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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2021 (29.04.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/079115 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04N 7/14* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/GB2020/052651

(22) International Filing Date:
22 October 2020 (22.10.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1915313.9 23 October 2019 (23.10.2019) GB
19275105.5 23 October 2019 (23.10.2019) EP

(71) Applicant: **BAE SYSTEMS PLC** [GB/GB]; 6 Carlton Gardens, London SW1Y 5AD (GB).

(72) Inventors: **KURTIS, Ashley**; BAE SYSTEMS, Warton Aerodrome, Warton, Preston Lancashire PR4 1AX (GB). **DANIEL, Kristian**; BAE SYSTEMS, Warton Aerodrome, Warton, Preston Lancashire PR4 1AX (GB).

(74) Agent: **BAE SYSTEMS PLC, GROUP IP DEPT**; PO Box 87, Farnborough Aerospace Centre, Farnborough Hampshire GU14 6YU (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, 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, 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,

(54) Title: SECURE COMMUNICATION BETWEEN DEVICES

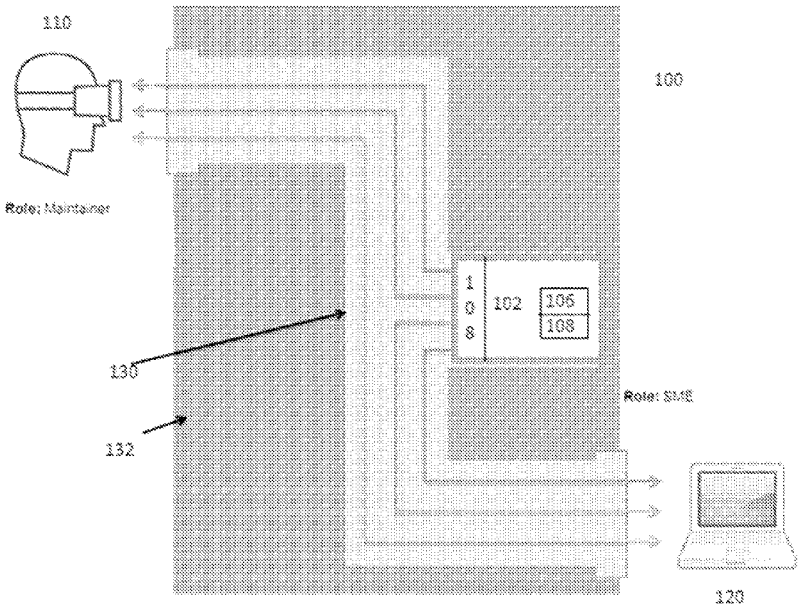

FIG. 1

(57) Abstract: A method of providing secure communication between first (110) and second (120) devices comprises the first device and the second device connecting to a server (102) via a secure communication channel (130). Encryption keys for the devices are generated and data relating to the encryption keys are exchanged via the server in the secure communication channel. A peer-to-peer connection for exchanging data is generated using encrypted connection information for the devices.

WO 2021/079115 A1

[Continued on next page]

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

Declarations under Rule 4.17:

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

Published:

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

SECURE COMMUNICATION BETWEEN DEVICES

The present invention relates to secure communication between devices.

Secure data transfer is important in many situations. For example, there are currently no known video calling applications which provide a high standard of security for streaming sensitive data from one user to another. At this point in time some companies provide secure video calling, which is facilitated via their own cloud technology. However, for users of sensitive information, such as the military, there is a concern that a third party could potentially access that data when a call is taking place.

Embodiments of the present invention are intended to address at least some of the above technical problems.

Embodiments can allow users to securely exchange data, including making video calls, between devices (e.g. wearable devices and PCs), regardless of where they are in the world. The communication can take place peer-to-peer via a secure communication channel that is encrypted at either end.

