The Certificate Strikes Back

ADCS’s Path to Entra

Fletcher Davis

Senior Manager – Research & Data Science

Introductions

Fletcher Davis

- Senior Manager of Research & Data Science @ BeyondTrust
- Former Red Team @ CrowdStrike & Mandiant
- Twitter: @gymR4T

Agenda

- **Foundation: Understanding The Components**
  - Active Directory Certificate Services (ADCS)
  - Microsoft Entra Certificate-Based Authentication (CBA)
- **Crossing The Bridge: Pivoting From AD to Entra**
  - Attack Chain & Demo
  - Posture Recommendations
  - Detection Strategies
- **Takeaways**

Acknowledgements

- Will Schroeder - SpecterOps
- Lee Christensen – SpecterOps
- Jonas Bülow Knudsen - SpecterOps
- Andy Robbins – SpecterOps
- Uwe Gradenegger – m2trust

Bridging Silos

- Organizations are highly complex and connected systems
- Understanding trust relationships and interconnections is essential for effective threat response

Requires a holistic approach on protecting the entire ecosystem rather than isolated components

Active Directory Certificate Services

Fundamentals

What is ADCS?

– Speed Run Edition

- Active Directory Certificate Services (ADCS) is a Microsoft Server role that functions as Microsoft's Public Key Infrastructure implementation
- Allows organizations to issue and manage digital certificates for authentication, encryption, and digital signatures
- Key components:
  - Certificate Authority
  - Certificate Template
  - Digital Certificate

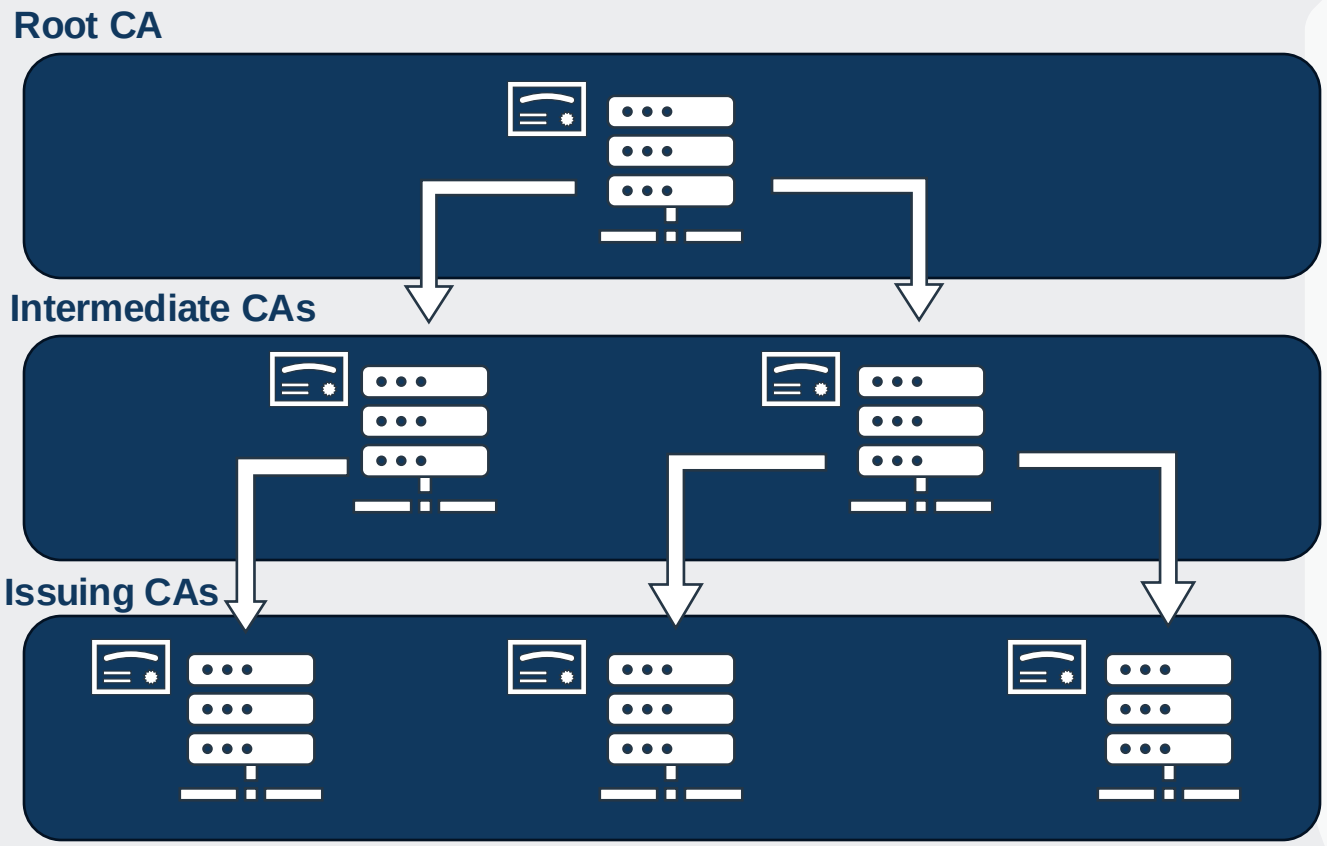
https://posts.specterops.io/certified-pre-owned-d95910965cd2

