OCTOBER 24, 2023

Introduction to claims authentication

Related to AVEVA Identity Manager Service "AIMS"

Presented By: Roger Ward



© 2023 AVEVA Group Limited and its subsidiaries. All rights reserved



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

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



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.

)
0	
	\equiv

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





eyJhbGciOiJIUzI
1NiJ9.eyJuYW11I
joiSm91IENvZGVy
In0.5dlp7GmziL2
QS06sZgK4mtaqv0
_xX4oFUuTDh1zHK
4U



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.ey
JzdWIiOiIxMjM0NTY30DkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36P0k6yJV_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"



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:
 - o 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



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"

	Q 🕞 🛛 📰 🕨 🖬 🕪					
rvices (Local)	Services (Local)	-				
	AVEVA Identity Manager	Name	Description	Status	Startup Type	Log On As
	Stop the service Restart the service	AVCTP service AVEVA Certificate Renewal AVEVA Data Store	This is Audi Automatica Provides a li	Running	Manual (Trig Manual Automatic	Local Service Local System NT SERVICE\ArchestrADataStore
		AVEVA Identity Manager	Provides Sin	Running	Automatic	NT SERVICE\AIMTokenHost
	Description: Provides Single Sign On (SSO) for AVEVA applications.	AVEVA Service Manager AVEVA Watchdog Azure Hybrid Instance Meta AzureAttestService	Facilitates Ia Manages th Azure Hybri	Running Running Running Running	Manual Automatic Automatic (D Automatic	NT SERVICE\AsbServiceManager NT SERVICE\Watchdog_Service NT SERVICE\himds Local System



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:
 - o Ensuring the identity of remote server
 - o 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









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)

👼 Certi	ificate												×
General	Detai	s c	ertific	ation	Path								
Show								~					
51101.								Ŷ					
Field						Va	lue						^
📑 Si	ignature	algo	rithm			sh	a256	RSA					
📑 Si	- ignature	hash	n algo	rithm		sh	a256						
🛛 🛅 Is	suer					R۱	NARE)-PIS	RV23	ASB	Root	CA	
	alid from	n				Sa	turda	ay, Au	igust	12, 2	023 !	5:0	
	alid to					Fr	iday,	Augu	st 7, 1	2043	5:00	:00	
S S	ubject					R۱	NARE)-PIS	RV23	ASB	Root	CA	
P	ublic key	'				RS	SA (20	048 B	lits)				
PI	ublic key	para	mete	ers		05	00						
. E							5.12			·/ -			
308	32 01	0 a	02	82	01	01	0 0	b 5	22	a 1	14	16	^
0 c 6	59 0a	10	5 d	e f	e 2	а0	70	42	a 9	54	e d	55	
CC C)6 d4	50	42	5 d	с6	СС	fb	63	0e	5 c	d 1	0 d	
C 9 C	178d	cd	6a - 0	53	03	1a	2 C	b9	21	2a	20	a 8	
91 Z	17 59 De fo	48 £1	19 25	/6 6 f	50 d 1	2 C	44	D I 6 7	4 C + 2	/I fa	53 16	60 60	
4 f 8	30 10 38 91	90		03	ui 7a	1 h	60 60	5 h	75	re re	10 61	02	
4b b	ba 48	cd	3 f	03	38	ca	e 9	5 b	2 b	9 e	cb	2 e	
e4 c	:7 d1	с8	33	97	3 a	1 e	0 f	e 9	fa	28	10	1 d	
f8 f	E7 ba	9 c	d 8	a f	25	84	08	33	21	21	bе	d f	~
					ł	Edit P	rope	rties	•	C	òopy t	to File	
												O	K

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)

Certificate	
General Details Certification Pa	th
Show: <all></all>	~
Field	Value
🛅 Version	V3
🛅 Serial number	7182be5970f5e8a4
📕 Signature algorithm	sha256RSA
📴 Signature hash algorithm	sha256
🛅 Issuer	RWARD-PISRV23 ASB Root CA
🛅 Valid from	Saturday, August 12, 2023 5:0
🛅 Valid to	Friday, August 7, 2043 5:00:00
🛅 Subject	RWARD-PISRV23 ASB Root CA
SNAZSOKSA	
	Edit Properties Copy to File



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

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

PCS Framework 7.1.0		-		\times
	Welcome to the PCS Setup As part of this installation, the setup supporting software prior to and fo following software will be installed needed prerequisites are missing, in	S Framewo p may need to insi llowing the main i or upgraded as n nstallation will not	tall or upgranstallation.	.0 ade The If
	Module Name Microsoft .NET Framework 4.8 Microsoft Visual C++ 2022 Redis Microsoft Visual C++ 2022 Redis Microsoft Windows Desktop Ru Microsoft ASP .NET Runtimes Operations Control Logger PCS Framework 7.1.0	Module Version 4.8 14.34.31938 14.34.31938 6.0.15 6.0.15 22.1.000 7.1.23152.2	Status Installed Installed Installed	Com Sam Sam Sam Will I Sam Sam
AVEVA	<			>
		ОК	Cano	el

- 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

Local Users and Groups (Local)	Name	Description		^	Actions
Users Groups	System Managed Acc	Members of this group are managed by the s			Groups
	B Users	Users are prevented from a Members of this group ca	making accidental o		More
		members of this group ca	IT HOST AVEVA SERVIC		aaAdminis
	aaAdministrators Properties		? ×		More
	General		-		
	N		~		
	aaAdministrators				
	-				
	Description: Members of this group can host AVEVA services				
	Members:				
	SI\ward				
		Changes to a user's grou	ap membership		

- Install AVEVA Identity Manager from AVEVA PCS for PI install kit
- 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.

Configurator	>
File Help	
Common Platform System Management Serve	Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.
	This machine is the System Management Server. There should only be one System Management Server in your topology for all AVEVA products. All other machines should be configured to connect to this System Management Server.
	When configuring other machines, you should validate that the security code shown in the Configurator matches:
	10 49 4D E9 BF 73 94 9F C8 93 3A 3F E8 7E F3 97 8D FA 8B F5
	 No System Management Server configured. (NOT RECOMMENDED) This option also allows you to remove any existing certificates that were managed by the System Management Server.
	You can connect to an existing System Management Server or configure a new System Management Server by selecting one of the first two options, respectively. When you click Configure, a certificate and the web ports to use for communication are configured. To modify these configurations, click
	Advanced Advanced
e	Configuration Messages
Refresh All Me	ssages Configure Close

- 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



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

0	θ
tovil 2Nivbmáli Návc2Vydmij2 Nogg	uoo Mix
	20x6.2%/dm8/Y Ddivc2%/dm8/Z Divog

- Install AVEVA Identity Manager from AVEVA PCS for PI install kit
- 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	_		×
<pre>PS C:\Users\roger.ward> \$accessToken = ConvertToString "<access token="">" -AsPlainText -Force >></access></pre>	Secur	eStrin	g ^
<pre>>> Add-PcsAuthenticationProvider -ClientId <clien \$accesstoken="" -endpoint="" -name="" -servicesendpoint="" aveva.com="" avevaconnect="" https:="" pre="" serv="" signin.conne="" token="" tt<=""></clien></pre>	t id> ct.AV ices.	-Acce EVA.co connec	vss vm t.

- Install AVEVA Identity Manager from AVEVA PCS for PI install kit
- 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



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



1. Install PI Data Archive 2023

- Remember to select "Configure certificate for TLS Encryption"
- Select "OpenID Connect Authentication requires configuration"

AVEVA PI Server 2023 Installer (Administrator)						
Certificates Selection Select certificates for ser	ver communication.					
Welcome Feature Selection Feature Rules SQL Server Connection SQL Server Rules Data Archive Certificates Selection PI to Data Hub PI to Data Hub Rules Service Accounts Summary Installation Progress Complete	TLS Certificate Image: Configure certificate for TLS Encryption. SSL Certificate thumbprint: Select Remove Click Select to choose a new certificate.					

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

A Identity Server Registration	_		\times
Machines running AVEVA software must be co other so that encrypted communications can b connecting them to a System Management Se	onfigured to e utilized. rver.	o trust each This is don	h e by
AVEVA Identity Manager URL:]	
Components: AF Server PI Data Archive PI	Notification	าร	
	ОК	Cano	el

- 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

Mapping Se	🖇 🤱 Add New Map	ping	×				-
	Server:	KG-PI-0-M0	~			-	
	Authentication:	() Windows () Open ID Connect					
	Role:	Required		Select an OIDC Mapping		- D	×
	Role ID:		3	a select an one chapping		-	~
	Description: Select a role or client id available from the AIM server below. Click OK to map the role or client id to the selected PI Identity. Roles						
				Roles	Provider	Description	Pro ^
	PI Identity:	Required		aaAdministrators	Windows Active Directory		Wir
	Mapping is disa	bled		Access Control Assistance Operators	Windows Active Directory		Wit
				Account Operators	Windows Active Directory		Wir
		Create	Cancel	Administration	AVEVA Connect		AV
		anosis	direct	Administrators	Windows Active Directory		Wit
				Allowed RODC Password Replication Group	Windows Active Directory		Wit
				ArchestrAWebHosting	Windows Active Directory		Wr
in Dee				AsbCoreServices	Windows Active Directory		Wit
sion reco	ord			ASBSolution	Windows Active Directory		Wa
				Authorised Officers	AVEVA Connect		AV
	2			Backup Operators	Windows Active Directory		Wir
				Bar Team Service Account Group	AVEVA Connect		AV
0. 111	B. 0. 11103 (11)	(12 (damy) cm file 5 cdi c prodg		Cert Publishers	Windows Active Directory		Wr
	ogram Files\PI\	PI\adm>rem net start pirec	alc	Certificate Service DCOM Access	Windows Active Directory		Wit
C:\Pro	nt mode: Open			Contemple Domain Controllers	Windows Active Directory		W
C:\Pro Currer				Cryptographic Operators	Windows Active Directory		W
C:\Pro Currer				Denied NODC Password Replication Group	Windows Active Directory		WE V
C:\Pro Currer C:\Pro	ogram Files\PI\	PI\adm>		<			>
C:\Pro Currer C:\Pro	ogram Files\PI\	Al/adm>		<			>



- Do I need to be connected to the internet to be able to use OIDC?
 Yes! (<u>AIM server</u> 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!

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.



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