According to an aspect of the present invention there is provided a (computer-implemented) method of providing secure communication between first and second devices, the method comprising:

the first device and the second device connecting to a server via a secure communication channel;

generating (e.g. by the first device or the server) encryption keys for the first device;

generating (e.g. by the second device or the server) encryption keys for the second device;

transferring (e.g. from the first device or the server) data relating to the encryption keys (e.g. a first public key) for the first device to the second device via the server in the secure communication channel;

transferring (e.g. from the second device or the server) data relating to the encryption keys (e.g. a second public key) for the second device to the first device via the server in the secure communication channel;

generating (e.g. by the first device or the server) peer-to-peer connection information for the first device and encrypting the peer-to-peer connection information for the first device using the data relating to the encryption keys for the second device;

generating (e.g. by the second device or the server) peer-to-peer connection information for the second device and encrypting the peer-to-peer connection information for the second device using the data relating to the encryption keys for the first device;

transferring (e.g. from the first device or the server) the encrypted peer-to-peer connection information for the first device to the second device via the server in the secure communication channel;

transferring (e.g. from the second device or the server) the encrypted peer-to-peer connection information for the second device to the first device via the server in the secure communication channel;

the first device decrypting the encrypted peer-to-peer connection information for the second device (e.g. using the public key for the first/second device);

the second device decrypting the encrypted peer-to-peer connection information for the first device (e.g. using the public key for the second/first device);

the first device and the second device using the decrypted peer-to-peer connection information for the first device and the decrypted peer-to-peer connection information for the second device to open a peer-to-peer connection in the secure communication channel, and

the first device and the second device exchanging data via the peer-to-peer connection.

The method may further comprise:

the first/second device including a security code in data transferred to the second/first device (via the server in the secure communication channel and/or via the peer-to-peer connection), and

the first/second device checking for inclusion of the security code in the data and only preforming further steps on the data if the security code is included in the data.

The security code may be included in the data relating to the encryption keys for the first or second, respectively, device; the encrypted peer-to-peer connection information for the first or second device, and/or the data exchanged with the first or second device via the peer-to-peer connection. For example, the first/second device may add the security code, e.g. a byte (a few digits), to a beginning and/or an end of the data, which may be used for generating the public key for the first/second device. The data may then only be able to be encrypted/decrypted if it includes the security code. The security code could be a known secret between users of the first device and the second device which only they know when making a call.

The method may further comprise:

deleting the encryption keys for the first device and/or the encryption keys for the second device after the exchanging of data has ended.

The encryption keys (for each of the first device and the second device) may comprise a public key and a private key. The transferred data relating to the encryption keys for the first or the second device may comprise the public key for the first or second device, respectively.

The peer connection information for the first/second device may comprise Session Description Protocol, SDP, information and may further comprise Interactive Connectivity Establishment, ICE, information. Embodiments may transfer the SDP then the ICE information in sequence between the first/second devices.

The method may further comprise: the server notifying, via the secure communication channel, the second device of the first device requesting to communicate with the second device, and

the server notifying the first device of acceptance of the communication request by the second device via the secure communication channel.

The secure communication channel may be implemented using a high threat gateway component. The secure communication channel may be implemented using a cloud computing service.

The exchanged data may comprise audio and/or video data and/or instant messaging data. The exchanged data may comprise an audio or video call data.

According to a further aspect of the invention there is provided a method for a first device to perform secure communication with a second device, the method comprising:

connecting to a server via a secure communication channel;

generating encryption keys for the first device;

transferring data relating to the encryption keys for the first device to the second device via the server in the secure communication channel;

receiving data relating to encryption keys for the second device via the server in the secure communication channel;

generating peer-to-peer connection information for the first device and encrypting the peer-to-peer connection information for the first device using the data relating to the encryption keys for the second device;

transferring the encrypted peer-to-peer connection information for the first device to the second device via the server in the secure communication channel;

receiving encrypted peer-to-peer connection information for the second device via the server in the secure communication channel;

decrypting the encrypted peer-to-peer connection information for the second device using the encryption keys for the first device;

using the peer-to-peer connection information for the first device and the decrypted peer-to-peer connection information for the second device to open a peer-to-peer connection in the secure communication channel, and

exchanging data with second device via the peer-to-peer connection.