Certificate Authority

- Responsible for attesting to the identity of users, computers, and organizations
- Core component of Active Directory Certificate Services
- Issues, validates, and revokes certificates
- Windows Server supports different types:
  - Enterprise Certificate Authority
    - Integrated with Active Directory Domain Services (AD DS)
    - Issues certificate templates
  - Standalone Certificate Authority
    - Do not require Active Directory Domain Services (AD DS)
    - Do not issue certificate templates

https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/certification-authority-role

Certificate Authority



Root Certificate Authority

- Top of the certification hierarchy
- Self-signed certificate
- If Root CA is compromised, all CAs in the hierarchy and all certificates issued are considered compromised
- You can maximize security by maintaining the Root CA in an offline state

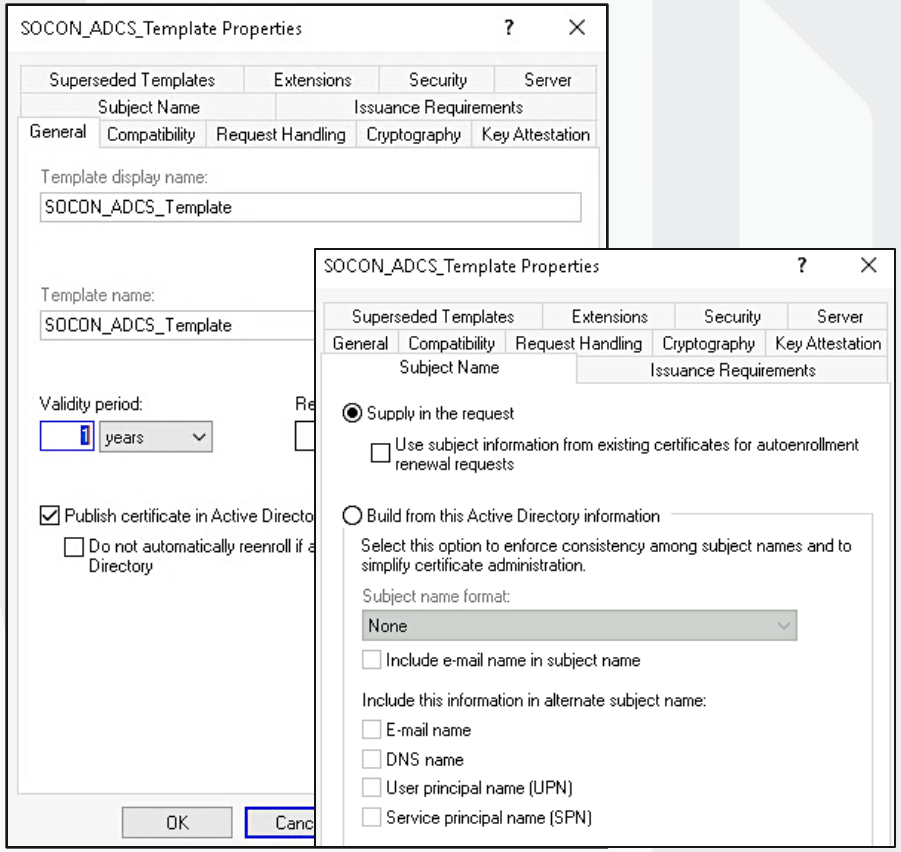
Subordinate Certificate Authority

- Comprised of intermediate and Issuing CAs
- Tiering increases security, flexibility, and scalability
- First Subordinate CA in the hierarchy obtains its certificate from the Root CA

