



(51) International Patent Classification:

G06F 21/12 (2013.01) G06F 21/53 (2013.01)
G06F 21/60 (2013.01) H04L 9/08 (2006.01)

(21) International Application Number:

PCT/US2016/012726

(22) International Filing Date:

8 January 2016 (08.01.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/101,293 8 January 2015 (08.01.2015) US

(71) Applicant: INTERTRUST TECHNOLOGIES CORPORATION [US/US]; 920 Stewart Drive, Sunnyvale, California 94085-3913 (US).

(72) Inventor: MITCHELL, Stephen G.; 1770 Quail Hollow Rd., Ben Lomond, California 95005 (US).

(74) Agent: THAYER, Linda J.; 901 New York Avenue, NW, Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, Washington, District of Columbia 20001-4413 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) Title: CRYPTOGRAPHIC SYSTEMS AND METHODS

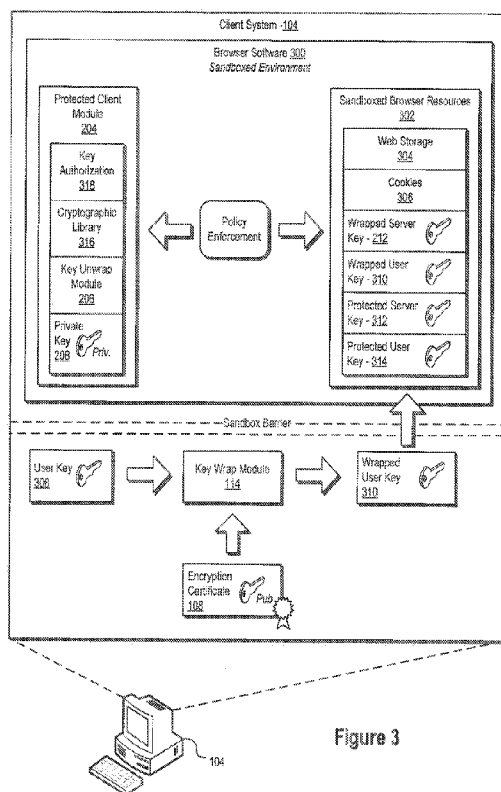


Figure 3

(57) Abstract: Systems and methods are described that use cryptographic techniques to improve the security of applications executing in a potentially untrusted environment associated with a software application. Embodiments of the disclosed systems and methods may, among other things, facilitate cryptographic operations within an execution environment associated with browser software of a client system while maintaining security of cryptographic keys imported into the environment. As the security of keys is maintained in an execution environment implementing embodiments of the disclosed systems and methods, users and/or systems may be more willing to consign their keys for use in connection with cryptographic operations performed in such environments.



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:**Declarations under Rule 4.17:**

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

CRYPTOGRAPHIC SYSTEMS AND METHODS

RELATED APPLICATIONS

[0001] This application claims the benefit of priority under 35 U.S.C. §119(e) to U.S. Provisional Patent Application No. 62/101,293, filed January 8, 2015, and entitled “CRYPTOGRAPHIC SYSTEMS AND METHODS,” which is hereby incorporated by reference in its entirety.

COPYRIGHT AUTHORIZATION

[0002] Portions of the disclosure of this patent document may contain material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the U.S. Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND AND SUMMARY

[0003] The present disclosure relates generally to systems and methods for performing cryptographic operations. More specifically, but not exclusively, the present disclosure relates to systems and methods that use cryptographic techniques to protect secure information shared with a potentially untrusted execution environment associated with a software application.

[0004] Conventional cryptographic services implemented within browser software of a client system may be vulnerable to certain attacks. For example, a server provisioning a cryptographic implementation to browser software of a client system and/or a communication channel associated with the same may be compromised (*e.g.*, via a man-in-the-middle attack or the like). In view of these potential vulnerabilities, a user of a client system may be unwilling to provide certain secure user keys or other sensitive data to cryptographic implementations and/or other data processing methods operating within browser software downloaded from an untrusted server. Similarly, a server may be unwilling to provide certain secure server keys to browser software of an untrusted client system.

[0005] Certain embodiments of the systems and methods disclosed herein provide for secure implementation of cryptographic services including trusted credential and/or key management services operating within browser software executing on a client system. In some embodiments, a user may trust their secure keys to a cryptographic implementation operating within browser software based on the cryptographic service being signed and/or otherwise protected or authenticated by a trusted service (*e.g.*, a trusted third party cryptographic service or the like). Similarly, a server may trust its secure keys to a cryptographic implementation operating within the browser software of a client system. In certain embodiments, the disclosed systems and methods may enable trusted credential and/or secure user key management within a sandboxed area of the client system associated with the browser software, thereby protecting the integrity of the trusted credentials and/or secure keys.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The inventive body of work will be readily understood by referring to the following detailed description in conjunction with the accompanying drawings, in which:

[0007] **Figure 1** illustrates a trust configuration process consistent with embodiments disclosed herein.

[0008] **Figure 2** illustrates a process of provisioning a client system with a protected client module consistent with embodiments disclosed herein.

[0009] **Figure 3** illustrates an exemplary implementation of a cryptographic service included in browser software executing on a client system consistent with embodiments disclosed herein.

[0010] **Figure 4** illustrates a flow chart of an exemplary cryptographic operation consistent with embodiments disclosed herein.

[0011] **Figure 5** illustrates a system that may be used to implement certain embodiments of the systems and methods of the present disclosure.

DETAILED DESCRIPTION

[0012] A detailed description of systems and methods consistent with embodiments of the present disclosure is provided below. While several embodiments are described, it should be understood that the disclosure is not limited to any one embodiment, but instead encompasses numerous alternatives, modifications, and equivalents. In addition, while numerous specific details are set forth in the following description in order to provide a thorough understanding of the embodiments disclosed herein, some embodiments can be practiced without some or all of these details. Moreover, for the purpose of clarity, certain technical material that is known in the related art has not been described in detail in order to avoid unnecessarily obscuring the disclosure.

[0013] Some embodiments of the disclosure may be understood by reference to the drawings, wherein like parts may be designated by like numerals. The components of the disclosed embodiments, as generally described and illustrated in the figures herein, could be arranged and designed in a wide variety of different configurations. Thus, the following detailed description of certain illustrative embodiments is not intended to limit the scope of the disclosure, as claimed, but is merely representative of possible embodiments of the disclosure. In addition, the steps of any method disclosed herein do not necessarily need to be executed in any specific order, or even sequentially, nor need the steps be executed only once, unless otherwise specified.

[0014] Embodiments of the systems and methods disclosed herein may employ trusted key management in connection with cryptographic services implemented within browser software executing on a client system. In certain embodiments, the systems and methods may use a trusted service operating as a root-of-trust. Credentials (*e.g.*, certificates, keys, and/or the like) may be provisioned by the trusted service to client and/or server systems for use in connection with protecting the security of keys used in cryptographic operations performed by a protected client module executing within browser software of the client system (*e.g.*, a JavaScript application and/or the like). In certain embodiments, the protected client module may be protected using a variety of cryptographic and/or white-box cryptographic techniques employed by the trusted service. Using such an architecture, the integrity

of keys shared by a user of client system and/or the server system with the protected client module may be maintained. Although certain embodiments disclosed herein are discussed in connection with client modules executing within browser software of a client system, it will be appreciated that the disclosed embodiments may be further employed in connection with any other type of software and/or execution environments and in a variety of configurations and/or architectures.