According to a further aspect of the invention there is provided a method for a sever to allow a first device and a second device to perform secure communication, the method comprising:

connecting to the first device via a secure communication channel;

connecting to the second device via the secure communication channel;

receiving data relating to encryption keys for the first device via the secure communication channel;

receiving data relating to encryption keys for the second device via the secure communication channel;

transferring the data relating to encryption keys for the first device to the second device via the secure communication channel;

transferring the data relating to encryption keys for the second device to the first device via the secure communication channel;

receiving encrypted peer-to-peer connection information for the first device and transferring the encrypted peer-to-peer connection information for the first device via the secure communication channel to the second device, and

receiving encrypted peer-to-peer connection information for the second device and transferring the encrypted peer-to-peer connection information for the second device via the secure communication channel to the first device.

According to a further aspect of the present invention there is provided a computer-readable storage medium comprising instructions which, when executed by a computer, cause the computer to perform at least one of the methods described herein. The method may comprise the method performed by the first/second device. The method may comprise the method performed by the server.

According to another aspect of the present invention there is provided a data transfer server comprising a processor configured to perform a method of allowing a first device and a second device to perform secure communication substantially as described herein.

According to another aspect of the present invention there is provided a device comprising a processor configured to perform a method of performing secure communication with a second device substantially as described herein.

According to another aspect of the present invention there is provided a system adapted/configured to provide secure communication between first and second devices, the system comprising a server and at least the first device and the second device configured substantially as described herein.

The system may further comprise secure communication channel hardware.

BRIEF DESCRIPTION OF THE FIGURES

For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings in which:

Figure 1 is a block diagram of an example system, and

Figure 2 is a diagram schematically illustrating operation of the example system.

DETAILED DESCRIPTION OF EMBODIMENTS

Figure 1 is a diagram of an example embodiment of a secure communication system 100. The example system comprises a server computing device 102 that has (or is in communication with) at least a memory 104 and a processor 106. The server may comprise a commercially-available Personal Computer (PC), a server rack or the like. The memory can contain data and instructions for processing/execution by the processor. The server can further comprise (or be in communication with) one or more wired or wireless communications interface 108. The server may also comprise (or be in communication with) further well-known features, such as a user interface, display, and so on, which need not be described herein in detail.

The example system 100 further comprises first and second devices. These may comprise various types of computing devices, e.g. a PC, smartphone, tablet, wearable device, etc. Each device will comprise (or be in communication with) at least a processor, memory and communications interface. In embodiments the first 110 and second 120 device are configured to exchange data by means of a secure communication channel 130 that can be controlled by the server 102.

In some embodiments the secure communication channel 130 may take the form of a secure pipeline, which may be implemented using high threat gateway hardware, such as Microsoft Forefront Threat Management Gateway™. The secure communication channel may comprise a communication channel that is dedicated to transferring data by embodiments and which may not be used for transferring other data. The transferred data in the channel may be encrypted using the techniques described herein. Data within the secure communication channel can therefore be effective isolated from the wider internet 132. In other embodiments the secure communication channel may be implemented using a server 102 located within a cloud computing service (e.g. Microsoft Azure Servers™). This cloud server may be accessible over the internet. Encrypted signalling messages can be sent over the internet to the cloud server (e.g. via its IP Address). The cloud server can then re-direct data to the intended recipient/device, thereby effectively providing the secure communication channel.

Applications executed by the first device 110, the second device 120 and the server 102 can facilitate secure communication/data transfer, including video calls, between the first and second devices in the system 100 via the secure communication channel 130. The secure communication channel can be accessed by any device which has been configured to do so by an operator/controller user of the system 100, regardless of their connection to any other network, if any. Whenever a device has its application open, it will be connected to server via the secure communication channel. Once connected, any data sent via the secure communication channel, and through the internet in some cases, is intended to be secure and safe from being intercepted. All data/content, as well as signalling messages related to setting up a secure connection in the secure communication channel, will travel via the channel to

the server, where it will be redirected to the destination device. Audio/video calls can take place via this secure communication channel in some embodiments.

In some embodiments WebRTC is used to produce the applications, although it will be understood that alternative packages can be used. WebRTC comprises a set of open source APIs that give developers the ability to create real time video calls peer-to-peer. The APIs can allow developers to gain control of a device's media capabilities (e.g. microphone and/or webcam). WebRTC also allows a user to specify the video format and quality to ensure any video latency is low. To the inventor's knowledge WebRTC has not previously been used in combination with a secure network connection/channel.

