
cisco Live!
ALL IN

The bridge to possible

Authentication, Authorization and Provision

for Cisco Collaboration - Part 2

Paulo Jorge Correia
Principal Sales Architect
@paucorre

BRKCOL-2007b

Cisco Webex App

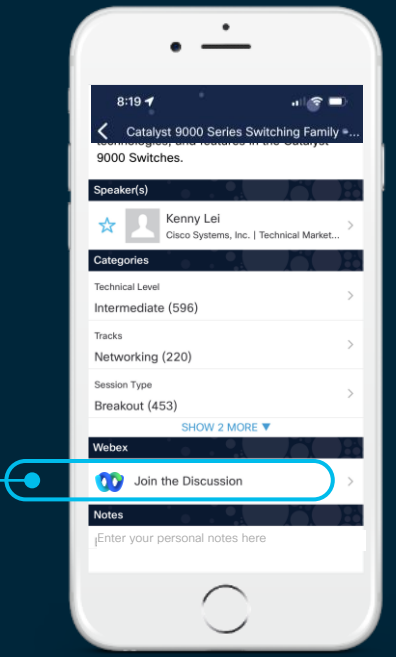
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.

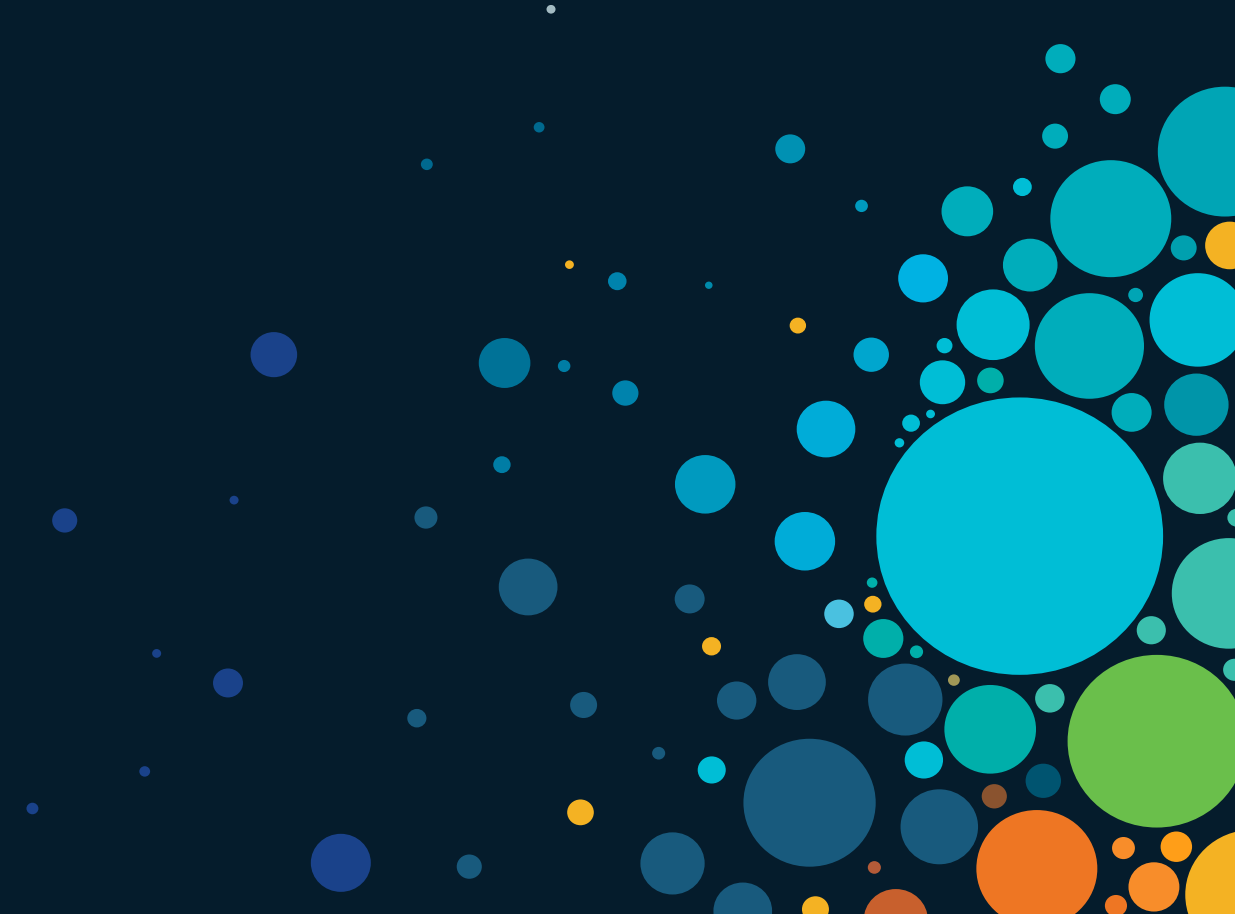


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2007b

Agenda

- Introduction
- Webex AuthN/AuthZ improvements
  - SSO Wizard and Certificate Management
  - Token Management
  - Password Management
- AuthN/AuthZ flows for the Webex App
- OpenID Connect and PKCE how does it work?
- Conclusions and Key Takeaways

Introduction



World's Biggest Data Breaches & Hacks

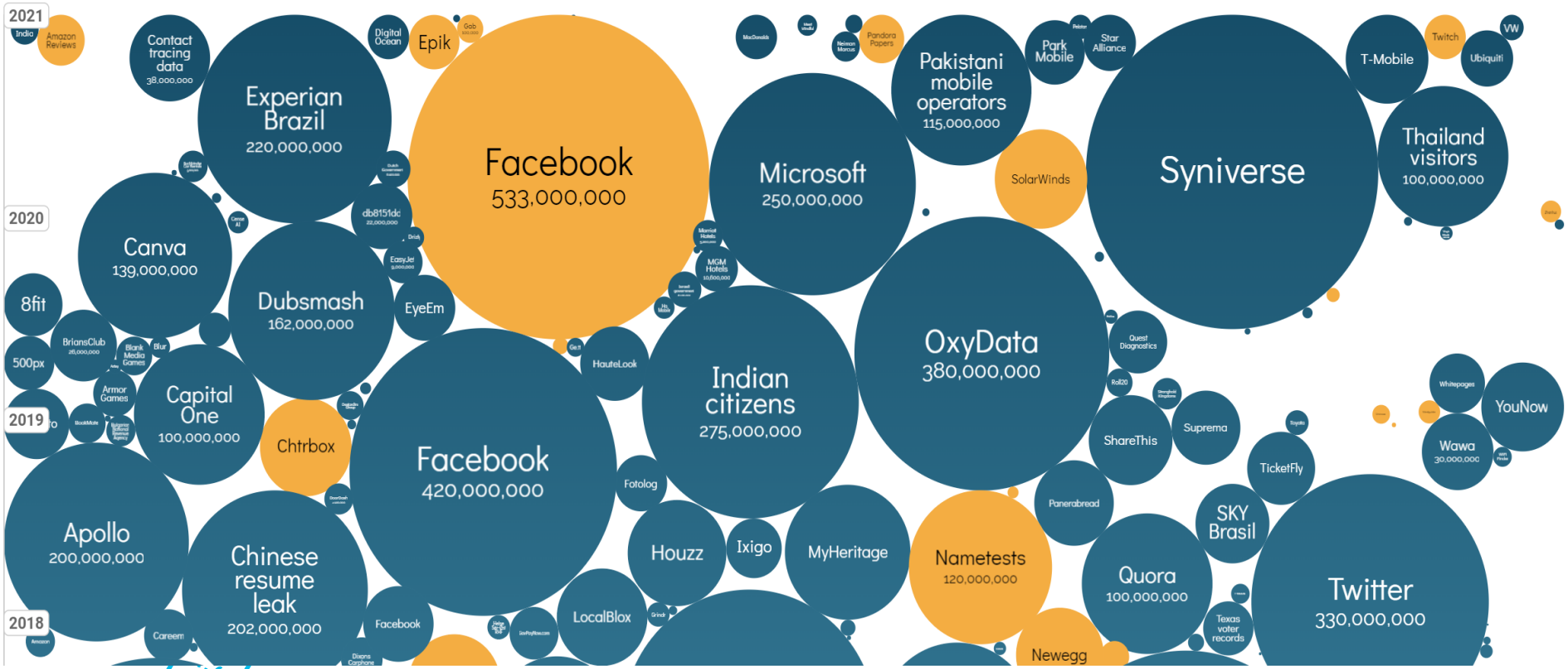
interesting story

Selected events over 30,000 records

UPDATED: Oct 2021

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

size: records lost **filter** search...



Cisco Identity Architecture for Collaboration

Customer IdM

Authentication

SSO with SAMLv2
SSO with OIDC
Local Auth

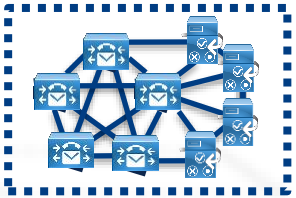
Provision

SCIM /
Manual /
API / LDAP
Directory Connector /
SAML JIT /
CUCM /
Account Linking

Collab Services

webex by CISCO

Identity Service



Collab Clients

Webex App

Jabber

Webex Devices

Contact Center

Which Protocols do we see in Identity Management

SAML Security Assertion Markup Language defined under OASIS Security Services Technical Committee (SSTC) Standards.

OAuth is an Authorization Framework defined by IETF under RFC 6749

SCIM System for Cross-domain Identity Management, 2.0 was release under IETF as RFC 7643 and 7644

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol.