[0015] In certain embodiments, the systems and methods described herein can, for example, be used in connection with digital rights management (“DRM”) technologies such as those described in commonly assigned, co-pending U.S. Patent Application No. 11/583,693 (“the ‘693 application”), service orchestration technologies such as those described in commonly assigned co-pending U.S. Patent Application No. 10/863,551 (“the ‘551 application”), and/or content delivery technologies such as those described in commonly assigned co-pending U.S. Patent Application No. 12/785,406 (“the ‘406 application”) (the contents of ‘693 application, the ‘551 application, and the ‘406 application hereby being incorporated by reference in their entireties), as well as in other contexts. It will be appreciated that these systems and methods are novel, as are many of the components, systems, and methods employed therein.

[0016] **Figure 1** illustrates a trust configuration process consistent with embodiments disclosed herein. In certain embodiments, a trusted service 100 may interact with a server system 102 and/or a client system 104 in connection with a trust configuration process. The trusted service 100, the server system 102, the client system 104, and/or other services and/or systems (not shown) used in connection with the disclosed embodiments may comprise any suitable computing system or combination of systems configured to implement embodiments of the systems and methods disclosed herein. In certain embodiments, the trusted service 100, the server system 102, the client system 104, and/or other systems or services may comprise at least one processor system configured to execute instructions stored on an associated non-transitory computer-readable storage medium. As discussed in more detail below, the trusted service 100, the server system 102, the client system 104, and/or other systems or services may further comprise a secure processing unit (“SPU”) configured to perform sensitive operations such as trusted credential and/or key management, secure policy management, and/or other aspects of the systems and

methods disclosed herein. The trusted service 100, the server system 102, and/or the client system 104, and/or other services or systems may further comprise software and/or hardware configured to enable electronic communication of information between the devices and/or systems via one or more associated network connections.

[0017] The client system 104 may comprise a computing device executing one or more applications configured to implement certain embodiments of the systems and methods disclosed herein. In certain embodiments, the client system 104 may comprise a laptop computer system, a desktop computer system, a smartphone, a tablet computer, and/or any other computing system and/or device that may be utilized in connection with the disclosed systems and methods. In some embodiments, the client system 104 may comprise software and/or hardware configured to, among other things, implement cryptographic operations using software executing within browser software of the client system 104 and/or a sandboxed environment associated with the same. As discussed in more detail below, in some embodiments, such cryptographic functionality may be implemented using, at least in part, one or more protected applications (*e.g.*, client modules) executing within a browser of the client system 104.

[0018] Communication between the client system 104, server system 102, trusted service 100, and/or one or more other service providers may be facilitated by a network comprising any suitable number of networks and/or network connections. The network connections may comprise a variety of network communication devices and/or channels and may utilize any suitable communication protocols and/or standards facilitating communication between the connected devices and systems. The network connections may comprise the Internet, a local area network, a virtual private network, and/or any other communication network utilizing one or more electronic communication technologies and/or standards (*e.g.*, Ethernet or the like). In some embodiments, the network connections may comprise a wireless carrier system such as a personal communications system (“PCS”), and/or any other suitable communication system incorporating any suitable communication standards and/or protocols. In further embodiments, the network connections may comprise an analog mobile communications network and/or a digital mobile communications network utilizing, for example, code division multiple access (“CDMA”), Global System for Mobile Communications or Groupe Special Mobile (“GSM”), frequency division

multiple access (“FDMA”), and/or time divisional multiple access (“TDMA”) standards. In certain embodiments, the network connections may incorporate one or more satellite communication links. In yet further embodiments, the network connections may utilize IEEE’s 802.11 standards, Bluetooth®, ultra-wide band (“UWB”), Zigbee®, and or any other suitable communication protocol(s).

[0019] As part of the trust configuration process, the trusted service 100 may generate and issue one or more trusted credentials to the server system 102 and/or the client system 104. In certain embodiments, a trusted credential may comprise a certificate including one or more cryptographic components. For example, as illustrated, the trusted service 100 may generate an encryption certificate 108 that includes a cryptographic key using a certificate generation module 106. In some embodiments, the cryptographic key included in the encryption certificate 108 may be a public cryptographic key. Although embodiments disclosed herein are discussed in connection with a trusted credential that comprises an encryption certificate 108 including a public key, it will be appreciated that any suitable trusted credential may be used in connection with the disclosed embodiments. As discussed in more detail below, the encryption certificate 108 may be used in connection with facilitating trust between a server system 102, a client system 104, and/or a module executing on the same (*e.g.*, a script executing in browser software and/or the like)

[0020] The encryption certificate 108 may be communicated to the server system 102 and/or the client system 104. In certain embodiments, the encryption certificate 108 may be issued to the server system 102 from the trusted service 100, which may in turn issue the encryption certificate 108 to the client system 104. In other embodiments, the encryption certificate 108 may be issued to the client system 104 by the trusted service 100 directly and/or via one or more other intermediate services and/or systems. Similarly, the encryption certificate 108 may be issued to the server system 102 via one or more intermediate services and/or systems.

[0021] Upon receiving the encryption certificate 108, the server system 102 may use the encryption certificate 108 in connection with a server trust configuration process 110. In certain embodiments, the encryption certificate 108 may be loaded in a trusted certificate library maintained by the server system 102 as part of the server trust configuration process 110 for use in connection with future trusted and/or

cryptographic operations. In certain embodiments, prior to committing secret information to the trusted service 100, the server system 102 may verify that the trusted service 100 is trusted as part of the server trust configuration process 110. Trust may be verified and/or otherwise established in a variety of suitable ways. For example, trust may be verified and/or otherwise established by determining that the trusted service 100 meets trust and/or security requirements articulated by the server system 102 and/or another service. After trust has been verified and/or established, the encryption certificate 108 may be used by the server system 102 to encrypt information in connection with the disclosed embodiments.

[0022] The server system 102 may generate a key wrap module 112 as part of a key wrap module generation process 112. In certain embodiments, the key wrap module 112 may use the encryption certificate 108 to perform a key wrapping operation. In some embodiments, the key wrap module 114 may be used to encapsulate cryptographic keys, thereby protecting wrapped cryptographic keys while in untrusted storage and/or during transmission over untrusted communication channels. In certain embodiments, the key wrap module 114 may comprise an asymmetric encryption algorithm that utilizes the public key included in the encryption certificate 108 to wrap and/or otherwise protect a cryptographic key. In some embodiments, the key wrap module 114 may be configured to perform a key wrapping operation using an RSA encryption algorithm, although other suitable key wrapping algorithms and/or processes may also be used in connection with the disclosed embodiments. Although in the illustrated embodiments the key wrap module 112 is shown as being generated and distributed by the server system 102, it will be appreciated that the key wrap module 112 may be generated and distributed by the trusted service 100 and/or one or more other services.

[0023] In some embodiments, the encryption certificate 108 may be separate from the key wrap module 114 and may be accessed by the key wrap module 114 in connection with key wrapping operations (*e.g.*, from a certificate library and/or the like). In other embodiments, the encryption certificate 108 may be included as a component within the key wrap module 114.

[0024] The key wrap module 114 and/or the encryption certificate 108 may be transmitted to the client system 104 for use in connection with key wrapping and/or

other cryptographic operations. In certain embodiments, upon receiving the encryption certificate 108, the client system 104 may use the encryption certificate 108 in connection with a client trust configuration process 116. In certain embodiments, prior to committing secret information to the trusted service 100 and/or modules and/or applications protected by the same, the client system 104 may verify that the trusted service 100 is trusted as part of the client trust configuration process 116. Trust may be verified and/or otherwise established in a variety of suitable ways. For example, trust may be verified and/or otherwise established by determining that the trusted service 100 meets trust and/or security requirements articulated by the client system 104 and/or another service. After trust has been verified and/or established, the encryption certificate 108 may be used by the client system 104 to encrypt information in connection with the disclosed embodiments.

