



Modern Auth & SSO for Networkers

Making sense of modern auth suites for those that miss the good ol' days of RADIUS and TACACS+ :)

Josh Green – Leader, Duo Security

Aaron T. Woland – Distinguished Engineer, Security

BRKSEC-2144

\$ whoami



Cisco role: Distinguished Engineer,
Security

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder how
I have been doing this for >30 years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco now!
Youngest is 3!

Fun fact 3: Just completed Cybersecurity
Master's Degree from SANS Institute
(Oct 2024)

\$whois Josh?



Cisco role: Leader, Duo TME

Experience: Over 15 years industry experience. Background in identity and access management (and molecular biology).

Fun fact 1: Pilot and space nut

Fun fact 2: Polyglot

Fun fact 3: Skier

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 November 15, 2024.

CISCO *Live!*

[https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKSEC-2144](https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2144)



Please fill out the survey



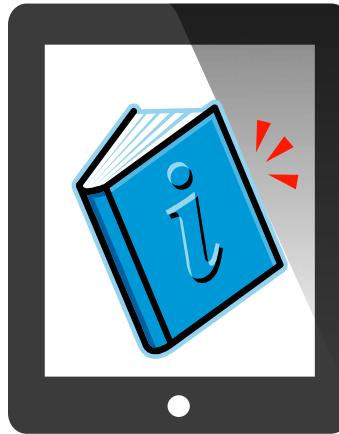
Drop your email in the comments – we WILL respond!

Important: Hidden Slide Alert



Look for this “For Your Reference” Symbol
in your PDF’s

There is a tremendous amount of hidden
content, for you to use later!



For Your Reference

ABSTRACT



For Your
Reference

Modern Auth and SSO explained for Network Engineers

AAA: Authentication, Authorization & Accounting does not mean “RADIUS”.

Those of us in Network Security are usually familiar with 802.1X and authenticating to networks for wireless, wired, and even VPN. AAA is a principle, not a product.

The concepts are universal and still apply when you hear the “new” authentication protocol types like: OAuth, SAML, OIDC, FIDO, etc. This session will focus on explaining modern web-based authentication protocols & teaching about them in a way that compares & contrasts them to network security authentication methods. In other words: come learn about the latest in authentication protocols and how to understand them with your networking background. If you know all about SAML & OAuth already, but don’t understand 802.1X or EAP – this session is also for you!

Expert leaders from Cisco's Duo Security business, Aaron Woland and Jeff Groesbeck, will entertain you while educating you on this important and growing area of security.



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

As the unofficial “Cisco History Professor” I tend to explain technology with a bit of a history lesson, so you can understand how we got to where we are.

-Aaron T. Woland
random guy in IT since the Dinosaurs



A Brief History of Identity

Tribes

Most people never left their village. Identity was easy. Everyone knew everyone. The identity "data breach" was impossible.

Wax Seals

Originating in China, delicate wax seals provide authentication AND evidence of message tampering

Encryption

The first known use of codebooks to encipher messages between parties.
Encryption was born on paper.

Biometric ID

The first photo ID concept was created.

~12k Years Ago

5000BC

1600-1064BC

~200BC-400AD

1379AD+

1677AD

1876AD

Agriculture & Villages

As people created larger settlements, it became impossible to know everyone. Trusted 3rd parties can make introductions.

The first stamped signature appears in Sumeria.

Passwords

Roman soldiers are given nightly-changing "watchwords" to identify travellers arriving at garrisons after dark.

MFA

English Parliament requires both signatures and wax seals on official documents.

“Authentication, Authorization & Accounting is an age-old security principal that should apply to all things Security related”

- Aaron T Woland, pompous windbag

AAA



I'd like 40K from Chuck Robbins' Account



Do You Have Identification?

Authentication

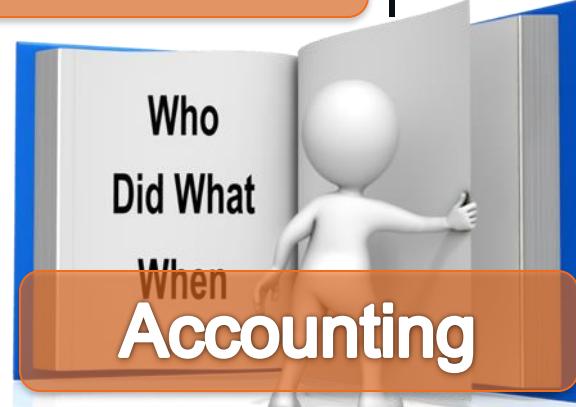
Yes, I Do. Here it Is.



Sorry, Aaron Weland is not Authorized

Authorization

To Withdraw Money From Chuck Robbins' Account



AAA in a networking world

- In “our” world, we have thought of 2-types of AAA:
 - Controlling access to networks.
 - Dial-up (*yes, I'm that old*)
 - 802.1X
 - Remote Access VPN
 - Or access to our terminals / CLI's (i.e.: TACACS+)
- Basically, we want to know who and what is connecting to your network or CLI before granting access, and let that access be specific.

Network access AAA

ISE is sort of like the “airport security” of the network, if you will.

AuthN

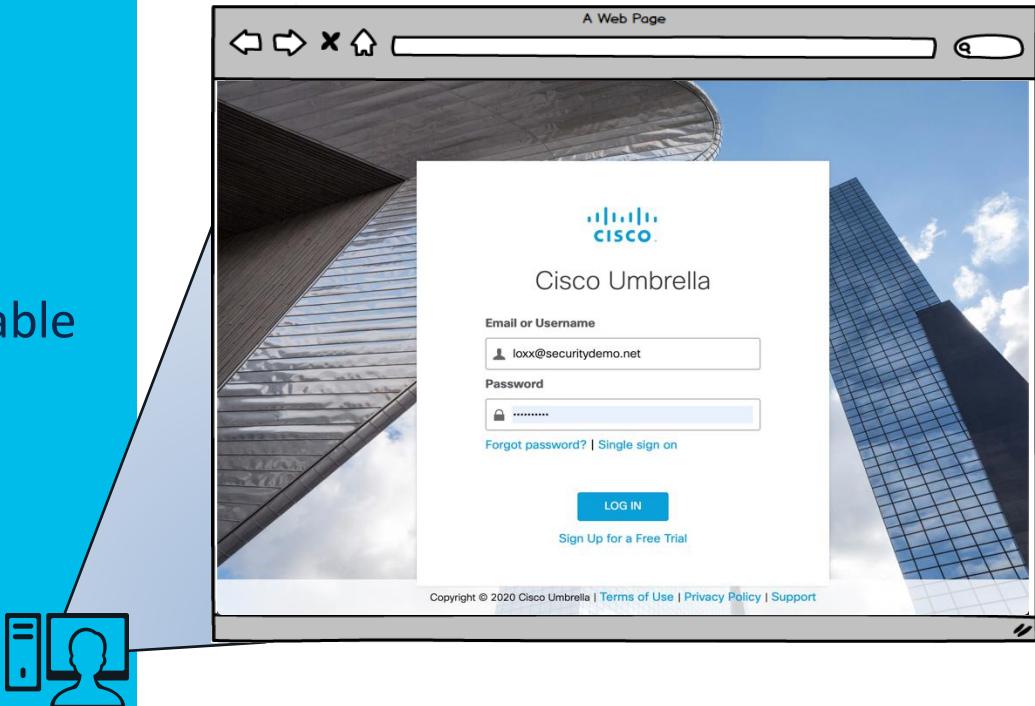
- It validates who you are by checking your credential (username/password/certificate) and that the credential is trusted.
 - Did the username/password match
 - Was the certificate signed by a trusted authority
 - Proof of possession

AuthZ

- It validates the device is allowed
 - Is it an allowed type (Profile)
 - Does it meet the security requirements (Posture)

Application Access

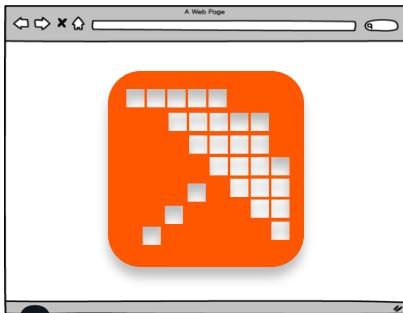
- While WE spend so much time focused on network authentication:
- The same principals are applicable to applications & web sites



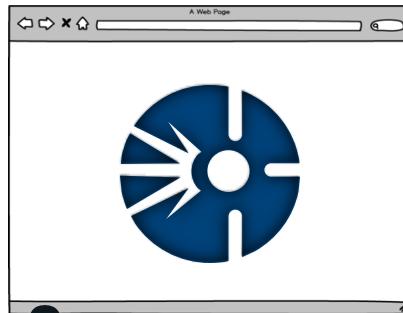
Application Access

- Must login to web apps (like the Cisco Live app)
- Identify WHO the human is & what access they get to the app
 - Speakers get different access than attendees

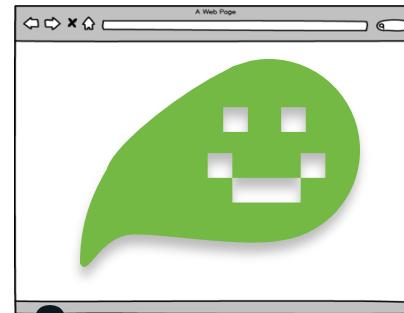
Apps could maintain its own User DB



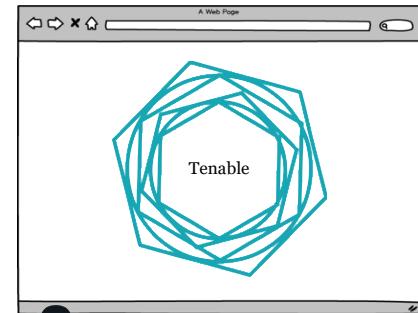
user1 / pwd
user2 / pwd
user3 / pwd



user1 / pwd
user2 / pwd
user3 / pwd



user1 / pwd
user2 / pwd
user3 / pwd

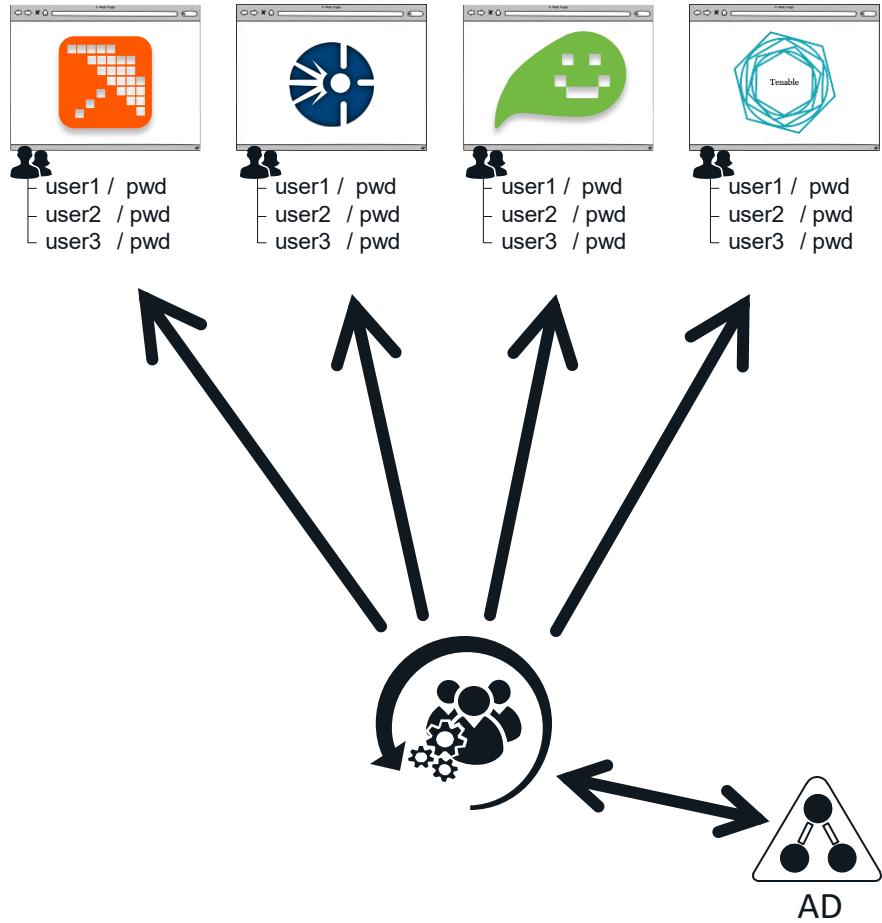


user1 / pwd
user2 / pwd
user3 / pwd

Note: this is not the case for many NEW apps, they instead rely on the Identity Provider for everything. CII (aka: Oort) is an example.

Enter: Identity Management Products

- Solution to keep all user accounts across all these web apps in sync.
 - Examples:
 - - Tivoli Identity Manager
 - - Oracle Identity Manager
 - - Okta Identity Management
 - - etc.



System for Cross-domain Identity Management

*SCIM = standard for
automating the exchange of
user identity information
between identity systems.*

Aaron likes to equate it to an LDIF export & import in LDAP

Example

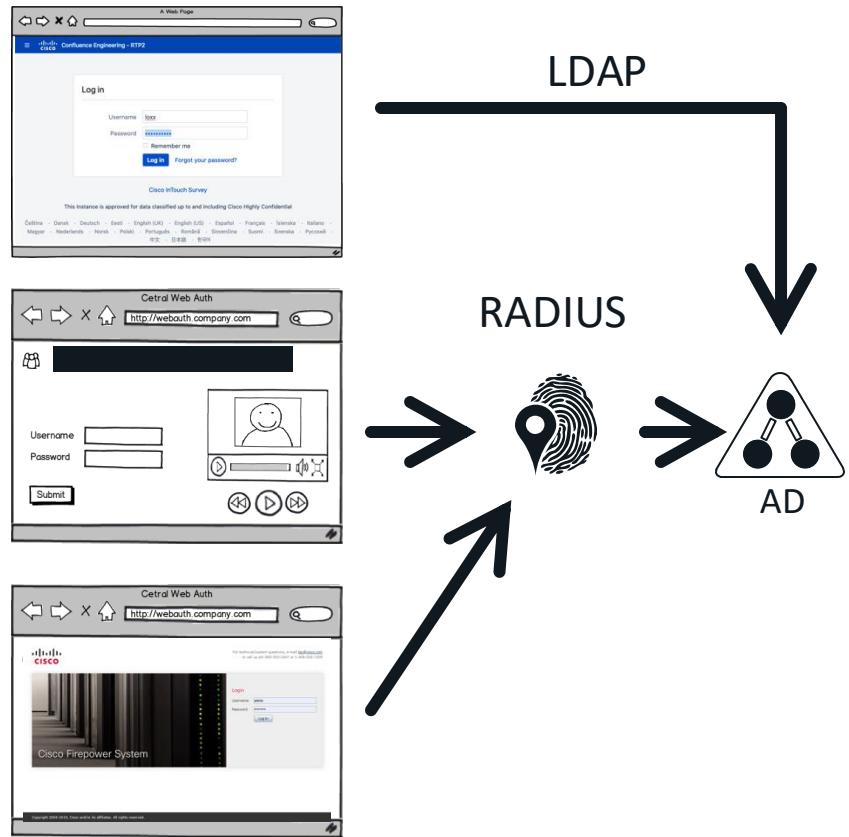
- Example of what an IAM would do when you change your password
- *** Cisco Infosec policy won't let me show you the REAL screen, so I mocked up a fake*

<http://password.company.com>

Account	Target System	Password Changed?	Result
loxx	Prod AD	Yes	Success
loxx	Linux NIS	Yes	Success
loxx	Stage AD	Yes	Success
aawoland	OpenLDAP	Yes	Success
loxx	Call Mgr	Yes	Success
loxx	WebEx	Yes	Success

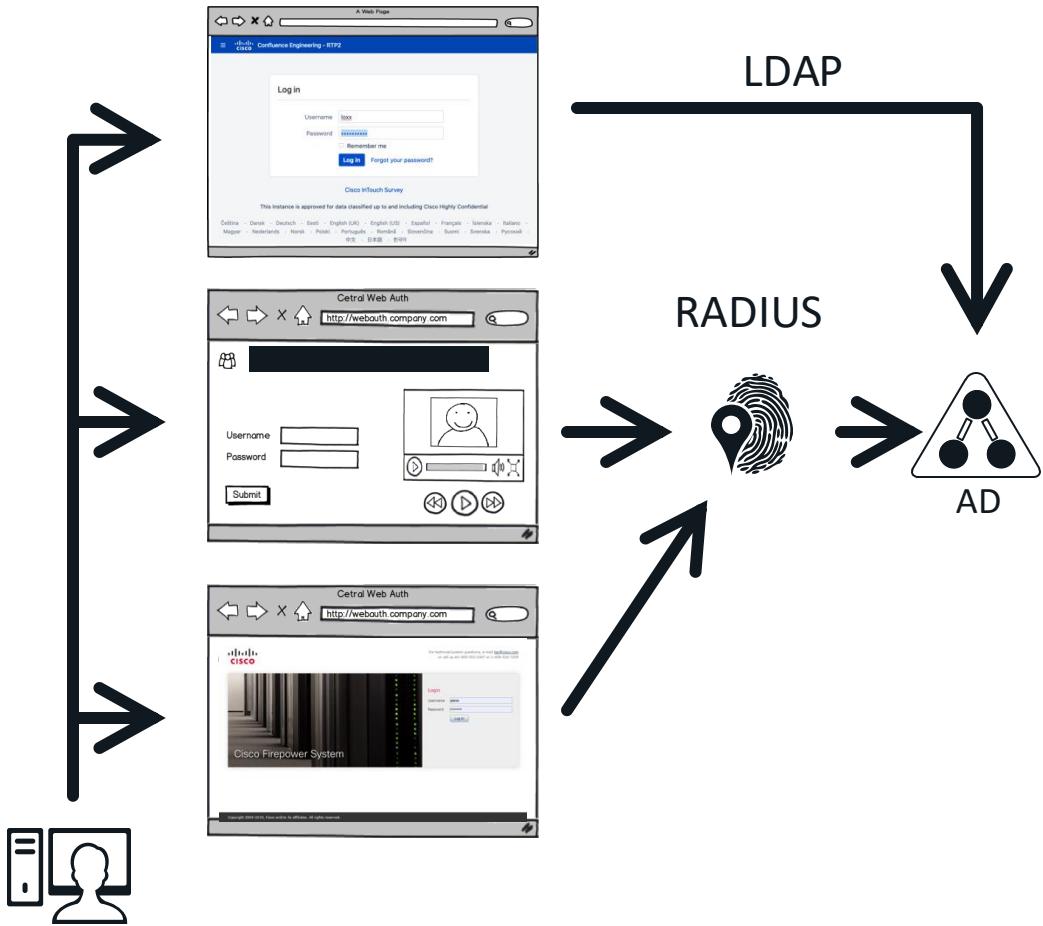
Some tried RADIUS or LDAP logins

- Provided a single location for username/passwords
- But still requires user to login each & every app separately



Bad User Experience

- Still requires a user to log in to each app
 - Same username / password
 - But must use it separately
- Is this Single-Sign-On?



