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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 January 2022 (13.01.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/010525 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/50* (2021.01)
H04W 12/033 (2021.01) *H04W 4/80* (2018.01)
H04W 12/06 (2021.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2020/062368

(22) International Filing Date:
25 November 2020 (25.11.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/925,343 10 July 2020 (10.07.2020) US

(71) Applicant: **WESTERN DIGITAL TECHNOLOGIES, INC.** [US/US]; 5601 Great Oaks Parkway, San Jose, CA 95119 (US).

(72) Inventors: **MASTENBROOK, Brian, Edward**; C/-5601 Great Oaks Parkway, San Jose, CA 95119 (US). **ARNOD, David, Robert**; C/-5601 Great Oaks Parkway, San Jose, CA 95119 (US).

(74) Agent: **MORGAN, Devin S.**; PATENT LAW WORKS LLP, 310 East 4500 South, Suite 400, Salt Lake City, UT 84107 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,

WO 2022/010525 A1

(54) Title: WIRELESS SECURITY PROTOCOL

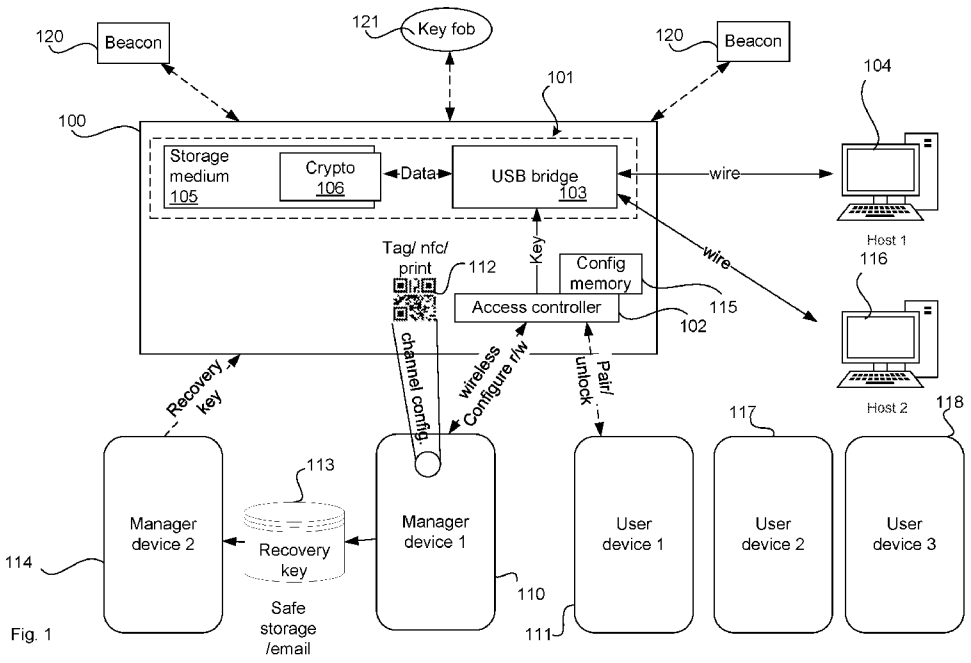

Fig. 1

(57) Abstract: This disclosure relates to a data storage device. A data port transmits data between a host computer system and the data storage device over a data channel. The device repeatedly broadcasts advertising packets over a wireless communication channel different from the data channel. Each advertising packet comprises a random value and a message authentication code calculated based on the random value and an identity key. The identity key is readable by a device to be connected and in proximity of the data storage device out of band of the data channel and the communication channel. The identity key enables the device to be connected to verify the message authentication code based on the random value and the identify key to thereby authenticate the data storage device.

[Continued on next page]

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))*

Wireless security protocol

Technical Field

[0001] This disclosure relates to a wireless security protocols.

Background

[0002] The Bluetooth standard has gained widespread popularity due to its simplicity in pairing devices with each other. In particular for applications with low security requirements, such as connecting a media player or phone to a wireless headset, Bluetooth is the solution of choice.

[0003] However, there are concerns for applications with high security requirements. For example, in some application scenarios a manager device is to be connected wirelessly to a data storage device, such as to an external hard disk drive (HDD) or solid state drive (SSD) that can be connected to a host computer system via a Universal Serial Bus (USB). If a manager device, such as a mobile phone is to be connected wirelessly to such devices to perform administrator tasks, it is important that this connection is secure to prevent unauthorized access, corruption or loss of data stored on the data storage device. Current Bluetooth standards are associated with concerns, in particular in relation to privacy. It is desirable that the manager device does not need to share private information, such as keys, device information etc., with an unknown data storage device before the data storage device is authenticated. It would be undesirable, for example, if a malicious device could integrate a near field communication (NFC) chip that impersonates a valid data storage device and successfully pairs with the manager device to gain information about the manager device.

Summary

[0004] This disclosure relates to a security protocol that is based on an out of band communication of an identity key from a server to client. The identity key can then be used to secure a communication channel and can then be authenticated by the server using a certificate linked to a root certificate accessible by the client. As a result, the client and the server do not need to share any private information until the server is authenticated.

[0005] More particularly, before the connection is established the server calculates a message authentication code (MAC) using the identity key and a random value. The random value is sent to the client with the MAC. The client can re-compute the MAC based on the random value and the identity key obtained out of band. In response to determining that the received MAC and the re-calculated MAC match, the client has authenticated the server. It is noted that this initial authentication is possible without the server or the client having to provide any private information. Since the MAC is calculated using the identity key, only user devices in proximity can re-calculate the MAC. To all other devices, the advertising packets appear random. In case of multiple servers sending advertising packets and multiple identity keys being available, the client can try each identity key and attempt re-calculation of the MAC. If it matches, the client has established that the matching identity key is for the device with the matching MAC.

[0006] Disclosed herein is a data storage device comprising a data path, a data store and an access controller. The data path comprises a data port configured to transmit data between a host computer system and the data storage device over a data channel, wherein the data storage device is configured to register with the host computer system as a block data storage device; a non-volatile storage medium configured to store encrypted user content data; and a cryptography engine connected between the data port and the storage medium and configured to use a cryptographic key to decrypt the encrypted user content data stored on the storage medium in response to a request from the host computer system. The data store is configured to store an identity key. The access controller is configured to repeatedly broadcast advertising packets over a wireless communication channel different from the data channel, each advertising packet comprising a random value and a message authentication code calculated based on the random value and the identity key. The identity key is readable by a device to be connected and in proximity of the data storage device out of band of the data channel and the communication channel. The identity key configured to enable the device to be connected to verify the message authentication code based on the random value and the identity key to thereby authenticate the data storage device.

[0007] In some embodiments, the data store is further configured to store a data storage device certificate that is configured to be cryptographically linked to a root certificate that is accessible by the device to be connected; and the access controller is further configured to calculate a signature verified by the data storage device certificate and to send the data storage device certificate and the signature to the device to be connected to enable the device to be connected to authenticate the data storage device.

[0008] In some embodiments, the certificate comprises a hash value of the identity key to bind the certificate to the data storage device from which the identity key is readable out of band.

[0009] In some embodiments, the root certificate is accessible by the device to be connected through an application installed on the device to be connected from an authenticated provider cryptographically associated with the root certificate.

[0010] In some embodiments, the advertising address of the broadcast advertising packets is selected uniformly at random.

[0011] In some embodiments, each advertising packet further comprises a service identifier of the data storage device, and wherein the message authentication code is calculated based on the random value, the identity key and the service identifier.

[0012] In some embodiments, the access controller is further configured to receive through the wireless communication channel from the device to be connected, a first nonce value; generate a second nonce value and broadcast through the wireless communication channel, a the second nonce value; derive a cryptographic key from the identity key, the first nonce value and the second nonce value using a key-derivation function; and secure the wireless communication channel with the device to be connected using the cryptographic key.

[0013] In some embodiments, the communication channel is Bluetooth Low Energy.

[0014] In some embodiments, the identity key is readable by the device to be connected by means of a quick response (QR) code affixed to the data storage device or means of a near field communication (NFC) tag integrated in the data storage device.

[0015] Disclosed herein is a client device comprising a processor and memory, the memory comprising instructions executable by the processor to: receive an identity key from a server out of band of the wireless communication channel; receive an advertisement packet broadcast by the server over the wireless communication channel, the advertisement packet comprising a random value and a message authentication code calculated by the server device based on the random value and the identity key; verify the message authentication code based on the random value and the identity key to thereby authenticate the server; and upon authentication of the

server, generate a cryptographic key based on the identity key to secure the wireless communication channel with the server device.

[0016] In some embodiments, the memory further comprises instructions executable by the processor to access a root certificate cryptographically linked to a certificate of the server,

[0017] Disclosed herein is a method for securing a wireless communication channel between a client device to be connected and a server device. The method comprises repeatedly performing the steps of generating a random value; calculating based on the random value and an identity key a message authentication code, the identity key being readable by the client device to be connected and in proximity of the server device out of band of the wireless communication channel, the identity key enabling the client device to verify the message authentication code based on the random value and the identity key to thereby authenticate the server device; and broadcasting an advertising packet over the wireless communication channel, the advertising packet comprising the random value and the message authentication code calculated based on the random value and the identity key.

[0018] In some embodiments, the method further comprises in response to receiving a connection request from the client device, sending a server certificate issued by the server device to the client device, the server certificate comprising a hash value of the identity key to bind the certificate to the server device from which the identity key is readable out of band.

[0019] In some embodiments, the server certificate is cryptographically linked to on a root certificate that is accessible by the client device.

[0020] In some embodiments, the method further comprises calculating a signature; and in response to receiving the connection request from the client device, sending the signature to the client device.

[0021] In some embodiments, the signature is verified by the server certificate by using a private key to calculate the signature, the private key being verified by the server certificate.

[0022] In some embodiments, the server certificate comprises a public key, corresponding to the private key, for verifying the signature.

[0023] In some embodiments, the method further comprises calculating a hash of the identity key, a nonce received from the client device, and the random value; and calculating the signature for the hash based on the identity key and verified by the server certificate.

[0024] In some embodiments, authenticating the server device comprises receiving a server certificate from the server device issued by the server device and a signature calculated by the server device based on the identity key and verified by the server certificate; verifying the server certificate against a root certificate; verifying the signature against the server certificate; and upon verification of the signature, securing the wireless communication channel with the server device.

[0025] Disclosed herein is a server device for securing a wireless communication channel between a client device to be connected and the server device, the server device comprising a processor configured to repeatedly perform the steps of generating a random value; calculating based on the random value and an identity key a message authentication code, the identity key being readable by the client device and in proximity of the server device out of band of the wireless communication channel, the identity key enabling the client device to verify the message authentication code based on the random value and the identity key to thereby authenticate the server device; and broadcasting an advertising packet over the wireless communication channel, the advertising packet comprising the random value and the message authentication code calculated based on the random value and the identity key.

Brief Description of Drawings

[0026] A non-limiting example will now be described with reference to the following drawings:

Fig. 1 illustrates a data storage device, according to an embodiment.

Fig. 2 illustrates a section of the configuration memory of the data storage device of Fig. 1, according to an embodiment.

Fig. 3 illustrates a control flow between the authorized device and the access controller of Fig. 1, according to an embodiment.

Fig. 4 illustrates a certificate issued by the data storage device and sent by the authorized device to the data storage device to unlock the data storage device, according to an embodiment.

Fig. 5 illustrates a method for securing a wireless communication channel between a client device and a server device, according to an embodiment.

Fig. 6 illustrates a protocol for securing a communication channel between a data storage device and a client device to be connected, according to an embodiment.

Description of Embodiments

[0027] Fig. 1 illustrates a data storage device (DSD) 100 comprising a data path 101 and an access controller 102, according to an embodiment. The data path 101 comprises a wire-based data port 103, which is provided in Fig. 1 by a USB bridge, for transmission of data between a host computer system 104 and the DSD 100. In other embodiments, the data path 101 comprises a wireless data port (not shown) for wireless transmission of data between the host computer system 104 and the DSD 100. The DSD 100 registers with the host computer system 104 as a mass data storage device providing the functionality to the operating system of the host computer system 104 of a block data storage device. DSD 100 further comprises a non-transitory storage medium 105 to store encrypted user content data, noting that the user content data is the data that a user would typically want to store on a DSD, such as files including image files, documents, video files, etc. The storage medium may be a solid state drive (SSD), hard disk drive (HDD) with a rotating magnetic disk or other non-volatile storage media. Further, the storage medium may be a block data storage device, which means that the user content data is written in blocks to the storage medium 105 and read in blocks from the storage medium 105.

Command set

[0028] In one example, storage medium 105 comprises a cryptography engine 106 in the form of a dedicated and/or programmable integrated circuit that encrypts data to be stored on storage medium 105 and decrypts data to be read from storage medium 105. In such examples, the storage medium may provide a Small Computer System Interface (SCSI) or Advanced Technology Attachment (ATA) command set according to the Opal specification by the Trusted Computing Group (TCG).

[0029] Program code stored on the cryptography engine 106 enables the cryptography engine 106 to receive, interpret and execute commands received from host computer system 104. For example, cryptography engine 106 may be configured to implement the standard ATA or serial ATA (SATA) and/or ATA Packet Interface (ATAPI) command set, which is available from

Technical Committee T13 noting that identical functionalities can be implemented within TCG Opal, SCSI and other proprietary architectures. The command set comprises a READ SECTORS command with a command input of the count of sectors and the starting sector (noting that "sector" is used synonymously with "block" herein). Accordingly, there is a corresponding write command. It is noted that there is a data storage device driver installed on host computer system 104. The data storage device driver (not shown) uses the command set to provide high-level services to the operating system, such as file read functionalities. In some examples, the data storage device driver is a generic driver supplied as part of the operating system without support for device-specific encryption commands since the encryption functionality is hidden from the host computer system 104 and handled internally within DSD 100 as described below. This means that no additional drivers need to be installed to use the full functionality disclosed herein.

[0030] The command set provided by the cryptography engine 106 to the data port 103 (but not forwarded to host computer system 104) may include a command set from the ATA SECURITY feature set. In particular, the command set may include the command SECURITY SET PASSWORD or a corresponding command from TCG Opal to set a password for reading and writing user content data to the storage medium 105.

[0031] In this sense, cryptography engine 106 is connected between the data port 103 and the storage medium 105 and is configured to use a cryptographic key to encrypt user content data to be stored on the storage medium 105 and to decrypt the encrypted user content data stored on the storage medium 105 in response to a request from the host computer system 104. In some examples, the ATA SECURITY feature set is used only by data port 103 and not by host 104. That is, the access controller 102 provides the necessary input for the data port 103 to issue the ATA SECURITY commands to the cryptography engine 106. For example, the access controller 102 may provide a key to the data port 103, which the data port 103 then forwards to the cryptography engine 106 via the SECURITY SET PASSWORD command. The interface between the access controller 102 and the data port 103 may be an Inter-Integrated Circuit (I2C) bus, which is particularly useful in cases where this bus is already implemented in existing chips. However, it is possible to use many other communication architectures including bus, point-to-point, serial, parallel, memory based and other architectures.

[0032] Note that the separation of functionalities in dedicated chips as shown in Fig. 1 is only one possible example implementation. Therefore, it is possible to combine functionalities or split the functionalities further. For example, data port 103 may be integrated with access controller

102 into a single chip with a single core. In other cases, the data port 103 and the access controller 102 can be integrated with cryptography engine 106 into a single dedicated chip with a single core. Of course, all chips may have multiple cores.

[0033] In one example, the following components are used:
Data port 103: USB 3.1 Gen 2 10 gigabits per second (Gb/s) interface
Access controller 102: nRF52840 system-on-chip (SoC) from Nordic Semiconductor

[0034] It is noted that for the functionality disclosed herein, the access controller 102 plays the leading role and will be described in more detail below, noting again that the tasks may be separated into separate chips in other examples. When reference is made to a 'configuration' of the access controller 102 or the access controller 102 being 'configured' to perform a certain step, this is to be understood to relate to program code that is stored on non-volatile memory in the DSD 100 on program memory (not shown for clarity) and executed by the access controller 102.

[0035] In other examples, some or all steps disclosed herein may be performed by hardware circuitry without program code. In particular, encryption primitives may be implemented by dedicated hardware circuitry for performance and security reasons. For example, commands that are particularly computationally demanding, such as elliptic curve multiplication or exponentiation, may be implemented by an Arithmetic Logic Unit (ALU) specifically designed for this calculation, such that the calculation can be performed in a single or a smaller number of processor cycles compared to using a sequential program in a general purpose microcontroller. It is further noted that the chips included in DSD 100 are microcontrollers, which means in this context that they do not run under an operating system that provides a hardware abstraction layer but the program code acts directly on the hardware circuit. While elliptic curve cryptography is used herein as examples for reasons of computational efficiency and security, it is noted that other public-key cryptosystems, such as the Rivest-Shamir-Adelman (RSA) cryptosystem, could equally be used.