[0025] In certain embodiments, the encryption certificate 108 may be loaded in a trusted certificate library maintained by the client system 104 as part of the user trust configuration process 116 for use in connection with future trusted and/or cryptographic operations. Similarly, the key wrap module 114 may be loaded into one or more cryptographic libraries of the client system 104 for use in connection with trusted and/or cryptographic operations performed by the client system 104.

[0026] Various trust configuration processes illustrated in connection with **Figure 1** may be performed at a variety of suitable times. For example, in some embodiments, the server system 102 and/or client system 104 may be provisioned with an encryption certificate 108 and/or key wrap module 114 at a time of manufacture. In other embodiments, various aspects of the trust configuration processes may be performed in connection with a system registration process (*e.g.*, a server and/or client registration process or the like). In yet further embodiments, aspects of the trust configuration processes may be performed when a protected client module is transmitted to a client system 104 from the server system 102 for execution within browser software of the client system 104, as is discussed in more detail below.

[0027] **Figure 2** illustrates a process of provisioning a client system 104 with a protected client module 204 consistent with embodiments disclosed herein. In certain embodiments, the server system 102 may transmit a client module 200 to the trusted service 100 for protection. In some embodiments, the client module 200 may be

generated by the server system 102. In further embodiments, a developer of the client module 200 may transmit the client module 200 to the server system 102 and/or the trusted service 100 for distribution to one or more client systems 104 and/or for protection by the trusted service 100.

[0028] The client module 200 may comprise a software application configured to be executed by the client system 104. For example, in some embodiments, the client module 200 may be configured to be executed within browser software of the client system. In some embodiments, the client module 200 may comprise a JavaScript application downloaded to a client system 102 in connection with accessing a webpage using associated browser software. Consistent with embodiments disclosed herein, the client module 200 may implement certain cryptographic operations (*e.g.*, operations using cryptographic keys and/or the like), which may be protected by the trusted service 100.

[0029] Upon receipt of the client module 200, the trusted service 100 may engage in a protected module generation process 202. In certain embodiments, the protected module generation process 202 may utilize any suitable software code protection method to yield a protected client module 204 including, for example, white-box cryptographic protection methods, fully homomorphic encryption (“FHE”) methods, software obfuscation methods, functional encryption methods, and/or the like. For example, in certain embodiments, white-box protection methods may allow secret information associated with the client module 200 (*e.g.*, secure keys such as a private key) to remain encrypted and/or otherwise protected, even during execution of code associated with the client module 200. In some embodiments, such white-box cryptographic methods may protect software code and/or associated secret information from being exposed in clear text during execution of the module. Among other things, this may allow execution and/or storage of the client module 202 on and/or in a memory of a client system 104 having an open architecture.

[0030] In certain embodiments, the protected client module 204 may comprise a key unwrap module 206. The key unwrap module 206 may be configured to unwrap a cryptographic key using a private cryptographic key 208 included in the protected client module 204 to yield a protected cryptographic key (*e.g.*, a white-box protected cryptographic key). For example, in some embodiments, the key unwrap module 206

may receive a cryptographic key wrapped using the public cryptographic key included in the encryption certificate 108 generated and/or provisioned by the trusted service 100 as part of a trust configuration process. The key unwrap module 206 may utilize the private cryptographic key 208 included in the protected client module 204 corresponding to the public key to unwrap the wrapped cryptographic key and yield a protected cryptographic key that may then be used in connection with certain cryptographic operations performed by the protected client module 204. In some embodiments, the private cryptographic key 208 may comprise a white-box protected cryptographic key.

[0031] The protected client module 204 may be transmitted to the server system 102 by the trusted service 100 for distribution to one or more client systems 104. The server system 102 may distribute the protected client module 204 to the client system 104 under a variety of circumstances. For example, in some embodiments, the protected client module 204 may comprise a protected JavaScript application. When browser software executing on the client system 104 accesses an associated webpage, the protected JavaScript application may be downloaded by the client system 104 from the server system 102 for execution within an environment associated with the browser software. In some embodiments, the protected JavaScript application may not be permanently installed on the client system 104, but be cached for use during a single and/or over a limited number of sessions and/or period of time.

[0032] In some embodiments, the protected client module 204 may perform cryptographic operations utilizing a variety of cryptographic keys. For example, the protected client module 204 may perform a secure cryptographically-enforced transaction between the server system 102 and the client system 104 using keys associated with the server system 102 and/or the client system 104. Similarly, the protected client module 204 may use keys associated with the server system 102 and/or the client system 104 in connection with various web analytics methods, network authentication methods (*e.g.*, Kerberos network authentication protocol methods), financial transaction methods including EMV payments, and/or the like. It will be appreciated that embodiments disclosed herein may also be utilized in connection with protecting secret information used in various non-cryptographic operations performed by the protected client module 204.

[0033] In certain embodiments, the server system 102 may not trust the integrity and/or security of the client system 104, and thus may not wish to provide its unencrypted keys to the client system 104 for use in connection with various operations including, for example, cryptographic operations. Accordingly, the server system 102 may use the key wrap module 114 to wrap a server key 210 using the public key included in the encryption certificate 108. After the server key 210 has been wrapped, the wrapped server key 212 may be transmitted to the client system 104 for use in connection with various cryptographic operations performed by the protected client module 204.

[0034] **Figure 3** illustrates an exemplary implementation of a cryptographic service included in browser software 300 executing on a client system 104 consistent with embodiments disclosed herein. In certain embodiments, certain software code executing on the client system 104 may be sandboxed and/or otherwise executed in some type of a limited virtualized environment. Software code executing in a sandbox may be restricted to accessing and/or using a controlled set of resources, functions, and/or services associated with the client system. For example, a sandbox may allow software code executing therein to only access a certain subset of storage disk space and/or memory associated with the client system. Access to certain input/output channels, networking resources, processing resources, and/or the like may be similarly controlled and/or restricted.

[0035] In certain embodiments, browser software 300 executing on the client system 104 may be sandboxed, thereby protecting the client system 104 from nefarious code executing within the browser software 300. In certain embodiments, the browser software 300 may have access to defined sandboxed resources 302 of the client system 104. The sandboxed resources 302 may comprise certain portions and/or locations of storage on the client system 104 that may store, for example, cached and/or otherwise stored website information 304, cookies 306, and/or trusted credentials such as keys 312, 310-314. The sandboxed resources 302 may further comprise certain processing resources, functions, services, and/or interfaces of the client system 104 accessible by the browser software 300 and/or modules executing in an environment associated with the same. In other embodiments, the sandboxed resources 302 may comprise a secure clock, a secure random number generator, a secure user interface, and/or the like.

[0036] A protected client module 204 may be loaded into the execution environment of the browser software 300 to facilitate implementation of certain cryptographic services within the browser software 300 consistent with embodiments disclosed herein. In certain embodiments, the interaction between the browser software 300 and/or modules executing in the sandboxed environment of the browser software 300 may be managed by one or more articulated policies. For example, in certain embodiments, the protected client module 304 may only be allowed access to sandboxed browser resources 302 associated with the module 304 (*e.g.*, web storage 304, cookies 306, and/or keys 212, 310-314). Similarly, in some embodiments, a same-origin policy may be enforced by the browser software 300 to allow a specific browser application to access cookies and/or other information generated by the application while restricting access to cookies and/or other information generated by other applications. In this manner, the specific resources included in the sandboxed browser resources 302 may vary between various browser-executed applications.