Figure 2 schematically illustrates an example of operation of the system 100. In the example the first device 110 comprises a set of Virtual/Augmented Reality goggles and the second device 120 may comprise a PC or the like. In the example scenario, the user of the first device is a maintainer user looking to obtain advice from a subject matter expert who is a user of the second device. Advantageously, the data exchange between the two users can take the form of a video call so that the subject matter expert user can provide substantially real-time visual assistance. For instance, images captured using a camera associated with the expert's PC 120 can be displayed on the maintainer's goggles 110, possibly superimposed or displayed in a semi-transparent manner on the maintainer's view of his surroundings. This can help demonstrate how to manipulate a piece of equipment that the maintainer is located next to and/or provide onscreen textual/graphical information, etc. However, it should be understood that the types of use, users and devices can vary. Alternative embodiments may transfer audio data and/or other data, such as instant messages. It will also be understood that in alternative embodiments more than two devices can communicate with each other in a real-time/simultaneous manner using the data transfer system.

At steps 250, 252 the applications running on the first 110 and the second 120 devices connect to the server 102 via the secure communication channel 130. This can involve any suitable processing steps, communications standards

or protocols, and so on, as determined when the applications are created or configured. To start the video call the maintainer user of the first device can select a Subject Matter Expert user whose device (e.g. the second device 120) is currently connected to the server 102. The server may make information (e.g. details of the user/subject matter) regarding the devices/users that are connected to it available over the secure communication channel. The server can inform applications being executed on each connected device which other devices are connected to, or disconnected from, the server.

Before any data transfer takes place, users can specify which video codecs and video quality, etc, they would like to use. At step 254, the first device 110 sends a request to communicate with the second device 120 to the server 102 via the secure communication channel 130. At step 256 the server conveys the request to the second device and its user can then indicate to the sever and first device that it accepts the call at step 258. Before the peer-to-peer communication/video call can take place, each instance of the application running on the first 110 and the second 120 device may perform the steps described below.

For each connection/call that is set up, the instances of the applications running on the first 110 and the second 120 devices will each create a private and public key. Thus, at step 260 the first device generates a private key and public key, and at step 262 the second device 120 also generates its own private and public keys. A private key will not normally be shared with any person or device other than the device that created it; however, the public keys will be exchanged between the devices. By means of the combination of the device's own private key and the other device's public key at least the signalling messages used to set up a peer-to-peer connection between the devices can be encrypted and decrypted. The public keys can be exchanged using the secure communication channel 130 for security; however, even if an attacker was somehow able to get hold of a public key, they would still be unable to decrypt messages because they also need the corresponding private key. A message that a sender encrypts using the recipient's public key can be decrypted only by the recipient's paired private key. Whenever a new call is to take place, the

private and public keys can be reset. Thus, keys are generated and destroyed on a per communication session/call basis.

At step 264 the first device 110 transfers data representing its public key via the secure communication channel 130 to the server 102, which then forwards it to the second device 120 via the secure communication channel at step 265. Similarly, at step 266 the second device provides data representing its public key to the server via the secure communication channel 130, which then forwards it to the first device via the secure communication channel at step 267. The exchange of the keys can allow data transfer in the system 100 to feature end-to-end encryption. Thus, before any signalling message is sent to the other device it can be encrypted.

In some embodiments there can also be an option to include an additional password/security code which will be included in at least the encryption key exchange process. Preferably, the password will not be exchanged via any signalling method over the secure communication channel or any other communications network connection between the two devices, but, instead, it may only be known by the users of the devices by prior personal arrangement or the like. In some embodiments the additional protection may comprise adding a security/verification code, e.g. a byte (a few digits), to the beginning and/or the end of a secret agreement/message that is used for generating the public keys. All or some data transferred between the devices will then only be able to be encrypted/decrypted if they include these extra digits. The digits could be a personal secret shared between the users of the two devices.