Webex AuthN/AuthZ improvements

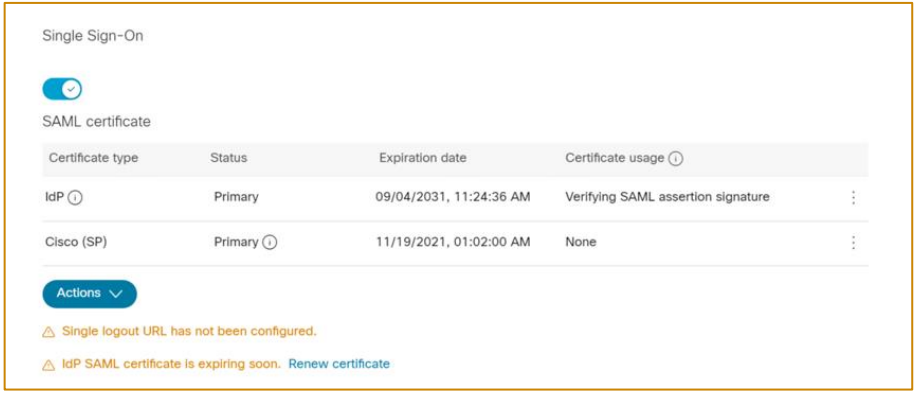
SSO Wizard and Certificate Management

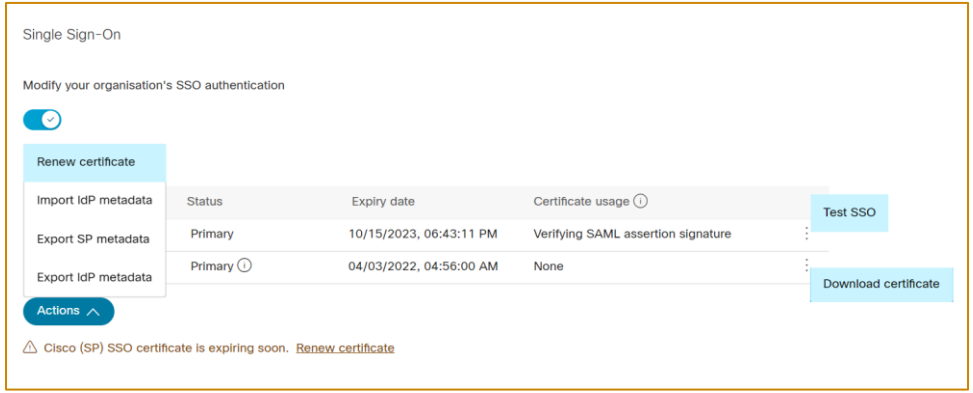
In the Organization Setting we can verify all the information on current agreements with:

- Dates
- Certificate usage
- Expiration notice
- SLO warning

It also allows to quickly change any SSO tasks:

- Turn On/Off
- Metadata manipulation
- Certificate Renew/Download
- Test SSO

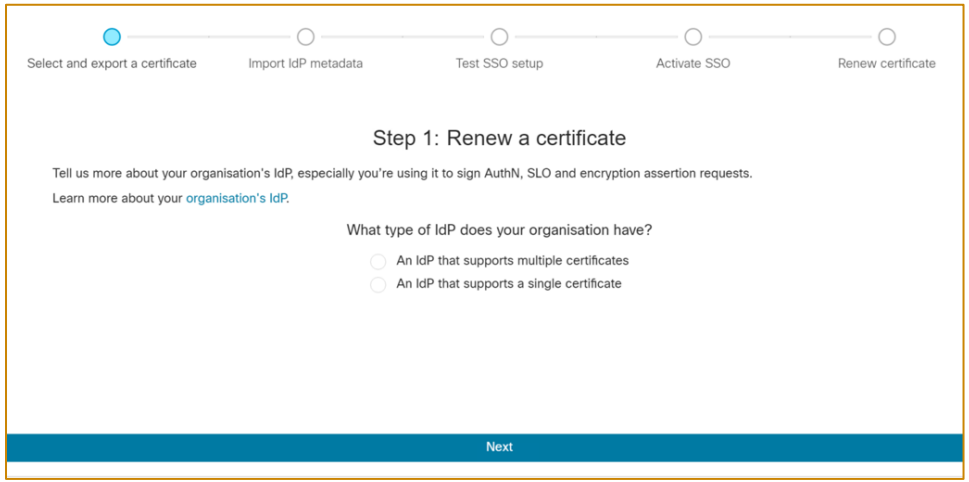




SSO Wizard and Certificate Management

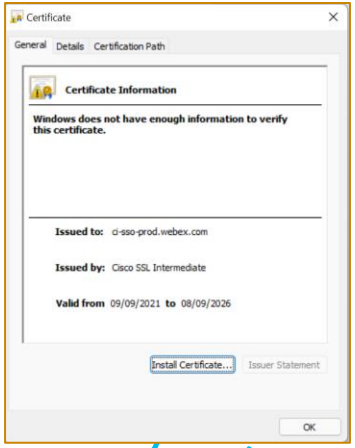
There are two possible flows that can be started by our customer:

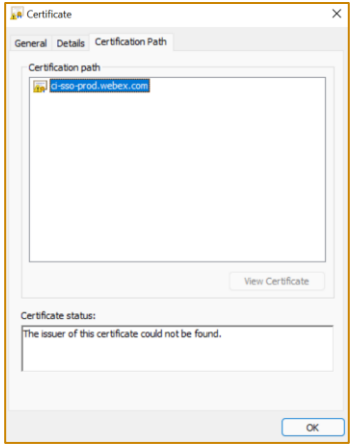
- Initial configuration
- SP and/or IdP certificate renewal

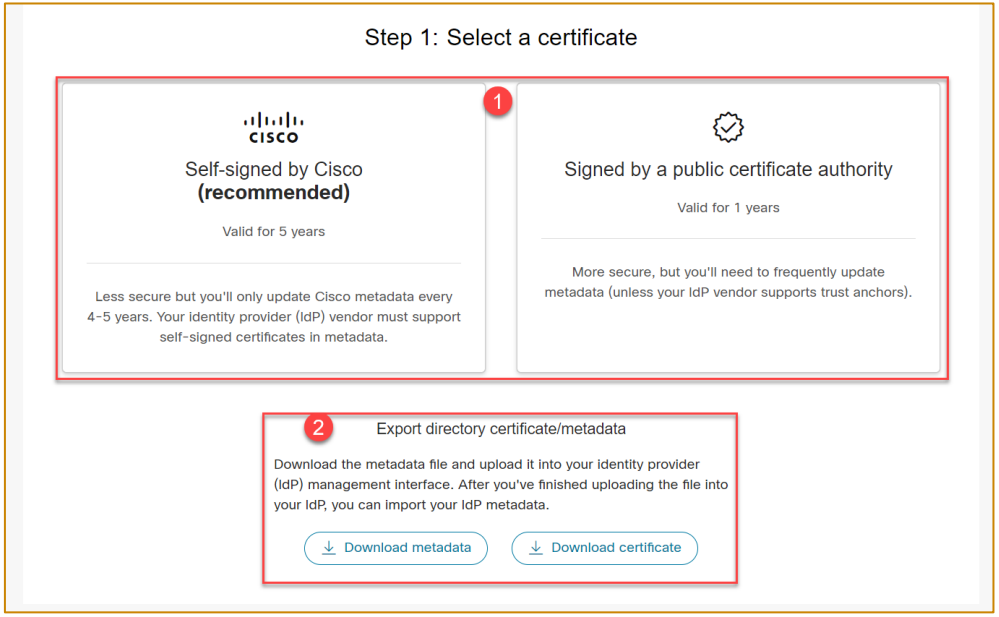


SSO Wizard and Certificate Management

- The certificate for SAML Signing and Encryption (we are not talking about communication cert) can be Self-signed or CA. Most of the SAML configurations use Self-signed, CA Signed isn't very important since most SAML implementations do strict certificate checking
- After choosing which kind of cert to use, you can provide to the IdP manager a Certificate or a Metadata file, depending on the IDP capabilities.
- The certificate is not generated when you run the wizard, it is created in specific time of the year

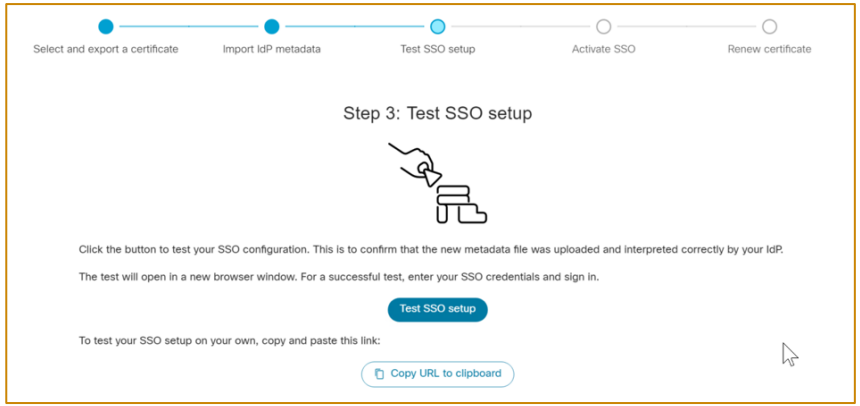


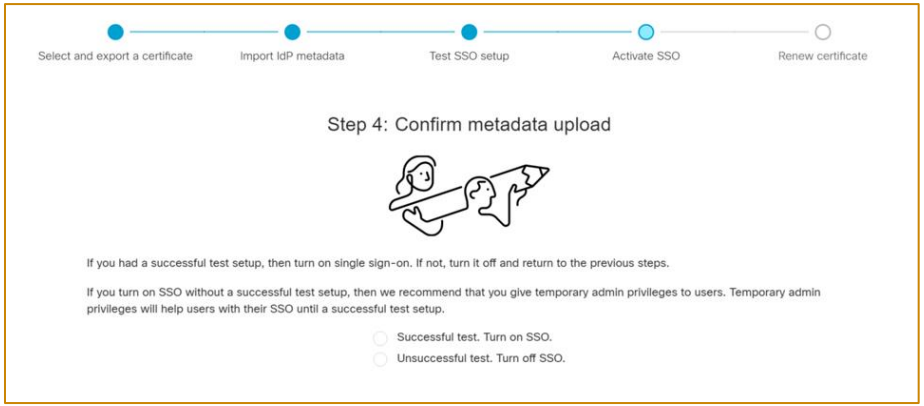




SSO Wizard and Certificate Management

- For the SSO test, it is recommended that you copy the URL and start a new browser in private mode, to avoid false positives because of previous cookies.
- The wizard doesn't go away if you don't provide indication if the test was Successful or Unsuccessful.