New Term: Federation /fĕd"ə-rā'shĕn/

*Delegation of authority
by otherwise independent
entities*

-Josh Green, Geek

Federation /fĕd"ə-rā'shĕn/ (dictionary.com)



*the formation of a [union],
with a central [authority], by a
number of separate [entities],
each of which retains control
of its own internal affairs.*



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



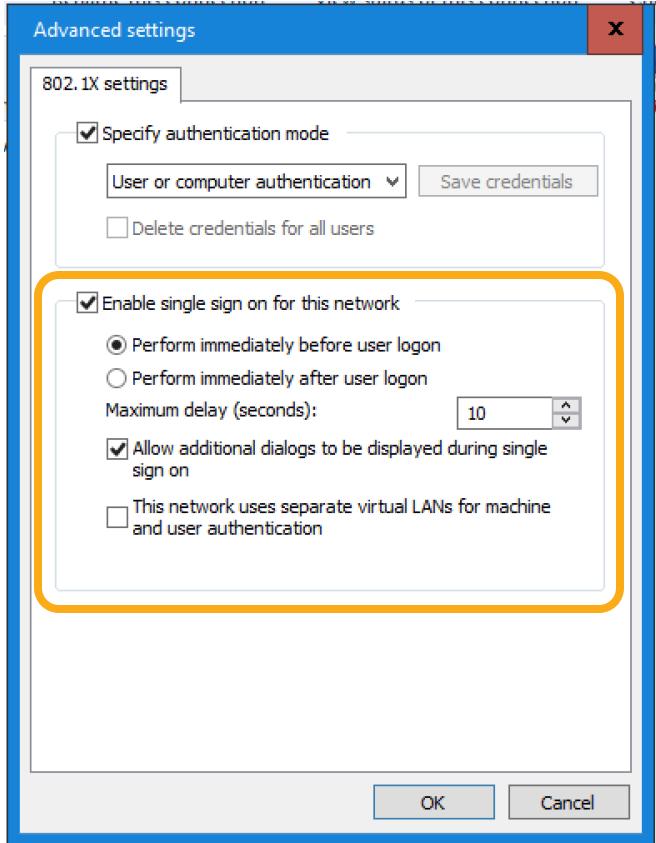
Enter: Single Sign On

Single Sign On (SSO): one key to unlock multiple doors

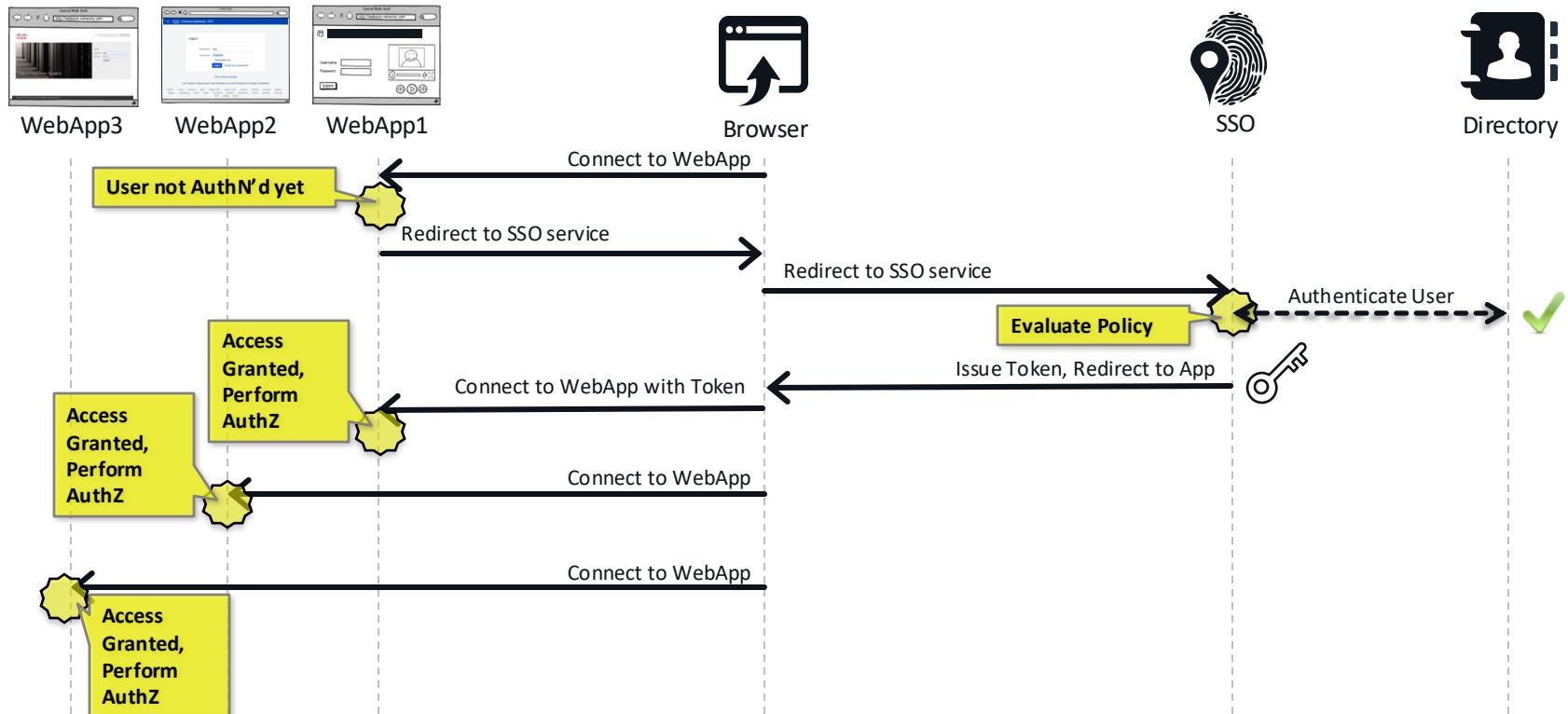
SSO itself is the process that allows a single authentication to be used across multiple web sites or applications

Note: you can have federation without SSO, but you cannot have SSO w/o federation

SSO w/ Dot1X Supplicant



SSO [somewhat] Explained



SSO principals

- AuthN One Time
 - Each app uses the same AuthN, performs AuthZ locally
 - Tries to use existing auth
 - If no existing, will send user for authentication

Note: the fact that the app is still still doing local AuthZ shows federation.



Demo Video: Single Sign On with Duo



Recycle Bin



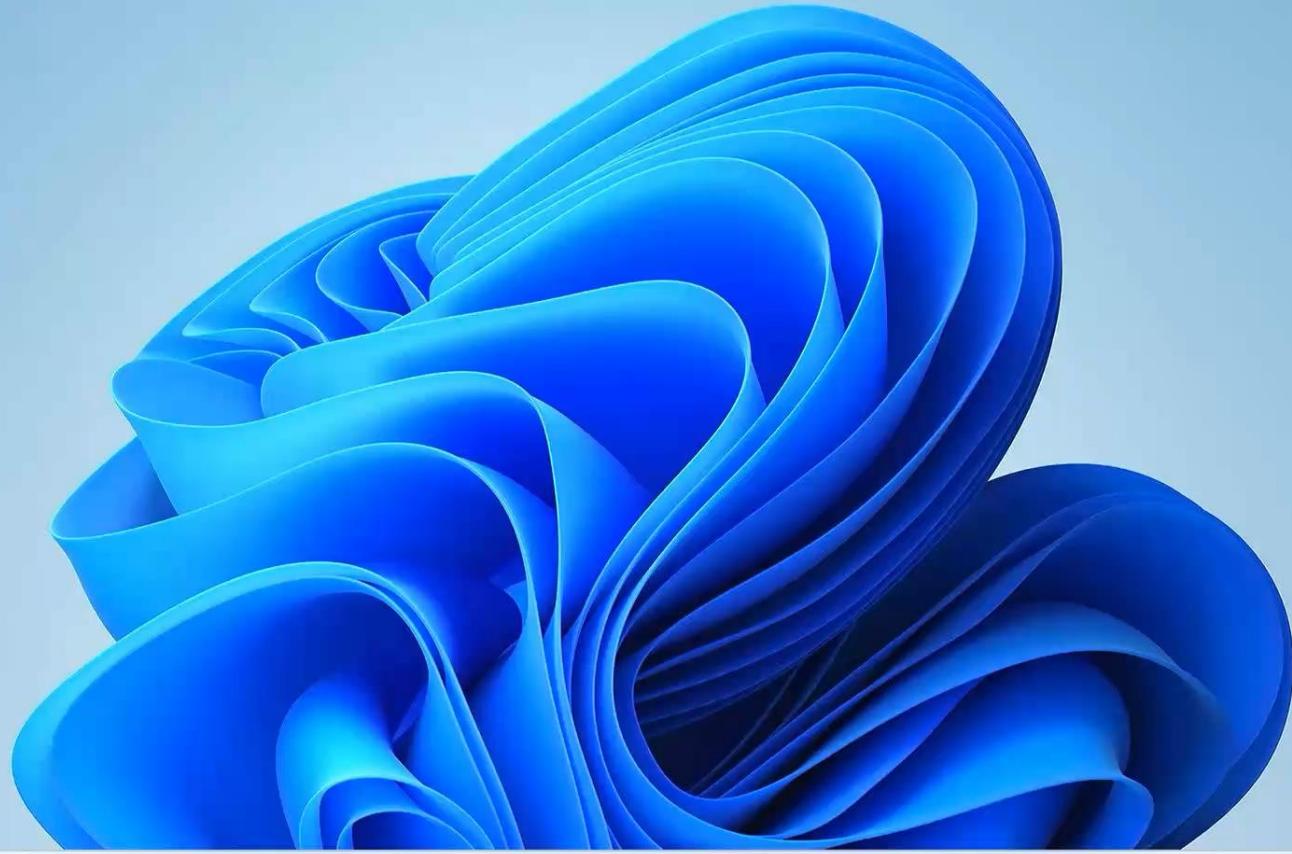
Google
Chrome



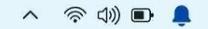
Microsoft
Edge



Webex



Search



CISCO Live!

BRKSEC-2144

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

32

For Your
Reference

CISCO

Single Sign-On

lee@zerotrustdemo.com [edit](#)

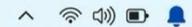
Password

Log in

Secured by Duo



Search





For Your
Reference



Check for a Duo Push

Verify it's you by approving the notification...

Sent to "iOS" (*****5672)



[Other options](#)

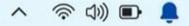
Remember me

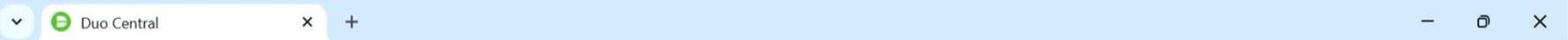
[Need help?](#)

Secured by Duo



Search





← → ⌂ zerotrust.login.duosecurity.com/central/



grid Duo Central Salesforce



Search

[Manage Devices](#)



For Your
Reference

Cisco
Webex

Cisco Webex

JIRA

JIRA - Internal Only

cisco Meraki

Meraki



Microsoft 365



Outlook



Salesforce - Single Sign-On



Identity Services Engine

ZTA Client Access - ISE

Secured by Duo

sso-1a4ab80e.sso.duosecurity.com/saml2/sp/DIAOLDZKLY9MUQ7GT2EG/sso



Search



CISCO Live!

BRKSEC-2144

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

35

Duo Central Log In Using | Salesforce

duo-tme-dev-ed.my.salesforce.com

Duo Central Salesforce

 For Your Reference



Log In Using

[Log in with DuoSSO](#)

[Log In with a Different Account](#)

© 2024 Salesforce, Inc. All rights reserved.


Introducing the Serviceblazer Community on Slack.

Connect with fellow service and field service professionals in a dedicated space on Slack. Share expertise and learn from your peers in real time.

[JOIN ON SLACK](#)



Search

CISCO Live!



Search Setup



Setup

Home

Object Manager

Quick Find

Setup Home

Release Updates

Lightning Usage

Sales Cloud Everywhere

ADMINISTRATION

> Users

> Data

> Email

PLATFORM TOOLS

> Apps

> Feature Settings

SETUP
Home

Create ▾



Get Started with Einstein Bots

Launch an AI-powered bot to automate your digital connections.

Get Started



Mobile Publisher

Use the Mobile Publisher to create your own branded mobile app.

Learn More ↗



Real-time Collaborative Docs

Transform productivity with collaborative docs, spreadsheets, and slides inside Salesforce.

Get Started ↗

Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



Enter: Security Assertion Markup Language (SAML)



Security Assertion Markup Language (SAML)

The XACML working group had to find something to do with their stuff ☺

- Open Standard (OASIS Consortium)
 - v2 is most common, standardized back in 2005
 - Allows the SSO product to pass credentials to applications, so a single credential can be used across many web sites / apps
 - Uses XML for the data

Definitions

Web-based
Auth's



Browser
aka: User Agent

Acts as the “client”. Each AuthN session is stored per-UserAgent
(ex: Outlook, Chrome, Safari, etc.)

Like combo of supplicant & authenticator in dot1x.



Service Provider (SP)



IdP



Directory

802.1X



Supplicant



Authenticator



Authentication Server



Directory

Definitions

Web-based
Auth's



Browser
aka: User Agent



Service
Provider (SP)



IdP



Directory

The application that needs to be logged into.
(ex: ServiceNow, SalesForce, etc.)

Like the Authenticator in dot1x

802.1X



Supplicant



Authenticator



Authentication
Server



Directory

Definitions

Web-based
Auth's



Browser
aka: User Agent



Service
Provider (SP)



Identity
Provider (IdP)



Directory

Handles the authentication, issues assertion, etc.
(ex: PING, EntralD, Shibboleth, etc.)

Like the Authentication Server in dot1x

802.1X



Supplicant



Authenticator



Authentication
Server



Directory

Definitions

Web-based
Auth's



Browser
aka: User Agent



Service
Provider (SP)



Identity
Provider (IdP)



Directory

The ID store. Could be built into the IdP or could be separate (like AD).
(ex: AD, LDAP, JDBC, etc.)

Same as the ID Store with dot1x

802.1X



Supplicant



Authenticator



Authentication
Server



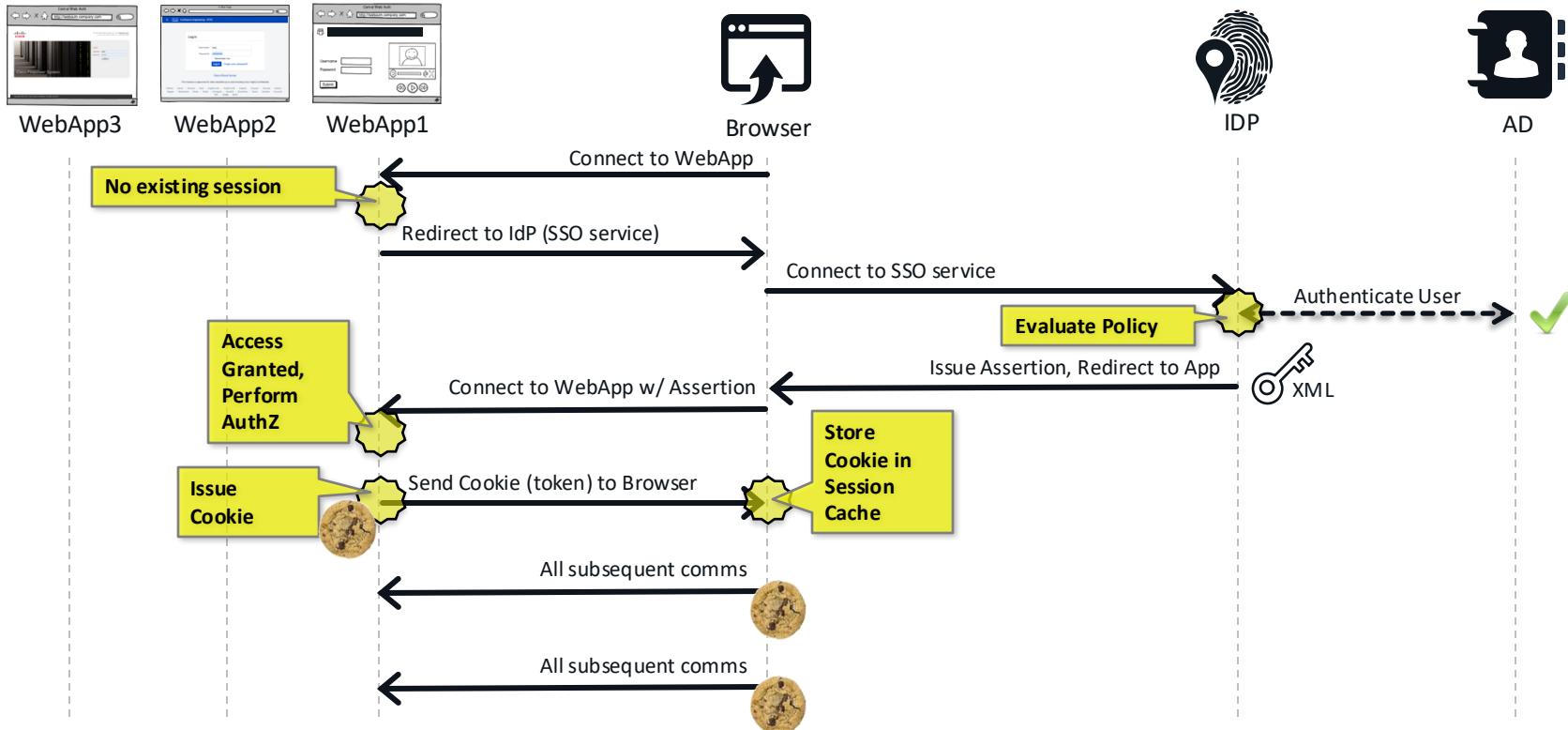
Directory



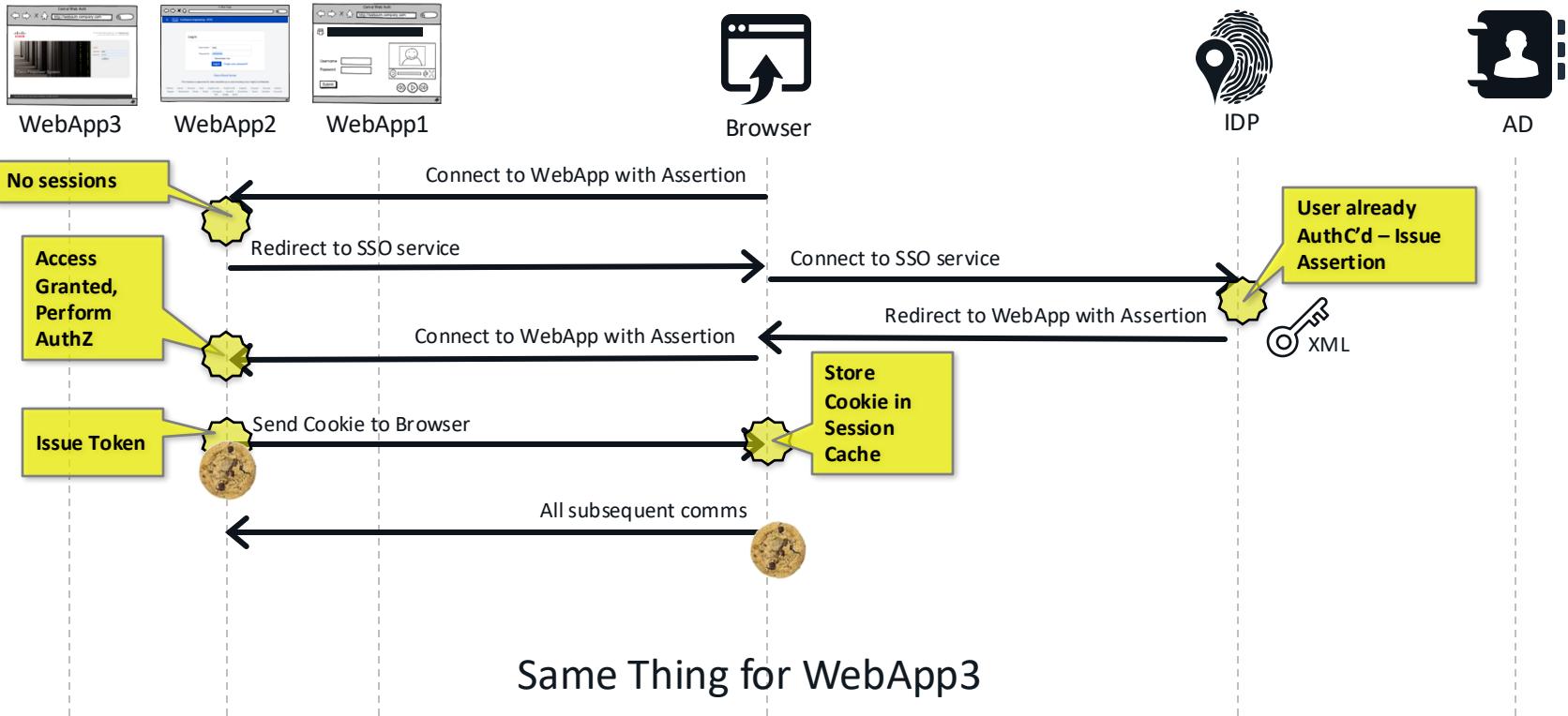
More Definitions

- **Assertion:** In SAML, an assertion is a package of information that the IdP sends to the SP. This information typically includes authentication statements, attributes about the user, and authorization decisions.
 - Often interchanged with term “Token”
- **Assertion Consumer Service (ACS):** This is a specific endpoint (URL) on the Service Provider's side where the SAML assertion is sent. The ACS is responsible for receiving the SAML response from the IdP, processing it, and then using the information contained within to authenticate and potentially authorize the user.