[0036] Returning back to Fig. 1, there are a number of devices in addition to host computer system 104 that are external to the DSD 100 and that act in the process of unlocking the DSD 100 and providing a key to the cryptography engine 106 so that, ultimately, decrypted data in plain text can be provided to host computer system 104.

[0037] In particular, there is a first manager device 110, which is a mobile phone in most examples. Installed on the manager device 110 is an application ('app') to perform the following steps. In this way, the following steps can be implemented in software by the manufacturer of the DSD 100 and distributed to the manager device 110 through a commonly accessible app store, such as Apple's App Store or Google Play. The app installed on manager device 110 performs steps to take ownership of the DSD 100 at which point all data on the DSD 100 is erased or otherwise made inaccessible. For example, data may be crypto-erased by securely deleting all cryptographic keys stored on DSD 100.

[0038] For simplicity of presentation, this disclosure describes steps as simply being performed by manager device 110 if they are implemented by the app. The manager device 110 sets up the DSD 100, which means the various different keys are generated to support the process disclosed herein. Manager device 110 registers a user device 111 with the DSD, so that the user device 111 is then referred to as the "authorized device" 111. In most examples, the authorized device 111 is also a mobile phone with an app installed that implements the steps described as being performed by the authorized device 111. However, other types of devices can be used as authorized devices, which will be explained below in relation to beacons and key fobs.

Taking ownership

[0039] The first step in using DSD 100 after purchase, unpacking and power-up is to install the app on manager device 110 and register a device as the manager device 110. For this process, the manager device 110 obtains a unique identifier of the DSD from the DSD. This unique identifier is referred to as the identity key (IDK). In the example illustrated in Fig. 1, the identity key is encoded in a quick response (QR) code 112 which is affixed to an external surface of the DSD 100. The app installed on manager device 110 has access to a camera and has a software module that extracts the encoded information from an image of the QR code 112. The manager device 110 captures an image of the QR code 112 using the camera, and decodes the identity key of DSD 100 from the QR code. In one example, the QR code encodes a Uniform Resource Locator (URL). In that case, a generic app can capture the QR code, which then automatically directs the phone to an application store where the app can be downloaded. The URL also includes the identity key so that the app can decode that identifier once the app is installed.

[0040] In another example, manager device 110 may read another tag or NFC chip affixed or integrated with DSD 100 to obtain the identity key. Using that identity key, the manager device

110 can then initiate a communication, such as wirelessly (e.g., over Bluetooth), with the DSD 100 and in particular, with the access controller 102.

Recovery Key

[0041] Upon taking ownership of the DSD 100, the access controller 102 generates a recovery key and provides the recovery key to the manager device 110. The recovery key can then be stored on a secure storage 113 or printed and locked away. Ultimately, the recovery key can be used by a backup manager device 114 to assume the manager role that the manager device 110 previously had.

Registration of authorized device

[0042] Once the DSD 100 is initially configured during the take ownership process, manager device 110 registers the authorized device 111. Typically, there may be multiple authorized devices registered with a single DSD 100 so manager device 110 registers the authorized device as one of multiple authorized devices. More particularly, access controller 102 receives from the manager device 110 a public key associated with a private key stored on user device 111. The manager device 110 itself may have received the public key from the user device 111 via email, by scanning a QR code displayed on the user device 111 or any other way. At this point in time, device 111 is not yet authorized and therefore, simply referred to as "user device 111". Once user device 111 is authorized, it is referred to as "authorized device 111". Access controller 102 creates authorization data that indicates that user device 111 is an authorized device (as described below) and stores the authorization data associated with the public key on the configuration memory 115 to register the user device 111 as one of the multiple authorized devices. This means keys and other data associated with authorized device 111 are created and stored as described below. A user can then use the authorized device 111 to unlock the DSD 100 simply by bringing the authorized device 111 into wireless communication range, such as within Bluetooth range. Again, the steps performed by authorized device 111 are encoded in an app installed on authorized device 111. Depending on configuration parameters, the user may be required to unlock authorized device 111 before DSD 100 can be unlocked.

[0043] More particularly, access controller 102 has access to a non-volatile configuration data store, such as configuration memory 115, which may be a flash memory that is external to the access controller 102 (but may equally be integrated into access controller 102). Configuration

memory 115 may also store the program code that implements the steps described herein as being executed by access controller 102. It is noted that some examples herein are configured under the assumption that an attacker can readily unsolder and read out the content of the configuration memory 115 but should not be able to decrypt the user content data with that information. That is, in those examples, no keys are stored persistently in plain text on configuration memory 115 or elsewhere in DSD 100 on non-volatile memory.

[0044] Once the cryptographic keys are available in plain text, they are stored only in volatile memory (not shown). This means that a power-down of the DSD 100 erases all cryptographic keys stored in plain text. Additional circuitry may be provided to reset all remaining charges on power-down, power-up or external reset, so that it is physically impossible in practice to recover any information from volatile memory. In many cases, power-down and erasure of all volatile memory occurs as a result of the user disconnecting the USB cable from the host computer system 104. In other examples, a secondary power supply is used which needs to be disconnected to power down the DSD 100 to delete the volatile memory.

Challenge-Response

[0045] Configuration memory 115 has stored thereon data that is specific for the registered authorized device 111. This data may be referred to as an identifier of the authorized device 111 or as a public key associated with a corresponding private key stored on the authorized device 111. The public key may be a "transport public key" (TPK) and is generated by the authorized device 111 on first launch of the app by executing an elliptic curve cryptography (ECC) primitive ECC-Pub({transport private key}). (Recall that while elliptic curve cryptography is used herein as examples for reasons of computational efficiency and security, it is noted that other cryptographic techniques could equally be used.) The corresponding private key is stored on authorized device 111. The access controller 102 is configured to use the identifier (e.g., transport public key) or generate and store a further public key, to generate a challenge for the authorized device 111. It is noted here that the challenge is unique in the sense that each challenge is different, so that a subsequent challenge is different from any previous challenges. As described below, this is achieved by multiplying the stored data by a random blinding factor. Then, the access controller 102 sends the challenge to the authorized device 111 over a communication channel that is different from the data path. For example, the data path may include a wire-based USB connection while the communication channel between the access controller 102 and the authorized device 111 is a wireless (e.g., Bluetooth) connection.

[0046] In one example, a re-enrolment process takes place responsive to the authorized device connecting with the DSD 100 for the first time after the authorization data was created and stored on configuration memory 115 associated with the public key of the authorized device 111 received from the manager device 110. During the re-enrolment process, DSD 100 updates the authorization data and as set out below may request authorized device 111 to generate an unlocking public key (and a corresponding unlocking private key) in addition to the transport public key. The authorized device 111 then provides the unlocking public key to the access controller 102.

[0047] This has the advantage that the two corresponding private keys (transport private key and unlocking private key) can be stored separately on the authorized device and both keys can have different access policies. For example, transport public key may be accessible at any time, even if the authorized device 111 is locked (e.g., by a screen lock or time out), so as to allow continuous communication between authorized device 111 and DSD 100. To unlock DSD 100, however, the access policy of the unlocking private key may require that the user unlocks authorized device 111, enters a personal identification number (PIN), provides biometric or other authentication. This way, DSD 100 cannot be unlocked by a stolen authorized device. Since unlocking DSD 100 is performed only once while DSD 100 is powered, the increased security does not significantly reduce user convenience.

[0048] The authorized device 111 can calculate a response to the challenge that cannot be calculated by any other device that is not registered with the DSD. More specifically, the correct response cannot be calculated by a device that does not have access to data that corresponds to the identifier stored on configuration memory 115. For example, authorized device 111 uses the stored unlocking private key that is associated with the corresponding unlocking public key stored on configuration memory 115, to calculate the response to the challenge.

[0049] The access controller 102 receives the response to the challenge from the authorized device 111 over the communication channel. It is noted here that if the access controller 102 simply validates the response to the challenge and upon success, reads the cryptographic key from configuration memory 115, the cryptographic key would be stored in plain text, which is undesirable since this would enable an attacker to disassemble the DSD 100 and read the key from configuration memory 115 to access the user content data stored on storage medium 105.

Calculate key

[0050] So, instead, access controller 102 calculates the cryptographic key based at least partly on the response from the authorized device 111. This means the cryptographic key is not a pure function of the response but involves other values as described in more detail below. In summary, the cryptographic key is stored in encrypted form on configuration memory 115 and the response, which is based on the private key stored on the authorized device, enables the calculation of the secret that decrypts the cryptographic key.

[0051] Throughout this disclosure, reference may be made to 'wrapping' of keys, which simply means that the key is encrypted by another key (i.e., by the "secret"). In many cases of 'wrapping' the encryption is symmetric such that a single secret (key) exists that can decrypt the encrypted key (without a public key associated with the secret). In one example, symmetric encryption uses the Advanced Encryption Standard (AES) primitive.

[0052] Finally, access controller 102 provides the cryptographic key to the cryptography engine 106 (via data port 103 in this example) to decrypt the encrypted user content data stored on the storage medium 105 of the DSD 100. As mentioned above, once the access controller 102 has calculated the cryptographic key, the access controller 102 provides the cryptographic key to the data port 103 in plain text and the data port 103 issues the SECURITY SET PASSWORD command to the cryptography engine 106 including the cryptographic key.

[0053] It is noted that where reference is made to 'unlocking' the device, this can refer to the entire process described above including the challenge, the response to the challenge and sending of the cryptographic key to the cryptography engine 106 to allow plain text read commands issued by the host computer system. In other examples, the challenge and the response to the challenge are considered as being part of a separate 'connect' step. During the following 'unlocking' step the access controller 102 then sends the cryptographic key to the data port 103 to allow access to the user content data.

[0054] It is noted, as an aside, that it may be possible for an attacker to eavesdrop on the key transmission from the access controller 102 to the data port 103 and then to the cryptography engine 106. However, the transmission of the key is not over a public network, so this eavesdropping would require gaining access to and disassembling the unlocked DSD without removing power from the DSD 100. This scenario may be discarded as a threat since in this scenario the user content data is available anyway on host computer system 104. In other words, while the DSD 100 is connected and unlocked, data is available to the rightful user and the

attacker. But once the user disconnects the DSD from host computer system 104, this eavesdrop attack is not possible anymore. Therefore, this attack is not further considered.

[0055] For completeness it is noted that once the cryptography engine 106 has received the cryptographic key, the host computer system 104 can issue ordinary READ SEGMENT commands and transparently access the encrypted data without any perceivable difference to accessing an unencrypted device. This is particularly the case where the cryptography engine has hardware cryptography modules to enable encryption and decryption at or above the read and write speed of the storage medium 105 and/or the data port 103. However, the user can disconnect the DSD 100 to lock it. This way, the DSD 100 can be carried by the user through insecure locations where the DSD 100 can be lost or stolen, but it is very difficult for another person to decrypt the encrypted user content data stored on storage medium 105. If the user maintains possession of the DSD, the user can connect it to a second host computer system 116, conveniently unlock the DSD 100 with his authorized device 111 (e.g., phone) and readily access the encrypted user content data stored on the storage medium 105.

[0056] For user convenience, the data port 103 can be configured such that if the DSD is locked, it registers with host computer system 104 as a mass data storage device with storage medium not present, similar to an SSD card reader with no card inserted. Once the authorized device 111 is connected to DSD 100 and the DSD 100 is unlocked, data port 103 switches to storage medium present, similar to a card reader that had an SSD card inserted. Such a configuration would avoid any warnings from being generated by the operating system of the host computer system 104 about the data not being accessible or access being denied. Instead, all user interaction would be performed by the app installed on the authorized device, which is fully controlled by the manufacturer of the DSD, so user experience can be optimized. As shown in Fig. 1, there may be further mobile phones acting as authorized devices 117 and 118.

Beacons and key fobs

[0057] Considering Fig. 1 again, it can be seen that there are further devices, such as beacons 120 and key fob 121. These devices can also be considered as “authorized devices” since they can operate essentially the same as the authorized device 111. Before initial registration by the manager device 110, these devices are referred to as “device to be authorized”. When reference is made to a “user device” herein (mainly describing mobile phone 111 before initial registration), this also applies to the beacons 120 and key fob 121 except when noted otherwise,

such as in cases where user input is required. Beacons 120 and key fob 121 also have their own private key stored securely so that they can respond to a challenge that is specific for one beacon or key fob. However, since the beacons 120 and key fob 121 have no user input, the initiation of communication may be slightly different. More particularly, beacon 120 and key fob 121 may periodically send advertisements to broadcast their existence and the DSD 100 then initiates the communication with beacon 120 and/or key fob 121, which prompts them to send their transport public key. This is in contrast to the authorized device 111, which sends the transport public key to the DSD 100 to initiate the communication.

[0058] In further examples, beacons 120 are in a de-activated state when they are powered up and need to be activated by a manager device 110 or an authorized device 111. This activation may follow a similar process as unlocking DSD 100. That is, manager device 110 or authorized device 111 or both are registered with each beacon 120 with their transport public keys and respond to a challenge as described herein. Thus, a device may be registered as a manager device or an authorized device with one of the beacons 102 and/or key fob 121 without being registered with the DSD 100 itself. If the response to the challenge is valid, beacons 120 then unlock DSD 100. In yet a further example, beacons 120 are registered with each other, such that manager device 110 and/or authorized device 111 need to activate only one of the beacons 120 and the remaining beacons become activated automatically. In other words, the activation 'spreads' through the beacon network as long as the beacons are in range of each other.

[0059] It is noted that the only piece of information that the authorized devices 111, 117, 118, 120 and 121 provide to the manager device 110 to become registered is one public key for each device. In other words, each device provides its own public key corresponding to a private key that is securely stored on that device. Therefore, if an attacker intercepts the initial communication between one of the devices 111, 117, 118, 120 and 121 and the manager device 110, the only information that the attacker can obtain is the public key. As the name suggests, the public key is not secret and can be generally known. Therefore, the attacker has not gained any advantage. Further, the manager device 110 cannot use the public key to gain access to anything else related to the authorized devices. For example, the manager device cannot decrypt or unlock any other data storage devices with which the authorized device has been registered by other manager devices.

[0060] The access controller 102 receives the public keys of the authorized devices from the manager device 110 and generates authorization data. Access controller 102 stores the

authorization data on configuration memory 115 waiting for the authorized device to connect for the first time. On the first connection, access controller 102 performs a challenge-response for the authorized device and upon success, updates the authorization data to indicate that the authorized device is now fully registered. This first connection process is referred to as "re-enrolment" herein and details of generating the authorization data and the re-enrolment are provided below.

Elliptic curve cryptography

[0061] In one example, the challenge generated by the DSD 100 and sent to the authorized device 111 is based on elliptic curve cryptography. This has the advantages of shorter keys, which leads to more efficient communication and storage. Further, a large number of phones currently on the market provide dedicated functionality of elliptic curve cryptography within a secure hardware module. The secure hardware module securely stores the user's private keys and performs cryptographic primitives within the secure hardware module without the key leaving the secure hardware module and being sent to a general purpose processor core where the key may be subject to an attack for unauthorized retrieval. In one embodiment, the secure hardware module includes a separate processor that executes its own microkernel, which is not directly accessible by the operating system or any programs running on the phone. The secure hardware module can also include non-volatile storage, which is used to store 256-bit elliptic curve private keys. In one embodiment, the secure hardware module is a Secure Enclave coprocessor that is available on some Apple devices.

Authorized device data record

[0062] Fig. 2 illustrates a section of configuration memory 115, according to an embodiment. More specifically, Fig. 2 illustrates one record 201, in configuration memory 115, which is associated with one of multiple authorized devices and referred to herein as "authorization data". Further data records for further authorized devices are schematically indicated as empty dashed boxes but not considered in detail as they operate in a similar manner to record 201. In particular, each further data record comprises authorization data generated by the access controller 102 in response to receiving a public key of a user device from the manager device 110 and then updated during the first connection of the user device (then "authorized device"). For convenience, the data structure of configuration memory 115 is referred to as a 'table' comprising one or more 'records', where each record relates to one registered authorized device

and each record has multiple fields. It is noted, however, that other data structures can be used, such as JavaScript Object Notation (JSON), Extensible Markup Language (XML), binary formats, etc. In one example, each entry has a fixed length and the table has a fixed number of rows (i.e., entries). Within this disclosure, a 'record' may also be known as a 'row' or 'entry'.

