting that the encryption of the identity with the temporary key provides a logical binding between the delivered identity and the physical device that presented the temporary key. This binding is what enables a user to associate an incorporeal identity, such as a cryptographic key, and real world object. While this binding does not prove the identity of the device (this is the responsibility of a certificate verification protocol), it gives the user confidence in the device that bares that identity.

[0028] 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.

[0029] 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.

[0030] The machine-readable instructions may, for example, be executed by 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 apparatus (for example, user equipment and rendering 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.

[0031] 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.

[0032] For example, the instructions may be provided on a non-transitory computer readable storage medium encoded with instructions, executable by a processor.

[0033] With reference to figure 3 for example, memory 305, 313 can comprise machine-readable instructions which are executable by processor 303, 311. The instructions can comprise instructions to:

[0034] generate a passphrase using a processor of the rendering apparatus;

[0035] attest to the validity of the passphrase at user equipment or submitting the passphrase to the user equipment;

[0036] encrypt a rendering apparatus identity using a cryptographic session key agreed on the basis of the passphrase; and

[0037] transfer the rendering apparatus identity from the user equipment to a user apparatus.

[0038] 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 a operation for realizing

functions specified by flow(s) in the flow charts and/or block(s) in the block diagrams.

[0039] 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.

[0040] 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.

[0041] 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.

[0042] 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 registering the identity of a rendering apparatus, the method comprising:

generating a passphrase using a processor of the rendering apparatus;

attesting to the validity of the passphrase at user equipment or submitting the passphrase to the user equipment;

encrypting a rendering apparatus identity using a cryptographic session key agreed on the basis of the passphrase; and

transferring the rendering apparatus identity from the user equipment to a user apparatus.

2. A method as claimed in claim 1, further comprising;

decrypting the encrypted rendering apparatus identity using the cryptographic session key.

3. A method as claimed in claim 2, wherein the encrypted rendering apparatus identity is decrypted at the user equipment.

4. A method as claimed in claim 1, wherein the passphrase is generated as part of a password authenticated key exchange protocol.

5. A method as claimed in claim 1, wherein attesting to the validity of the passphrase at user equipment further comprises:

entering the passphrase to the user equipment; and

comparing the entered passphrase to a pre-defined agreed passphrase stored in a memory of the user equipment.

6. A method as claimed in claim 1 wherein attesting to the validity of the passphrase at user equipment further comprises:

providing a confirmation that the generated passphrase is the same as a pre-defined agreed passphrase stored in a memory of the user equipment.

7. A method as claimed in claim 1, further comprising using the identity of the rendering apparatus to enable secure communication with the user equipment.

8. User equipment comprising a processor to:

attest to the validity of a passphrase or receive an input representing the passphrase;

encrypt a rendering apparatus identity using a cryptographic session key agreed on the basis of the passphrase; and

transfer the rendering apparatus identity from the user equipment to a user apparatus.

9. User equipment as claimed in claim 8, the processor further to:

decrypt the encrypted rendering apparatus identity using the cryptographic session key.

10. User equipment as claimed in claim 8, the processor further to:

compare the entered passphrase to a pre-defined agreed passphrase stored in a memory of the user equipment.

11. User equipment as claimed in claim 8, the processor to:

use the identity of the rendering apparatus to enable secure communication with the user equipment.

12. A non-transitory machine-readable storage medium encoded with instructions executable by a processor of user equipment, the machine-readable storage medium comprising:

instructions to:

attest to the validity of a passphrase or receive an input representing the passphrase;

encrypt a rendering apparatus identity using a cryptographic session key agreed on the basis of the passphrase; and

transfer the rendering apparatus identity from the user equipment to a user apparatus.

13. A non-transitory machine-readable storage medium as claimed in claim 12, further comprising instructions to decrypt the encrypted rendering apparatus identity using the cryptographic session key.

14. A non-transitory machine-readable storage medium as claimed in claim 12, further comprising instructions to compare the entered passphrase to a pre-defined agreed passphrase stored in a memory of the user equipment.

15. A non-transitory machine-readable storage medium as claimed in claim 12, further comprising instructions to use the identity of the rendering apparatus to enable secure communication with the user equipment.

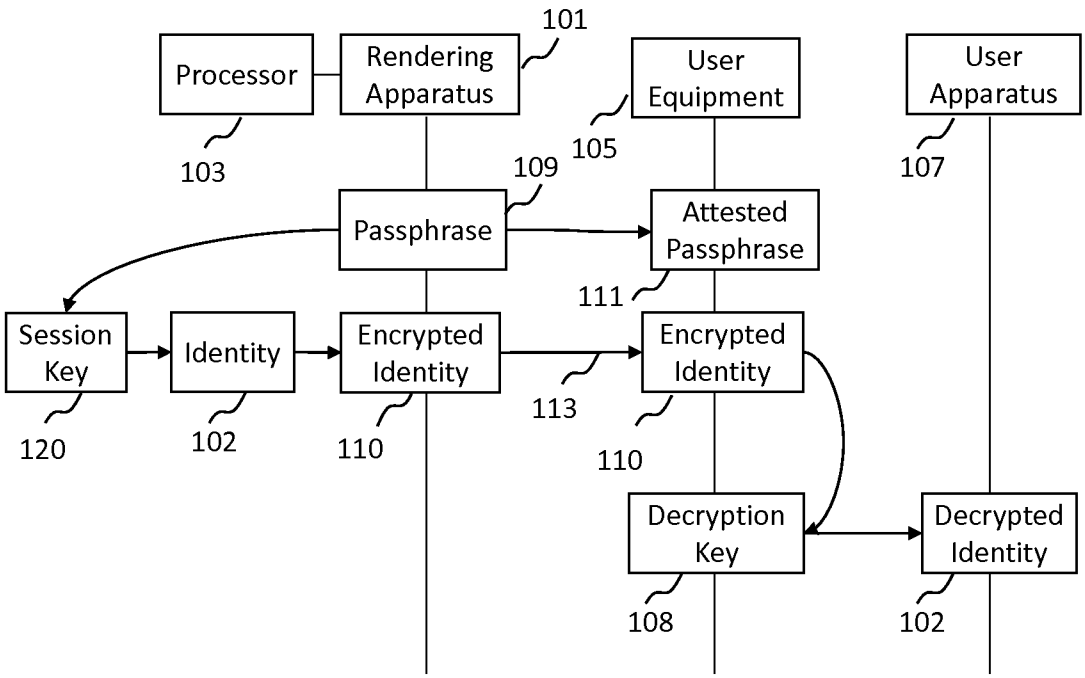
Processor
Rendering Apparatus
101
User Equipment
User Apparatus
103
105
107
109
Passphrase
Attested Passphrase
111
Session Key
Identity
Encrypted Identity
Encrypted Identity
113
120
102
110
110
Decryption Key
Decrypted Identity
108
102

Figure 1

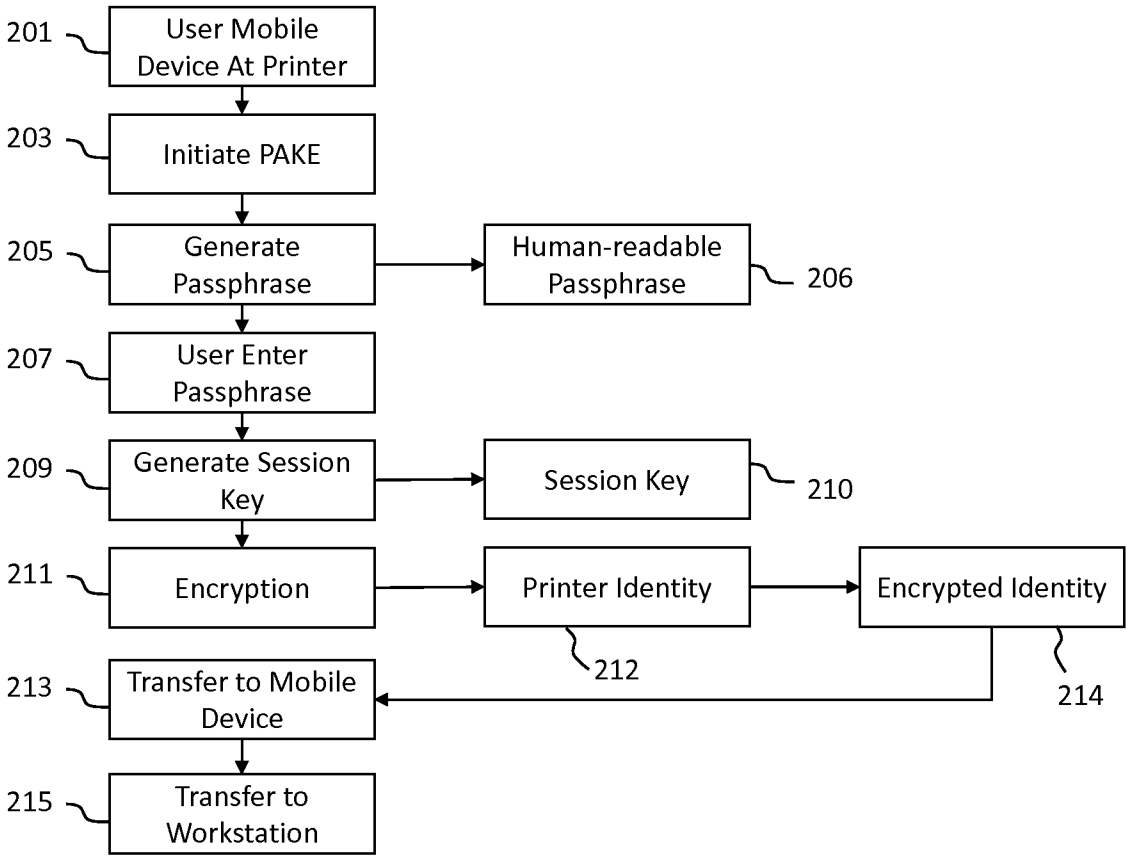
201
User Mobile Device At Printer
203
Initiate PAKE
205
Generate Passphrase
Human-readable Passphrase
206
207
User Enter Passphrase
209
Generate Session Key
Session Key
210
211
Encryption
Printer Identity
Encrypted Identity
212
214
213
Transfer to Mobile Device
215
Transfer to Workstation

Figure 2

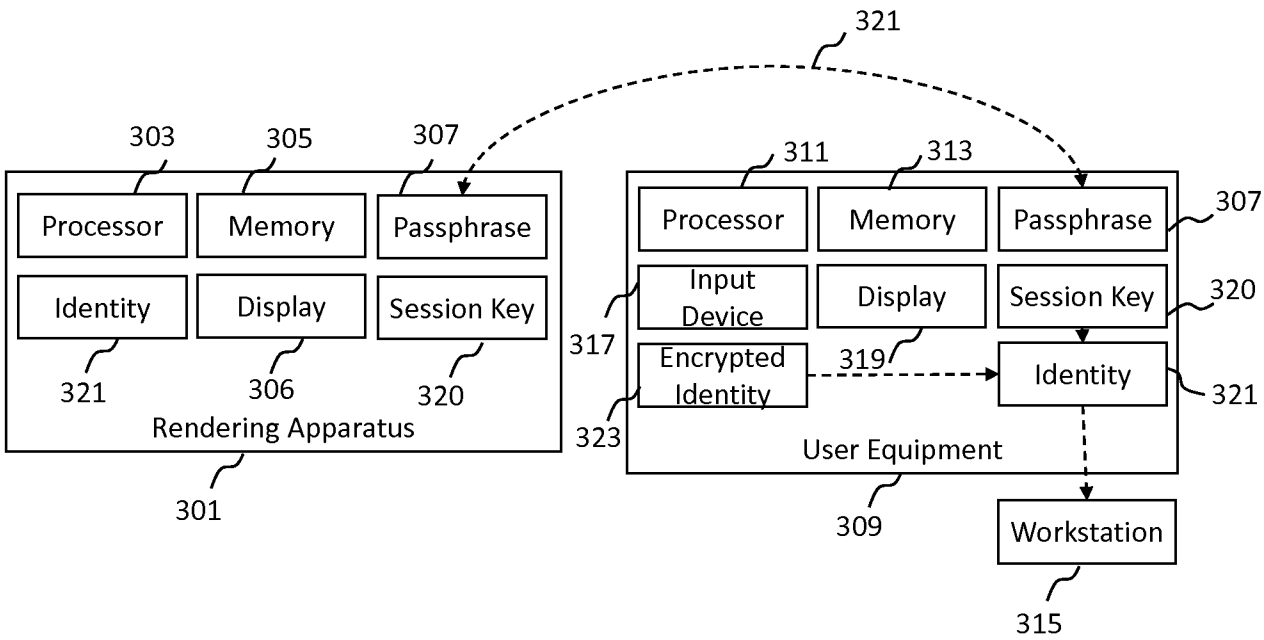
321
303
305
307
311
313
Processor
Memory
Passphrase
Processor
Memory
Passphrase
307
Identity
Display
Session Key
Input Device
Display
Session Key
320
317
321
306
320
Encrypted Identity
319
Identity
321
323
Rendering Apparatus
User Equipment
301
309
Workstation
315

Figure 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 2017/042641

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 *(2006.01)*
G06F 21/46 *(2013.01)*

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)

H04L 9/00, 9/28, 9/32, G06F 21/00, 21/30, 21/45, 21/46

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, Information Retrieval System of FIPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0083750 A1 (SONY CORPORATION) 12.04.2007, paragraphs [0013], [0024], [0030], [0048], [0068]-[0072], [0081], [0083], [0091], [0092], [0110]-[0114], [0156], [0223], [0224], [0229]	1-15
Y	US 7248693 B1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.) 24.07.2007, column 1, lines 46-56, column 3, lines 1-25, column 6, lines 27-32, 51-56, claim 28	1-15
A	US 9674162 B1 (AMAZON TECHNOLOGIES, INC.) 06.06.2017	1-15
A	US 7984298 B2 (HUAWEI TECHNOLOGIES CO., LTD.) 19.07.2011	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
03 April 2018 (03.04.2018)	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
I. Kryazhev
Telephone No. (495) 531-64-81