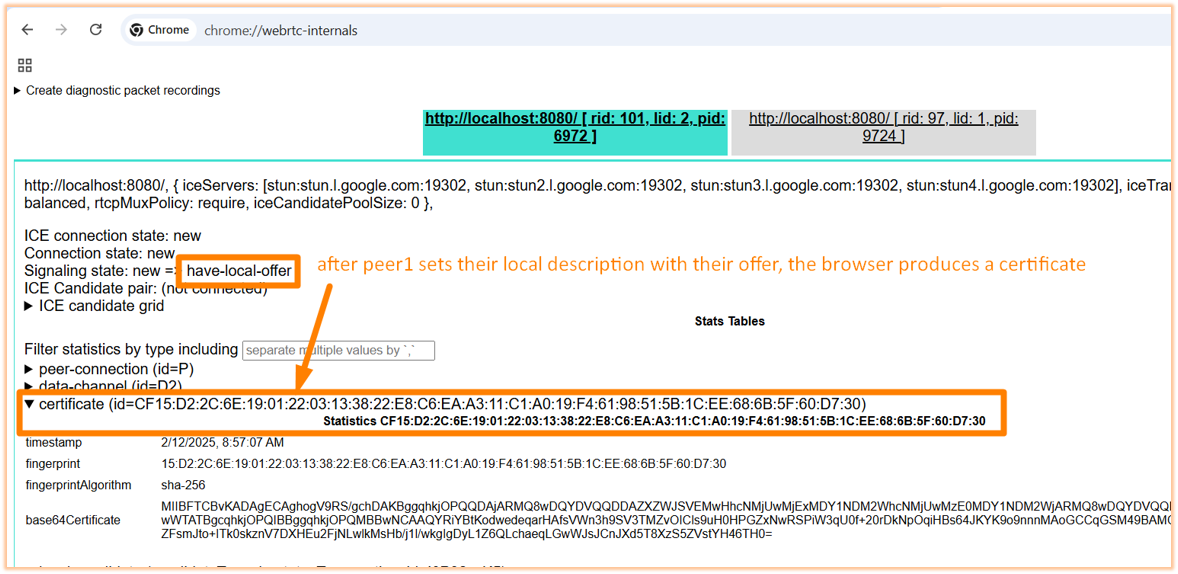
**Certificates**

Data Channels use DTLS when sending and receiving data. This is mandatory and built into the protocol. This involves a handshake process (client hello, server hello, etc) where cryptographic parameters are negotiated. The handshake includes exchanging certificates to authenticate the two peers involved.

* Internally, when **RTCPeerConnection** is instantiated, at some point your browser will create a new certificate.
* This certificate is then used during the DTLS handshake to authenticate the peer and establish a secure channel.
* By securing data in this way, browserA can be certain that the only person who can decrypt data once a connection has been established, is browserB and visa versa. In other words, it prevents man-in-the-middle attacks.

In case you are wondering, yes you can see the certificate in webrtc-internals:



And yes, the other peer when they set their remote description will also produce their own certificate that is sent to the other peer.