[0063] Record 201 comprises a field for a pre-authorization key 202, which is used responsive to the authorized device 111 connecting to the DSD 100 for the first time. During this first connection, access controller 102 performs a number of steps that are referred to as "re-enrolment" as described below in more detail. The pre-authorization key 202 is generated from the identifier (e.g., the transport public key) of the authorized device 111. For example, access controller 102 may generate the pre-authorization key 202 by applying a key derivation function using the x-coordinate of the transport public key as an input parameter together with an authorized device slot key as salt value to the derivation function. The authorized device slot key may be a pseudo-random number (e.g., 16-bytes) stored on configuration memory 115 and can be used to encrypt data in authorized device certificates so that only the issuing DSD 100 can recover the information.

[0064] At that point, it can be said that the records stored on the configuration memory 115 are indexed by preauthorization key 202 based on an identifier of the authorized device (e.g., the transport public key). As described below with reference to Fig. 4, the index of record 201 may be stored in a certificate, as a slot number, during re-enrolment and at that point the pre-authorization key 202 can be replaced by a random value to make the configured DSD indistinguishable from a new device from the factory even with possession of the transport public key.

[0065] Record 201 further comprises a field for a first copy of a metadata wrapping key (MWK) 203 and a pre-authorization metadata wrapping key (PMWK) 214. Some fields in record 201 are encrypted which is indicated by double-lined boxes, where the single solid line boxes, inside the double-lined boxes, indicate the 'payload' such as the metadata wrapping key 203 and the pre-authorization metadata wrapping key 214. The corresponding encryption key, used to encrypt the payload, is noted at the bottom of the double-lined box. So, for example, metadata wrapping key 203 is encrypted by an authorized device metadata key (ADMK) 204. It should be noted that each encryption box may comprise an additional nonce that is concatenated with the payload data. This guarantees that the encrypted entry cannot be distinguished from random data

even with the possession of the encrypted data, such as the transport public key of the authorized device.

[0066] Record 201 further comprises a field for authorized device metadata (ADM) 205, which is a concatenation of a device type 206 (e.g., recovery key, key fob, beacon, phone, computer, watch, etc.), a role of the device 207 (e.g., manager or user), a name of the device 208 (e.g., "John's phone"), a transport public key 209, unlocking key metadata 210 (e.g., key restrictions of whether fingerprint, pin or no unlock is required), an ephemeral public key 211, and an unlocking public key 212. In one embodiment, the ephemeral public key 211 is an elliptic curve public key generated from a random ephemeral private key (EPK) using an Elliptic Curve Cryptography (ECC) primitive ECC-Pub(EUK). The ephemeral private key is not stored on configuration memory 115 or on the authorized device 111 but is discarded after creating the ephemeral public key. This means that the ephemeral private key is not stored on non-volatile memory but only on volatile memory. As result, a power-down of the memory leads to complete and irrecoverable loss (e.g., destruction) of the ephemeral private key. The unlocking public key 212 corresponds to an unlocking private key stored on authorized device 111 and is generated by authorized device 111 and provided to the access controller 102.

[0067] The authorized device metadata (concatenated with a further nonce) is encrypted by the metadata wrapping key (MWK) 213 that is also stored in encrypted form at 203. The main purpose of storing the encrypted metadata wrapping key 203 in entry 201 is to allow a manager user, who has access to the authorized device metadata key 204, to access the encrypted authorized device metadata 205. If the metadata wrapping key was not accessible to the manager, the manager would not be able to retrieve from the DSD 100 any information about which authorized devices are currently registered. In one example, the authorized device metadata key 204 is a single key for all authorized devices and is stored encrypted by a manager key. The manager key may be a pseudo-random value (e.g., 32 bytes) and generated by access controller 102 responsive to storage medium 105 being erased. The manager key is encrypted and stored for each paired manager device 110/114.

[0068] Record 201 further comprises a field for a second copy of device's role 220 concatenated with a user key 221 and a second copy of the metadata wrapping key 222. It is noted that both role 207/220 and metadata wrapping key 203/222 are stored in two copies, which are identical but encrypted using different keys. The purpose of storing two copies of the role 207/220 is to enable the access controller 102 to verify the role during connection (responsive to

the authorized device metadata being decrypted) as well as during unlocking (responsive to the user key 221 being decrypted). The purpose of storing the first copy of the metadata wrapping key 203 is to provide it to a manager device having access to the authorized device metadata key. The purpose of the second copy of the metadata wrapping key 222 is to provide it to a pre-authorized device during the first connection. The concatenated values 220, 221, 222 together are encrypted by an ephemeral unlock secret (EUS) 223 that is originally generated by a Diffie-Hellman method using the ephemeral private key corresponding to ephemeral public key 211 and the unlocking public key 212. The ephemeral unlock secret 223 can be recovered using the ephemeral public key 211 and an associated unlocking private key stored on the authorized device 111 and corresponding to unlocking public key 212. In other words, the ephemeral unlock secret 223 can be generated at the initial connection of the authorized device 111 to the DSD 100 using the ephemeral private key and the unlocking public key 212. It is noted that the ephemeral private key itself is not stored but nevertheless, the ephemeral unlock secret 223 can be recovered as described above. This means, the user key 221 is decryptable based on the response from the authorized device. It is noted that the user key 221 is identical for all authorized devices and can be used to decrypt user content data. This does not necessarily mean that the user key itself decrypts the user content data. There may be further keys that the user key decrypts and the final key decrypts the user content data. The terms "using a key to decrypt user content data" and "enable decryption of the user content data" refer to indirect encryption via multiple keys in a chain. In contrast "the key decrypts the data" refers to direct decryption of the data with the key, such as modulo multiplication of the encrypted data by the key. Here, the user key 221 is used to decrypt the data indirectly and may be the starting point of a chain of keys that are decrypted sequentially until finally, the chain ends at the key that decrypts the user content data. While in most examples disclosed herein, the ephemeral unlock secret 223 decrypts the user key 221, it is also possible that the cryptographic key is derived from the response to the challenge in other ways. For example, the response to the challenge may directly be used as the cryptographic key that decrypts the user content data.

[0069] This allocation of keys and metadata enables a configuration where the entire configuration information about authorized devices, manager devices, and other aspects is stored on the DSD 100 itself. However, the authorized devices require a key stored on the respective authorized device to unlock the DSD 100. If an unregistered user without access to any keys wants to access the entire configuration of the device, such as retrieve a list of registered devices, the unregistered user would need only the recovery key to become registered as a manager

device and gain access to the manager key. The DSD 100 can then provide the entire contents of configuration memory 115 to the new manager device using the manager key. Further, there can be two manager devices and both can register or remove authorized devices. The other manager device would be able to obtain configuration updates by synchronizing its own records with the data stored on configuration memory 115. In some examples, the DSD 100 is configured to erase records 201 of all authorized devices (but not delete the user content data or the user key 221, which may be stored as another copy in encrypted form on configuration memory 115 separate from entry 201 and other entries) if the recovery key is used to gain access but that is a policy decision.

[0070] Fig. 3 illustrates the control flow 300 between an authorized device 111 and an access controller 102, according to an embodiment. First, the authorized device 111 initiates a connect method by sending 301 its transport public key. This step can be easily re-played by an attacker. Access controller 102 then replies 302 with a request for a certificate and in response to this request, authorized device 111 sends 303 a certificate previously obtained from the access controller 102 through the re-enrolment process.

Certificate

[0071] Fig. 4 illustrates a certificate 400 issued by the data storage device 100 and sent by the authorized device 111 to the data storage device to unlock the data storage device, according to an embodiment. In this example, the certificate 400 comprises multiple type-length-value (TLV) fields, where the type value indicates the kind of field that is part of the certificate, length is the size of the value field (typically in bytes), and value is a variable-sized series of bytes which contains data for this part of the certificate.

[0072] Certificate 400 begins with a TLV atom that indicates the type of certificate that follows. This is referred to as the certificate role 401 and has a 2 byte value to indicate that this is an authorized device certificate.

[0073] Certificate 400 belongs to a certificate chain. Access controller 102 uses the chain to validate and authenticate certificate 400. To indicate which chain certificate 400 belongs to, certificate 400 has a 4 byte root certificate identifier (ID) 402. The certificate identifier of each certificate in the certificate chain is the same. Certificate identifiers that do not match indicate an invalid certificate. In one example, a root certificate identifier indicates whether the certificate

chain is a production or a development certification chain. In other examples, other groups may be indicated by respective certificate identifiers.

[0074] Certificate 400 further comprises a 1 byte indicator of certificate depth 403. A certificate's depth is defined as its distance from the root certificate within its certificate chain. The root certificate is defined to have a depth of zero. As a given certificate chain is processed the depth fields are validated to ensure integrity of the chain.

[0075] Certificate 400 also comprises a 64 byte certificate transport public key 404 (e.g., according to the National Institute of Standards and Technology (NIST) P-256 elliptic curve). Each certificate is denoted/indexed via a transport public key. Each type of public key will have its own dedicated tag type. That is, the tag type will denote the cipher suite used to generate the transport public key, such as the P-256 cipher suite.

[0076] Certificate 400 further comprises a data field 405 (explained below) and is authenticated via a signature 406. Access controller 102 receives certificate 400 and validates the signature before trusting or using any of the certificate's contents. To enable signature validation, the 64 byte signer public key 407 is provided as part of the certificate. The signature 406 itself is 64 bytes in length and computed over all prior TLVs 401-405, 407 encountered within the certificate, regardless if they are recognized by the implementation or not. More particularly, the signature 406 is derived from a hash of the certificate data. The specific data that is signed is certificate dependent, but contains all TLVs used to represent the certificate, including TLVs that are not recognized. The key used to generate the signature is a logical identity key and is associated with signer public key 407.

[0077] Data field 405 comprises the slot number 410, which denotes the index of the record 201 within configuration memory 115. Data field 405 also comprises a further copy of the metadata wrapping key 411 (in addition to the two copies shown in Fig. 2). The data field 405 is encrypted with the authorized device slot key (ADSK) 412, which is a 16 byte pseudo random value stored in configuration memory 115 and is used to encrypt data in authorized device certificates so that only the issuing DSD 100 can recover the information.

Unlocking the data storage device

[0078] Returning to Fig. 3, if the authorized device 111 wishes to unlock the DSD 100, the authorized device 111 sends 303 the certificate 400, which includes the encrypted metadata wrapping key (MWK) 213/411 to access controller 102. The certificate 400 also includes the slot number 410, which is an index of the record 201 in configuration memory 115.

[0079] Access controller 102 uses the authorized device slot key stored in configuration memory 115 to decrypt 304 data field 405, and extract the slot number and metadata wrapping key. Access controller 102 then queries configuration memory 115 to read 305 the appropriate record 201 from configuration memory 115 and decrypts 306 the authorized device metadata 205 using the metadata wrapping key. This yields the ephemeral public key 211, which may also be referred to as an identifier of the authorized device because it uniquely identifies the authorized device since the ephemeral public key 211 is cryptographically associated with an unlocking private key stored only on authorized device 111. Access controller 102 may perform additional checks 307, such as validate that the transport public key 209 included in the authorized device metadata 205 matches the transport public key 404 presented in the certificate 400. Further, access controller 102 validates the role 401 against the valid set of values, and associates the role with the connection. This means that access controller 102 is aware of the current role (authorized device or manager device) during the duration of connection. For example, access controller 102 stores a parameter value on volatile memory that indicates the role 401 provided in the certificate. If any of the preceding checks fail, the authorized device is deemed to be revoked and an error to that effect is issued. Otherwise, the connection attempt succeeds and the access controller 102 sends 308 a connected confirmation message to the authorized device 111.

[0080] At this stage, the authorized device 111 is connected and the unlock process begins 319 by the authorized device 111 sending 320 an unlock request to access controller 102. The unlock request includes the unlocking public key associated with the private unlocking key stored on the authorized device's secure hardware module. Access controller 102 matches 321 the received unlocking public key against the unlocking public key 212 stored in the authorized device metadata record 205. Next, access controller 102 generates 322 a new blinding value (also referred to as unlock blinding key (UBK)), which essentially is an ephemeral private scalar and is generated randomly.

[0081] Access controller 102 then generates the challenge based on the identifier of the authorized device (e.g., ephemeral public key 211) multiplied by the unlock blinding key (UBK). More particularly, access controller 102 multiplies 323 the ephemeral public key 211 by the

unlock blinding key, returning the full X and Y coordinates of the result, noting that this operation is performed on an elliptic curve. Access controller 102 then sends 324 the X and Y coordinates to the authorized device 111 as the challenge. It is noted here that this challenge is based on the identifier of the authorized device 111 because the ephemeral public key is one factor of the multiplication resulting in the challenge. It is further noted that for each unlock request (i.e., 320) a different unlock blinding key is generated to avoid man-in-the-middle attacks.

[0082] Further, access controller 102 computes 325 the inverse of the unlock blinding key (UBK^{-1}). The access controller 102 can compute the inverse of the unlock blinding key while waiting for a response from the authorized device 111.

[0083] The authorized device 111 calculates a response to the challenge by multiplying 326 the challenge with the unlocking private key, which is stored in the authorized device's secure hardware module and which corresponds to unlocking public key 212 stored on configuration memory 115. This may involve the execution of a cryptographic primitive that can be executed entirely within the secure hardware module within the authorized device 111. Authorized device 111 then sends back 327 the result in a response message. Access controller 102 multiplies 328 the returned result with the inverse of the unlock blinding key to compute the ephemeral unlock secret (EUS) 223.

[0084] In mathematical notation, P represents the ephemeral public key, and k represents the unlock blinding key created at step 322 in Fig. 3. Access controller 102 calculates 323 the product k*P and sends 324 it to the authorized device 111. The authorized device 111 multiplies 326 the challenge with the unlocking private key j to calculate j*k*P and returns 327 the result to access controller 102. The access controller 102 multiplies 238 this response with the inverse of the unlock blinding key k^{-1} to calculate

$k^{-1}*j*k*P$

which is equal to j*P due to commutative nature of elliptic curves

(i.e., $k^{-1}*j*k*P = k*k^{-1}*j*P = j*P$).

Access controller 102 then uses j*P as the ephemeral unlock secret (i.e., key) to decrypt 329 user key 221. That is, access controller 102 uses the ephemeral unlock secret to decrypt the user key 221, stored on the DSD 100, which is encrypted with the ephemeral unlock secret. More particularly, access controller 102 decrypts 329 the user key, which then decrypts 330 a "user drive key", which is then, finally, sent 331 to cryptography engine 106 via TCG commands. That

is, the user drive key may be generated by access controller 102 using a key derivation function based on the user key. The user drive key is the TCG credential used to unlock the DSD 100 and may be equated to the "cryptographic key" described herein. In the case of Opal, this is the User2 credential.

[0085] It is noted that the ephemeral unlock secret is generated during the re-enrolment process by deriving a symmetric key from the result of an Elliptic Curve Diffie-Hellman process using the unlocking private key stored on the authorized device 111 and the unlocking public key 212. The resulting key is used to encrypt the user key 221 but not stored in DSD 100. Instead, it is re-generated each time an authorized device requests to unlock the DSD 100, as described above.

[0086] In a further example, the unlocking private key j, in the equations above, can be replaced by a product of the unlocking private key with a value derived from a passphrase. The unlocking private key would still be stored in the secure hardware module of the authorized device but the unlocking private key alone would not be able to decrypt the user content data stored on the DSD 100. Instead, the user needs to enter the passphrase to calculate the response to the challenge and send 327 that response. This would simply replace j above with the product of j with the passphrase value. The DSD would be oblivious of that change because the ephemeral unlock secret 223 would be generated in the same way as above from the view of the access controller 102.

Registration and re-enrolment

[0087] It is noted that the data record 201 shown in Fig. 2 is shown after the authorized device 111 has completed the re-enrolment process and is allowed to decrypt the encrypted user content data. Again, there are three steps overall: First, the manager device 110 registers a user device 111 once as one of multiple authorized devices. Second, the authorized device 111, on first connection with the access controller 102, re-enrols once to complete the generation of the involved keys. Third, the authorized device 111 subsequently connects with the access controller 102 to unlock the DSD 100. This third step can occur multiple times.

[0088] During the (initial) registration step initiated by the manager device 110, access controller 102 receives from the manager device 110 a public key corresponding to a private key stored on the user device 111. In response, access controller 102 creates authorization data, which is similar to the data record 201 in Fig. 2 with the exception that the unlocking public key

212 field holds the transport public key 209 (as received from the manager device 110) because the unlocking public key has not yet been generated. Access controller 102 generates the pre-authorization key 202 that is essentially an index to locate the record 201. The pre-authorization key is generated by a key generation function using the x coordinate of the received transport public key 209 and a salt value. The salt value may be an authorized device slot key, which may be a 16-bytes pseudo-random value generated during the "take ownership" process, stored on the configuration memory 115, and not shared with the authorized device. This way the salt can be different after each "factory reset", such as each time a manager device takes ownership of the DSD 100.

