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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 April 2021 (01.04.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/056069 A1

(51) International Patent Classification:
G06F 21/34 (2013.01) *H04L 9/32* (2006.01)
G06F 21/62 (2013.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/AU2020/051020

(22) International Filing Date:
25 September 2020 (25.09.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2019903591 25 September 2019 (25.09.2019) AU

(71) Applicant: **COMMONWEALTH SCIENTIFIC AND INDUSTRIAL RESEARCH ORGANISATION** [AU/AU]; Clunies Ross St, Acton, Australian Capital Territory 2601 (AU).

(72) Inventors: **GUABTNI, Adnene**; C/- Clunies Ross St, Acton, Australian Capital Territory 2601 (AU). **O'CONNOR, Hugo**; C/- Clunies Ross St, Acton, Australian Capital Territory 2601 (AU).

(74) Agent: **FB RICE PTY LTD**; Level 23, 44 Market Street, Sydney, New South Wales 2000 (AU).

(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, IT, 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,

(54) Title: CRYPTOGRAPHIC SERVICES FOR BROWSER APPLICATIONS

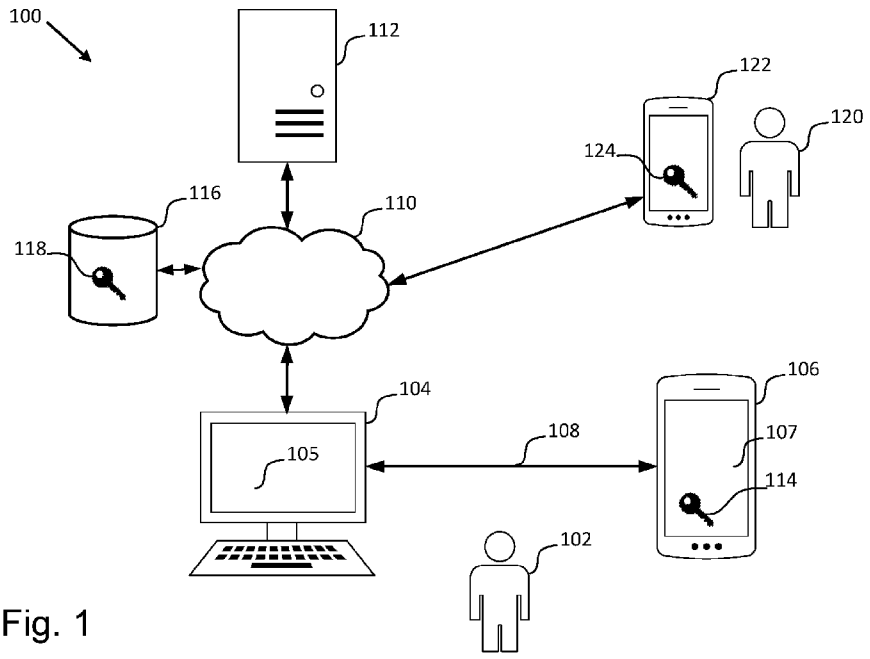

Fig. 1

(57) Abstract: This disclosure relates to the provision of cryptographic services to web browsers, and more specifically, to systems and methods for providing cryptographic results to a browser from a cryptographic device over a persistent peer-to-peer connection. A method for obtaining cryptographic services for a browser executing a webpage comprising the steps of establishing a persistent peer-to-peer connection over a wireless Internet Protocol communication network between the browser and a cryptographic device, in response to receiving user input to the webpage, transmitting, by the browser, data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device, for cryptographic processing of the data by the cryptographic device using a cryptographic key stored on the cryptographic device to produce a cryptographic result, and receiving, by the browser, the cryptographic result over the persistent peer-to-peer connection from the cryptographic device, and providing the cryptographic result to the webpage.

WO 2021/056069 A1

[Continued on next page]

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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).

Published:

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

"Cryptographic services for browser applications"

Cross-Reference to Related Applications

[0001] The present application claims priority from Australian Provisional Patent Application No 2019903591 filed on 25 September 2019, the contents of which are incorporated herein by reference in their entirety.

Technical Field

[0002] Aspects of this disclosure relate generally to the provision of cryptographic services to web browsers and more specifically to systems and methods for providing cryptographic services to a browser by a cryptographic device.

Background

[0003] Many webpages now facilitate or require the use of cryptographic functions to provide authentication, encryption and other security features to users.

[0004] For example, two step (or two factor) authentication is a method of authenticating a user by utilising a secret that the user knows, such as a password, and a cryptographic secret that the user can generate through use of a cryptographic device and can provide to the webpage. This form of authentication is becoming more prevalent in line with the increased demand for enhanced security.

[0005] Additionally, many web enabled applications now provide functionality that enables a user to apply encryption and decryption to data for privacy purposes, or to interface with cryptographic applications such as blockchain ledgers.

[0006] Unfortunately, users often find the use of cryptographic services provided by web pages to be cumbersome and inefficient to use. Furthermore, an increased risk of unintentional or malicious security breaches means that there is a focus on ensuring that such cryptographic services be highly resistant to hacking or tampering by malicious parties.

[0007] Accordingly, there is a need for a private, secure and convenient means of providing authentication and cryptography services to web enabled applications, such as browsers.

[0008] Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present disclosure as it existed before the priority date of each of the appended claims.

Summary

[0009] There is provided a method for obtaining cryptographic services for a browser executing a webpage. The method comprises establishing a persistent peer-to-peer connection over a wireless Internet Protocol communication network between the browser and a cryptographic device, in response to receiving user input to the webpage, transmitting, by the browser, data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device, for cryptographic processing of the data by the cryptographic device using a cryptographic key stored on the cryptographic device to produce a cryptographic result, and receiving, by the browser, the cryptographic result over the persistent peer-to-peer connection from the cryptographic device, and providing the cryptographic result to the webpage.

[0010] The method may further comprise the steps of receiving, by the cryptographic device, from the browser, data via the persistent peer-to-peer connection between the browser and the cryptographic device, performing, by the cryptographic device, the cryptographic function on the data using the cryptographic key stored on the cryptographic device, to produce the cryptographic result, and transmitting, by the cryptographic device, the cryptographic result to the browser, over the persistent peer-to-peer connection.

[0011] The persistent peer-to-peer connection may remain established over multiple iterations of the steps of transmitting, by the browser, the data over the persistent peer-to-peer connection to the cryptographic device, and receiving, by the browser, the cryptographic result over the persistent peer-to-peer connection from the cryptographic device.

[0012] The cryptographic device may send confidential data stored on the cryptographic device, from the cryptographic device to the browser. Furthermore, the cryptographic device may sign, encrypt, verify or decrypt the data with the cryptographic key to produce the cryptographic result.

[0013] The browser may embed the cryptographic result in the webpage. Additionally, the browser may provide the cryptographic result to a server hosting the webpage, which may result in the browser receiving an updated webpage from the server hosting the webpage.

[0014] A persistent peer-to-peer connection may be established via the browser signalling information. The cryptographic device may receive the signalling information, and in response, transmit response information, to the browser, necessary to establish a peer-to-peer connection. The signalling information may be signalled 'out of band', for example via a Quick Response (QR) code displayed within the browser.

[0015] The signalling information may include an authentication challenge, which may be signed by the cryptographic device by applying an authentication key to the challenge information to produce a challenge response.

[0016] The cryptographic device may transmit a signalling response back to the browser, which include cryptographic device identification information and the challenge response. The response may also include a public key which is complementary to the private key stored on the cryptographic device.

[0017] The software describing the browser's establishment and management of the peer-to-peer connection may be injected into the webpage by the browser. The software may be described by JavaScript libraries which are invoked by a call to the libraries embedded in the webpage code.

[0018] According to another aspect of the disclosure, there is provided a method of obtaining cryptographic services for a browser executing a webpage on a user device, the method comprising establishing a persistent peer-to-peer connection between the browser and a cryptographic device, in response to receiving user input to the webpage, transmitting, by the browser, data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device, applying, by the cryptographic device, a cryptographic function to the data using a cryptographic key stored on the cryptographic device, to produce a cryptographic result; and transmitting, by the cryptographic device, the cryptographic result to the browser, over the persistent peer-to-peer connection.

[0019] According to another aspect of the disclosure, there is provided a method of providing cryptographic services to a browser executing a webpage, the method comprising receiving data from the browser, via a persistent peer-to-peer connection between the browser and a cryptographic device, performing, by the cryptographic device, a cryptographic function on the data using a cryptographic key stored on the cryptographic device, to produce a cryptographic result, and transmitting, by the cryptographic device, the cryptographic result to the browser, over the persistent peer-to-peer connection.

[0020] According to another aspect of the disclosure, there is provided a browser executing a webpage on a user device, the browser configured to, establish a persistent peer-to-peer connection between the browser and a cryptographic device, in response to receiving a user input to the webpage, transmit data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device for cryptographic processing of the data using a cryptographic key stored on the cryptographic device, to produce a cryptographic result, and receive the cryptographic result over the persistent peer-to-peer connection from the cryptographic device.

[0021] According to another aspect of the disclosure, there is provided a cryptographic device configured to establish a persistent peer-to-peer connection between a browser executing a webpage, and an cryptographic application executing on the cryptographic device, receive data from the browser, via the persistent peer-to-peer connection, perform a cryptographic function on the received data, using a cryptographic key stored on the cryptographic device, to produce an cryptographic result, transmit the cryptographic result to the browser, via the persistent peer-to-peer connection.

Brief Description of Drawings

[0022] Examples will now be described with reference to the following drawings, in which:

Fig. 1 illustrates a network diagram;

Fig. 2 is block diagram of the cryptographic device of Figure 1;

Fig. 3 is a flowchart illustrating a method, as performed by a browser, of establishing a peer-to-peer connection between a browser and a cryptographic device;

Fig. 4 is a flowchart illustrating a method, as performed by a cryptographic device, of establishing a peer-to-peer connection between a browser and a cryptographic device;

Fig. 5 is a flowchart illustrating a method, as performed by a browser, for obtaining

cryptographic services;

Fig. 6 is a flowchart illustrating a method, as performed by a cryptographic device, for providing cryptographic services;

Fig. 7 is a message flow diagram illustrating request and response messages being transmitted between a browser and a cryptographic device; and

Figs. 8a-f illustrates a browser displaying webpages.

Description of Embodiments

Network overview

[0023] Fig. 1 illustrates a network diagram 100 in accordance with an aspect of this disclosure. A user 102 is in operation of a device, exemplified by a personal computer 104, displaying a webpage within a web browser 105 executing on the personal computer 104. It is to be understood that in other examples, the browser may be executing on a mobile phone, or other suitable web enabled device.

[0024] The user 102 is also in operation of a cryptographic device 106, exemplified by a mobile phone. The mobile phone includes software and hardware configured to perform cryptographic functions using one or more cryptographic keys 114 stored on the cryptographic device 106.

[0025] It is to be understood that the description of the cryptographic device as a mobile phone is not intended to be limiting. A cryptographic device in accordance with this disclosure could be a device which is specifically dedicated to providing cryptographic processing services and providing cryptographic results over a peer-to-peer connection, a full function device such as a personal computer, a headless device without a screen and interface, or any device which is capable of performing the functionality as attributed to the cryptographic device herein.

[0026] Instead of having to establish a connection with the browser each time a cryptographic service is required, the web browser 105 executing on the personal computer 104 is persistently in communication with the mobile phone via a persistent peer-to-peer connection 108. The web browser 105 is also in communication with a web server 112 via an internet connection 110, such that the web browser is able to download and display webpages from web server 112 via internet connection 110.

[0027] In cases where authentication of the user is required, one or more public keys 118 associated with the user 102 may be stored in memory storage 116 which is accessible by the web server 112. The memory storage 116 may be located within web server 112 or remote from web server 112, as depicted in Fig. 1.

[0028] Another party 120 is also illustrated. The other party may be another user or application. The other party 120 is in operation of a cryptographic device 122, which in the example shown in Fig. 1 is a mobile phone. The other party may be a communication partner of the user 102, with which the communication partner has exchange public keys via the Public Key Infrastructure, or the like. If the other party is a communication partner of the user 102, one or more public keys 124 associated with the user 102 may be stored on the other party's device 122. A role of the other party 120 will be described in subsequent sections.

Cryptographic device

[0029] Fig. 2 is a block diagram of the cryptographic device 106 of Fig. 1. The cryptographic device 106 comprises a processor configured to control operation of the device through the execution of a cryptographic application stored, at least in part, on memory storage 212. Memory storage 212 also stores identification information associated with the one or more user identities of the user 102. The identification information may include user names, email addresses, user identification numbers, and the like.

[0030] Additionally, memory storage 212 stores one or more cryptographic keys 114 to be used by the cryptographic application in the provision of cryptographic services to the browser 105 and in the authentication of the user's identify, if this is required.