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786436%28v=ws.11%29

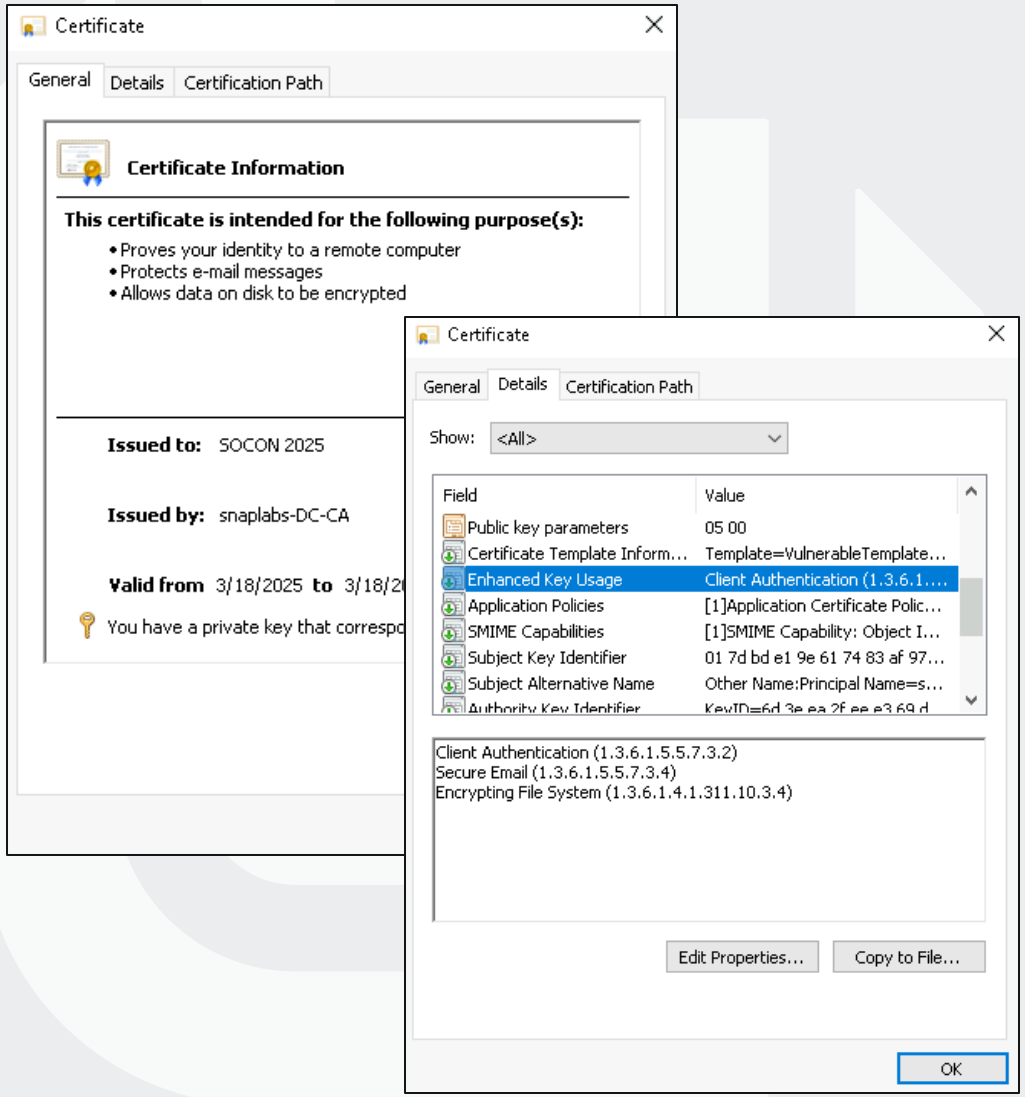
Certificate Template

- Predefined configurations that specify a certificates properties and purpose
  - Common purposes:
    - Client Authentication (1.3.6.1.5.5.7.3.2)
    - Code Signing (1.3.6.1.5.5.7.3.3)
    - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
  - Certificate validity period
  - Issuance requirements
    - Manager approval
    - Authorized signatures
- Published by Enterprise Certificate Authorities



Digital Certificate

- Electronic document that cryptographically verifies the authenticity of a digital entity
- Binds a public key to a specific identity
  - Validated by CA's digital signature
- Issued by Certificate Authority upon certificate request (CSR)
- Contains identifying information and usage purposes
  - Ex. Client Authentication, etc.



Certificate Enrollment Process

Client

Client initiates certificate enrollment process by generating a new public/private key pair.

The client stores the certificate in the Windows Certificate Store.