[0089] Creating the authorization data stored in record 201 further comprises generating the metadata wrapping key 222, such as by generating a 16-bytes pseudo-random value. Access controller 102 stores the metadata wrapping key in field 222. Further, access controller 102 generates the ephemeral unlock secret 223 and encrypts the role 220 (e.g., "authorized device"), user key 221 and the new metadata wrapping key 222 with the ephemeral unlock secret 223. Then access controller 102 generates an ephemeral public key 211 from the ephemeral unlock secret 223 and discards ephemeral unlock secret 223.

[0090] Recall that during the (initial) registration step initiated by the manager device 110, access controller 102 creates authorization data, which is similar to the data record 201 in Fig. 2. In contrast to Fig. 2, the authorized device metadata 205 is not encrypted by the new metadata wrapping key but by a pre-authorized metadata wrapping key because the actual metadata wrapping key 222 is not yet available to the authorized device 111. The pre-authorized metadata wrapping key may be identical to the pre-authorization key 202 at this stage or generated separately. It is noted that the pre-authorized metadata wrapping key, which now encrypts the authorized device metadata 205 can be generated only by the access controller 102 and not provided by the authorized device 111 because the authorized device 111 does not have access to the authorized device slot key that is used to generate the pre-authorized metadata wrapping key.

[0091] So, responsive to the authorized device 111 first connecting with the access controller 102, authorized device 111 sends its transport public key to access controller 102. Access controller 102 uses the transport public key and the stored authorized device slot key to generate the pre-authorization key 202. Access controller 102 can then search for the pre-authorization key 202 in the configuration memory 115 to retrieve record 201. Access controller 102 can also

use the pre-authorization key as the pre-authorization metadata wrapping key to decrypt the authorized device metadata 205.

[0092] As described above, access controller 102 generates a challenge using the ephemeral public key 211 and an unlock blinding key. Access controller 102 then creates the ephemeral unlock secret 223 from the response. It is noted that only the authorized device 111 with the private key corresponding to transport public key 209 can create a valid response. This means that even if an attacker disassembles the configuration memory 115 and reads the authorized device slot key to generate the pre-authorization metadata wrapping key to decrypt the ephemeral public key 211, the attacker would still not be able to generate the ephemeral unlock secret 223.

[0093] Access controller 102 validates the response by checking that the response works as ephemeral unlock secret 223 and in response, updates the authorization data in record 201. More particularly, access controller 102 checks whether field 212 for the unlocking public key is identical to the transport public key 209. In response to both being identical (as set out above), access controller 102 requests a new unlocking public key from authorized device 111 and stores the returned key as unlocking public key 212.

[0094] Access controller further decrypts the metadata wrapping key 222 that was generated during registration by the manager device 110. At this stage, access controller 102 may re-generate the ephemeral unlock secret 223, encrypt role 220, user key 221, and metadata wrapping key 222, re-generate and store the ephemeral public key 211 and discard the ephemeral unlock secret 223. Finally, access controller encrypts the authorized device metadata 205 with the metadata wrapping key 222 and overwrites the pre-authorization key 202 with random values to make the configuration memory 115 indistinguishable from random data even with the possession of the transport public key and/or the unlocking public key. This concludes the update of the authorization data stored in record 201 and the registration process. As a result, the authorized device 111, as one of multiple authorized devices, is now allowed to decrypt the encrypted user content data through the unlocking steps set out above.

[0095] The process described above, involving the creating and update of authorization data, enables the registration of multiple authorized devices using only their public keys during the first step of registration by the manager device 110. This way, no secret information needs to be

shared that could potentially be intercepted and used for malicious unlocking of other devices of the user.

[0096] Fig. 5 illustrates a method 500 for securing a wireless communication channel between a client device and a server device, according to an embodiment. Method 500 is performed by access controller 102 and comprises access controller 102 repeatedly performing the following steps. Access controller 102 generates 501 a random value, such as by executing a pseudo-random function. Access controller 102 may also access a source of entropy, such as a physical random noise, such as thermal noise. Access controller 102 then calculates 502 based on the random value and the identity key a message authentication code. As set out above, the identity key is readable by manager device 110 in response to being in proximity of the data storage device 100. The identity key is readable out of band of the wireless communication channel. This means that the identity key is obtained over a channel that is different from the wireless communication channel. For example, the manager device 110 may obtain the identity key by reading a QR code or interrogating an NFC chip. Since both steps are only possible when both devices are in close proximity, the availability of the identity key can serve as a proof of possession of the data storage device 100. Further, the identity key enables the manager device 110 to verify the message authentication code based on the random value and the identity key to thereby authenticate the data storage device 100. Once the message authentication code is calculated, access controller 102 broadcasts 503 an advertising packet over the wireless communication channel. The advertising packet comprises the random value and the message authentication code calculated based on the random value and the identity key. The manager device 110 receives the advertising packet and can determine that it originated from data storage device 110 due to the matching message authentication code as described below.

Communication protocol

[0097] Fig. 6 illustrates a protocol 600 for securing a communication channel between the DSD 100, according to an embodiment. DSD 100 is also referred to as the “server device” 100 and the manager device 110 is also referred to as the “client device”. In some examples described herein, the communication channel of protocol 600 is described in relation to Bluetooth Low Energy (BLE). However, protocol 600 may be used over other transport mechanisms such as USB Human Interface Device (HID), User Datagram Protocol (UDP) networking, among others.

[0098] Protocol 600 is based on the out of band communication of the identity key (IDK) from the server device 100 to the client device 110 at step 601. The identity key is stored in the configuration memory 115 of the server device 100 and is accessible to the client device 110 using an out of band channel, such as by scanning a QR code or reading an NFC chip as described above.

[0099] At step 602, the access controller of server device 100 repeatedly broadcasts advertising packets over the wireless communication channel. Each advertising packet comprises a random value and a message authentication code (MAC) calculated based on the random value and the identity key. For example, server device 100 calculates the MAC as a keyed hash of the random value or by encrypting the random value using the identity key. The random value may be selected uniformly at random, or through the output of a pseudo random function that simulates the given property. The advertising packet may further comprise a service identifier that identifies the server device 100 as supporting the protocol 600. The address of the broadcast advertising packets may be selected uniformly at random as the address is not required to resolve the advertising packet of the server device 100.

[0100] Advantageously, the broadcast packet sent by the server device does not contain any identifying information that is predictable to a malicious or eavesdropping third-party. In fact, a third-party without the identity key would not be able to resolve the broadcast packet, negating any attempts in tracking of the server device 100.

[0101] Once the client device 110 receives the advertising packet, at step 603 the client device verifies the received MAC based on the received random value and the identity key obtained at step 601, thereby resolving and authenticating the server device 100. More particularly, the client re-computes the MAC based on the random value and the identity key obtained out of band and compares this with the received message authentication code. In other words, client device 110 performs the same steps on the random value that server device 100 has performed. In response to determining that the received MAC and the re-calculated MAC match, the client device 110 has authenticated the server device 100. It is noted that this initial authentication is possible without the server device 100 or the client device 110 having to provide any private information. Since the MAC is calculated using the identity key, only client devices in proximity can re-calculate the MAC. To all other devices, the advertising packets appear random. In case of multiple servers sending advertising packets and multiple identity keys being available, the client device 110 can try each identity key and attempt re-calculation of the MAC. If it matches, the

client device 110 has established that the matching identity key is for the device with the matching MAC.

[0102] At step 603, the client device 110 resolves the broadcasted advertising packet using the contents of the advertising packet. This packets are referred to as advertising packets because they generally advertise the presence server device 100. This should not be confused with the specific BLE advertising packet according to the BLE standard. While the BLE standard includes resolvable private addresses that may be used here, the address of BLE advertising packets is only 48 bits long (24 bits for a random value and 24 bits for the resolution tag of a resolvable private address). In contrast, the BLE data packets offer enough space for 64 bits for the random value and 64 bits for the message authentication code according to protocol 600. If the random value is selected uniformly at random, the expected number of n-bit values that must be collected in order to observe a collision of random values is roughly 2^(n/2). Therefore, the 24 bits of the resolvable private address in BLE advertising packets encounters a collision roughly every 4000 random values, while the random value when using BLE data packets encounters a collision roughly every 4 billion random values. This advantageously allows the client device 100 of protocol 600 to more confidently confirm that a collision of random values indicates that the given server is identical to one seen before.

[0103] Upon successfully verifying and authenticating the server device 100 at 603, the client device 110 randomly generates and sends a client nonce value to the server device 100 at step 604 to connect to the server device 100. In some embodiments, the client device 110 additionally sends supplementary data to the server such as supported cipher suites and/or protocol version.

[0104] Upon receipt of the client nonce value (and optionally supplementary data), at step 605 the server device 100 randomly generates and sends a server nonce value to the client device 110. In some embodiments, the server device 100 additionally sends supplementary data to the client such as a selected cipher suite and/or protocol version.

[0105] It is advantageous that the client device 110 is able to resolve/identify the server device's broadcast packet and connect using the identity key obtained out of band. The connection process did not itself broadcast information that could be used by an adversary to identify the server device 100 or client device 110.

[0106] Both the client and server devices then derive keys from the identity key, the client nonce value, the server nonce value and optionally the supplementary data using a standard key-derivation function. The supplementary data can be included to bind the resulting key material to the specific exchange process between the server device 100 and client device 110. The resulting key derived by both the client device 110 and server device 100 may be used to encrypt the exchange of data and to establish an encrypted and secure communication channel.

[0107] Steps 601 to 607 do not facilitate any exchange of private information such as keys, device information etc., between the server and client device until the server device 100 is authenticated. However, it may be desirable to additionally conduct a second key exchange process, encrypted by the resulting key, based on the server certificates in order to ensure that a trusted authority has assigned the given identity to the server device 100. This would prevent a compromised identity key to be used by a malicious device (by integrating an NFC chip or QR code) to impersonate a valid server device 100, thereby preventing the malicious device from successfully pair with the client device 100.

[0108] In order to further authenticate the server device 100, the resultant key derived at steps 606 and 607 is used to encrypt a second key exchange based on the server certificates. At step 608, the client requests a server certificate from the server device 100. The server certificate is stored in the data store 105 of the server device 100, and is cryptographically linked to a root certificate of a trusted authority of the client device 110. The root certificate is accessible by the client device, for example, through an application installed on the client device, the application from an authenticated provider cryptographically associated with the root certificate.

[0109] At step 609, the server device 100 obtains the server certificate from the configuration memory 115 and cryptographically signs the identity key with a key verified by the server certificate to generate a signature. In other words, the certificate comprises the public key for verifying the signature and the signature can be cryptographically verified using the public key from the server certificate. In other embodiments, the server device 100 also generates a hash of the identity key and includes the hash into the certificate. This provides a cryptographic binding between the certificate-authenticated connection and the identity key obtained out of band, such as by scanning the QR code. The hash may also include the value of the client and server nonces in a transcript hash to be signed by the key verified by the server certificate to generate a signature.

[0110] The server device 100 then sends the signature and server certificate to the client device at step 610. The signature and server certificate is encrypted using the key derived at step 606 and 607 to prevent other parties from intercepting this private data. The client device 110 cryptographically verifies the server certificate against the root certificate accessible by the client device 110 and cryptographically verifies the signature of the identity key (or the hash thereof) against the server certificate at step 611. In other words, client device 110 calculates the hash of the identity key obtained out of band and compares the calculated hash against the hash provided in the certificate.

[0111] Upon verification of the signature and server certificate, the client device can ensure that the server device 100 is the one and only physical device which has been assigned the given identity key by the trusted authority. At step 612, the client device and server device encrypt the communication channel using the verified signature to securely exchange data.

[0112] At this stage, server device 100 may also issue a certificate to client device 110 as described above, so that client device can authenticate itself to server device 100.

Registering the data storage device

[0113] The data port 103 registers, with the host computer system 104, as a block data storage device. For example, Universal Serial Bus (USB) devices provide information in the form of a USB device descriptor. The USB device descriptor contains relevant information about the device. Accordingly, in embodiments in which the data storage device is connected to a host computer system via a USB connection, the data storage device registers with the host computer system as a block data storage device by configuring its USB device descriptor to indicate that the data storage device is a block data storage device.

[0114] The USB device descriptor provides structured information regarding the USB device such as the class of device, protocols supported, type of device, manufacturer and other configuration parameters. An operating system of a host computer can obtain the USB device descriptor of the data storage device by sending various standard control requests (e.g., GET_DESCRIPTOR requests) to the data storage device. In response to receiving these requests, the data storage device provides the USB_DEVICE_DESCRIPTOR to the host computer system, thus registering the data storage device with the host computer system as a block data storage device .The host computer interprets the USB_DEVICE_DESCRIPTOR to

determine the configuration and capabilities of the data storage device. The host computer system may then store information regarding the data storage device in the registers of the operating system of the host computer system.

[0115] 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.

CLAIMS:

1. A data storage device comprising a data path, a data store and an access controller, wherein:

the data path comprises:

a data port configured to transmit data between a host computer system and the data storage device over a data channel, wherein the data storage device is configured to register with the host computer system as a block data storage device;

a non-volatile storage medium configured to store encrypted user content data; and

a cryptography engine connected between the data port and the storage medium and configured to use a cryptographic key to decrypt the encrypted user content data stored on the storage medium in response to a request from the host computer system;

the data store is configured to store an identity key;

the access controller is configured to:

repeatedly broadcast advertising packets over a wireless communication channel different from the data channel, each advertising packet comprising a random value and a message authentication code calculated based on the random value and the identity key; and

the identity key is readable by a device to be connected and in proximity of the data storage device out of band of the data channel and the communication channel, the identity key configured to enable the device to be connected to verify the message authentication code based on the random value and the identity key to thereby authenticate the data storage device.

2. The data storage device of claim 1, wherein:

the data store is further configured to store a data storage device certificate that is configured to be cryptographically linked to a root certificate that is accessible by the device to be connected; and

the access controller is further configured to:

calculate a signature verified by the data storage device certificate; and

send the data storage device certificate and the signature to the device to be connected to enable the device to be connected to authenticate the data storage device.

3. The data storage device of claim 2, wherein the certificate comprises a hash value of the identity key to bind the certificate to the data storage device from which the identity key is readable out of band.

4. The data storage device of claim 2, wherein:

the root certificate is accessible by the device to be connected through an application installed on the device to be connected from an authenticated provider cryptographically associated with the root certificate.

5. The data storage device of claim 1, wherein the advertising address of the broadcast advertising packets is selected uniformly at random.

6. The data storage device of claim 1, wherein:

each advertising packet further comprises a service identifier of the data storage device; and

the message authentication code is calculated based on the random value, the identity key and the service identifier.

7. The data storage device of claim 1, wherein the access controller is further configured to:

receive through the wireless communication channel from the device to be connected, a first nonce value;

generate a second nonce value;

broadcast through the wireless communication channel, the second nonce value;

derive a cryptographic key from the identity key, the first nonce value and the second nonce value using a key-derivation function; and

secure the wireless communication channel with the device to be connected using the cryptographic key.

8. The data storage device of claim 1, wherein the communication channel is Bluetooth Low Energy.

9. The data storage device of claim 1, wherein the identity key is readable by the device to be connected by means of a quick response (QR) code affixed to the data storage device or by means of a near field communication (NFC) tag integrated in the data storage device.

10. A client device comprising a processor and memory, the memory comprising instructions executable by the processor to:

receive an identity key from a server out of band of a wireless communication channel;

receive an advertisement packet broadcast by the server over the wireless communication channel, the advertisement packet comprising a random value and a message authentication code calculated by the server device based on the random value and the identity key;

verify the message authentication code based on the random value and the identity key to thereby authenticate the server; and

upon authentication of the server, generate a cryptographic key based on the identity key to secure the wireless communication channel with the server device.

11. The client device of claim 10, wherein the memory further comprises instructions executable by the processor to access a root certificate cryptographically linked to a certificate of the server,

12. A method for securing a wireless communication channel between a client device to be connected and a server device, the method comprising repeatedly performing the steps of:

generating a random value;

calculating based on the random value and an identity key a message authentication code, the identity key being readable by the client device and in proximity of the server device out of band of the wireless communication channel, the identity key enabling the client device to verify the message authentication code based on the random value and the identity key to thereby authenticate the server device; and

broadcasting an advertising packet over the wireless communication channel, the advertising packet comprising the random value and the message authentication code calculated based on the random value and the identity key.

13. The method of claim 12, further comprising in response to receiving a connection request from the client device, sending a server certificate issued by the server device to the

client device, the server certificate comprising a hash value of the identity key to bind the certificate to the server device from which the identity key is readable out of band.

14. The method of claim 13, wherein the server certificate is cryptographically linked to a root certificate that is accessible by the client device.