[0031] The memory storage 212 may comprise a plurality of individual or interconnected memory storage components. Furthermore, the memory storage 212 may comprise components internal to the cryptographic device, and/or may comprise separate components which are in communication with the cryptographic device, or may comprise a combination thereof.

[0032] The device 106 further comprises a network interface 208. According to the embodiment illustrated in Fig. 2, the network interface 208 is a wireless internet interface, which is configured to receive and transmit information wirelessly to and from the internet.

[0033] The device 106 further comprises one or more input/output interfaces 214. The I/O interface may comprise: a camera, configured to capture images and provide said images to the processor; a user input in the form of a touch screen, number pad or keyboard; and an output in the form of a display screen or a status light. Other input/output interfaces may be provided which enable the user to provide and receive information to the device.

[0034] The processor of the cryptographic device executes a cryptographic application, which controls the provision of cryptographic processing services and manages the establishment and operation of the peer-to-peer connection.

[0035] The cryptographic device 106 may include a cryptographic hardware accelerator 210 which is configured to perform cryptographic processing, such as encryption, decryption and signing in hardware. The inclusion of a cryptographic hardware accelerator may be desirable to improve the performance or the security of the cryptographic device.

[0036] The cryptographic processing services may be provided by the cryptographic application executing on the processor, or by the hardware accelerator, or by a combination thereof. The cryptographic device may be configured to provide asymmetric cryptography, such as RSA or others, and may also be configured to provide symmetric cryptography.

Cryptographic keys

[0037] The cryptographic keys stored within memory storage 212 may include one or more keys which are used to provide cryptographic services to the browser. The type of keys stored on the device will depend upon the type of cryptographic services provided by the device. The cryptographic device may perform asymmetrical or symmetrical cryptography, or a combination of the two.

[0038] Asymmetric cryptography uses public and private keys to encrypt and decrypt data. The public key may be shared with other parties; however, the private key remains secure and unknown to other parties. In contrast, symmetric cryptography uses only a single key to apply and remove a cryptographic function on data.

[0039] Where the device 106 provides asymmetric cryptographic processing, the cryptographic device may generate a public/private key pair. Alternatively, the cryptographic keys may be pre-configured during manufacture or setup of the cryptographic device. The public key may be

stored in memory storage 212 and communicated to communication parties as required. In contrast, private keys will not be communicated external to the device, and will be stored in memory storage 212. The cryptographic device may also store public keys received from communication partners.

[0040] As noted above, memory storage 212 may comprise a plurality of different memory components. For enhanced security, private keys may be stored in a memory component which is resistant to malicious access by an external party.

[0041] Since the cryptographic device performs cryptographic processing for the browser, advantageously, the private key remains stored on the device, and there is no need to communicate the private key outside the device 106. Accordingly, there is no need to entrust the user's private key with another party, such as a web server. As the private key is not stored by another party, there is no concern that the private key will be disclosed unintentionally by the other party, or discovered through a security breach of the other party.

[0042] The cryptographic keys stored in memory storage 212 may also include one or more keys used to authenticate the identity of the user. A key used to authenticate the identity of the user may be a private key which is associated with a corresponding public key, in the case that asymmetric cryptography is used during authentication. Although enhanced security would result from an authentication key differing from the one or more cryptographic keys used to provide cryptographic services to the browser, it is envisaged that, for some implementations, a cryptographic device may use the same cryptographic key for the provision of cryptographic services to the browser and for the authentication of the user's identity.

Communication parties

[0043] As illustrated in Fig. 1, a communication partner 120 of a user may exist. A communication partner is another user to which the user 102 has provided a public key 124 corresponding to the user's private key (one of 114). The communication partner may also have provided the user 102 with a public key associated with a private key of the communication partner. Through use of the user's public key 124, the communication partner 120 can provide cryptographically processed information, such as digital signatures and encrypted information, to the user 102. Furthermore, though the user's use of the communication partner's public key, the communication partner can verify the authenticity of data signed by the communication partner's public key, or decrypt data encrypted by the communication partner's public key.

Multiple user identities

[0044] In some situations, it may be desirable for the cryptographic device to be configured to maintain a plurality of identities for the user (or set of users) of the device. Situations in which this may be advantageous include where the user operates both a personal and business identity, or where the user has an administrator role in addition to their user role. Alternatively, or additionally, the user may elect to maintain a plurality of identities and private keys for security or privacy purposes.

[0045] To accommodate a plurality of identities, the cryptographic device may be configured to store a plurality of cryptographic keys within the memory store 212, so that each user identity may be associated with a unique cryptographic key for enhanced security. The user of the device may select one of the plurality of user identities when establishing a persistent peer-to-peer connection with a browser. Additionally, it is to be understood that a cryptographic device may establish a plurality of separate persistent peer-to-peer connections between one or more browsers, whereby each of the separate connections may be associated with a different user identity.

Configuration process

[0046] An exemplary mechanism for configuring the cryptographic device and the browser to perform methods in accordance with this disclosure, will now be described. However, it will be appreciated that there are numerous mechanisms and variations via which the cryptographic device and the browser may be configured to perform methods in accordance with this disclosure.

[0047] The user 102 downloads a cryptographic application 107 from an application server to cryptographic device 106 and installs the cryptographic application. The application server may be the same entity as web server 112. The user 102 triggers the execution of the cryptographic application and creates a user account, for an identity of the user, by providing identifying information such as a user name and authentication information such as a password, phrase or other secret information known to the user. This identifying information and authentication information is provided by the cryptographic application to the server 112 for storage. It is noted, however, that persistent storage of the identifying and authentication information on server 112 is not essential and the keys maybe the only data stored in cryptographic device 106.

[0048] If two-factor authentication is desired, the cryptographic application may also generate a private/public key pair to be associated with the user identity for authentication purposes, storing the private key in the memory storage 212, and providing the public key to the server 112, or a storage location 116 accessible by the server 112. Accordingly, it will be possible for the server who has access to the public key, to verify the identity of the user by applying the public key to a digital signature that the user has signed with their private key.

[0049] The user 102 uses the browser to download a webpage 105 of a website from the web server 112. The user may log into the website 105 using the same user identification information used to create an account for the cryptographic application. Accordingly, the user may be logged into both the website and the cryptographic application on the cryptographic device; however this is not essential.

[0050] The user may now take steps to establish a persistent peer-to-peer connection between the browser and the cryptographic device, so that the cryptographic device may provide cryptographic services to the browser.

Persistent peer-to-peer connections

[0051] A persistent peer-to peer connection provides a communication channel between two internet connected applications, e.g. a browser 105 and a cryptographic application 107 executing on a cryptographic device.

[0052] Communication across the persistent peer-to-peer connection may be achieved via various communication protocols. One peer-to-peer communication protocol which may be applied in accordance with aspects of this disclosure is the Web Real-Time Communication (WebRTC) application programming interface (API). WebRTC provides web browsers and other internet connected applications with real-time communications via simple APIs, including the RTCPeerConnection API, which provides a mechanism for establishing a peer-to-peer connection, and the RTCDataChannel API, which provides a mechanism to transmit arbitrary data over the peer-to-peer connection.

[0053] Accordingly, a peer-to-peer connection, allows peer devices to communicate bit streams, files, audio or video communications and other data forms, by providing a direct communication channel between peers, over the Internet Protocol. This eliminates the need for a dedicated server to relay communications from a transmitting peer to a receiving peer.

Signalling

[0054] To establish a peer-to-peer connection between one internet connected application and another internet connected application, to the participants perform a signalling process, whereby identifying and locating information is exchanged between the peer applications. Signalling allows the applications to exchange metadata to coordinate communication.

[0055] Exemplary information communicated during the signalling process includes network data, which reveals where the applications are located on the internet (IP address and port) so that each application can locate the other. Other information that may be communicated during the signalling process includes session control information which determines when to initialise, close and modify the peer-to-peer connection; and configuration data, which indicates the functional range of the applications, and what type of data can be communicated across the connection. Additionally, signalling may include an authentication and authorisation mechanism to verify the identity of the user.

Signalling methods

[0056] One method of implementing a peer-to-peer connection is to provide signalling information via a server; however, there are situations in which it may be undesirable to use a server to facilitate the signalling process due to limited server bandwidth, speed or privacy concerns. Accordingly, it may be desirable to provide a signalling mechanism that does not necessitate the use of a server, to establish a peer-to-peer connection.

[0057] Signalling information may be sent from a first peer to a second peer 'out of band', meaning that the signalling information is transmitted via a communication means that is not the channel over which the peer-to-peer connection will be established. One method for transmitting the signalling information 'out of band' is to provide the signalling information as a QR code which can be displayed on a display of the initiating peer device. A responding peer can then receive the signalling information by capturing the QR code using a camera input.

[0058] An initiating peer may transmit signalling information to a responding peer through other 'out of band' mechanisms including, but not limited to, SMS, email, Near Field Communications, Bluetooth, hardwired connection, manual input or via USB.

Embodiment - Establishing a persistent peer-to-peer-connection

[0059] A method of establishing a persistent peer-to-peer connection between a browser and a cryptographic device, using a QR code to transmit the signalling information, will be described with reference to Fig. 3, which illustrates a method 300 as performed by a browser 105, and Fig. 4, which illustrates a complementary method 400 as performed by a cryptographic application 107 executing on a cryptographic device, in the form of a mobile phone 106. The exemplary methods illustrated in Figures 3 and 4 use the WebRTC protocol to establish the persistent peer-to-peer connection.

[0060] In step 302, the user authenticates themselves to the webpage executing within the browser, by entering a username and password to log into the webpage. Alternatively, some other means of user authentication may be utilised. In some situations, step 302 may not be required, as the cryptographic device may provide user identification during the establishment of the persistent peer-to-peer connection.

[0061] At step 302, it may also be appropriate for the user or the browser to configure parameters pertaining to the type of cryptographic services that are desired.

[0062] In step 304, in response to receiving an input trigger from the user, such a mouse click on a webpage button or URL, the browser displays a QR code which encodes signalling information to initiate the establishment of a persistent peer-to-peer connection between the browser 105 and the cryptographic device 106. The signalling information includes the public-facing IP address of the browser, as well as the port and transport protocol to be used for the persistent peer-to-peer connection. The signalling information may also include additional information, such as information which identifies the webpage.

Signalling via QR Code

[0063] The mobile phone scans 404 the QR code using the phone's camera. The image of the QR code is then provided to a cryptographic application executing on the phone. In step 406, the cryptographic application decodes the QR code to extract the signalling information.

Authentication challenge

[0064] In some applications, it may be desirable to authenticate, during establishment of the persistent peer-to-peer connection, that the cryptographic device is appropriately associated with user identity used to log into the browser. In other applications, this authentication process may

not be needed or desired; for example, if the webpage allows connections as a guest, or where the user's identity has been otherwise authenticated.

[0065] In the embodiment illustrated in Figures 3 and 4, the browser requires the authentication of the cryptographic device in relation to the user's logged in identity. Accordingly, the signalling information provided in the QR code, in step 304, also includes authentication challenge data, which will be used to authenticate that the cryptographic device is associated with the user identity used to log in to the browser. The authentication challenge data may be a pseudo-randomly generated bit-string.

[0066] In step 408, the cryptographic application determines the authentication challenge data from the QR code, and in step 410, the cryptographic device calculates a signature of the challenge data using an authentication key stored on the cryptographic device, to produce signed authentication challenge data. The authentication key may be the private key of a public/private key pair which identifies the user identity by which the user logged into the cryptographic device and the browser in steps 302 and 402, respectively.

[0067] In step 412, the cryptographic application prepares a signalling response message, which includes cryptographic device identification information, such as an IP address and a port of the cryptographic device. The cryptographic device identification information may also include a list of cryptographic services supported by the device. The signalling response message also includes the signed authentication challenge data.

[0068] The cryptographic application then transmits 412 the signalling response message, via the internet, to the browser at the IP address and port specified in the QR code.

[0069] In step 306, the browser receives the signalling response message from the cryptographic device. Accordingly, now both the browser and the cryptographic device know the connection details (IP address and port) of the other peer, and therefore a persistent peer-to-peer connection can be established. However, in the exemplary embodiment illustrated in Figures 3 and 4, the browser requires authentication of the user's identify before establishment of the persistent peer-to-peer connection.

[0070] In step 308, the browser extracts the signed authentication challenge data from the signalling response message received from the cryptographic device, and provides the signed

authentication challenge data to the web server 112. Retrieving the public key 118 associated with the user identity with which the user logged into the web page, the web server 112 verifies that the authentication challenge data has been signed with the user's private key, by considering the challenge data with the digital signature and the user's public key.

[0071] If there is a discrepancy which indicates that the private key used to sign the authentication challenge data is not complementary to the public key associated with the user's logged in identity, then the browser may elect to abort 314 the establishment of the persistent peer-to-peer connection.

