July 2020

AUTHENTICATED ACCESS INTO SECURE MEETINGS FOR VIDEO CONFERENCING SYSTEMS

Selim Baygin

Ivan Varghis

Aaron Belcher

Kevin Collins

AUTHENTICATED ACCESS INTO SECURE MEETINGS FOR VIDEO CONFERENCING SYSTEMS

AUTHORS:

Selim Baygin
Ivan Varghis
Aaron Belcher
Kevin Collins

ABSTRACT

A mechanism is provided to positively identify audio and video endpoints as belonging to a customer's organization. The mechanism configures a meeting to admit Organization Authenticated endpoints without further checks, to require User Authentication, or to require User Verification. The mechanism ensures the endpoint belongs to a person who is also an authorized user in the same organization for secure and expedited access into meetings. An additional mechanism is provided to notify meeting hosts for users trying to enter the meeting where they do not meet the security policies. Further, the mechanism allows a host to determine whether to accept or reject users.

DETAILED DESCRIPTION

Collaboration, by definition, is the act of many participants getting together in a meeting context, to work on a common project and share ideas.

Today's collaboration environment is one where many different types of applications and/or devices may be used to participate in these meetings. Some of these methods lend themselves to inherent authentication capabilities (e.g., entering a username and a password), whereas others simply do not have those capabilities.

Some users may require, due to their specific area of work (e.g., law firms, financial services firms), that only authenticated users who belong to their organization are admitted into the meeting, and that others are kept in a waiting area.

However, traditional video conferencing systems that rely on Session Initiation Protocol (SIP) or H.323 protocols do not offer a mechanism to validate the physical user trying to join the meeting, in the same way as, e.g., web browser based authentication works.

They also do not offer a secure way to automatically verify that the device belongs to a particular organization (Org).

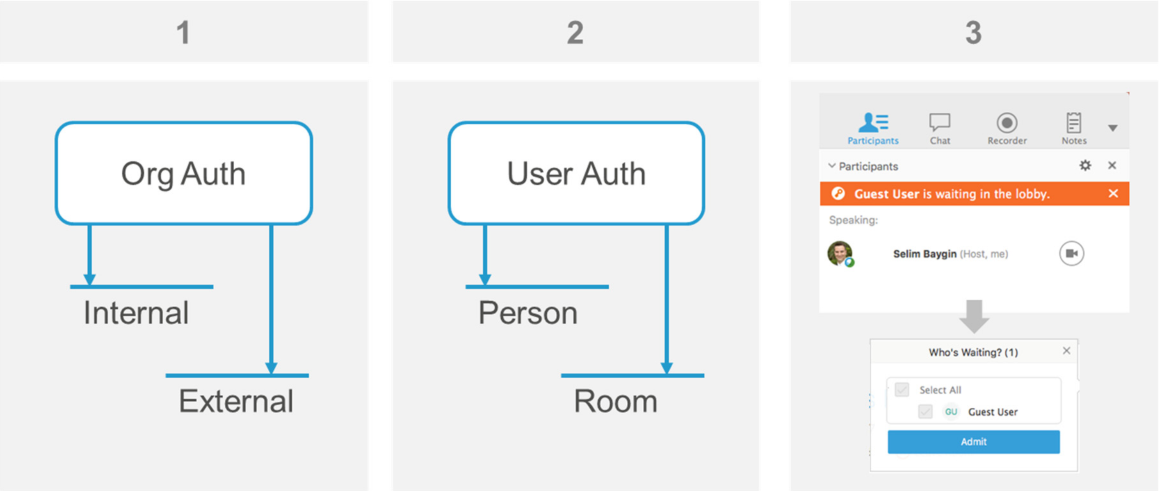
In order to provide a robust mechanism that authenticates, otherwise untrustworthy audio and video conferencing applications or devices (referred to as "endpoints" from this point on), one has to be able to identify what pieces of information would be deemed acceptable to validate the authenticity of said endpoints.

In that regard, an administrator should be able to configure Secure Sockets Layer (SSL) or Transport Layer Security (TLS) certificate attributes that an endpoint must present to be considered part of the administrator's organization. These attributes can include things such as serial numbers, fingerprints, common names, and trusted certificate chains that lead up to a root certificate authority and its own certificate attributes. This is called "Org Authentication".