15. The method of claim 13, further comprising:

calculating a hash of the identity key, a nonce received from the client device, and the random value; and

calculating the signature for the hash based on the identity key and verified by the server certificate.

16. The method of claim 13, further comprising:

calculating a signature of the server certificate; and

in response to receiving the connection request from the client device, sending the signature to the client device.

17. The method of claim 16, wherein the signature is verified by the server certificate by using a private key to calculate the signature, the private key being verified by the server certificate.

18. The method of claim 17, wherein the server certificate comprises a public key, corresponding to the private key, for verifying the signature.

19. The method of claim 12, wherein authenticating the server device comprises:

receiving a server certificate from the server device issued by the server device and a signature calculated by the server device based on the identity key and verified by the server certificate;

verifying the server certificate against a root certificate;

verifying the signature against the server certificate; and

upon verification of the signature, securing the wireless communication channel with the server device.

20. A server device for securing a wireless communication channel between a client device to be connected and the server device, the server device comprising a processor configured to repeatedly perform the steps of:

generating a random value;

calculating based on the random value and an identity key a message authentication code, the identity key being readable by the client device and in proximity of the server device out of band of the wireless communication channel, the identity key enabling the client device to verify the message authentication code based on the random value and the identity key to thereby authenticate the server device; and

broadcasting an advertising packet over the wireless communication channel, the advertising packet comprising the random value and the message authentication code calculated based on the random value and the identity key.

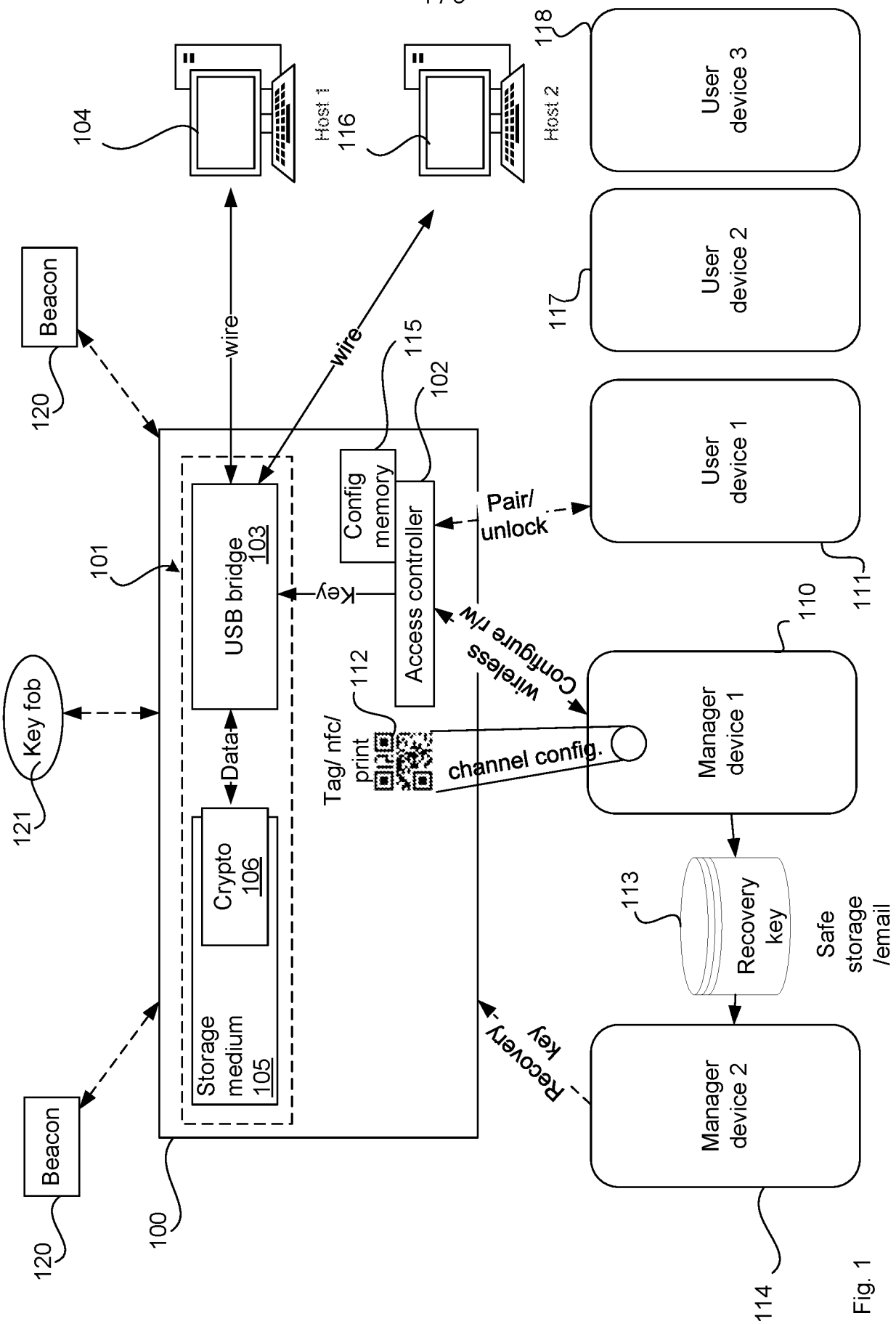
Host 1
116
Host 2
104
118
User device 3
User device 2
117
User device 1
111
Beacon
120
wire
wire
115
102
Config memory
Pair/ unlock
101
USB bridge 103
Key
Access controller
Wireless Configure r/w
110
Manager device 1
Key fob
121
112
Tag/ nfc/ print
channel config.
Data
Crypto 106
Storage medium 105
113
Recovery key
Safe storage /email
Recovery key
Manager device 2
Beacon
120
100
114

Fig. 1

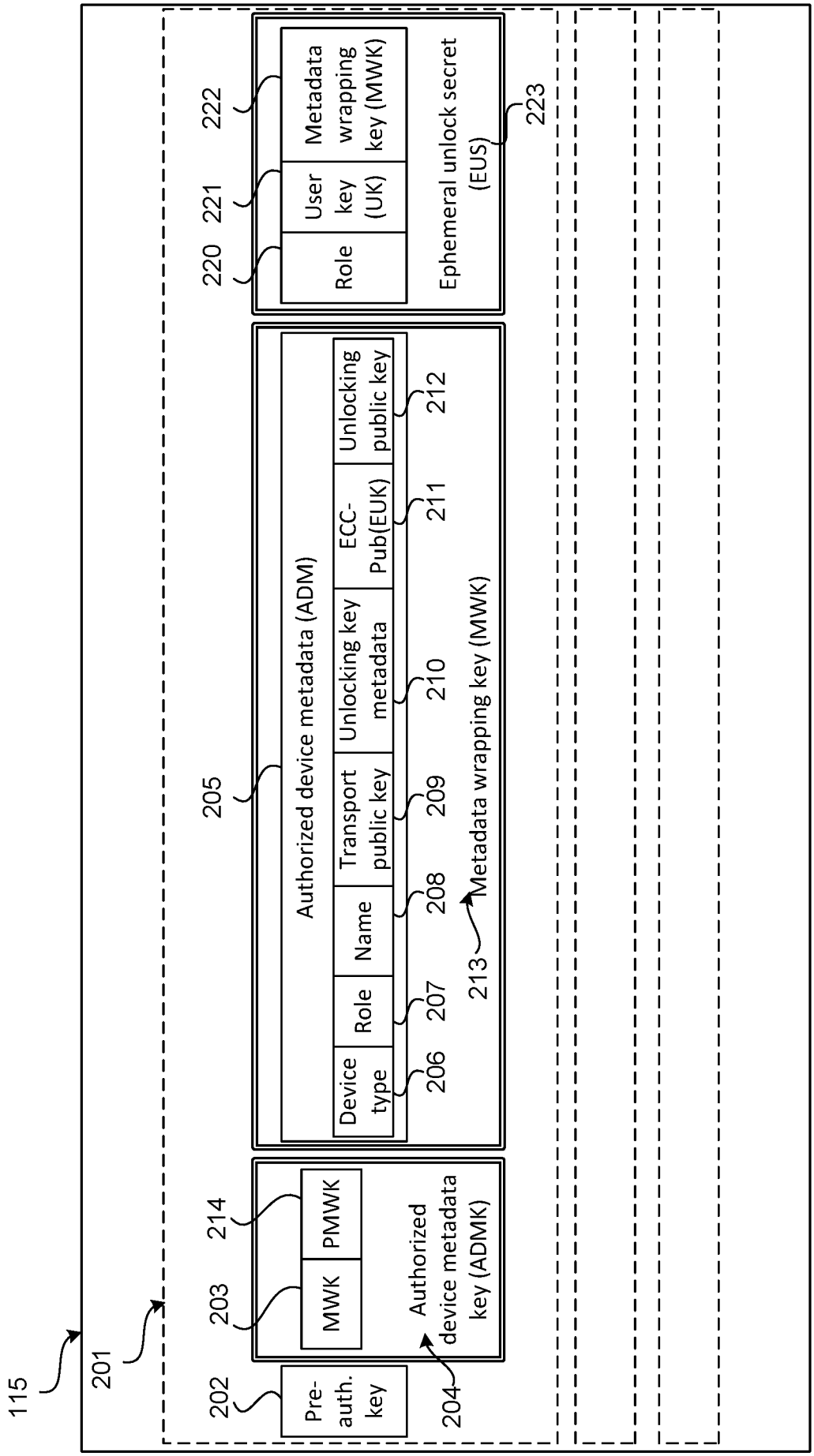
115
201
202
Pre-auth. key
204
214
203
MWK
PMWK
Authorized device metadata key (ADMK)
205
Authorized device metadata (ADM)
Device type
206
Role
207
Name
208
Transport public key
209
Unlocking key metadata
210
ECC-Pub(EUK)
211
Unlocking public key
212
213
Metadata wrapping key (MWK)
220
Role
221
User key (UK)
222
Metadata wrapping key (MWK)
Ephemeral unlock secret (EUS)
223

Fig. 2

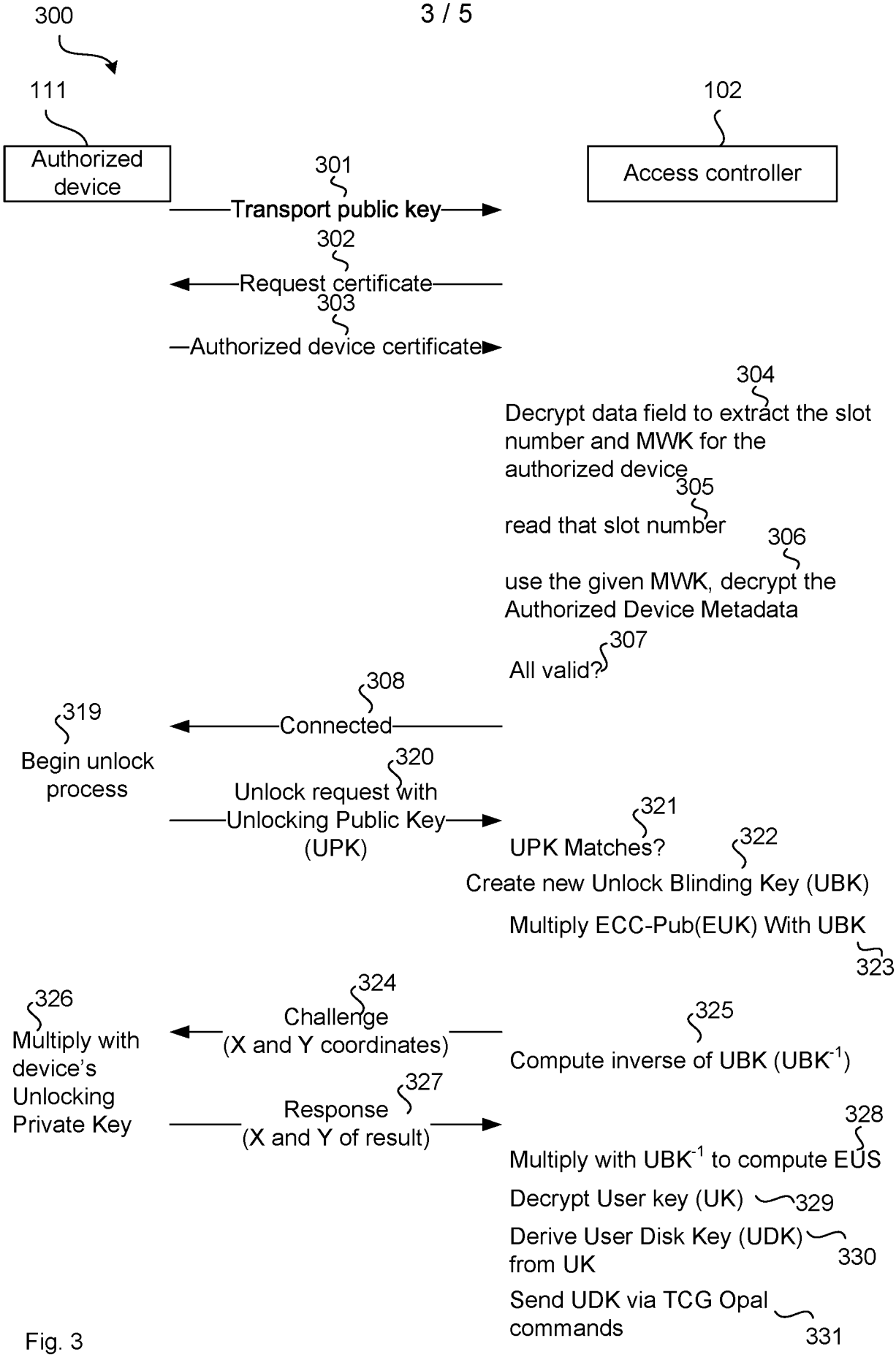
300
111
Authorized device
102
Access controller
301
Transport public key
302
Request certificate
303
Authorized device certificate
304
Decrypt data field to extract the slot number and MWK for the authorized device
305
read that slot number
306
use the given MWK, decrypt the Authorized Device Metadata
307
All valid?
308
Connected
319
Begin unlock process
320
Unlock request with Unlocking Public Key (UPK)
321
UPK Matches?
322
Create new Unlock Blinding Key (UBK)
Multiply ECC-Pub(EUK) With UBK
323
324
Challenge (X and Y coordinates)
325
Compute inverse of UBK (UBK-1)
326
Multiply with device's Unlocking Private Key
327
Response (X and Y of result)
328
Multiply with UBK-1 to compute EUS
Decrypt User key (UK)
329
Derive User Disk Key (UDK) from UK
330
Send UDK via TCG Opal commands
331

Fig. 3

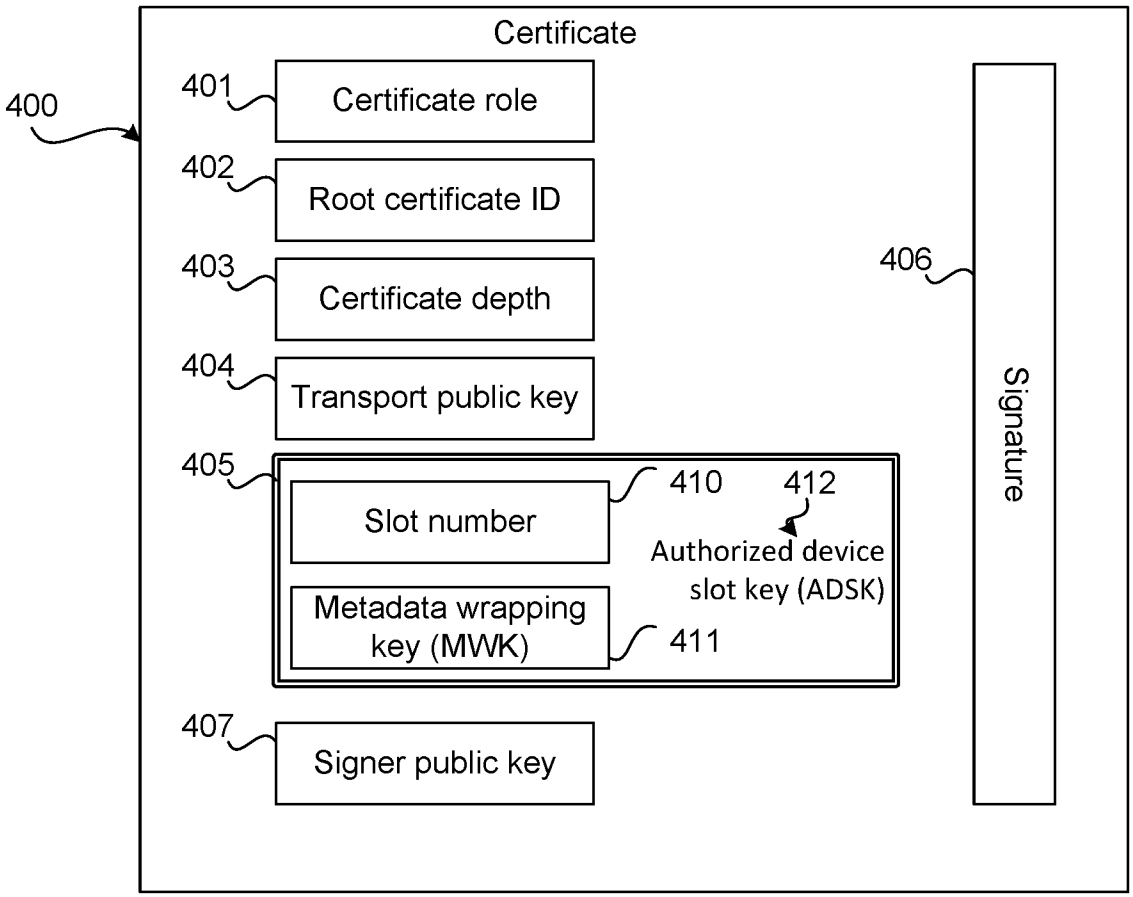
Certificate
400
401
Certificate role
402
Root certificate ID
403
Certificate depth
404
Transport public key
405
410
412
Slot number
Authorized device slot key (ADSK)
Metadata wrapping key (MWK)
411
407
Signer public key
406
Signature