[0072] Otherwise, the browser considers that the user's identity has been authenticated, and the browser 105 proceeds with negotiating session parameters 312, 414 with the cryptographic device 106 over the persistent peer-to-peer connection 108.

[0073] In accordance with the WebRTC API, the Session Description Protocol (SPD) may be used to describe the parameters of the persistent peer-to-peer connection, including the types of media to be exchanged between the browser and the cryptographic device, transport protocols, bandwidth information and other metadata, as desired to be negotiated.

[0074] Once the session parameters have been settled, the persistent peer-to-peer connection is established 316, 416 and the provision of cryptographic services to the browser, may begin.

Browser method

[0075] Fig. 5 illustrates a method 500 for obtaining cryptographic services for a browser executing a webpage. In step 504, the browser takes steps to establish the persistent peer-to-peer connection with the cryptographic device. The establishment of the persistent peer-to-peer connection may occur in response to the browser receiving user input such as the click of a webpage button, or a URL.

[0076] An exemplary method for establishing a persistent peer-to-peer connection has been described in relation to Figures 3 and 4; however, alternative methods for establishing a persistent peer-to-peer connection may be utilised. Once the peer-to-peer connection has been established, the browser awaits a user input 506 to indicate that cryptographic processing is requested.

[0077] The user input 506 can take a variety of forms. By way of non-limiting examples, the user input 506 may be in the form of a mouse-click on a webpage button or hyperlink, selecting text and right clicking to select a menu option, the use of the browser navigation icons or menu.

[0078] In step 508, the browser forms a request message in the form of a data packet which includes including data to be cryptographically processed by the cryptographic device and other information, as required, to specify the parameters of the cryptographic processing. It is envisaged that in some cases, it will not be necessary to specify the parameters of the cryptographic processing, in particular, in situations where the cryptographic device is configured to only provide one processing function, or where the processing function to be performed by the device has already been specified during the establishment of the persistent peer-to-peer connection.

[0079] In step 510, the browser waits for and receives a response message from the cryptographic device over the peer-to-peer connection. The response message contains the result of the cryptographic processing of the data by the cryptographic device. In response to receiving this cryptographic result, the browser provides the cryptographic result to the webpage 512. Depending upon the configuration of the webpage, the browser provides the cryptographic result to the webpage via various means, including, but not limited to, updating the webpage to display the cryptographic result, embedding or entering the cryptographic result into the code of the webpage, entering the result into a web form input of the web page, providing the result as an AJAX HTTP request, or a HTML parameter value. Additionally, or alternatively, the browser may provide the cryptographic result to the server 112 hosting the webpage, which may result in the server 112 providing a revised or new webpage to be displayed in the browser 105. Alternatively, the cryptographic result may remain local to the webpage, and not be transmitted to the webserver or other applications.

[0080] Following, step 512, the method of the browser returns to step 506 in which the browser waits to receive further input from the user. Notably and advantageously, the peer-to-peer connection is persistent, which means it remains established and open for multiple iterations of steps 506 to 512. Therefore, further requests can be processed with minimal latency, and with less user input.

Device method

[0081] Fig. 6 illustrates a method 600 performed by the cryptographic device 106, according to one aspect of the present disclosure.

[0082] In step 602, the cryptographic device 106 establishes a persistent peer-to-peer connection 108 with the web browser 105. An exemplary method for establishing a persistent peer-to-peer connection has been described in relation to Figures 3 and 4; however, alternative methods for establishing connection 108 may be utilised.

[0083] In step 604, the cryptographic device 106 waits to receive a request message from the browser 105 over the persistent peer-to-peer connection 108. The request message may be in the form of a data packet containing an indication of the cryptographic function requested to be performed. The data packet may also contain data to which the cryptographic function is to be applied, or an indication of such data, and additional information as required by a particular embodiment. The format and contents of the request message may be configured during the establishment of the peer-to-peer connection, or may be preconfigured into the browser and the cryptographic device.

[0084] In step 606, cryptographic device 106 analyses the request message transmitted by the browser over the peer-to-peer connection to determine the cryptographic function to be applied, and the data to which that function should be applied. Depending upon the configuration of the cryptographic device, the device may also seek confirmation from the user to proceed with performing the cryptographic function as requested. The device may seek confirmation by displaying the details of the cryptographic function request on a display of the device, and then wait to receive input from the user to thereby confirm that the cryptographic processing should proceed.

[0085] The device 106 then selects an appropriate cryptographic key 114 from the memory storage 212. In embodiments where a plurality of cryptographic keys are stored in memory storage 212, the selection of the appropriate key may depend upon the user identity under which the persistent peer-to-peer connection was established, the type of cryptographic processing requested by the browser, the type of data to be cryptographically processed, or other factors.

[0086] The device 106 then performs cryptographic processing 606 on the determined data, using the selected cryptographic key, to produce a cryptographic result. In step 608, the

cryptographic result is then packaged by the device into a response message which is transmitted back to the browser via the persistent peer-to-peer connection.

[0087] The method of the device then returns to step 604, whereby the device waits for further request messages from the browser to be received over the persistent peer-to-peer connection.. Notably and advantageously, the peer-to-peer connection which was established in step 602 is persistent, which means that it remains established through multiple iterations of steps 604, 606 and 608.

Transport layer encryption

[0088] To ensure transmissions between the browser and the cryptographic device are secure, a transport layer encryption protocol may be applied to messages transmitted over the persistent peer-to-peer connection. An exemplary transport layer encryption protocol is Datagram Transport Layer Security (DTLS), which is designed to protect data privacy and prevent eavesdropping and tampering. It will be appreciated, however, that many other transport layer encryption protocols that are compatible with the Internet Protocol may be used.

[0089] Transport layer encryption may be applied to request messages transmitted by the browser to the cryptographic device. Furthermore, transport layer encryption may be applied to response messages transmitted by the cryptographic device to the browser. Accordingly, the cryptographic result embedded in the response message, may be further encrypted due to the application of transport layer encryption.

Persistent peer-to-peer connection

[0090] Fig. 7 is a message flow diagram 700 which illustrates request and response messages being transmitted between the browser 105 and the cryptographic device 106, over an established peer-to-peer connection 108, in accordance with an aspect of this disclosure. At the establishment of the persistent peer-to-peer connection 108, there may be a series of messages 705 transmitted between the browser and the cryptographic device which negotiate the parameters of the communication session.

[0091] Messages 706 and 708 are a request and response pair, in which the browser has requested cryptographic processing from the device, and has received a cryptographic response from the cryptographic device. Similarly, messages 710 and 712 are another request and

response pair, in which the browser has requested further cryptographic processing from the device, and has received a further cryptographic response from the cryptographic device.

[0092] Advantageously, multiple request and response pairs may be transmitted over the persistent peer-to-peer connection while established, as illustrated by request and response messages 714 and 716. Advantageously, the browser need not establish a connection each time cryptographic processing is required.

[0093] Eventually, the browser may determine that the services of the cryptographic device are no longer required, for example, if the user logs out of the webpage, or takes action to sever the persistent peer-to-peer connection. The browser may then take steps to close the persistent peer-to-peer connection, thus freeing up resources associated with the connection. If the peer-to-peer connection is a WebRTC connection, the connection maybe closed by invoking the RTCPeerConnection.close() method, which terminates agents associated with the WebRTC connection. A close message 718 may be transmitted, which triggers the cryptographic device to close the connection, and to cease listening for further request messages via the connection.

[0094] It is understood that a peer-to-peer connection may close unexpectedly, due to a fault at the browser or at the cryptographic device, or a network fault. To ameliorate the effect of a closure of the connection, and to enable fast reestablishment of a connection, the browser may store the connection details (e.g. IP address and port) of the cryptographic device so that the connection may be reactivated through the renegotiation of session parameters.

Embodiment – Browser connecting

[0095] An embodiment of the methods as described in Figures 5 and 6, will now be illustrated with reference to Figs. 8a-f.

[0096] Figs. 8a-f illustrates a browser 802 displaying webpages 803a-f.. Webpages 803a-f are illustrative of one or more webpages of a website in which users can post messages to a message board. Various forms of message boards exist, including those within social media platforms. Message boards enable users to post content, which is attributed to the user and viewable or accessible by other parties.

[0097] The browser task bar 804 is located at the top of the browser and provides navigational control to the user of the browser. Located in the middle of the webpage 803a is a web form

element 806a in the form of a text box. The user may enter data into this text box in the usual manner.

[0098] To the right of the webpage 803a, is an interface 808a which indicates whether the browser is connected to a cryptographic device via a persistent peer-to-peer connection. As indicated by the unlocked padlock icon 809, the browser illustrated in Fig. 8 is not currently connected to a cryptographic device via a persistent peer-to-peer connection. A Connect button 810, is provided under the padlock icon 809. A user may click the Connect button 810 to trigger the browser to initiate the establishment of a persistent peer-to-peer connection to a cryptographic device.

[0099] Fig 8b illustrates the browser 802 displaying a modified version 803b of webpage 803a, as a result of the user clicking the Connect button 810 on webpage 803a. In the example illustrated in Fig 8b, the browser 802 displays a Scan to Connect box 812 in the middle of webpage 803b. This box contains a QR code 814 which encodes signalling information sufficient to initiate the establishment of a persistent peer-to-peer connection between the browser 802 and a cryptographic device.

[0100] The further steps taken by the browser and the cryptographic device to establish the persistent peer-to-peer connection have been described with regards to Figures 3 and 4.

Embodiment - Signing

[0101] Fig 8c illustrates the webpage 803c, executing in browser 802, upon establishment of the persistent peer-to-peer connection between the browser 802 and the cryptographic device. The locked padlock icon 809c provides a visual representation to the user that the peer-to-peer connection is currently established.

[0102] It can be seen that the user has entered the text “Hello world” 807 into web form element 806c. To post the message directly to the message board, so that other users may see the message, the user may click on the Post button 819c. However, the user may want to provide assurance that the message 807 to be posted to the message board originated from that user, and that the message has not been altered before being posted to the message board. Accordingly, the user may elect to sign the message by calculating a signature over the message contents. To achieve this, the user clicks on the Sign button 818, as indicated by the shading pattern of button 818. In response, the browser packages the user’s message 807 into a request for cryptographic

processing by signing, and transmits the request to the cryptographic device over the peer-to-peer connection. The cryptographic device applies a digital signature to the user's message 807, for example, by applying a one-way hash of the user's message using a public/private key pair stored in memory storage 212, in accordance with the steps 604 to 608 of Fig. 6, and transmits the digital signature to the browser in a response message.

[0103] The browser receives the digital signature and, in accordance with the example illustrated in Fig. 8d, provides the signature to the web page. The webpage displays the digital signature 817 below the user's message 807 in the web form element 806d. Alternatively, a browser in accordance with this disclosure, may not display the digital signature within the browser, but may embed the digital signature information within data associated with the webpage. The browser may visually depict that the user's message 807 has been signed through the use of different colouring, shading, location upon the webpage, indicative icons or the like.

[0104] It is noted that, the browser may initiate the message signing process upon posting the message, as a matter of course, or as dependent upon the configuration of the webpage or the user. Furthermore, a browser in accordance with this disclosure, may initiate the posting of the user's message 807 upon signing the message, as a matter of course, or as dependent upon the configuration of the webpage or the user.

[0105] Fig. 8e illustrates the browser 802 with the user's message 821 and its associated signature 822 posted to the message board.

Embodiment – Encrypting

[0106] In addition to the option of signing the message, as provided by the Sign button 818, the user has the option of encrypting the message 807 for decryption by communication partner 120. Such message encryption, as performed by Author C, is illustrated in relation to message 826.

[0107] To encrypt the message 807, the user clicks on the Encrypt button 820. In response, the browser packages the user's message 807 into a request for cryptographic processing by encryption, and transmits the request to the cryptographic device over the persistent peer-to-peer connection. The cryptographic device encrypts the user's message 807 using the communication partner's public key stored on the cryptographic device, for example in accordance with the steps 604 to 608 of Fig. 6, and transmits the encrypted message to the browser, as a cryptographic result, in a response message.

[0108] The browser receives the encrypted message and provides the cryptographic result to the webpage. As exemplified by message 826, the webpage may display the encrypted message in association with the user's identity.

Embodiment - Verifying

[0109] Figures 8c-e also illustrate message verification functionality, according a further aspect of the present disclosure. As indicated by status box 808c-e in Figs. 8c-e, a peer-to-peer connection remains established between the browser and a cryptographic device. A Verify button 827 is collocated with a message 824 posted by exemplary author, Author B. Message 824 is also collocated with digital signature 825, which provides *prime facia* indication that message 824 has been signed by Author B.