SAML for Single-Sign-On



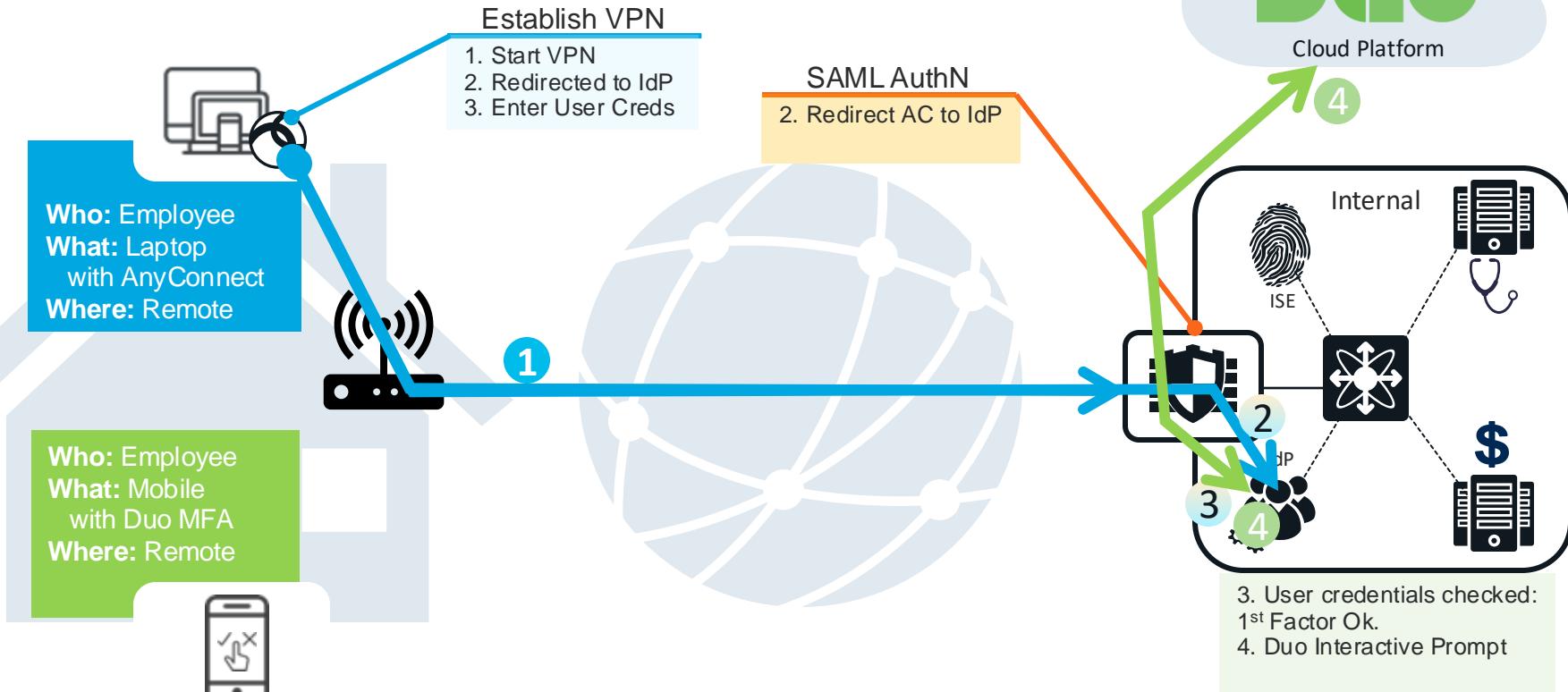
SAML for Single-Sign-On



Same Thing for WebApp3

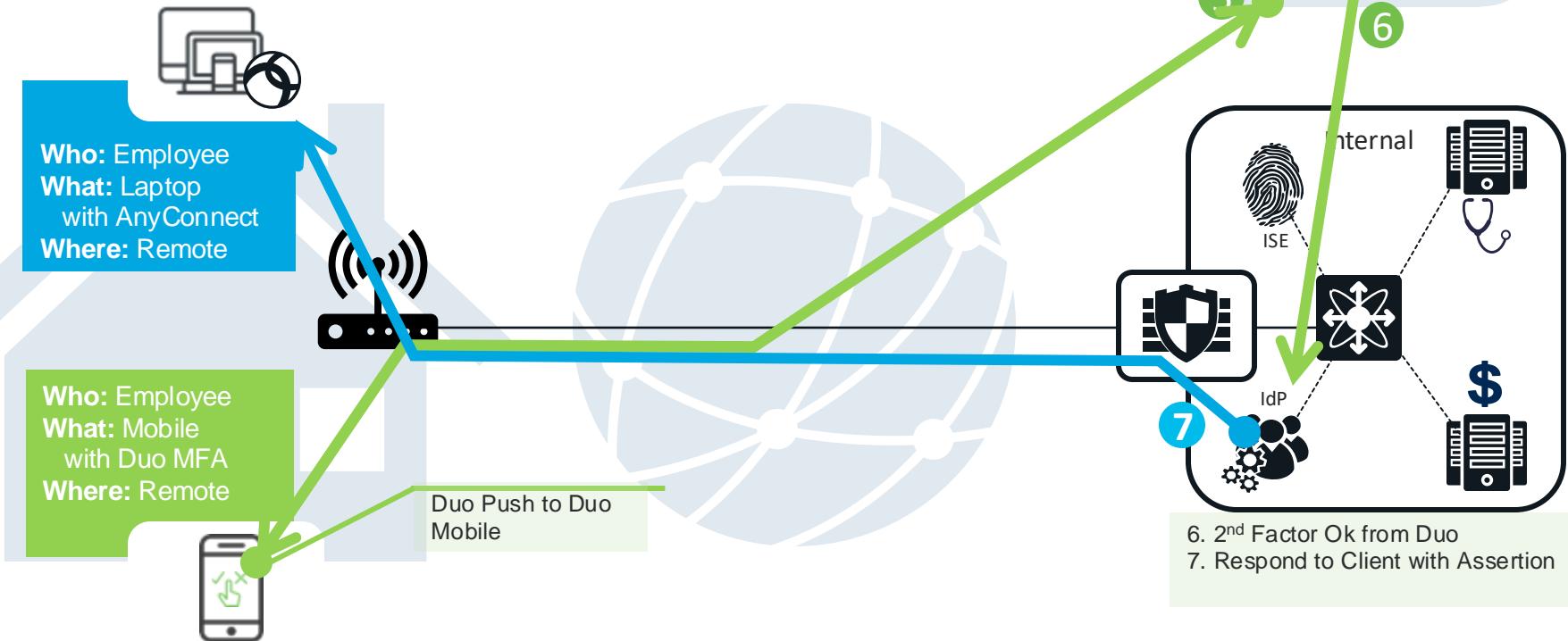
The key to SAML is browser redirects!

For Your Reference



The key to SAML is browser redirects!

For Your Reference



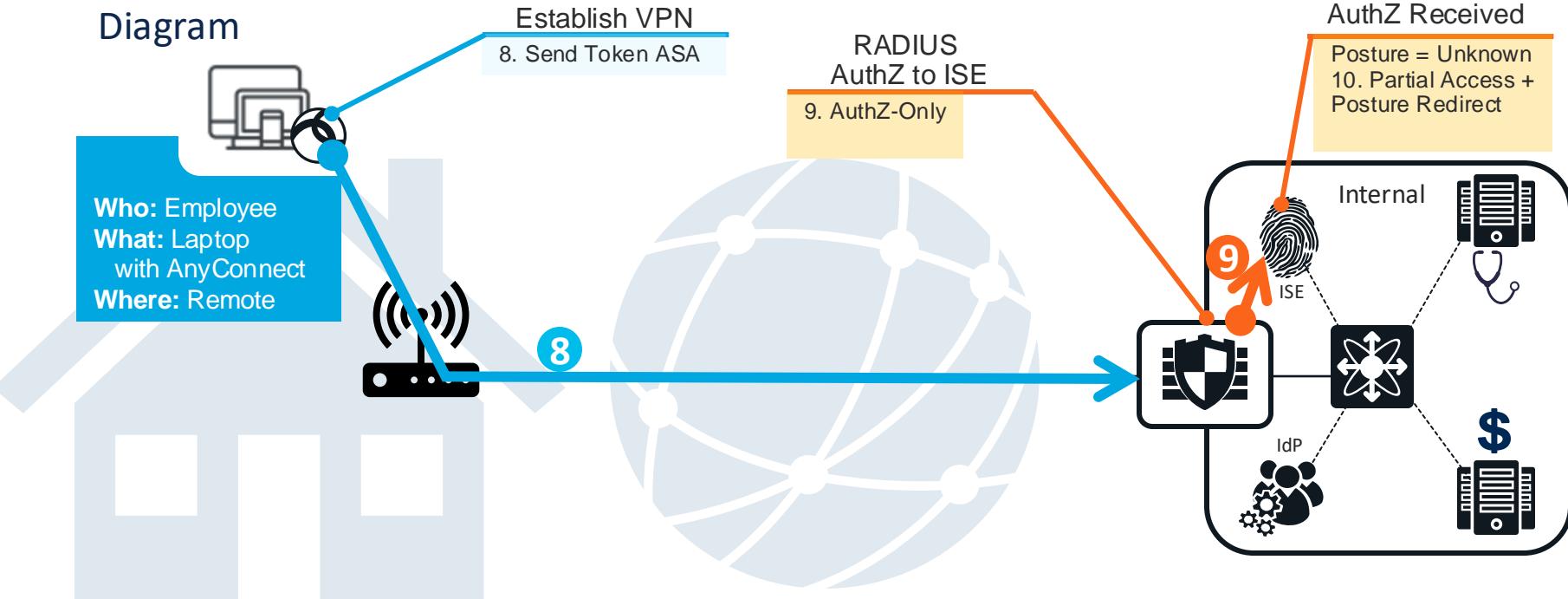


For Your Reference

*included hidden slide to show full flow w/ ISE Posture

Solution Overview

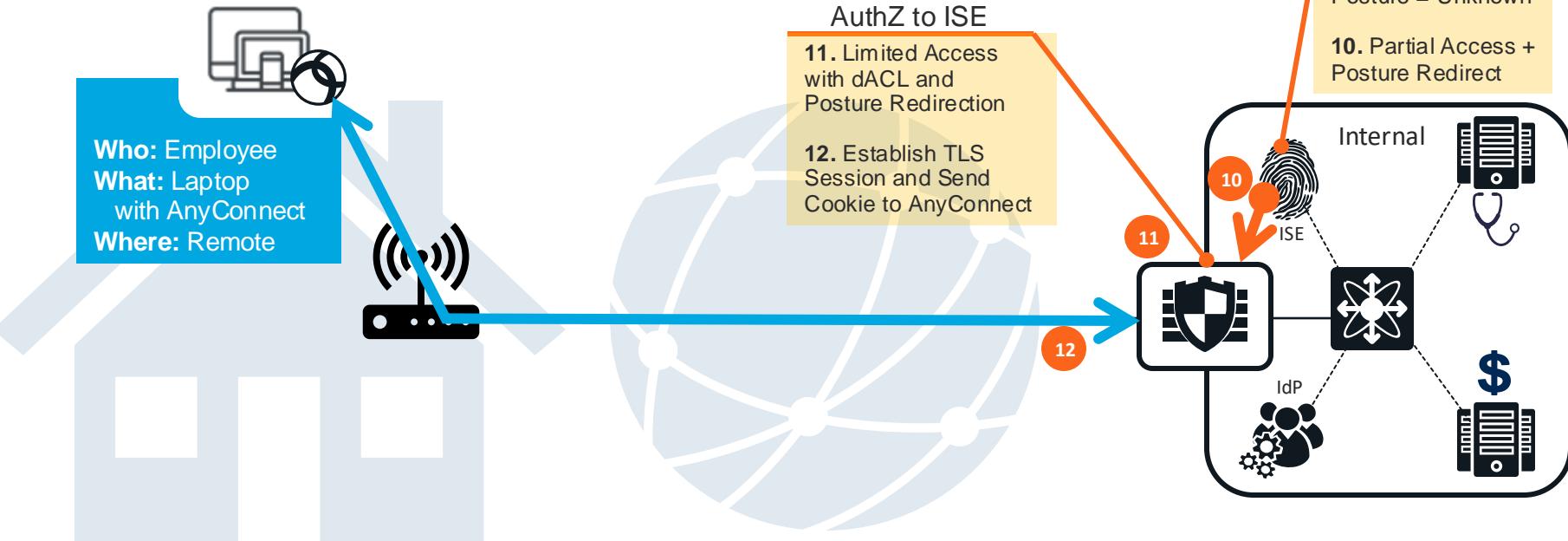
Diagram





Solution Overview

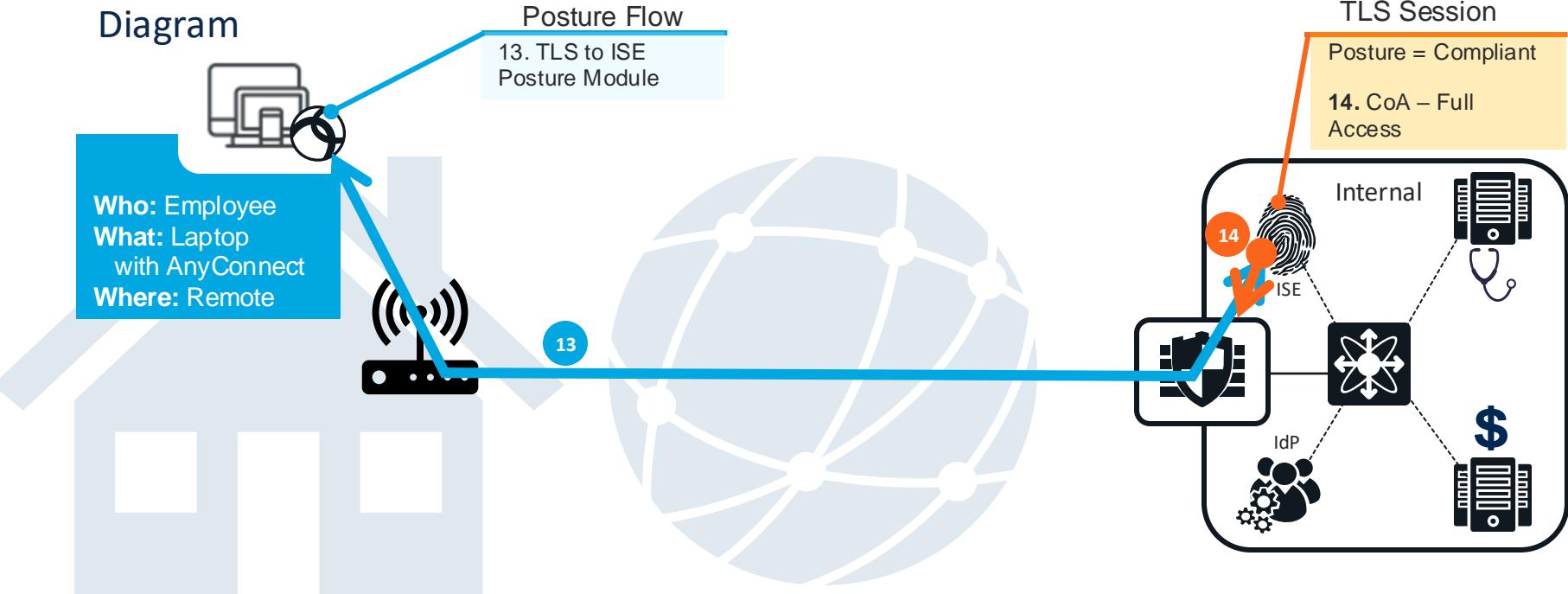
Diagram





Solution Overview

Diagram

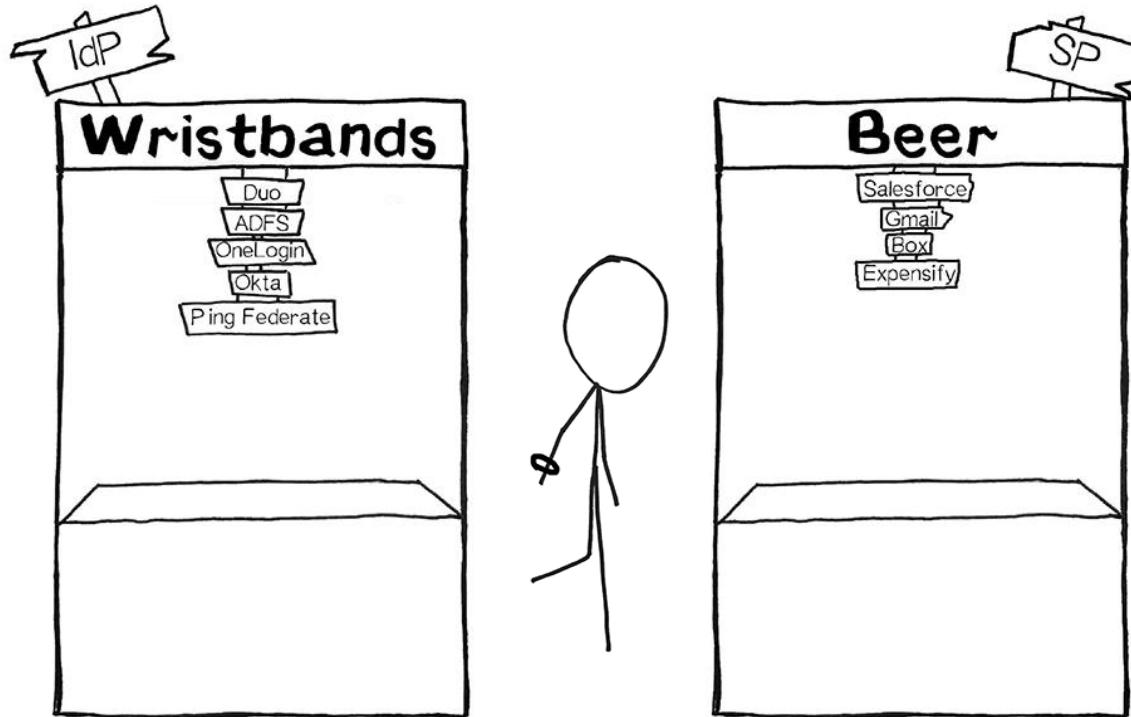


Solution Overview

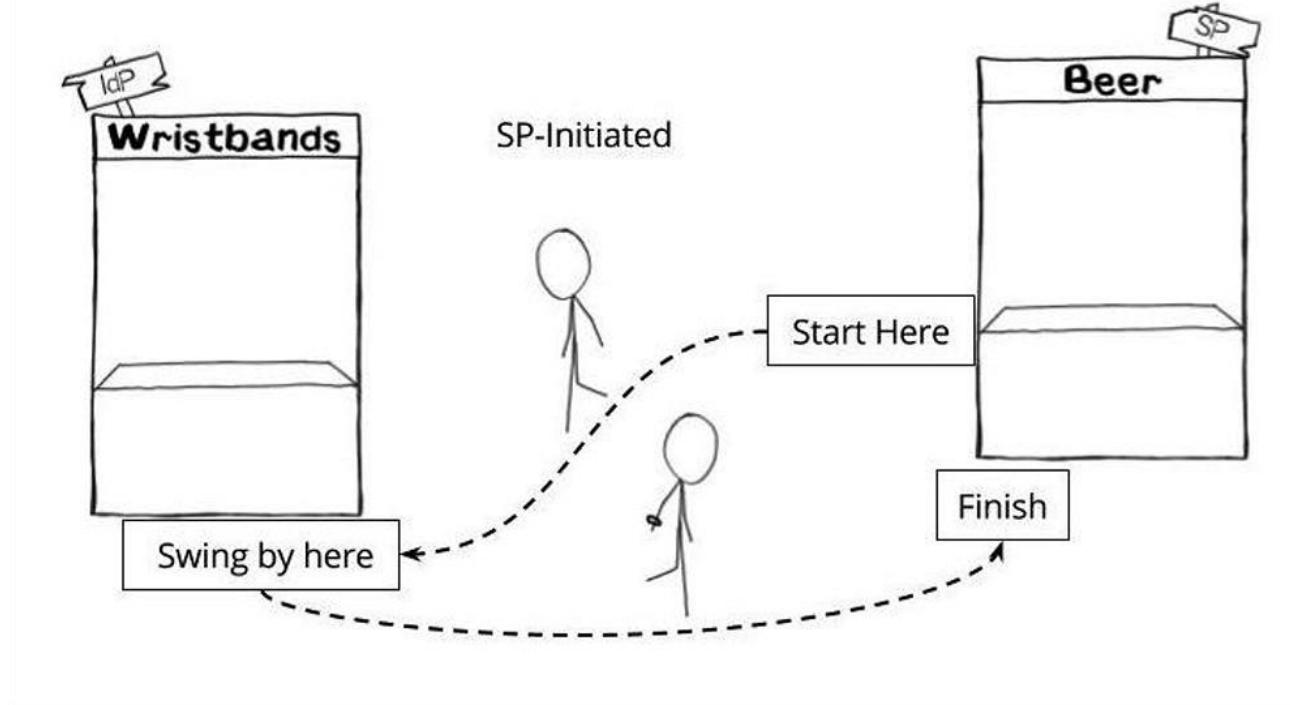
Diagram



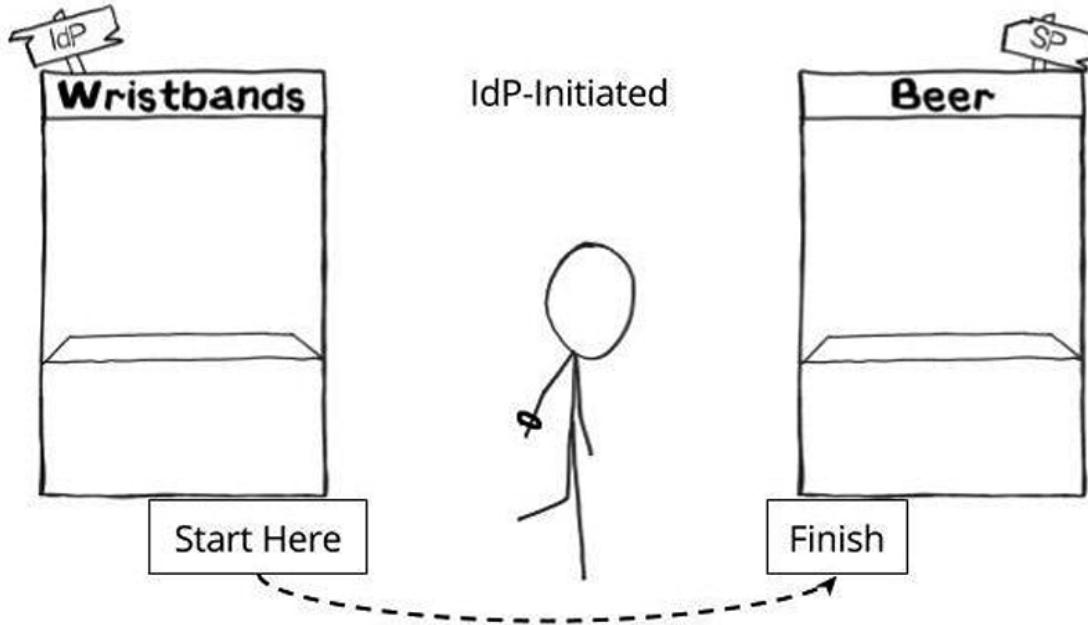
The Beer Drinker's Guide to SAML



The Beer Drinker's Guide to SAML



The Beer Drinker's Guide to SAML



IDP vs. SP Initiated Login

IdP Initiated Login

Centralized App Launch Location – end-user logs in to the central portal with SSO.

