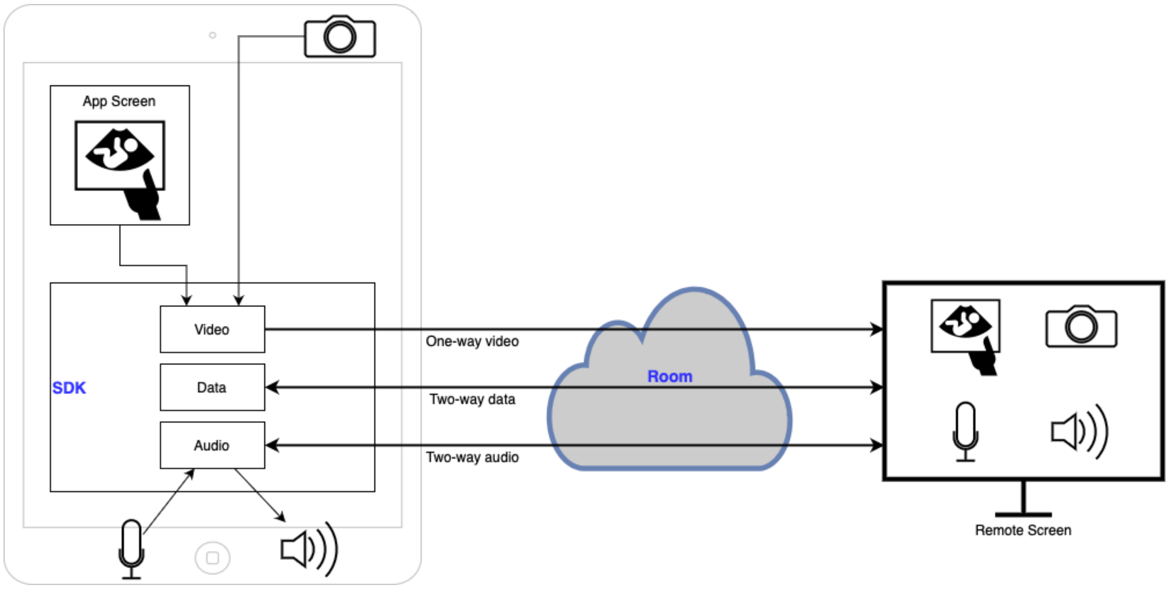
Clarius Live White Paper

Introduction

Clarius Live aims to share in real time the ultrasound image stream and the smart device's camera with a remote user for the purpose of providing real-time feedback. The camera provides context to the remote user like the probe placement.



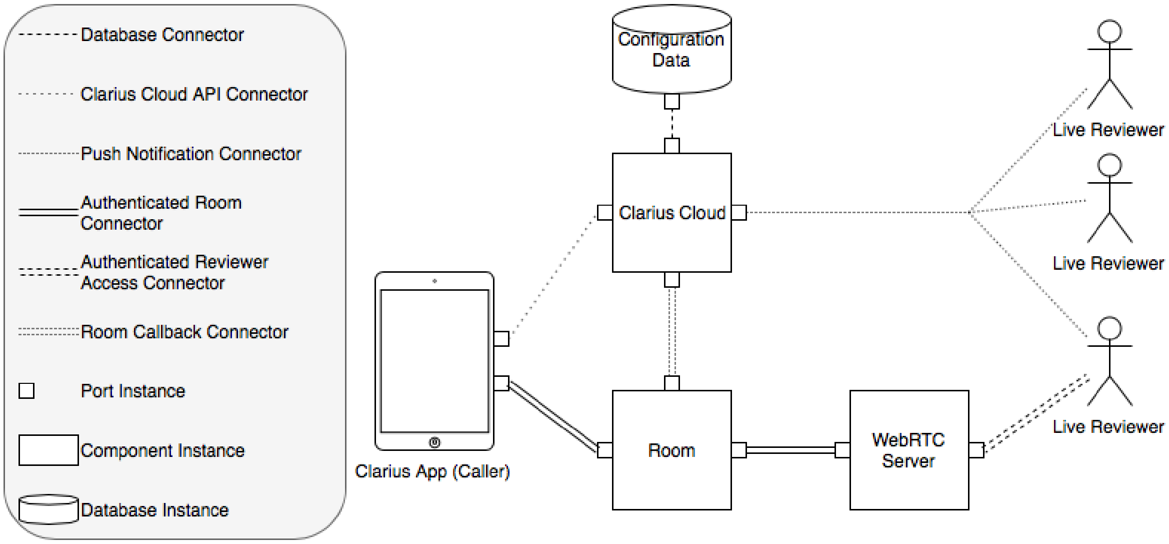
Technical Choices

Video calls will be transmitted with WebRTC, an open standard to transmit video/audio/data.