[0110] A user of browser 802 may use the cryptographic device to verify that the digital signature 825 associated with message 824 has been produced by Author B. In the exemplary scenario as illustrated in Fig 8a-e, the user of browser 802 and the cryptographic device is a communication partner of Author B, and has exchanged public keys with Author B via the Public Key Infrastructure. Accordingly, the cryptographic device 106 stores two keys associated with Author B: a public key to be used when transmitting information to Author B; and a private key to be used when receiving information from Author B. The public key which is complementary to the stored private key has been provided to Author B, and is used by Author B to calculate a signature 825 of message 824.

[0111] Accordingly, when the user clicks on the Verify button 827 collocated with message 824 and digital signature 825, the browser forms a request message containing message 824, digital signature 825, information identifying Author B (such as a username), and an indication that the request pertains to a verification function. The browser transmits this request message to the cryptographic device via the established peer-to-peer connection.

[0112] Upon receipt of the request message, the cryptographic device determines the private key associated with Author B, and uses the private key to determine whether the digital signature 825 transmitted in the request message, has been produced over message 824 and Author B's private key. The cryptographic device then forms a response message, to be transmitted to the browser over the peer-to-peer connection, including a cryptographic result which either verifies the validity of digital signature 825, or refutes the validity of digital signature 825, in accordance with the cryptographic device's determination.

[0113] The browser provides the cryptographic result to the webpage. Depending upon the functionality coded in the webpage, the webpage may indicate a verified signature through a change in colour, shading, collocated icons or otherwise. Similarly, a webpage may indicate a refuted signature by changing the appearance of the message 824 and digital signature 825, or by removal of the same.

Embodiment - Decrypting

[0114] Figures 8c-e also illustrate message decryption functionality, according a further aspect of the present disclosure. As indicated by status box 808c-e in Figs. 8c-e, a persistent peer-to-peer connection remains established between the browser and a cryptographic device. A Decrypt button 828 is collocated with a message 826 posted by exemplary author, Author C.

[0115] Message 826 has been encrypted using asymmetric encryption prior to posting by Author C, using a public cryptographic key associated with the user. In order for the user of the browser 802 to view the unencrypted contents of message 826, it will be necessary to decrypt message 826 using the user's private cryptographic key.

[0116] In the exemplary scenario as illustrated in Fig 8c-e, the user of browser 802 and the cryptographic device is a communication partner of Author C, and has exchanged public keys with Author C via the Public Key Infrastructure. Accordingly, the cryptographic device currently stores a public key associated with Author C, and a private key for communication with Author C. The public key which is complementary to the private key for communication with Author C has been provided to Author C, and is used by Author C to produce encrypted message 826.

[0117] Accordingly, when the user clicks on the Decrypt button 828 collocated with encrypted message 826, the browser forms a request message containing encrypted message 826, information identifying Author C (such as a username), and an indication that the request pertains to a decryption function. The browser transmits this request message to the cryptographic device via the established peer-to-peer connection.

[0118] Upon receipt of the request message, the cryptographic device retrieves from the memory source 812 a public cryptographic key associated with Author C and suitable to decrypt encrypted message 826. The cryptographic device then decrypts encrypted message 826 by applying the public cryptographic key, and returns the decrypted message, as a cryptographic result, to the browser, in a response message, via the persistent peer-to-peer connection 108.

[0119] The browser provides the cryptographic result to the webpage. Depending upon the functionality coded in the webpage, the webpage may display the decrypted message from Author C in place of the encrypted message 826. The cryptographic result may remain local to the webpage, and not transmitted to the webserver or other applications.

Signing, Verifying and Decrypting Files and other data

[0120] In relation to Fig 8a-e, there has been described methods of signing text based data (i.e. messages posted to a message board), verifying signatures associated with text based data, encrypting and decrypting text based message; however, the above described techniques may also have application in signing, verifying, encrypting and decrypting data other than text messages posted to a message board.

[0121] In particular, the methods and devices described herein may be applied to applications such as the signing of documents of certificate, transcripts, medical prescriptions, photographs and any data to which encryption and/or signatures may be applied using a cryptographic key.

Embodiment – Uploading Files

[0122] A cryptographic device in accordance with another aspect of the present disclosure, may be configured to transmit confidential information from the cryptographic device to the browser securely. For example, Fig. 8f illustrates browser 802 displaying a further version of webpage 803f, which enables the uploading of encrypted or signed files. The locked padlock icon 809f indicates that a peer-to-peer connection has been established between the browser and a cryptographic device associated with Author A. The "Upload signed file" button 830 provides the user of the browser with the functionality to provide a file signature for a file, whereby the file signature may be verified by the user's communication partner 120. This functionality includes applying a cryptographic key to the file, and uploading the file and its associated signature from the cryptographic device to the browser via the persistent peer-to-peer connection.

[0123] To enable this functionality, the following steps may be taken. The user 802, as Author A, selects a file to be uploaded and clicks on the "Upload signed file" button 830. The browser transmits a request message, which includes a file reference and a request for the creation of a file signature, to the cryptographic device 106 via the peer-to-peer connection 108. The cryptographic device 108 locates and retrieves the file from memory source 212, and applies the

public key of communication partner 120 to the file contents to calculate a file signature. The cryptographic device transmits the file and its associated signature, as a cryptographic result, to the browser, in a response message, via the peer-to-peer connection.

[0124] The browser then provides the cryptographic result to the webpage. Depending upon the configuration of the webpage, the browser may then upload the file and its associated signature to a web server, and may provide an indication of the uploaded file upon the webpage. For example, text 834 indicates the previous upload of a file entitled 'Academic transcript (Author A).pdf". A file signature has been created by the cryptographic device for this file 834, as indicated by the tick icon 838.

[0125] The provision of file signatures with uploaded files enables a communication partner of the uploading user to be able to verify that the file originated from the uploading user, and has not been altered since uploading. The communication partner 120 applies the communication partner's private key to the file to determine whether the associated signature verifies the file.

[0126] Furthermore, file encryption functionality can be provided in much the same way as the generation of file signatures as described above. The user 102, as Author A, selects a file to be uploaded and clicks on the "Upload encrypted file" button 832. The browser transmits a request message, which includes a file reference and a request for an encryption of the file, to the cryptographic device 106 via the peer-to-peer connection 108. The cryptographic device 108 locates and retrieves the file from memory source 212, and applies the communication partner's public cryptographic key to the file contents to encrypt the file. The cryptographic device transmits the encrypted file to the browser, as a cryptographic result, in a response message, via the persistent peer-to-peer connection.

[0127] The browser provides the cryptographic result to the webpage. Depending upon the configuration of the webpage, the browser may then upload the encrypted file to a web server, and may provide an indication of the uploaded encrypted file upon the webpage. For example, text 836 indicates the previous upload of an encrypted file entitled 'Curriculum Vitae (Author A).pdf". This file has been encrypted by the cryptographic device, as indicated by the padlock icon 840.

[0128] The communication partner 120 may apply the communication partner's private key to the file to decrypt the file.

[0129] It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the above-described embodiments, without departing from the broad general scope of the present disclosure. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

[0130] Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

CLAIMS:

1. A method for obtaining cryptographic services for a browser executing a webpage, the method comprising:

establishing a persistent peer-to-peer connection over a wireless Internet Protocol communication network between the browser and a cryptographic device;

in response to receiving user input to the webpage, transmitting, by the browser, data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device, for cryptographic processing of the data by the cryptographic device using a cryptographic key stored on the cryptographic device to produce a cryptographic result; and

receiving, by the browser, the cryptographic result over the persistent peer-to-peer connection from the cryptographic device, and providing the cryptographic result to the webpage,

wherein establishing the persistent peer-to-peer connection comprises the steps of,

signalling, by the browser, signalling information including challenge information,

receiving, by the browser, response information from the cryptographic device, the response information including a challenge response based on the challenge information.

2. The method of claim 1, further comprising:

receiving, by the cryptographic device, from the browser, data via the persistent peer-to-peer connection between the browser and the cryptographic device;

performing, by the cryptographic device, the cryptographic function on the data using the cryptographic key stored on the cryptographic device, to produce the cryptographic result; and

transmitting, by the cryptographic device, the cryptographic result to the browser, over the persistent peer-to-peer connection.

3. The method of claim 1 or 2, wherein the persistent peer-to-peer connection remains established over multiple iterations of the steps of:

transmitting, by the browser, the data over the persistent peer-to-peer connection to the cryptographic device; and

receiving, by the browser, the cryptographic result over the persistent peer-to-peer connection from the cryptographic device.

4. The method of claim 1, further comprising sending confidential data stored on the cryptographic device, from the cryptographic device to the browser.

5. The method of any one of the preceding claims, wherein the cryptographic processing of the data by the cryptographic device comprises signing or encrypting the data with the cryptographic key to produce the cryptographic result.

6. The method of any one of the preceding claims, wherein the browser embeds the cryptographic result in the webpage.

7. The method of any one of the preceding claims, wherein the browser provides the cryptographic result to a server hosting the webpage.

8. The method of claim 7, wherein the browser receives an updated webpage from the server hosting the webpage, in response to providing the cryptographic result to the server.

9. The method of any one of the preceding claims, wherein the signalling information is necessary to establish a peer-to-peer connection, and the response information is necessary to establish a peer-to-peer connection.

10. The method of claim 9, wherein the signalling information is signalled via a communication channel other than the peer-to-peer connection.

11. The method of claim 9 or 10, wherein signalling the signalling information comprises displaying a QR code which encodes the signalling information.

12. The method of any one of the preceding claims, wherein the method further comprises injecting, by the browser, software that defines the method into the webpage.

13. The method of claim 9, wherein the signalling information includes user device identification information and the challenge information and the cryptographic device signs the challenge information by applying an authentication key to the challenge information to produce the challenge response.

14. The method of claim 9, wherein the response information includes cryptographic device identification information and the challenge response.

15. The method of any one of the preceding claims, wherein the data is indicative of data entered by a user of the browser into an input field of the webpage.

16. The method of any one of the preceding claims, wherein establishing a persistent peer-to-peer connection between the browser and the cryptographic device occurs in response to receiving establishment input from the user of the user device.

17. A method of obtaining cryptographic services for a browser executing a webpage on a user device, the method comprising:

establishing a persistent peer-to-peer connection between the browser and a cryptographic device;

in response to receiving user input to the webpage, transmitting, by the browser, data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device;

applying, by the cryptographic device, a cryptographic function to the data using a cryptographic key stored on the cryptographic device, to produce a cryptographic result; and

transmitting, by the cryptographic device, the cryptographic result to the browser, over the persistent peer-to-peer connection,

wherein establishing the persistent peer-to-peer connection comprises the steps of,

signalling, by the browser, signalling information including a challenge information,

receiving, by the cryptographic device, the signalling information,

transmitting, by the cryptographic device, response information including a challenge response based on the challenge information.

18. A method of providing cryptographic services to a browser executing a webpage, the method comprising:

establishing a persistent peer-to-peer connection between the browser and a cryptographic device;

receiving data, from the browser, via a persistent peer-to-peer connection between the browser and the cryptographic device;

performing, by the cryptographic device, a cryptographic function on the data using a cryptographic key stored on the cryptographic device, to produce a cryptographic result; and

transmitting, by the cryptographic device, the cryptographic result to the browser, over the persistent peer-to-peer connection,

wherein establishing the persistent peer-to-peer connection comprises the steps of,

receiving, from the browser, signalling information including challenge information,

transmitting, by the cryptographic device, response information including a challenge response based on the challenge information.

19. A browser executing a webpage on a user device, the browser configured to:

establish a persistent peer-to-peer connection between the browser and a cryptographic device;

in response to receiving a user input to the webpage, transmit data indicated by the user input over the persistent peer-to-peer connection to the cryptographic device for cryptographic processing of the data using a cryptographic key stored on the cryptographic device, to produce a cryptographic result; and

receive the cryptographic result over the persistent peer-to-peer connection from the cryptographic device,

wherein establishing the persistent peer-to-peer connection comprises the steps of,

signalling signalling information including challenge information,

receiving response information including a challenge response based on the challenge information.

20. A cryptographic device configured to:

establish a persistent peer-to-peer connection between a browser executing a webpage, and an cryptographic application executing on the cryptographic device;

receive data from the browser, via the persistent peer-to-peer connection;

perform a cryptographic function on the received data, using a cryptographic key stored on the cryptographic device, to produce an cryptographic result;

transmit the cryptographic result to the browser, via the persistent peer-to-peer connection,

wherein establishing the persistent peer-to-peer connection comprises the steps of,

receiving signalling information including challenge information,

transmitting response information including a challenge response based on the challenge information.