Following the key exchange the first 110 and the second 120 devices can exchange, via the secure communication channel 130 and the server 102, information useable to create a peer-to-peer data transfer connection between the two devices. This can involve one or more messages being exchanged between the devices that are encrypted using the keys generated and exchanged in the previous steps. In some embodiments, before the peer-to-peer data transfer can take place, both of the devices must exchange their own SDPs (Session Description Protocol; standard available at

https://tools.ietf.org/html/rfc4566), as well as ICE (Interactive Connectivity Establishment; standard available at https://tools.ietf.org/html/rfc5245) candidates. SDPs contain information on what media capabilities each device has, and what video/audio codecs they will use for the video call. The ICE candidates describe how the peer-to-peer connection will take place, including IP addresses and ports at which the device can be accessed. In alternative embodiments different connection information can be generated and exchanged; for example, different video call connection information, or connection information required for exchanging audio or other (e.g. text/image) data.

At steps 268, 270 the first 110 and the second 120 devices each generate the respective SDP and ICE information. The SDP and exchange ICE candidate data then can be encrypted using the keys previously generated and exchanged. In order to exchange SDPs and ICE candidates, the application executed on the server 102 can function as a Signalling Server. The main purpose of this is to pass along signalling messages useable to set up the peer-to-peer connection/channel to the intended recipients. Both the SDPs and ICE candidates contain sensitive information, including the IP address of the devices making the call. If any of these signalling messages were intercepted by a third party then they could potentially re-route the call to themselves, or stop the call from taking place altogether. In order to overcome these issues, embodiments can use the signalling server located within the secure communication channel, with any/all signalling messages being encrypted end-to-end.

Thus, at step 272 the first device 110 transfers encrypted data representing its SDP information via the secure communication channel 130 to the server 102, which then forwards it to the second device 120 via the secure communication channel at step 274. At step 276 the second device provides transfers encrypted data representing its SDP information the server via the secure communication channel, which then forwards it to the first device via the secure communication channel at step 278 Following this, at step 282 the first device 110 transfers encrypted data representing its ICE information via the secure communication channel 130 to the server 102, which then forwards it to the second device 120 via the secure communication channel at step 284. At step 286 the second

device provides transfers encrypted data representing its ICE information the server via the secure communication channel, which then forwards it to the first device via the secure communication channel at step 288.

At step 290, after the ICE Candidates have been exchanged, the peer-to-peer video call can begin. Users of the devices 110, 120 are able to converse with one another with low latency. When the call is ended (step 292) by one of the users, the private and public keys for that session can be deleted by each of the devices (steps 294, 296), or, alternatively, this could be done under the control of the server 102.

In summary, embodiments can provide a secure communication capability, including video calling, that can ensure the security of sensitive information. Embodiments are considered particularly secure because they involve multiple/ chained security features, including the use of encryption keys, the secure communication channel and additional security codes.

It will be understood that embodiments can be implemented using any suitable software, programming language, data editors, etc, and may be represented/stored/processed using any suitable data structures. In alternative embodiments, at least some of the devices can be based on analogue computing elements. It will also be understood that the steps described herein as part of the detailed embodiments may be re-ordered, omitted and/or repeated. Additional steps may also be performed. Some steps may be performed concurrently instead of sequentially. Further, different components may perform some of the steps. For instance, the encryption keys for at least one of the devices may be generated by another device, e.g. the server, that may then transfer the public and private keys to the first device and/or transfer the public key to the other device.

Attention is directed to any papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings) may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

CLAIMS

1. A computer-implemented method of providing secure communication between a first device (110) and a second device (120), the method comprising:

the first device and the second device connecting to a server (102) via a secure communication channel (130);

generating encryption keys for the first device;

generating encryption keys for the second device;

transferring data relating to the encryption keys for the first device to the second device via the server in the secure communication channel;

transferring data relating to the encryption keys for the second device to the first device via the server in the secure communication channel;

generating peer-to-peer connection information for the first device and encrypting the peer-to-peer connection information for the first device using the data relating to the encryption keys for the second device;

generating peer-to-peer connection information for the second device and encrypting the peer-to-peer connection information for the second device using the data relating to the encryption keys for the first device;

transferring the encrypted peer-to-peer connection information for the first device to the second device via the server in the secure communication channel;

transferring the encrypted peer-to-peer connection information for the second device to the first device via the server in the secure communication channel;

the first device decrypting the encrypted peer-to-peer connection information for the second device;

the second device decrypting the encrypted peer-to-peer connection information for the first device;

the first device and the second device using the decrypted peer-to-peer connection information for the first device and the decrypted peer-to-peer connection information for the second device to open a peer-to-peer connection in the secure communication channel, and

the first device and the second device exchanging data via the peer-to-peer connection.

