Multi-Source SAML Authentication with WebEx

Overview

The approach recommended by Cisco for large institutions for authentication into the WebEx website is by using an institution-wide directory service via SAML 2.0. With this method, the institution uses a directory service (Active Directory, eDirectory, OID, OpenLDAP, etc.) which either supports SAML itself (such as the ADFS module within Active Directory) or which is connected to an external SAML Identity Provider (Okta, PingFederate, Shibboleth, SimpleSAMLphp, etc.) using LDAP to bind WebEx's authentication to their own.

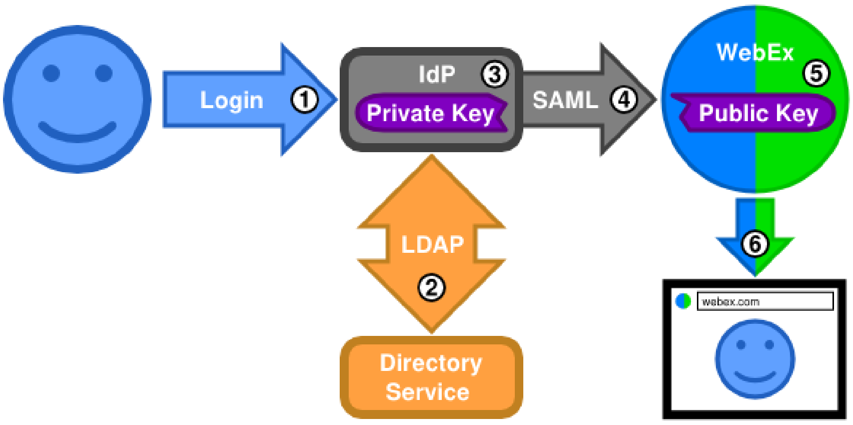
Once a user's browser is authenticated with the institution's portal via their Directory Service or Identity Provider (IdP), they can be automatically signed into all systems which federate with it and support Single sign-on (SSO).

When CirQlive MEETS is being used for integrating an institution's Learning Management System (LMS) with WebEx, and this is the only method by which a connection to WebEx will be created, the process is similar. MEETS has its own IdP which is capable of signing Security Assertions to authenticate itself with WebEx's APIs on behalf of users, which can be done once a private and public key pair have been generated and entered into MEETS and WebEx, respectively.

When it comes to institutions using both their own directory service or IdP **as well as** CirQlive MEETS, this process becomes slightly more complex, as there are now two separate pathways which both need the ability to log into WebEx. Unfortunately, WebEx was designed to only expect a single source of federated authentication and consequently only allows for a single authentication key for such. Due to this limitation, it is necessary for all platforms authenticating to WebEx to do so using the same set of authentication keys.

This document will outline the method by which each system connects to WebEx when in use without the other, followed by various solutions for correlating multiple systems so that they are all capable of effectively connecting to WebEx without conflicting amongst themselves, as well as describing some security best-practices when doing so.

Authentication Architecture of Directory Service with IdP



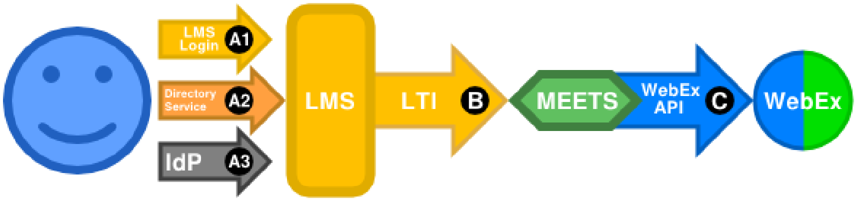
Authentication from a directory service directly into WebEx works as follows:

1. A user logs in to the SAML Identity Provider (IdP).
2. The IdP verifies the user's credentials by querying the Directory Service via LDAP.
3. Once the user's credentials have been verified, the IdP signs a Security Assertion using a Private Key.
4. The assertion is sent using the SAML communication protocol (by way of the user's browser) to the Service Provider (SP), in this case, WebEx.
5. The SP validates the signed Security Assertion against the Public Key it has stored which corresponds to the Private Key which was used by the IdP to sign it. (This Public Key will have been previously loaded into the SP during its configuration and is usually embedded within an X.509 Certificate.) The correlation of these two keys is the foundation of SAML's method for secure authentication.
6. The user is now authenticated and the WebEx site appears in the user's browser.