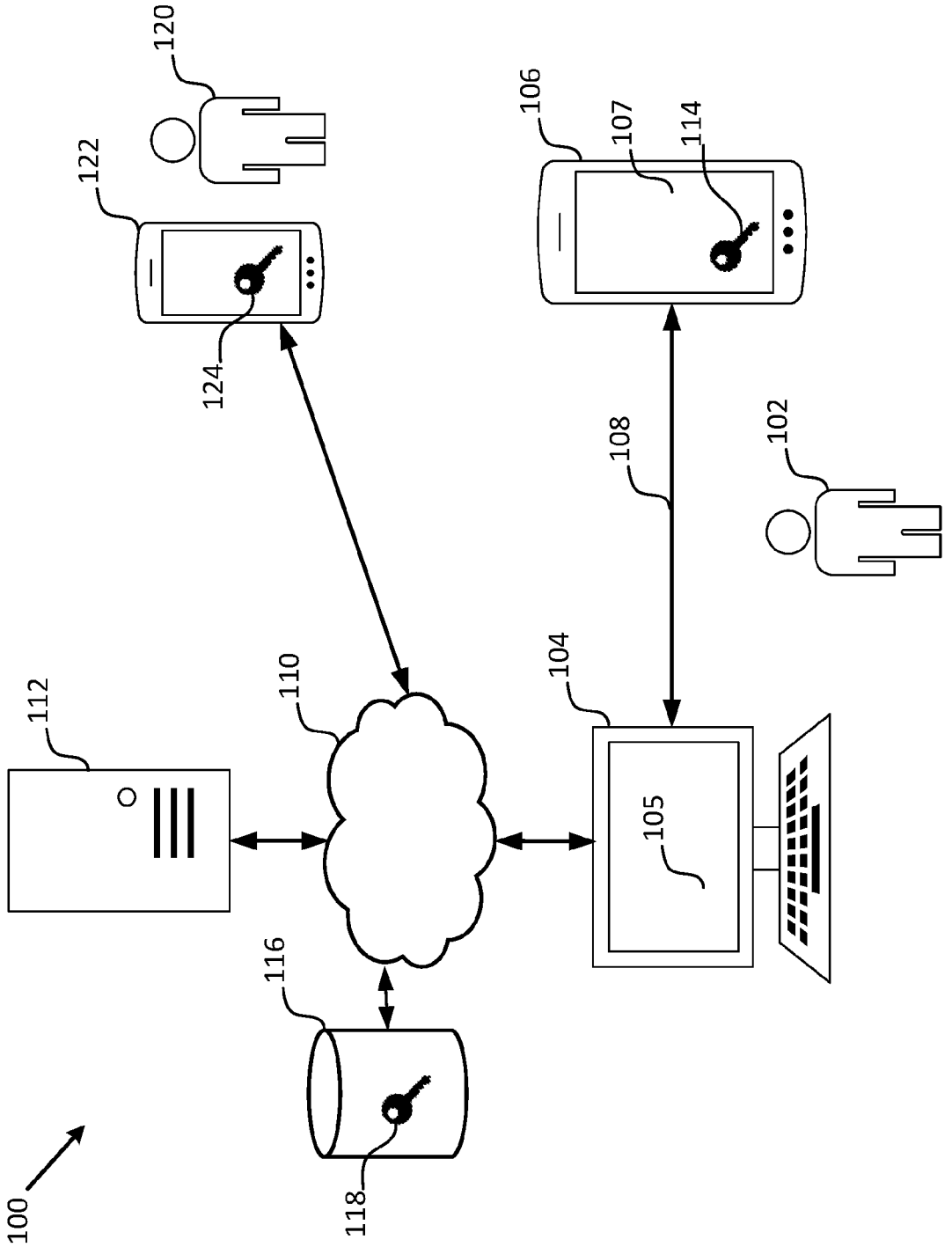

Fig. 1

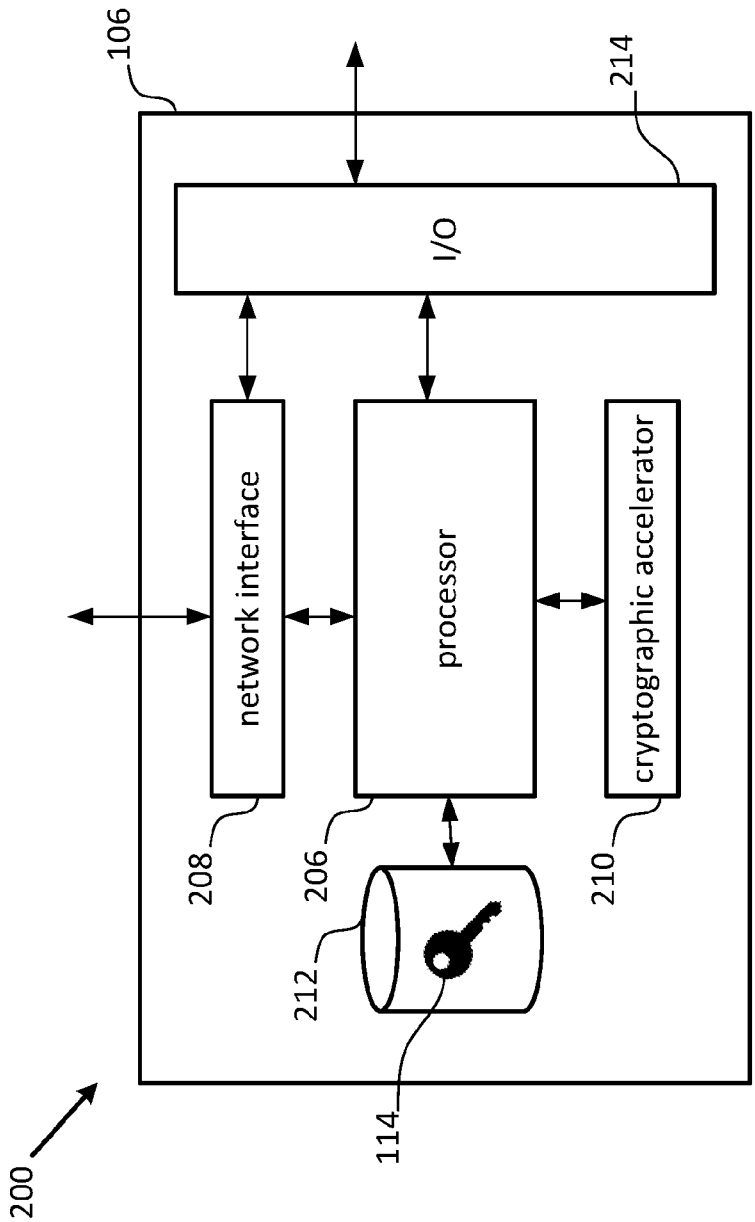
106
214
I/O
network interface
processor
cryptographic accelerator
208
206
210
212
114
200

Fig. 2

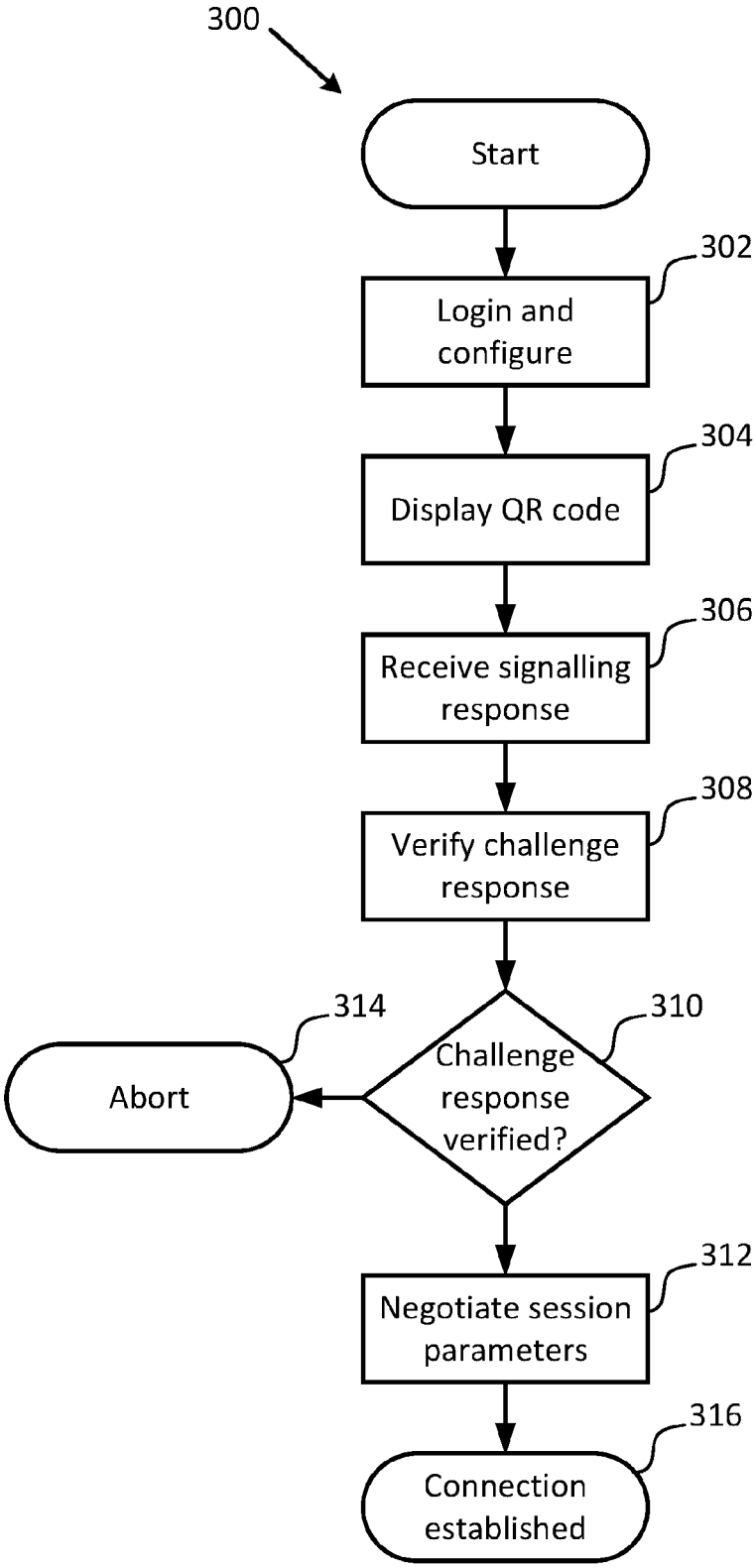
300
Start
302
Login and configure
304
Display QR code
306
Receive signalling response
308
Verify challenge response
310
Challenge response verified?
314
Abort
312
Negotiate session parameters
316
Connection established

Fig. 3

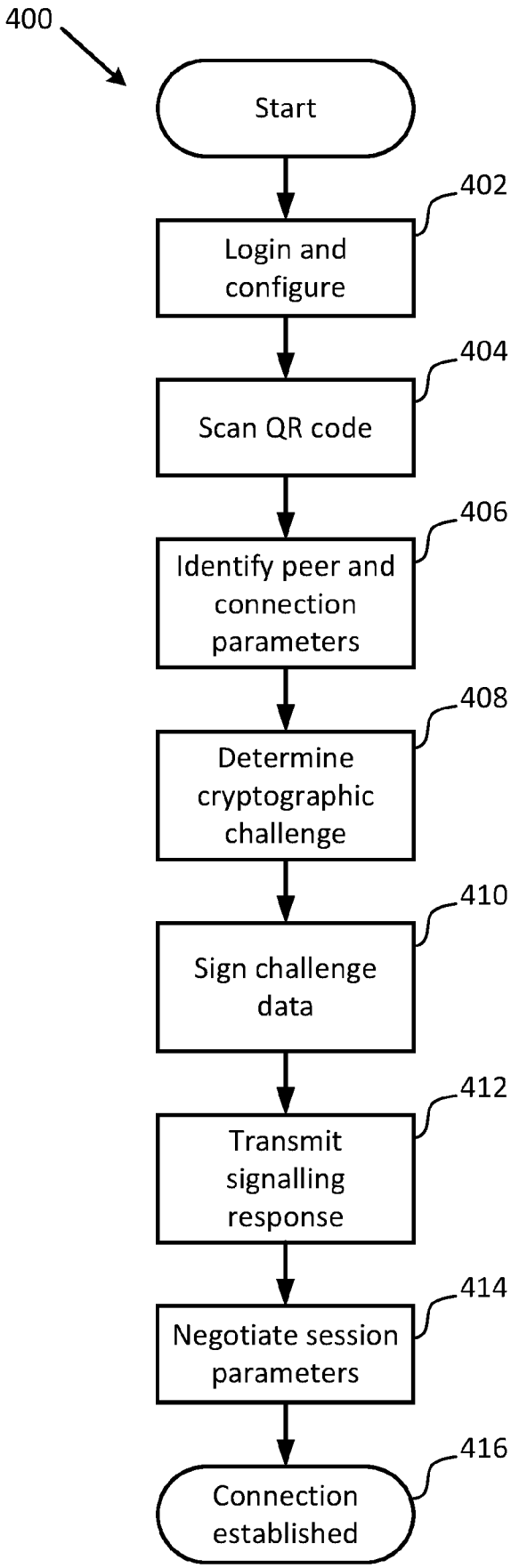
400
Start
402
Login and configure
404
Scan QR code
406
Identify peer and connection parameters
408
Determine cryptographic challenge
410
Sign challenge data
412
Transmit signalling response
414
Negotiate session parameters
416
Connection established