The public key is included in the Certificate Signing Request (CSR), while the private key is stored locally.

Certificate can be used to perform actions defined in certificates EKU

The client establishes a network connection to the Enterprise CA and sends the CSR to the server

SOCON Template

EKU: Client Auth

Enrollment Rights: Domain Users

Requires Manager Approval: No

Enterprise CA

The Enterprise CA performs a series of verification checks prior to issuing a certificate.

Checks include:

- Template exists and CSR information complies with settings
- Client exists and is authorized to request a certificate

Once client and CSR pass checks, the Enterprise CA issues the certificate

The information in the certificate is based on the CSR and certificate template

The certificate is signed with the CA private key

https://posts.specterops.io/certified-pre-owned-d95910965cd2

Common Misconfigurations

- Misconfigured Certificate Templates
  - Allowing certificate requesters to specify subjectAltName (SAN) in CSR
- Poorly configured certificate template access control
  - Unintended Access Control Entries (ACEs) over certificate template
    - Active Directory principals can edit security settings in templates
- Poorly configured certificate authority access control
  - Unintended Access Control Entries (ACEs) over certificate authority

Misconfigured Certificate Template Abuse

https://posts.specterops.io/certified-pre-owned-d95910965cd2

ADCS Resources

adcs abuse

All | Images | Videos | News | Shopping | Short videos | Forums | More | Tools

Black Hills Information Security
https://www.blackhillsinfosec.com › Blog

Abusing Active Directory Certificate Services - Part One

Oct 5, 2023 — Certipy is a Python-based offensive security tool that can be used to enumerate and **abuse** vulnerable **ADCS**. Certipy is the tool I use most ...

NCC Group
https://www.nccgroup.com › research-blog › defending-...

An Expert Guide to Fortifying Active Directory Certificate ...

An Enterprise Security Certificate (ESC) attack is a cyber-attack which **abuses** misconfigured certificate templates granting higher privileges to attackers.

BeyondTrust
https://www.beyondtrust.com › Resources › Blog

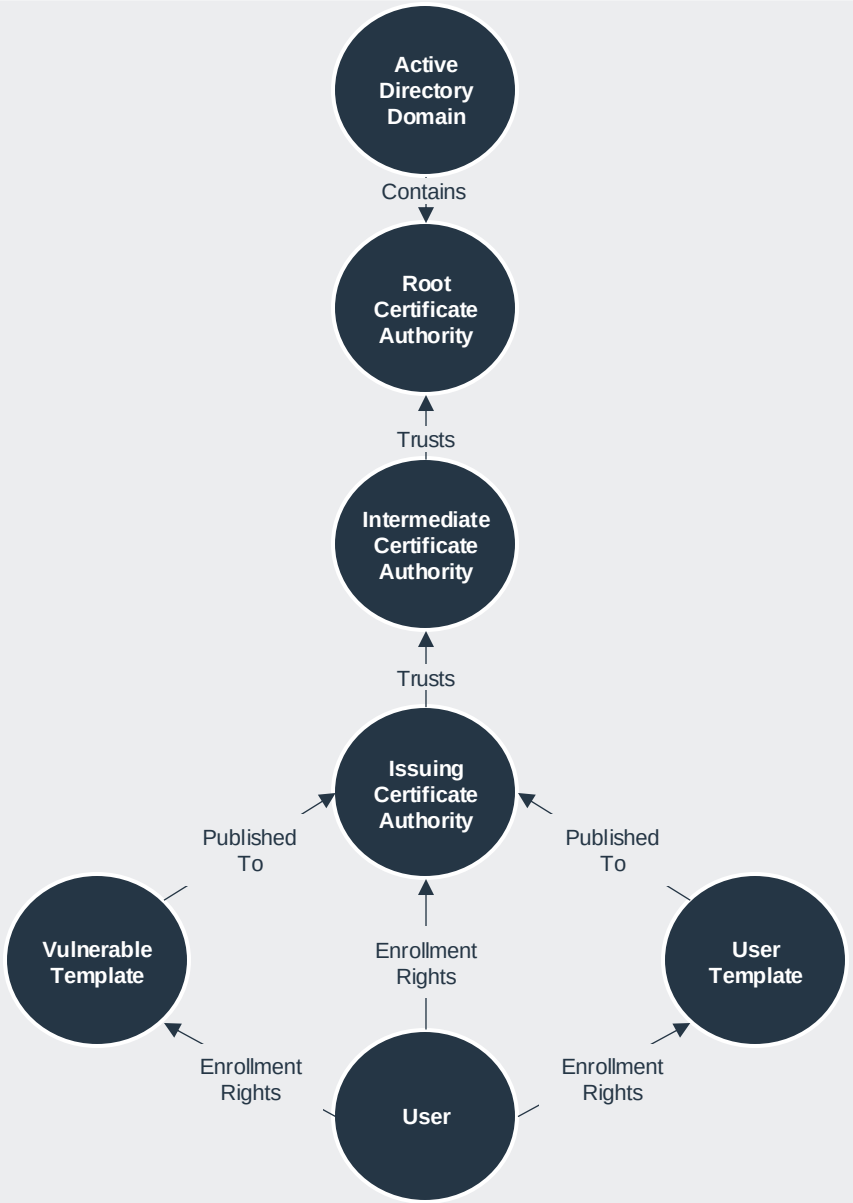
AD CS 101: How to Detect and Mitigate ESC1 Attacks