[0037] A user of the client system 104 may wish to use a cryptographic key 308 in connection with a cryptographic operation performed by the protected client module 204 executing in the sandboxed environment of the browser software 300. The user, however, may not necessarily trust applications executing within the browser software 300, and thus may not wish to provide their unencrypted user key 308 to the execution environment of the browser software 300. Accordingly, the client system 104 may use a key wrap module 114 provisioned as part of the trust configuration process detailed above to wrap the user key 308 using the public key included in the provisioned encryption certificate 108. In certain embodiments, by wrapping the user key 308 with the public key included in the encryption certificate 108, the client system 104 may limit use of the user key 308 to trusted applications protected by a trusted service.

[0038] In certain embodiments, the encryption certificate 108 may also comprise descriptions of various functions and/or permissions relating to how a key wrapped with information included in the encryption certificate 108 (*e.g.*, the public key) will be used by the protected client module 104. In some embodiments, such descriptive information may allow a user of the client system 104 to better determine what operations they are consigning their secret user key 308 to prior to wrapping the key using information included in the encryption certificate 108 and importing the

wrapped key 310 into the execution environment associated with the browser software 300. In some embodiments, functions and/or permissions relating to how a key is used by the protected client module 204 and/or other related modules and/or systems may be enforced by a key authorization module 318 included in the protected client module 204 and/or the browser software 300.

[0039] After the user key 308 has been wrapped, the resulting wrapped user key 310 may be imported to the execution environment of the browser software 300 for use in connection with cryptographic operations implemented by the protected client module 204. In certain embodiments, the key unwrap module 206 included in the protected client module 204 may be configured to unwrap the wrapped user key 310 using the private cryptographic key 208 provisioned to the protected client module 204 by the trusted service to yield a protected user key 314. In certain embodiments, the protected user key 314 may comprise a white-box protected user key. Accordingly, the protected user key 314 may be exposed outside the sandboxed environment of the browser software 300 (*e.g.*, to a remote server system and/or the like) without compromising the security of the user key. The protected user key 314 may be used in connection with cryptographic operations performed by the protected client module 204 and/or by a remote server system.

[0040] Certain cryptographic operations performed by the protected client module 204 may further use a key provided by a server system. For example, certain secure transactions may utilize both a user key and a server key. Accordingly, a wrapped server key 212 sent to the execution environment of the browser software 300 by a server system may further be unwrapped using the key unwrap module 206 included in the protected client module 204 to generate a protected server key 312. Like the protected user key 314, the protected server key 312 may comprise a white-box protected user key. Accordingly, the protected server key 312 may be exposed outside the server system (*e.g.*, to the execution environment of the browser software 300) without compromising the security of the server key.

[0041] Key unwrapping consistent with the disclosed embodiments may be performed at a variety of times. For example, in some embodiments, key unwrapping may be performed using the key unwrap module 206 when the wrapped server key 212 and/or the wrapped user key 310 are initially loaded into the execution

environment of the browser software 300. In further embodiments, key unwrapping may be performed when keys used in connection with a cryptographic operation are requested by the protected client module 204. In certain embodiments, unwrapped protected keys 312, 314 may be utilized in connection with cryptographic operations performed using a cryptographic library 316 of the protected client module 204. In yet further embodiments, key unwrapping may be included as part of platform and/or service communication methods (*e.g.*, SSL communication methods and/or the like).

[0042] Although certain embodiments disclosed herein are discussed in connection with the use of a key wrap module 114 to protect various secret information including user and server keys (*e.g.*, user key 308), it will be appreciated that other protection mechanisms may also be used in connection with the disclosed embodiments. For example, in some embodiments, keys may be communicated to the protected client module 204 via a secure and/or otherwise authenticated communications channel. In some embodiments, the secure and/or authenticated communication channel may protect the keys from being exposed in the clear.

[0043] A variety of cryptographic operations may be performed using the protected keys 312, 314. For example, the protected client module 204 may use the protected keys 312, 314 in connection with a secure cryptographically-enforced transaction between a server system and the client system 104. Other cryptographic operations using embodiments of the disclosed systems and methods include, without limitation, data encryption/decryption operations, cryptographic signing operations, cryptographic signature verification operations, and/or the like. In yet further embodiments, the protected keys 312, 314 may be used in a variety of other operations that may not necessarily be cryptographic operations.

[0044] In certain embodiments, the protected client module 204 may implement a safe application program interface (“API”). In certain embodiments, the safe API may expose certain defined functions that may not be used to compromise the integrity of secret information imported to the protected client module 204 and/or the associated browser software 300 such as secure keys (*e.g.*, keys 212, 310-314). In certain embodiments, such defined functions may be articulated in metadata and/or other information associated with the keys. For example, in certain embodiments, functions such as unwrapping a wrapped user key 310 and making it directly available

may not be exposed by the safe API. In this manner, the integrity of the imported secure user key 310 may be maintained by the protected client module 204. Similarly, specific permitted uses of secure keys 212, 310-314 by the protected client module 204, the browser software 300, and/or other software and/or systems may be enforced by implementation of a safe API, thereby preventing the keys 212, 310-314 from being used in arbitrary ways.

[0045] In some embodiments, a safe API may further utilize certain code verification techniques to ensure that the integrity of secret information imported into a protected client module 204 and/or associated browser software is maintained. For example, the safe API may validate the integrity of its inputs and/or perform certain authorization checks. In certain embodiments, the safe API may perform and/or otherwise verify certain key authorizations using any suitable technique (*e.g.*, DRM license checks and/or the like). In some embodiments, this functionality may, among other things, reduce the potential of repeated or rogue activations from detrimentally impacting an overall trust ecosystem and/or its various participants.

[0046] In further embodiments, a user of the client system 104 may trust their secure user keys 308 to a trusted service. In certain embodiments, the trusted service may be trusted by the user through assurance and/or auditing of certain security implementations. The trusted service may protect the secret user keys 308 using white-box cryptographic protection methods and may distribute protected user keys 314 to the client system 104. Similarly, a server may trust its keys to the trusted service, which may protect the server keys using white-box cryptographic protection methods and may similarly distribute the protected server keys 312 to the server system and/or the client system. The protected client module 204 executing within the browser software 300 of the client system 104 may then access the protected keys 312, 314 in connection with various operations including, for example, cryptographic operations. In certain embodiments, such an implementation may reduce the burden on the client system 104 and/or a server system associated with performing key wrapping and/or unwrapping operations.

[0047] In certain embodiments, the browser software 300 executing on the client system 104 may use Google[®] Native Client (“NaCl”) and/or any other suitable sandboxing technology to facilitate safe execution of native code within an

environment associated with the browser software 300. In some embodiments, native code that is written in a defined manner may be executed within the sandboxed environment. In certain embodiments, the defined manner in which the native code is written may be analyzable and verifiable as being secure by the browser software 300 executing the code. For example, native code may be analyzed to determine that the code may only call certain permissible functions. In some embodiments, such an implementation may allow for executing of web-based applications (*e.g.*, a protected client module 204) at near-native speeds on the client system 104.

[0048] Embodiments of the disclosed systems and methods may be utilized in connection with a variety of applications. For example, in some embodiments, a protected client module 204 may be utilized in connection with implementing a Kerberos Ticket Granting Service (“TGS”). In some embodiments, various secure resources used in connection with the Kerberos TGS (*e.g.*, a secure random number generator, secure storage, etc.) may be provided by the client system 104 via a trusted SPU and/or the like. In further embodiments, a protected client module 204 may be used in connection with implementing a EMV payment service to, among other things, protect a user’s account information (*e.g.*, credit card number) and/or sign payment tokens using associated keys (*e.g.*, symmetric keys).