Fig. 4

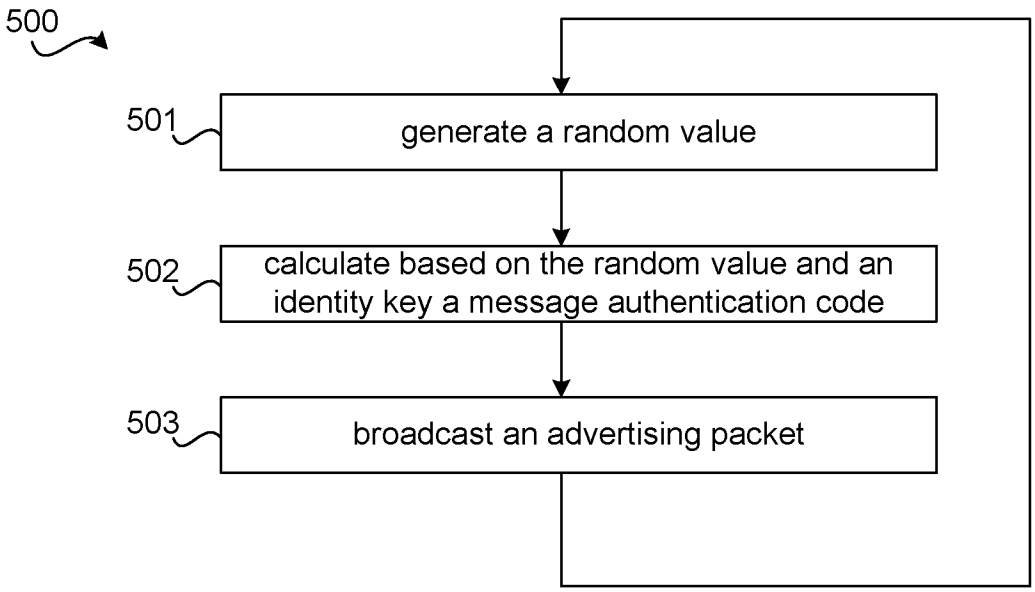
500
501
generate a random value
502
calculate based on the random value and an identity key a message authentication code
503
broadcast an advertising packet

Fig. 5

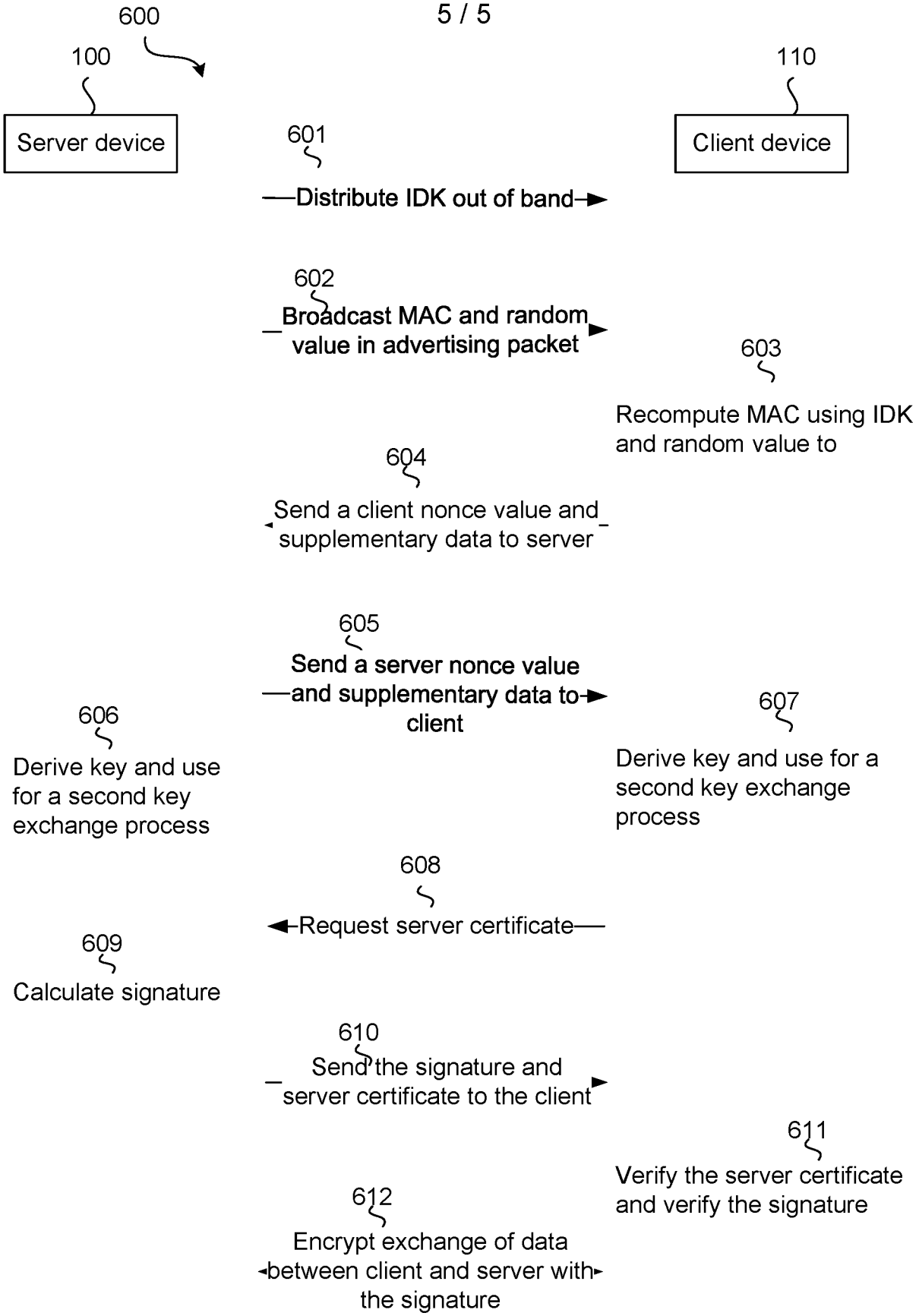
600
100
Server device
110
Client device
601
Distribute IDK out of band
602
Broadcast MAC and random value in advertising packet
603
Recompute MAC using IDK and random value to
604
Send a client nonce value and supplementary data to server
605
Send a server nonce value and supplementary data to client
606
Derive key and use for a second key exchange process
607
Derive key and use for a second key exchange process
608
Request server certificate
609
Calculate signature
610
Send the signature and server certificate to the client
611
Verify the server certificate and verify the signature
612
Encrypt exchange of data between client and server with the signature

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2020/062368

A. CLASSIFICATION OF SUBJECT MATTER
IPC (20210101) H04L 29/06, H04W 12/033, H04W 12/06, H04W 12/50, H04W 4/80, H04L 9/32
CPC (20160801) H04L 63/0428, H04W 12/033, H04W 12/06, H04W 12/50, H04W 4/80, H04L 9/3247
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)
IPC (20210101) H04L 29/06, H04W 12/033, H04W 12/06, H04W 12/50, H04W 4/80, H04L 9/32
CPC (20160801) H04L 63/0428, H04W 12/033, H04W 12/06, H04W 12/50, H04W 4/80, H04L 9/3247

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)
Databases consulted: Google Patents, Google Scholar, Orbit, Similari (AI-based)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2016054251 A1 07 Apr 2016 (2016/04/07) the whole doc.	1-20
Y	US 20140115656 A1 24 Apr 2014 (2014/04/24) the whole doc.	1-20
Y	US 20060205354 A1 14 Sep 2006 (2006/09/14) the whole doc.	1-20
Y	US 20190052468 A1 14 Feb 2019 (2019/02/14) the whole doc.	2,11,14,16,19
A	US 20180176112 A1 21 Jun 2018 (2018/06/21) the whole doc.	1-20

[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
16 Feb 2021	21 Feb 2021
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Email address: pctoffice@justice.gov.il	Authorized officer RUSS Eran Telephone No. 972-73-3927225

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2020/062368

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 3304956 A1 11 Apr 2018 (2018/04/11) the whole doc.	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
WO 2016054251 A1	07 Apr 2016	WO 2016054251 A1	07 Apr 2016
		AU 2015287997 A1	02 Feb 2017
		AU 2015287997 B2	22 Aug 2019
		AU 2019268179 A1	12 Dec 2019
		CA 2954630 A1	14 Jan 2016
		EP 3022720 A1	25 May 2016
		EP 3022720 B1	31 Jan 2018
		EP 3343525 A1	04 Jul 2018
		US 9009805 B1	14 Apr 2015
		US 9082018 B1	14 Jul 2015
		US 9158974 B1	13 Oct 2015
		US 9170707 B1	27 Oct 2015
		US 9213903 B1	15 Dec 2015
		US 9224044 B1	29 Dec 2015
		US 2016041724 A1	11 Feb 2016
		US 9354794 B2	31 May 2016
		US 2016093338 A1	31 Mar 2016
		US 9420331 B2	16 Aug 2016
		US 9449229 B1	20 Sep 2016
		US 2016283795 A1	29 Sep 2016
		US 9479822 B2	25 Oct 2016
		US 2016012609 A1	14 Jan 2016
		US 9489580 B2	08 Nov 2016
		US 9501915 B1	22 Nov 2016
		US 2016092044 A1	31 Mar 2016
		US 9544636 B2	10 Jan 2017
		US 2016094994 A1	31 Mar 2016
		US 9600726 B2	21 Mar 2017
		US 2016316176 A1	27 Oct 2016
		US 9602860 B2	21 Mar 2017

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 2016314355 A1	27 Oct 2016
		US 9609380 B2	28 Mar 2017
		US 2017046574 A1	16 Feb 2017
		US 9672427 B2	06 Jun 2017
		US 2017098126 A1	06 Apr 2017
		US 9674570 B2	06 Jun 2017
		US 2016093336 A1	31 Mar 2016
		US 9779307 B2	03 Oct 2017
		US 2016092738 A1	31 Mar 2016
		US 2018025230 A9	25 Jan 2018
		US 9886161 B2	06 Feb 2018
		US 2016316256 A1	27 Oct 2016
		US 9940523 B2	10 Apr 2018
		US 2018211114 A1	26 Jul 2018
		US 10108862 B2	23 Oct 2018
		US 2016005280 A1	07 Jan 2016
		US 10127783 B2	13 Nov 2018
		US 2016005281 A1	07 Jan 2016
		US 10140827 B2	27 Nov 2018
		US 2018173960 A1	21 Jun 2018
		US 10180775 B2	15 Jan 2019
		US 2016004390 A1	07 Jan 2016
		US 10192120 B2	29 Jan 2019
		US 2017195313 A1	06 Jul 2017
		US 10262210 B2	16 Apr 2019
		US 2019057259 A1	21 Feb 2019
		US 10452921 B2	22 Oct 2019
		US 2018158300 A1	07 Jun 2018
		US 10467872 B2	05 Nov 2019
		US 2019205653 A1	04 Jul 2019
		US 10586112 B2	10 Mar 2020

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 2019035241 A1	31 Jan 2019
		US 10789821 B2	29 Sep 2020
		US 2019121501 A1	25 Apr 2019
		US 10867496 B2	15 Dec 2020
		US 2020319738 A1	08 Oct 2020
		US 10896585 B2	19 Jan 2021
		US 2016092737 A1	31 Mar 2016
		US 2016105617 A1	14 Apr 2016
		US 2017270365 A1	21 Sep 2017
		US 2018012077 A1	11 Jan 2018
		US 2019066473 A1	28 Feb 2019
		US 2019156126 A1	23 May 2019
		US 2020143645 A1	07 May 2020
		WO 2016007541 A1	14 Jan 2016
US 20140115656 A1	24 Apr 2014	US 2014115656 A1	24 Apr 2014
---	---	---	---
		US 9135459 B2	15 Sep 2015
		AU 2013242802 A1	08 May 2014
		AU 2013242802 B2	31 May 2018
		CN 103778075 A	07 May 2014
		CN 103778075 B	18 Jan 2017
		DE 102013111339 A1	24 Apr 2014
		JP 2014086089 A	12 May 2014
		JP 6298268 B2	20 Mar 2018
		KR 20140067180 A	05 Jun 2014
		KR 102017828 B1	03 Sep 2019
		NL 2011611 A	23 Apr 2014
		NL 2011611 B1	23 May 2017
		TW 201428536 A	16 Jul 2014
		TW I595379 B	11 Aug 2017
		US 2015356308 A1	10 Dec 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 9785784 B2	10 Oct 2017
US 20060205354 A1	14 Sep 2006	US 2006205354 A1	14 Sep 2006
		US 7386275 B2	10 Jun 2008
		CN 1832425 A	13 Sep 2006
		CN 1832425 B	11 May 2011
		DE 102006010193 A1	19 Oct 2006
		DE 102006010193 B4	13 Feb 2014
		FR 2887716 A1	29 Dec 2006
		FR 2887716 B1	15 Jul 2016
		GB 0604884 D0	19 Apr 2006
		GB 2424151 A	13 Sep 2006
		GB 2424151 B	29 Aug 2007
		HK 1099977 A1	31 Aug 2007
		IE 20060163 A1	20 Sep 2006
		SG 126048 A1	30 Oct 2006
		TW 200644666 A	16 Dec 2006
		TW I328775 B	11 Aug 2010
		US 2008248751 A1	09 Oct 2008
		US 7715795 B2	11 May 2010
US 20190052468 A1	14 Feb 2019	US 2019052468 A1	14 Feb 2019
		US 10397000 B2	27 Aug 2019
		EP 3669294 A1	24 Jun 2020
		IL 272662 D0	31 Mar 2020
		IL 272662 A	30 Nov 2020
		JP 2020530726 A	22 Oct 2020
		KR 20200037847 A	09 Apr 2020
		TW 201911806 A	16 Mar 2019
		TW I691195 B	11 Apr 2020
		WO 2019036073 A1	21 Feb 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 20180176112 A1	21 Jun 2018	US 2018176112 A1	21 Jun 2018
		AU 2009246654 A1	19 Nov 2009
		AU 2009246654 B2	04 Oct 2012
		AU 2010254812 A1	12 Jan 2012
		AU 2011205426 A1	23 Aug 2012
		AU 2011205426 B2	16 Jan 2014
		AU 2012101191 A4	25 Oct 2012
		AU 2012101191 B4	09 May 2013
		AU 2012232977 A1	18 Apr 2013
		AU 2012261958 A1	16 Jan 2014
		AU 2012261958 B2	21 Apr 2016
		AU 2012316484 A1	17 Apr 2014
		AU 2013260186 A1	04 Dec 2014
		AU 2013262803 A1	27 Nov 2014
		AU 2013262803 B2	21 Jul 2016
		AU 2013344629 A1	04 Jun 2015
		AU 2013344629 B2	02 Mar 2017
		AU 2014100584 A4	03 Jul 2014
		AU 2014100584 B4	05 Mar 2015
		AU 2014100585 A4	03 Jul 2014
		AU 2014100585 B4	12 Mar 2015
		AU 2014235244 A1	24 Sep 2015
		AU 2014235244 B2	13 Apr 2017
		AU 2014235245 A1	24 Sep 2015
		AU 2014235245 B2	02 Mar 2017
		AU 2014235246 A1	24 Sep 2015
		AU 2014235246 B2	17 Aug 2017
		AU 2014235248 A1	24 Sep 2015
		AU 2014235248 B2	11 May 2017
		AU 2014274913 A1	12 Nov 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		AU 2014274913	B2	11 May 2017
		AU 2014275224	A1	24 Dec 2015
		AU 2014275224	B2	31 Aug 2017
		AU 2015100708	A4	09 Jul 2015
		AU 2015100708	B4	03 Mar 2016
		AU 2015100709	A4	09 Jul 2015
		AU 2015100709	B4	10 Mar 2016
		AU 2015101019	A4	10 Sep 2015
		AU 2015101020	A4	10 Sep 2015
		AU 2015101020	B4	21 Apr 2016
		AU 2015101021	A4	10 Sep 2015
		AU 2015101021	B4	19 May 2016
		AU 2015101022	A4	10 Sep 2015
		AU 2015101022	B4	19 Nov 2015
		AU 2015101023	A4	10 Sep 2015
		AU 2015101023	B4	05 Nov 2015
		AU 2015101183	A4	08 Oct 2015
		AU 2015101183	B4	19 Nov 2015
		AU 2015101188	A4	08 Oct 2015
		AU 2015101188	B4	20 Oct 2016
		AU 2015214079	A1	18 Aug 2016
		AU 2015214079	B2	08 Sep 2016
		AU 2015214079	C1	19 Jan 2017
		AU 2015217268	A1	21 Jul 2016
		AU 2015217268	B2	01 Mar 2018
		AU 2015266650	A1	13 Oct 2016
		AU 2015266650	B2	01 Feb 2018
		AU 2015266693	A1	06 Oct 2016
		AU 2015266693	B2	01 Feb 2018
		AU 2015298710	A1	09 Feb 2017
		AU 2015298710	B2	17 Oct 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		AU 2015312215 A1	06 Oct 2016
		AU 2015312215 B2	19 Oct 2017
		AU 2015312369 A1	23 Mar 2017
		AU 2015312369 B2	05 Apr 2018
		AU 2016100090 A4	10 Mar 2016
		AU 2016100090 B4	27 Oct 2016
		AU 2016100367 A4	05 May 2016
		AU 2016100367 B4	24 Nov 2016
		AU 2016100383 A4	05 Dec 2016
		AU 2016100383 B4	22 Dec 2016
		AU 2016100383 C4	17 May 2018
		AU 2016100476 A4	26 May 2016
		AU 2016100476 B4	22 Dec 2016
		AU 2016100765 A4	23 Jun 2016
		AU 2016102002 A4	15 Dec 2016
		AU 2016102002 B4	19 Jan 2017
		AU 2016102031 A4	22 Dec 2016
		AU 2016102031 B4	24 Aug 2017
		AU 2016200568 A1	18 Feb 2016
		AU 2016204091 A1	07 Jul 2016
		AU 2016204091 B2	15 Mar 2018
		AU 2016204683 A1	21 Jul 2016
		AU 2016204683 B2	25 Jan 2018
		AU 2016204980 A1	16 Mar 2017
		AU 2016211504 A1	21 Sep 2017
		AU 2016211504 B2	26 Oct 2017
		AU 2016215440 A1	17 Aug 2017
		AU 2016215440 B2	14 Mar 2019
		AU 2016229847 A1	21 Sep 2017
		AU 2016229847 B2	27 Sep 2018
		AU 2017100070 A4	02 Mar 2017