Clicks one of the tiles & is directed to the SP (application) with the token "in-hand".

Preferred when a simplified user-experience is desired w/ a single place to access all the applications.

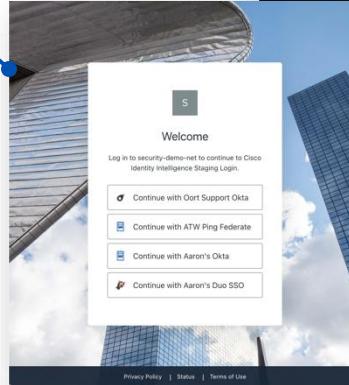
Examples: **Security Cloud Sign-on & Duo Central**

SP Initiated Login

Application triggered login – when logging into the application itself, the end-user is redirected to the IdP for authentication.

Examples: **CII & Webex**

CISCO Live!



The screenshot shows the Cisco Application Portal interface. At the top right are "Manage Devices" and "Logout" buttons. A search bar is at the top center. Below it is a grid of tiles representing different services:

- Ask Duo Anything
- Dashboard
- Brand & Marketing Assets
- Cisco Central
- Duo Enlighten
- Gatekeeper
- Lessonly [CiscoSecure]
- LEVEL UP
- Omi
- Omi [FAM]
- RingCentral
- slack

Below the tiles is a section titled "Welcome back, Aaron!" with a "Your applications" section showing "Security Provisioning and Administration" and a "Other applications" section listing various Cisco products like Cisco Cloudlock, Cisco Meraki, Cisco Umbrella, Secure Access, Secure Cloud Analytics, and Secure Workload.



For Your Reference



For Your
Reference

- **IDP-Initiated Login** is best for centralized access and is user-friendly for accessing multiple applications from one place.
- **SP-Initiated Login** offers more control to the SP and may provide a more contextual experience for users when accessing specific resources.
- The choice between the two often depends on the specific use case, organizational needs, and user experience considerations.



For Your
Reference

Example: Moving from RADIUS to SAML for SSO with VPN



FTD VPN SAML conversion



For Your
Reference

← → ⌂ admin-1a4ab80e.duosecurity.com/applications/DIG3UJWCDYARPJ6CTFKT

cisco DUO Search Account Duo Security Help Jeff Groesbeck

Applications FTD ravpn01 - Single Sign-On Authentication Log Remove Application

See the [Cisco Firepower SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Identity Provider Entity ID [Copy](#)

SSO URL [Copy](#)

Logout URL [Copy](#)

Downloads

Identity Provider Certificate [Download certificate](#) [Copy certificate](#) Expires: 01-19-2038

Service Provider

Cisco Firepower Base URL *

Enter the Cisco Firepower Base URL hostname.

Connection Profile Name *

Enter the Connection Profile Name you are protecting with SSO.

Sidebar:

- Collapse
- Home
- Users
- Devices
- Policies
- Applications
- Reports
- Monitoring
- Accounts
- Billing
- Settings

FTD VPN SAML conversion



For Your
Reference

cisco-tme-zerotrust.app.us.cdo.cisco.com/ddd/#ObjectManager

Defense Orchestrator
FMC / Objects / Object Management

Search Deploy jgroesbe@cisco.com

Home Analysis Policies Devices Objects Integration

AAA Server
RADIUS Server Group
Single Sign-on Server
Access List Address Pools Application Filters AS Path BFD Template Cipher Suite List Community List DHCP IPv6 Pool Distinguished Name DNS Server Group External Attributes File List FlexConfig Geolocation Interface Key Chain

Edit Single Sign-on Server

Name* Duo_SSC

Identity Provider Entity ID* https://sso-1a4ab80e.sso.duose...

SSO URL* https://sso-1a4ab80e.sso.duose...

Logout URL

Base URL https://ravpn01.zerotrustdemo.c...

Identity Provider Certificate* Duo_SSO_new

Service Provider Certificate 2024_star_zerotrustdemo_com

Request Signature --No Signature--

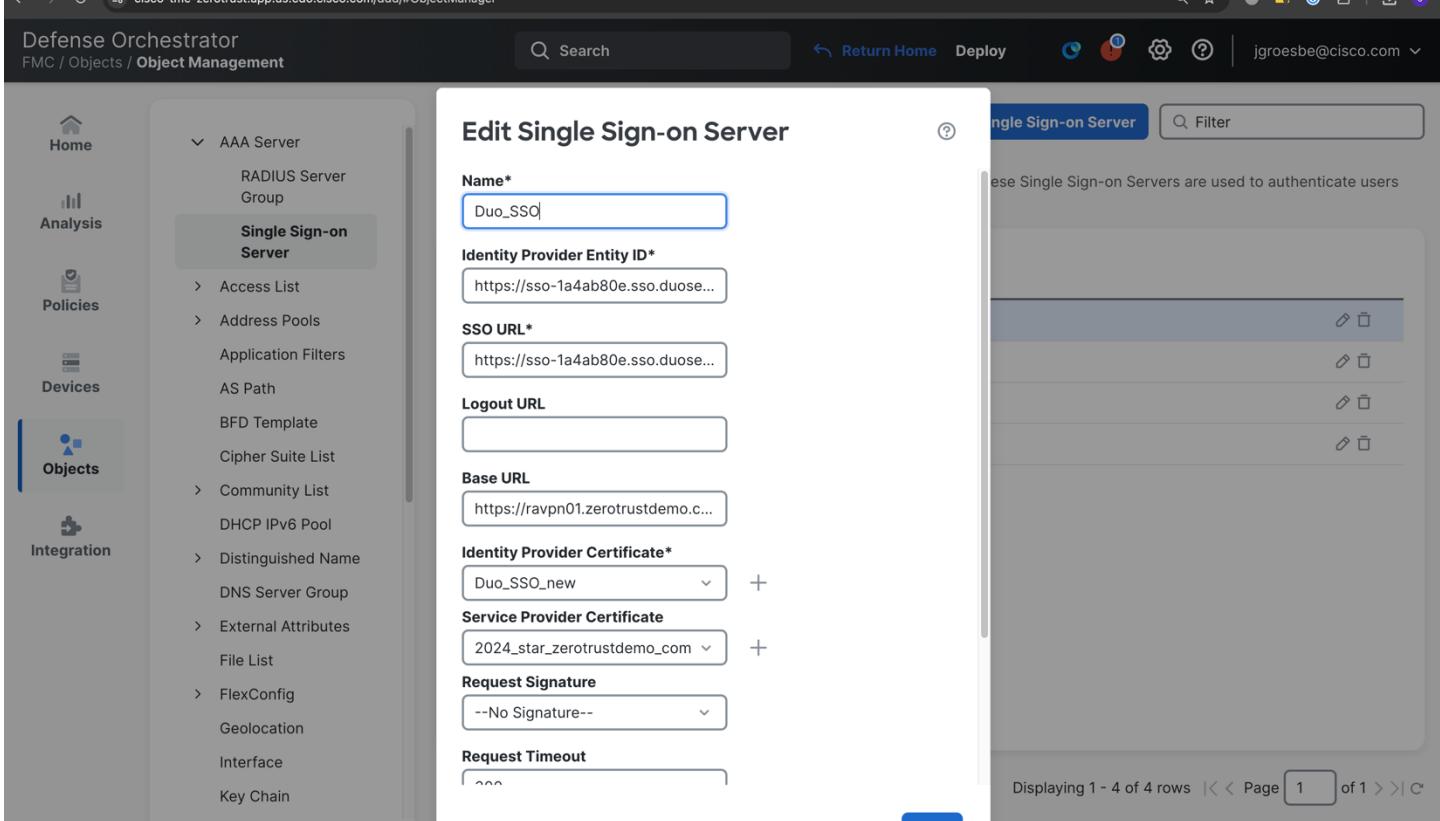
Request Timeout

Single Sign-on Server Filter

These Single Sign-on Servers are used to authenticate users

Displaying 1 - 4 of 4 rows |< < Page 1 of 1 > >| C

Cancel Save



FTD VPN SAML conversion



For Your
Reference

Defense Orchestrator
FMC / Objects / Object Management

Search | Return Home | Deploy | Help | jgroesbe@cisco.com

AAA Server
RADIUS Server Group
Single Sign-on Server
Access List
Address Pools
Application Filters
AS Path
BFD Template
Cipher Suite List
Community List
DHCP IPv6 Pool
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain

Edit Single Sign-on Server

Logout URL: https://sso-1a4ad8ue.sso.auose...

Base URL: https://ravpn01.zerotrustdemo.c...

Identity Provider Certificate*: Duo_SSO_new

Service Provider Certificate: 2024_star_zerotrustdemo_com

Request Signature: ~No Signature--

Request Timeout: 300 seconds (1-7200)

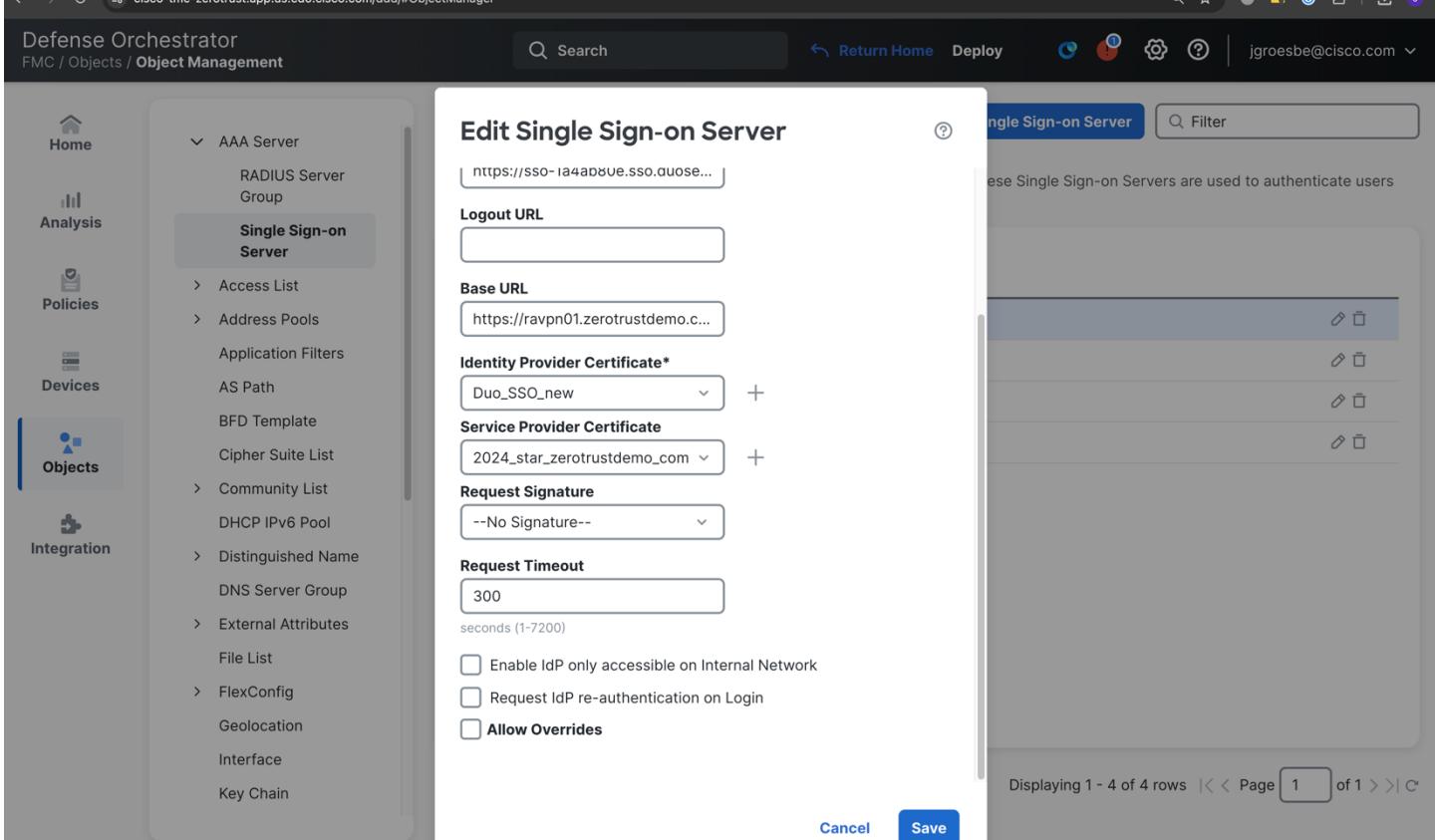
Enable IdP only accessible on Internal Network

Request IdP re-authentication on Login

Allow Overrides

Displaying 1 - 4 of 4 rows | < < Page 1 of 1 > > | C

Cancel Save



FTD VPN SAML conversion



For Your
Reference

cisco-tme-zerotrust.app.us.cdo.cisco.com/ddd/#RaVpnEditConnProfile;uuid=0EDBD69E-1DD7-0ed3-0000-004294969103;type=RA.VPNH.VPN

Defense Orchestrator

FMC / Devices / VPN / Edit Connection Profile

Edit Connection Profile

Connection Profile: **ravpn**

Group Policy: **DfltGrpPolicy**

Client Address Assignment: **AAA** Aliases

Authentication

Authentication Method: **SAML**

Authentication Server: **Duo_SSO (SSO)**

Override Identity Provider Certificate

VPN client embedded browser

Default OS Browser

Authorization

Authorization Server: **ise-authz (RADIUS)**

Allow connection only if user exists in authorization database

Save Cancel

Policy Assignments (1)
Dynamic Access Policy: None

Devices

- DefaultWEBVPNGroup
- ravpn**
- ravpn-ise
- ravpn-cert



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



Open Authorization (OAuth)

OAuth 2.0 is a security standard where you give one application permission to access your data in another application

v2 is most used, v1 still exists in the wild...

Open Authorization v2 (OAuth2)

- Open Standard
 - Token exchange protocol
 - Designed for **application to application**, authorized by a user.
 - User authorizes the application.
 - IdP issues a token (JSON Web Token [JWT]) to the app
 - Allows the app to make API calls on behalf of the user.



Key Concepts of OAuth

OAuth deals with authorization.

- **User Initiates:** A user wants to connect their account from one service (e.g., Twitter) to another (e.g., a third-party app).
- **Redirect to Provider:** The app redirects the user to the service provider's site (e.g., Twitter's login page).
- **Consent:** The user logs in and is asked to approve the app's request for specific data or actions.
- **Authorization Code:** If approved, the service provider gives the app an authorization code.
- **Token Exchange:** The app uses this code to get an access token from the service provider.
- **Access:** The app can now access the user's data or perform actions on their behalf using this token.

- **Tokens:**

- **Access Token:** Accesses the user's resources. The app uses it in API calls.
- **Refresh Token:** Gets a new access token when the current one expires, without needing user interaction again.

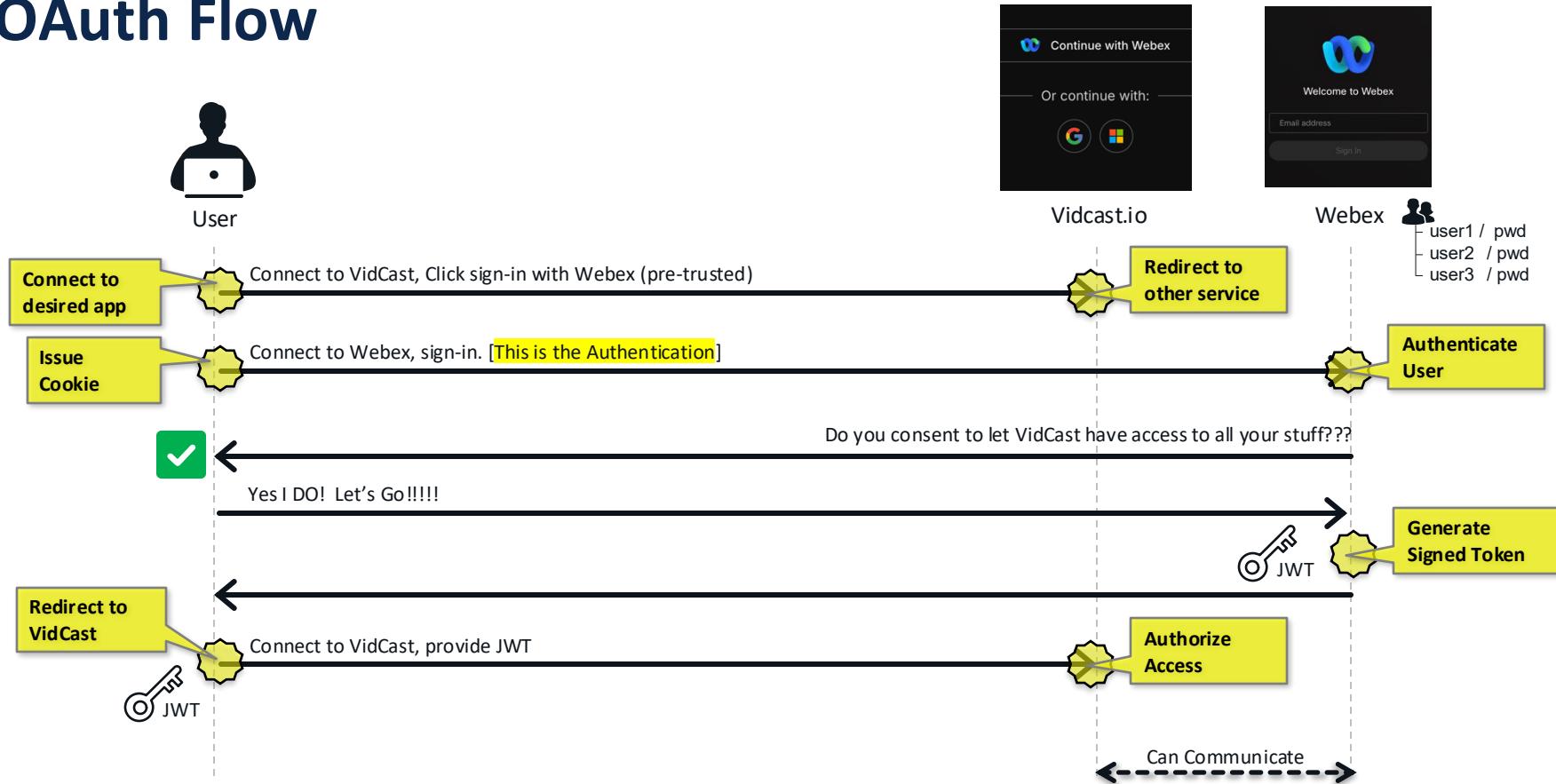
- **Advantages:**

- **Security:** Users don't share their passwords with third-party apps.
- **Flexibility:** Services can grant limited, revocable permissions.
- **User Control:** Users can see and revoke permissions at any time.