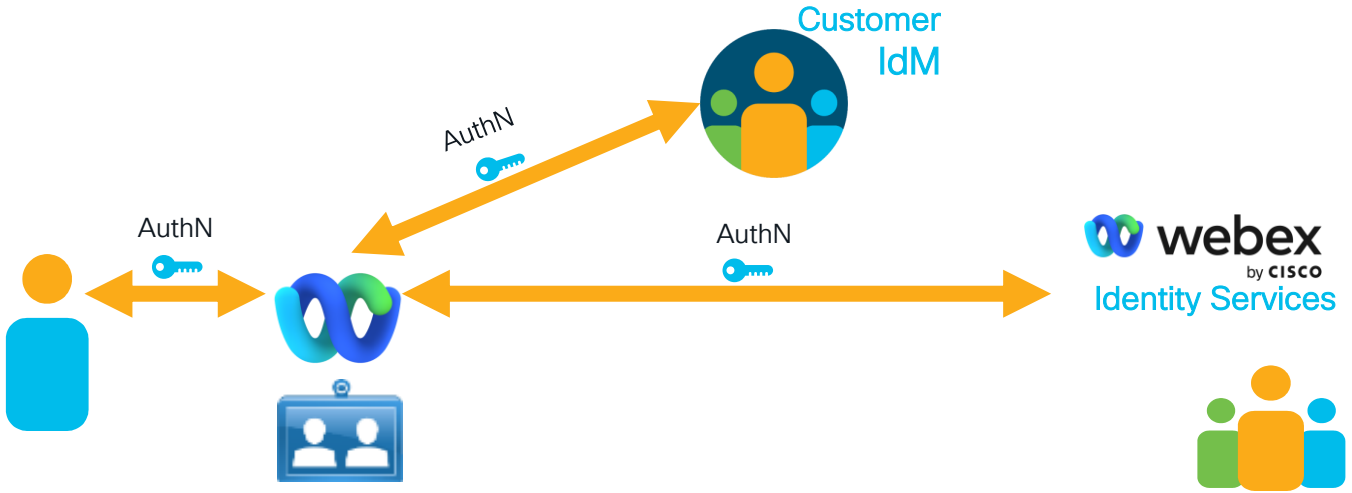




Token Management

What is the AuthN/AuthZ experience today ?

When the Client or Video Device first connects to the network

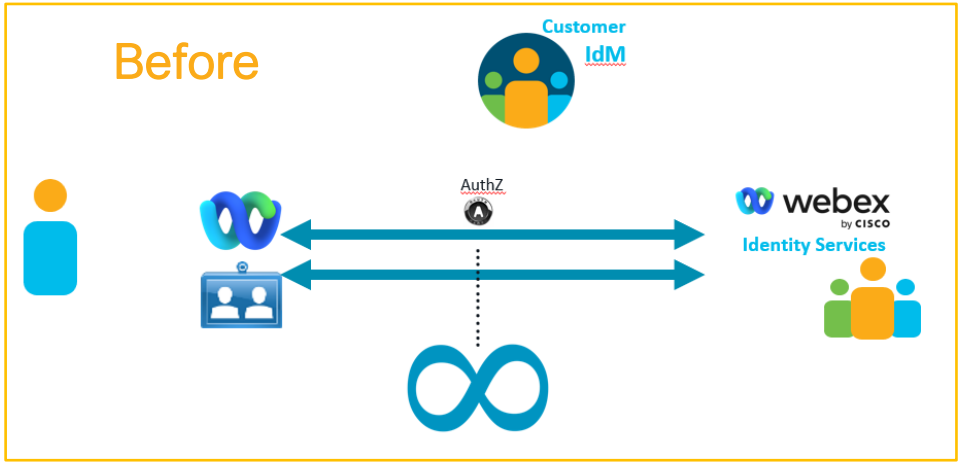


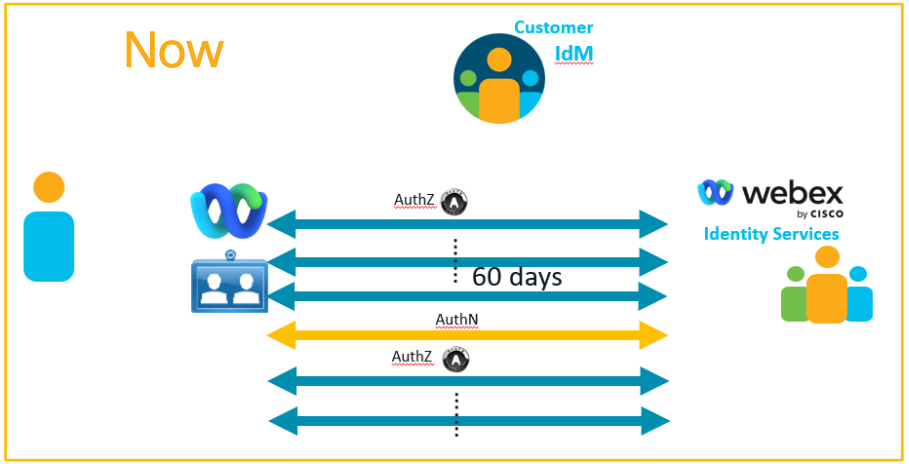
Token Management

What is the AuthN/AuthZ experience today ?

Every 12 hours the Client or Device refreshes the OAuth Access token (with the refresh token)

With the introduction of this feature, we adopt a new behavior where the Refresh tokens are not automatically extended when the client comes for another Access Token.





Token Management

What is the new AuthN/AuthZ experience?

IT Administrators **can customize** when the Users need to AuthN again.

This **requires IT Pro Pack**

iOS and Android SW Clients

Windows, MacOS and Web Clients

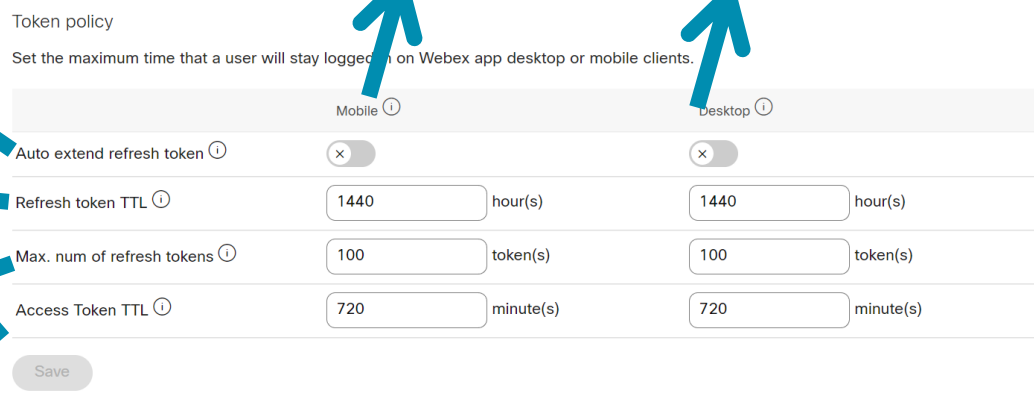
If enabled it has the same behavior as before, refresh tokens are automatically extended

How long refresh token lasts.

- If Auto Extend on – is the maximum duration that the client can be disconnected, before AuthN again, but might never need auth AuthN again.
- If Auto Extend Off – is when the Client need to AuthN again.

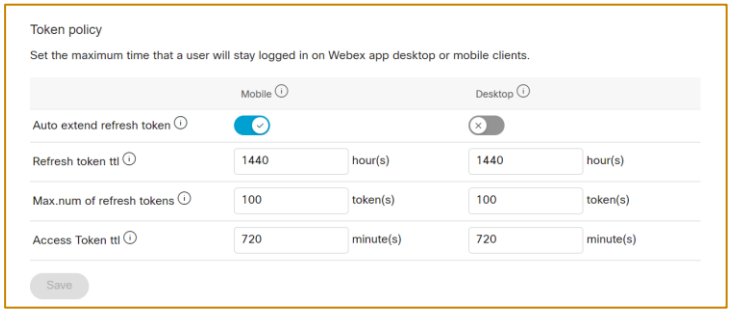
Maximum number of Clients that the User can have under their account

How long before getting another OAuth Access token



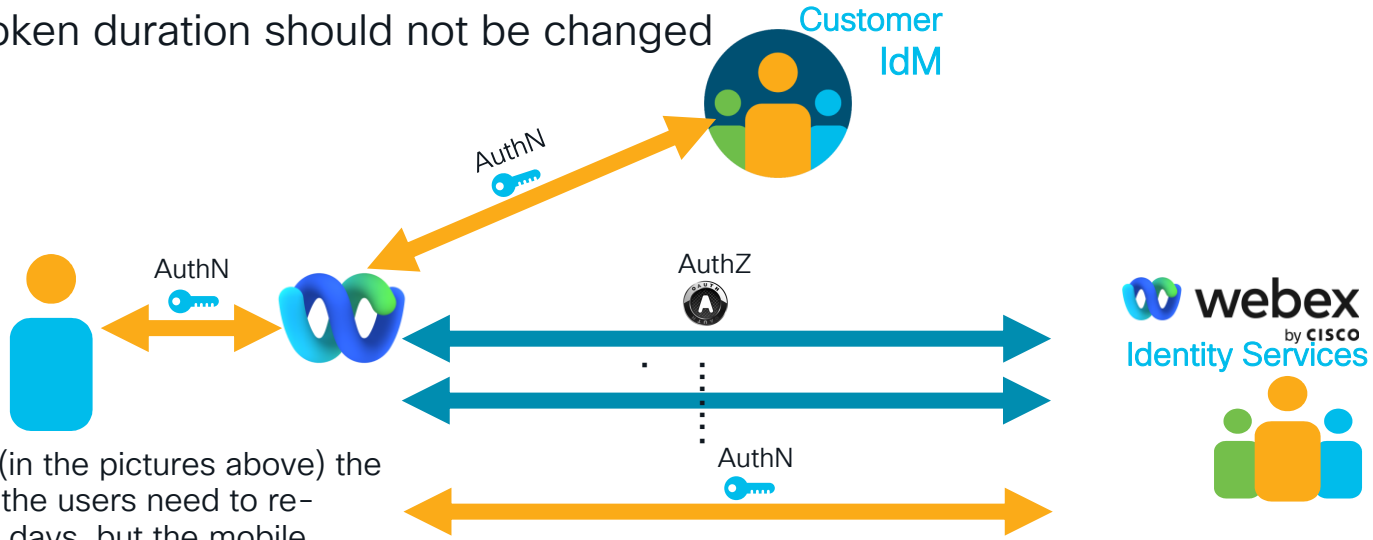
Token Management

What is the new AuthN/AuthZ experience?