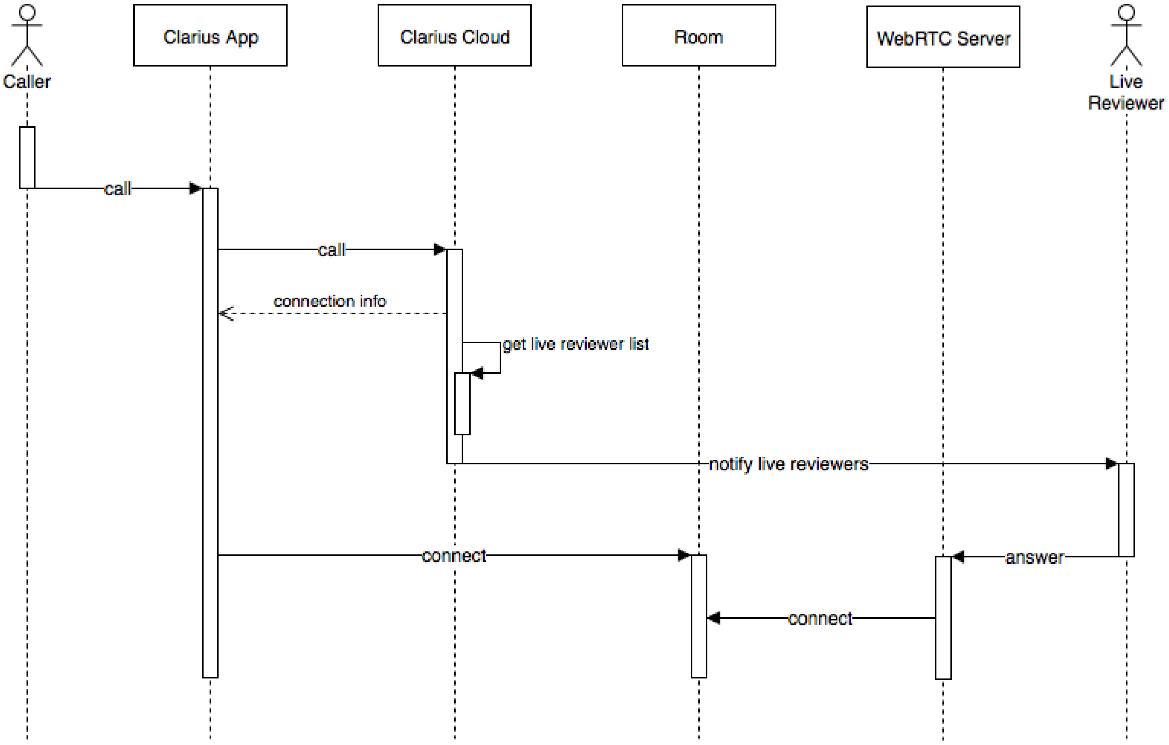
Push notifications will be delivered using SMS and/or e-mail.

Architecture

Component diagram:



Sequence diagram to start a Clarius Live call:



Mode of Operation

The caller is the operator of the app. Before starting a call, the operator must sign in the app with their Clarius credentials. To start a call, the operator must first select a recipient. Upon starting a call, the app will start recording the screen, camera and microphone (can be forbidden by user). The recipient will receive a link pointing to a web page hosted on the Clarius Cloud that will establish the connection to the caller. Access restrictions depend on the type of call.

There are two types of calls:

1. Institution calls: reviewers must be Clarius users and they must be enrolled in the Clarius Live group (this group is managed from the Clarius Cloud admin interface). The caller will only be able to reach reviewers from the same institution. If the caller belongs to more than one institution, they will have to select one institution before the call and only the reviewers from the selected institution will be able to join the call. When reviewers open the Clarius Live link, they will have to sign in to the Clarius Cloud with their Clarius credentials before joining the call.
2. Direct calls: reviewers can be anyone, not only Clarius users. It is the operator's responsibility to obtain permission to contact the reviewers and to ensure the contact information (phone number or email) corresponds to the intended reviewer. Anyone with the link will be able to join the call.

The type of call is selected from the Clarius App call menu.

Third Party Software

Streaming is implemented using Twilio's video SDK.

In the component diagram above, this corresponds to the "Room" and "WebRTC server" components as well as the associated connectors.

More about Twilio video: https://www.twilio.com/docs/video/overview

Security

1. During the call configuration:
    a. All transmissions within the Clarius System (App and Cloud) are encrypted with HTTPS (same as all other communications not related to Clarius Live).
    b. All transmissions between the Clarius System (App and/or Cloud) and the Twilio System are encrypted using HTTPS.
2. During the call:
    a. WebRTC mandates encrypted communications.
    b. The content of the communications (audio/video/data) is not recorded.
3. Room access:
    a. All reviewer links expire after 60 minutes.
    b. Rooms are immediately terminated when the caller terminates the call (attempting to join a terminated room with a still-valid link will fail).
    c. Rooms are automatically terminated after a grace period of a few minutes if the caller unexpectedly disconnects (for example in case of loss of Internet access).
    d. Access restriction depends on the call type:
        i. Institution call: reviewer must sign in the Clarius Cloud before joining the call.
        ii. Direct call: no access restriction in place—anyone with the link can join the call.

Privacy

Twilio services are HIPAA-compliant, see: https://www.twilio.com/hipaa.

Anyway, the Clarius System never transmits any Personal Health Information (PHI) over Clarius Live.

However, if the caller’s screen contains PHI, for example in the form of a user annotation on the imaging screen or by navigating to the demographics page, then the reviewer will be able to see this information.

It is the caller’s responsibility to obtain permission to contact the reviewer (either SMS or e-mail).