OCTOBER 24, 2023

Introduction to claims authentication

Related to AVEVA Identity Manager Service "AIMS"

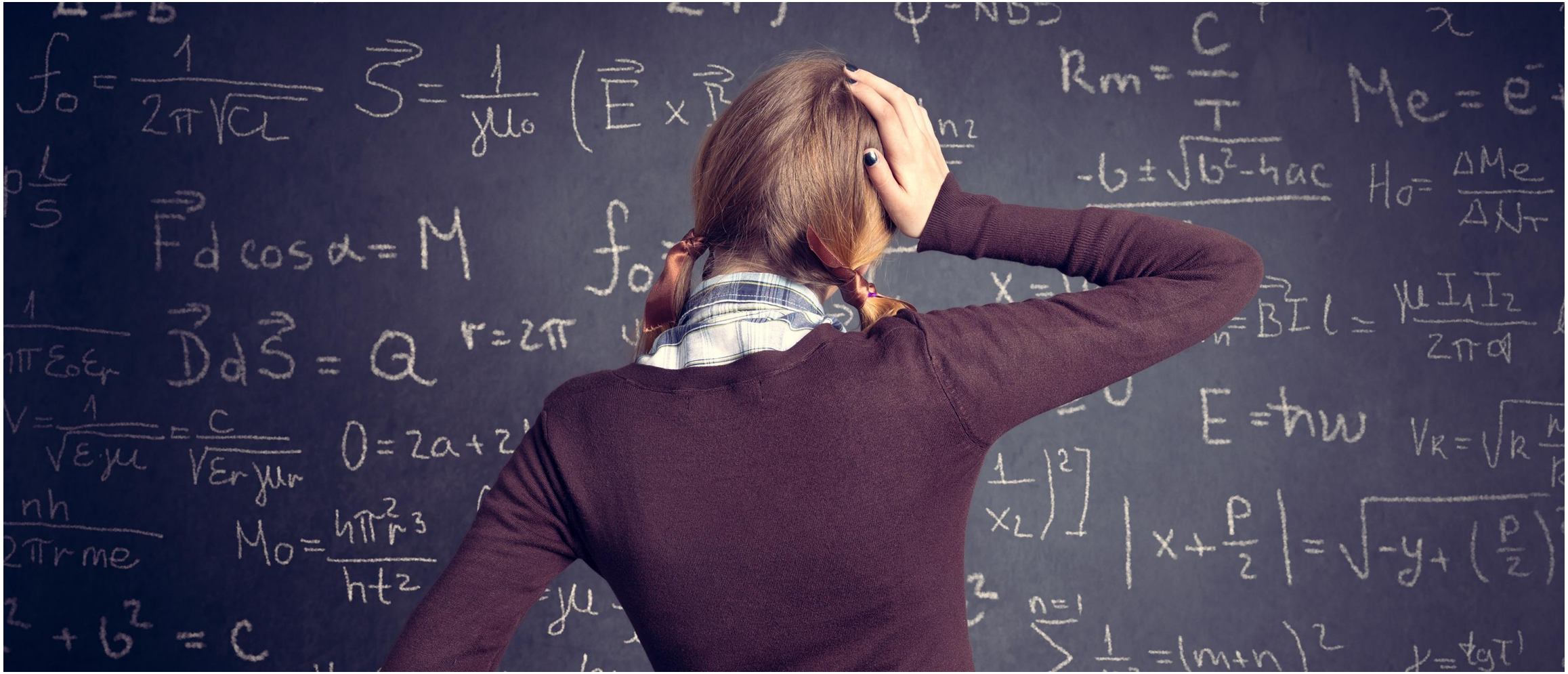
Presented By: Roger Ward

Roger Ward

Tech Support Senior Engineer

- AVEVA
- roger.ward@aveva.com

Claims authentication



Claims authentication: word soup

Goals

- Explain the benefits of claims authentication
- Explain claims authentication
- Summarize how to implement claims authentication

AVEVA

Agenda

Background

- Problems with current authentication methods
- Benefits of claims authentication

Claims authentication

- Define claims authentication
- Tokens
- OIDC
- Federation
- TLS and certificates
- AIM

Setting it up (an overview)

- Setting up AIM
- Setting up PI Data Archive 2023

Conclusion

- FAQ
- Q&A

AVEVA

Current authentication methods

Current authentication methods

Explicit login

- Users must sign in separately to Windows and Data Archive
- System managers must maintain separate user account for every user on Data Archive
- Not very secure (can be brute forced)

Current authentication methods (cont.)

PI trusts

- Tedious to maintain according to best practices
- No native support for encryption
- Not scalable
- Can be spoofed

Current authentication methods (cont.)

Windows Integrated Security (e.g. NTLM, Kerberos)

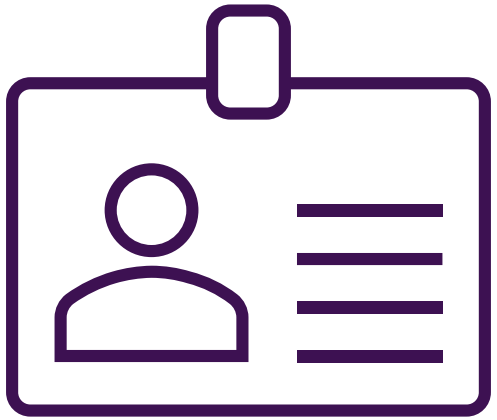
- Dependent on Windows Active Directory
- Difficult to use across domain boundaries
- Reliance on Windows Credential Manager in workgroups
- Must reauthenticate for each new session

Benefits of claims authentication

- Removes dependence on Windows Active Directory
- Flexible (interoperable with a wide range of identity providers)
- Enables single sign-on (SSO) functionality
- Removes need for multiple username/password combos
- Enables seamless integration of On-prem, Private Cloud, and AVEVA™ Data Hub

What is claims-based authentication?

- Any authentication protocol that relies on the communication of verifiable “claims” (i.e. assertions/info) about a user requesting access
- These claims are often packaged into data structures called “tokens”.
- Access is granted to whomever bears the token
- Claims auth. = token auth. = bearer auth.



Tokens

What is a token?

- Small, cryptographically verifiable set of structured data (i.e. claims) about the end-user
- Issued by an authorization server
- Held by clients
- Passed to a resource server whenever access is requested
- Verified by a resource server
- Expire after a certain length of time
- Commonly in JWT (JSON Web Token) format

JWT (JSON Web Token) format

Example:

- **Header**
  - Info about token type and the signing algorithm
  - Base64 encoded
- **Payload**
  - Claims (i.e. info) about the user
  - Token creation/expiration time
  - Base64 encoded
- **Digital signature**
  - Hash of the header and payload fields
  - Used to verify the integrity of the token


```
eyJhbGciOiJIUzI1NiJ
9.eyJuYW1lIjoiSm9lI
ENvZGVyIn0.5dlp7Gmz
iL2QS06sZgK4mtaqv0_
xX4oFUuTDh1zHK4U
```

Anatomy of a JWT (cont.)

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

Types of JWTs

ID token

- holds authentication info (e.g. ID)
- provided by OIDC

Access token (AKA bearer token)

- holds authorization information (e.g. CRUD operations)
- provided by OAuth 2.0
- held by client and passed to resource server when a resource is requested
- expires quickly (five minutes by default)

Refresh token

- provided by OIDC along with access token
- used to get a new access token without user interaction
- expires slowly (30 hours by default)

OpenID Connect (OIDC)

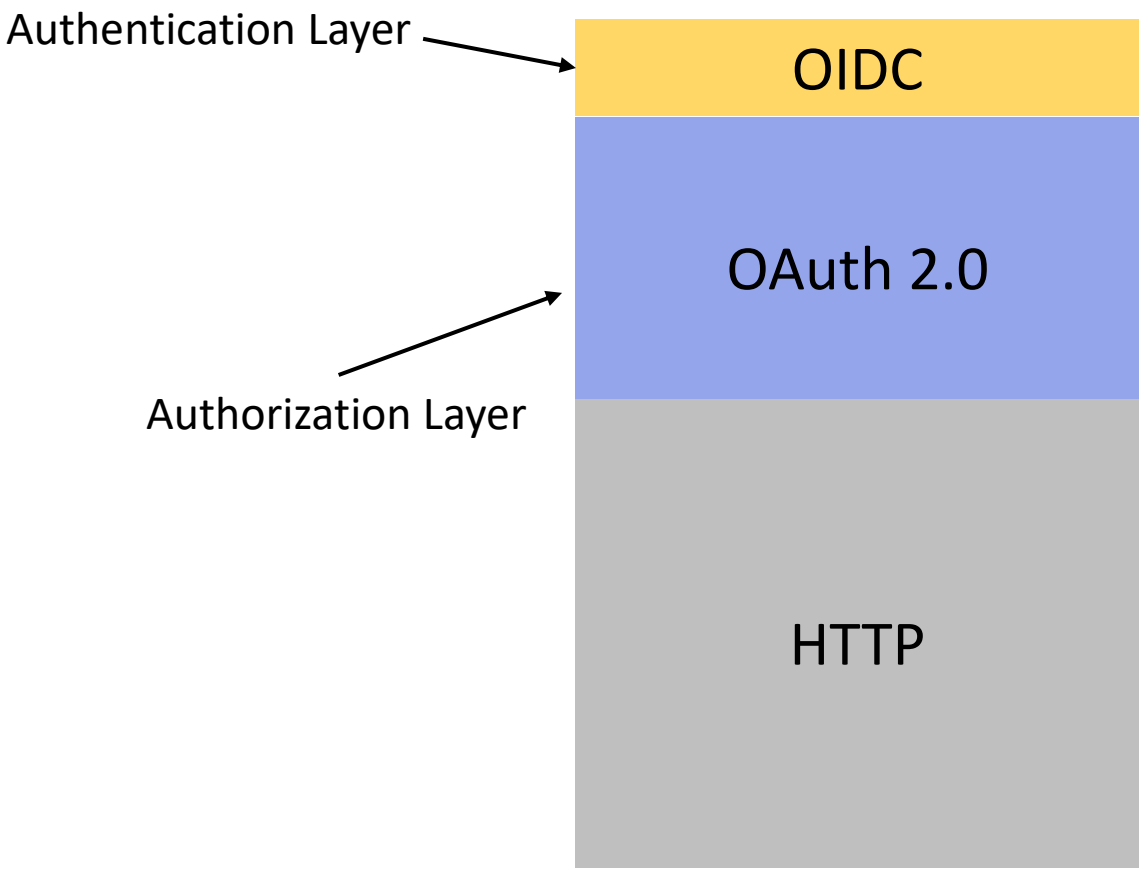
Brief history of common token-based authentication protocols

- SAML (2002)
  - OG SSO protocol
  - Incorporates authentication and authorization
  - Privacy drawbacks
- OAuth 1.0 (2007)
  - Improvement on SAML
  - Authorization only (no native support for authentication)
- OAuth 2.0 (2012)
  - Hardening against AS (authorization server) mix-up attack
- OIDC (2014)
  - Authentication layer built on top of OAuth 2.0

What is OIDC?