[0049] It will be appreciated that a number of variations can be made to the architecture and relationships presented in connection with **Figures 1-3** within the scope of the inventive body of work. For example, without limitation, in some embodiments, some or all of the functions performed by the trusted service 100 may be performed by the server system 102. Similarly, some or all of the functions performed by the client system 104 may be performed by the server system 102. Furthermore, one or more other services and/or systems not necessarily illustrated may be utilized in connection with implementing various aspects of the embodiments of the disclosed systems and methods. Although certain embodiments are discussed in connection with protecting secure cryptographic keys, it will be appreciated that the disclosed embodiments may be further used in connection with protecting any suitable secret information including, without limitation, passwords, personal information, sensitive data, and/or the like. Thus it will be appreciated that **Figures 1-3** are provided for purposes of illustration and explanation, and not limitation.

[0050] **Figure 4** illustrates a flow chart of an exemplary cryptographic method 400 consistent with embodiments disclosed herein. The illustrated method 400 may be implemented in a variety of ways, including using software, firmware, hardware, and/or any combination thereof. In certain embodiments, various aspects of the method 400 may be implemented by a client system, a server system, a trusted service, and/or any other related service or system as described above. Certain embodiments included in the illustrated method 400 may implement secure cryptographic operations within a sandboxed execution space of browser software executing on a client system. It will be appreciated, however, that embodiments of the disclosed systems and methods may be similarly implemented in a variety of other execution spaces. In addition, it will be appreciated that cryptographic operations consistent with the disclosed embodiments may incorporate all of the elements of the illustrated method 400 or a subset thereof, and may proceed in any suitable order.

[0051] At 402, a wrapped user key may be received via an import process in an execution environment associated with browser software. In certain embodiments, the wrapped user key may have been wrapped using a public key included in an encryption certificate provisioned to a client system executing the browser software from a trusted service. A wrapped server key may be similarly received in the execution environments of the browser software at 404. Like the wrapped user key, the wrapped server key may have been wrapped using a public key included in an encryption certificate provisioned to the server system from a trusted service. The wrapped keys may be provided to the execution environment associated with the browser software and/or a protected application executing within the same through a platform API, a cookie, user interaction (*e.g.*, user input via a browser widget or the like), etc.

[0052] The wrapped user key may be unwrapped by a component of a protected application such as a key unwrapping module executing within the execution environment of the browser software at 406. In certain embodiments, the wrapped user key may be unwrapped using, at least in part, a private key provisioned to the protected application from the trusted service corresponding to the public key included in the encryption certificate used to wrap the user key. Unwrapping the wrapped user key may generate a white-box protected user key.

[0053] At 408, the wrapped server key may be unwrapped by the key unwrapping module of the protected application executing within the execution environment of the browser software. Like the wrapped user key, the wrapped server key may be unwrapped using, at least in part, a private key provisioned to the protected application from the trusted service corresponding to the public key included in the encryption certificate used to wrap the server key. Unwrapping the wrapped server key may generate a white-box protected server key.

[0054] A cryptographic operation may be performed by the protected client module using the generated protected server and/or user keys at 410. In certain embodiments, the security of the user and/or server keys may be maintained, as the corresponding protected cryptographic keys used in connection with the cryptographic operation may remain white-box protected in the execution space of the browser application and/or elsewhere that they may be sent in connection with the operation. Accordingly, a user of the client system and/or the server system may be more willing to import wrapped representations of their secure keys into the otherwise potentially untrusted execution space of the browser software.

[0055] **Figure 5** illustrates a system 500 that may be used to implement certain embodiments of the systems and methods of the present disclosure. The system 500 may comprise a trusted service, a server system, a client system, and/or any other system configured to implement certain aspects the systems and methods described herein. In certain embodiments, the system 500 may perform some or all of the disclosed functions associated with a trusted service, a server system, a client system, and/or any other related system and/or service as disclosed herein.

[0056] As illustrated in **Figure 5**, the system 500 may include: a processor 502; system memory 504, which may include high speed RAM, non-volatile memory and/or one or more bulk non-volatile computer-readable storage mediums (*e.g.*, a hard disk, flash memory, etc.) for storing programs and other data for use and execution by the processor 502; an interface 516 (*e.g.*, an input/output interface) that may include a display and/or one or more input devices such as, for example, a touchscreen, a keyboard, a mouse, a track pad, and the like; a port 506 for interfacing with removable memory 508 that may include one more diskettes, optical storage mediums, and/or other computer-readable storage mediums (*e.g.*, flash memory,

thumb drives, USB dongles, compact discs, DVDs, etc.); a network interface 510 for communicating with other systems via a network 530 using one or more communication technologies; and one or more buses 532 for communicatively coupling the aforementioned elements.

[0057] In certain embodiments, the network 530 may comprise the Internet, a local area network, a virtual private network, and/or any other communication network utilizing one or more electronic communication technologies and/or standards (*e.g.*, Ethernet or the like). In some embodiments, the network interface 510 and/or network 530 may be part of a wireless carrier system, such as a PCS, and/or any other suitable communication system incorporating any suitable communication standards and/or protocols. In further embodiments, the network interface 510 and/or the network 530 may be part of an analog mobile communications network and/or a digital mobile communications network utilizing, for example, CDMA, GSM, FDMA, and/or TDMA standards. In still further embodiments, the network interface 510 and/or the network 530 may incorporate one or more satellite communication links and/or use IEEE's 802.11 standards, near-field communication, Bluetooth[®], UWB, Zigbee[®], and or any other suitable standard or standards.

[0058] In some embodiments, the system 500 may, alternatively or in addition, include a SPU 514 that is protected from tampering by a user of system 500 or other entities by utilizing secure physical and/or virtual security techniques. An SPU 514 can help enhance and/or facilitate the security of sensitive operations such as private management of secret or otherwise secure information including cryptographic keys, and other aspects of the systems and methods disclosed herein. In certain embodiments, the SPU 514 may operate in a logically secure processing domain and be configured to protect and operate on secret information. In some embodiments, the SPU 514 may include internal memory storing executable instructions or programs configured to enable the SPU 514 to perform secure operations. In further embodiments, the SPU 514 may facilitate certain secure platform resources including, without limitation, secure random number generators, secure clocks, secure user interfaces, secure storage, and/or the like.

[0059] The operation of system 500 may be generally controlled by the processor 502 operating by executing software instructions and programs stored in the system memory 504 (and/or other computer-readable media, such as removable memory 508). The system memory 504 may store a variety of executable programs or modules for controlling the operation of the system 500. For example, the system memory 504 may include an operating system (“OS”) 520 that may manage and coordinate, at least in part, system hardware resources and provide for common services for execution of various applications and a trust and privacy management system 522 for implementing trust and privacy management functionality including protection and/or management of secret information. The system memory 504 may further include, without limitation, communication software 524 configured to enable in part communication with and by the system 500, applications 526, cryptographic keys 528 (*e.g.*, wrapped keys, protected keys, etc.), browser software and/or protected applications and/or client modules 518 configured to execute within an execution space associated with the same, and/or any other information and/or applications configured to implement embodiments of the systems and methods disclosed herein.

[0060] One of ordinary skill in the art will appreciate that the systems and methods described herein can be practiced with computing devices similar or identical to that illustrated in **Figure 5**, or with virtually any other suitable computing device, including computing devices that do not possess some of the components shown in **Figure 5** and/or computing devices that possess other components that are not shown. Thus it should be appreciated that **Figure 5** is provided for purposes of illustration and not limitation.

[0061] The systems and methods disclosed herein are not inherently related to any particular computer, electronic control unit, or other apparatus and may be implemented by a suitable combination of hardware, software, and/or firmware. Software implementations may include one or more computer programs comprising executable code/instructions that, when executed by a processor, may cause the processor to perform a method defined at least in part by the executable instructions. The computer program can be written in any form of programming language, including compiled or interpreted languages, and can be deployed in any form, including as a standalone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. Further, a computer program can be

deployed to be executed on one computer or on multiple computers at one site or distributed across multiple sites and interconnected by a communication network. Software embodiments may be implemented as a computer program product that comprises a non-transitory storage medium configured to store computer programs and instructions, that when executed by a processor, are configured to cause the processor to perform a method according to the instructions. In certain embodiments, the non-transitory storage medium may take any form capable of storing processor-readable instructions on a non-transitory storage medium. A non-transitory storage medium may be embodied by a compact disk, digital-video disk, a magnetic tape, a magnetic disk, flash memory, integrated circuits, or any other non-transitory digital processing apparatus memory device.

[0062] Although the foregoing has been described in some detail for purposes of clarity, it will be apparent that certain changes and modifications may be made without departing from the principles thereof. It should be noted that there are many alternative ways of implementing both the systems and methods described herein. Accordingly, the present embodiments are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope and equivalents of the appended claims.

WHAT IS CLAIMED IS:

1. A method performed by a system comprising a processor and a non-transitory computer-readable storage medium storing instructions that, when executed, cause the system to perform the method, the method comprising:

receiving a wrapped user key associated with a user in an execution environment associated with a software application;

generating, using a protected client module executing within the execution environment provisioned to the system by a trusted service, a protected user key based on the wrapped user key and a protected private key associated with the protected client module; and

performing, by the protected client module, at least one secure operation within the execution environment using the protected user key.

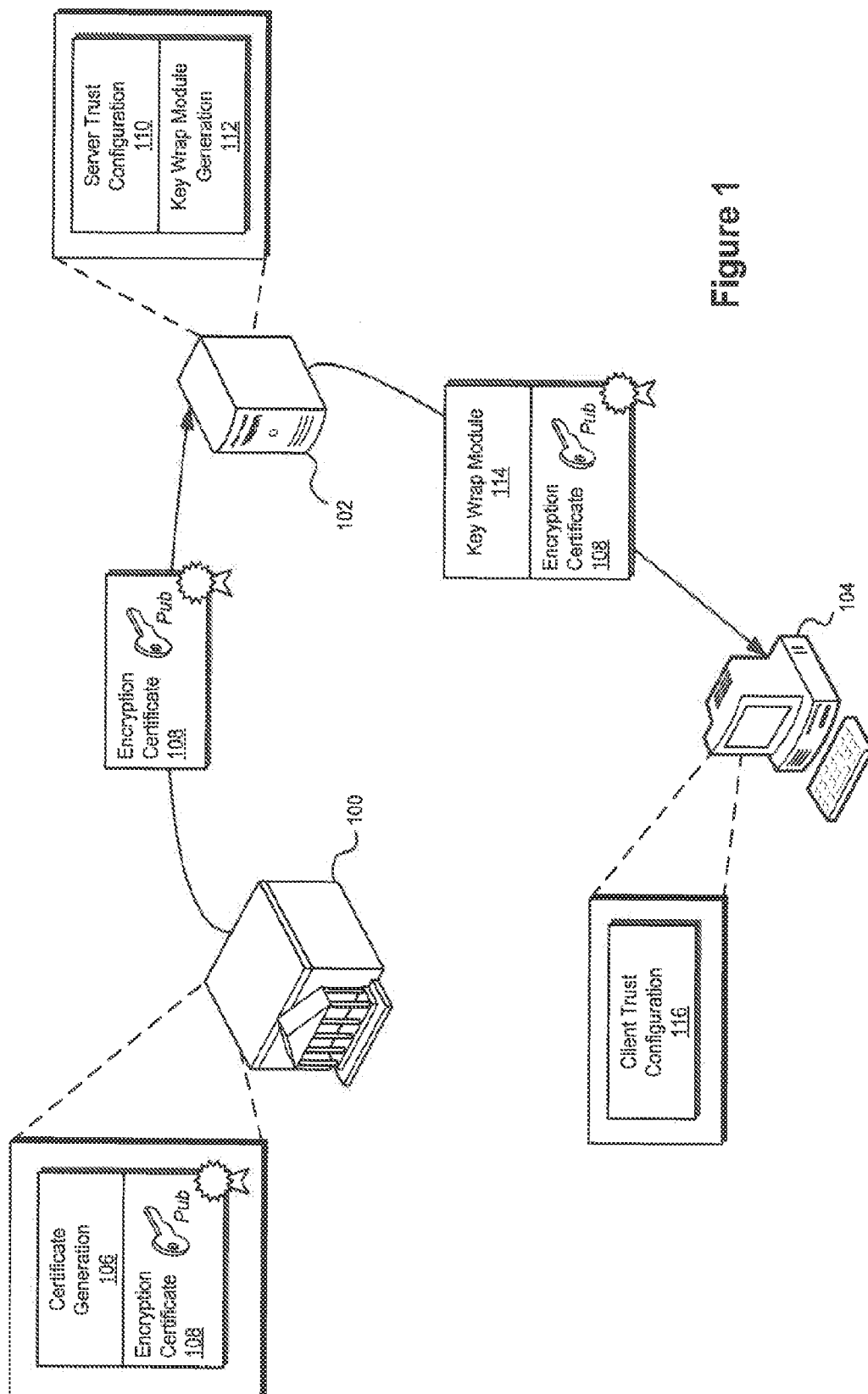
2. The method of claim 1, wherein the execution environment comprises a sandboxed execution environment.

3. The method of claim 1, wherein the software application comprises a browser application.

4. The method of claim 3, wherein the protected client module comprises a script application executing within the execution environment associated with the browser application.

5. The method of claim 1, wherein the wrapped user key comprises a user key wrapped using a public key provisioned by the trusted service corresponding to the protected private key.
6. The method of claim 1, wherein the protected private key comprises a white-box protected private key.
7. The method of claim 6, wherein the protected user key comprises a white-box protected user key.
8. The method of claim 1, wherein the method further comprises:
 - receiving a wrapped server key associated with a server in the execution environment associated with the software application;
 - generating, using the protected client module executing within the execution environment, a protected server key based on the wrapped server key and the protected private key.
9. The method of claim 8, wherein the wrapped server key comprises a server key wrapped using a public key provisioned by the trusted service corresponding to the protected private key.
10. The method of claim 9, wherein the protected server key comprises a white-box protected server key.
11. The method of claim 8, wherein performing the at least one secure operation further comprises performing the at least one secure operation further using the protected server key.

12. The method of claim 1, wherein the secure operation comprises a cryptographic transaction.
13. The method of claim 1, wherein the secure operation comprises an encryption operation.
14. The method of claim 1, wherein the secure operation comprises a decryption operation.
15. The method of claim 1, wherein the secure operation comprises a cryptographic signature operation.
16. The method of claim 1, wherein the secure operation comprises a cryptographic signature verification operation.