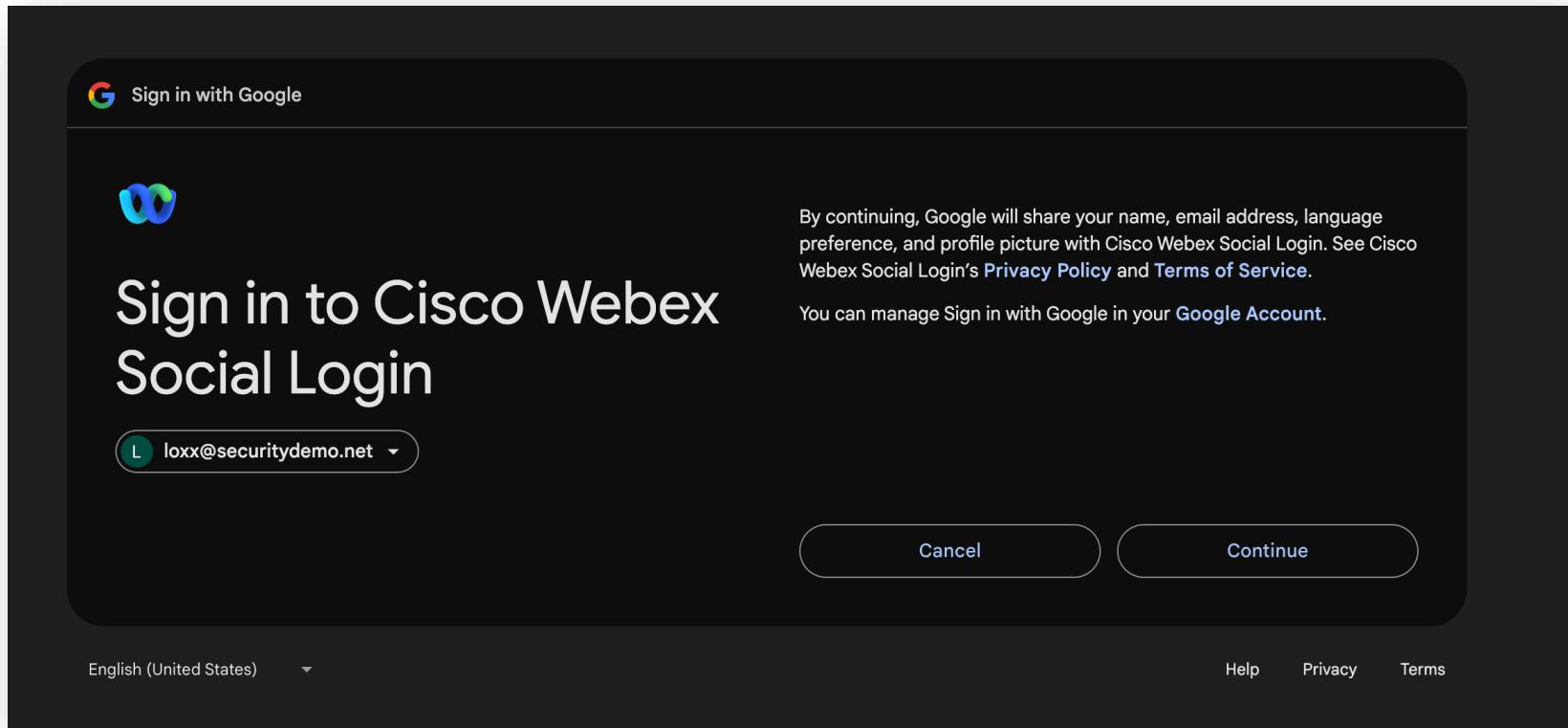
- **Versions:**

- **OAuth 1.0:** Introduced the basic framework but was complex and included cryptographic signing.
- **OAuth 2.0:** Simplified the process, removed the need for cryptographic signing in most flows, and introduced different grant types (like authorization code, implicit, resource owner password credentials, client credentials).

OAuth Flow



Example of Consent



The image shows a dark-themed web browser window displaying a Cisco Webex Social Login consent screen. At the top left is a "Sign in with Google" button with the Google logo. Below it is a Cisco logo. The main title "Sign in to Cisco Webex Social Login" is centered. A user email "loxx@securitydemo.net" is shown in a dropdown menu. To the right, text explains that by continuing, Google will share name, email, language preference, and profile picture with Cisco Webex Social Login, linking to its Privacy Policy and Terms of Service. It also mentions managing sign-in via Google Account. At the bottom are "Cancel" and "Continue" buttons. The footer includes language selection ("English (United States)"), and links for Help, Privacy, and Terms.

Sign in with Google

Sign in to Cisco Webex Social Login

loxx@securitydemo.net

By continuing, Google will share your name, email address, language preference, and profile picture with Cisco Webex Social Login. See Cisco Webex Social Login's [Privacy Policy](#) and [Terms of Service](#).

You can manage Sign in with Google in your [Google Account](#).

Cancel Continue

English (United States) ▾

Help Privacy Terms



Open ID Connect (OIDC)

OIDC is a thin layer that sits **on top** of OAuth 2.0 to add login and profile information about the user into the exchange. This transforms the exchange to add **authentication** to OAuth2's authorization!

OIDC is now an alternative to
SAML for SSO.

OAuth is App to App AuthZ.



Open ID Connect

- Wraps a framework around OAuth2 for user login, making it more appropriate for user single-sign-on.

OIDC Glossary

Relying Party - This is the application that Lee is logging into! It is the same as a Service Provider in SAML.

Resource Owner - This is Lee! Lee owns their identity, data, and controls actions performed on their account.

Client - The application that wants to access data or perform actions on behalf of the Resource Owner.

Authorization Server - An application that knows the Resource Owner and where the Resource Owner already has an account. This is called an *OpenID Provider* in OIDC!

Resource Server - An API or service that the client wants to use on behalf of the resource owner. This will sometimes be the same provider as the Authorization Server

OIDC Glossary

Redirect URI- Sometimes called the “Callback URL”, this is the URL that the Authorization Server will redirect the Resource Owner to after granting permission to the client.

Response Type - The type of information that the client expects to receive. The most common is “code”

Scope - The granular permissions that the client wants. These can be authorization-oriented (access to data or to perform actions) or identity-oriented.

Consent - The Authorization Server verifies with the Resource Owner that they would like to give the client the permission to use the scopes.

OIDC Glossary

Client ID - An ID that verifies the identity of the Client with the Authorization Server

Client Secret - A password that is shared between the Client and Authorization Server

Authorization Code- A temporary code the Client gives the Authorization Server in exchange for an Access Token

Access Token - A key that gives Client permission to request data or perform actions with the Resource Server on your behalf.

ID Token - A JSON Web Token or JWT that contains information about you, the Resource Owner, such as your name, ID, manager, or pretty much anything else in your user profile.

Claim - This is data in the ID Token! These will be AD or SAML IdP attribute:value pairings.



OIDC compared to SAML

- SAML is older than OIDC.
- SAML transmits user attributes using XML format and browser redirects, while OIDC uses JSON format and communicates directly from the client application to the OpenID Provider.
- OIDC enables complete machine-to-machine authentication.
- OIDC is considered to be more secure*
 - *Depending on which grant type is being used

Which should you choose?

- Often won't have a choice as not many application vendors implement both!
- OIDC is being increasingly common for new integrations.

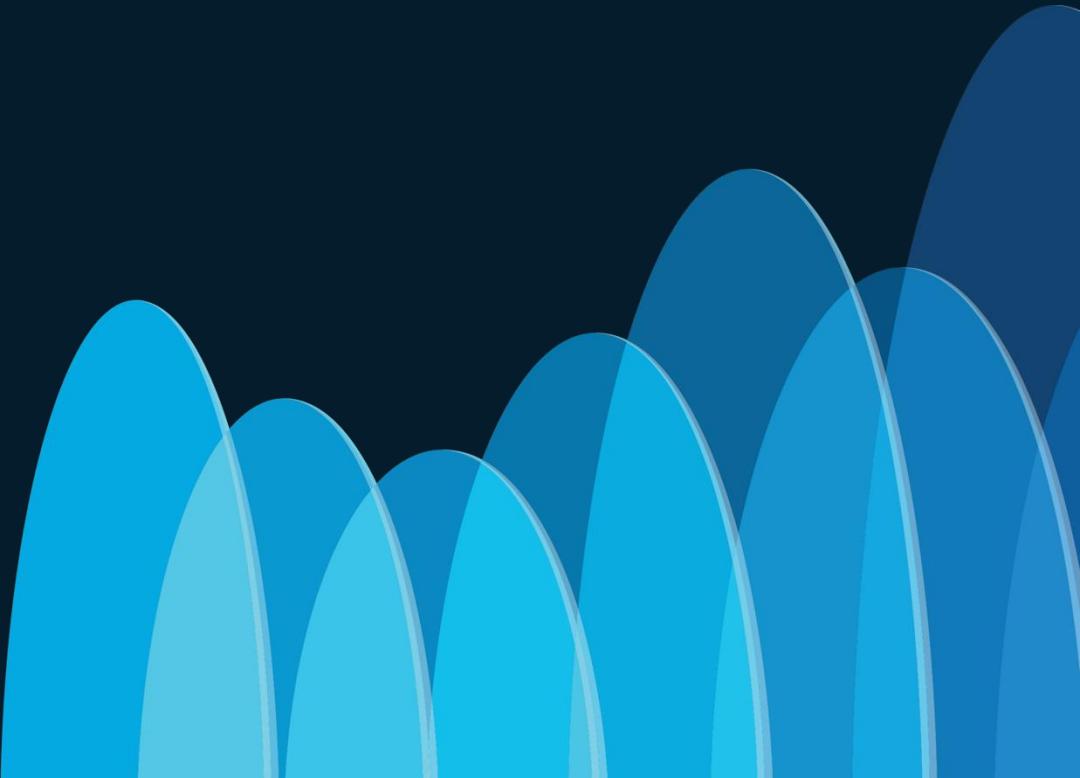


Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



Web Authentication (WebAuthN)



Web Authentication (WebAuthN)

- An API websites use to talk to web browsers
- An API spec for accessing public key credentials
- Developed by FIDO Alliance, ratified by the W3C
- Manages both registration and authentication
- Can be used for primary or secondary authentication

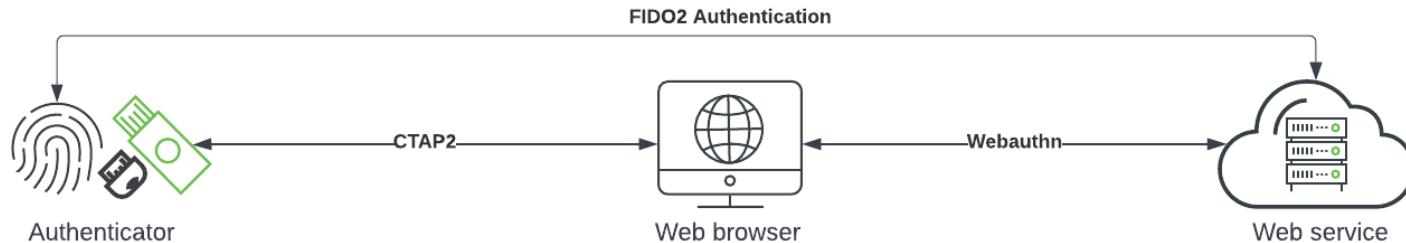


WebAuthn.io

FIDO2 Authentication



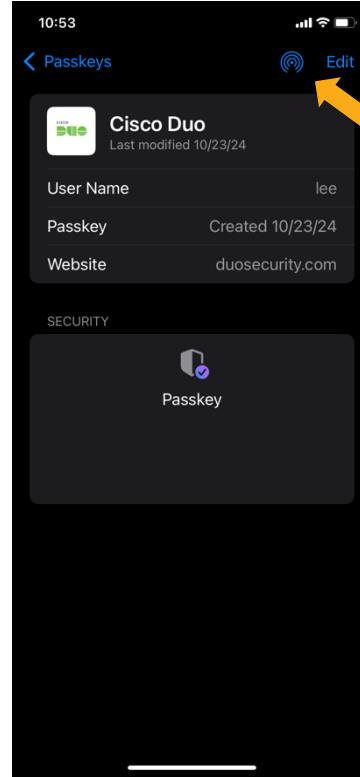
- Developed by FIDO alliance
- WebAuthN + Client to Authenticator Protocol v2 (CTAP2)
- CTAP: API for browser to authenticator communication
- Can be used for MFA or password-less



Passkeys

- Passkeys are essentially just a new (and easier) name for WebAuthn + FIDO2 credentials
- Passkeys, however, don't have to just be device bound
- Shared passkeys make things a whole lot easier for end users
 - Credentials can be synced using secure methods (icloud keychain/passwords app, Google password manager, etc)
- There 'may' be security concerns with sharing.... Think personal icloud account across possibly work AND personal device
- AND...

Shared Passkeys



Airdrop!

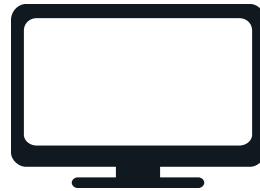
To ANYONE!

Authentication

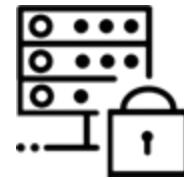
Authenticator



Browser



Web Server

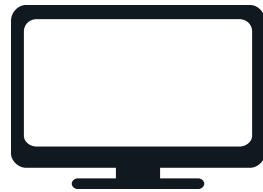


Authentication : Send User Info

Authenticator



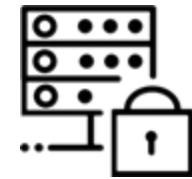
Browser



User Bob



Web Server

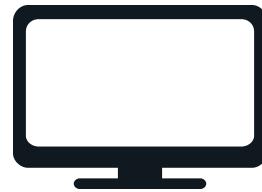


Authentication : Challenge

Authenticator

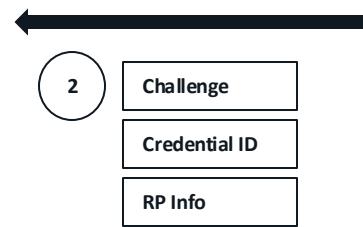
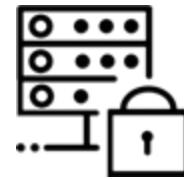


Browser



User Bob

Web Server

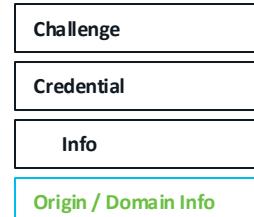


Authentication : Challenge + Domain

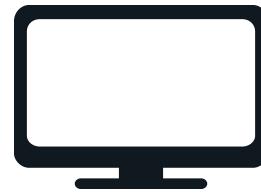
Authenticator



3

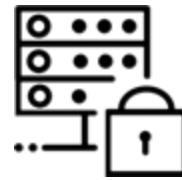


Browser



User Bob

Web Server

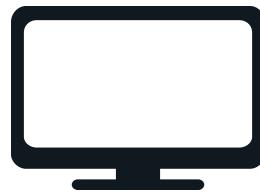


Authentication : User Verification

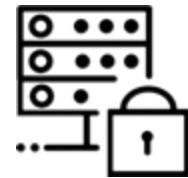
Authenticator



Browser



Web Server



CISCO Live!

4

User Verification

Perform Biometric

Security Key Gesture

Mobile Push

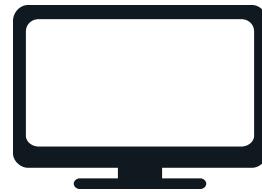


Authentication : User Verification & Assertion

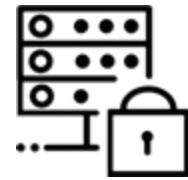
Authenticator



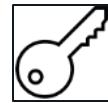
Browser



Web Server



Signed Assertion



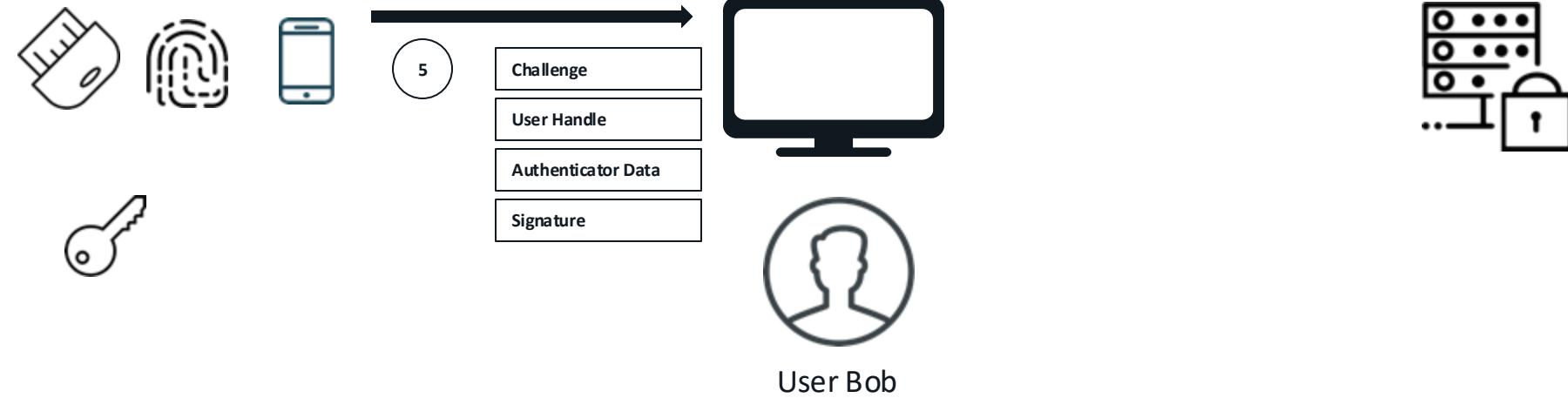
User Bob

Authentication : Authenticator Assertion

Authenticator

Browser

Web Server

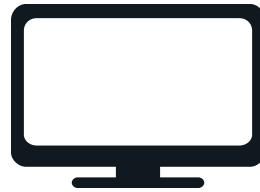


Authentication : Challenge Response

Authenticator

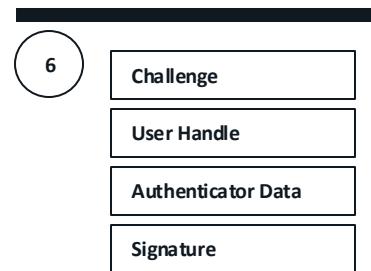


Browser



User Bob

Web Server

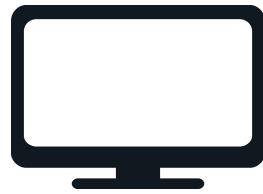


Authentication : Success!

Authenticator



Browser



User Bob

Web Server



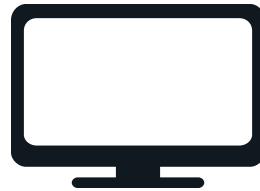
7

Advantages of WebAuthn : Asymmetric Cryptography

Authenticator



Browser



Web Server



Private Key

Authentication leverages an asymmetric key pair.

Anyone can have the public key, while the private key is never sent or shared.

Asymmetry means more security!



User Bob

Advantages of WebAuthn : Phishing

Authenticator



Browser



Web Server



Private Key



No password used during the authentication experience.

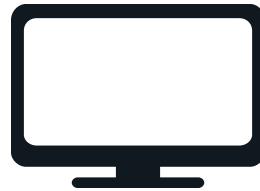
You can't phishing credentials if they aren't used at login!

Advantages of WebAuthn : Man In the Middle

Authenticator



Browser



Web Server



The Private Key never leaves the authenticator.

User Bob verifies identity to unlock the Private Key at auth time.

Meaning there is no sensitive information transferred that can be intercepted.

You can't steal information that isn't being sent!