Refresh Token lifetime must be between 24 and 1440 hours.

Access token duration should not be changed



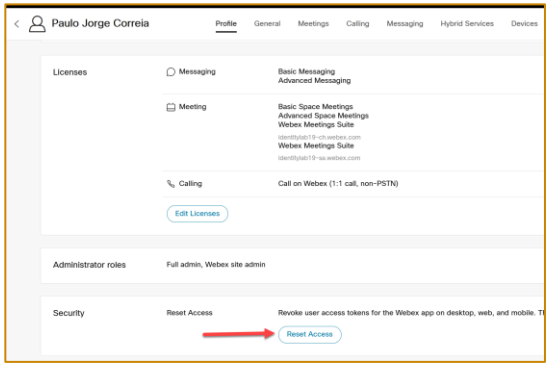
In our example (in the pictures above) the desktop clients the users need to re-AuthN every 60 days, but the mobile clients will never need to AuthN again

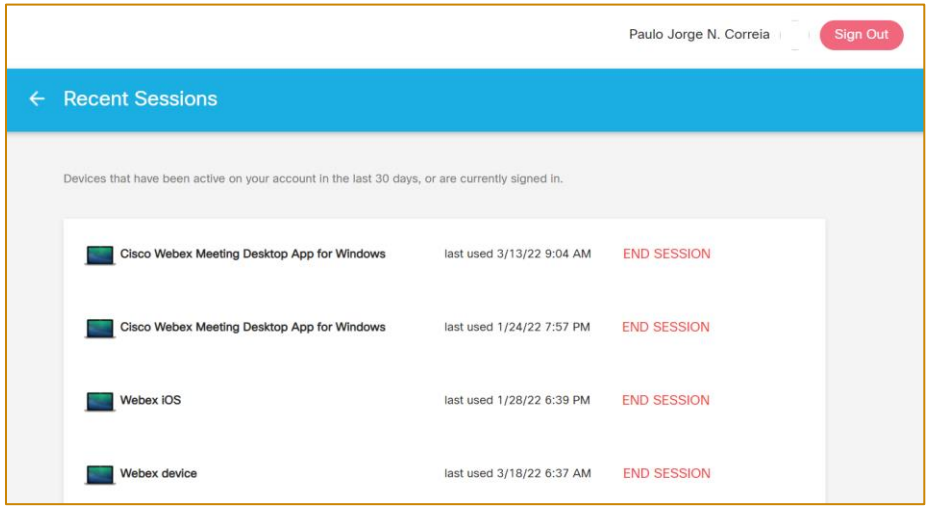
Token Management

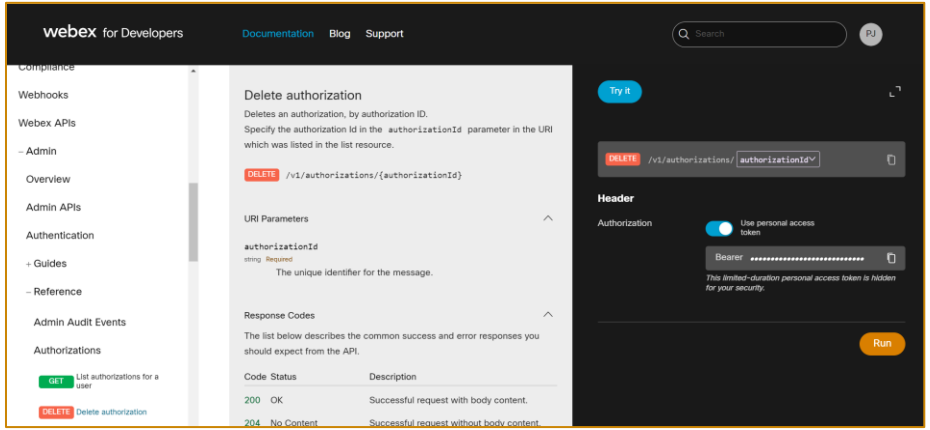
Revoke tokens

Tokens can be revoke in different ways :

- By Administration, via Control Hub
- By User or Integration in the behalf of the User via API's
- By user from the Webex App or Web Browser (https://idbroker.webex.com/idb/profile#/)



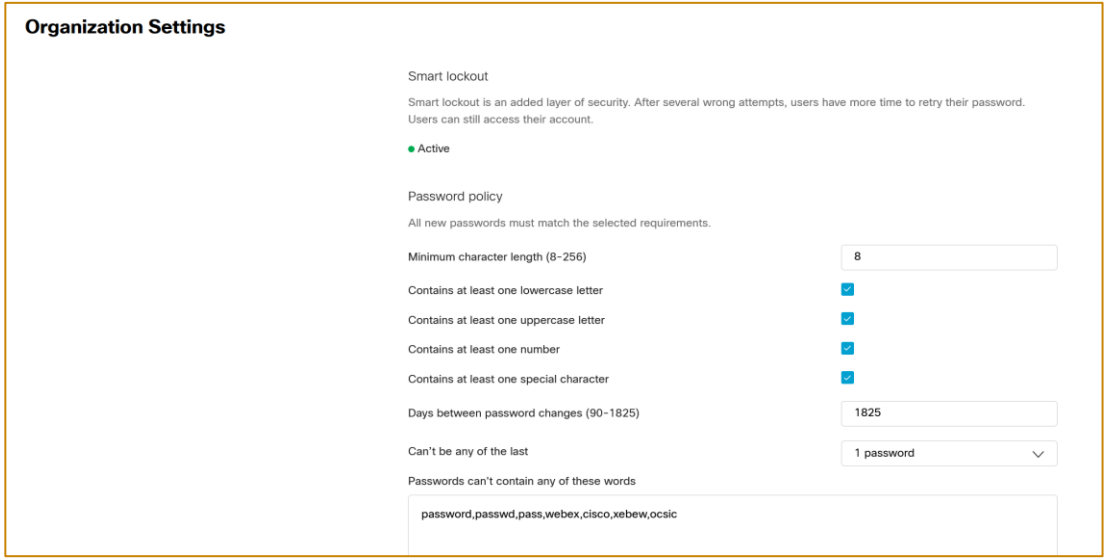




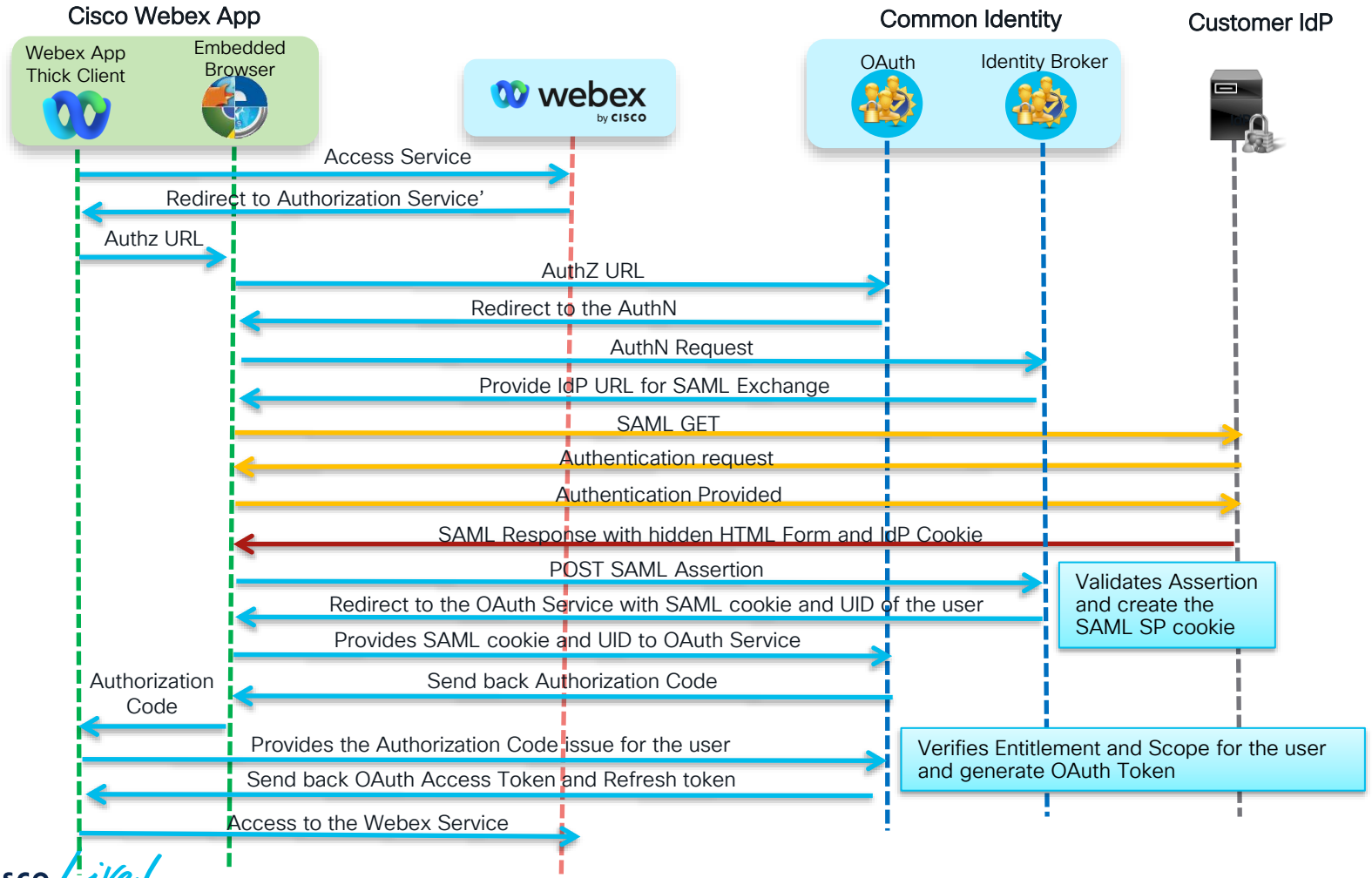
Password Management

Password policy can now be created in Webex Control Hub, where customers **can create their own password complexity**

We never lock any account, but increase the time between authentication requests, making it almost impossible to login when you fail the password many times.