- OIDC = OpenID Connect
- Open, decentralized, token-based authentication protocol
- Compliments OAuth 2.0
- Requires TLS for secure communication of tokens
- Supports multiple flows (i.e. methods) to receive a token
  - Authorization code flow
  - Implicit flow
  - Hybrid flow
  - Client credentials flow*
  - Resource owner password credentials flow*
  - Refresh token flow*

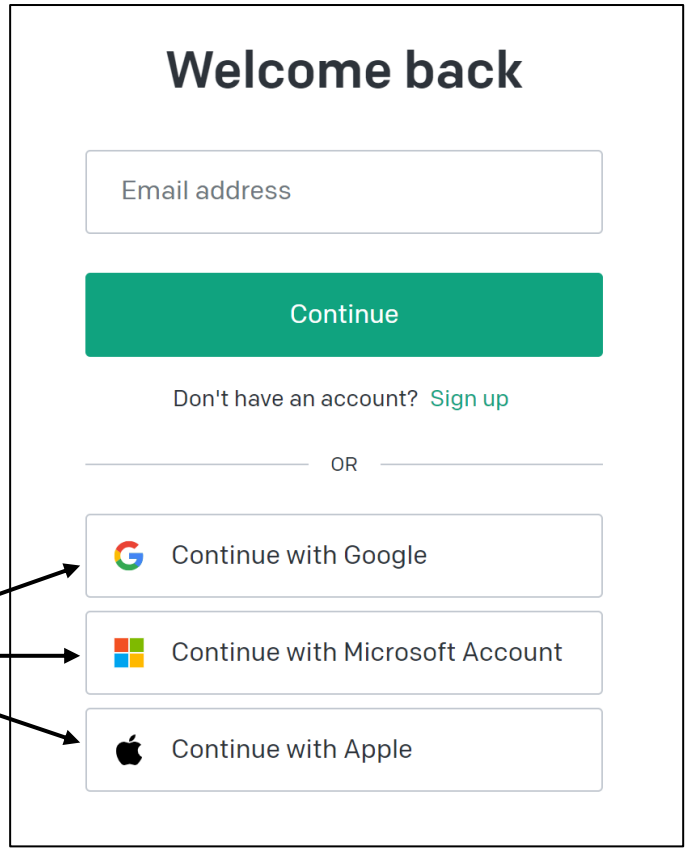
* OAuth 2.0 flow



What OIDC authentication looks like

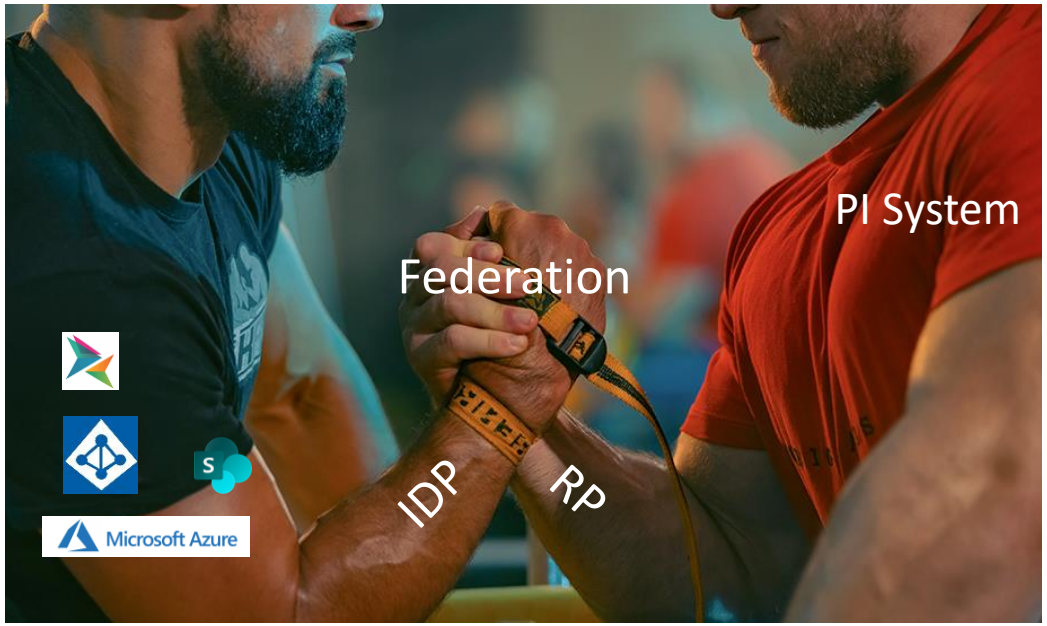
- Allows users to be authenticated via third-party identity provider (IdP)
- Third-party IdP is said to be “federated”

Third-party identity providers (IdPs)



What is a federation?

- The establishment of a trust relationship between a Relying Party (RP) and a third-party Identity Provider (IdP)
- In the context of the AVEVA™ PI System™:
  - RP = The PI System
  - 3rd Party IdP = any IdP that supports SAML 2 or OIDC
- “Trust” is somewhat misleading. Relationship is actually cryptographically verifiable
- Trust is established via initial exchange of certain info including:
  - Client ID
  - Client Secret



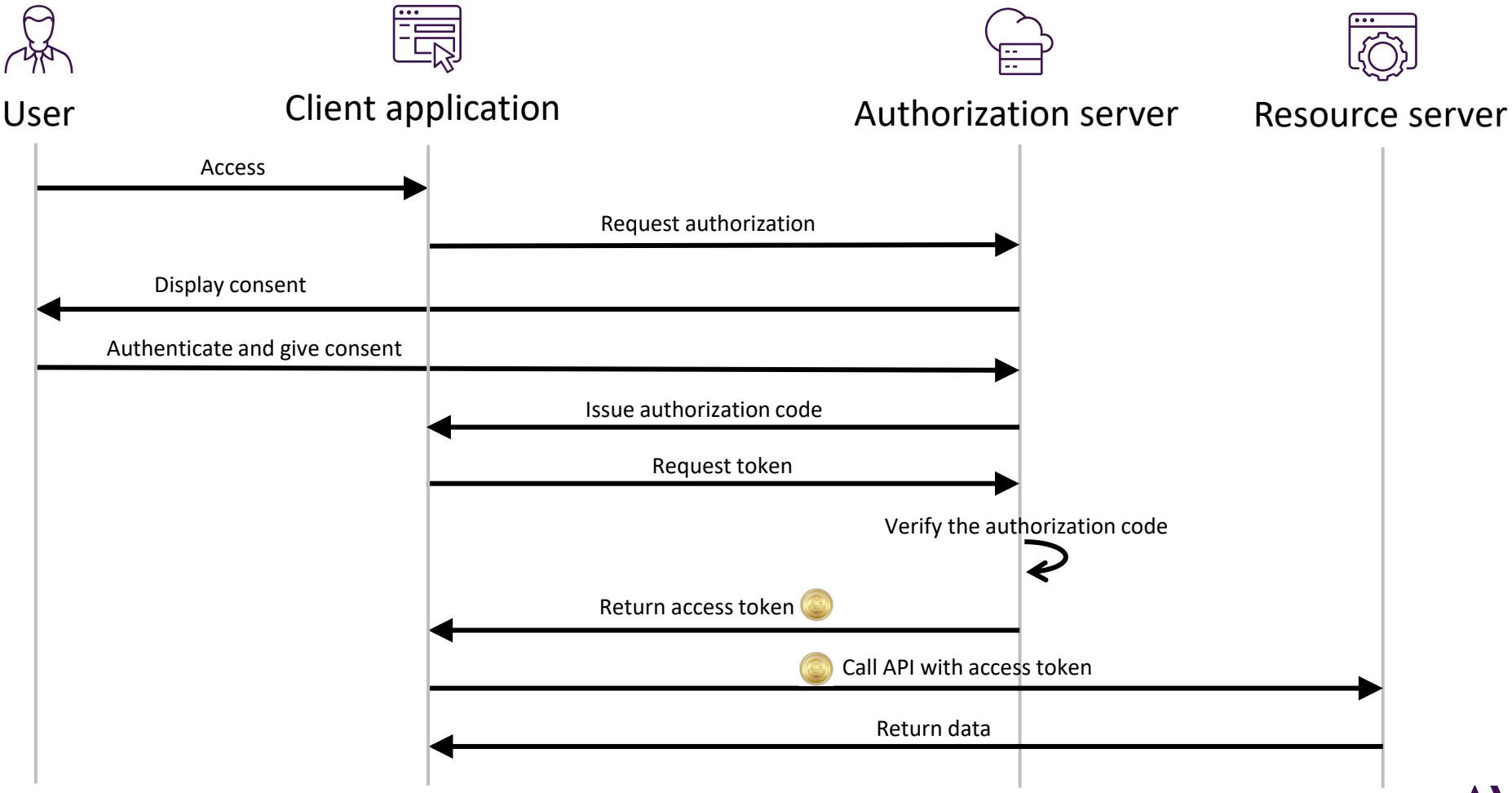
Supported IdPs

- Windows Active Directory (default)
- AVEVA™ Connect, common cloud platform (recommended)
- Azure Active Directory
- Google
- Literally any other IdP that supports SAML 2, ADFS, or OIDC