2. A method according to claim 1 further comprising:

the first (110) or the second (120) device including a security code in data transferred to the second or the first device, respectively, and

the first or the second device checking for inclusion of the security code in the transferred data and only preforming further steps on the data if the security code is included in the data.

3. A method according to claim 2, wherein the security code is included in the data relating to the encryption keys for the first (110) and the second (120) device, and the security code is included in the encrypted peer-to-peer connection information for the first or second device, and the security code is included in the data exchanged with the first or second device via the peer-to-peer connection.

4. A method according to claim 3, wherein the first (110) or the second (120) device may add the security code to a beginning and/or an end of the data.

5. A method according to any preceding claim, may further comprising:

deleting the encryption keys for the first device (110) and/or the encryption keys for the second device (120) after the exchanging of data has ended.

6. A method according to any preceding claim, wherein the encryption keys for each of the first device (110) and the second device (120) comprise a public key and a private key, and wherein the transferred data relating to the encryption keys for the first and the second device each comprise the public key for the first or second device, respectively.

7. A method according to any preceding claim, wherein the peer connection information for the first (110) and the second (120) device comprises Session Description Protocol, SDP, information and Interactive Connectivity Establishment, ICE, information.

8. A method according to any preceding claim, further comprising:

the server (102) notifying, via the secure communication channel (130), the second device (120) of the first device (110) requesting to communicate with the second device, and

the server notifying the first device of acceptance of the communication request by the second device via the secure communication channel.

9. A method according to any preceding claim, wherein the secure communication channel is implemented using high threat gateway hardware or a cloud computing service.

10. A method according to any preceding claim, wherein the exchanged data comprises audio and/or video data.

11. A method for a first device (110) to perform secure communication with a second device (120), the method comprising:

connecting to a server (102) via a secure communication channel (130);

generating encryption keys for the first device;

transferring data relating to the encryption keys for the first device to the second device via the server in the secure communication channel;

receiving data relating to encryption keys for the second device via the server in the secure communication channel;

generating peer-to-peer connection information for the first device and encrypting the peer-to-peer connection information for the first device using the data relating to the encryption keys for the second device;

transferring the encrypted peer-to-peer connection information for the first device to the second device via the server in the secure communication channel;

receiving encrypted peer-to-peer connection information for the second device via the server in the secure communication channel;

decrypting the encrypted peer-to-peer connection information for the second device using the encryption keys for the first device;

using the peer-to-peer connection information for the first device and the decrypted peer-to-peer connection information for the second device to open a peer-to-peer connection in the secure communication channel, and

exchanging data with second device via the peer-to-peer connection.

12. A method for a sever (102) to allow a first device (110) and a second device (120) to perform secure communication, the method comprising:

connecting to the first device via a secure communication channel (130);

connecting to the second device via the secure communication channel;

receiving data relating to encryption keys for the first device via the secure communication channel;

receiving data relating to encryption keys for the second device via the secure communication channel;

transferring the data relating to encryption keys for the first device to the second device via the secure communication channel;

transferring the data relating to encryption keys for the second device to the first device via the secure communication channel;

receiving encrypted peer-to-peer connection information for the first device and transferring the encrypted peer-to-peer connection information for the first device via the secure communication channel to the second device, and

receiving encrypted peer-to-peer connection information for the second device and transferring the encrypted peer-to-peer connection information for the second device via the secure communication channel to the first device.

13. A computer-readable storage medium comprising instructions which, when executed by a computer, cause the computer to perform at least a method according to any preceding claim.

14. A first computing device (110) comprising a processor configured to perform a method of performing secure communication with a second device (120) according to claim 11.

15. A data transfer server (102) comprising a processor configured to perform a method of allowing a first device (110) and a second device (120) to perform secure communication according to claim 12.