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		AU 2017100070	B4	28 Sep 2017
		AU 2017100197	A4	23 Mar 2017
		AU 2017100197	B4	26 Oct 2017
		AU 2017100198	A4	23 Mar 2017
		AU 2017100198	B4	26 Oct 2017
		AU 2017201064	A1	09 Mar 2017
		AU 2017201064	B2	01 Mar 2018
		AU 2017201068	A1	09 Mar 2017
		AU 2017204217	A1	13 Jul 2017
		AU 2017204217	B2	18 Oct 2018
		AU 2017261594	A1	07 Dec 2017
		AU 2017261594	B2	15 Aug 2019
		AU 2017268569	A1	21 Dec 2017
		AU 2017268569	B2	13 Jun 2019
		AU 2018200428	A1	08 Feb 2018
		AU 2018200628	A1	15 Feb 2018
		AU 2018200628	B2	27 Jun 2019
		AU 2018201089	A1	08 Mar 2018
		AU 2018202559	A1	10 May 2018
		AU 2018202559	B2	31 Oct 2019
		AU 2018203722	A1	21 Jun 2018
		AU 2018203722	B2	19 Dec 2019
		AU 2018204265	A1	05 Jul 2018
		AU 2018204265	B2	12 Mar 2020
		AU 2018204265	C1	25 Jun 2020
		AU 2018204430	A1	05 Jul 2018
		AU 2018204430	B2	11 Jul 2019
		AU 2018204430	C1	30 Jan 2020
		AU 2018279037	A1	17 Jan 2019
		AU 2018279037	B2	28 May 2020
		AU 2019200296	A1	07 Feb 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		AU 2019200296 B2	19 Sep 2019
		AU 2019201583 A1	28 Mar 2019
		AU 2019201583 B2	18 Jul 2019
		AU 2019201583 B9	25 Jul 2019
		AU 2019213441 A1	29 Aug 2019
		AU 2019213441 B2	28 Jan 2021
		AU 2019246830 B1	07 Nov 2019
		AU 2019250251 A1	07 Nov 2019
		AU 2019283923 A1	16 Jan 2020
		AU 2020200685 A1	20 Feb 2020
		AU 2020200685 B2	12 Nov 2020
		AU 2020202534 A1	07 May 2020
		AU 2020202534 B2	04 Jun 2020
		AU 2020204506 A1	23 Jul 2020
		AU 2020220088 A1	03 Sep 2020
		AU 2020250323 A1	12 Nov 2020
		AU 2020289822 A1	21 Jan 2021
		BR PI0912741 A2	13 Oct 2015
		BR 102012024861 A2	14 Feb 2017
		BR 112012017826 A2	26 Sep 2017
		BR 112012017826 A8	01 Sep 2020
		BR 112012017826 B1	05 Jan 2021
		BR 122012028965 A2	27 Mar 2018
		BR 122012028966 A2	30 Jul 2019
		BR 122012028968 A2	30 Jul 2019
		BR 122012028969 A2	30 Jul 2019
		BR 122012028969 B1	05 Jan 2021
		BR 122012028970 A2	30 Jul 2019
		BR 122012028971 A2	30 Jul 2019
		BR 122012028972 A2	01 Sep 2020
		BR 122012028973 A2	30 Jul 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)			Publication Date
		BR	122012028974	A2	30 Jul 2019
		CA	2787351	A1	21 Jul 2011
		CA	2787351	C	08 Dec 2015
		CA	2791277	A1	30 Mar 2013
		CA	2791277	C	15 Jan 2019
		CA	2791791	A1	21 Jul 2011
		CA	2791791	C	18 Oct 2016
		CA	2792412	A1	21 Jul 2011
		CA	2792412	C	22 Dec 2015
		CA	2792442	A1	21 Jul 2011
		CA	2792442	C	17 May 2016
		CA	2792570	A1	21 Jul 2011
		CA	2792570	C	31 May 2016
		CA	2793002	A1	21 Jul 2011
		CA	2793002	C	21 Jun 2016
		CA	2793118	A1	21 Jul 2011
		CA	2793118	C	08 Aug 2017
		CA	2793248	A1	21 Jul 2011
		CA	2793248	C	01 Nov 2016
		CA	2793741	A1	21 Jul 2011
		CA	2793741	C	31 May 2016
		CA	2793743	A1	21 Jul 2011
		CA	2793743	C	06 Oct 2015
		CA	2954559	A1	21 Jul 2011
		CA	2954559	C	04 Dec 2018
		CA	3000109	A1	21 Jul 2011
		CA	3000109	C	23 Jun 2020
		CA	3023918	A1	30 Mar 2013
		CA	3077914	A1	21 Jul 2011
		CN	101582053	A	18 Nov 2009
		CN	101582053	B	22 Jan 2014

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)			Publication Date
		CN	102792320	A	21 Nov 2012
		CN	102792320	B	24 Feb 2016
		CN	103226949	A	31 Jul 2013
		CN	103226949	B	01 Feb 2017
		CN	103582896	A	12 Feb 2014
		CN	103778082	A	07 May 2014
		CN	103778082	B	05 Apr 2017
		CN	103959751	A	30 Jul 2014
		CN	104335205	A	04 Feb 2015
		CN	104335205	B	19 Oct 2018
		CN	104395860	A	04 Mar 2015
		CN	104395860	B	22 Jun 2018
		CN	104412201	A	11 Mar 2015
		CN	104412201	B	21 Sep 2018
		CN	104685470	A	03 Jun 2015
		CN	104685470	B	30 Nov 2018
		CN	104834419	A	12 Aug 2015
		CN	104834419	B	15 Jan 2019
		CN	104937553	A	23 Sep 2015
		CN	104937553	B	19 Nov 2019
		CN	105051494	A	11 Nov 2015
		CN	105051494	B	26 Jan 2018
		CN	105051495	A	11 Nov 2015
		CN	105051495	B	23 Jul 2019
		CN	105051496	A	11 Nov 2015
		CN	105051496	B	17 Jan 2020
		CN	105143828	A	09 Dec 2015
		CN	105143828	B	13 Sep 2019
		CN	105191387	A	23 Dec 2015
		CN	105191387	B	26 Mar 2019
		CN	105247511	A	13 Jan 2016

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)			Publication Date
		CN	105283840	A	27 Jan 2016
		CN	105283840	B	05 Jul 2019
		CN	105284099	A	27 Jan 2016
		CN	105284099	B	17 May 2019
		CN	105303372	A	03 Feb 2016
		CN	105320454	A	10 Feb 2016
		CN	105320454	B	31 Dec 2019
		CN	105320455	A	10 Feb 2016
		CN	105320455	B	22 Mar 2019
		CN	105321067	A	10 Feb 2016
		CN	105335087	A	17 Feb 2016
		CN	105335087	B	23 Jul 2019
		CN	105379234	A	02 Mar 2016
		CN	105379234	B	19 Apr 2019
		CN	105388998	A	09 Mar 2016
		CN	105388998	B	27 Aug 2019
		CN	105389078	A	09 Mar 2016
		CN	105389078	B	05 May 2020
		CN	105487790	A	13 Apr 2016
		CN	105718185	A	29 Jun 2016
		CN	105718185	B	02 Aug 2019
		CN	105808200	A	27 Jul 2016
		CN	105808200	B	10 Sep 2019
		CN	105844462	A	10 Aug 2016
		CN	105844462	B	17 Dec 2019
		CN	105981352	A	28 Sep 2016
		CN	105981352	B	13 Mar 2018
		CN	106068490	A	02 Nov 2016
		CN	106068490	B	22 Feb 2019
		CN	106462123	A	22 Feb 2017
		CN	106462123	B	22 Dec 2020

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)			Publication Date
		CN	106537397	A	22 Mar 2017
		CN	106537397	B	13 Dec 2019
		CN	106664226	A	10 May 2017
		CN	106664226	B	22 May 2020
		CN	106797333	A	31 May 2017
		CN	106797333	B	16 Oct 2020
		CN	106797493	A	31 May 2017
		CN	106961334	A	18 Jul 2017
		CN	106961334	B	19 May 2020
		CN	107209655	A	26 Sep 2017
		CN	107209655	B	11 Aug 2020
		CN	107430489	A	01 Dec 2017
		CN	107633397	A	26 Jan 2018
		CN	107633397	B	08 Nov 2019
		CN	107667337	A	06 Feb 2018
		CN	107683439	A	09 Feb 2018
		CN	107683439	B	30 Jun 2020
		CN	107683601	A	09 Feb 2018
		CN	107683601	B	21 May 2019
		CN	107851046	A	27 Mar 2018
		CN	107921317	A	17 Apr 2018
		CN	108090760	A	29 May 2018
		CN	108133367	A	08 Jun 2018
		CN	108133742	A	08 Jun 2018
		CN	108133742	B	14 Apr 2020
		CN	108259159	A	06 Jul 2018
		CN	108259159	B	05 Feb 2021
		CN	108337380	A	27 Jul 2018
		CN	108845664	A	20 Nov 2018
		CN	109062463	A	21 Dec 2018
		CN	109324732	A	12 Feb 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)			Publication Date
		CN	109599161	A	09 Apr 2019
		CN	109631935	A	16 Apr 2019
		CN	110068352	A	30 Jul 2019
		CN	110072131	A	30 Jul 2019
		CN	110083411	A	02 Aug 2019
		CN	110110952	A	09 Aug 2019
		CN	110110953	A	09 Aug 2019
		CN	110113427	A	09 Aug 2019
		CN	110232489	A	13 Sep 2019
		CN	110248019	A	17 Sep 2019
		CN	110264145	A	20 Sep 2019
		CN	110298653	A	01 Oct 2019
		CN	110298653	B	11 Dec 2020
		CN	110388935	A	29 Oct 2019
		CN	110413357	A	05 Nov 2019
		CN	110599157	A	20 Dec 2019
		CN	110807631	A	18 Feb 2020
		CN	110889690	A	17 Mar 2020
		CN	110932888	A	27 Mar 2020
		CN	111035394	A	21 Apr 2020
		CN	111081345	A	28 Apr 2020
		CN	111128339	A	08 May 2020
		CN	111180039	A	19 May 2020
		CN	111180040	A	19 May 2020
		CN	111210891	A	29 May 2020
		CN	111289010	A	16 Jun 2020
		CN	111337048	A	26 Jun 2020
		CN	111538446	A	14 Aug 2020
		CN	111601306	A	28 Aug 2020
		CN	111857527	A	30 Oct 2020
		CN	204650490	U	16 Sep 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		CN 204650596	U	16 Sep 2015
		CN 205158436	U	13 Apr 2016
		CN 205334368	U	22 Jun 2016
		CN 205486013	U	17 Aug 2016
		CN 205608658	U	28 Sep 2016
		CN 206193905	U	24 May 2017
		CN 206193906	U	24 May 2017
		CN 206649467	U	17 Nov 2017
		DE 102012019178	A1	04 Apr 2013
		DE 112013002410	T5	22 Jan 2015
		DE 112013002421	T5	05 Feb 2015
		DE 112015002326	T5	23 Mar 2017
		DE 112015003083	T5	11 May 2017
		DE 202014004555	U1	18 Sep 2014
		DE 202014004560	U1	12 Sep 2014
		DE 202015004267	U1	11 Dec 2015
		DE 202015004268	U1	13 Nov 2015
		DE 202015005394	U1	08 Dec 2015
		DE 202015005395	U1	17 Nov 2015
		DE 202015005397	U1	08 Dec 2015
		DE 202015005399	U1	12 Nov 2015
		DE 202015005400	U1	08 Dec 2015
		DE 202015006055	U1	02 Feb 2016
		DE 202015006066	U1	14 Dec 2015
		DE 202015009088	U1	06 Sep 2016
		DE 202015009089	U1	09 Sep 2016
		DE 202016001214	U1	23 Jun 2016
		DK 201570496	A1	18 Jul 2016
		DK 178589	B1	01 Aug 2016
		DK 201570563	A1	14 Mar 2016
		DK 178595	B1	08 Aug 2016

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		DK 201570666	A1	25 Jul 2016
		DK 178771	B1	09 Jan 2017
		DK 178771	B9	31 Aug 2020
		DK 201570666	A9	31 Aug 2020
		DK 201570495	A1	29 Feb 2016
		DK 178931	B1	12 Jun 2017
		DK 201570550	A1	14 Mar 2016
		DK 178964	B1	10 Jul 2017
		DK 201570668	A1	25 Jul 2016
		DK 179222	B1	12 Feb 2018
		DK 201670042	A1	22 Aug 2016
		DK 179348	B1	14 May 2018
		DK 201770126	A1	20 Mar 2017
		DK 179417	B1	18 Jun 2018
		DK 201670320	A1	06 Jun 2016
		DK 179583	B1	20 Feb 2019
		DK 201570497	A1	29 Feb 2016
		DK 201570498	A1	22 Feb 2016
		DK 201570499	A1	29 Feb 2016
		DK 201570775	A1	09 Jan 2017
		DK 201670319	A1	30 May 2016
		DK 201670656	A1	19 Sep 2016
		DK 201770125	A1	13 Mar 2017
		DK 201770191	A1	27 Mar 2017
		DK 201770292	A1	08 May 2017
		EP 2283424	A2	16 Feb 2011
		EP 2526511	A2	28 Nov 2012
		EP 2526511	A4	21 Dec 2016
		EP 2575128	A2	03 Apr 2013
		EP 2575128	A3	14 Aug 2013
		EP 2715625	A2	09 Apr 2014