Multiple SPs may be connected to the same IdP, allowing users to use a single set of credentials everywhere.

Authentication Architecture of MEETS

Architecture Overview



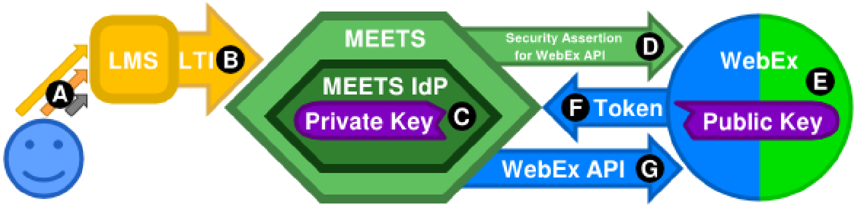
A. Depending on how it is set up, the LMS's user authentication may be:
   1. Internal to the LMS itself
   2. Utilizing the institution's Directory Service
   3. Via an IdP.

   As the distinction of which particular method is not relevant to the focus in this document of how the LMS connects to MEETS nor to how WebEx is accessed, this will be treated as a single "the user logs in to the LMS" step for the remainder of this document.

B. The LMS's connection to the CirQlive MEETS integration platform is federated via the LTI protocol. An important note is that even though users may be authenticating with the **LMS** via an SSO technology, the **LTI protocol** does not itself make use of SSO when connecting to additional services, and therefore the SSO information is not passed on to MEETS. The information it does pass on is:
   - The user's first and last name
   - The user's email address
   - The name of the course
   - The role within the course which the user plays (such as teacher/student)
   - LMS-specific internal IDs for the user and course which **do not** correlate to directory IDs, human-readable course numbers, or any other IDs that may exist anywhere else

C. MEETS communicates with WebEx services via the WebEx APIs.

MEETS Authentication to WebEx using Security Assertions



One of MEETS's operating models includes the ability for it to authenticate itself to WebEx on behalf of the user using Security Assertions. (Other modes are discussed in their respective pieces of documentation and are not relevant to the present discussion.) This mode works as follows:

A. The user uses one of the methods described above to log into the LMS

B. As described above, the LMS authenticates the user to MEETS using the LTI protocol, and sends along the user's email address as part of its information.

C. MEETS informs its own built-in Identity Provider (IdP) of the need to authenticate itself to WebEx on behalf of the user (using the user's email address either directly or for an ID lookup). The MEETS IdP signs a Security Assertion using a Private Key.

D. MEETS sends the signed Security Assertion directly to WebEx.

E. WebEx validates the signed Security Assertion against the Public Key it has stored which corresponds to the Private Key which was used by the MEETS IdP to sign it. Note that WebEx makes use of the Security Assertions in a **non-standard** manner for this authentication step and does not make use of any other SAML-related specifications beyond this step, as WebEx's APIs **do not** use the complete SAML 2.0 protocol for federated authentication and identity management; They offer their own communication protocol instead.

F. WebEx sends back a login token to be used for the actual API communication.

G. MEETS then has access to continue communication with WebEx on behalf of the user via its APIs.

Note that rather than authenticating the user themselves, this process authenticates the **MEETS platform** to perform API functions **on behalf** of the user.

Setup and Best Practice

A Private and Public Key Pair will need to be generated for MEETS to use with WebEx, the former of which must be loaded into MEETS along with some ID information, and the latter of which is required by WebEx to be embedded within an X.509 Certificate and then loaded into it along with the same ID information.

It is important to note that since the user is authenticated based on their email address (directly or indirectly), the email address used for a particular user in the LMS must match the one which is used within WebEx for the same user. In the same vein, it is also important to note that in order to be secure and to prevent users from impersonating each other, the LMS must be configured to either require confirmation or verification of ownership when users change their email addresses, or else disallow users from modifying their own email addresses entirely.