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



Gotcha's (it's not all Sunshine & Roses)

BACK IN MY DAY



imgflip.com

RADIUS DID IT ALL

Long Live the King: RADIUS

- With RADIUS: there was structure:
- Attribute Value Pairs (AVPs)
 - i.e.: User-Name: [username]
 - The RADIUS server knew what to expect
 - It could be extended with Vendor Specific Attributes (VSAs).

```
▽ Attribute Value Pairs
▷ AVP: l=24 t=User-Name(1): host/winxp.example.com
▷ AVP: l=6 t=Service-Type(6): Framed(2)
▷ AVP: l=6 t=Framed-IP-Address(8): 192.168.2.100
▷ AVP: l=6 t=Framed-MTU(12): 1500
▷ AVP: l=19 t=Called-Station-Id(30): 00-1A-A2-7E-7F-03
▷ AVP: l=19 t=Calling-Station-Id(31): 00-16-D4-2E-E8-BA
▷ AVP: l=89 t=EAP-Message(79) Last Segment[1]
▷ AVP: l=18 t=Message-Authenticator(80): 1a71a57045f7ea6
▷ AVP: l=2 t=EAP-Key-Name(102):
▷ AVP: l=49 t=Vendor-Specific(26) v=Cisco(9)
▷ AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
▷ AVP: l=6 t=NAS-Port(5): 50001
▷ AVP: l=17 t=NAS-Port-Id(87): FastEthernet0/1
▷ AVP: l=74 t=State(24): 333743504d53657373696f6e49443d4
▷ AVP: l=6 t=NAS-IP-Address(4): 192.168.1.60
```

SAML / OAuth

- SAML & OAuth: part of the Token but can have many different schemas
- Must program each side to know what field is
- Dictate the schema via URL
 - Ex: Use “email” as username
 - Defined in the metadata

! – Example: XDR UI App OAuth Token

```
{  
    "https://schemas.cisco.com/iroh/identity/claims/user/email": "loxx@securitydemo.net",  
    "https://schemas.cisco.com/iroh/identity/claims/user/idp/id": "sxso",  
    "https://schemas.cisco.com/iroh/identity/claims/user/nick": "Aaron Woland",  
    "email": "loxx@securitydemo.net",  
    "aud": [  
        "iroh-ui",  
        "login"  
    ],  
    "https://schemas.cisco.com/iroh/identity/claims/user/role": "admin",  
    "sub": "9992027f-a88b-4b0e-8a38-58ad317c58af",  
    "iss": "IROH Auth",  
    "https://schemas.cisco.com/iroh/identity/claims/scopes": [  
        "event:read",  
        "cisco/feature-flag/xdr",  
        "insights",  
        "vault/configs:read",  
        "integration",  
        "private-intel",  
        "admin",  
        "profile",  
        "inspect",  
        "asset",  
        ! - SNIP  
        "ao"  
    ],  
    "exp": 1731003921,  
    "https://schemas.cisco.com/iroh/identity/claims/oauth/client/name": "Threat Response",  
    "https://schemas.cisco.com/iroh/identity/claims/oauth/user/id": "9992027f-a88b-4b0e-8a38-58ad317c58af",  
    "https://schemas.cisco.com/iroh/identity/claims/org/id": "2e0e9eaf-eaf7-4449-9c07-9fb1828aec78",  
    "https://schemas.cisco.com/iroh/identity/claims/oauth/grant": "login",  
    ! - SNIP  
}
```

Lack of Standards / Easy Behaviors

Example is Auth0, a CIAM

Integrating to a SAML IdP, it requires me to write this mapping out manually.

- Define which schema to figure out email.
- Define which attribute to use to find groups.

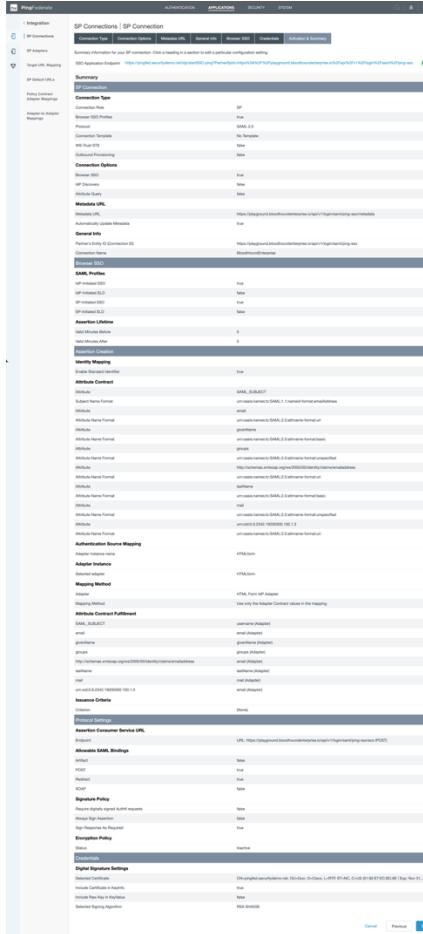
The screenshot shows the 'Mappings' tab of the Auth0 SAML configuration for 'Aaron's Duo SSO'. It displays a JSON code block for mapping user attributes:

```
1  {
2    "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
3    "groups": "memberOf"
4 }
```

Below the code, there is a 'Save Changes' button.

Lack of Standards / Easy Behaviors

- Can get REALLY complex
 - This shows a powerful, but complex IDP
 - Each & everything is customizable
 - There aren't really any preconfigured drop downs, etc..



Lack of Standards / Easy Behaviors

Some Vendors try to make it easier
(ahem: Duo)

- Supported schemas are selectable via a drop down.

Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

SAML Response

NameID format *

urn:oasis:names:tc:SAML:1:1:nameid-format:emailAddress

The format that specifies how the NameID is sent to the service provider.

NameID attribute *

<Email Address>

NameID is a SAML attribute that identifies the user. Enter an IdP attribute or select a bridge attribute that automatically chooses the NameID attribute based on the IdP. Create custom <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name>.

Signature algorithm *

SHA256

Signature encryption algorithm used in the SAML assertion and response.

Signing options *

Sign response
 Sign assertion

Choose at least one option for signing the SAML response. Your service provider will use these to verify the response's authenticity.

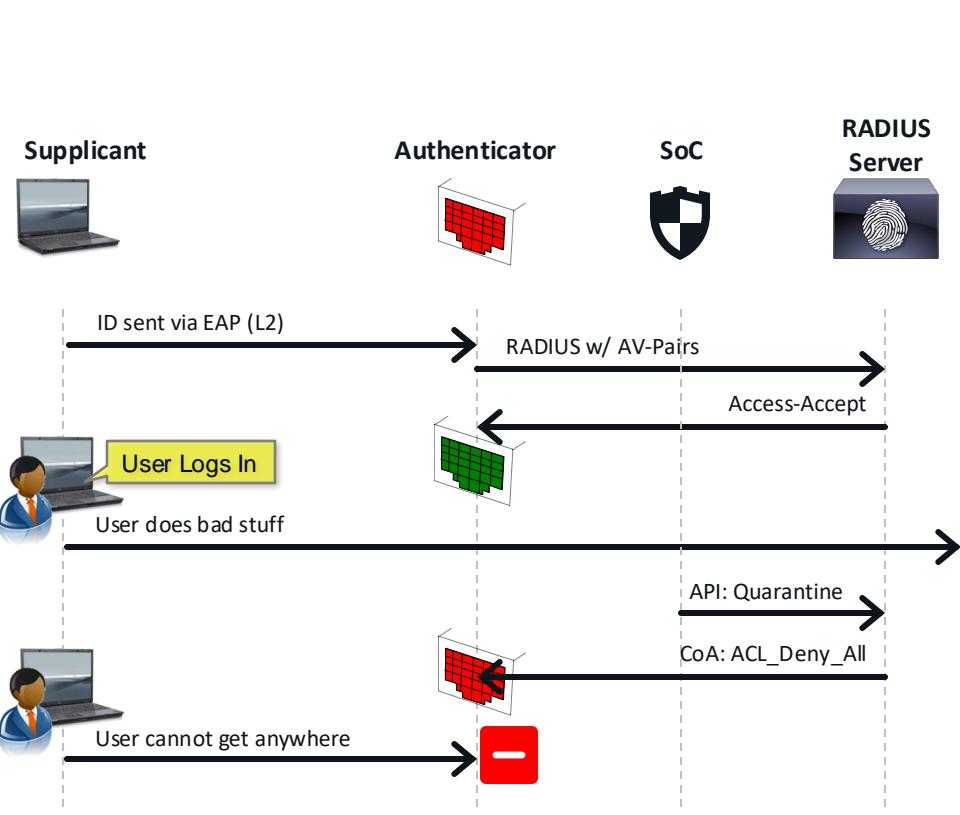
Assertion encryption

Encrypt the SAML assertion

Change of Authorization (CoA)

Described in **RFC 3576** and its successor **RFC 5176**

- Allows RADIUS server to disconnect or force other change in the authorization status of a user/endpoint.
 - Disconnect
 - Port-bounce
 - Re-Authenticate
 - Apply ACL



Continuous Authorization Evaluation Protocol (CAEP)

- Designed for real-time access control adjustments
 - i.e: Change of Authorization
- Meant to overcome the AuthN once & AuthZ until token expires problem

Shared Signals

- Enables sharing of security-related information across different services or systems
 - Kind of like STIX, but not.
 - Because we have to re-invent everything in Web AAA
- Used with CAEP for identity-related security events

Requires Human Interaction

- SAML, OAuth & OIDC
 - Are interactive
 - Require someone to click objects, or input usernames to obtain the token.
 - Makes coding scripts more tricky
 - Think: Python script to automate certain actions
 - Once you have the Token it's easy, but how do you get it via script?



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



Identity's Future is
so bright, it needs
shades!



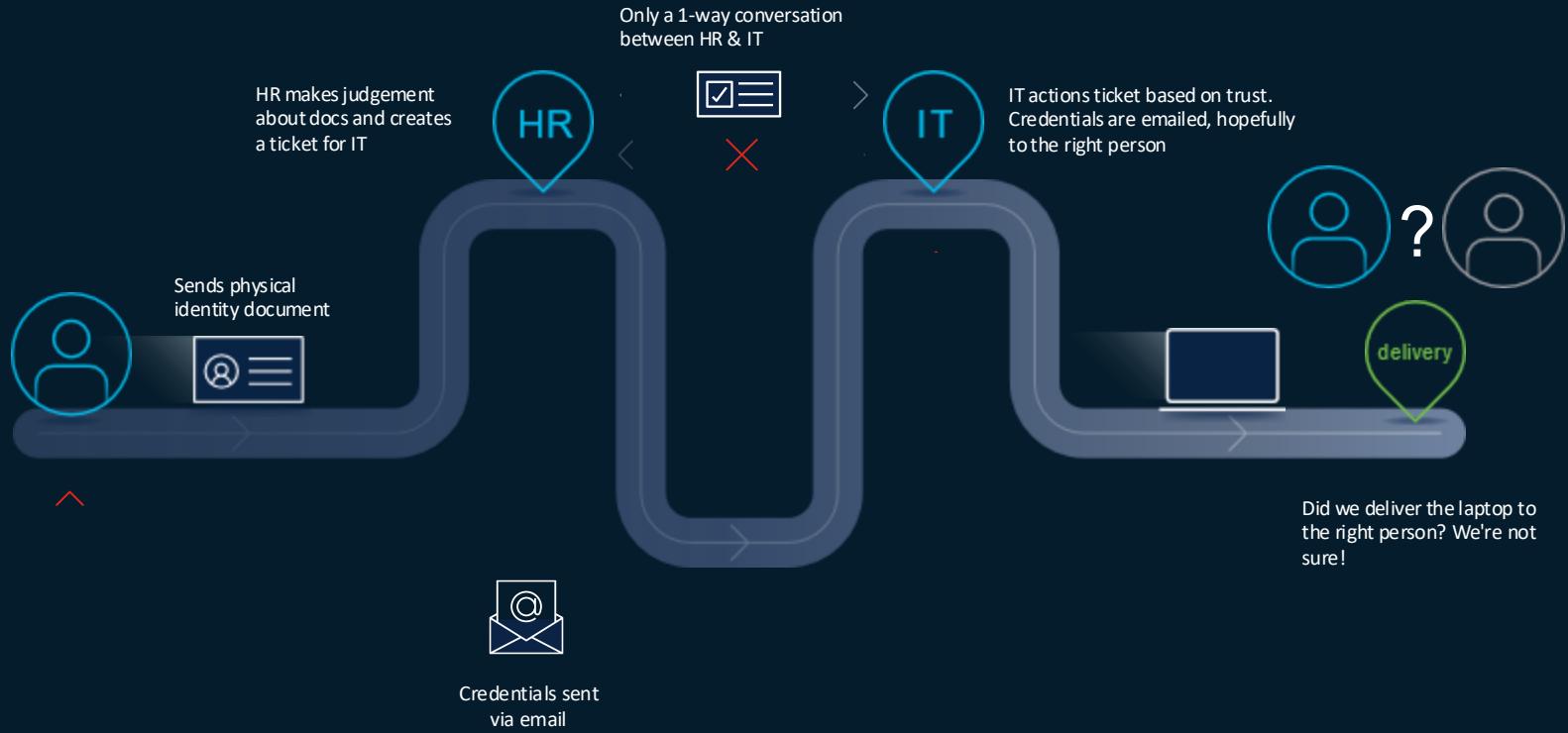
Verifiable Credentials – Why?

A series of overlapping, translucent blue shapes resembling waves or petals, positioned in the lower right corner of the slide.

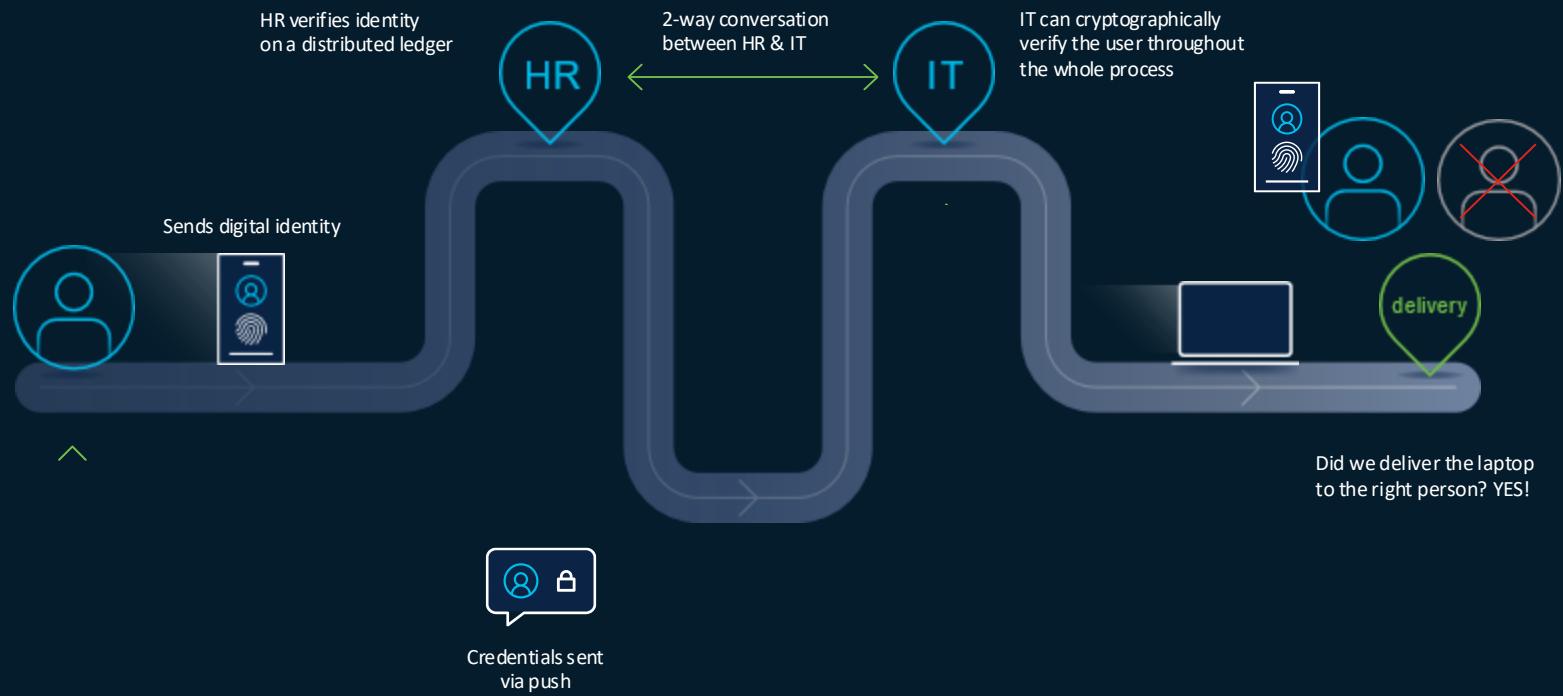
“The electric light did not come from the continuous improvement of candles.”

• Oren Harari

Jill onboards at ACME - Today



Jill onboards at ACME - Tomorrow



digitalcreds-duo1.duo.test/digitalcredsserv/info-collection-trigger

6jan golang rust Two application sh... ipc kafka opa general concepts frontend Duo Central duo-dev swift interview posture PoC Verified-Creds

 HR Page

Create Candidate Info Collection link

Employers enter details from Resume and creates a link which is shared with the Candidates who shares the ID proof that matches.

First Name

Last Name

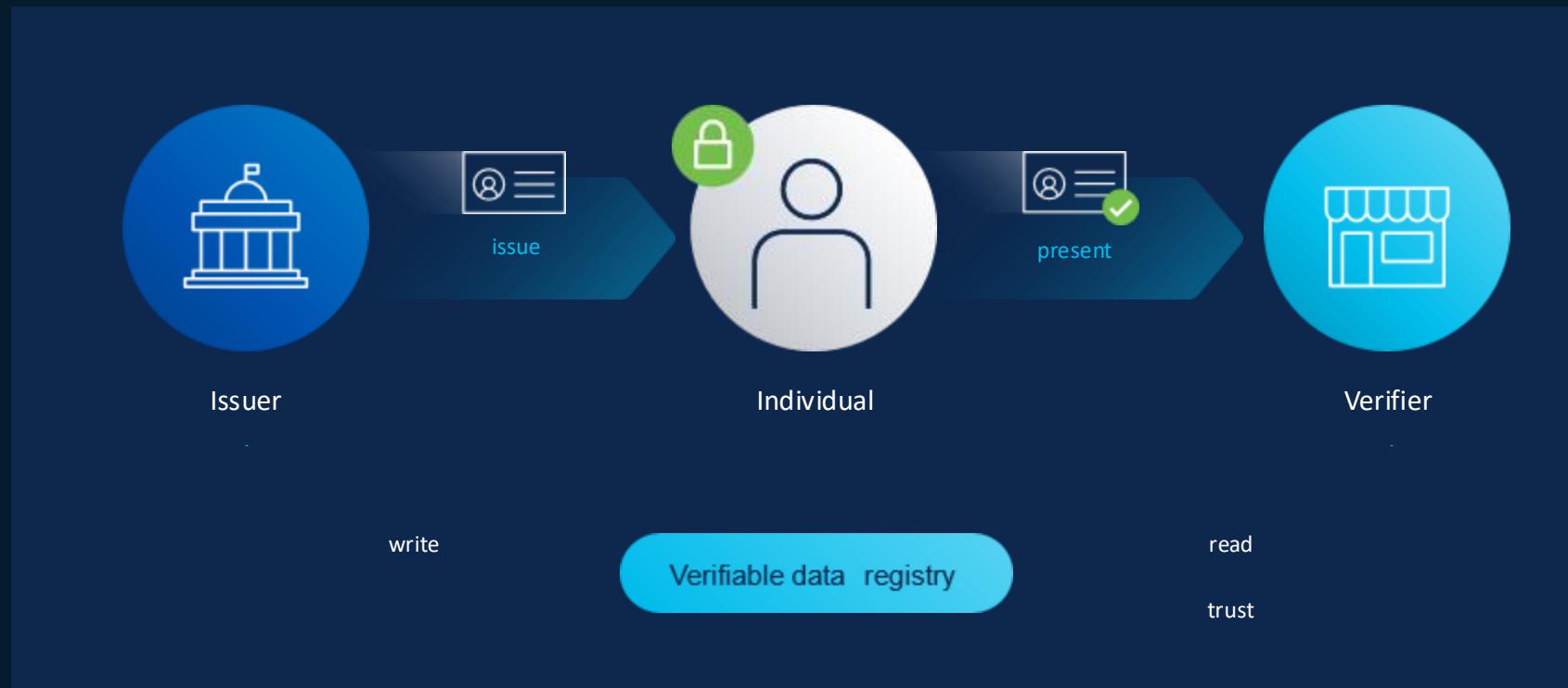
Email

Trigger Digital Credentials collection

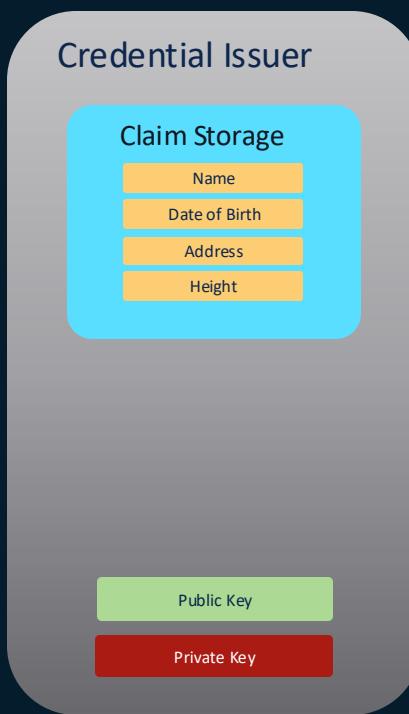
Secured by Duo

Verifiable Credentials – What?