In addition, an administrator should be able to configure a method to challenge the endpoint user for a security token, that would further validate that the user is who s/he says s/he is.

Furthermore, the system should provide a method to extract attributes from the call setup information from the endpoint to associate it with the end user identity in the organization. This is called "User Authentication".

Finally, an administrator should be able to configure a method to challenge the endpoint user for a security token, that would further validate that the user is who s/he says s/he is. This is called "User Verification".



Guest User is waiting in the lobby.

Figure 1 – High Level Approach

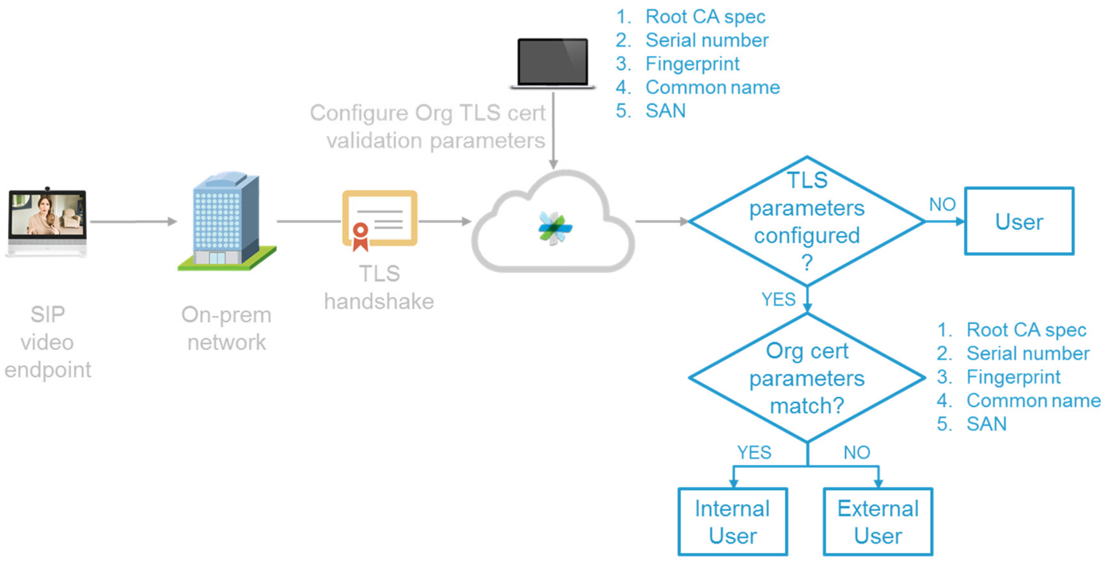


Figure 2 – Org Authentication

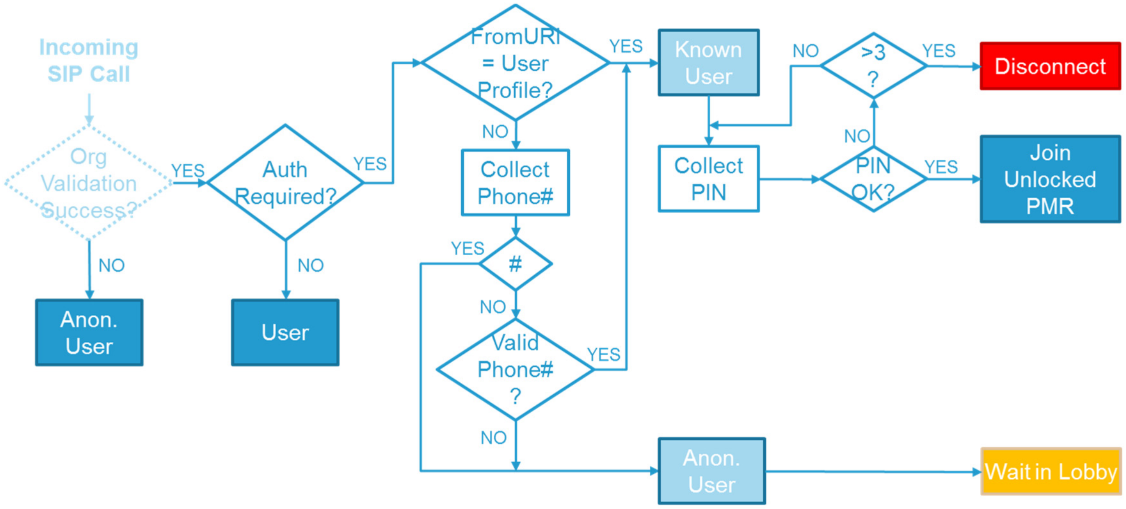


Figure 3 – User Authentication and User Verification

Reference is made to Figures 1 – 3 above.