Authentication Architecture for Multiple Concurrent Systems

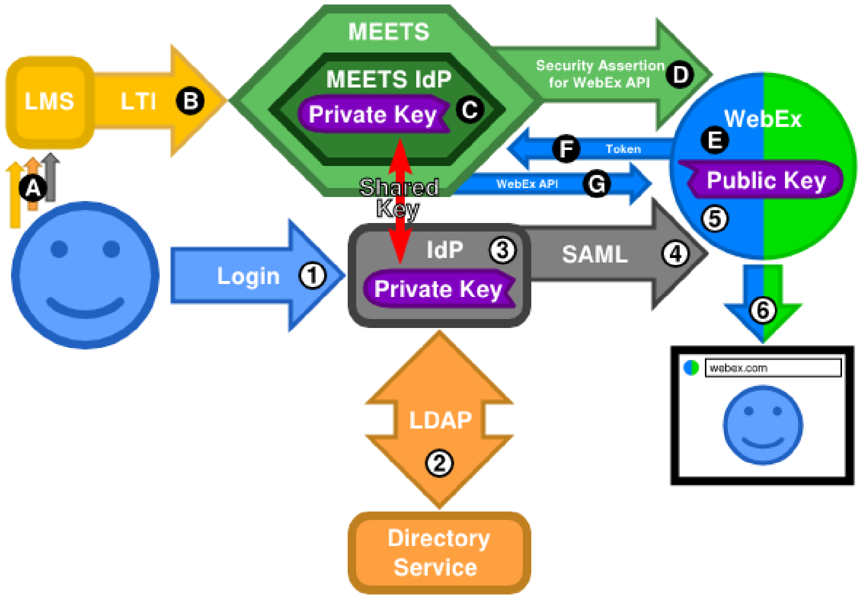
As mentioned above, WebEx was designed to only expect a single source of federated authentication and consequently only allows for a single set of authentication keys. As such, all systems authenticating to WebEx must use the same private key, even if they are otherwise not connected to each other.

CirQlive recommends one of the following three architectures to allow the institution's IdP (or IdPs) to authenticate to WebEx alongside and concurrently with the MEETS IdP.

Architecture #1: Parallel Pathways with a Shared Private Key

This architecture is the most popular one and simplest to set up. It functions by simply using the same key pair for both IdPs.

This architecture is generally recommended for institutions that host their own IdP(s) on-prem or can otherwise manage and access their own Private Keys.



MEETS authentication is done as follows:

A. As above, the user logs into the LMS using whatever method is configured.
B. As above, the LMS federates its connection to MEETS using LTI
C. As above, the MEETS IdP signs an assertion with a Private Key. From the IdP's perspective, this is no different from ordinary usage. The only item of note is that the ownership of the Private Key being used is shared equally between both parallel IdPs being used (the institution's IdP and this one).
D. As above, MEETS sends the assertion directly to WebEx.
E. As above, WebEx uses the assertion in a non-standard manner and verifies the assertion against the corresponding Public Key.
F. As above, WebEx sends back a login token to be used for the API communication.
G. As above, MEETS uses that login token to continue its communication with WebEx via its APIs.

Directory service authentication is done as follows:

1. As above, the user logs in to the institution's IdP.
2. As above, the IdP verifies the user's credentials by querying the Directory Service via LDAP.
3. As above, the institution's IdP signs an assertion with a Private Key. From the IdP's perspective, this is no different from ordinary usage. The only item of note is that the ownership of the Private Key being used is shared equally between both parallel IdPs being used (MEETS IdP and this one).
4. As above, the IdP uses the SAML communication protocol to send the assertion to WebEx via the user's browser.
5. As above, WebEx validates the assertion against the corresponding Public Key.
6. As above, the user is now authenticated and the WebEx site appears in the user's browser.

Setup and Best Practice

The setup for this architecture is to simply ensure that the same Private Key is present in both the MEETS IdP and the institution's IdP, and that the Public Key which corresponds to it is the one which has been uploaded to WebEx. In addition, there are a few other pieces of identifying information which must match in all three places (MEETS IdP, institution's IdP, and WebEx itself). The exact setup is described more fully in the MEETS SAML Administration Manual.

It is important to note that SAML is built upon XML Security's XML Signature which is notorious for having a large attack surface, which in turn affects SAML [1] [2] [3] [4]. Therefore, in order to minimize possible attacks, an IdP should be using a separate key pair for each Service Provider (SP) which differs from the key pairs used for every other SP. This is especially true when there are multiple IdPs which are intended to share access between some SPs but not others.