Fig. 4

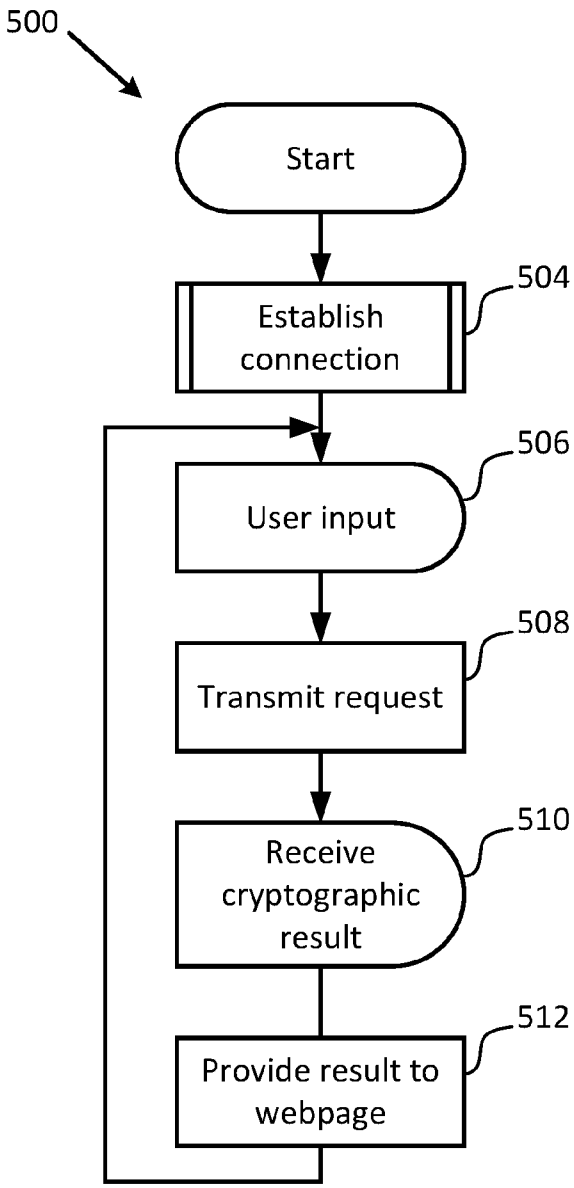
500
Start
Establish connection
504
User input
506
Transmit request
508
Receive cryptographic result
510
Provide result to webpage
512

Fig. 5

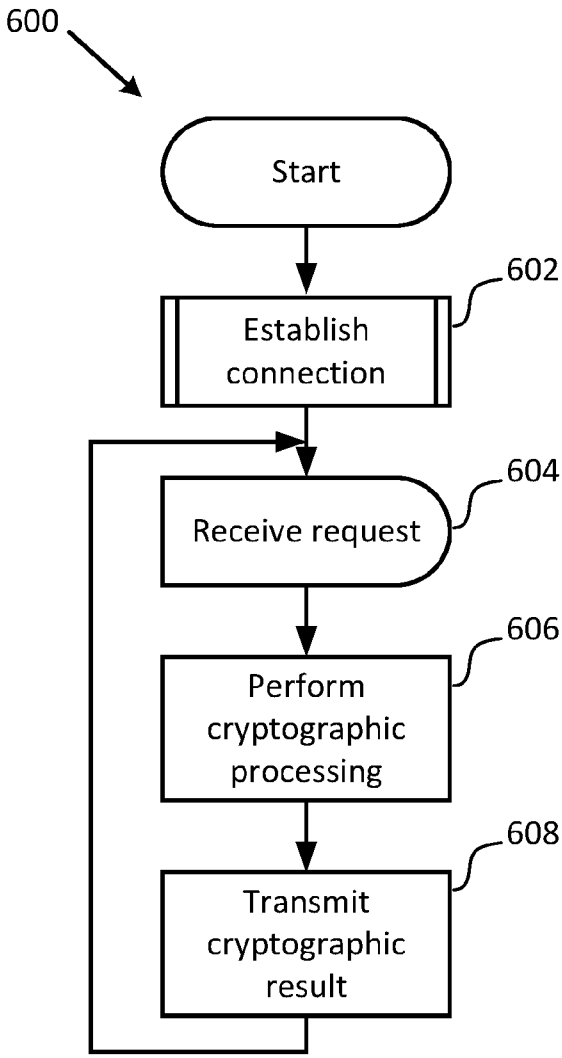
600
Start
602
Establish connection
604
Receive request
606
Perform cryptographic processing
608
Transmit cryptographic result

Fig. 6

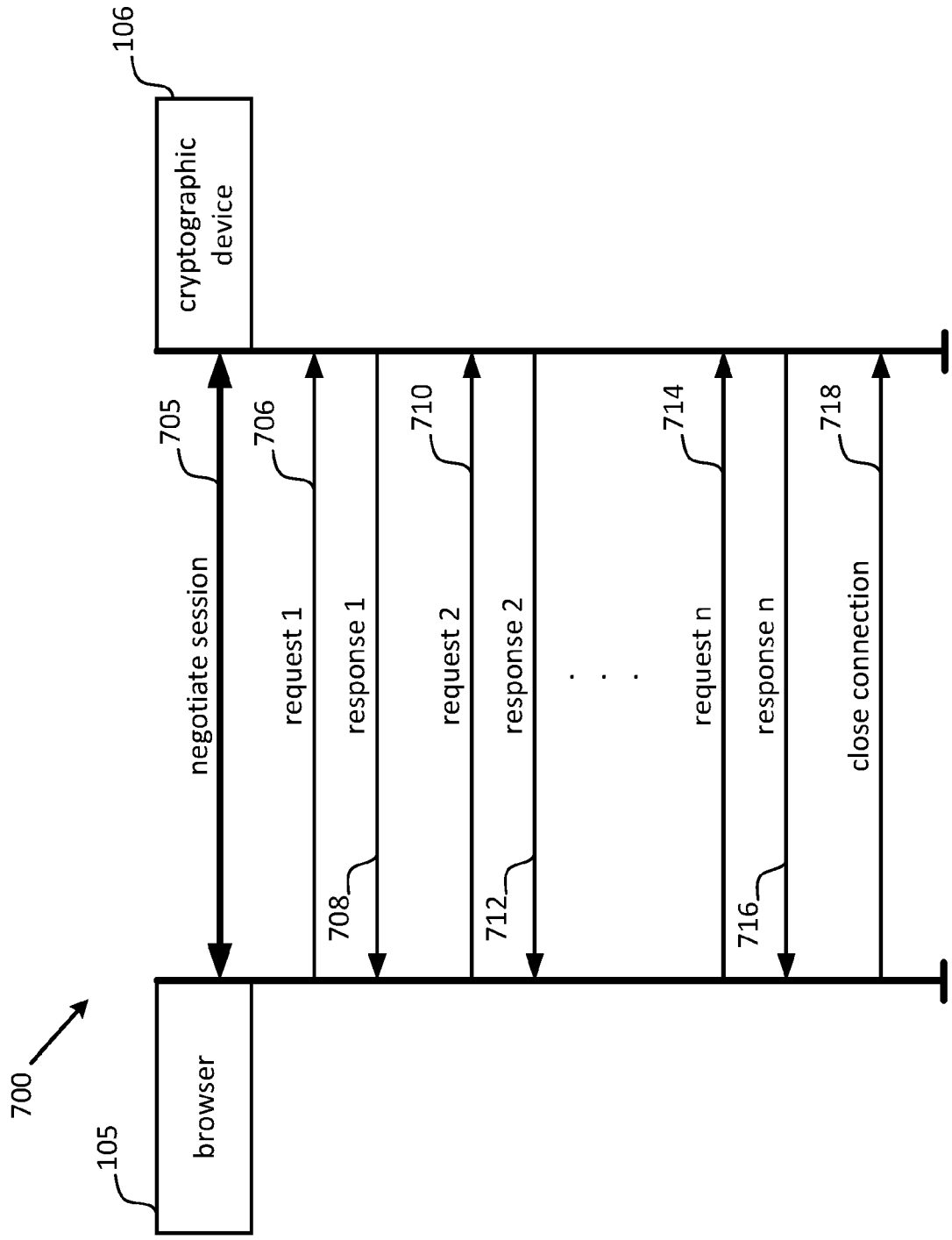
106
cryptographic device
705
negotiate session
706
request 1
708
response 1
710
request 2
712
response 2
. . .
714
request n
716
response n
718
close connection
700
105
browser

Fig. 7

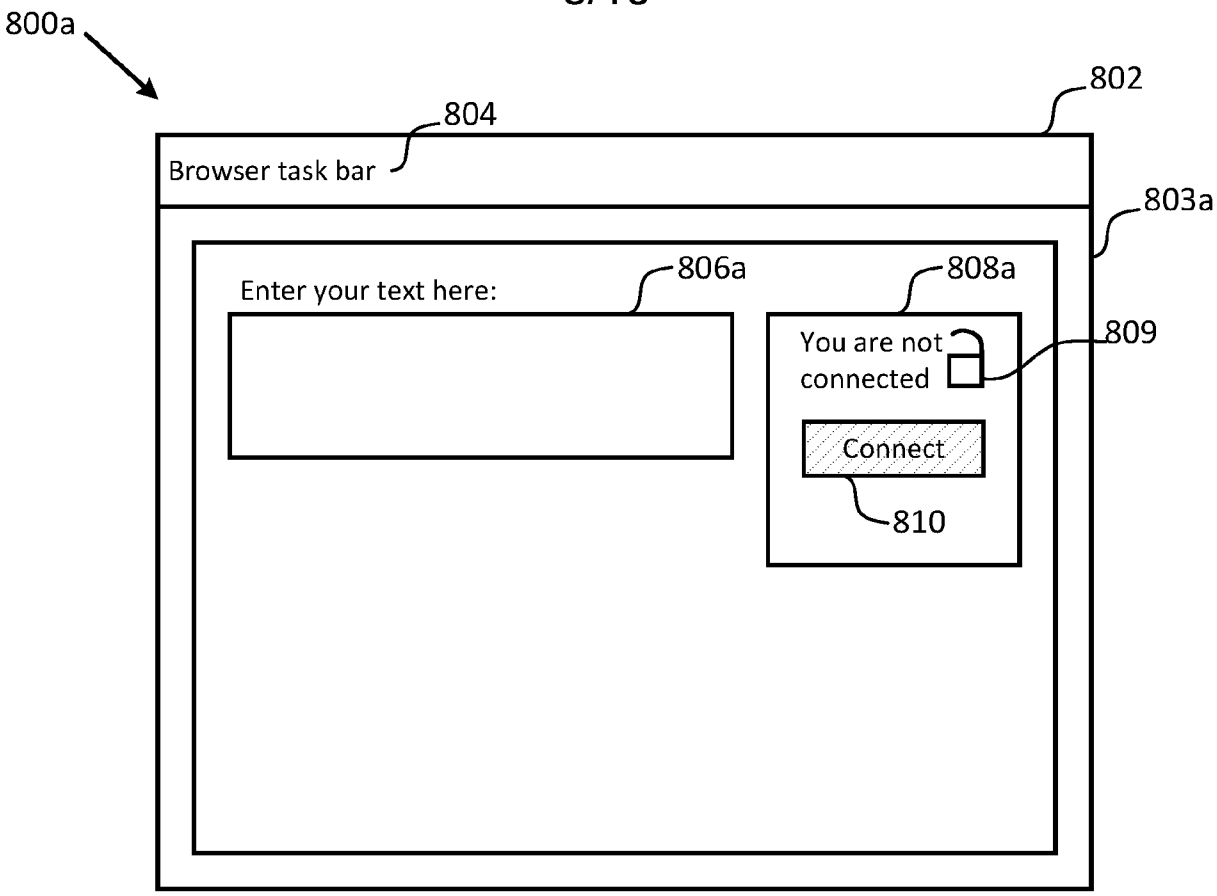
800a
802
804
Browser task bar
803a
Enter your text here:
806a
808a
You are not connected
809
Connect
810