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		EP 2715625 A4	29 Oct 2014
		EP 2761860 A1	06 Aug 2014
		EP 2761860 B1	23 Oct 2019
		EP 2778614 A1	17 Sep 2014
		EP 2778614 B1	20 Jul 2016
		EP 2778615 A2	17 Sep 2014
		EP 2778615 A3	29 Jul 2015
		EP 2778615 B1	12 Sep 2018
		EP 2847693 A2	18 Mar 2015
		EP 2847693 A4	13 Jan 2016
		EP 2920693 A1	23 Sep 2015
		EP 2946171 A2	25 Nov 2015
		EP 2946172 A1	25 Nov 2015
		EP 2972104 A1	20 Jan 2016
		EP 2992418 A1	09 Mar 2016
		EP 3005075 A1	13 Apr 2016
		EP 3005150 A2	13 Apr 2016
		EP 3005150 A4	15 Jun 2016
		EP 3005668 A1	13 Apr 2016
		EP 3005668 B1	19 Dec 2018
		EP 3072040 A1	28 Sep 2016
		EP 3101392 A1	07 Dec 2016
		EP 3103246 A1	14 Dec 2016
		EP 3103246 B1	06 Dec 2017
		EP 3108426 A1	28 Dec 2016
		EP 3108427 A1	28 Dec 2016
		EP 3129907 A2	15 Feb 2017
		EP 3131023 A1	15 Feb 2017
		EP 3149547 A1	05 Apr 2017
		EP 3149547 B1	26 Jun 2019
		EP 3149548 A2	05 Apr 2017

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		EP 3154014 A1	12 Apr 2017
		EP 3156958 A1	19 Apr 2017
		EP 3158425 A1	26 Apr 2017
		EP 3175344 A1	07 Jun 2017
		EP 3176742 A1	07 Jun 2017
		EP 3189409 A1	12 Jul 2017
		EP 3189409 B1	29 Jan 2020
		EP 3189416 A2	12 Jul 2017
		EP 3189416 B1	15 Jul 2020
		EP 3190747 A1	12 Jul 2017
		EP 3190747 B1	14 Nov 2018
		EP 3195096 A1	26 Jul 2017
		EP 3195096 B1	12 Aug 2020
		EP 3200185 A1	02 Aug 2017
		EP 3201773 A1	09 Aug 2017
		EP 3251068 A1	06 Dec 2017
		EP 3254452 A1	13 Dec 2017
		EP 3254452 B1	26 Dec 2018
		EP 3268844 A1	17 Jan 2018
		EP 3268844 A4	12 Dec 2018
		EP 3281388 A1	14 Feb 2018
		EP 3281388 B1	07 Aug 2019
		EP 3286642 A1	28 Feb 2018
		EP 3286702 A1	28 Feb 2018
		EP 3313050 A1	25 Apr 2018
		EP 3313050 B1	23 Jan 2019
		EP 3329376 A1	06 Jun 2018
		EP 3333740 A1	13 Jun 2018
		EP 3337583 A1	27 Jun 2018
		EP 3337583 A4	10 Apr 2019
		EP 3373122 A1	12 Sep 2018

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		EP 3392876	A1	24 Oct 2018
		EP 3445002	A1	20 Feb 2019
		EP 3445002	B1	24 Jul 2019
		EP 3454227	A1	13 Mar 2019
		EP 3483807	A1	15 May 2019
		EP 3484134	A1	15 May 2019
		EP 3493509	A1	05 Jun 2019
		EP 3493509	B1	21 Oct 2020
		EP 3537238	A1	11 Sep 2019
		EP 3543939	A1	25 Sep 2019
		EP 3591943	A1	08 Jan 2020
		EP 3594828	A1	15 Jan 2020
		EP 3719644	A1	07 Oct 2020
		EP 3742272	A1	25 Nov 2020
		GB 0907592	D0	10 Jun 2009
		GB 2459956	A	18 Nov 2009
		GB 2459956	B	25 Aug 2010
		GB 201009318	D0	21 Jul 2010
		GB 2472482	A	09 Feb 2011
		GB 2472482	B	21 Sep 2011
		GB 201213633	D0	12 Sep 2012
		GB 2490444	A	31 Oct 2012
		GB 201217449	D0	14 Nov 2012
		GB 2495222	A	03 Apr 2013
		GB 2495222	B	26 Oct 2016
		HK 1137831	A1	06 Aug 2010
		HK 1200621	A1	07 Aug 2015
		HK 1205312	A1	11 Dec 2015
		HK 1206835	A1	15 Jan 2016
		HK 1212486	A1	10 Jun 2016
		HK 1219144	A1	24 Mar 2017

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		HK 1220023	A1	21 Apr 2017
		HK 1220525	A1	05 May 2017
		HK 1220535	A1	05 May 2017
		HK 1220536	A1	05 May 2017
		HK 1221037	A1	19 May 2017
		HK 1221038	A1	19 May 2017
		HK 1221039	A1	19 May 2017
		HK 1222726	A1	07 Jul 2017
		HK 1222922	A1	14 Jul 2017
		HK 1222923	A1	14 Jul 2017
		HK 1223694	A1	04 Aug 2017
		HK 1224110	A1	11 Aug 2017
		HK 1255480	A1	16 Aug 2019
		HK 1255490	A1	16 Aug 2019
		JP 2010033548	A	12 Feb 2010
		JP 5137899	B2	06 Feb 2013
		JP 2013080476	A	02 May 2013
		JP 5698203	B2	08 Apr 2015
		JP 2013047954	A	07 Mar 2013
		JP 5781043	B2	16 Sep 2015
		JP 2014222516	A	27 Nov 2014
		JP 5948372	B2	06 Jul 2016
		JP 2014222514	A	27 Nov 2014
		JP 5956511	B2	27 Jul 2016
		JP 2014222513	A	27 Nov 2014
		JP 5957038	B2	27 Jul 2016
		JP 2014222512	A	27 Nov 2014
		JP 5973500	B2	23 Aug 2016
		JP 2014222509	A	27 Nov 2014
		JP 6027052	B2	16 Nov 2016
		JP 2014518409	A	28 Jul 2014

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		JP 6144256	B2	07 Jun 2017
		JP 2017511028	A	13 Apr 2017
		JP 6166484	B2	19 Jul 2017
		JP 2014222510	A	27 Nov 2014
		JP 6175413	B2	02 Aug 2017
		JP 2017091551	A	25 May 2017
		JP 6178911	B2	09 Aug 2017
		JP 2014222515	A	27 Nov 2014
		JP 6193181	B2	06 Sep 2017
		JP 2015519838	A	09 Jul 2015
		JP 6193361	B2	06 Sep 2017
		JP 2017505959	A	23 Feb 2017
		JP 6276867	B2	07 Feb 2018
		JP 2015122104	A	02 Jul 2015
		JP 6285883	B2	28 Feb 2018
		JP 2017531225	A	19 Oct 2017
		JP 6322765	B2	09 May 2018
		JP 2017526073	A	07 Sep 2017
		JP 6349030	B2	27 Jun 2018
		JP 2014222517	A	27 Nov 2014
		JP 6353711	B2	04 Jul 2018
		JP 2015501022	A	08 Jan 2015
		JP 6353786	B2	04 Jul 2018
		JP 2014222511	A	27 Nov 2014
		JP 6356501	B2	11 Jul 2018
		JP 2018152085	A	27 Sep 2018
		JP 6464299	B2	06 Feb 2019
		JP 2017517788	A	29 Jun 2017
		JP 6482574	B2	13 Mar 2019
		JP 2017520045	A	20 Jul 2017
		JP 6498703	B2	10 Apr 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		JP 2017224300 A	21 Dec 2017
		JP 6498725 B2	10 Apr 2019
		JP 2017097874 A	01 Jun 2017
		JP 6509798 B2	08 May 2019
		JP 2018170020 A	01 Nov 2018
		JP 6518362 B2	22 May 2019
		JP 2017532069 A	02 Nov 2017
		JP 6526700 B2	05 Jun 2019
		JP 2018514828 A	07 Jun 2018
		JP 6532950 B2	19 Jun 2019
		JP 2018136975 A	30 Aug 2018
		JP 6532979 B2	19 Jun 2019
		JP 2016529580 A	23 Sep 2016
		JP 6545155 B2	17 Jul 2019
		JP 2017527026 A	14 Sep 2017
		JP 6545255 B2	17 Jul 2019
		JP 2018514838 A	07 Jun 2018
		JP 6577044 B2	18 Sep 2019
		JP 2019164826 A	26 Sep 2019
		JP 6632756 B2	22 Jan 2020
		JP 2017117441 A	29 Jun 2017
		JP 6666828 B2	18 Mar 2020
		JP 2017531230 A	19 Oct 2017
		JP 6692344 B2	13 May 2020
		JP 2019164825 A	26 Sep 2019
		JP 6739591 B2	12 Aug 2020
		JP 2017139004 A	10 Aug 2017
		JP 6740162 B2	12 Aug 2020
		JP 2017142833 A	17 Aug 2017
		JP 6754716 B2	16 Sep 2020
		JP 2020129399 A	27 Aug 2020

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		JP 6773933 B2	21 Oct 2020
		JP 2018116728 A	26 Jul 2018
		JP 6828962 B2	10 Feb 2021
		JP 2013517566 A	16 May 2013
		JP 2016001477 A	07 Jan 2016
		JP 2017016683 A	19 Jan 2017
		JP 2017527033 A	14 Sep 2017
		JP 2018124998 A	09 Aug 2018
		JP 2019083036 A	30 May 2019
		JP 2019145121 A	29 Aug 2019
		JP 2020017285 A	30 Jan 2020
		JP 2020091895 A	11 Jun 2020
		JP 2020173835 A	22 Oct 2020
		JP 2020184364 A	12 Nov 2020
		JP 2020194555 A	03 Dec 2020
		JP 2020194557 A	03 Dec 2020
		JP 2021013173 A	04 Feb 2021
		KR 20110014194 A	10 Feb 2011
		KR 101275466 B1	14 Jun 2013
		KR 20120136417 A	18 Dec 2012
		KR 101511831 B1	14 Apr 2015
		KR 20120137424 A	20 Dec 2012
		KR 101511832 B1	15 Apr 2015
		KR 20120138826 A	26 Dec 2012
		KR 101511833 B1	14 Apr 2015
		KR 20130005310 A	15 Jan 2013
		KR 101536044 B1	13 Jul 2015
		KR 20140084325 A	04 Jul 2014
		KR 101543195 B1	07 Aug 2015
		KR 20120137425 A	20 Dec 2012
		KR 101555742 B1	25 Sep 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		KR 20120138827 A	26 Dec 2012
		KR 101555743 B1	25 Sep 2015
		KR 20130000423 A	02 Jan 2013
		KR 101577493 B1	14 Dec 2015
		KR 20120137434 A	20 Dec 2012
		KR 101588080 B1	25 Jan 2016
		KR 20120137440 A	20 Dec 2012
		KR 101588081 B1	25 Jan 2016
		KR 20120120316 A	01 Nov 2012
		KR 101593739 B1	12 Feb 2016
		KR 20140082771 A	02 Jul 2014
		KR 101617665 B1	03 May 2016
		KR 20120137435 A	20 Dec 2012
		KR 101654580 B1	06 Sep 2016
		KR 20130035983 A	09 Apr 2013
		KR 101683083 B1	07 Dec 2016
		KR 20150003877 A	09 Jan 2015
		KR 101697416 B1	17 Jan 2017
		KR 20160098522 A	18 Aug 2016
		KR 101706138 B1	13 Feb 2017
		KR 20140014300 A	05 Feb 2014
		KR 101752035 B1	28 Jun 2017
		KR 20160105995 A	08 Sep 2016
		KR 101775708 B1	06 Sep 2017
		KR 20170003608 A	09 Jan 2017
		KR 101776098 B1	07 Sep 2017
		KR 20150081322 A	13 Jul 2015
		KR 101786537 B1	18 Oct 2017
		KR 20160003103 A	08 Jan 2016
		KR 101816375 B1	08 Jan 2018
		KR 20160003138 A	08 Jan 2016

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)		Publication Date
		KR 101834624	B1	05 Mar 2018
		KR 20170021824	A	28 Feb 2017
		KR 101845191	B1	03 Apr 2018
		KR 20170117609	A	23 Oct 2017
		KR 101847508	B1	10 Apr 2018
		KR 20160115977	A	06 Oct 2016
		KR 101855027	B1	04 May 2018
		KR 20170023046	A	02 Mar 2017
		KR 101856412	B1	09 May 2018
		KR 20170032471	A	22 Mar 2017
		KR 101875907	B1	06 Jul 2018
		KR 20170113615	A	12 Oct 2017
		KR 101879558	B1	17 Jul 2018
		KR 20170029014	A	14 Mar 2017
		KR 101901796	B1	28 Sep 2018
		KR 20170076803	A	04 Jul 2017
		KR 101915185	B1	06 Nov 2018
		KR 20160014047	A	05 Feb 2016
		KR 101947229	B1	12 Feb 2019
		KR 20180039179	A	17 Apr 2018
		KR 101948492	B1	14 Feb 2019
		KR 20170104006	A	13 Sep 2017
		KR 101962243	B1	27 Mar 2019
		KR 20170141274	A	22 Dec 2017
		KR 101995660	B1	02 Jul 2019
		KR 20180107296	A	01 Oct 2018
		KR 102016160	B1	29 Aug 2019
		KR 20160142802	A	13 Dec 2016
		KR 102048375	B1	25 Nov 2019
		KR 20190032641	A	27 Mar 2019
		KR 102096222	B1	01 Apr 2020

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		KR 20190124345 A	04 Nov 2019
		KR 102101138 B1	14 Apr 2020
		KR 20170017011 A	14 Feb 2017
		KR 102101308 B1	16 Apr 2020
		KR 20170023047 A	02 Mar 2017
		KR 102106194 B1	29 Apr 2020
		KR 20200039824 A	16 Apr 2020
		KR 102132146 B1	08 Jul 2020
		KR 20200040907 A	20 Apr 2020
		KR 102138027 B1	27 Jul 2020
		KR 20200044778 A	29 Apr 2020
		KR 102143143 B1	10 Aug 2020
		KR 20190101510 A	30 Aug 2019
		KR 102143308 B1	10 Aug 2020
		KR 20180052112 A	17 May 2018
		KR 102145660 B1	18 Aug 2020
		KR 20200035486 A	03 Apr 2020
		KR 102147926 B1	25 Aug 2020
		KR 20180078355 A	09 Jul 2018
		KR 102156223 B1	15 Sep 2020
		KR 20200090960 A	29 Jul 2020
		KR 102186012 B1	04 Dec 2020
		KR 20190077611 A	03 Jul 2019
		KR 102197560 B1	31 Dec 2020
		KR 20150004413 U	09 Dec 2015
		KR 20160010523 A	27 Jan 2016
		KR 20160134627 A	23 Nov 2016
		KR 20170107572 A	25 Sep 2017
		KR 20180082637 A	18 Jul 2018
		KR 20180121686 A	07 Nov 2018
		KR 20190117819 A	16 Oct 2019

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		KR 20190132321 A	27 Nov 2019
		KR 20200038565 A	13 Apr 2020
		KR 20200096464 A	12 Aug 2020
		KR 20200101996 A	28 Aug 2020
		KR 20200108116 A	16 Sep 2020
		KR 20200136506 A	07 Dec 2020
		KR 20210000327 A	04 Jan 2021
		MX 338784 B	02 May 2016
		MX 342072 B	13 Sep 2016
		MX 348250 B	05 Jun 2017
		MX 2010012494 A	21 Dec 2010
		MX 2012008369 A	12 Sep 2012
		MX 2012011426 A	01 Apr 2013
		NL 2009544 A	03 Apr 2013
		NL 2009544 B1	24 May 2017
		NL 2012965 A	09 Dec 2014
		NL 2012965 C2	10 Mar 2015
		NL 2015232 A	07 Jul 2016
		NL 2015232 B1	10 Apr 2017
		NL 2015236 A	07 Jul 2016
EP 3304956 A1	11 Apr 2018	EP 3304956 A1	11 Apr 2018
		CA 2984367 A1	08 Dec 2016
		CN 107736046 A	23 Feb 2018
		JP 2018524865 A	30 Aug 2018
		KR 20170137955 A	13 Dec 2017
		KR 101861546 B1	29 Jun 2018
		KR 20180056809 A	29 May 2018
		TW 201701683 A	01 Jan 2017
		US 2016360404 A1	08 Dec 2016
		US 9706397 B2	11 Jul 2017

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2020/062368

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 2017272942 A1	21 Sep 2017
		US 10009763 B2	26 Jun 2018
		WO 2016195907 A1	08 Dec 2016