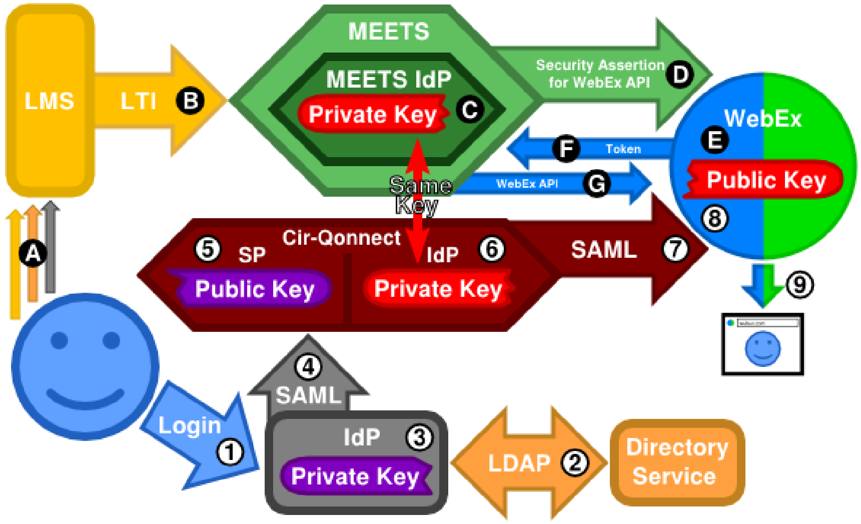
In this specific case, ideally, if the institution is not already using the aforementioned security recommendation, a distinct key pair should be generated for use only with WebEx, in order to provide MEETS access solely to WebEx services without potentially exposing access to other services which are not required. This is analogous to the real-world example of not using the same key for your house as you do for your car, office, and gym locker. While it may sound convenient to have one key for everything, you wouldn't want to trust your mechanic with the key to your house every time you brought your car in for a repair. You wouldn't want your visiting in-laws to be able to show up at your office just because they have a copy of your house key. And if you ever lost a key somewhere, you wouldn't want whoever found it to gain access to everything you own all at once.

If WebEx is the only SP of which the institution is making use, then the above paragraph does not apply, as there are no extra security considerations to account for. Keep in mind, however, that if any other services are added down the line, they should have unique keys generated for them as they are added, rather than re-using the one already in use for WebEx.

Architecture #2: Using CirQlive's Cir-Qonnect IdP as a Relay

This architecture allows an institution's existing IdP to use an existing key pair while avoiding the need to share a Private Key with CirQlive's systems. This is accomplished by using CirQlive's IdP, Cir-Qonnect, as an authentication relay rather than as an authentication originator.

This architecture is generally recommended if an institution is not able to manage their private keys directly, which is typical when using a hosted IdP service. However, when managing an IdP locally, the institution usually has full control over the keys they work with and is usually better off with the first architecture (along with its best practices).



MEETS authentication is done as follows:

A. As above, the user logs into the LMS using whatever method is configured.
B. As above, the LMS federates its connection to MEETS using LTI
C. Since the Private Key used for WebEx is within CirQlive's own system, MEETS has access to the same Private Key as is being used in Cir-Qonnect, which it uses to sign an assertion.
D. As above, MEETS sends the assertion directly to WebEx.
E. As above, WebEx uses the assertion in a non-standard manner and verifies the assertion against the corresponding Public Key.
F. As above, WebEx sends back a login token to be used for the API communication.
G. As above, MEETS uses that login token to continue its communication with WebEx via its APIs.

Directory service authentication is done as follows:

1. As above, the user logs in to the institution's IdP.
2. As above, the IdP verifies the user's credentials by querying the Directory Service via LDAP.
3. As above, the institution's IdP signs an assertion with a Private Key.
4. Rather than communicating with WebEx as the SP, the IdP uses SAML communication to send the assertion via the user's browser to the **Cir-Qonnect** SP instead.
5. The Cir-Qonnect SP uses the corresponding Public Key from the institution's IdP to validate the assertion, and passes it on internally to the Cir-Qonnect **IdP**.
6. The Cir-Qonnect IdP generates a second assertion with the exact same user data and signs it using a Private Key of **its own**.
7. The Cir-Qonnect IdP uses SAML communication via the user's browser to send its assertion to WebEx.
8. WebEx validates the signed assertion against **Cir-Qonnect**'s corresponding Public Key.
9. The user is now authenticated and the WebEx site appears in the user's browser.