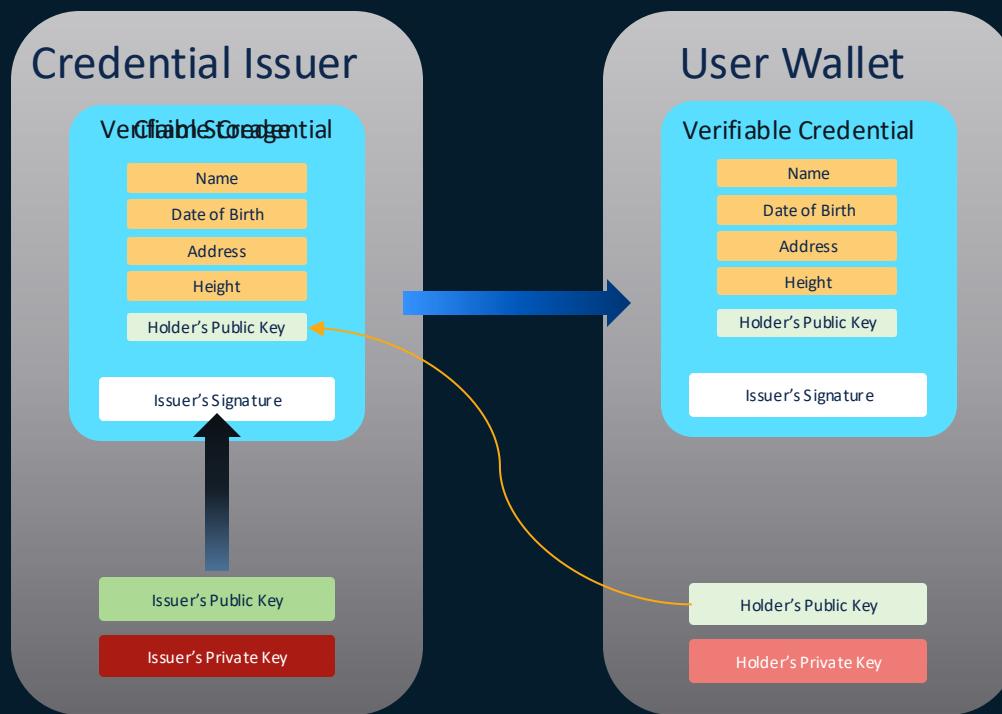
Verifiable Identity- High level flow diagram



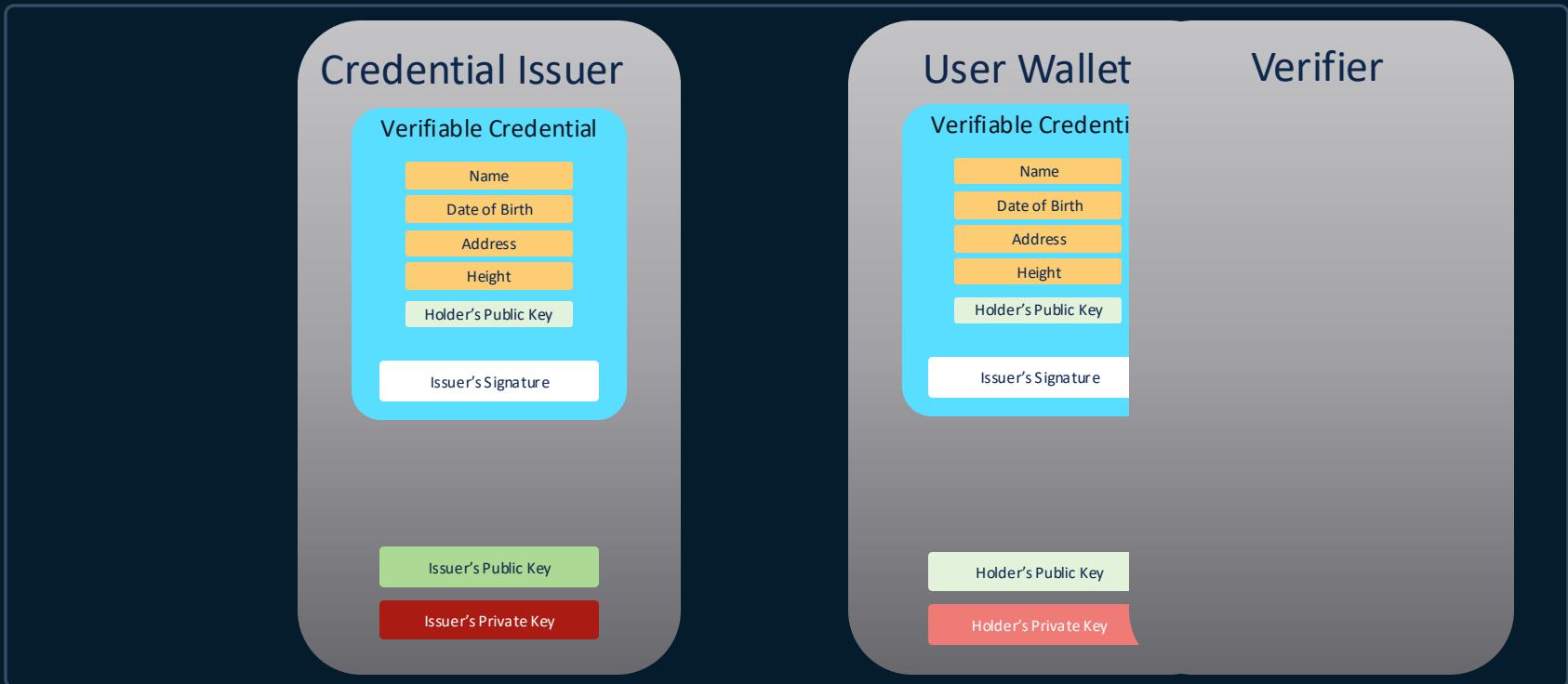
Credential Verification – How does it work?