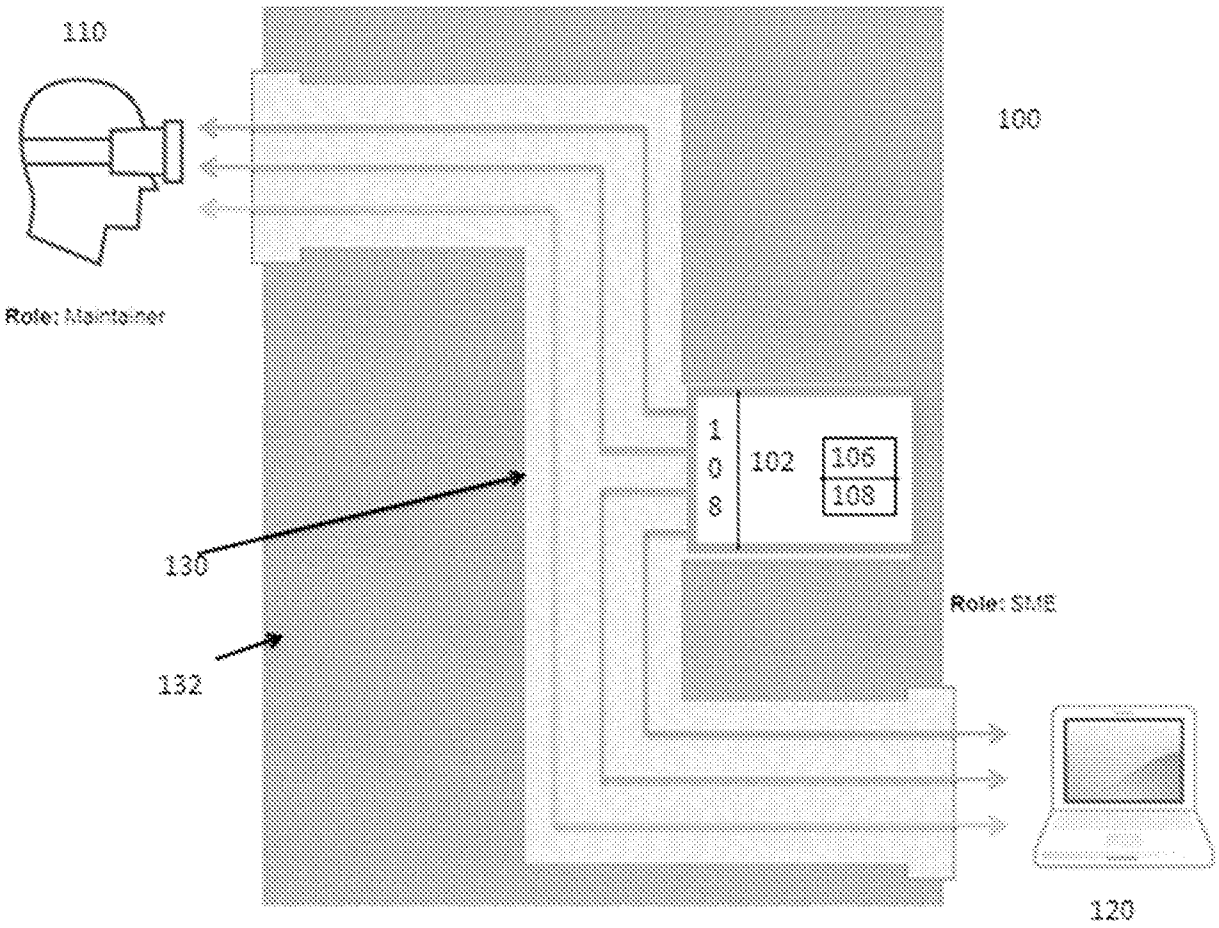

FIG. 1

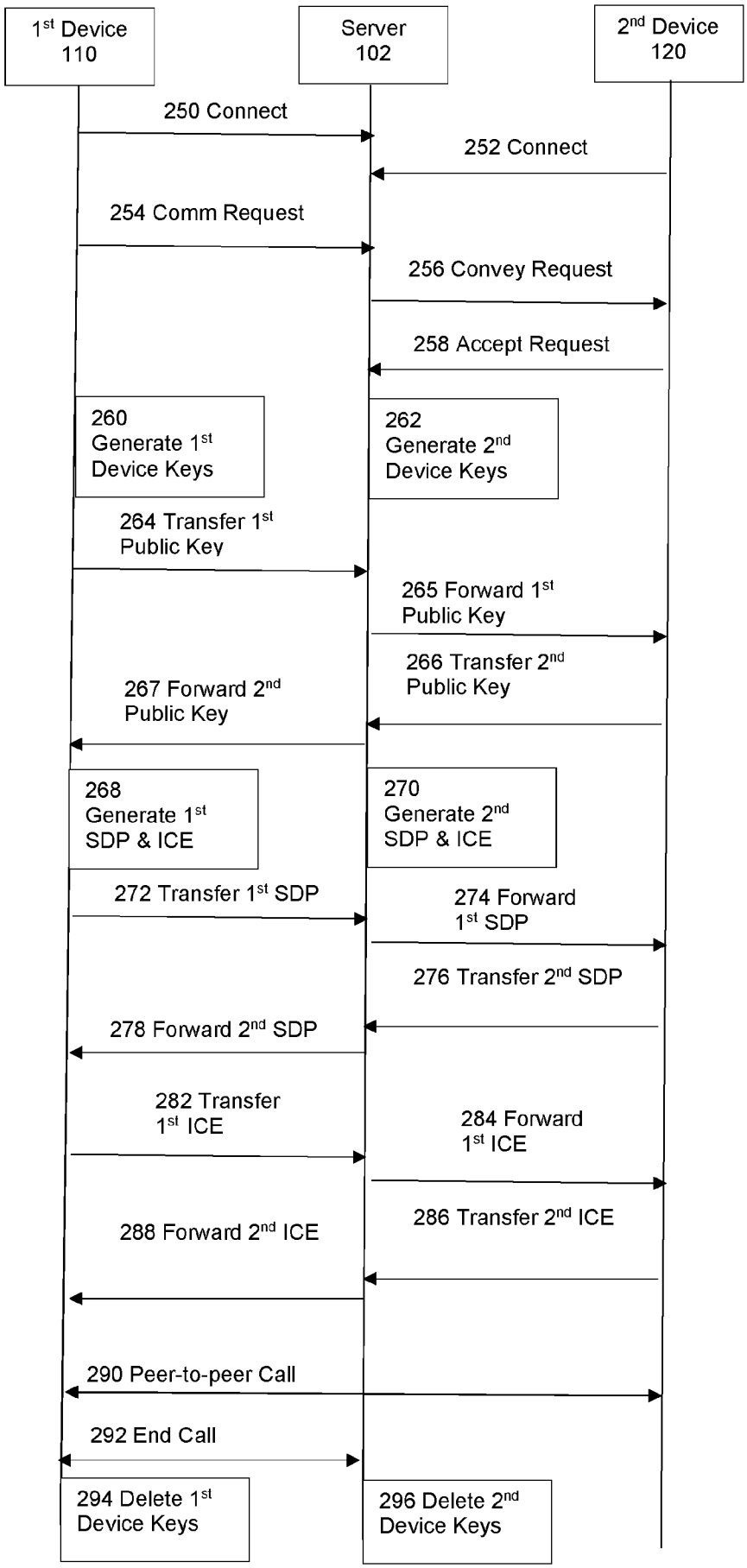
1st Device 110
Server 102
2nd Device 120
250 Connect
252 Connect
254 Comm Request
256 Convey Request
258 Accept Request
260 Generate 1st Device Keys
262 Generate 2nd Device Keys
264 Transfer 1st Public Key
265 Forward 1st Public Key
266 Transfer 2nd Public Key
267 Forward 2nd Public Key
268 Generate 1st SDP & ICE
270 Generate 2nd SDP & ICE
272 Transfer 1st SDP
274 Forward 1st SDP
276 Transfer 2nd SDP
278 Forward 2nd SDP
282 Transfer 1st ICE
284 Forward 1st ICE
286 Transfer 2nd ICE
288 Forward 2nd ICE
290 Peer-to-peer Call
292 End Call
294 Delete 1st Device Keys
296 Delete 2nd Device Keys

FIG. 2