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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2014 (05.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/083335 A4

(51) International Patent Classification:
G06F 21/35 (2013.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01) *H04W 12/08* (2009.01)
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/GB2013/053138

(22) International Filing Date:
27 November 2013 (27.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1221433.4 28 November 2012 (28.11.2012) GB
13/706,307 5 December 2012 (05.12.2012) US
1303677.7 1 March 2013 (01.03.2013) GB

(71) Applicant: HOVERKEY LTD [GB/GB]; Campus London, 4-5 Bonhill Street, London Greater London EC2A 4BX (GB).

(72) Inventor: YAU, Arnold; Campus London, 4-5 Bonhill Street, London Greater London EC2A 4BX (GB).

(74) Agent: KILBURN & STRODE LLP; 20, Red Lion Street, London, Greater London WC1R 4PJ (GB).

(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, 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))*

(88) Date of publication of the international search report:
18 June 2015

Date of publication of the amended claims: 23 July 2015

(54) Title: A METHOD AND SYSTEM OF PROVIDING AUTHENTICATION OF USER ACCESS TO A COMPUTER RESOURCE VIA A MOBILE DEVICE USING MULTIPLE SEPARATE SECURITY FACTORS

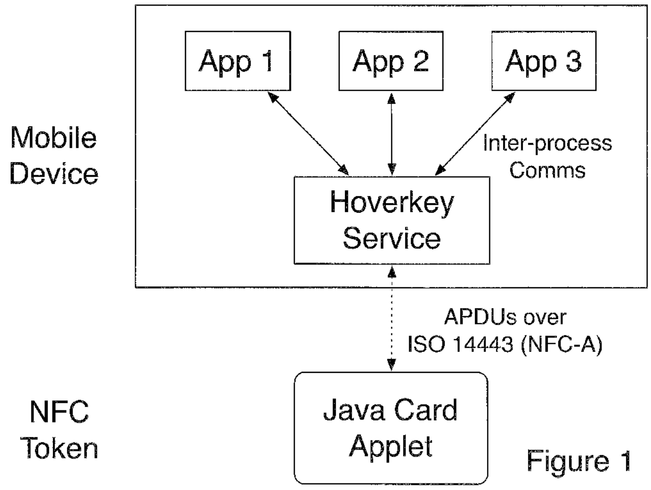

Figure 1

(57) Abstract: A method and system of authenticating a computer resource such as an application or data on a mobile device uses a contactless token to provide multi-factor user authentication. User credentials are stored on the token in the form of private keys, and encrypted data and passwords are stored on the device. When application user requires access to the resource an encrypted password is transmitted to and decrypted on the token using a stored private key. An unencrypted data encryption key or password is then transmitted back to the device under the protection of a cryptographic session key which is generated as a result of strong mutual authentication between the device and the token.

CLAIMS

AMENDED CLAIMS
received by the International Bureau on 19 May 2015 (19.05.2015)

1 A method of authenticating access to a computer resource via a mobile device comprising:

storing an encrypted resource authorization;

transmitting the encrypted authorization to a separate portable security token;

on the token, decrypting the encrypted authorization and generating at least partially therefrom an unlock response;

securely transmitting the unlock response to the mobile device;

requiring a user to authenticate separately on the mobile device; and

unlocking the resource if the required unlock response and the separate authentication are both valid.

2 A method as claimed in claim 1 in which the unlock response comprises a plain authorization, obtained by decrypting the encrypted authorization

3 A method as claimed in claim 1 in which the unlock response comprises a function of a plain authorization, obtained by decrypting the encrypted authorization, and additional information.

4 A method as claimed in claim 1 in which the authorization comprises a password, a PIN or a cryptographic key.

5 A method as claimed in any one of the preceding claims in which the unlock response is transmitted to the mobile device under the protection of an encryption key, such as a session key.

6 A method as claimed in any one of the preceding claims in which the token stores user credentials, the decryption on the token being based on the user credentials.

7 A method according to claim 6, wherein the user credentials are stored in the token in a secure location within the token.

8 A method according to claim 7, wherein the secure location is provided by hardware and/or software of the token.

9 A method as claimed in any one of the preceding claims in which the encrypted authorization is stored on the mobile device.

10 A method as claimed in any one of claims 1 to 8 in which the encrypted authorization is stored in the cloud and is retrieved from the cloud to the mobile device.

11 A method as claimed in any preceding claim in which the authentication on the mobile device is validated on the token before the unlock response is sent.

12 A method as claimed in any one of the preceding claims including running a service on the mobile device which controls device cryptographic functions and access to the resource.

13 A method as claimed in any one of the preceding claims including running an applet on the token which provides token cryptographic functions.

14 A method as claimed in claim 6 in which the user credentials are generated by the token and never leave the token.

15 A method as claimed in any one of the preceding claims, when dependent upon claim 6, in which the encrypted authorization can be decrypted solely with the corresponding user credentials stored on the token.

16 A method as claimed in any one of the preceding claims including verifying integrity on the token by a message authentication code received from the device.

17 A method as claimed in any one of the preceding claims in which the integrity of the encrypted authorization is verified on the token prior to decryption.

18 A method as claimed in any one of the preceding claims in which the device and the token perform cryptographic mutual authentication before transmission of the encrypted authorization.

19 A method as claimed in any one of claims 1 to 17 in which the encryption and decryption are by symmetric key cryptography

20 A method as claimed in claim 18 in which the mutual authentication is by symmetric key cryptography.

21 A method according to claim 18, wherein the mutual authentication is by asymmetric key cryptography.

22 A method according to any preceding claim, wherein the user authentication on the mobile device comprises a user secret.

23 A method as claimed in claim 22 in which the user secret is passed from the device to the token and is validated by the token before the decryption operation takes place.

24 A method according to any preceding claim, wherein user authentication on the mobile device is via biometric information, for example, a fingerprint and/or iris pattern.

25 A method according to claim 22 or 23, wherein the user secret comprises a personal identification number (PIN), an alphanumeric password, and/or one or more physical gestures comprising a swipe pattern on a touch panel, a pattern of movement detected by a motion detector on the device, a gesture detected by a camera on the device and/or a gesture detected by a microphone on the device.

26 A method as claimed in any one of the preceding claims in which the resource comprises an application running or stored on the mobile device, or accessible therefrom.

27 A method as claimed in any one of claims 1 to 25 in which the resource comprises data stored on the mobile device or accessible therefrom.

28 A system of authenticating access to a computer resource via a mobile device with a portable security token, comprising:
a mobile device;
a token including token storage for storing private user credentials, a token communications system, and a token processor providing cryptographic functions;

and wherein in use an encrypted authorization is transmitted by the device communications system to the token; is decrypted on the token using the user credentials; the token generating at least partially therefrom an unlock response, the unlock response being securely transmitted by the token communications system to the mobile device; requiring a user to authenticate separately on the mobile device; and unlocking the resource if the required unlock response and the separate authentication are both valid.

29 A system as claimed in claim 28 in which the authorization comprises an application password, a PIN or a cryptographic key.

30 A system as claimed in claim 28 including means for retrieving the encrypted authorization from the cloud.

31 A system as claimed in any one of claims 28 to 30 in which the unlock response is transmitted by the token communications system to the mobile device under the protection of an encryption key such as a session key.

32 A system as claimed in any one of claims 28 to 31 in which the token is a card.

33 A system as claimed in any one of claims 28 to 32 in which the device communications system and the token communications system communicate over the air.

34 A system as claimed in claim 33 in which communication is by NFC, Bluetooth, or Bluetooth Low Energy.

35 A system as claimed in any one of claims 28 to 34 in which the device communications system and the token communications system communicate when the token is placed in close proximity to or is touched to the device.

36 A system as claimed in any of claims 28 to 35, in which the separate authentication on the mobile device is validated on the token before the unlock response is sent.

37 A system according to any of claims 28 to 36, wherein the user authentication on the mobile device comprises a user secret.

38 A system as claimed in claim 37 in which the device communications system sends the user secret to the token which is validated by the token before the decryption operation takes place.

39 A system according to any preceding claim, wherein user authentication on the mobile device is via biometric information, for example, a fingerprint and/or iris pattern.

40 A system according to claim 37 or 38, wherein the user secret comprises a personal identification number (PIN), an alphanumeric password, and/or one or more physical gestures comprising a swipe pattern on a touch panel, a pattern of movement detected by a motion detector on the device, a gesture detected by a camera on the device and/or a gesture detected by a microphone on the device.

41 A system as claimed in any one of any one of claims 28 to 40 in which the device communications system sends a message authentication code (MAC) to the token, which is validated by the token before the decryption operation takes place.

42 A system as claimed in any one of any one of claims 28 to 41 in which the integrity of the encrypted authorization is verified on the token prior to decryption.

43 A system as claimed in any one of claims 28 to 42 in which the device and the token are arranged to perform cryptographic mutual authentication before transmission of the encrypted authorization.

44 A system as claimed in any one of claims 28 to 43 in which the token sends the unlock response only on positive confirmation by the user, for example by pressing a button on the token.

45 A system according to any of claims 28 to 44, wherein the token storage for storing private user credentials is provided by hardware and/or software of the token.

46 A hardware token for authenticating access to a computer resource via a mobile device, the token comprising:

token storage for the storage of a plurality of user credentials;

a token communications system for communicating with a mobile device;

a token processor providing cryptographic functions; and

wherein, in use:

on receipt by the token communications system of an encrypted authorization, the token processor verifies the integrity and decrypts the encrypted authorization and generates at least partially therefrom an unlock response, and wherein the token communications system securely transmits the unlock response for use by a mobile device.

47 A hardware token as claimed in claim 46 including an alphanumeric display.

48 A hardware token as claimed in claim 46 or claim 47 including user feedback means for example one or more user-operable buttons or touch-sensitive areas.

49 A hardware token as claimed in claim 46, 47 or 48, wherein the token storage for storing private user credentials is provided by hardware and/or software of the token.

50 A method, system or token according to any preceding claim, wherein the token is provided by any one of a keyfob, a badge, an NFC smartcard, a watch, a wearable ring, a fitness band, a wireless headset or a piece of jewellery.

51 A method, system or token according to any of claims 1 to 49, wherein the token is provided by a mobile computing device.

52 A method, system or token according to claim 51, wherein the mobile computing device provides other user functionality.

53 A method, system or token according to claim 51 or 52, wherein the mobile computing device comprises any one of a smart phone, smart watch, smart glasses, tablet device or laptop.

54 A method of authenticating a user to access a computer resource via a mobile device comprising:

storing an encrypted resource authorization;

transmitting the encrypted authorization to at least one separate portable security token device;

on the token device, decrypting the encrypted authorization and generating at least partially therefrom an unlock response;

securely transmitting the unlock response to the mobile device; and

providing access to the resource if the required unlock response is valid;

wherein a user is required to authenticate on the mobile device or on the token device, and the authentication is validated on the token device before the unlock response is sent.

55. A system of authenticating a user to access a computer resource via a mobile device with at least one portable security token device, comprising:

a mobile device;

at least one token device including token storage for storing private user credentials, a token communications system, and a token processor providing cryptographic functions;

and wherein in use an encrypted authorization is transmitted by the mobile device communications system to the token device; is decrypted on the token device using the user credentials; the token device generating at least partially therefrom an unlock response, the unlock response being securely transmitted by the token communications system to the mobile device; and providing access to the resource if the required unlock response is valid;

wherein a user is required to authenticate on the mobile device or on the token device, and the authentication is validated on the token device before the unlock response is sent.

56 A hardware token device for authenticating a user to access a computer resource via a mobile device, the token device comprising:

token storage for the storage of a plurality of user credentials;

a token communications system for communicating with a mobile device;

a token processor providing cryptographic functions; and

wherein, in use:

on receipt by the token communications system of an encrypted authorization, the token processor verifies the integrity and decrypts the encrypted authorization and generates at least partially therefrom an unlock response, wherein the token communications system securely transmits the unlock response for use by a mobile device, and wherein a user is required to authenticate on the mobile device or on the token device, and the authentication is validated on the token device before the unlock response is sent.