Fig. 8a

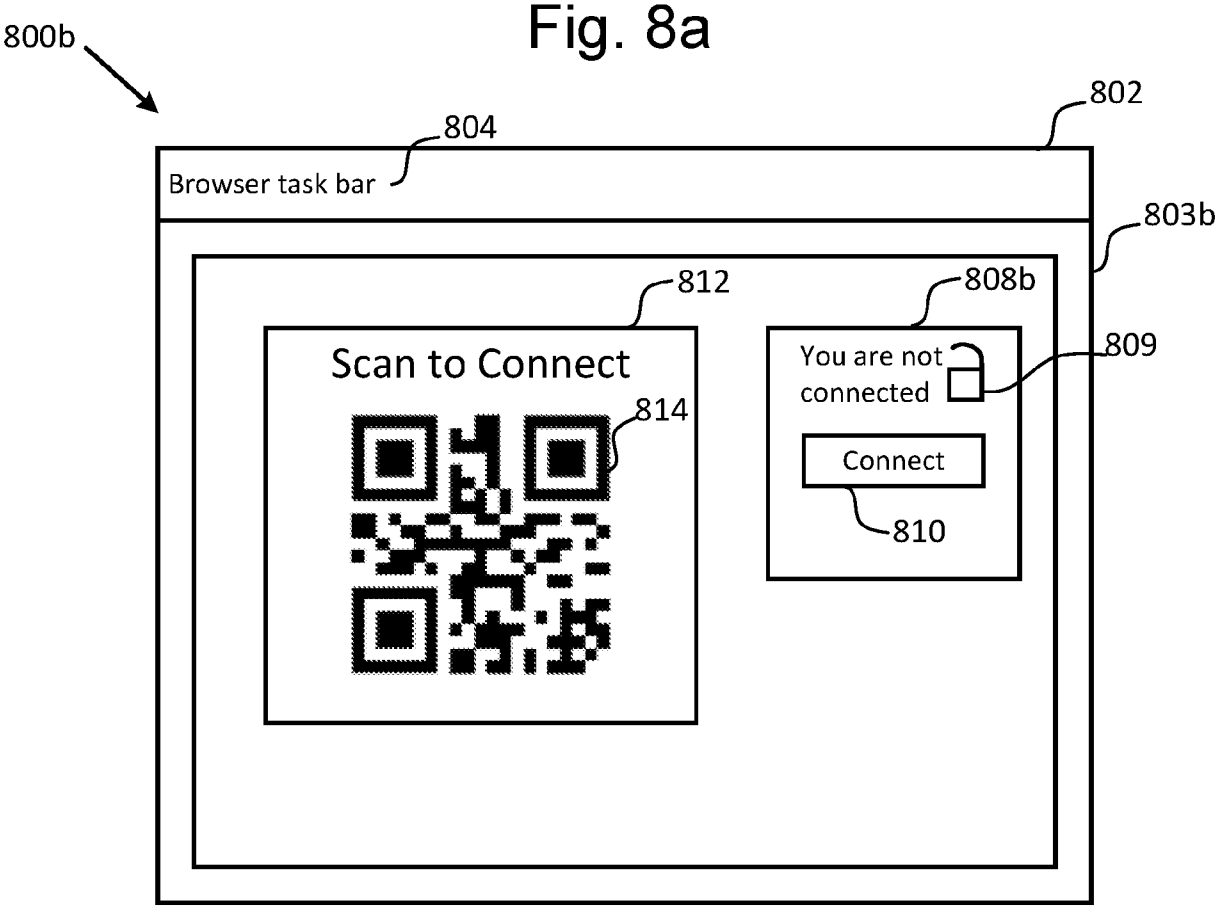
800b
802
804
Browser task bar
803b
812
808b
Scan to Connect
814
You are not connected
809
Connect
810

Fig. 8b

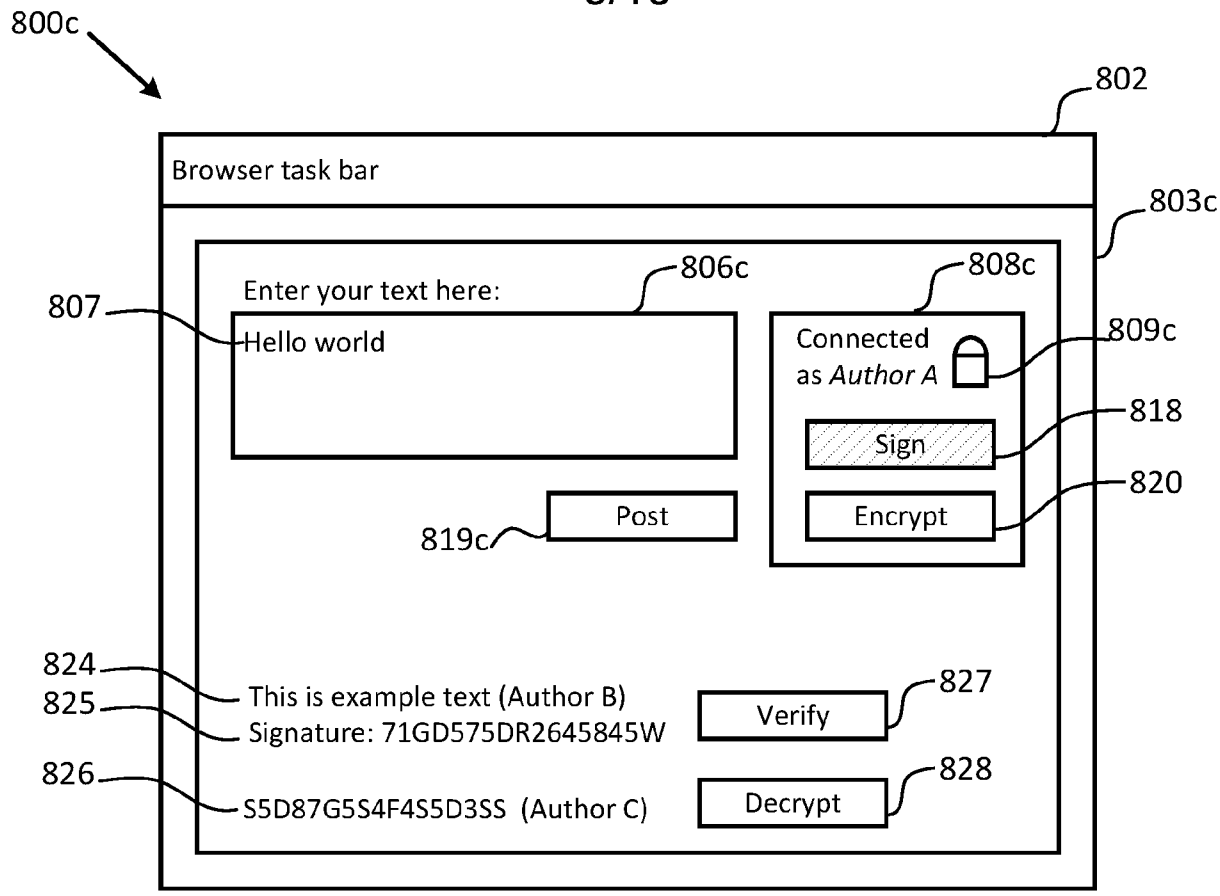
800c
802
Browser task bar
803c
Enter your text here:
806c
808c
807
Hello world
Connected as Author A
809c
818
Sign
820
Post
819c
Encrypt
824
This is example text (Author B)
825
Signature: 71GD575DR2645845W
827
Verify
826
S5D87G5S4F4S5D3SS (Author C)
828
Decrypt

Fig. 8c

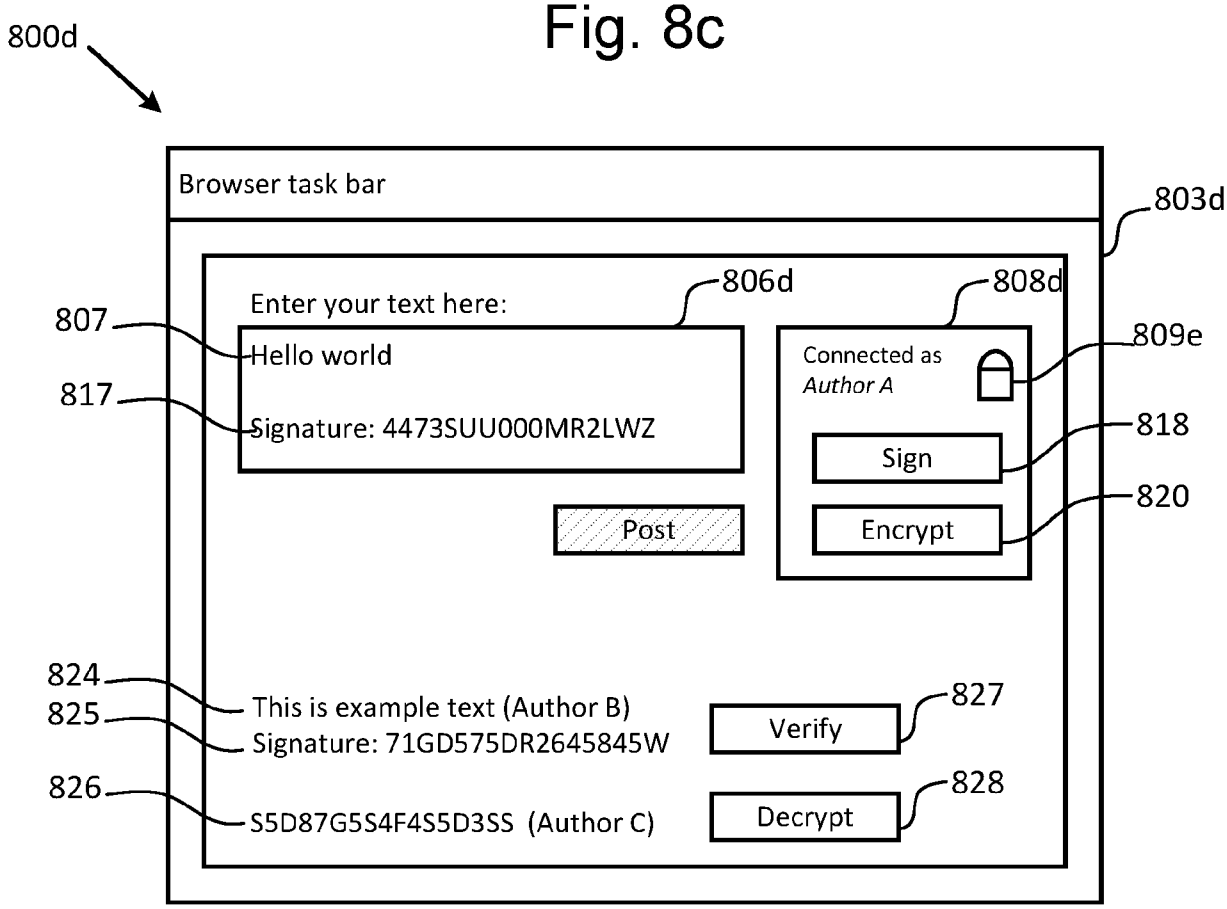
800d
Browser task bar
803d
Enter your text here:
806d
808d
807
Hello world
817
Signature: 4473SUU000MR2LWZ
Connected as Author A
809e
818
Sign
820
Post
Encrypt
824
This is example text (Author B)
825
Signature: 71GD575DR2645845W
827
Verify
826
S5D87G5S4F4S5D3SS (Author C)
828
Decrypt