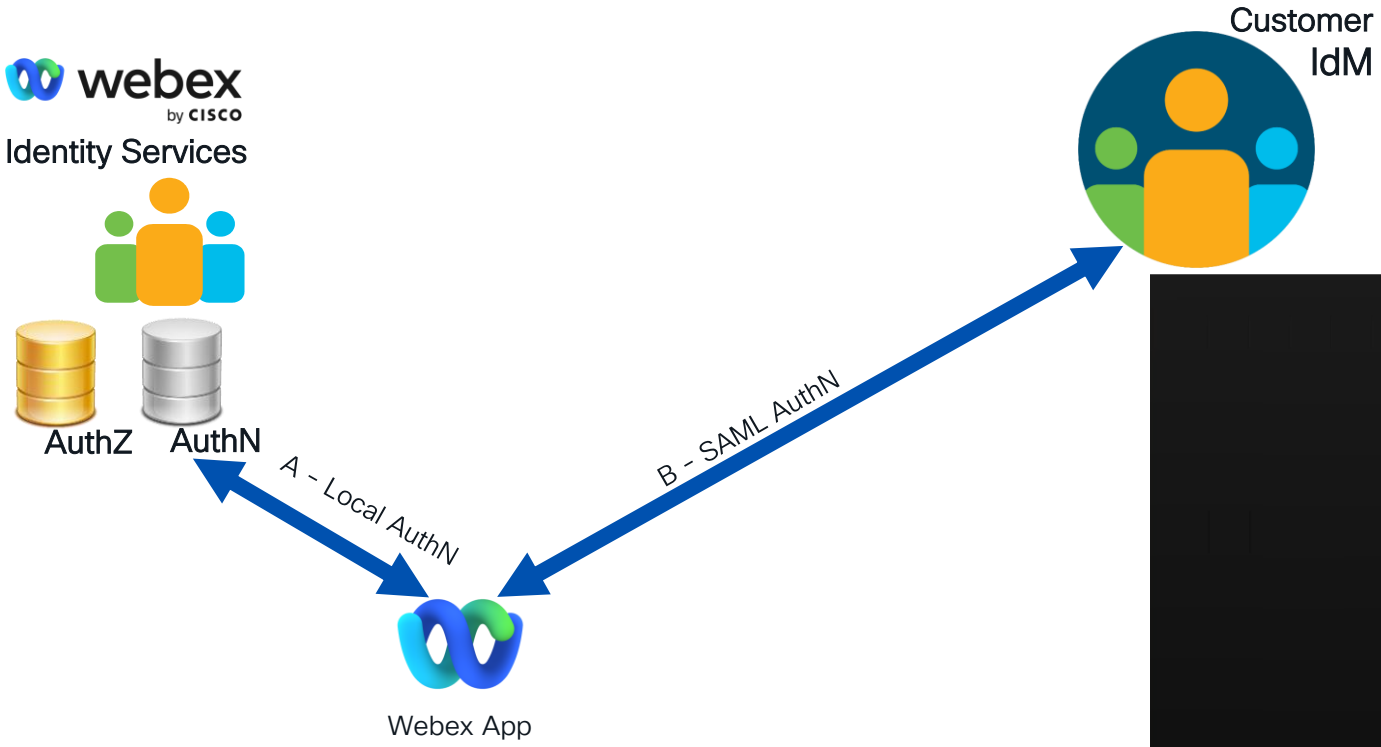


AuthN/AuthZ flows for the Webex App



Cisco Collaboration Applications

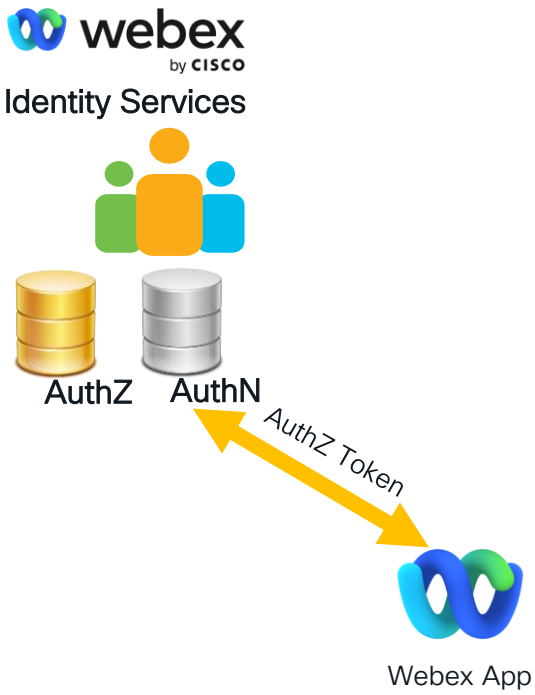
Cisco Webex app native services AuthN Flows



A | B - Only one of the AuthN flows

Cisco Collaboration Applications

Cisco Webex app native Services AuthZ flows



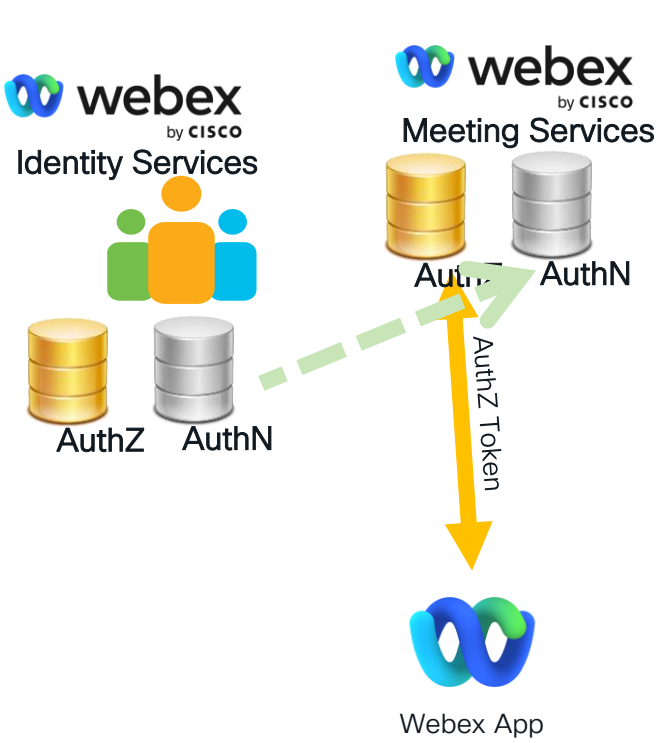
Collaboration Services:

Webex Calling

Webex Messaging

Cisco Collaboration Applications

Cisco Webex app with Meetings AuthZ flows

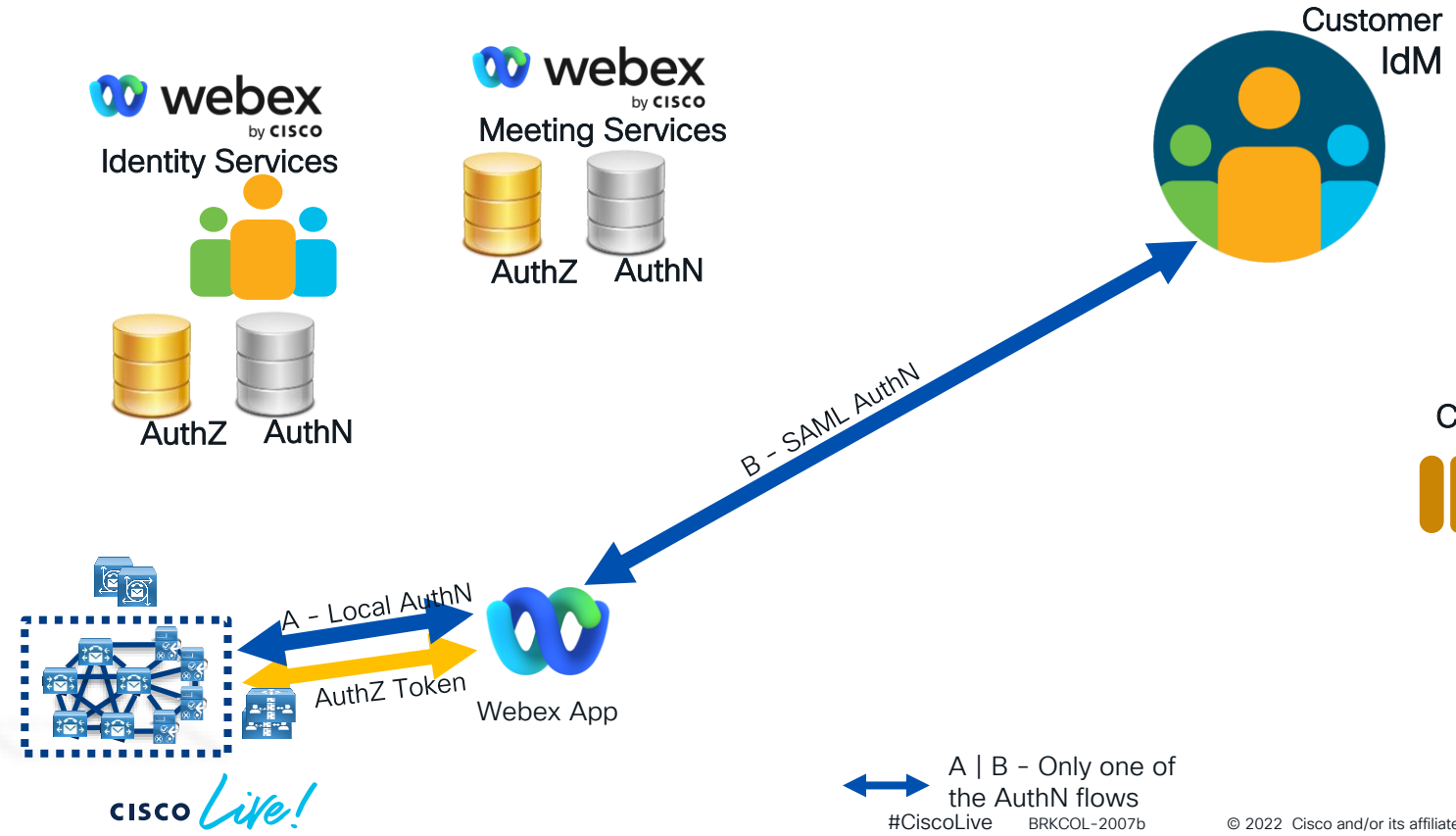


Collaboration Services:

Webex Meetings

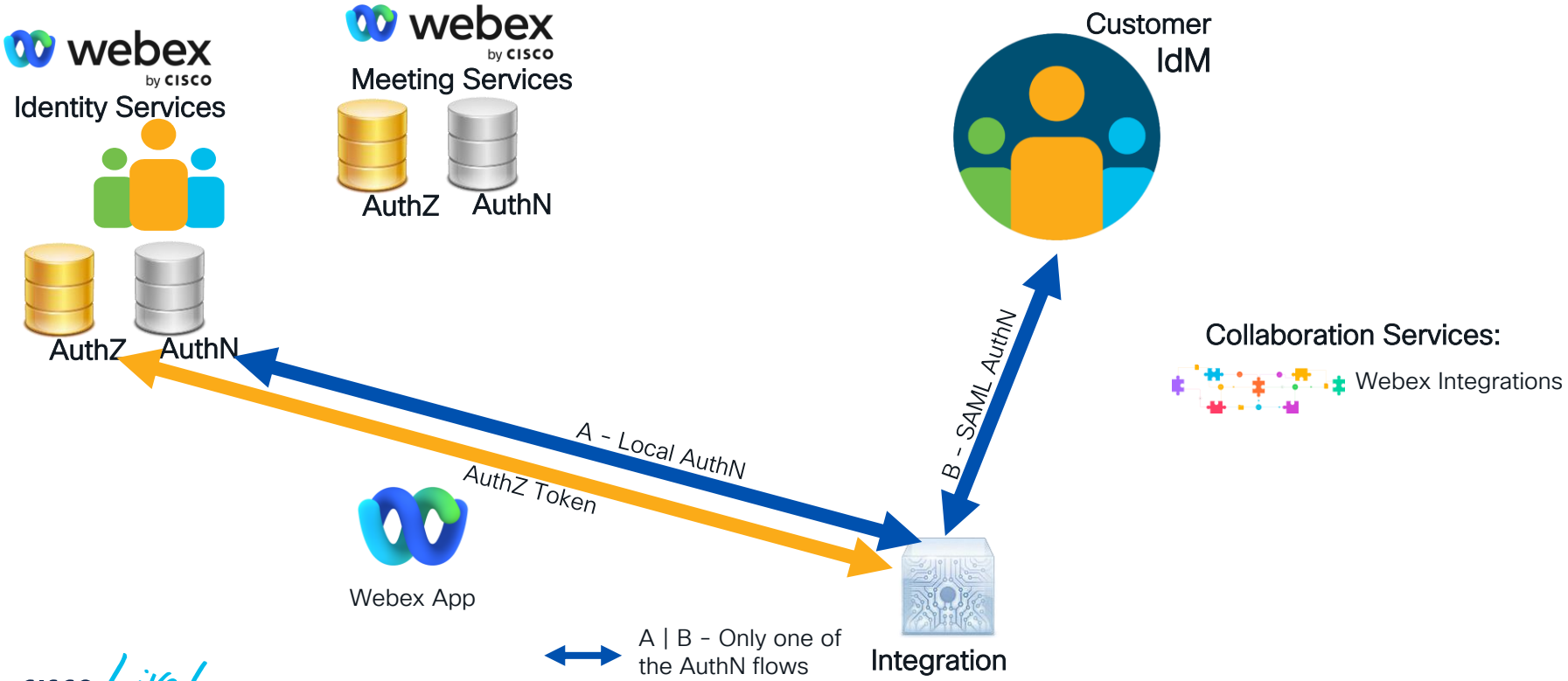
Cisco Collaboration Applications

Cisco Webex app with on-premises collaboration services AuthN/AuthZ flows



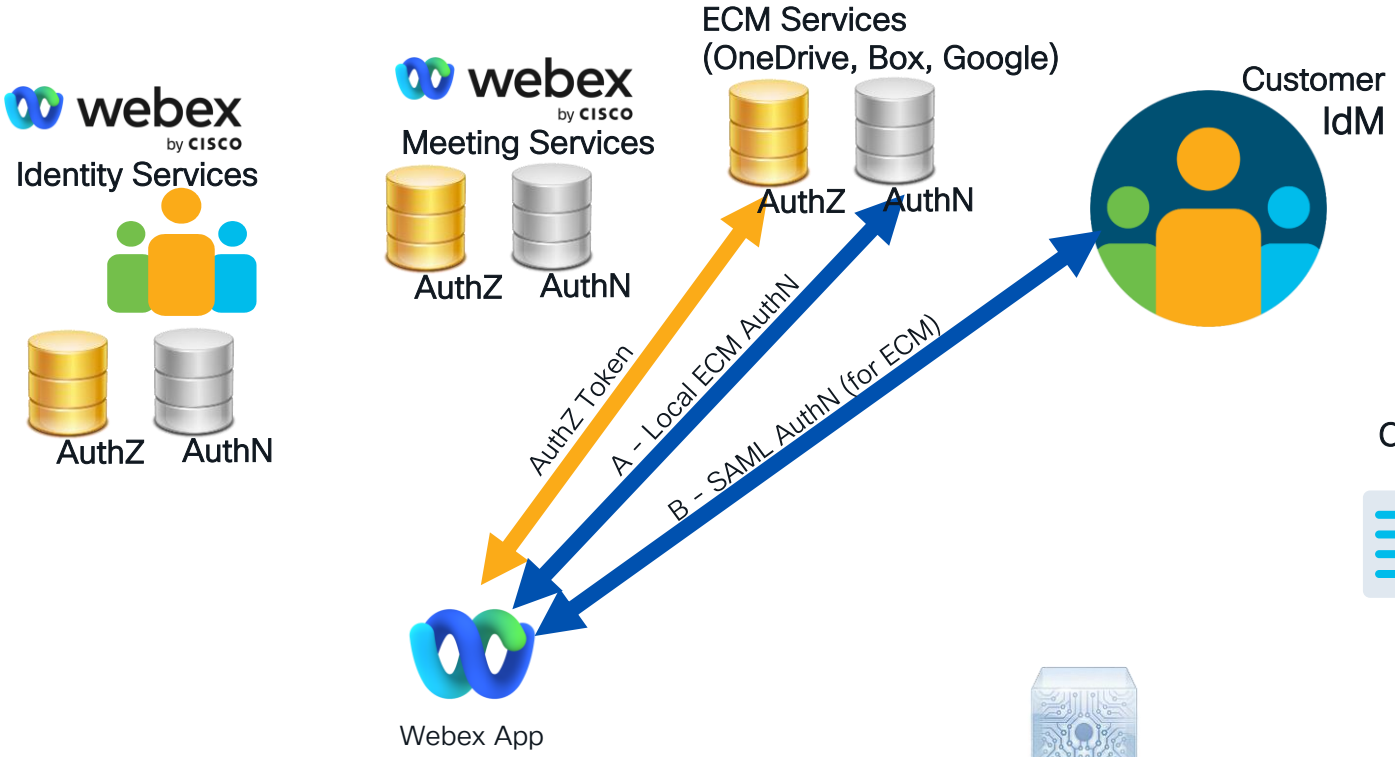
Cisco Collaboration Applications

Cisco Webex app with Integrations AuthZ flows



Cisco Collaboration Applications

Cisco Webex app with ECM AuthN/AuthZ flows

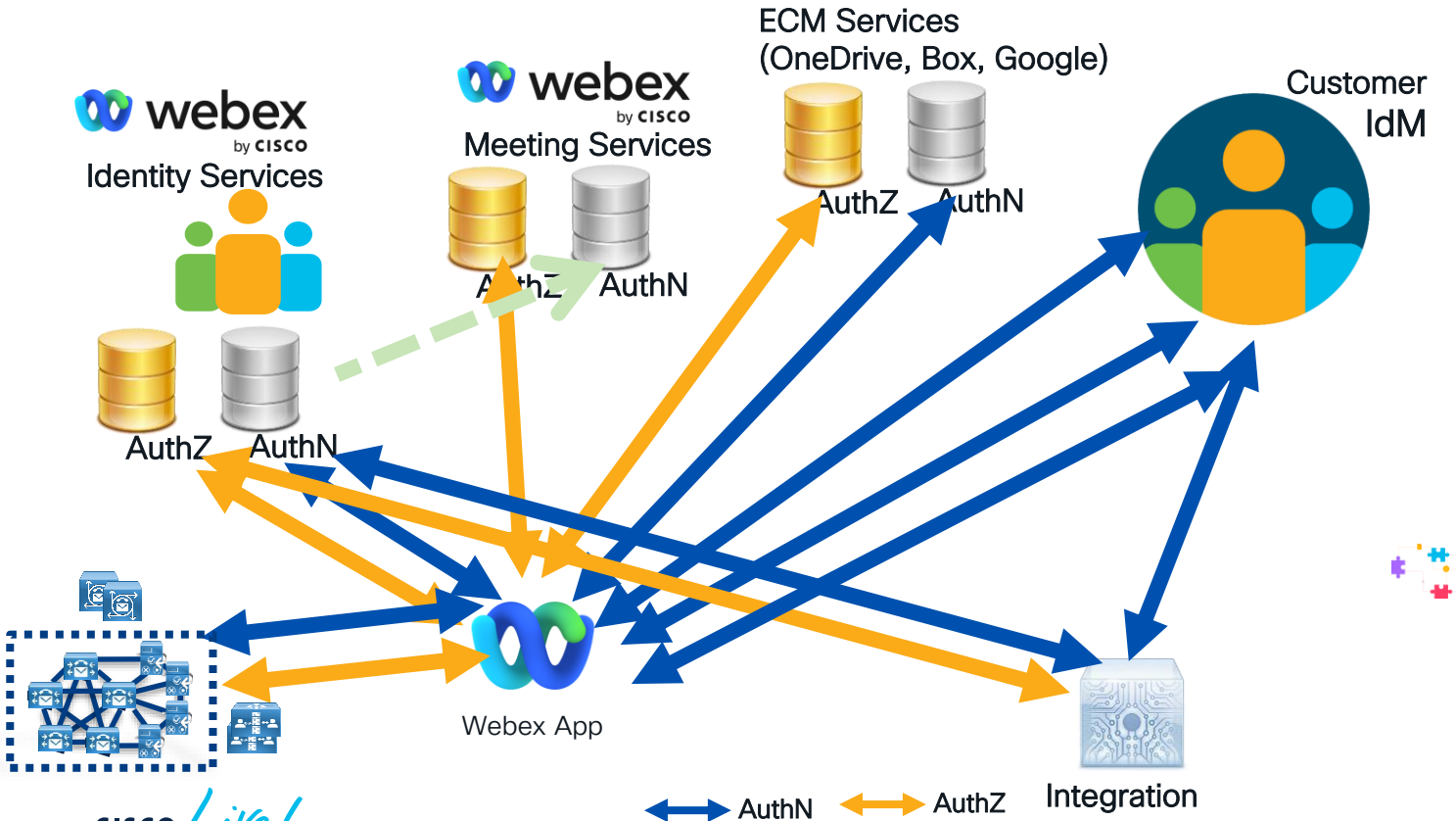


Collaboration Services:

Enterprise Content Management (OneDrive/Sharepoint, Box, Google Docs)

Cisco Collaboration Applications

Cisco Webex app with all AuthN/AuthZ flows



Collaboration Services:

- Webex Calling
- Webex Messaging
- Webex Meetings
- Enterprise Content Management (OneDrive/Sharepoint, Box)
- Webex Integrations
- CUCM/HCS/ UCM Cloud Calling

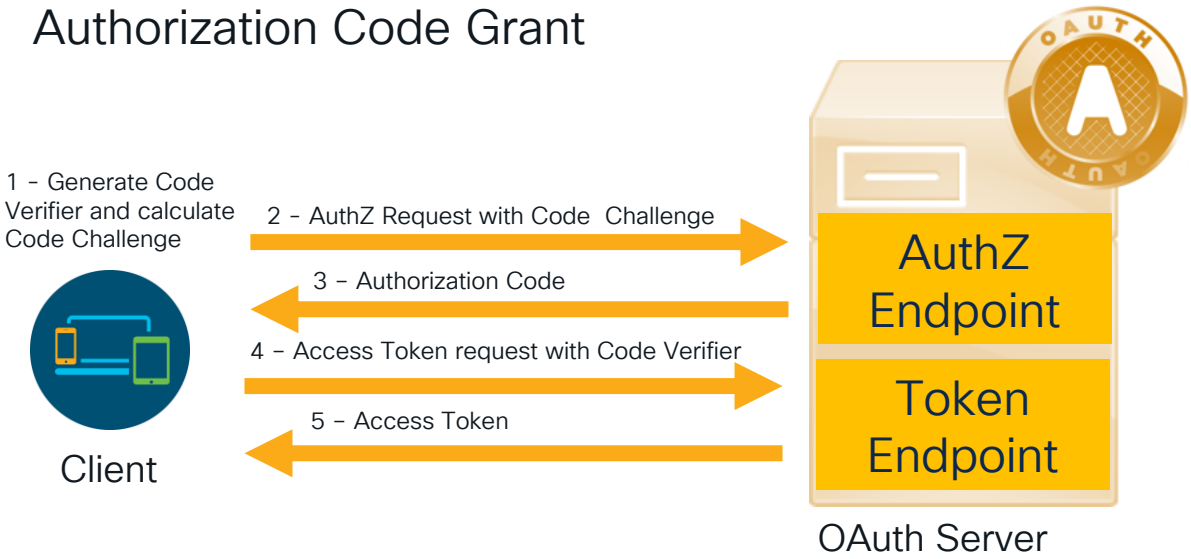
OpenID Connect and PKCE

how does it work?

What is PKCE ?

Proof Key for Code Exchange is defined in RFC 7636.

This mechanism allows to mitigate attacks to the interception of the authorization code in the OAuth Authorization Code Grant



What is OpenID Connect ?

OpenID Connect 1.0 is a **simple identity layer on top of the OAuth 2.0** protocol.

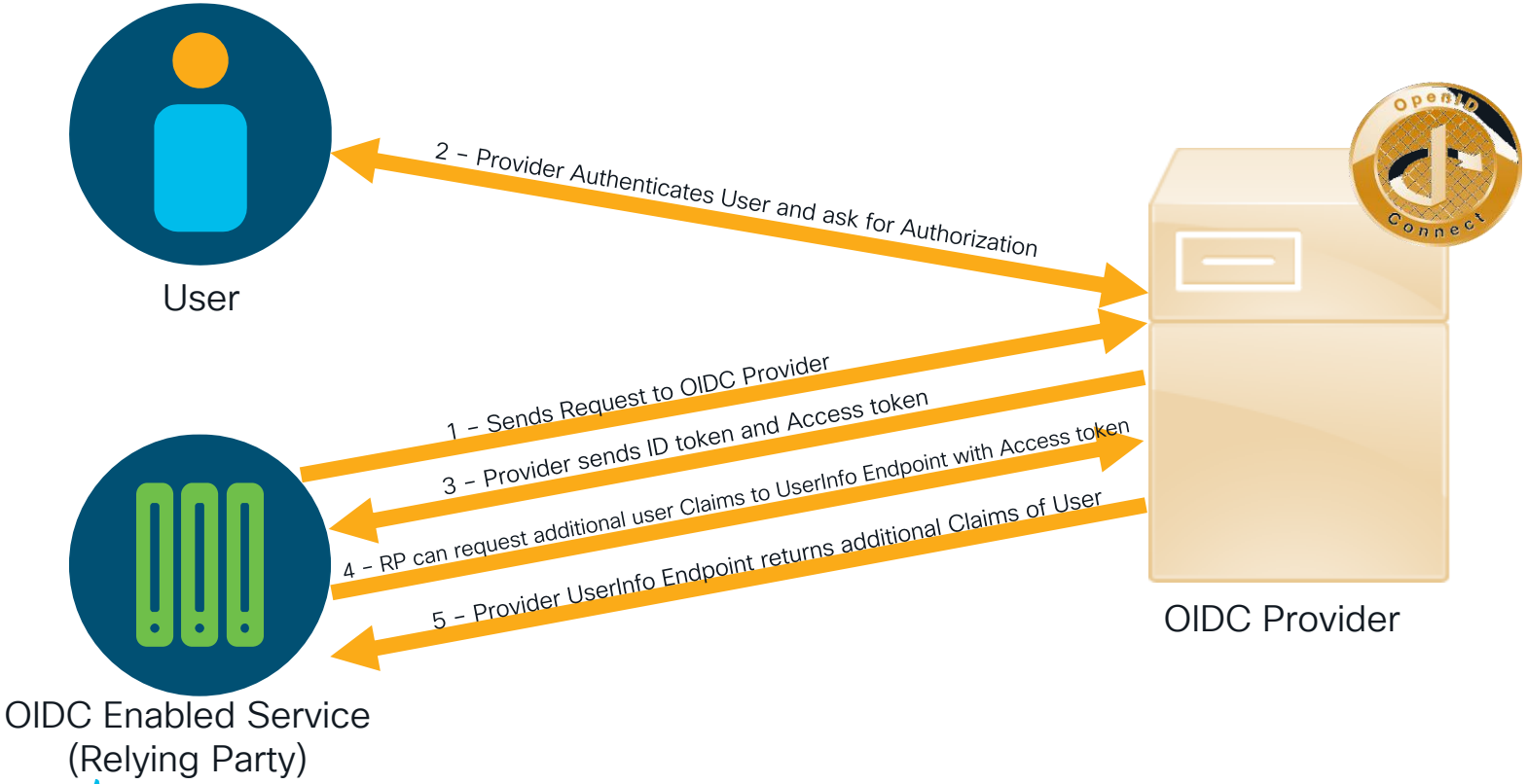
It allows Clients to **verify the identity of the End-User** based on the authentication performed by an Authorization Server.

It allows to **obtain basic profile information** about the End-User in an interoperable and REST-like manner.

The specification suite is extensible, allowing participants to use optional features such as **encryption of identity data**, **discovery of OpenID Providers**, and **session management**, when it makes sense for them.

OAuth 2.0

OpenID Connect Flow



ID Token

The **ID Token is a security token** that contains Claims about the **Authentication of an End-User** by an Authorization Server when using a Client, and potentially other requested Claims.

The ID Token is represented as a **JSON Web Token (JWT)**

More information in https://openid.net/specs/openid-connect-core-1_0.html#IDToken


```
"id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
  yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
  NzYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZ
  fV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5Nz
  AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzR0EHR9R6jgdqrOOF4daGU96Sr_P6q
  Jp6IcmD3HP99Obi1PRs-cwh3LO-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
  NqeGpe-gccMg4vfKjkM8FcGvnzZUN4_KSP0aAp1tOJ1zZwgjxqGByKHiOtX7Tpd
  QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJbOEoRoS
  K5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVVk4
  XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
```

```
{
 "iss": "https://server.example.com",
 "sub": "24400320",
 "aud": "s6BhdRkqt3",
 "nonce": "n-0S6_WzA2Mj",
 "exp": 1311281970,
 "iat": 1311280970,
 "auth_time": 1311280969,
 "acr": "urn:mace:incommon:iap:silver"
}
```


https://jwt.io/

Claims

It also defines a standard set of basic profile Claims.

Pre-defined sets of Claims can be requested using specific scope values or individual Claims can be requested using the claims request parameter.

The Claims can come directly from the OpenID Provider or from distributed sources as well.