In a typical call flow, the process would work as follows:

1. Administrator sets up Org Authentication parameters, such as certificate attributes of the administrator's organization as well as that of the Root Certificate Authority (CA) certificate attributes that has signed the administrator's organization's certificates.

2. User endpoint sets up an encrypted connection (e.g., SSL or TLS session) towards the meeting service.
3. Meeting service extracts the key Org Authentication attributes from the certificate handshake process.
4. Meeting service looks up the extracted attributes to the attributes the administrator configured by accessing an admin interface of the meeting service.
5. If the extracted attributes match the configured attributes, the meeting service will deem this connection as "Org Authenticated", meaning the endpoint belongs to the administrator's organization.
6. If the meeting is configured to allow an Org Authenticated endpoint, the system would admit the endpoint to the meeting at that point without prompting the user for a password, PIN, or other manually entered data. If the meeting requires further authentication, the system proceeds to the next step.

If the meeting requires User Authentication or User Verification, the process is as follows.

1. Ensure the person using the endpoint can be factually tied to an end user identity that exists in the administrator's organization. To this end, the meeting service would use parameters in the signaling that the endpoint presents to the meeting service. Since the encrypted connection between the endpoint and the meeting service has now been authenticated, it would be safe to trust the information presented by the endpoint to the meeting service.
2. Meeting service would look up the "From URI" of the endpoint in the meeting service database corresponding to the administrator's organization.
    1. If the data matches an end user's related attribute in his/her profile, the meeting service assumes the connection is coming from the end user's personal endpoint.
        1. If the meeting is configured to admit the endpoint based on User Authentication, the meeting service would admit the participant

without requiring any manually entered data. If the meeting requires User Verification, proceed to the next step.

        2. Meeting service would, then, prompt (using audio and/or video) for a security token. This could be a personal identification number (PIN).
        3. If the user provides the correct security tokens, matching those that were stored in the meeting service database, then the meeting service considers the user as "User *Verified*" and a personal use endpoint.
        4. The meeting service would label the user in the meeting based on the data in the meeting service database for an enhanced user experience.
    2. If the data does not match an end user's related attributes, then the meeting service assumes the connection is coming from a public endpoint, e.g., an endpoint in a conference room.
        1. To establish the identity of the person using the endpoint, the meeting service would prompt the user (using audio and/or video) for a phone number that would have been pre-configured in the meeting service database as well as the PIN for the user.
        2. If the user provides the correct phone number and PIN, then the meeting service would consider the user as "User Verified" and a personal use endpoint.
        3. If the user does not provide a phone number, but simply sends a "by-pass" command, e.g., pressing the # key on a numeric keypad, the meeting service would assume that the endpoint is a public use endpoint.
        4. The meeting service would label the participant using the display name that is provided by the endpoint.
3. Based on the authentication process above, the meeting service can now decide how to treat the user before admitting him or her into the meeting.

1. Disconnect the user if configured organization policy is NOT to admit endpoints that are not associated to the organization.
2. Connect the user directly into the meeting if the user is positively identified, and not a public use endpoint.
3. Place the user in a lobby area, for notification to the meeting host so that the host can take appropriate action, e.g., reject the user or admit user.

In summary, a mechanism is provided to positively identify audio and video endpoints as belonging to a customer's organization. The mechanism configures a meeting to admit Org Authenticated endpoints without further checks, to require User Authentication, or to require User Verification. The mechanism ensures the endpoint belongs to a person who is also an authorized user in the same organization for secure and expedited access into meetings. An additional mechanism is provided to notify meeting hosts for users trying to enter the meeting where they do not meet the security policies. Further, the mechanism allows a host to determine whether to accept or reject users.