25

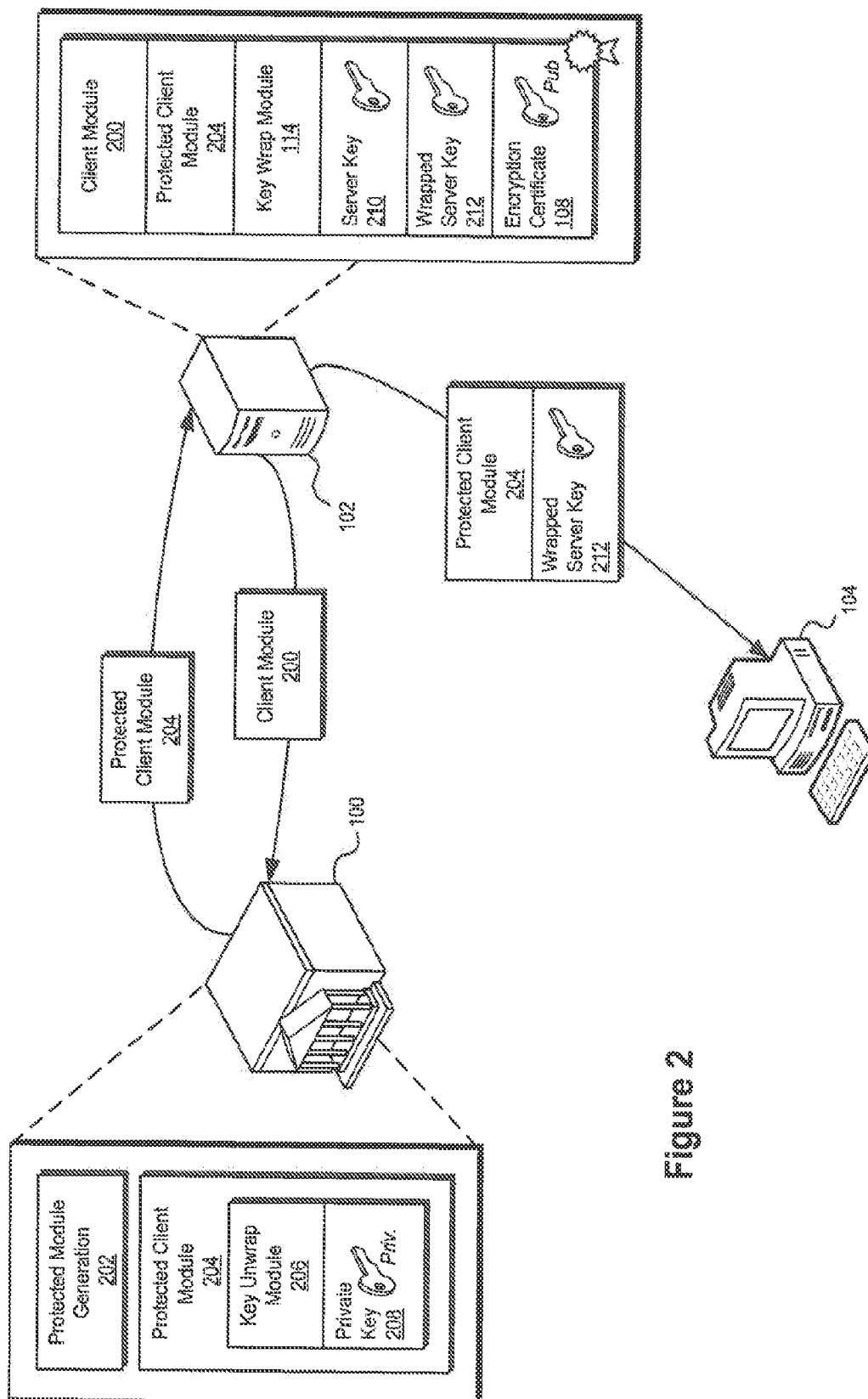
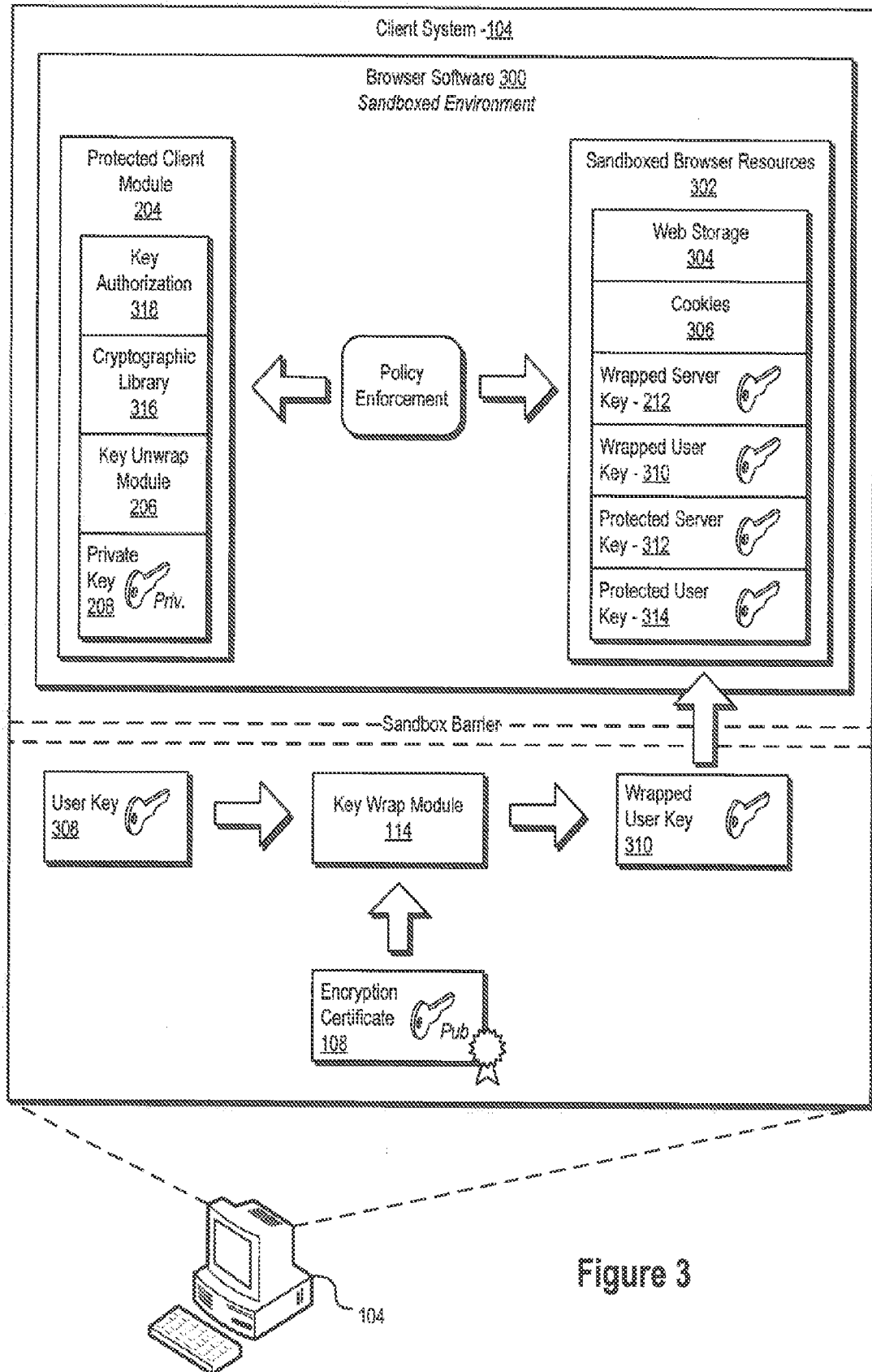


