MEDICOM

DATA TRANSFER ONE SHEET

SEPTEMBER 2019

www.medicom.us

Data Transfer Protocol

To ensure data is secured and successfully delivered to its intended recipients, Medicom's transfer protocol involves multiple steps: signaling, peer discovery, connection negotiation, media stream encryption and decryption before and after delivery, and persistent sending.

1 Signaling

Medicom initiates connections between two devices through Medicom's signaling server. When a sender initiates a transfer, Medicom first ensures that the target device is reachable and willing to establish a connection. Medicom can connect devices across distinct and disparate networks and behind one or more layers of NAT, both symmetric and asymmetric. Medicom uses proprietary STUN messaging to traverse NAT.

The target device is notified of the connection offer through Medicom, which can be configured to manually or automatically accept the offer. Once the target device accepts a connection offer, the Medicom server routes the response back to the device which initiated the exchange. If the target device is not online to accept the transfer, the device which initiated the exchange waits for the target device to come online.

2 Peer Discovery

Once devices agree to establish a connection, Medicom exchanges the information about the data stream. Medicom uses the Session Description Protocol (SDP) to describe the properties of the data about to be exchanged. Once this description is generated, the revised offer is sent to the target device via the signaling channel.

3 Connection Negotiation

After the devices agree to exchange the data, Medicom identifies potential routing paths and checks for connectivity. Medicom uses built-in Interactive Connectivity Establishment (ICE) to perform the necessary routing and connectivity checks. As soon as Medicom implements a shared signaling channel, a conduit between the two devices is established.

Unlike other distributed application architectures, Medicom's protocol does not require the use of UDP or the opening of ports; this is possible because Medicom's proprietary version of STUN communicates over common TCP ports. This proves to be an advantage to our customers as it maximizes system security since no vulnerable ports have to be opened to use Medicom.

Once Medicom establishes a conduit, the Medicom signaling server disconnects before the data transfers. Medicom creates an untraceable conduit that lasts the duration of the data transfer, preventing vulnerabilities that lead to man-in-the-middle attacks.

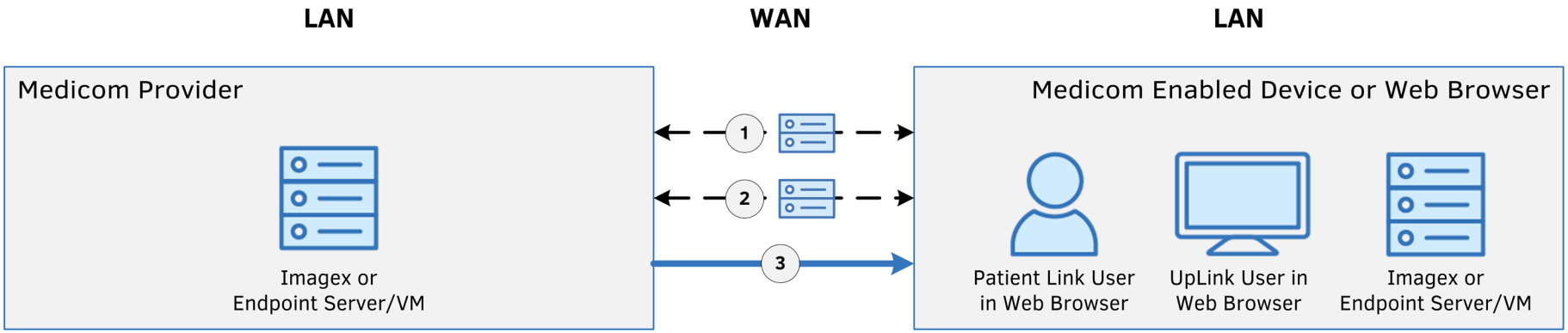
4 Data Stream Encryption and Decryption

Medicom's security features ensure privacy and protection of data. Medicom encrypts the media stream using the 2048 Bit Datagram Transport Layer Security (DTLS) method. DTLS is a standardized protocol and is designed to prevent eavesdropping and tampering. The method was modeled on the Transport Layer Security (TLS) protocol, which offers full encryption with asymmetric cryptography methods, data confidentiality, and message authentication. Each device uses their self-signed certificate based on 2048 RSA keys to exchange the private symmetric 2048 Bit DTLS key for each data transfer. This ensures data can be secured over any SSL based connection on the web.

5 Persistent Sending

Medicom's built-in data delivery algorithm monitors and validates that every piece of data is transferred between devices. This feature gives Medicom the capability of handling interruptions in internet connectivity, as well as computer and server restarts. For example, if data begins transferring and the internet stops working, or if a user has to restart a server, when the device comes back online, the data will resume transferring where it left off until the data is delivered.

Data Transfer Diagram



1. Medicom initiates connections between two devices through Medicom's signaling server. When a sender initiates a transfer, Medicom first ensures that the target device is reachable and willing to establish a connection. Medicom initiates connections between two devices through Medicom's signaling server. When a sender initiates a transfer, Medicom first ensures that the target device is reachable and willing to establish a connection.

2. Once devices agree to establish a connection, Medicom exchanges the information about the data stream. Medicom uses the Session Description Protocol (SDP) to describe the properties of the data about to be exchanged. Once this description is generated, the revised offer is sent to the target device via the signaling channel.

3. After the devices agree to exchange the data, Medicom identifies potential routing paths and checks for connectivity. Medicom uses built-in Interactive Connectivity Establishment (ICE) to perform the necessary routing and connectivity checks. As soon as Medicom implements a shared signaling channel, a conduit between the two devices is established.

Data Stream Encryption/Decryption

Medicom's security features ensure privacy and protection of data. Medicom encrypts the media stream using the 2048 Bit Datagram Transport Layer Security (DTLS) method. Each device uses their self-signed certificate based on 2048 RSA keys to exchange the private symmetric 2048 Bit DTLS key for each data transfer.

Legend

Communication with the Medicom Signaling Sever over HTTPS (TCP Port 443).

Encrypted, peer-to-peer conduit transmitting data using HTTPS (Port 443) or through a TCP port opened by STUN.