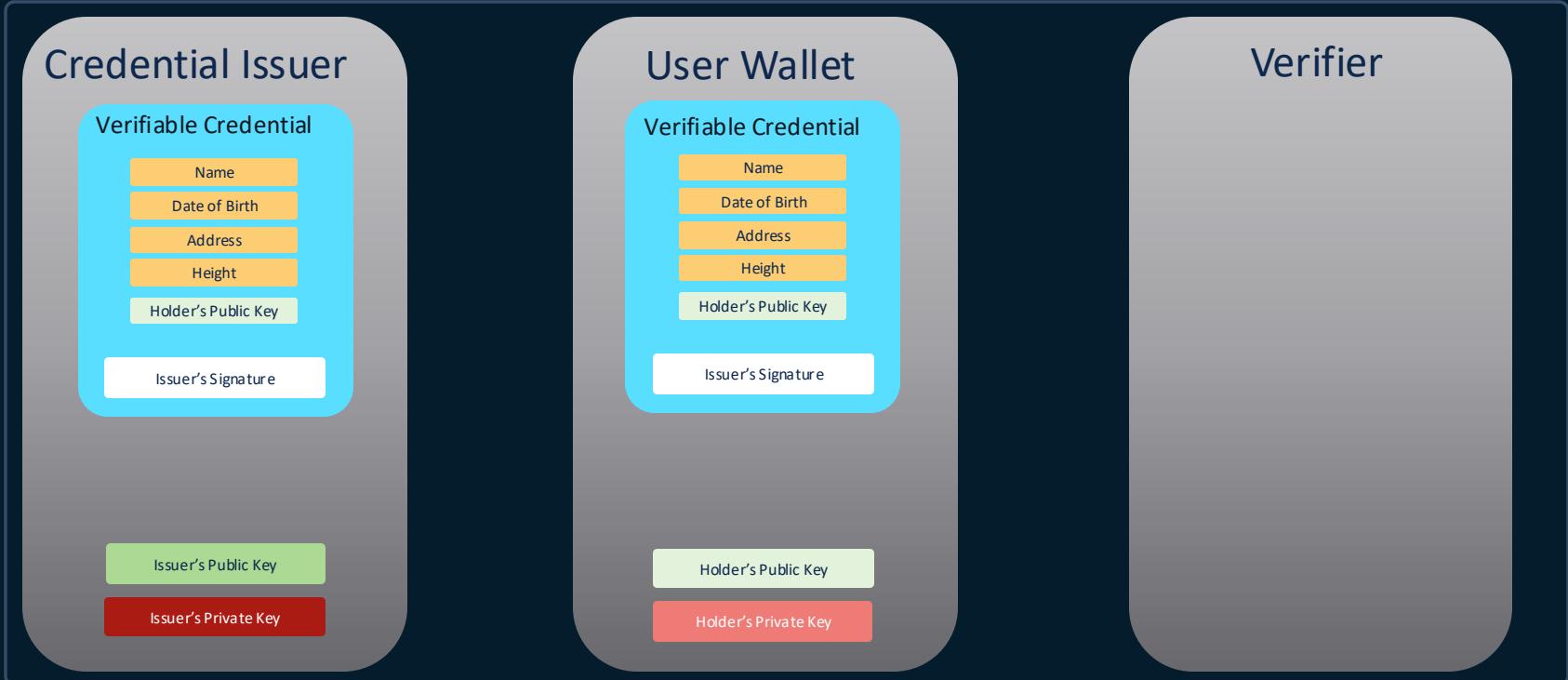
Credential Verification – Issuance



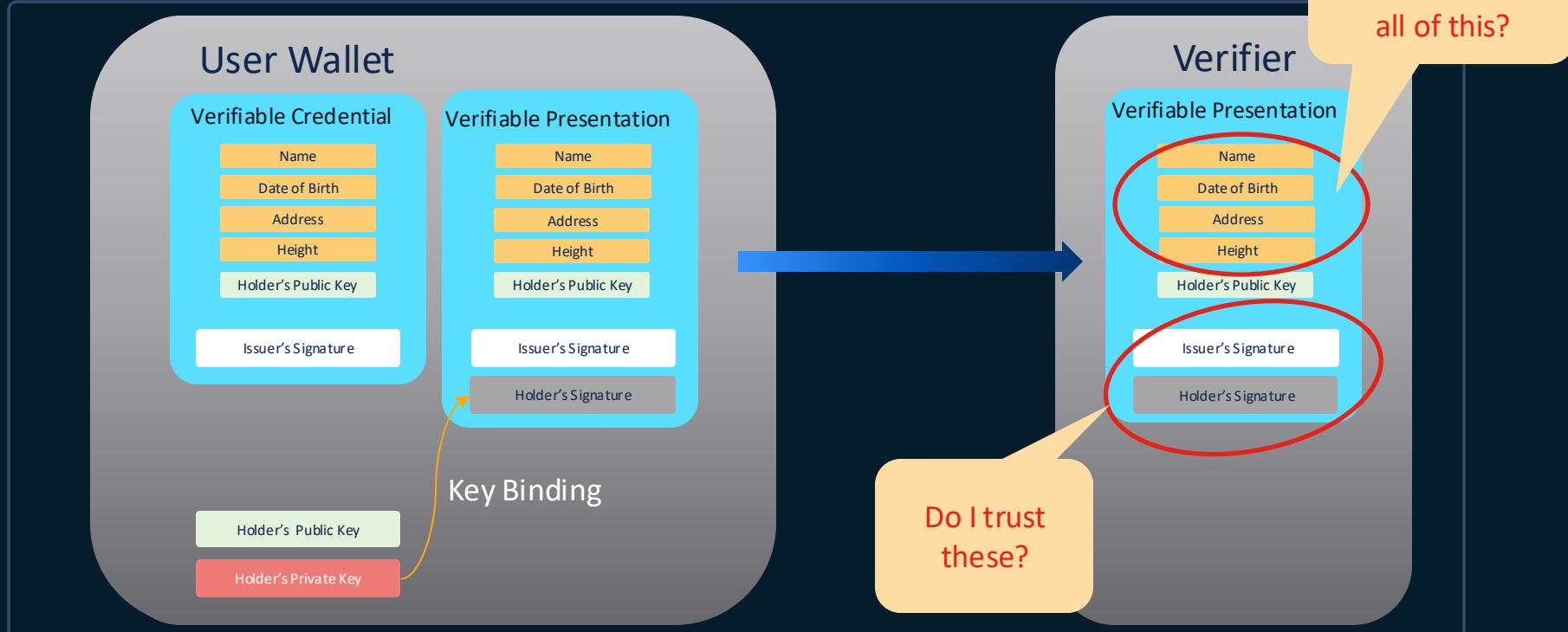
Credential Verification – Issuance



Credential Verification – Presentation



Credential Verification – Presentation



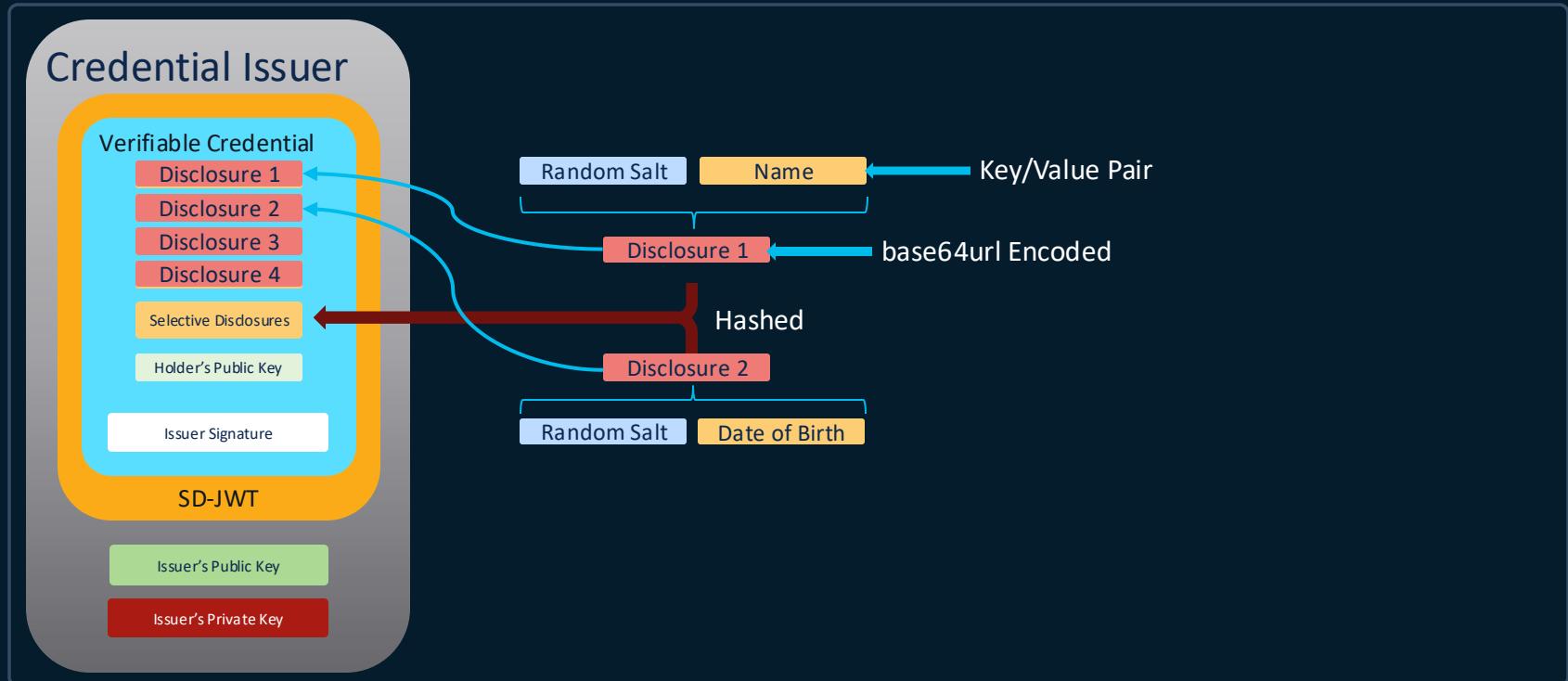


Credential Verification – Selective Disclosure



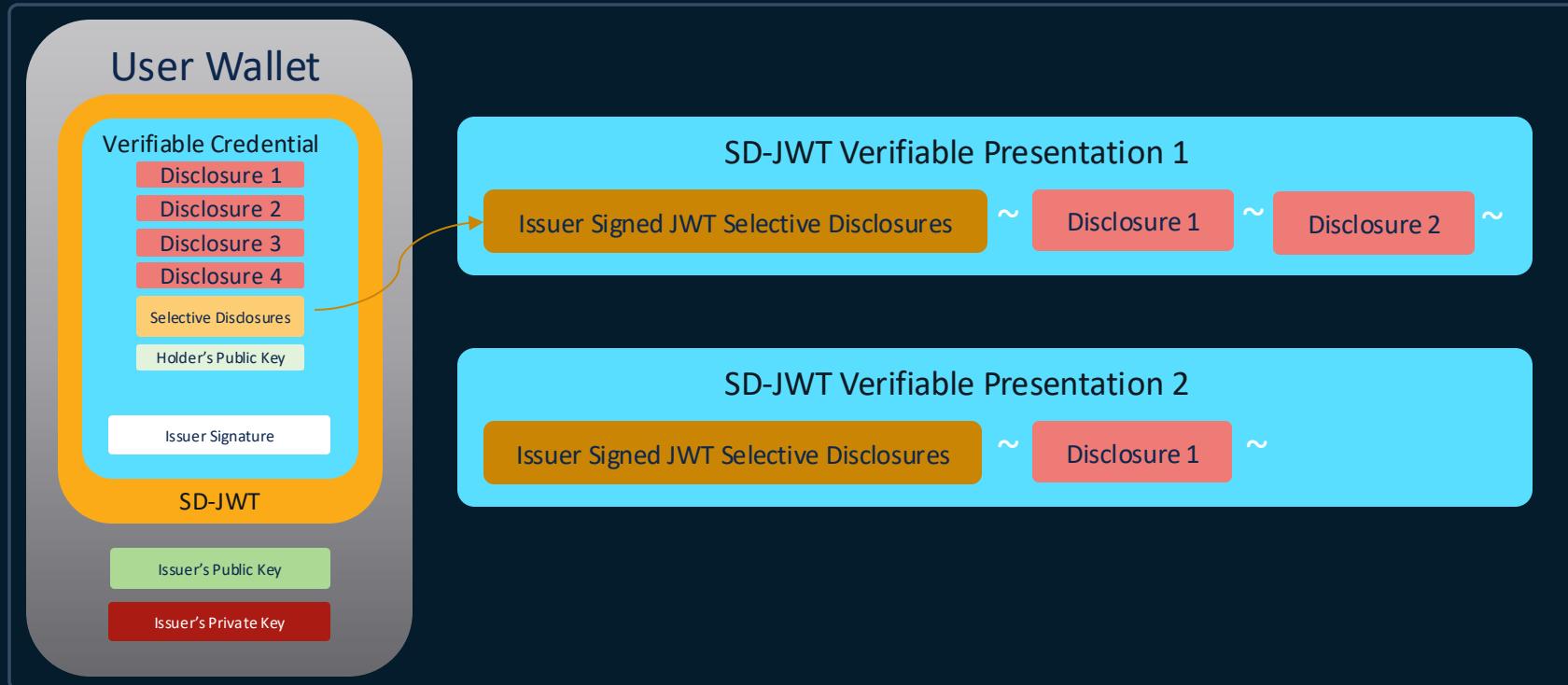


Credential Verification – Selective Disclosure



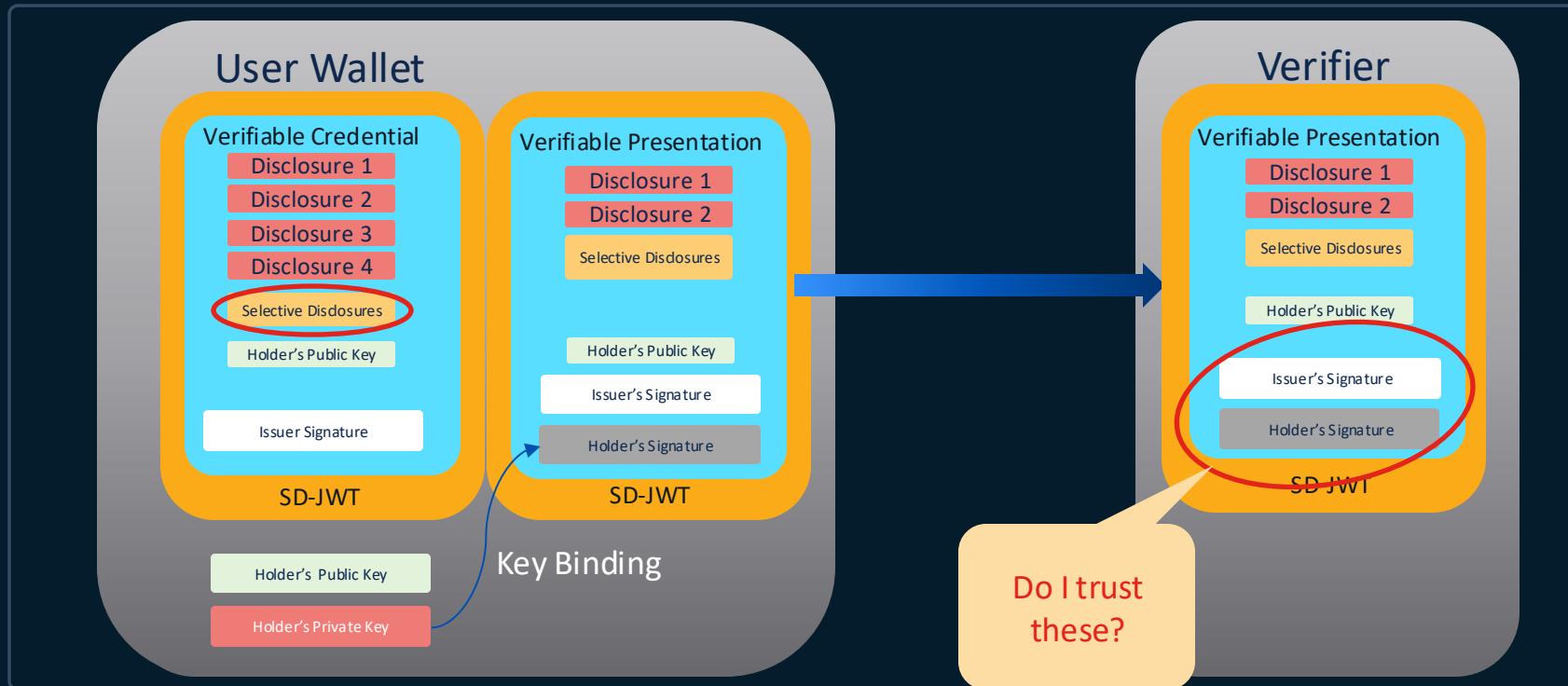


Credential Verification – Selective Disclosure





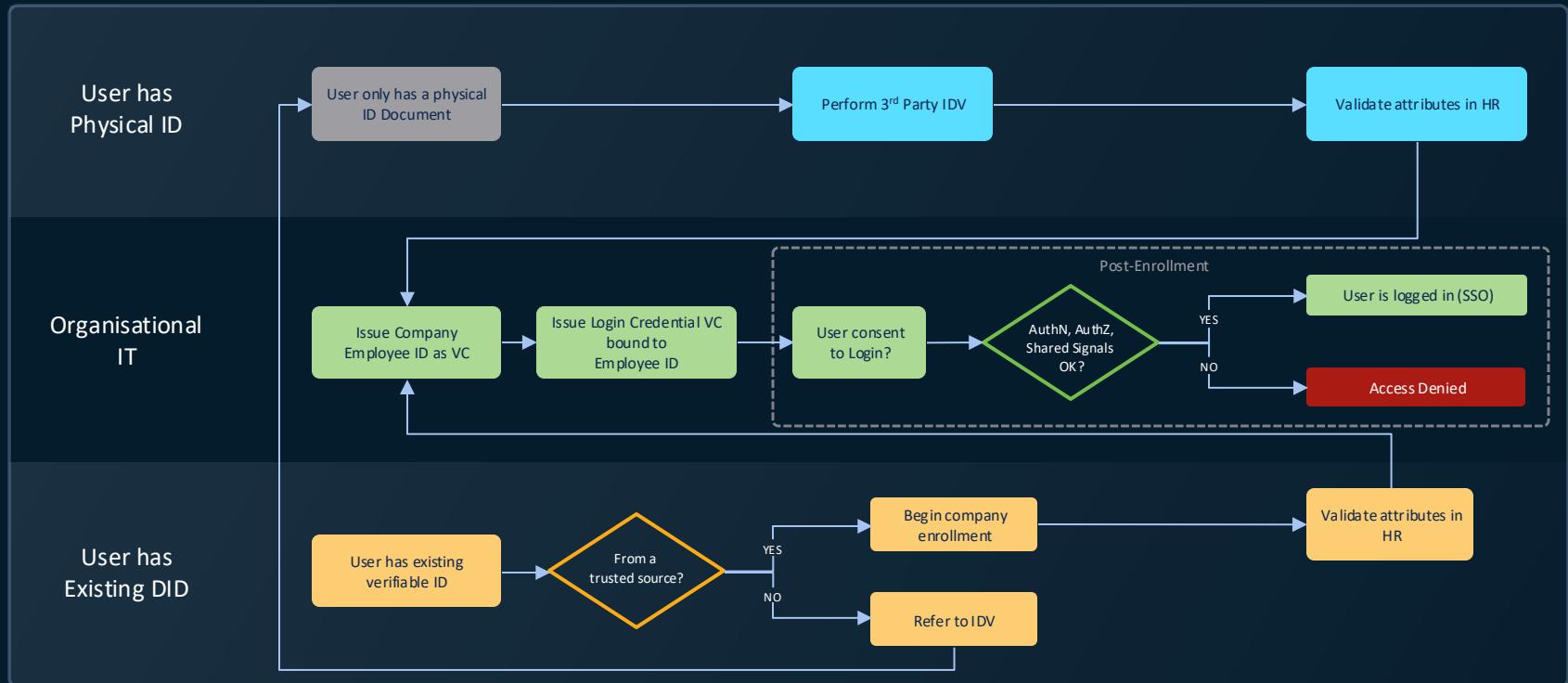
Credential Verification – Selective Disclosure



Verifiable Credentials – How?

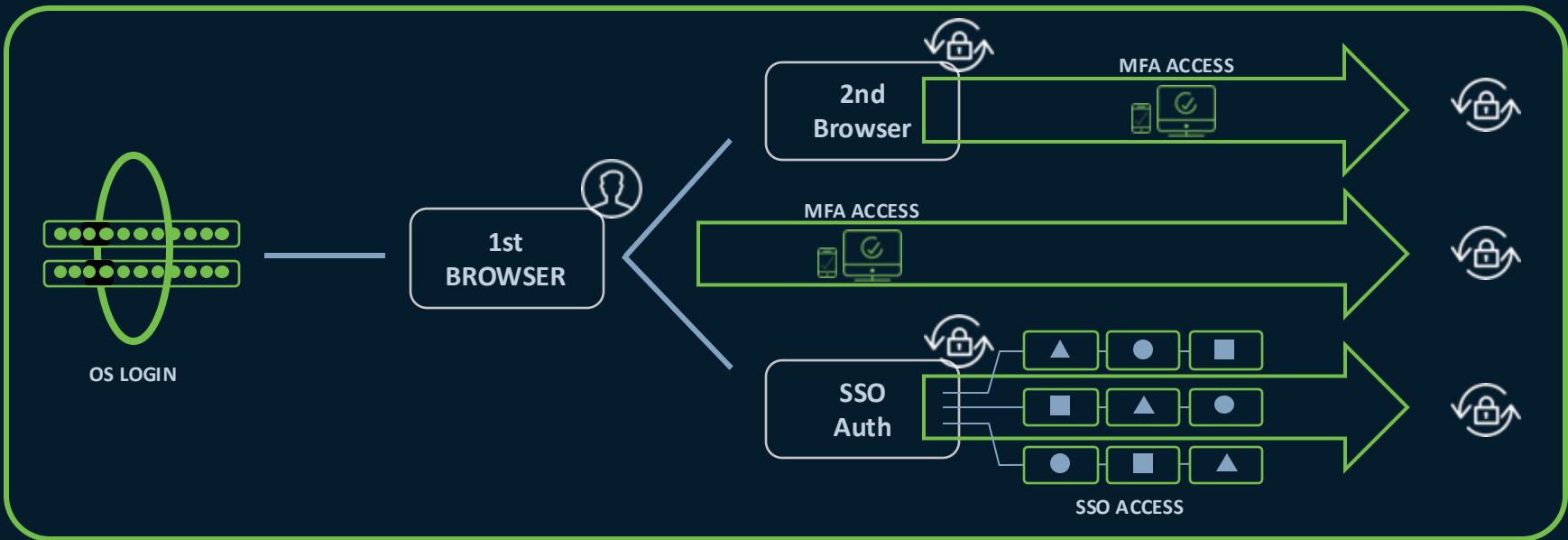
Digital Identity – How do we get onboard?

Digital Identity On-ramps



Last piece of the puzzle

Login Once, Access Everything Securely



Interactive authentication - end user friction



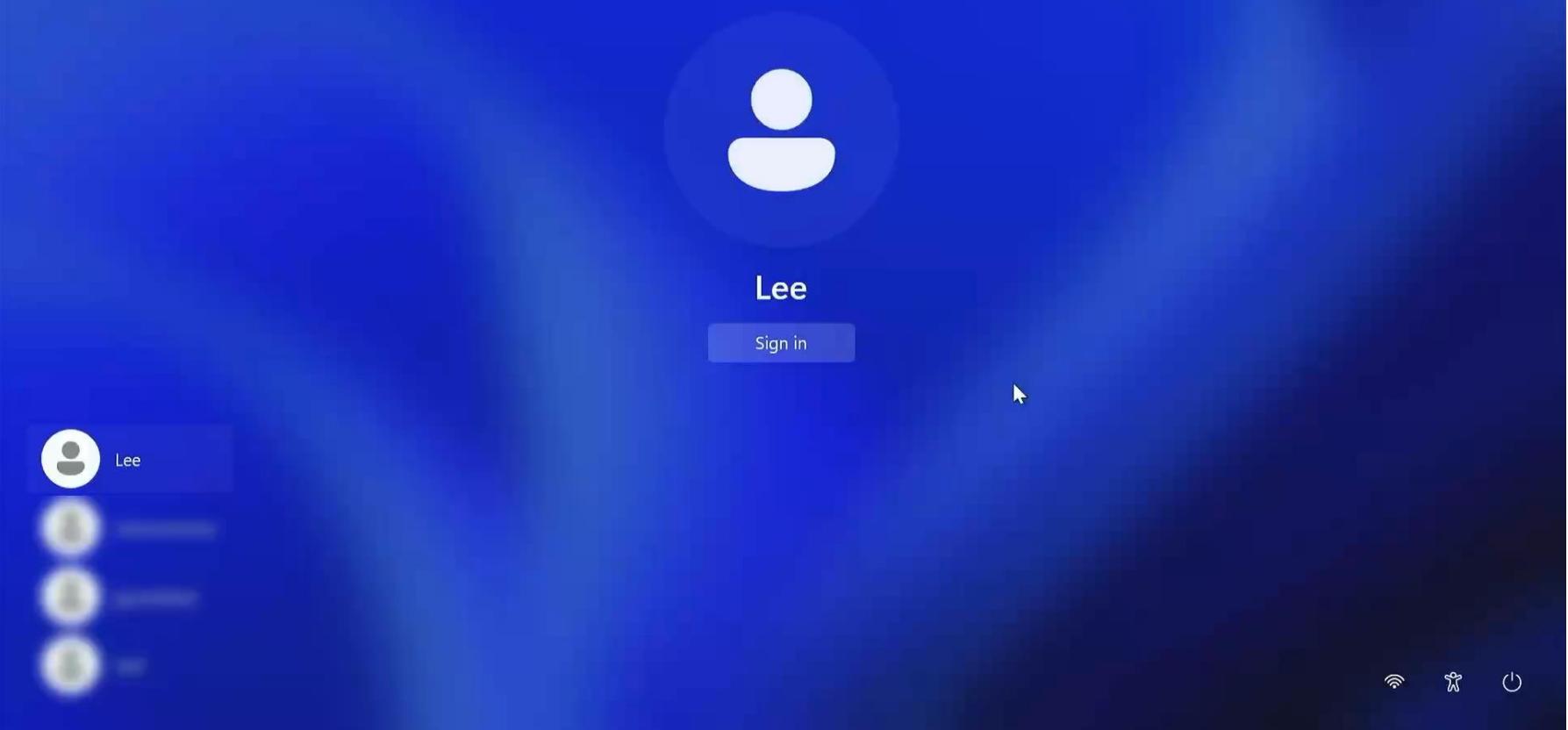
Authentication brokered through device, Duo, and Duo Desktop

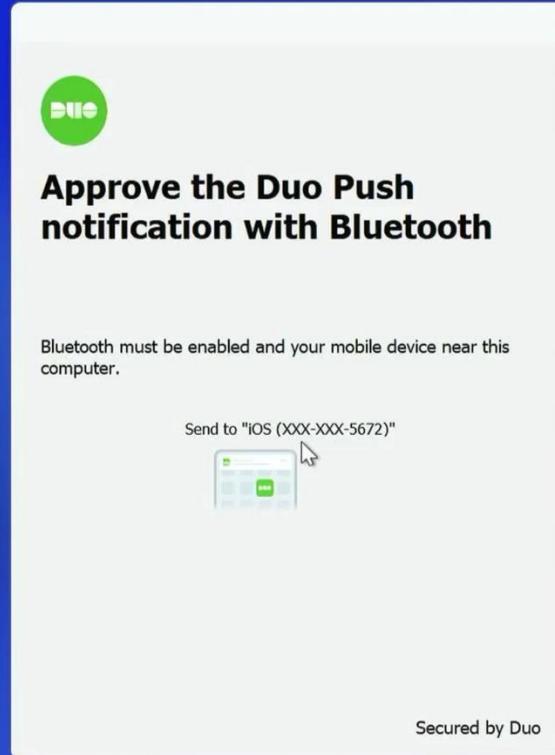
Remembered device session border



Demo Video: Complete Single Sign On with Duo Passport









Search

Manage Devices

lee ▾

Cisco
Webex

Cisco Webex

JIRA

JIRA - Internal Only

cisco Meraki

Meraki



Microsoft 365



Outlook



Salesforce - Single Sign-On



cisco
Identity Services Engine

ZTA Client Access - ISE

Secured by Duo



Search



CISCO Live!

BRKSEC-2144

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

135

Duo Central

zerotrust.login.duosecurity.com/central/

Outlook

Search

New Outlook

Quick steps

Mark all as read

Favorites

- Inbox 1
- Sent Items
- Drafts
- Deleted Items

lee@zerotrustde...

- Inbox 1
- Drafts
- Sent Items
- Deleted Items
- Junk Email

Focused Other

Jeffrey Groesbeck Can you check on th... 4/18/2024
Hello Lee, Can you connect to ou...

support@salesforce.com We received a request ... 4/3/2024
We recently received a request t...

support@salesforce.com Log in with your new S... 4/3/2024
Your username was changed by y...

March

G Google Security alert 3/29/2024
A new sign-in on Windows lee@...

Select an item to read
Nothing is selected

microsoft 365

For Your Reference

The screenshot shows the Microsoft Outlook web interface. The left sidebar lists 'Favorites' and an account section for 'lee@zerotrustde...'. The main pane displays the 'Focused' inbox with several unread messages. The top message is from Jeffrey Groesbeck with the subject 'Can you check on th...' and a timestamp of 4/18/2024. Below it are two messages from support@salesforce.com, both with exclamation marks and timestamps of 4/3/2024. The bottom message is from Google with the subject 'Security alert' and a timestamp of 3/29/2024. A large envelope icon is centered in the inbox area, and a callout bubble on the right says 'Select an item to read' with 'Nothing is selected' below it. The status bar at the bottom shows network, battery, and volume icons.

Duo Central

zerotrust.login.duosecurity.com/central/

Outlook

Search

New Outlook

Jeffrey Goresbeck

To: Lee

Thu 4/18/2024 1:58 PM

Hello Lee,

Cisco Secure Client

AnyConnect VPN: Ready to connect.

2202.vpn.sse.cisco.com/ZTLab_V

Connect

Zero Trust Access: Zero Trust Access is active.

Yes, will do.

Looking into it

Reply

Secured by Duo

For Your Reference

Home View Help

New mail

Inbox

Sent Items

Drafts

Deleted Items

lee@zerotrustde...

Inbox

Drafts

Sent Items

Deleted Items

Junk Email

Focused Other

Jeffrey Goresbeck

Can you check on th... 4/18/2024

Hello Lee, Can you connect to ou...

support@salesforce.com

We received a request ... 4/3/2024

We recently received a request t...

support@salesforce.com

Log in with your new S... 4/3/2024

Your username was changed by y...

March

G Google

Security alert 3/29/2024

A new sign-in on Windows lee@...

Windows Search

File Explorer

Edge

Chrome

PowerShell

Task View

The screenshot shows a Windows desktop environment with several windows open:

- Duo Central**: A browser window showing the URL jira.zerotrustdemo.com:8443.
- Cisco Secure Client - Zero Trust Access**: A modal window from the Cisco Secure Client. It displays the Cisco logo and the text "Cisco Secure Client". Below is a red exclamation mark icon. The main message reads: "Verify your identity" and "Your organization requires you to verify your identity. Click Continue to sign in and follow the authentication prompts." A large blue "Continue" button is centered at the bottom.
- Secure Client**: A separate window titled "Secure Client" containing two sections:
 - AnyConnect VPN:** Status: "Ready to connect." Includes a dropdown menu and a "Connect" button.
 - Zero Trust Access:** Status: "Verify your identity." Includes a "Details" button.

For Your
Reference

Duo Central

Jira Software

Dashboards

Projects

Issues

Boards

Create

Search



DCLOUD board

Sample Sprint 2

0 days remaining

Complete sprint

Board



QUICK FILTERS:

Only My Issues

Recently Updated

TO DO

IN PROGRESS

- DCLOUD-10 IN PROGRESS 2 sub-tasks As a developer, I can update story and task status with drag and drop (click the task to edit)

DCLOUD-11

Update task status by dragging and dropping from column to column >> Try dragging this task to "Done"



DCLOUD-12

When the last task is done, the story can be automatically closed >> Drag this task to "Done" too



Other Issues 5 issues

Cisco Secure Client



AnyConnect VPN:

Ready to connect.

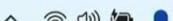
2202.vpn.sse.cisco.com/ZTLab_V

Connect



Zero Trust Access:

Zero Trust Access is active.



CISCO Live!



Sign in | Duo Central | Home | Salesforce | Jira - Internal

Import favorites | Duo Central | Salesforce | Jira - Internal

Search Setup

For Your Reference

Setup | Home | Object Manager

Quick Find

SETUP Home

Create

Get Started with Einstein Bots

Launch an AI-powered bot to automate your digital connections.

Get Started

Mobile Publisher

Use the Mobile Publisher to create your own branded mobile app.

Learn More

Real-time Collaborative Docs

Transform productivity with collaborative docs, spreadsheets, and slides inside Salesforce.

Get Started

duo-tme-dev-ed.lightning.force.com/lightning/setup/SetupOneHome/home

Search | File | Home | Help | Logout

CISCO Live!

Duo Desktop							
For Your Reference		8:42:56 PM AUG 6, 2024	✓ Granted Remembered device via Passport	lee	Duo Central	No detections	▶ Windows 11, version 23H2 (22631.3958) As reported by Duo Desktop
8:41:46 PM AUG 6, 2024	✓ Granted Remembered device	lee	JIRA - Internal Only	No detections	▶ Windows 11, version 23H2 (22631.3958) As reported by Duo Desktop	Remembered Device Location Unknown	
8:40:58 PM AUG 6, 2024	✓ Granted Remembered device via Passport	lee	Secure Access Users	No detections	▶ Windows 11, version 23H2 (22631.3958) As reported by Duo Desktop	Remembered Device Location Unknown	
8:40:32 PM AUG 6, 2024	✓ Granted Remembered device via Passport	lee	Microsoft 365 - zerotrustdemo.co m	No detections	▶ Windows 11, version 23H2 (22631.3958) As reported by Duo Desktop	Remembered Device Location Unknown	
8:40:13 PM AUG 6, 2024	✓ Granted Remembered device via Passport	lee	Duo Central	No detections	▶ Windows 11, version 23H2 (22631.3958)	Remembered Device Location	



Identity Governance and Administration (IGA)

- IGA is the central point where entitlements (who can access what) are managed
- Managing entitlements has both security and compliance impact

Cookie-less SSO

- Session Hijacking is a real attack vector
 - Bad guy sits between user & SP (the app)
 - App sends user the cookie
 - Bad guy copies those cookies & now uses the cookie to access the app “as the user”
- Removing cookies from the process, session hijacking becomes thing of the past
 - Duo will have cookie-less SSO w/ Duo Passport

The Future





Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion



Conclusions



Conclusions

- AAA is a basic security principle that is just as relevant today as it was 20 years ago.
- SAML & OIDC are for Single Sign On, while OAuth is for Application Authorization
- WebAuthN is more than just webauth in networking
- Passkeys are here, Passwordless is here – use them, but keep an eye to the future w/ Verifiable Credentials
- Duo makes Identity Easy and Secure
- You had fun in this session, even though the topic is boring

Good Links

- Shibboleth Consortium: <https://www.shibboleth.net/index/>
- OASIS: <https://www.oasis-open.org>
- Beer Drinkers Guide to SAML: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>
- Fighting Cookie Theft: <https://blog.chromium.org/2024/04/fighting-cookie-theft-using-device.html>
- A demo of Webauthn and Passkeys: <https://webauthn.io>

Please fill out the survey



Drop your email in the comments – we WILL respond!

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



A dark blue background featuring a series of overlapping, semi-transparent blue wave-like shapes that create a sense of depth and motion.

Continue your education

CISCO *Live!*

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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

Other Sessions

- Here at Cisco Live
 - Identity Intelligence Demystified [BRKSEC-2162]
Aaron Woland, Tuesday 14:00 (2pm)
 - Taking Authentication to the Next Level w/ Duo Security [BRKSEC-2584]
Stefan Duernberger, Thursday 08:30
- On Demand Sessions
 - Demystifying the World of Passkeys [BRKSEC-2202] (Clayton Ballreich)



Thank you