From the user's perspective, the experience is nearly identical to having the institution's IdP forward them directly to WebEx; The user logs in to the institution's IdP as usual, and gets pushed into the WebEx website. All user data is passed on exactly as received, so any special SAML attributes being used with WebEx will be passed along as expected. The only visible difference that users might notice is that, due to the fact that the backend routing between the login portal and WebEx now has one additional step in the middle, the URL in their browser will change an extra time as it passes the data through the relay, but even this is fully automatic and lasts only a second or two in most cases.

Setup and Best Practice

Setting up this architecture requires four parts:

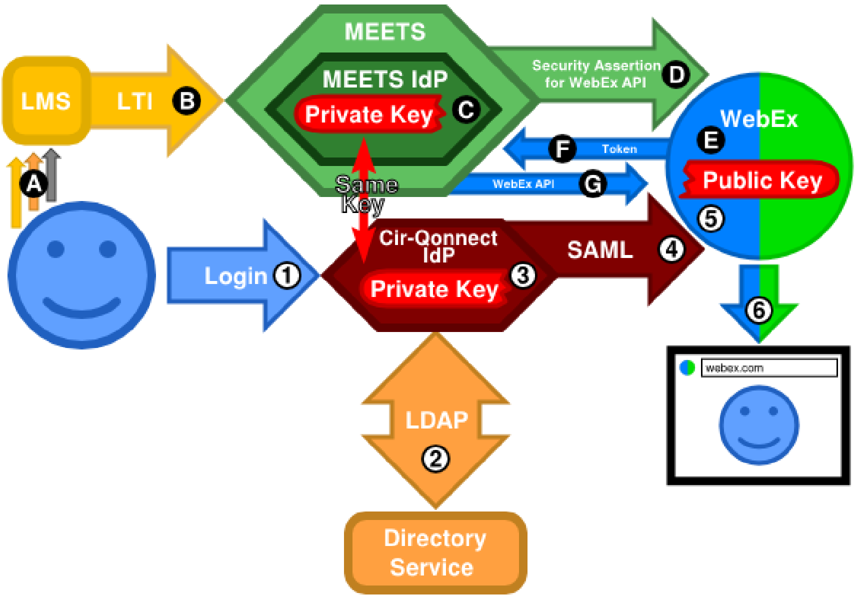
1. The institution's IdP: This is a standard IdP setup, and if a setup already exists for WebEx, it can simply be modified by changing the SP ID and URL from those of WebEx to the ones belonging to Cir-Qonnect.
2. Cir-Qonnect: This is a standard SP setup requiring the institute's IdP ID as well as the Public Key which corresponds to the Private Key used by the IdP for this connection.
3. WebEx: The corresponding Cir-Qonnect Public Key as well as the proper ID information need to be loaded into the WebEx SSO configuration.
4. MEETS IdP: MEETS will need to be configured to use the same Private Key and ID information as Cir-Qonnect.

As in the first architecture, it is best to use a separate key pair for each service being connected to from the institution's IdP.

Architecture #3: Using CirQlive's Cir-Qonnect IdP as the primary IdP

This architecture uses Cir-Qonnect itself as the institution's primary IdP, cutting out the middleman. This approach is very similar to the first architecture, although requires less hassle as the Private Keys are internal to CirQlive's systems and can therefore be accessed by both automatically rather than needing to be manually shared across two separate systems.

This architecture is generally recommended if an institution does not already have an IdP set up to connect to WebEx, and would like to achieve Singular Authentication with the LMS integration as well as still allowing users to access WebEx directly.



MEETS authentication is done as follows:

A. As above, the user logs into the LMS using whatever method is configured.
B. As above, the LMS federates its connection to MEETS using LTI
C. Since the Private Key used for WebEx is within CirQlive's own system, MEETS has access to the same Private Key as is being used by Cir-Qonnect, which it uses to sign an assertion.
D. As above, MEETS sends the assertion to WebEx.
E. As above, WebEx uses the assertion in a non-standard manner and verifies the assertion against the corresponding Public Key.
F. As above, WebEx sends back a login token to be used for the API communication.
G. As above, MEETS uses that login token to continue its communication with WebEx via its APIs.

Directory service authentication is done as follows:

1. As with any SAML IdP, a user logs in to the Cir-Qonnect IdP.
2. As with any SAML IdP, the Cir-Qonnect IdP verifies the user's credentials by querying the Directory Service via LDAP.
3. Since the Private Key used for WebEx is within CirQlive's own system, Cir-Qonnect has access to the same Private Key as is being used by MEETS, which it uses to sign an assertion.
4. As with a traditional IdP setup, Cir-Qonnect uses SAML communication to send the assertion to WebEx via the user's browser.
5. WebEx validates the signed assertion against the corresponding Public Key.
6. The user is now authenticated and the WebEx site appears in the user's browser.

Setup and Best Practice

1. As with any IdP, Cir-Qonnect needs to be configured to connect with the institution's directory service, and requires the directory service URL, distinguished name information, and the names of the important fields.
2. As with any IdP-SP relationship, WebEx will also need to be configured with the corresponding information.
3. MEETS will need to be configured to inform it that it should use the same Private Key and ID information as Cir-Qonnect.

Cir-Qonnect mandates certain best practices which are in many other IdPs only considered optional (for example, requiring separate keys for each Service Provider). As such, it ensures that your setup is adhering strictly to the relevant security precautions.

Auto Account Creation

Account Creation via SAML

WebEx has a feature which allows user accounts to be automatically created for users not previously seen by WebEx who are authenticating via SAML. When creating an account, WebEx requires an ID for the user (which, for example, may be taken from the directory service or IdP) as well as their email address. Which of these pieces of information WebEx uses to determine which user is which and whether they have an existing account depends on the Name ID option selected.

If the piece of information which WebEx uses for identification changes for a certain user, WebEx will will no longer be able to identify that user with their original WebEx account. WebEx will then proceed to create a new account for that user, as it now appears to WebEx as if they are someone else.

Account Creation via MEETS

MEETS has a feature which allows it to create user accounts automatically **as necessary for its own use**. MEETS does not have access to any IDs that are known by directory services or IdPs, nor any special permissions associated with the user beyond that which is provided by LTI for a particular course. Therefore, when auto-creating a WebEx account, MEETS will supply its own internal user IDs for that account which **will not correlate** to the IDs you may expect. Additionally, MEETS account creation is done via the user provisioning APIs **not** via the aforementioned SAML account creation, as WebEx's automatic SAML account creation does not take effect when authenticating a user via the API. As such, default settings for SAML auto-creation will not be applied to accounts created by MEETS.

Likewise, the SAML IdP (even in the case of Cir-Qonnect) does not have access to the user ID used by MEETS. It does, however, have access to the email address of the user.

As such, if you wish for the IdP to authenticate its users properly with WebEx accounts auto-created by MEETS, the Name ID option must be set to "Email Address". Please note that even when this recommendation is followed, accounts created by MEETS will still be using MEETS IDs and permission settings, rather than those of the IdP. The MEETS auto-creation feature is largely designed for cases where the users' only access to WebEx is through the LMS. If users will have the ability to access both through MEETS and through an IdP, it is recommended that MEETS's auto-creation be turned off to avoid conflicts or incorrect IDs or permissions.

It is important to note that as MEETS itself utilizes the WebEx APIs and is able to identify a user's account based on their email address regardless of which Name ID is set to be used, MEETS can therefore work with any account created by the IdP, even if it is using a user ID which is unknown to MEETS. This is true even in the case of using Cir-Qonnect, either as the primary IdP, or as a relay, as MEETS does not have direct access to Cir-Qonnect itself, but only to the underlying authentication information.

In short, MEETS's auto-creation feature is designed to facilitate the narrow use-case required by MEETS itself. If broader use-cases are required, WebEx's SAML auto-creation via the IdP is a better choice.

Extra note

There are additional fees for using CirQlive's standalone IdP service in addition to the MEETS LMS integration (architectures #2 and #3). These fees are to cover the additional cost of setting up the second platform, supporting it, and accommodating the additional usage outside of the LMS that comes along with it.