Fig. 8d

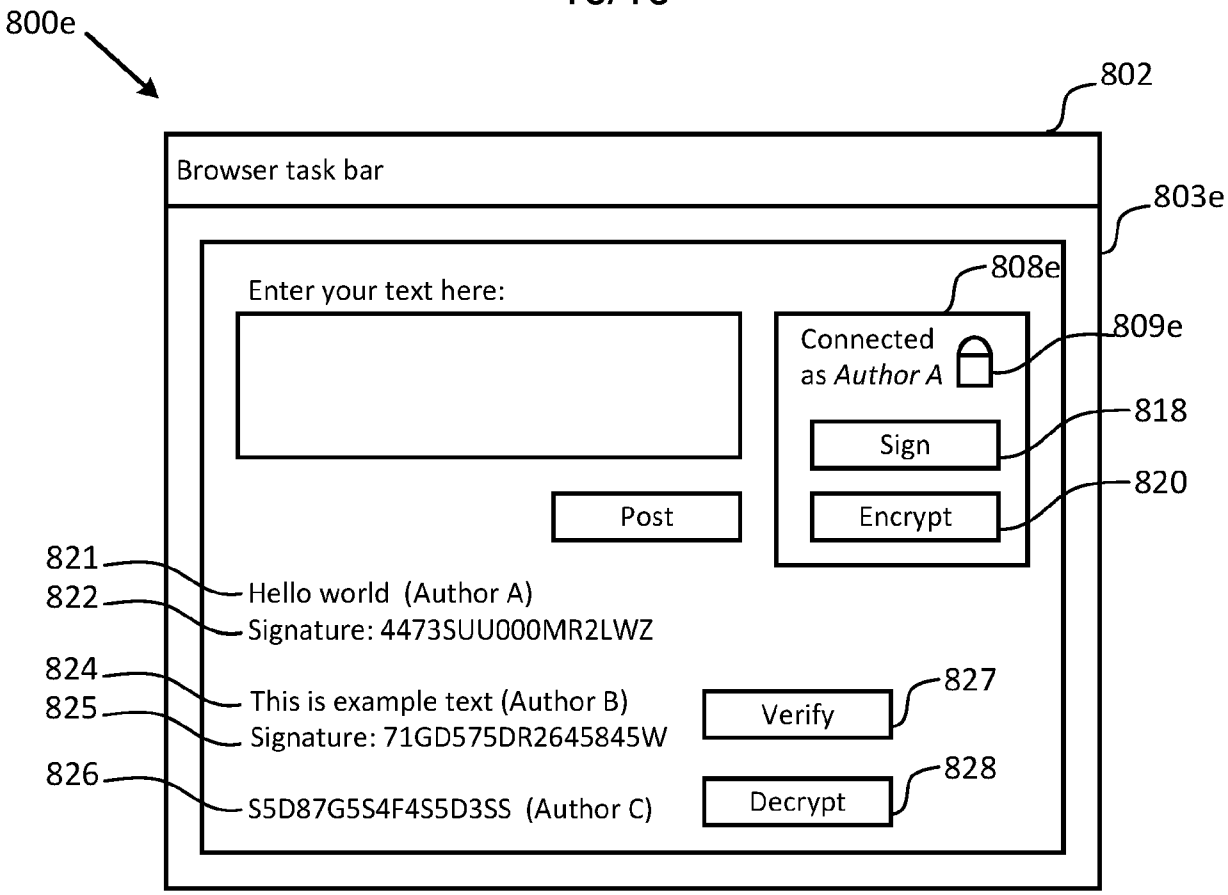
800e
802
Browser task bar
803e
Enter your text here:
808e
Connected as Author A
809e
818
Sign
820
Post
Encrypt
821
Hello world (Author A)
822
Signature: 4473SUU000MR2LWZ
824
This is example text (Author B)
825
Signature: 71GD575DR2645845W
827
Verify
826
S5D87G5S4F4S5D3SS (Author C)
828
Decrypt

Fig. 8e

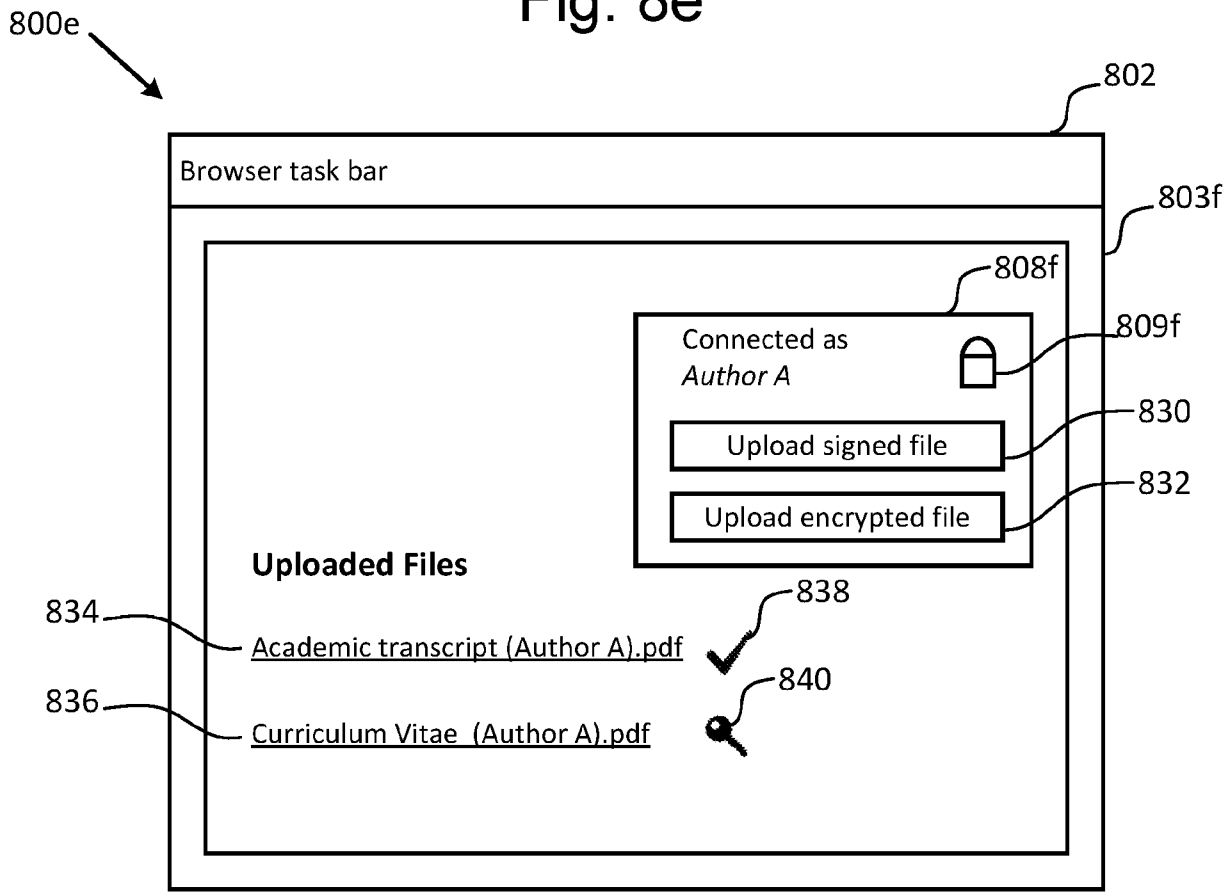
800e
802
Browser task bar
803f
808f
Connected as Author A
809f
830
Upload signed file
832
Upload encrypted file
Uploaded Files
838
834
Academic transcript (Author A).pdf
840
836
Curriculum Vitae (Author A).pdf

Fig. 8f

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2020/051020

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/34 (2013.01) G06F 21/62 (2013.01) H04L 9/32 (2006.01) H04L 9/08 (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)

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)

EPOQUE (PATENW), Espacenet, Google Scholar, Google Patents, The Lens, DWPI and internal databases using keywords and search terms such as:

G06F21/6263, G06F21/602, H04L67/02, H04L9/3234, H04L63/0853, G06F21/34, H04L9/0877, H04L9/0897, H04L67/104, H04L9/3271, browser, web page, web site, internet, online, web, app, program, input, interact, user, indentity, encrypt, cipher, encode, decode, sign, peer-to-peer, P2P, wireless, wifi, bluetooth, device, dongle, unit, external, third party, hardware security module, HSM, persistent, ongoing, session, WebRTC, connection, channel, protocol, handshake, signalling, challenge, response, key, Commonwealth Scientific and Industrial Research Organisation, Adnene Guabtni, Hugo O'Connor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] 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

"D" document cited by the applicant in the international application

"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	Date of mailing of the international search report
13 October 2020	13 October 2020

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
Email address: pct@ipaustralia.gov.au

Authorised officer

Jonty Goldin
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No. +61262850755

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/AU2020/051020**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2015/0096001 A1 (MOTOROLA MOBILITY LLC) 02 April 2015	
X	Whole document, in particular: Abstract; Paras 0029 - 0031, 0033 - 0034, 0036 - 0039, 0047 - 0048	1 - 11, 13 - 20
Y	As above	12
	US 2014/0222894 A1 (ORACLE INTERNATIONAL CORPORATION) 07 August 2014	
Y	Whole document, in particular: Abstract	12
A	Whole document, in particular Abstract; Para 0053	1 - 11, 13 - 20
	US 2018/0198621 A1 (SENYUK et al.) 12 July 2018	
A	Whole document	1 - 20
	US 2014/0123220 A1 (GENERAL INSTRUMENT CORPORATION) 01 May 2014	
A	Whole document	1 - 20
	US 7082535 B1 (NORMAN et al.) 25 July 2006	
A	Whole document	1 - 20
	US 2018/0034804 A1 (STEINER) 01 February 2018	
A	Whole document	1 - 20
	US 10284530 B1 (SYMANTEC CORPORATION) 07 May 2019	
A	Whole document	1 - 20
	WO 2016/112338 A1 (INTERTRUST TECHNOLOGIES CORPORATION) 14 July 2016	
A	Whole document	1 - 20
	US 9015857 B2 (SPRAGUE et al.) 21 April 2015	
A	Whole document	1 - 20

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2020/051020**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2015/0096001 A1	02 April 2015	US 2015096001 A1	02 Apr 2015
		US 9363251 B2	07 Jun 2016
		CN 106716433 A	24 May 2017
		CN 106716433 B	16 Aug 2019
		EP 3053080 A1	10 Aug 2016
		EP 3053080 B1	24 Apr 2019
		US 2016248764 A1	25 Aug 2016
		US 9729547 B2	08 Aug 2017
		WO 2015050890 A1	09 Apr 2015
US 2014/0222894 A1	07 August 2014	US 2014222894 A1	07 Aug 2014
		US 9712593 B2	18 Jul 2017
		US 2014223452 A1	07 Aug 2014
		US 9307031 B2	05 Apr 2016
		US 2014222930 A1	07 Aug 2014
		US 9331967 B2	03 May 2016
		US 2014222963 A1	07 Aug 2014
		US 9473581 B2	18 Oct 2016
		US 2014222957 A1	07 Aug 2014
		US 9509745 B2	29 Nov 2016
		US 2014222893 A1	07 Aug 2014
		US 9648049 B2	09 May 2017
		US 2014222890 A1	07 Aug 2014
		US 10476915 B2	12 Nov 2019
US 2018/0198621 A1	12 July 2018	US 2018198621 A1	12 Jul 2018
		US 10764056 B2	01 Sep 2020
US 2014/0123220 A1	01 May 2014	US 2014123220 A1	01 May 2014
		AU 2013338059 A1	18 Jun 2015
		AU 2013338059 B2	15 Jun 2017
		BR 112015009690 A2	22 May 2018
		CA 2899385 A1	08 May 2014
		EP 2901349 A1	05 Aug 2015
		KR 20150081328 A	13 Jul 2015
		KR 101722868 B1	05 Apr 2017
		MX 2015005454 A	15 Jan 2016
		MX 355757 B	27 Apr 2018

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2020/051020**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		US 2014123321 A1	01 May 2014
		US 9027159 B2	05 May 2015
		US 2014123172 A1	01 May 2014
		US 9172981 B2	27 Oct 2015
		US 2014123242 A1	01 May 2014
		US 9197910 B2	24 Nov 2015
		WO 2014070800 A1	08 May 2014

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2020/051020**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 7082535 B1	25 July 2006	US 7082535 B1	25 Jul 2006
US 2018/0034804 A1	01 February 2018	US 2018034804 A1	01 Feb 2018
		US 10708251 B2	07 Jul 2020
US 10284530 B1	07 May 2019	US 10284530 B1	07 May 2019
WO 2016/112338 A1	14 July 2016	WO 2016112338 A1	14 Jul 2016
		AU 2015266614 A1	15 Dec 2016
		CA 2950744 A1	03 Dec 2015
		CN 107155304 A	12 Sep 2017
		EP 3148560 A2	05 Apr 2017
		JP 2017520620 A	27 Jul 2017
		JP 2020121987 A	13 Aug 2020
		KR 20170010019 A	25 Jan 2017
		US 2016205074 A1	14 Jul 2016
		US 10205710 B2	12 Feb 2019
		US 2017258821 A1	14 Sep 2017
		US 2019038652 A1	07 Feb 2019
		US 2019364021 A1	28 Nov 2019
		US 2020179423 A1	11 Jun 2020
		WO 2015184441 A2	03 Dec 2015
		WO 2020072834 A1	09 Apr 2020
US 9015857 B2	21 April 2015	US 2013125247 A1	16 May 2013
		US 9015857 B2	21 Apr 2015
		CA 2855828 A1	23 May 2013
		EP 2771834 A1	03 Sep 2014
		US 2013125202 A1	16 May 2013
		US 9043866 B2	26 May 2015
		US 2013125201 A1	16 May 2013
		US 9047489 B2	02 Jun 2015
		US 2017243029 A1	24 Aug 2017
		US 9946898 B2	17 Apr 2018
		US 2017200023 A1	13 Jul 2017
		US 9977921 B2	22 May 2018
		US 2017206380 A1	20 Jul 2017

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2020/051020**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
		US 9990516 B2	05 Jun 2018
		US 2018247080 A1	30 Aug 2018
		US 10331908 B2	25 Jun 2019
		US 2018268169 A1	20 Sep 2018
		US 10552636 B2	04 Feb 2020
		US 2018330119 A1	15 Nov 2018
		US 10607029 B2	31 Mar 2020
		US 2019294823 A1	26 Sep 2019
		US 2020125764 A1	23 Apr 2020
		US 2020257826 A1	13 Aug 2020
		WO 2013074245 A1	23 May 2013

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.