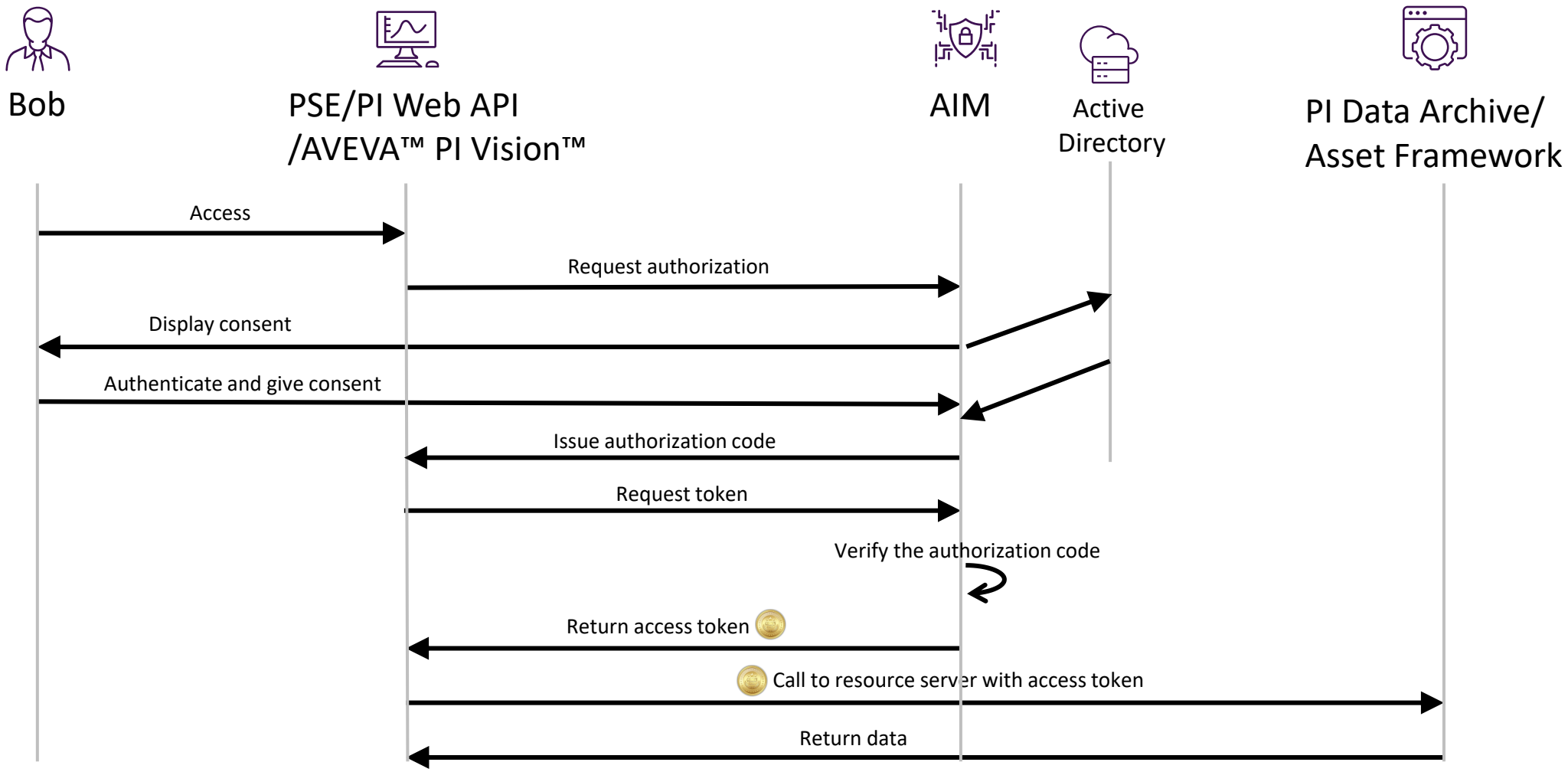
How OIDC works

How OIDC works

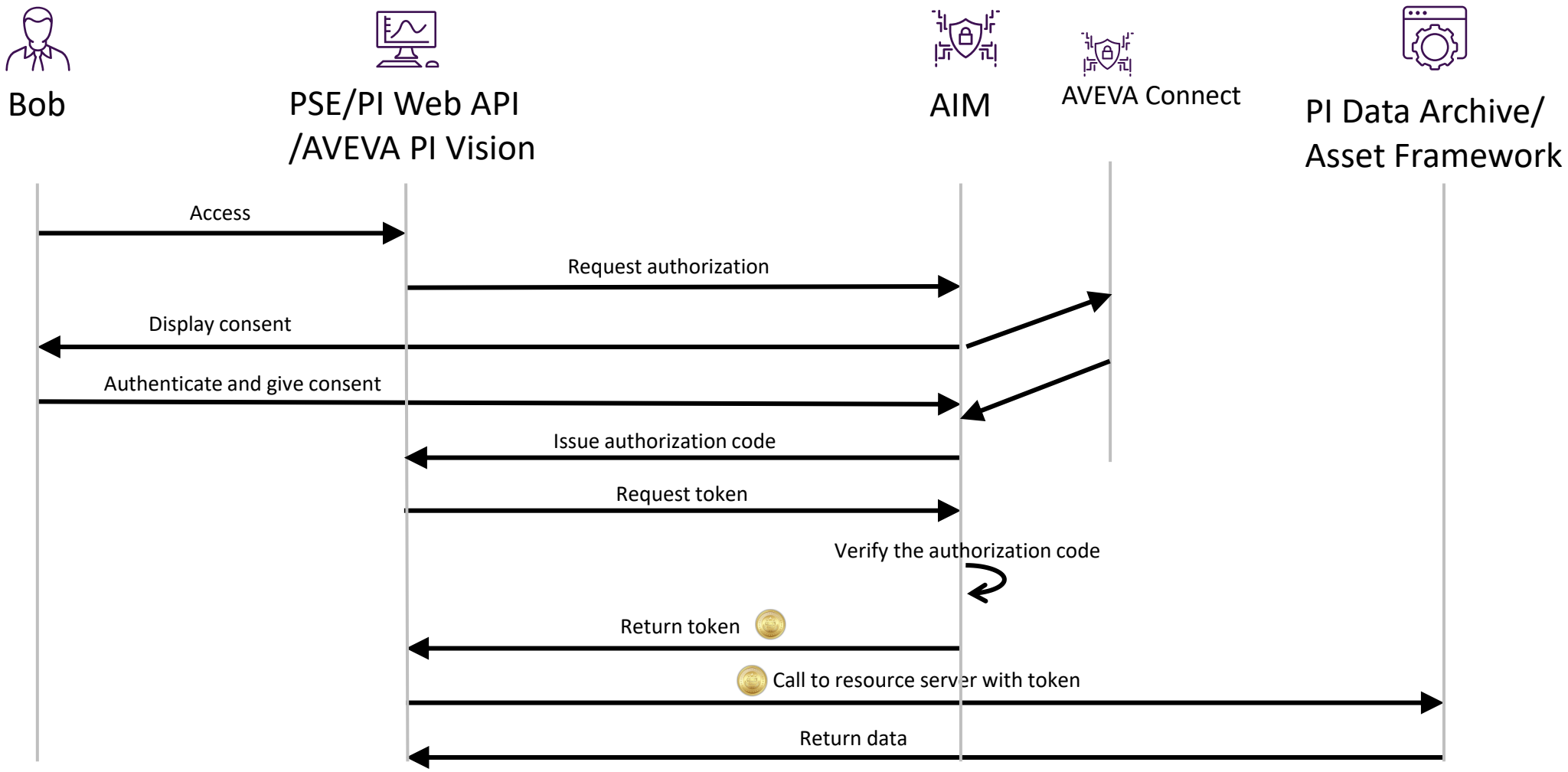
Authorization code flow



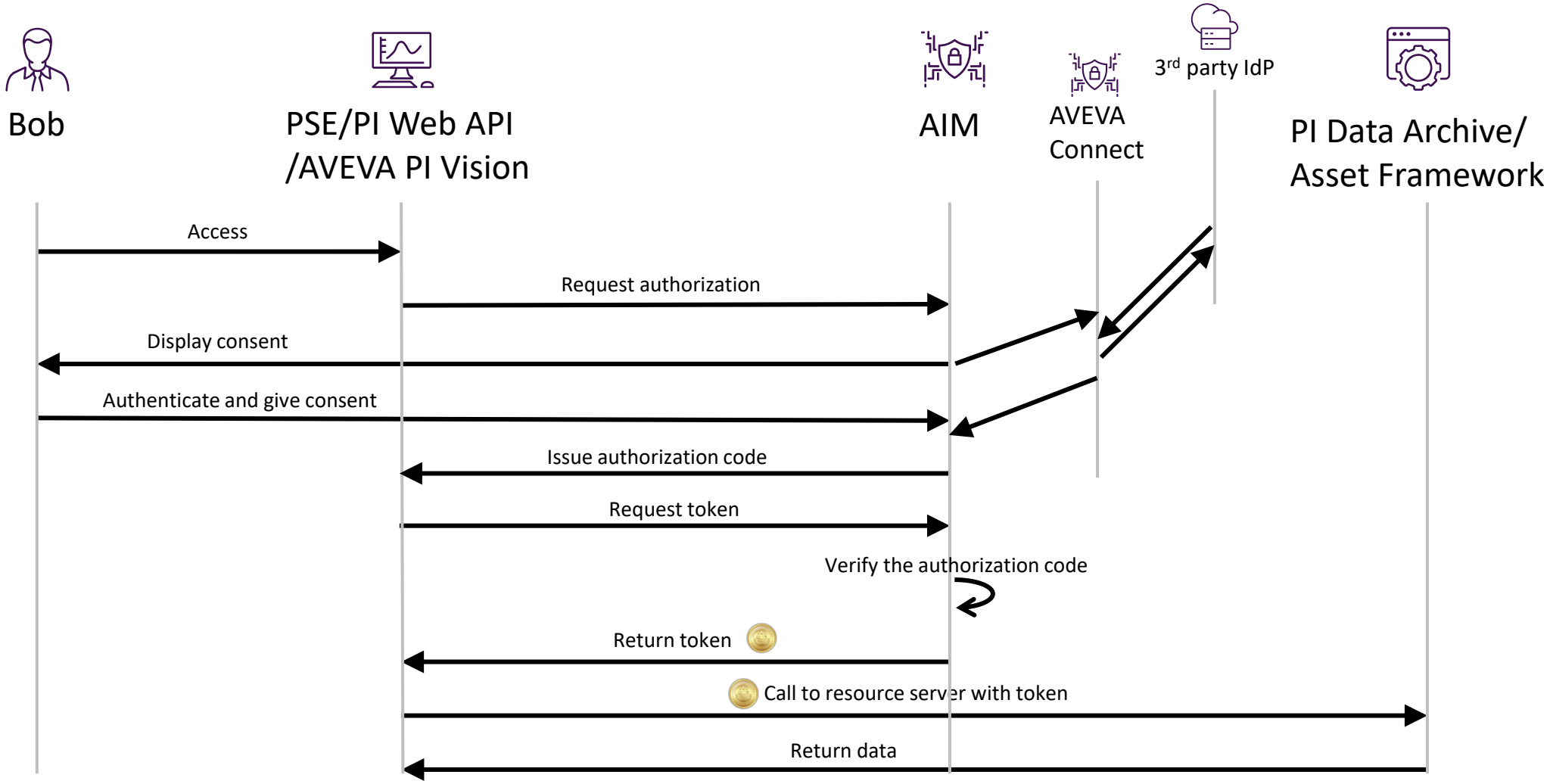
How OIDC works (in PI) (with Active Directory)



How OIDC works (in PI) (with AVEVA™ Connect)



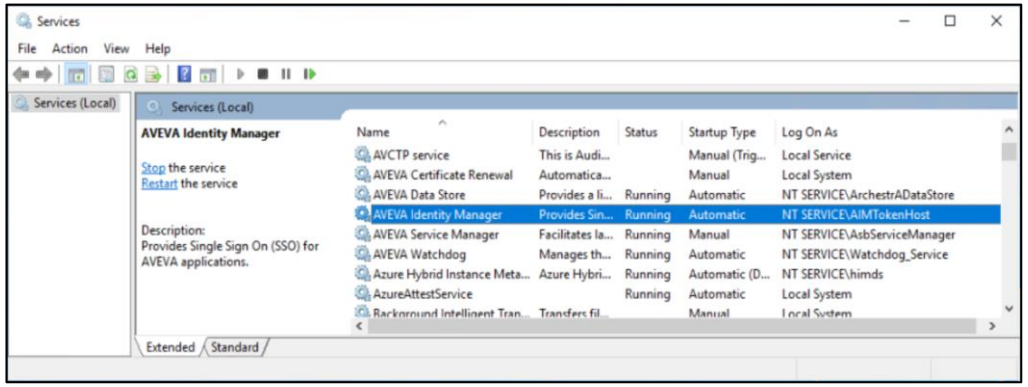
How OIDC works (in PI) (with 3rd party IdP)

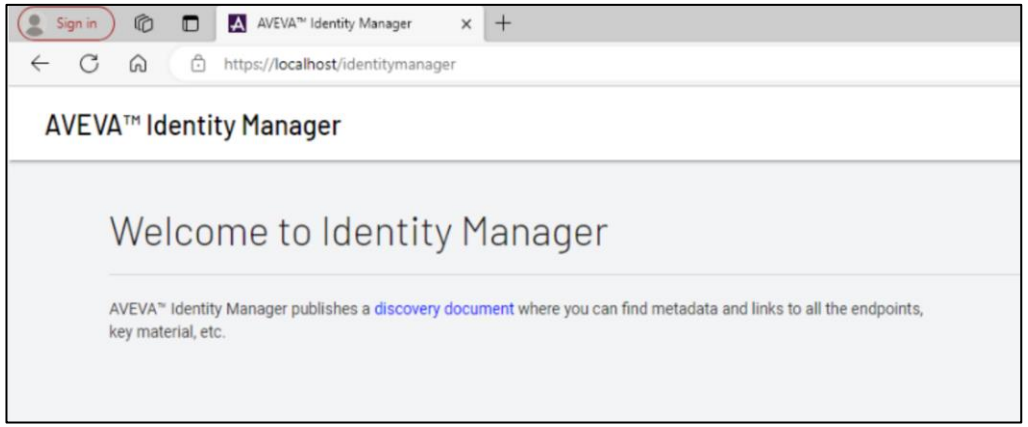


AVEVA Identity Manager

AVEVA Identity Manager (AIM)

- AIM is the identity service that integrates with identity providers (IdPs)
- Install kit: **Platform Common Services for the PI System**
- Runs as a service
- Only one AIM server needed per organization
- Server where AIM is installed is designated as the “System Management Server”
- Automatically registers itself with Active Directory (AD), and enables AD claims during initial installation
- Formerly known as “ArchestrA”

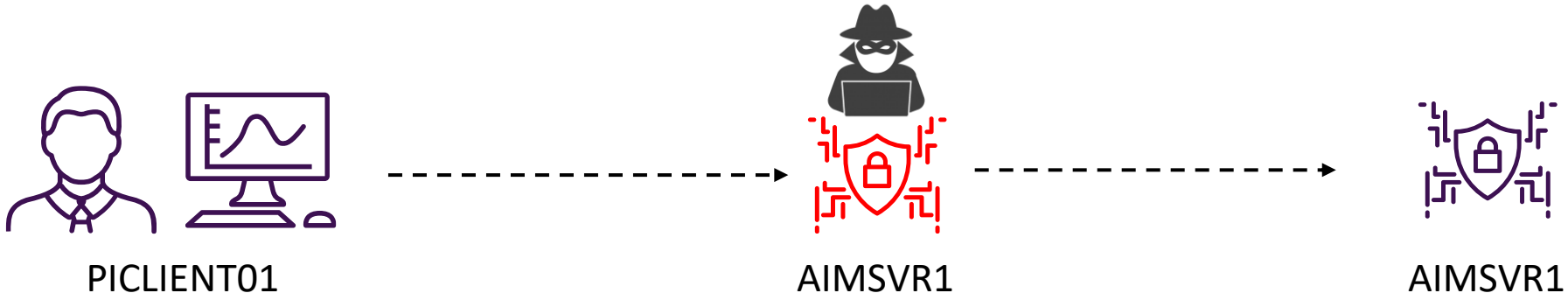




TLS and digital certificates

Why do we need TLS?

- Because it’s required by OIDC & OAuth 2.0
- Because it protects against man-in-the-middle (and related) attacks



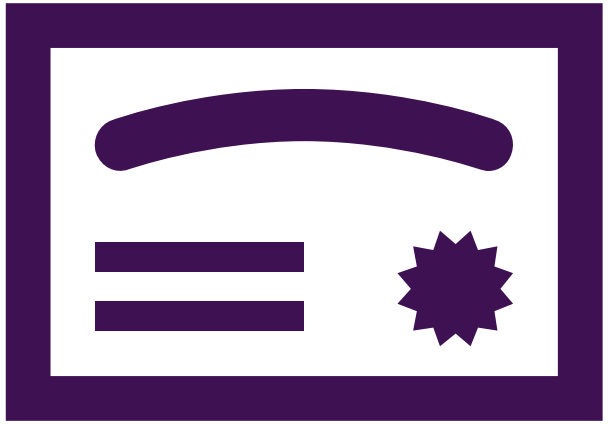
What is TLS?

Transport Layer Security

- Transport-layer cryptographic protocol designed to provide communications security over a computer network
- Interoperable with many different application-layer protocols (e.g. HTTP, SMTP, IMAP, FTP, DNS)
- Successor to SSL (Secure Sockets Layer)
- Two facets of TLS:
  - Ensuring the identity of remote server
  - Ensuring the privacy and integrity of communications between client and server

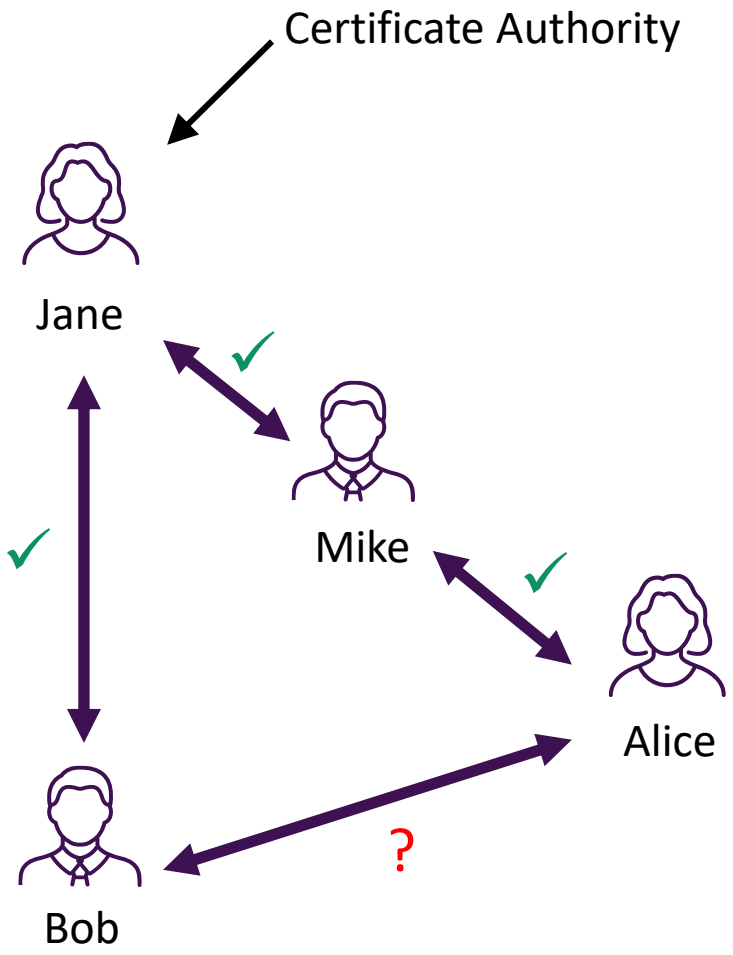
TLS, PKI, and digital certificates

- TLS is implemented using X.509 digital certificates and public key infrastructure (PKI)
- PKI is a security architecture that uses public and private key pairs as the basis for verifiable server identities and secure communications to/from those servers
- Public-private key pairs generated via algorithms such as RSA, ECC, or ECDH
  - Public key is used for encrypting data and establishing identity
  - Private key is used for decrypting data
- Digital certificates are files used to cryptographically link the public key to the server that owns it
- A certificate's trustworthiness is derived from its hierarchical chain of trusted entities



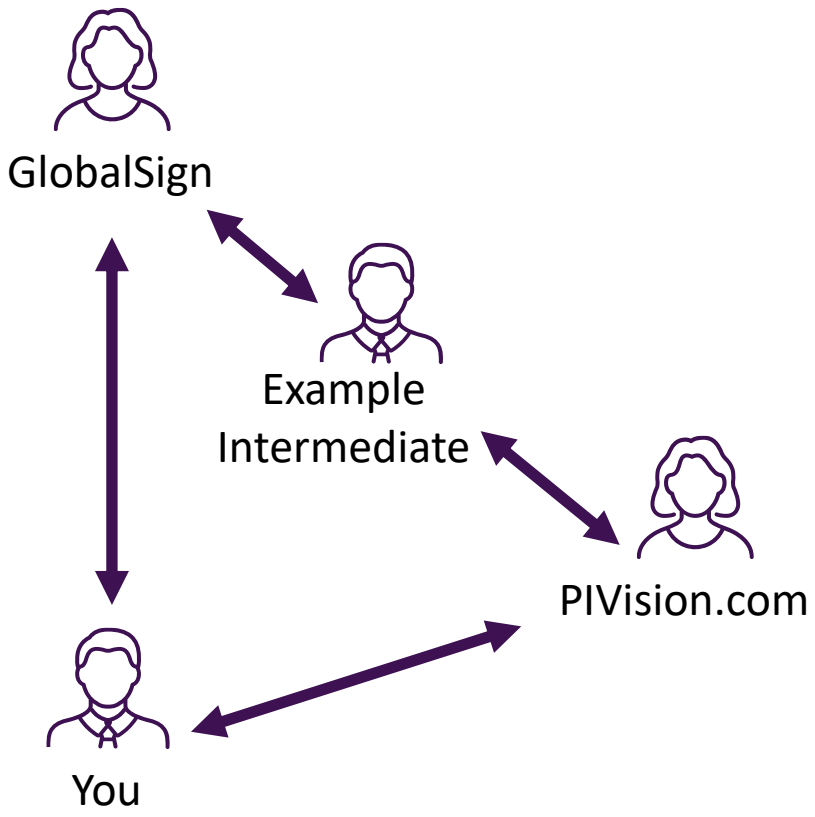
The chain of trust

- Example: Alice and Bob
- Top-level trusted entity is known as a “certificate authority”



The chain of trust

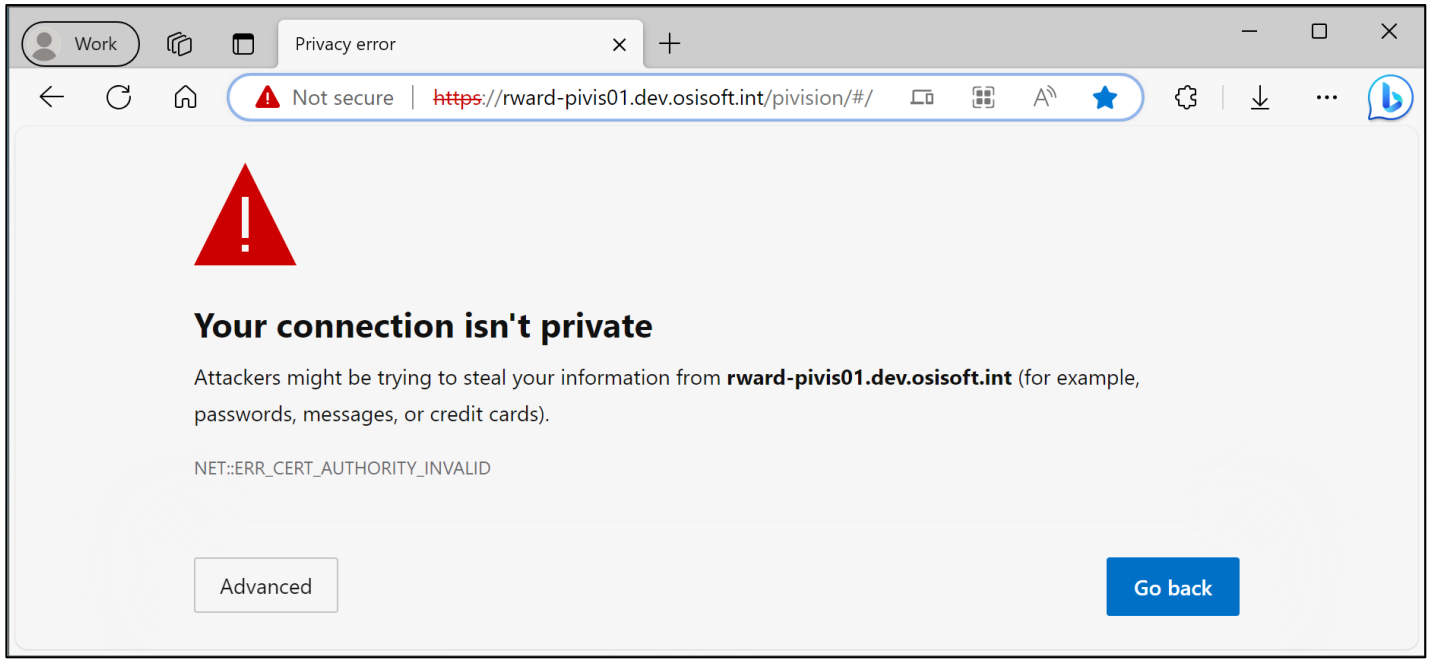
- Example: Alice and Bob
- Top-level trusted entity is known as a “certificate authority”
- List of certificate authorities are defined and maintained by the creators of the operating system.
- The certificate authorities for Windows Server are managed by Microsoft Trusted Root Certificate Program on a monthly cadence

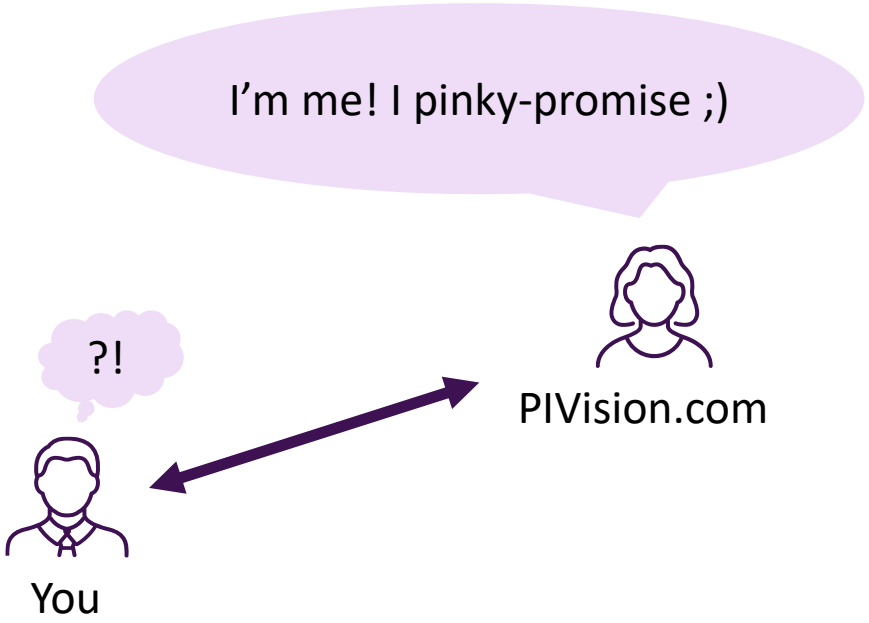


Types of certificates

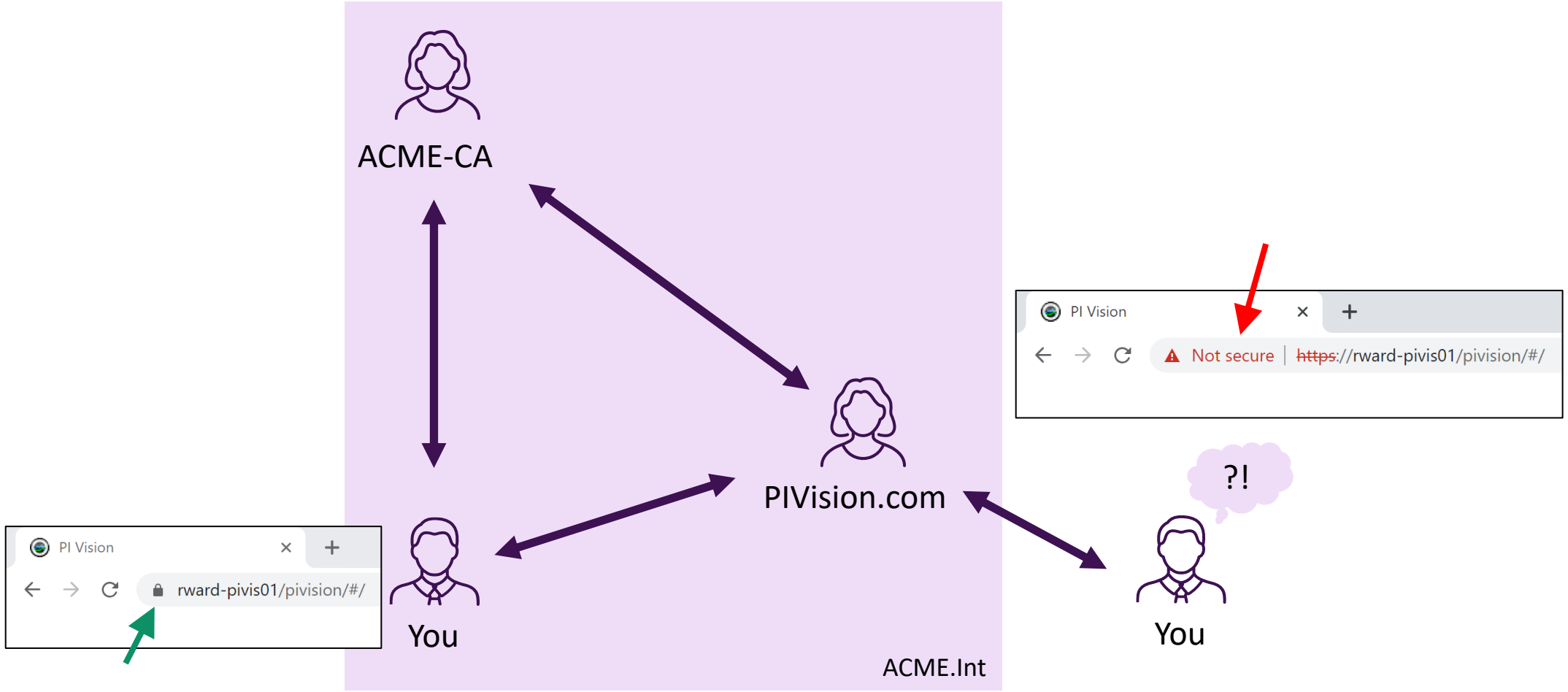
	Self-signed	Enterprise	Third-party
Ease of creation	Easy	Moderate	Harder
Usability	Not trusted anywhere by default	Only trusted inside domain	Trusted everywhere

Self-signed certificates

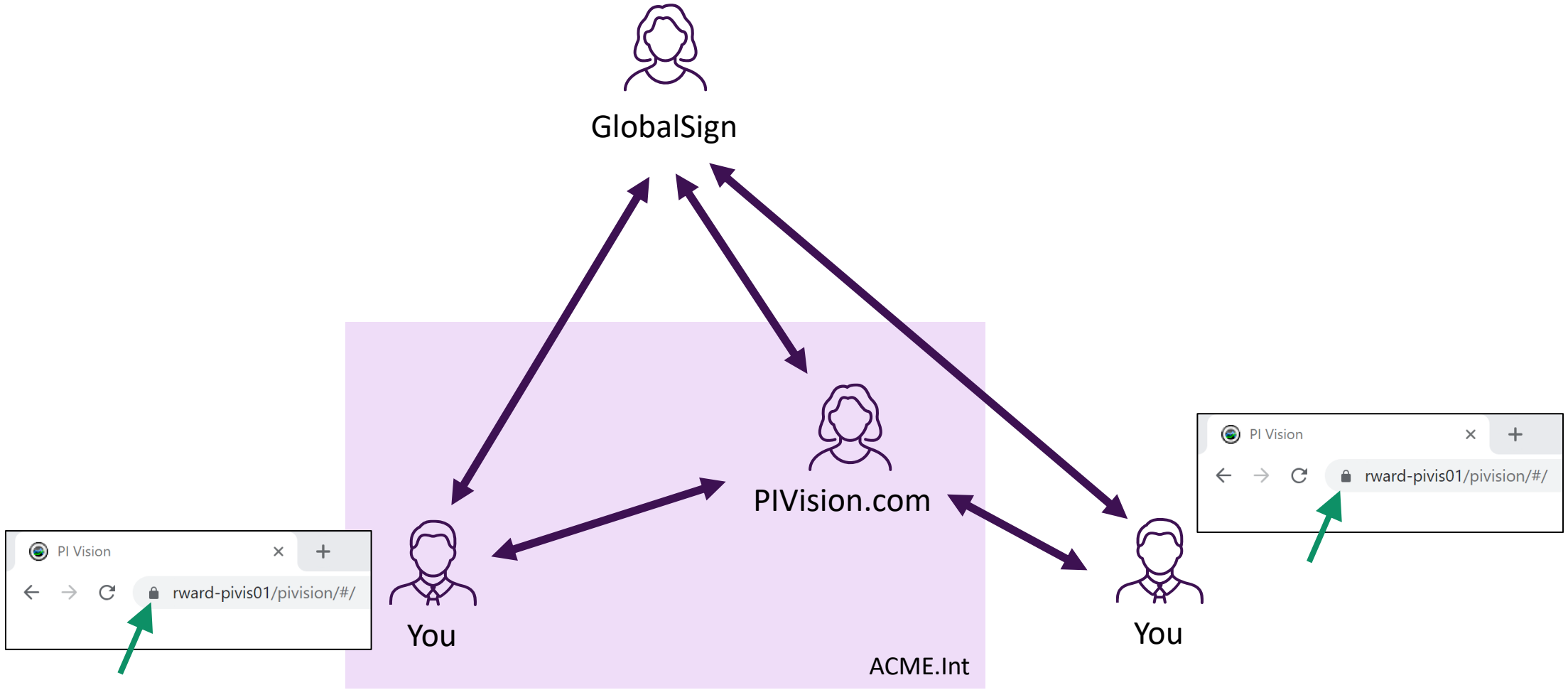




Enterprise certificates

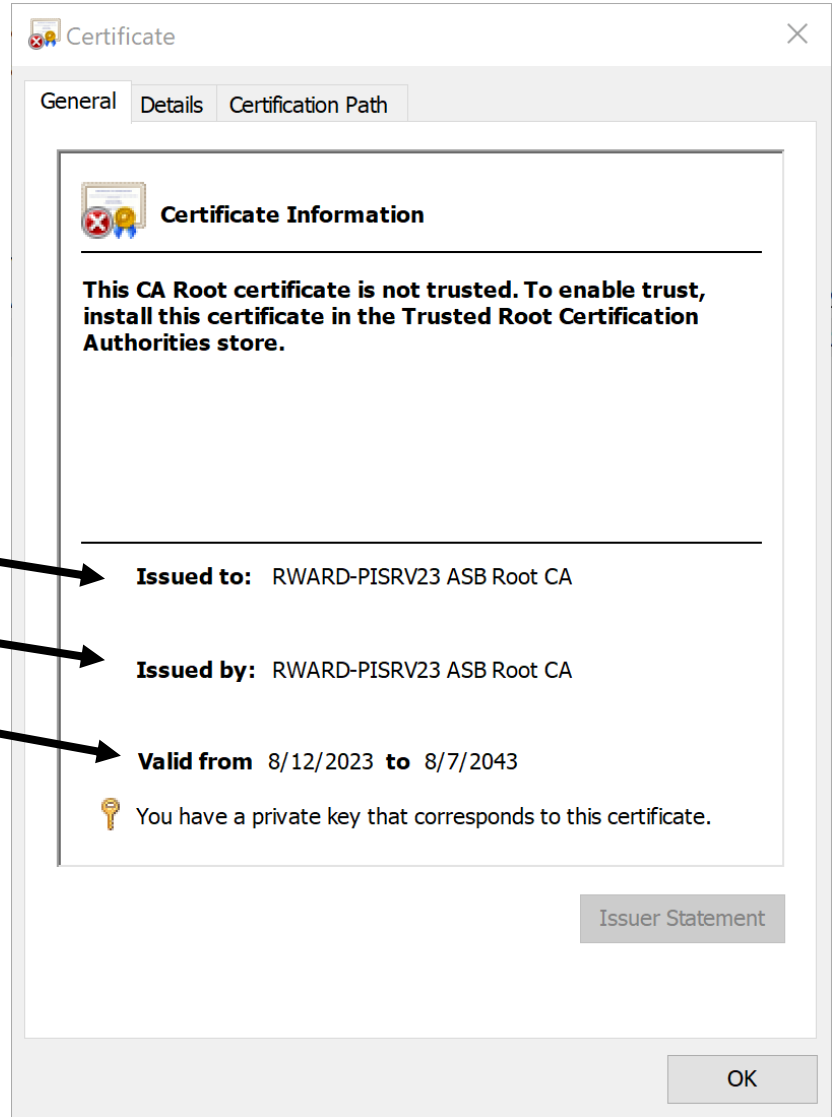


Third-party certificates



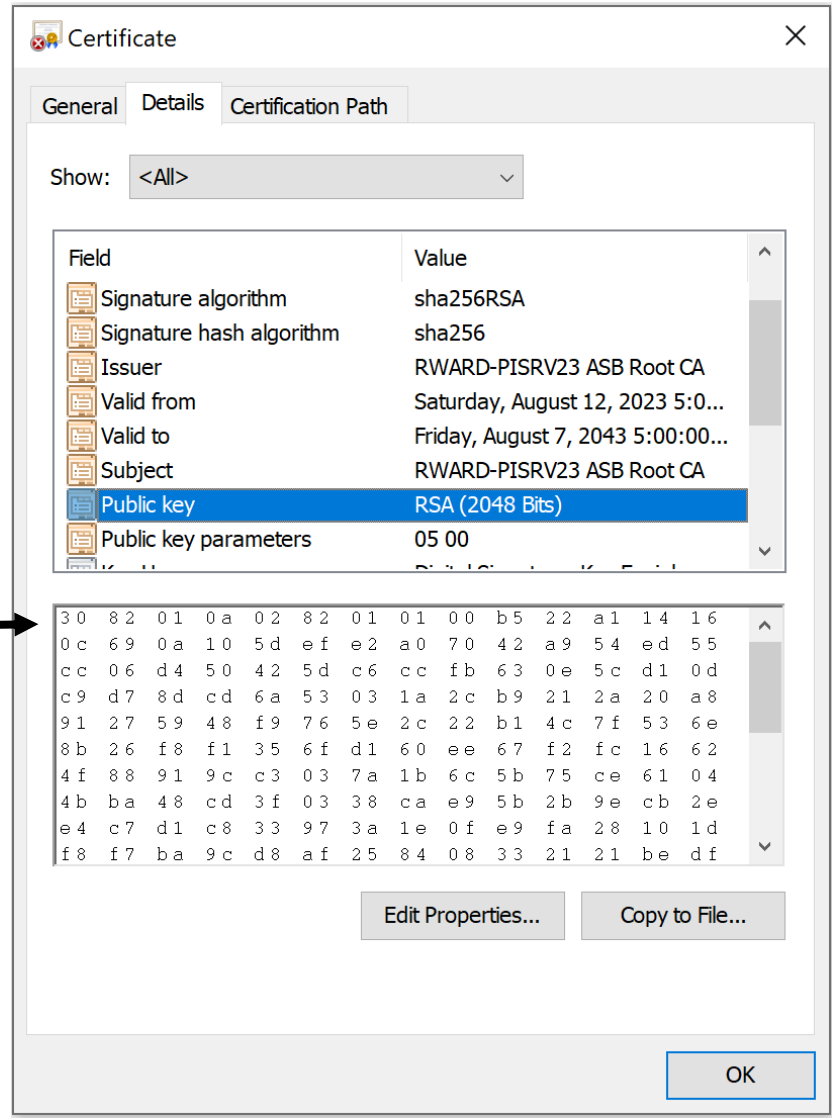
Anatomy of a digital certificate

- Essential components
  - “Issued to” field
  - “Issued by” field
  - Validity date range
  - Public key
  - Signature algorithm (used to verify digital signature)



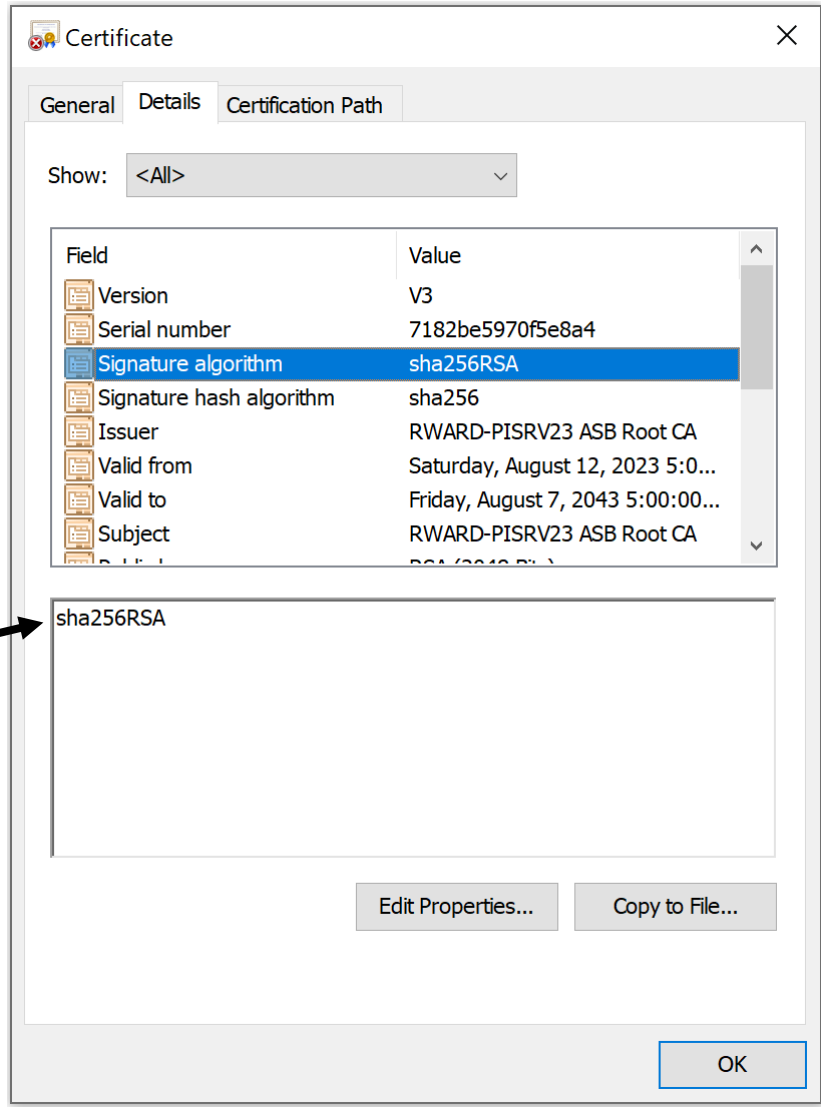
Anatomy of a digital certificate

- Essential components
  - “Issued to” field
  - “Issued by” field
  - Validity date range
  - Public key
  - Signature algorithm (used to verify digital signature)



Anatomy of a digital certificate

- Essential components
  - “Issued to” field
  - “Issued by” field
  - Validity date range
  - Public key
  - Signature algorithm (used to verify digital signature)



Exercise

Who are your certificate authorities?

iPhone

Settings > General > About > Certificate Trust settings > Learn more about trusted certificates > Current Trust Store

Android

Settings > Biometrics and security > Other security settings > View security certificates

Windows

Search > certmgr > Trusted Root Certification Authorities > Certificates

Certificates and the AVEVA PI System

- AVEVA™ PI Server 2023 components can be configured with certificates
  - PI data archive
  - Asset framework
  - Asset analytics
  - Notifications
  - AVEVA Identity Manager
- Applications on the same node can share a certificate
- Can be configured during install or post-install
- Must be trusted on client nodes
- Typically expire every six months

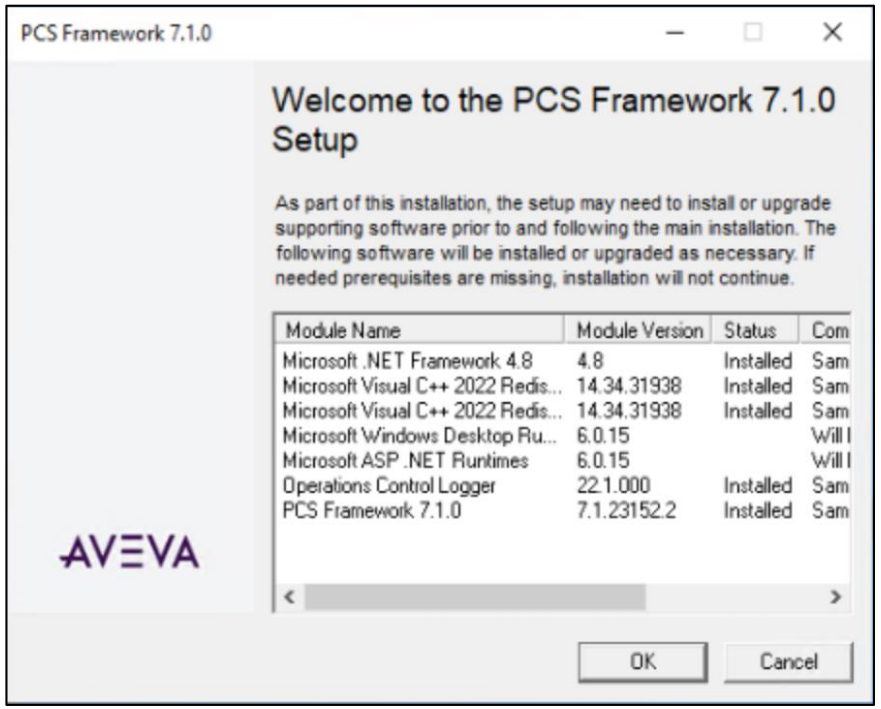
Setting it up (an overview)

Configuration checklist (overview)

1. Obtain third-party certificates
2. Install AIM
3. Register AIM with AVEVA Connect, common cloud platform
4. Install AVEVA PI Server 2023
5. Register AVEVA PI Server with AIM

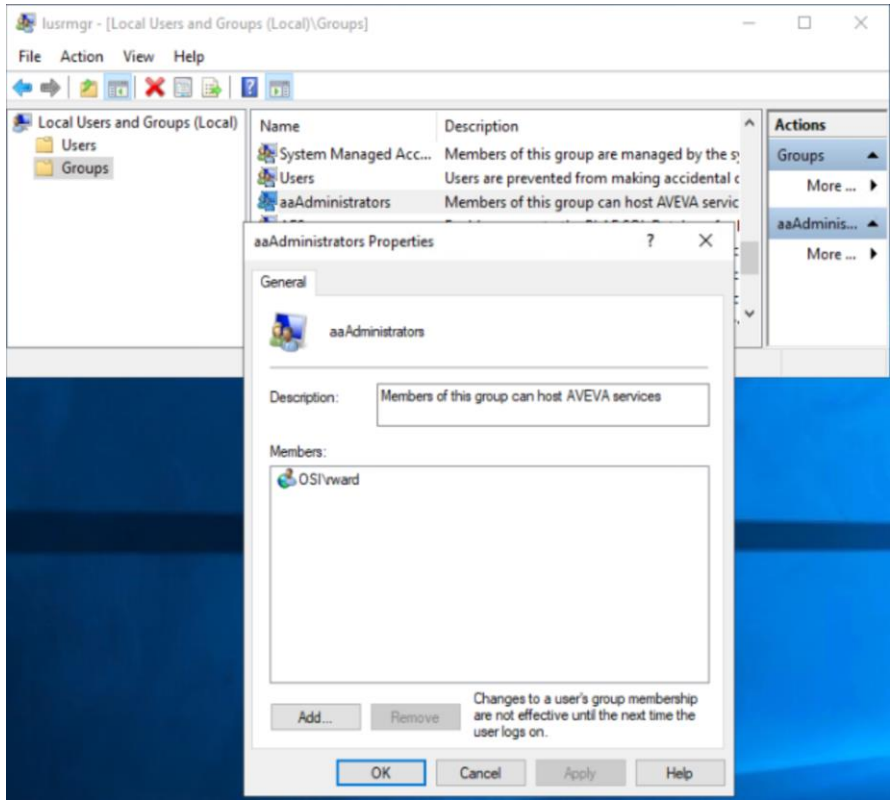
Configuration checklist (AIM)

1. Install AVEVA Identity Manager from **AVEVA PCS for PI** install kit



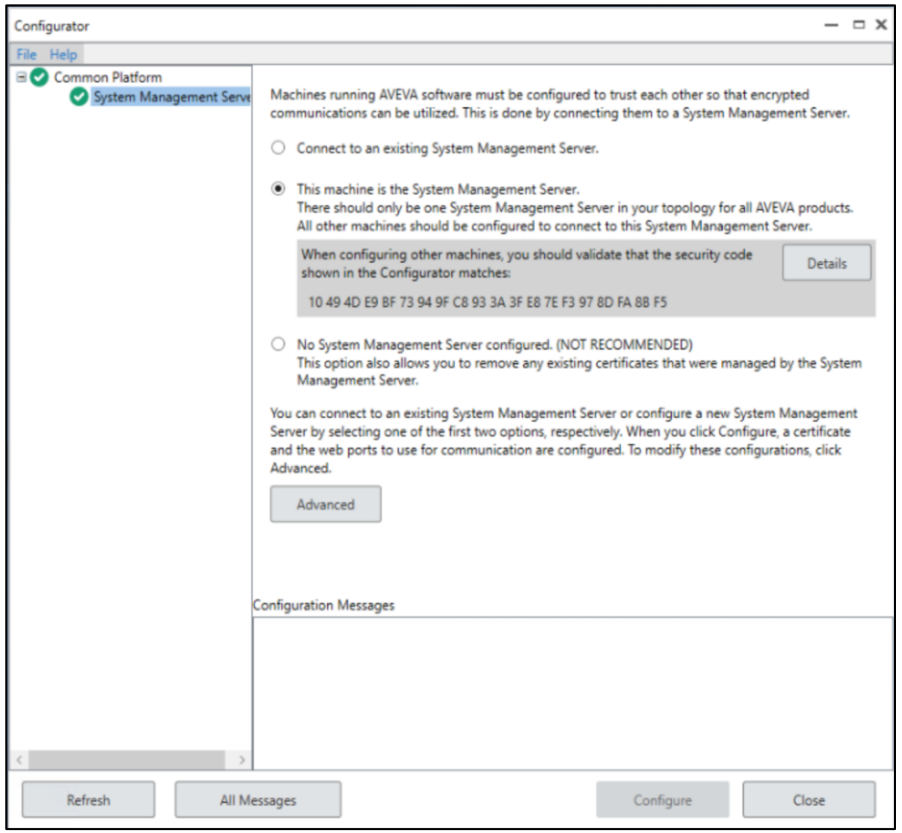
Configuration checklist (AIM)

1. Install AVEVA Identity Manager from **AVEVA PCS for PI** install kit
2. Add the user account used to configure and administer the AVEVA Identity Manager to the aaAdministrators group



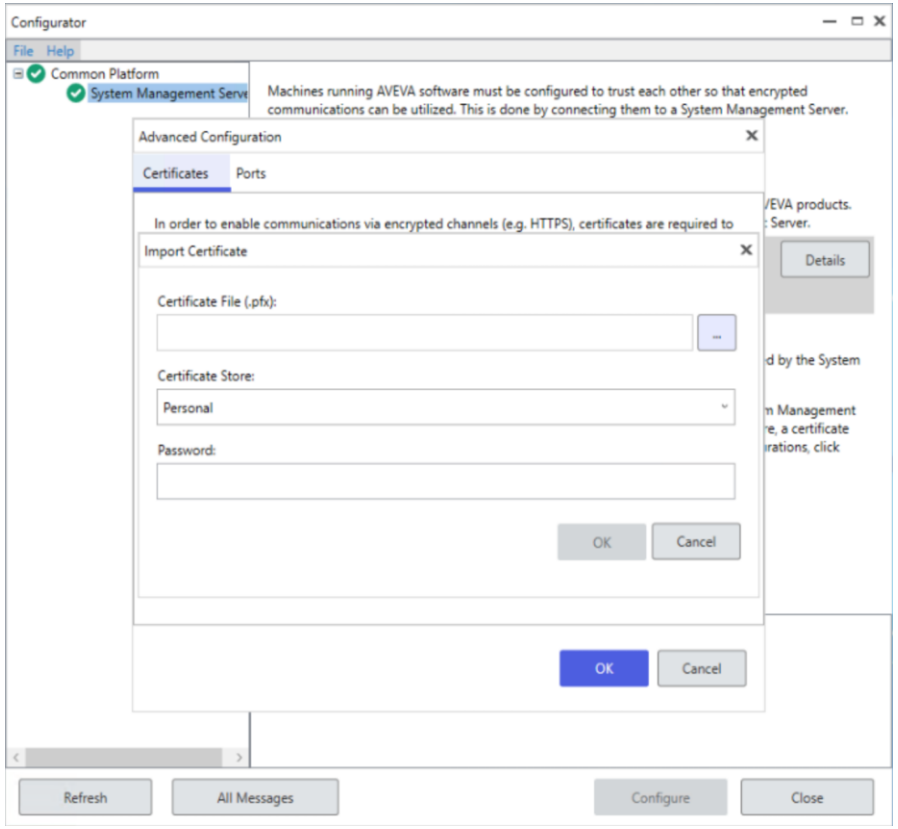
Configuration checklist (AIM)

1. Install AVEVA Identity Manager from AVEVA PCS for PI install kit
2. Add the user account used to configure and administer the AVEVA Identity Manager to the aaAdministrators group
3. Use the Configurator utility to set up AVEVA Identity Manager as the identity service.



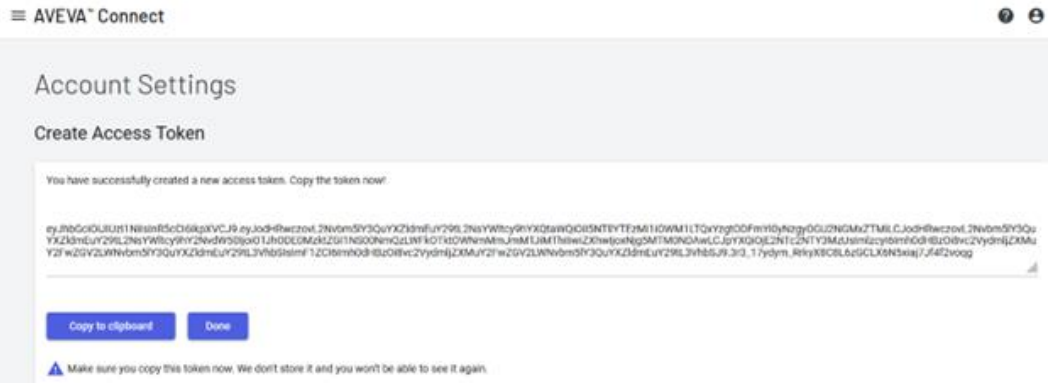
Configuration checklist (AIM)

1. Install AVEVA Identity Manager from AVEVA PCS for PI install kit
2. Add the user account used to configure and administer the AVEVA Identity Manager to the aaAdministrators group
3. Use the Configurator utility to set up AVEVA Identity Manager as the identity service
4. Import a certificate using the configurator utility



Configuration checklist (AIM)

1. Install AVEVA Identity Manager from AVEVA PCS for PI install kit
2. Add the user account used to configure and administer the AVEVA Identity Manager to the aaAdministrators group
3. Use the Configurator utility to set up AVEVA Identity Manager as the identity service
4. Import a certificate using the configurator utility
5. Create an application in the AVEVA Connect portal, create a **client ID**, and then generate an **access token**



Configuration checklist (AIM)

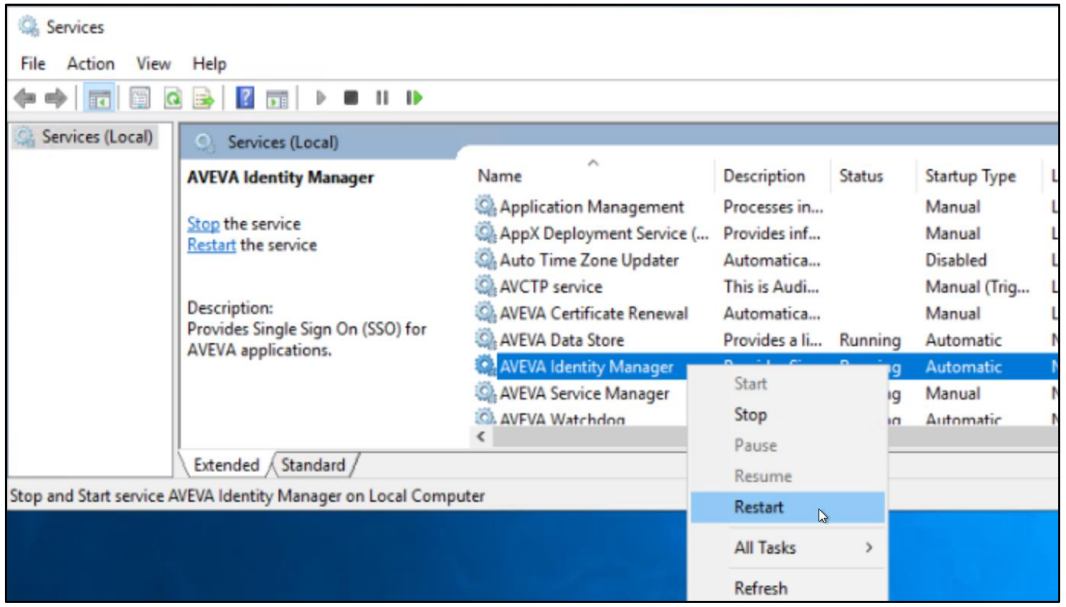
1. Install AVEVA Identity Manager from AVEVA PCS for PI install kit
2. Add the user account used to configure and administer the AVEVA Identity Manager to the aaAdministrators group
3. Use the Configurator utility to set up AVEVA Identity Manager as the identity Service
4. Import a certificate using the configurator utility
5. Create an application in the AVEVA Connect portal, create a **client ID**, and then generate an **access token**
6. Register the AVEVA Connect endpoints with AIM using PowerShell (run the PS commands on AIM node)

Windows PowerShell

```
PS C:\Users\roger.ward> $accessToken = ConvertTo-SecureString
-String "<access token>" -AsPlainText -Force
>>
>> Add-PcsAuthenticationProvider -ClientId <client id> -Access
Token $accessToken -Endpoint https://signin.connect.AVEVA.com
-Name AVEVAConnect -ServicesEndpoint https://services.connect.
AVEVA.com/tt
```

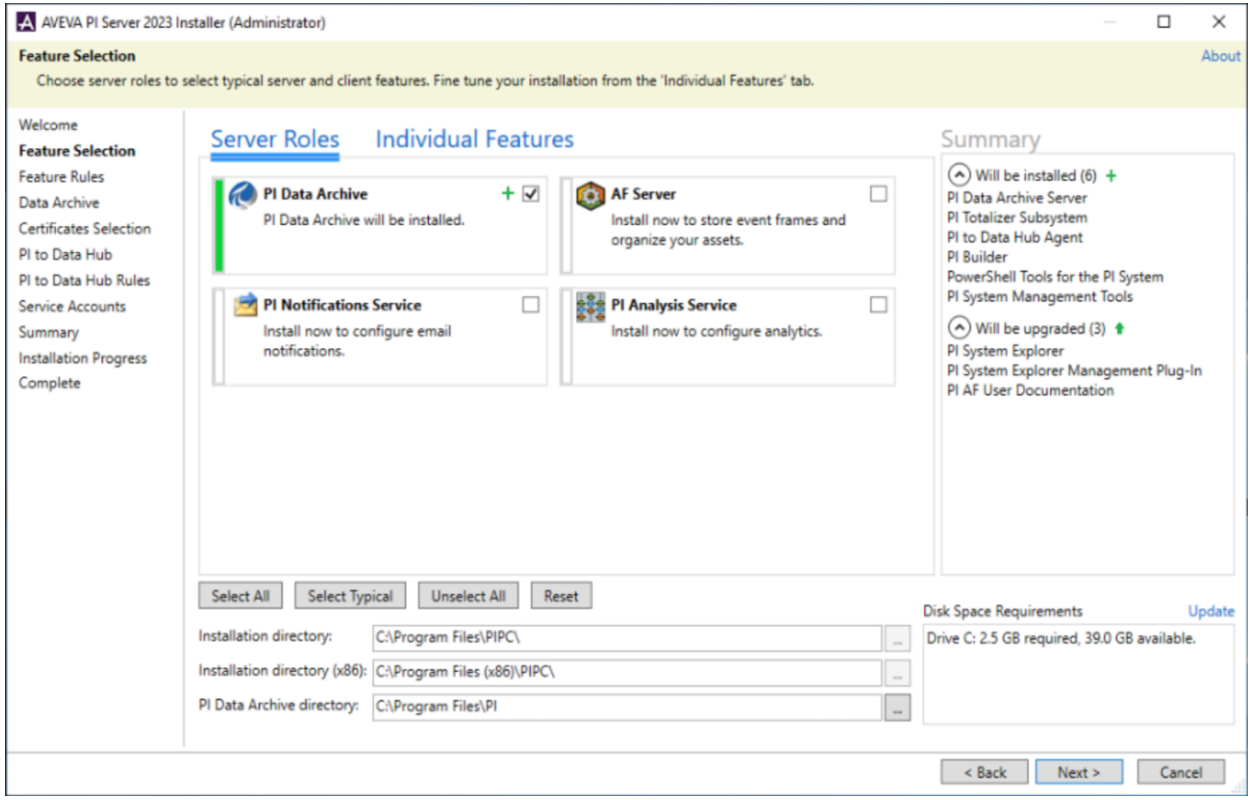
Configuration checklist (AIM)

1. Install AVEVA Identity Manager from AVEVA PCS for PI install kit
2. Add the user account used to configure and administer the AVEVA Identity Manager to the aaAdministrators group
3. Use the Configurator utility to set up AVEVA Identity Manager as the identity service
4. Import a certificate using the configurator utility
5. Create an application in the AVEVA Connect portal, create a **client ID**, and then generate an **access token**
6. Register the AVEVA Connect endpoints with AIM using PowerShell (run the PS commands on AIM node)
7. Restart AIM



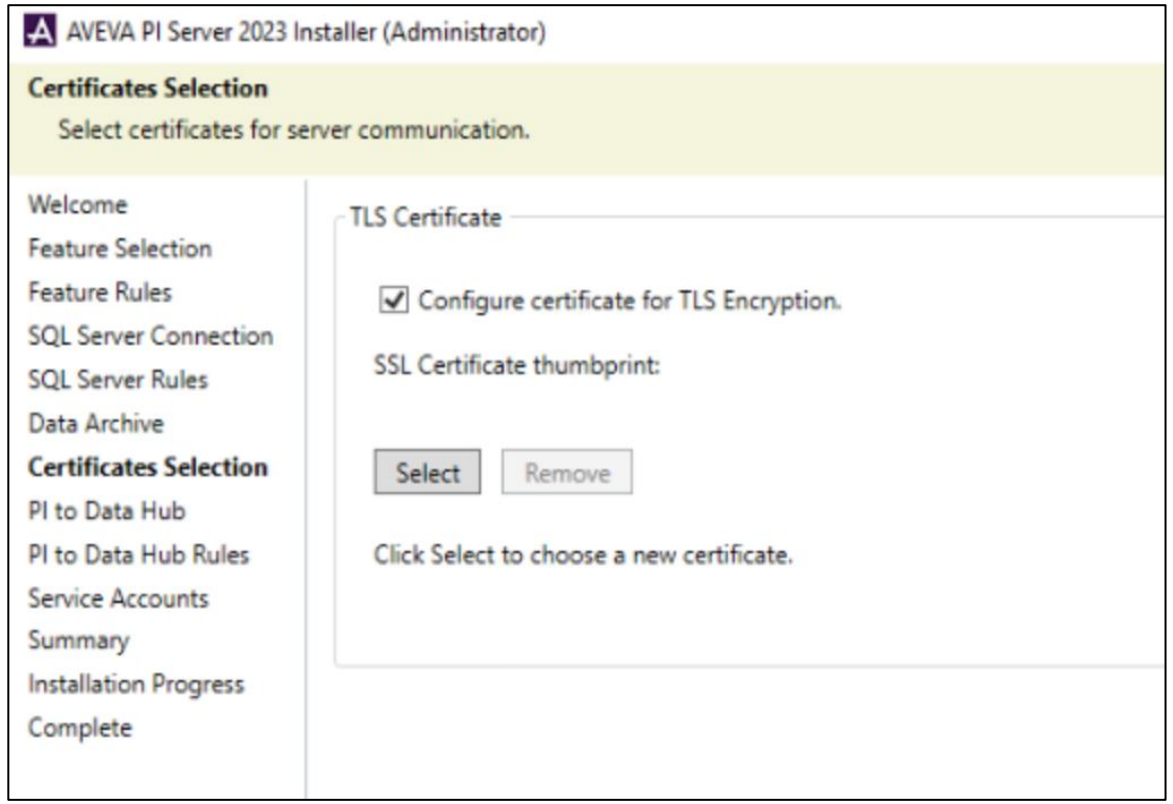
Configuration checklist (data archive)

1. Install PI Data Archive 2023 (as Administrator!)



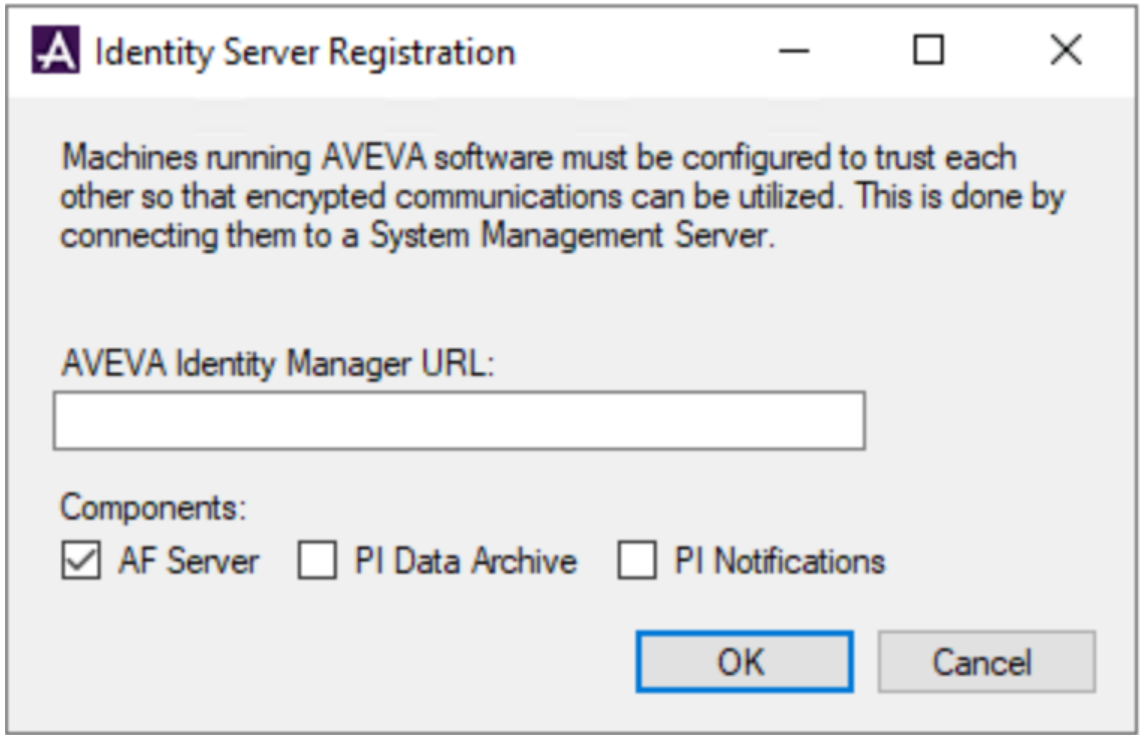
Configuration checklist (data archive)

1. Install PI Data Archive 2023
   - Remember to select “Configure certificate for TLS Encryption”
   - Select “OpenID Connect Authentication requires configuration”



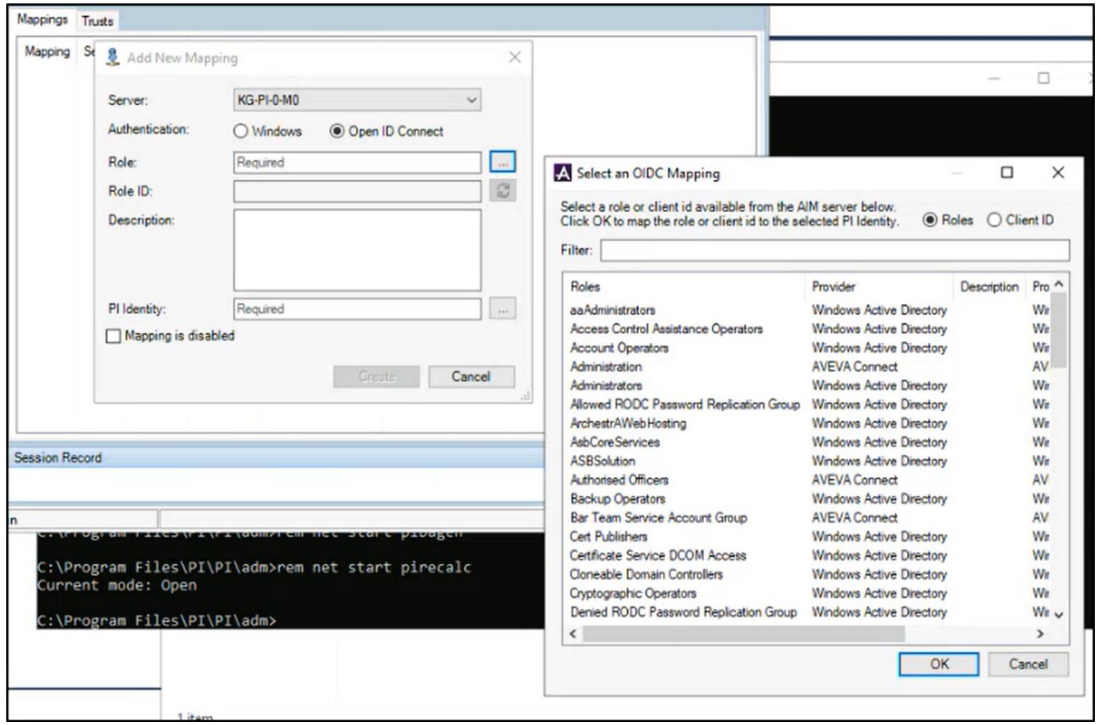
Configuration checklist (data archive)

1. Install PI Data Archive 2023
   - Remember to select “Configure certificate for TLS Encryption”
   - Select “OpenID Connect Authentication requires configuration”
2. Register PI DA with AIM



Configuration checklist (data archive)

1. Install PI Data Archive 2023
   - Remember to select “Configure certificate for TLS Encryption”
   - Select “OpenID Connect Authentication requires configuration”
2. Register PI DA with AIM
3. Map OIDC Roles to PI Identities



FAQ

- Do I need to be connected to the internet to be able to use OIDC?

  Yes! (AIM server does so it can reach reach the IdP)

- Will I still be able to use WIS with Active Directory the same as before?

  Yes!

- Can I upgrade from AVEVA PI Server 2018 to AVEVA PI Server 2023?

  Yes! (Talk to your account manager first)

- Does AVEVA PI System 2023 work with TLS 1.3.

  Not yet!

- Do I need certificates for AVEVA PI System 2023 components if I don't use claims authentication?

  No!

- Is AVEVA PI System network traffic encrypted without TLS?

  Without TLS, only connections authenticated via WIS are encrypted.

Questions?

Please wait for the microphone.

State your name and company.

Please remember to…

Navigate to this session in the mobile app to complete the survey.

Thank you!

AVEVA

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a world leader in industrial software, providing engineering and operational solutions across multiple industries, including oil and gas, chemical, pharmaceutical, power and utilities, marine, renewables, and food and beverage. Our agnostic and open architecture helps organizations design, build, operate, maintain and optimize the complete lifecycle of complex industrial assets, from production plants and offshore platforms to manufactured consumer goods.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. The company is headquartered in Cambridge, UK.

Learn more at www.aveva.com