More information in https://openid.net/specs/openid-connect-core-1_0.html#Claims

Example of UserInfo Response

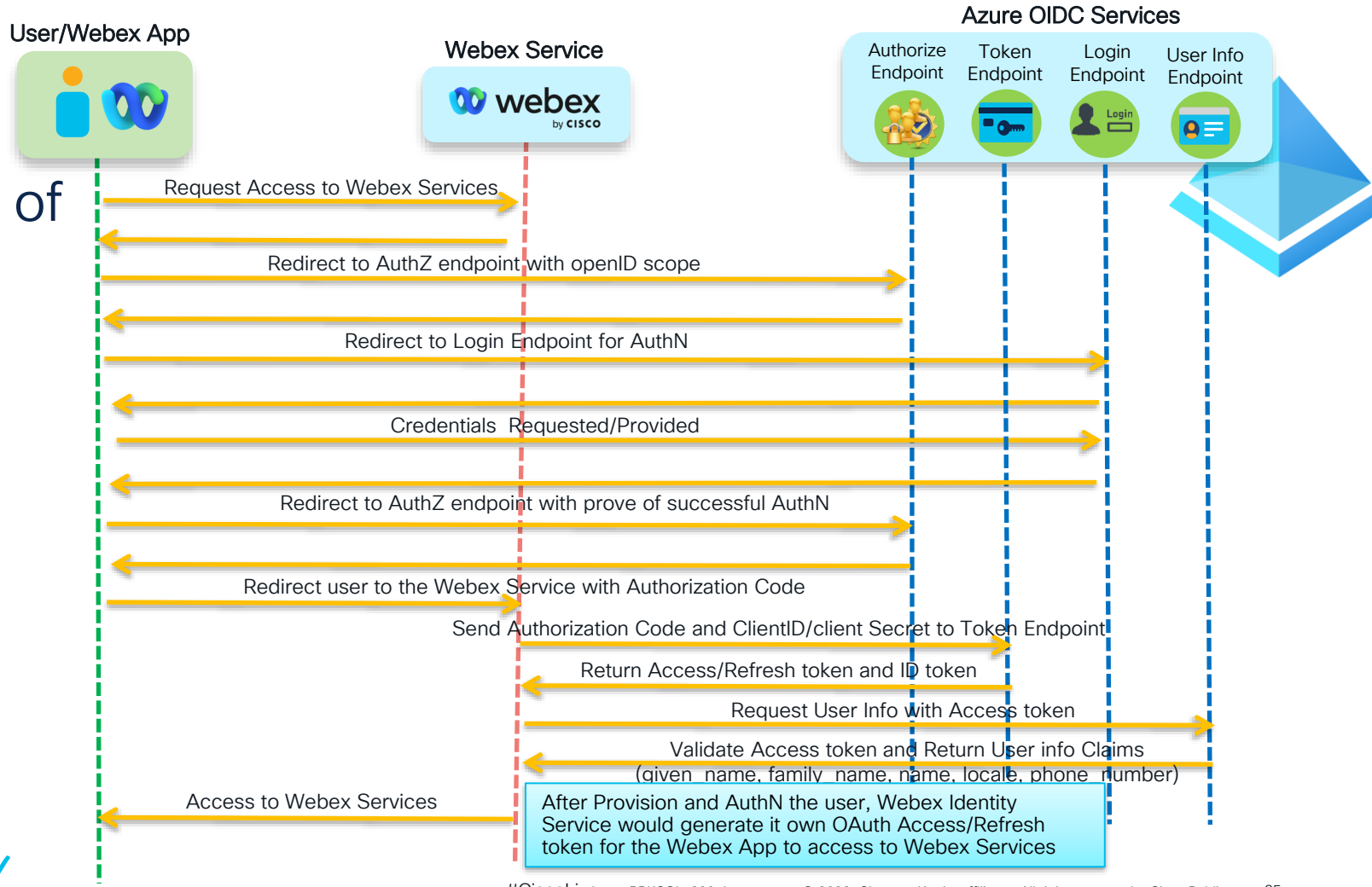
```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "sub": "248289761001",
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "preferred_username": "j.doe",
 "email": "janedoe@example.com",
 "picture": "http://example.com/janedoe/me.jpg"
}
```

Standard Claims

Member	Type	Description
sub	string	Subject - Identifier for the End-User at the Issuer.
name	string	End-User's full name in displayable form including all name parts, possibly including titles and suffixes, ordered according to the End-User's locale and preferences.
given_name	string	Given name(s) or first name(s) of the End-User. Note that in some cultures, people can have multiple given names; all can be present, with the names being separated by space characters.
family_name	string	Surname(s) or last name(s) of the End-User. Note that in some cultures, people can have multiple family names or no family name; all can be present, with the names being separated by space characters.
middle_name	string	Middle name(s) of the End-User. Note that in some cultures, people can have multiple middle names; all can be present, with the names being separated by space characters. Also note that in some cultures, middle names are not used.
nickname	string	Casual name of the End-User that may or may not be the same as the `given_name`. For instance, a `nickname` value of `Mike` might be returned alongside a `given_name` value of `Michael`.
preferred_username	string	Shorthand name by which the End-User wishes to be referred to at the RP, such as `janedoe` or `j.doe`. This value MAY be any valid JSON string including special characters such as `@`, `/`, or whitespace. The RP MUST NOT rely upon this value being unique, as discussed in **Section 5.7**.
profile	string	URL of the End-User's profile page. The contents of this Web page SHOULD be about the End-User.
picture	string	URL of the End-User's profile picture. This URL MUST refer to an image file (for example, a PNG, JPEG, or GIF image file), rather than to a Web page containing an image. Note that this URL SHOULD specifically reference a profile photo of the End-User suitable for displaying when describing the End-User, rather than an arbitrary photo taken by the End-User.
website	string	URL of the End-User's Web page or blog. This Web page SHOULD contain information published by the End-User or an organization that the End-User is affiliated with.
email	string	End-User's preferred e-mail address. Its value MUST conform to the **RFC 5322** [RFC5322] addr-spec syntax. The RP MUST NOT rely upon this value being unique, as discussed in **Section 5.7**.
email_verified	boolean	True if the End-User's e-mail address has been verified; otherwise false. When this Claim Value is `true`, this means that the OP took affirmative steps to ensure that this e-mail address was controlled by the End-User at the time the verification was performed. The means by which an e-mail address is verified is context-specific, and dependent upon the trust framework or contractual agreements within which the parties are operating.
gender	string	End-User's gender. Values defined by this specification are `female` and `male`. Other values MAY be used when neither of the defined values are applicable.
birthdate	string	End-User's birthday, represented as an **ISO 8601:2004** [ISO8601-2004] `YYYY-MM-DD` format. The year MAY be `0000`, indicating that it is omitted. To represent only the year, `YYYY` format is allowed. Note that depending on the underlying platform's date related function, providing just year can result in varying month and day, so the implementers need to take this factor into account to correctly process the dates.
zoneinfo	string	String from zoneinfo **[zoneinfo]** time zone database representing the End-User's time zone. For example, `Europe/Paris` or `America/Los_Angeles`.
locale	string	End-User's locale, represented as a **BCP47** [RFC5646] language tag. This is typically an **ISO 639-1 Alpha-2** [ISO639-1] language code in lowercase and an **ISO 3166-1 Alpha-2** [ISO3166-1] country code in uppercase, separated by a dash. For example, `en-US` or `fr-CA`. As a compatibility note, some implementations have used an

Example of OpenID Connect flow for Webex Azure Social Login

(AuthN & Provision)



OpenID Connect Discovery

As we saw before in OpenID Connect there are multiple endpoints that need to be target to get different results (Token, UserInfo, Authorization, etc.)

So the configuration can be request according to Discovery extensions https://openid.net/specs/openid-connect-discovery-1_0.html, in the end we just need to know the hostname for the service.

OpenID Provider Configuration Request

```
GET /.well-known/openid-configuration HTTP/1.1
Host: example.com
```

OpenID Provider Configuration Response

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "issuer":
   "https://server.example.com",
 "authorization_endpoint":
   "https://server.example.com/connect/authorize",
 "token_endpoint":
   "https://server.example.com/connect/token",
 "token_endpoint_auth_methods_supported":
   ["client_secret_basic", "private_key_jwt"],
 "token_endpoint_auth_signing_alg_values_supported":
   ["RS256", "ES256"],
 "userinfo_endpoint":
   "https://server.example.com/connect/userinfo",
 "check_session_iframe":
   "https://server.example.com/connect/check_session",
 "end_session_endpoint":
   "https://server.example.com/connect/end_session",
 "jwks_uri":
   "https://server.example.com/jwks.json",
 "registration_endpoint":
   "https://server.example.com/connect/register",
 "scopes_supported":
   ["openid", "profile", "email", "address",
    "phone", "offline_access"],
 "response_types_supported":
   ["code", "code id_token", "id_token", "token id_token"],
 "acr_values_supported":
   ["urn:mace:incommon:iap:silver",
    "urn:mace:incommon:iap:bronze"],
 "subject_types_supported":
   ["public", "pairwise"],
 "userinfo_signing_alg_values_supported":
   ["RS256", "ES256", "HS256"],
 "userinfo_encryption_alg_values_supported":
   ["RSA1_5", "A128KW"],
 "userinfo_encryption_enc_values_supported":
   ["A128CBC-HS256", "A128GCM"],
 "id_token_signing_alg_values_supported":
   ["RS256", "ES256", "HS256"],
 "id_token_encryption_alg_values_supported":
   ["RSA1_5", "A128KW"],
 "id_token_encryption_enc_values_supported":
   ["A128CBC-HS256", "A128GCM"],
 "request_object_signing_alg_values_supported":
   ["none", "RS256", "ES256"],
 "display_values_supported":
   ["page", "popup"],
 "claim_types_supported":
   ["normal", "distributed"],
 "claims_supported":
   ["sub", "iss", "auth_time", "acr",
    "name", "given_name", "family_name", "nickname",
    "profile", "picture", "website",
    "email", "email_verified", "locale", "zoneinfo",
    "http://example.info/claims/groups"],
 "claims_parameter_supported":
   true,
 "service_documentation":
   "http://server.example.com/connect/service_documentation.html",
 "ui_locales_supported":
   ["en-US", "en-GB", "en-CA", "fr-FR", "fr-CA"]
}
```

Conclusions and Key Takeaways

Conclusions and Key Takeaways

- Webex Identity Services improve the Token Management capabilities, to allow the fine tuning on Organization that have nonstandard Authorization policies.
- New Single Sign-On Wizard gather all feedbacks from our customers, to allow a better administration for the Collaboration Administrators.
- OpenID Connect is the summary of the best practices in the Identity space, bringing them together under a single protocol.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN