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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2014 (24.07.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/113196 A4

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) International Application Number:
PCT/US20 13/077724

(22) International Filing Date:
24 December 2013 (24. 12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/754,524	18 January 2013 (18.01.2013)	US
13/839,050	15 March 2013 (15.03.2013)	US
13/839,084	15 March 2013 (15.03.2013)	US
13/839,126	15 March 2013 (15.03.2013)	US

(71) Applicant: **APPLE INC.** [US/US]; 1 Infinite Loop, Cupertino, CA 95014 (US).

(72) Inventors: **BROUWER, Michael;** 1 Infinite Loop, M/S 301-2COS, Cupertino, CA 95014 (US). **DE ATLEY, Dallas, B.;** 1 Infinite Loop, M/S 301-2COS, Cupertino, CA 95014 (US). **ADLER, Mitchell, D.;** 1 Infinite Loop, M/S 301-2COS, Cupertino, CA 95014 (US).

(74) Agent: **ADELI, Mani;** Adeli & Tollen, LLP, 11859 Wilshire Blvd., Suite 500, Los Angeles, CA 90025 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Continued on nextpage]

(54) Title: KEYCHAIN SYNCHRONIZATION

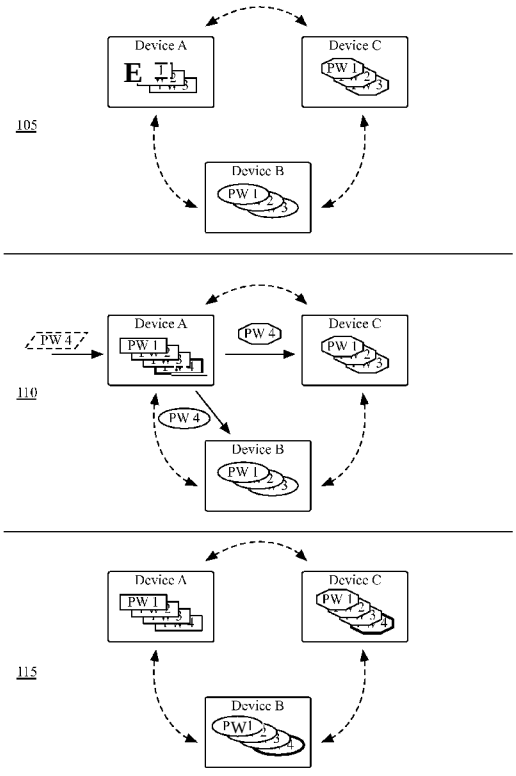

Figure 1

(57) Abstract: Some embodiments provide non-transitory machine-readable medium that stores a program which when executed by at least one processing unit of a device synchronizes a set of key chains stored on the device with a set of other devices. The device and the set of other devices are communicatively coupled to one another through a peer-to-peer (P2P) network. The program receives a modification to a keychain in the set of keychains stored on the device. The program generates an update request for each device in the set of other devices in order to synchronize the set of keychains stored on device with the set of other devices. The program transmits through the P2P network the set of update requests to the set of other devices over a set of separate, secure communication channels.

WO 2014/113196 A4

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))*

— *with amended claims (Art. 19(1))*

Date of publication of the amended claims: 12 September 2014

AMENDED CLAIMS
received by the International Bureau on 22 July 2014 (22.07.2014)

CLAIMS

We claim,

1. A non-transitory machine-readable medium storing a program which when executed by at least one processing unit of a first device synchronizes a set of keychains stored on the first device with keychains stored on a set of other devices, the first device and the set of other devices communicatively coupled to one another through a peer-to-peer (P2P) network, the program comprising sets of instructions for:

detecting that a particular keychain in the set of keychains stored on the device has been modified, wherein the particular keychain comprises a plurality of secure data items for use across the first device and set of other devices;

upon detection that the particular keychain has been modified, generating a separate update request for each device in the set of other devices in order to synchronize the particular keychain stored on device with the corresponding keychains stored on the other devices in the set of other devices; and

transmitting through the P2P network the generated update requests to the set of other devices over a set of separate, secure communication channels.

2. The non-transitory machine-readable medium of claim 1, wherein the modification to the keychain is an addition of a secure data item to the particular keychain.

3. The non-transitory machine-readable medium of claim 1, wherein the modification to the keychain is a modification of a secure data item in the particular keychain.

4. The non-transitory machine-readable medium of claim 1, wherein the modification to the keychain is a deletion of a secured data item in the particular keychain.

5. The non-transitory machine-readable medium of claim 1, wherein the P2P network is implemented by an overlay network configured according to a fully connected mesh topology.

6. The non-transitory machine-readable medium of claim 1, wherein the P2P network is implemented by an overlay network configured according to a star topology comprising a plurality of nodes, wherein a center node of the star topology is a cloud storage service and remaining nodes of the star topology comprise the device and the set of other devices.

7. A method for synchronizing a set of keychains stored on a first device with keychains stored on a set of other devices, the first device and the set of other devices

communicatively coupled to one another through a peer-to-peer (P2P) network, the method comprising:

detecting that a particular keychain in the set of keychains stored on the device has been modified, wherein the particular keychain comprises a plurality of secure data items for use across the first device and the set of other devices;

upon detection that the particular keychain has been modified, generating a separate update request for each device in the set of other devices in order to synchronize the particular keychain stored on device with the corresponding keychains stored on the other devices in the set of other devices; and

transmitting through the P2P network the generated update requests to the set of other devices over a set of separate, secure communication channels.

8. The method of claim 7, wherein transmitting through the P2P network the generated update requests to the set of other devices over the set of separate, secure communication channels comprises encrypting the update request for each particular other device with an encryption key such that the update request is decryptable by only the particular other device.

9. The method of claim 8, wherein the encryption key for encrypting the update request for a particular one of the other devices in the set of other devices comprises a public key of a public/private key pair of the particular other device.

10. The method of claim 7, wherein the plurality of secure data items of the particular keychain comprises at least one of a password, a private key, a certificate, and a secure note.

11. A non-transitory machine-readable medium storing a program which when executed by at least one processing unit of a first device processes requests to join a synchronization circle for synchronizing keychains, the synchronization circle comprising the first device and a set of other devices that share secure data, the program comprising sets of instructions for:

receiving a request for a particular device to join the synchronization circle;

determining whether the request is authenticated based on data received with the request; and

when the request is determined as authenticated, prompting a user for approval of the request; and

when approval of the request is received from the user, adding the particular device to the synchronization circle, wherein secure keychain data is shared between the first

device and the particular device after addition of the particular device to the synchronization circle.

12. The non-transitory machine-readable medium of claim 11, wherein the set of instructions for determining whether the request is authenticated comprises sets of instructions for:

verifying that a user associated with the synchronization circle submitted the request for the particular device to join the synchronization circle; and

verifying that the request for the particular device to join the synchronization circle is generated by the particular device.

13. The non-transitory machine-readable medium of claim 12, wherein the data received with the request for the particular device to join the synchronization circle comprises a signature of the request, wherein the set of instructions for verifying that the user associated with the synchronization circle submitted the request for the particular device to join the synchronization circle comprises sets of instructions for:

decrypting the signature of the request with a public key of a user signing public/private key pair; and

determining that the request matches the decrypted signature.

14. The non-transitory machine-readable medium of claim 12, wherein the data received with the request for the particular device to join the synchronization circle comprises a signature of the request, wherein the set of instructions for verifying that the request for the particular device to join the synchronization circle is generated by the particular device comprises sets of instructions for:

decrypting the signature of the request with a public key of a public/private key pair belonging to and generated by the particular device; and

determining that the request matches the decrypted signature.

15. The non-transitory machine-readable medium of claim 11, wherein the set of instructions for prompting the user for approval of the request comprises a set of instructions for displaying a request for a password to be entered on a display screen of the first device.

16. For a first device, a method for processing requests to join a synchronization circle for synchronizing keychains, the synchronization circle comprising the first device and a set of other devices that share secure data, the method comprising:

receiving a request for a particular device to join the synchronization circle;

determining whether the request is authenticated based on data received with the request; and

when the request is determined as authenticated, prompting a user for approval of the request; and

when approval of the request is received from the user, adding the particular device to the synchronization circle, wherein secure keychain data is shared between the first device and the particular device after addition of the particular device to the synchronization circle.

17. The method of claim 16, wherein adding the particular device to the synchronization circle comprises adding data uniquely identifying the particular device to a list of devices specified as members of the synchronization circle.

18. The method of claim 17, wherein adding the particular device to the synchronization circle further comprises generating a signature of the list of devices with a private key of a public/private device signing key pair belonging to and generated by the first device.

19. The method of claim 18, wherein adding the particular device to the synchronization circle further comprises storing the list of devices and the generated signature in a central location for sharing with the other devices in the synchronization circle.

20. The method of claim 16 further comprising synchronizing keychains with the particular device by sharing secure keychain data between the first device and the particular device, after adding the particular device to the synchronization circle.