CRYPE

Communication with privacy

The **native behavior** of CRYPE is to establish **direct, encrypted device-to-device (Peer-to-Peer, P2P) communication** whenever possible. This method ensures both high security and minimal latency, and is visually indicated by this icon:

When CRYPE users are located within the same local network, P2P communication will also be established between participants. This local P2P connection provides the same benefits of security and low latency and is represented by this icon:

However, if one or both participants are behind a **NAT** (Network Address Translation) or a restrictive firewall that prevents direct P2P connections, a **relay server (TURN server)** will act as an intermediary. The TURN server forwards encrypted communication between participants, ensuring seamless connectivity regardless of network restrictions. It is important to note that using a relay server introduces additional latency compared to direct P2P connections. A relay-based communication is indicated with this icon:

For successful communication, clients (desktop or mobile devices) must allow outgoing connections on specific protocols, URLs and ports as described in this documentation. If these are restricted, communication may rely entirely on the TURN server or is not possible at all.

CRYPE requires access to its signaling server on the internet as the initial point of contact. The signaling server is critical for facilitating the negotiation process to determine the optimal communication method between participants. This negotiation evaluates whether a direct P2P connection is possible or if a relay server (TURN) is necessary to establish the connection.

1. Detailed List of Outgoing Ports, Protocols, URLs and Encryption Used

a. CRYPE API Server

- **Purpose:** Managing the CRYPE user profiles and devices.
- **Application protocol:** https
- **URL:** https://backend.go.crype.eu
- **Ports:** 443 (TCP)
- **Direction:** OUTGOING
- **Encryption:** TLS 1.2 or 1.3

b. CRYPE WEB Client

- **Purpose:** For opening CRYPE application in a WEB-Browser instead of the installed CRYPE App
- **Application protocol:** https
- **URL:** https://go.crype.eu
- **Ports:** 443 (TCP)
- **Direction:** OUTGOING
- **Encryption:** TLS 1.2 or 1.3

c. Signaling server

- **Purpose:** The client establishes outgoing connections to the signaling server to exchange the CRYPE communication candidates and session data.
- **Application protocol:** WebSocketSecure (WSS)
- **URL:** wss:signal.go.crype.eu
- **Ports:** 443 (TCP)
- **Direction:** OUTGOING
- **Encryption:** TLS 1.2 or 1.3

d. Peer-to-peer (P2P) communication

- **Purpose:** Transmit encrypted audio, video, and data streams directly between devices.
- **Application Protocol:** SRTP for audio/video SCTP for global data communication
- **Ports:** 49152-65535 (UDP) randomly selected for communication.
  Each parallel connection to a CRYPE client requires one UDP port. If UDP ports are not open for connections, then Turn Server communication will be used as a fallback
- **Direction:** OUTGOING
- **Encryption:** DTLS 1.2 or 1.3

e. STUN server

- **Purpose:** The client communicates with the STUN server to determine client location in network and NAT type if P2P will not be possible.
- **Application Protocol:** Session Traversal Utilities for NAT (STUN)
- **URL:** stun:turn.go.crype.eu
- **Ports:** Port 443 is used (Default UDP, Fallback TCP)
- **Direction:** OUTGOING
- **Encryption:** TLS 1.2 or 1.3

f. TURN server

- **Purpose:** TURN is used when direct P2P connections are not possible. All data traffic is routed encrypted via a TURN "relay" server.
- **Application Protocol:** Traversal Using Relays around NAT (TURN)
- **URL:** turn:turn.go.crype.eu
- **Ports:** Port 443 is used (Default UDP, Fallback TCP)
- **Direction: OUTGOING**
- **Encryption:** TLS 1.2 or 1.3

2. Recommendations for Optimal Communication Configuration

Ensure Outgoing Connections:

1. Allow outgoing traffic to the following ports:
    - **443** (TCP & UDP)
2. Allow **dynamic ports** in the range **49152–65535 (UDP)** to enable peer-to-peer (P2P) communication.

3. Notes for Proxy Environments

If internet proxy servers are in use, administrators must ensure that communication with all CRYPE servers, ports and protocols, as outlined in this document, is not blocked. Depending on the restrictions imposed by the proxy server, communication outside the local network may be routed through a TURN server (Relay).

For CRYPE communication within the same local network, P2P communication is possible regardless of the presence of a proxy server.