March 2021

FRICTIONLESS ONBOARDING FOR END-TO-END ENCRYPTED COLLABORATIVE SYSTEMS

Uday Srinath

Nikhil Kapre

Qingwen Cheng

Nick Wooler

FRICTIONLESS ONBOARDING FOR END-TO-END ENCRYPTED COLLABORATIVE SYSTEMS

AUTHORS:
Uday Srinath
Nikhil Kapre
Qingwen Cheng
Nick Wooler

ABSTRACT

Many current systems require a user account to access system features or allow a guest mode to skip account creation. In collaboration software that includes a guest mode, there are two features that are currently supported: (1) Joining a meeting via a guest mode, and (2) Guest mode for an entire application using an anonymous token, which is a token for a particular session only and needs another guest session on re-entry; the guest session is not persisted on retry. As a result, it is critical to solve the problem of onboarding allowing users to enter the system easily in a "Try Now" or "Guest Mode" that provides a full-feature rich experience that a user would get if the user had signed-up for an account. The problem is even more challenging for collaboration software that utilizes end-to-end encryption. This proposal provides techniques to leverage the existing Open Authorization (OAuth) flow by deferring email verification and password creation to reduce the time involved to join a guest session in an end-to-end collaborative system. By utilizing techniques of this proposal, a persistent guest session can be facilitated on a given client device and a clear path can be provided to upgrade to a full free and/or paid account.

DETAILED DESCRIPTION

As noted, many current systems require a user account to access system features or allow a guest mode to skip account creation. One issue with account creation is that it typically involves additional steps. An additional issue is that many times a user is not sure about coming back to the system in the future and, thus, may not be ready for an upfront commitment. On some occasions, a guest mode account is not a fully-featured version of a system and only exposes a subset of the features, which may be inconvenient as the user does not get to test drive the entire system with all the bells and whistles.

This proposal overcomes these issues by facilitating frictionless onboarding for end-to-end encrypted collaborative systems. Figure 1, below, is an example flow diagram that illustrates features for frictionless onboarding that may be facilitated by this proposal.

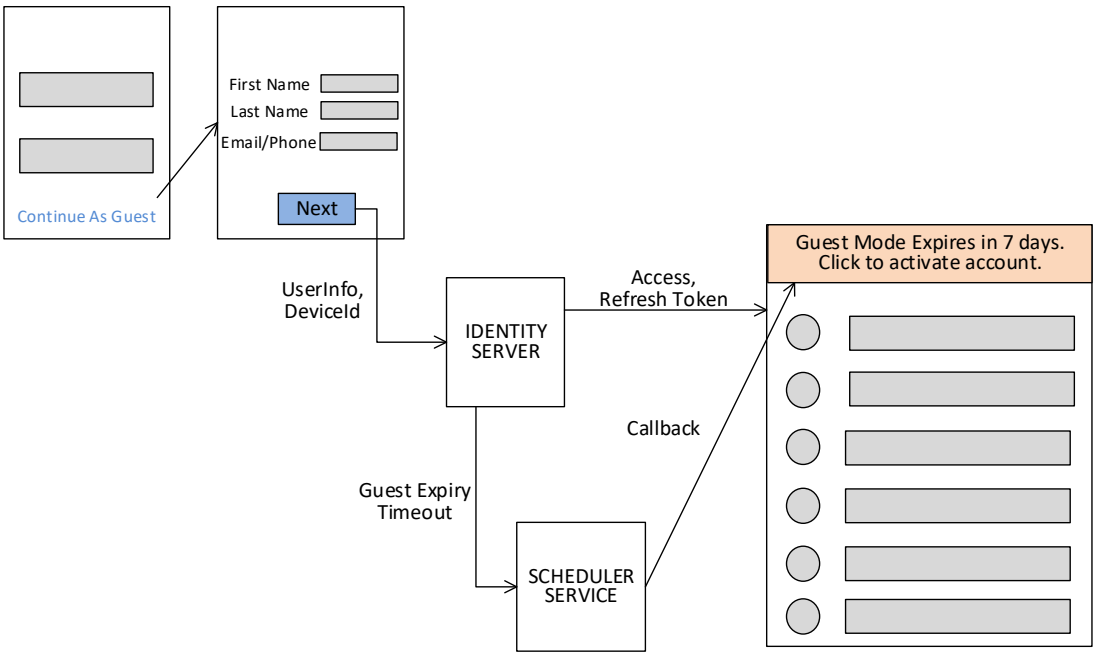

Figure 1: Frictionless Onboarding Flow Diagram for Guest Mode

As illustrated in Figure 1, consider that when a user attempts to access a collaboration system, there is an option for the user to select a "Continue As Guest" or a "Try Now" button or clickable text on the user interface, which is the entry point to start the guest mode or frictionless onboarding. Upon selecting the "Continue As a Guest" or "Try Now" option, the user can be directed to enter various user information (UserInfo), such as the user's First Name, Last Name (which may be required), and (optionally) email/phone number.

If an email is provided, an activation code can be sent to the email once the guest mode window expires. The activation code is to be utilized to convert the guest mode account to a full user account. If an email is not provided, a unique/anonymous email is generated for the user that is a random universally unique identifier (UUID), for example, 'e28766d4-3223-4d78-b0fc-519a8e9058ed@webex.com'. When the guest mode expires,

an email/phone number is requested from the user to send the activation code as a part of the guest mode to the full user account conversion.

In addition to user information, device identification (DeviceId) information is also captured for the user's device. In various instances, a DeviceId may include a Media Access Control (MAC) address for a desktop computer or other hardware, an International Mobile Equipment Identity (IMEI) for a mobile phone, and/or the like. The DeviceId for the user's device is critical to synchronize the same guest account for the user if the user initiates another session with the system utilizing the same device. This helps to ensure that users have one guest mode session from one device, with a clear path for account conversion.

As illustrated in Figure 1, the UserInfo and DeviceId is sent to an identity server, which generates an access/refresh token using a machine-on-behalf-of account. To further strengthen security the refresh token, expiry can be capped to the guest mode time window. Further as illustrated in Figure 1, the identity server writes the guest expiry time window to a scheduler service. The scheduler service can initiate callbacks every upon expiry of the guest mode time window (e.g., every 24-hours, etc.).

The guest mode expiry will be clearly indicated on a banner as a part of the user interface (via the scheduler service) and tapping the banner will allow the guest mode to the full user account conversion.

Once the guest mode window expires (via the scheduler service), a blocking user interface can be provided that exercises the guest mode to full user account conversion, depending on whether an email was or was not provided during initialization of the guest mode. In some instances, the guest to full user account conversion process can also be an entry point for a first paywall that allows users to upgrade a guest account to a paid account along with the free account conversion, if desired.

Once the account conversion from the guest mode to a full user account occurs, the identity server generates an access/refresh token using the user credentials via the OAuth flow. In some instance, for added security, the administrator can manage guest users and revoke tokens for guest users in case of issues (e.g., exercising a switch flip to revoke tokens).

Accordingly, techniques of this proposal leverage the existing OAuth flow by deferring email verification and password creation to reduce the time involved to join a guest session in an end-to-end collaborative system. Further, a persistent guest session can be facilitated on a given client device and a clear path can be provided to upgrade to a full free and/or paid account. Although techniques herein are discussed with reference to collaboration systems, other implementations may be realized, such as for use with webinars, enticing users with free content, and/or the like.