Figure 2



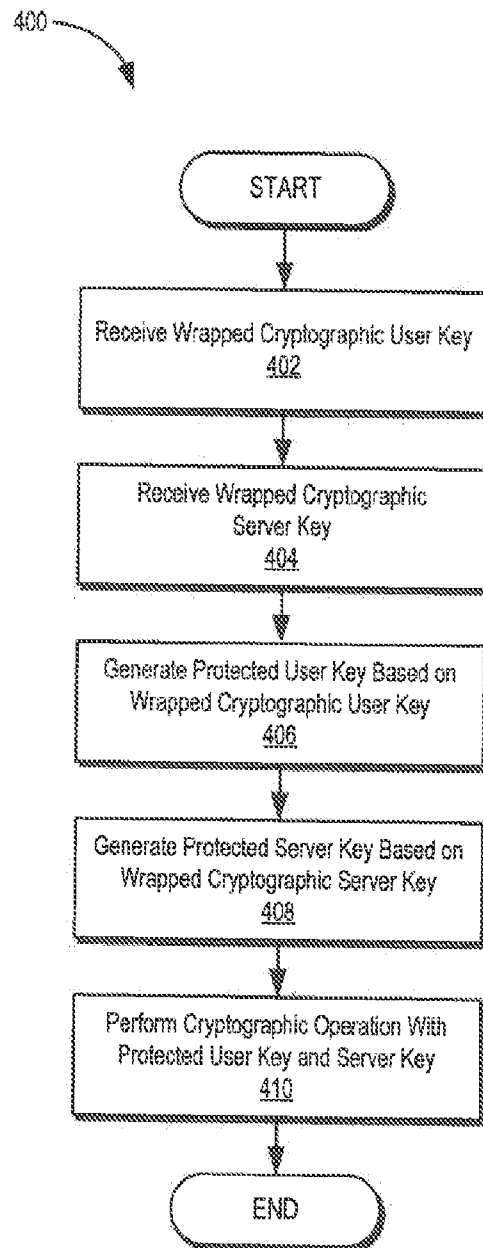


Figure 4

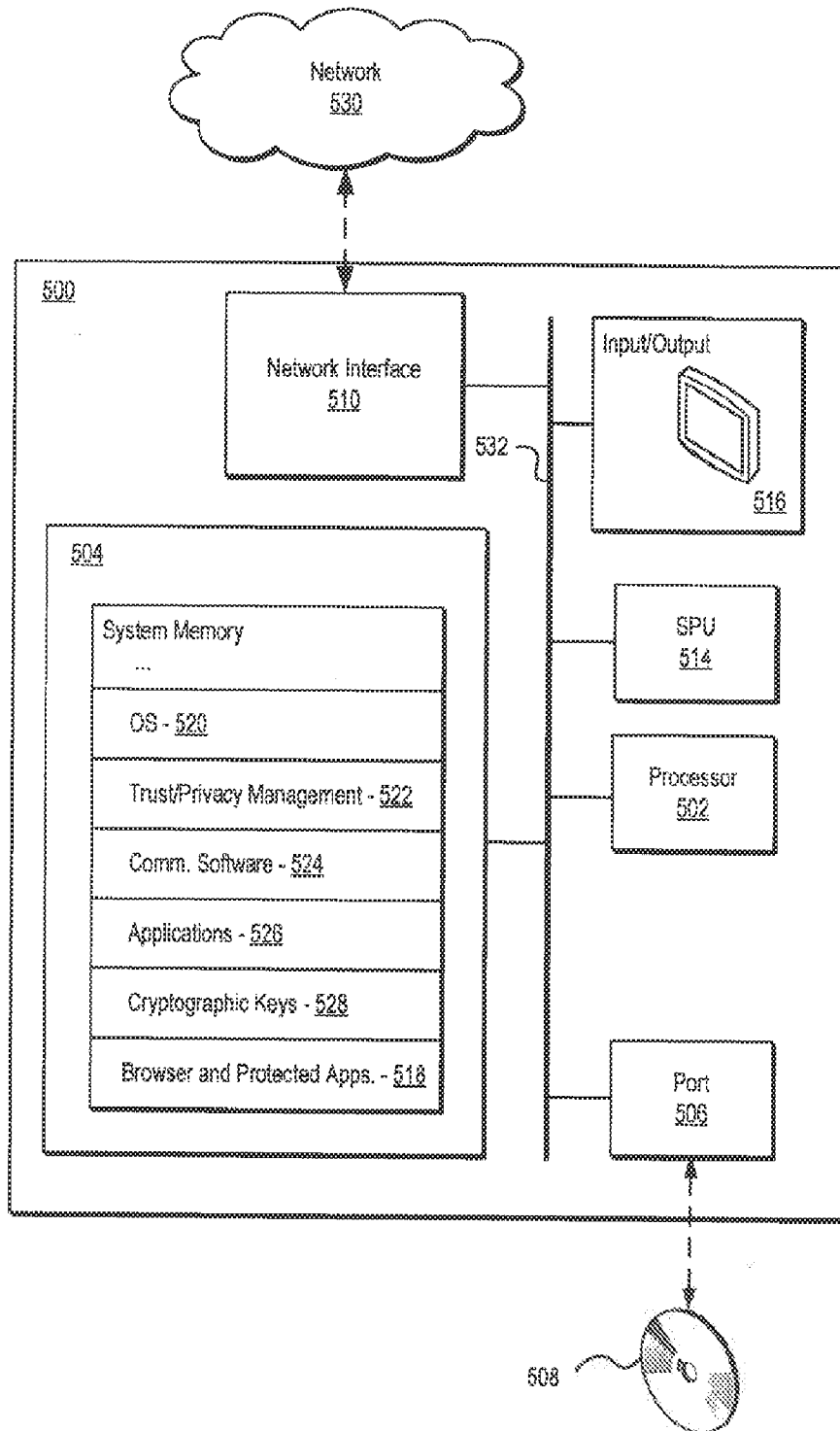


Figure 5

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/12(2013.01)i, G06F 21/60(2013.01)i, G06F 21/53(2013.01)i, H04L 9/08(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/12; H04L 9/14; H04L 29/08; H04L 29/06; H04L 9/32; H04L 9/00; G06F 21/60; G06F 21/53; H04L 9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & keywords: wrapp, cryptographic, encrypt, user key, private key, public key, sandbox, whitebox, browser, and similar terms**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008-0080708 A1 (DONALD KENT MCALISTER et al.) 03 April 2008 See paragraphs [0028]-[0031]; claims 1-2; and figures 3-4.	1-16
A	EP 2341682 A1 (KABUTO OY) 06 July 2011 See paragraphs [0007]-[0023].	1-16
A	US 2014-0289535 A1 (JOSEPH CHER CHUEN GAN) 25 September 2014 See paragraphs [0015]-[0023]; and figure 2.	1-16
A	US 2002-0172367 A1 (DAVID G. MULDER et al.) 21 November 2002 See paragraphs [0023]-[0027]; and figure 3.	1-16
A	US 2011-0314271 A1 (BOCCON-GIBOD GILLES et al.) 22 December 2011 See paragraphs [0022]-[0036]; and figure 1.	1-16



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier 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

02 May 2016 (02.05.2016)

Date of mailing of the international search report

03 May 2016 (03.05.2016)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

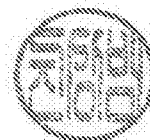
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

CHIN, Sang Bum

Telephone No. +82-42-481-8398



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/012726

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0080708 A1	03/04/2008	WO 2008-042175 A2 WO 2008-042175 A3	10/04/2008 30/10/2008
EP 2341682 A1	06/07/2011	FI 20096404 A FI 20096404 D0	30/06/2011 29/12/2009
US 2014-0289535 A1	25/09/2014	AU 2012-337403 A1 AU 2012-337403 B2 CN 103988467 A EP 2795829 A1 EP 2795829 A4 SG 189388 A1 US 9054865 B2 WO 2013-074041 A1	12/06/2014 30/04/2015 13/08/2014 29/10/2014 24/06/2015 31/05/2013 09/06/2015 23/05/2013
US 2002-0172367 A1	21/11/2002	CA 2386491 A1 WO 0209-3849 A2 WO 0209-3849 A3	16/11/2002 21/11/2002 23/01/2003
US 2011-0314271 A1	22/12/2011	US 2015-0244523 A1 US 8874896 B2	27/08/2015 28/10/2014