Jun 18, 2024 — ESC1 (Enterprise CA Security Configuration) Attacks – In blog one, we'll explore ESC1 attacks, which **abuse** misconfigured certificate templates ...

SpecterOps
https://posts.specterops.io › ...

Certified Pre-Owned. Active Directory Certificate Services...

Jun 22, 2021 — TL;DR Active Directory Certificate Services has a lot of attack potential! Check out our whitepaper "Certified Pre-Owned: **Abusing** Active ...

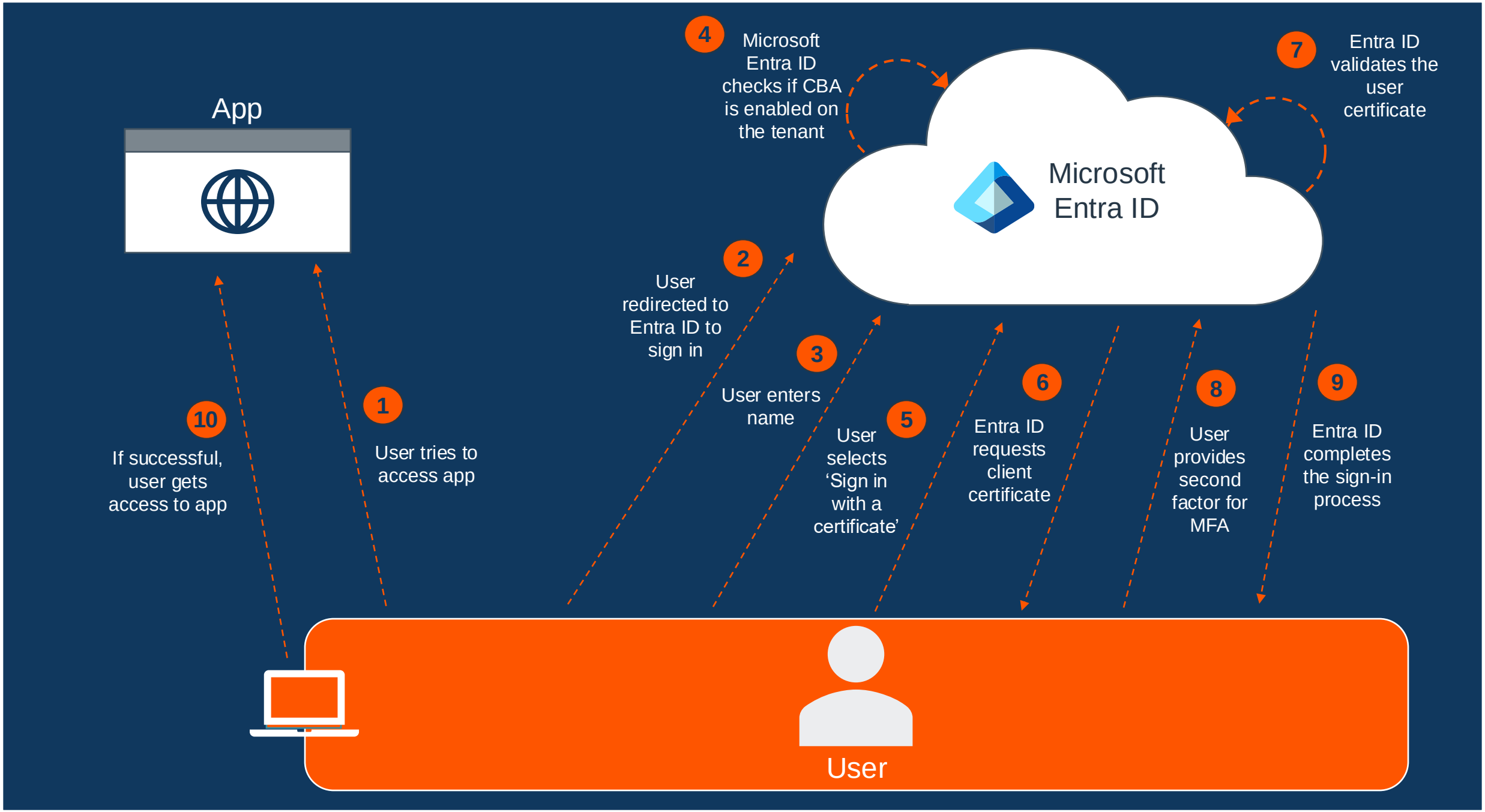

Active Directory Domain
Contains
Root Certificate Authority
Trusts
Intermediate Certificate Authority
Trusts
Issuing Certificate Authority
Published To
Published To
Vulnerable Template
User Template
Enrollment Rights
Enrollment Rights
Enrollment Rights
User

Microsoft Entra Certificate-Based Authentication

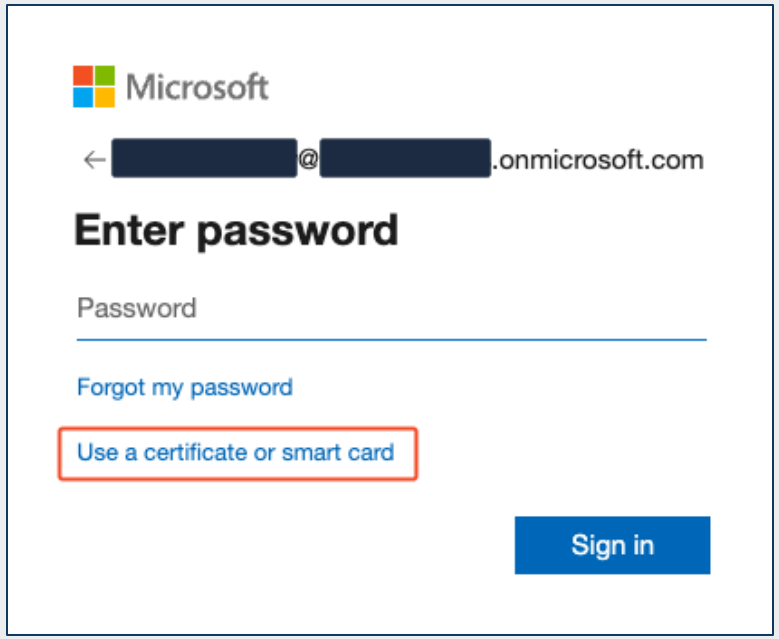
Overview

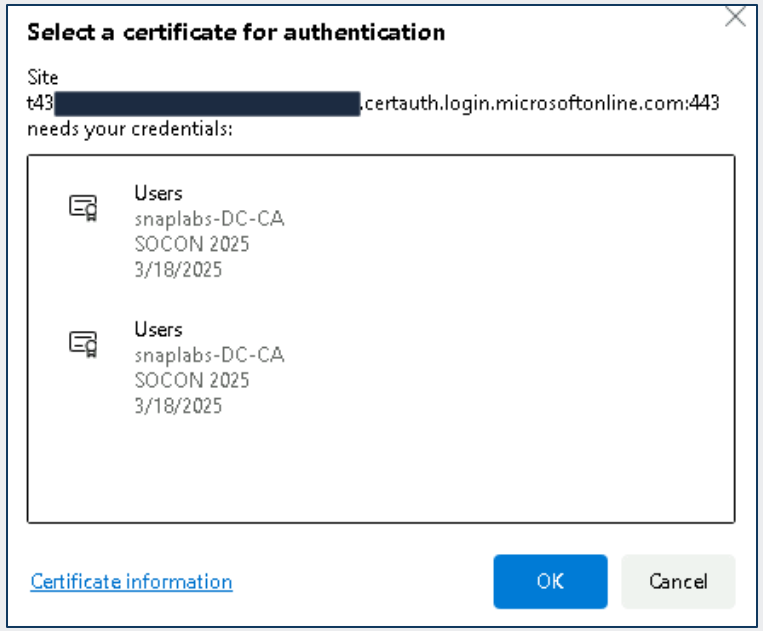
What is Microsoft Entra CBA?

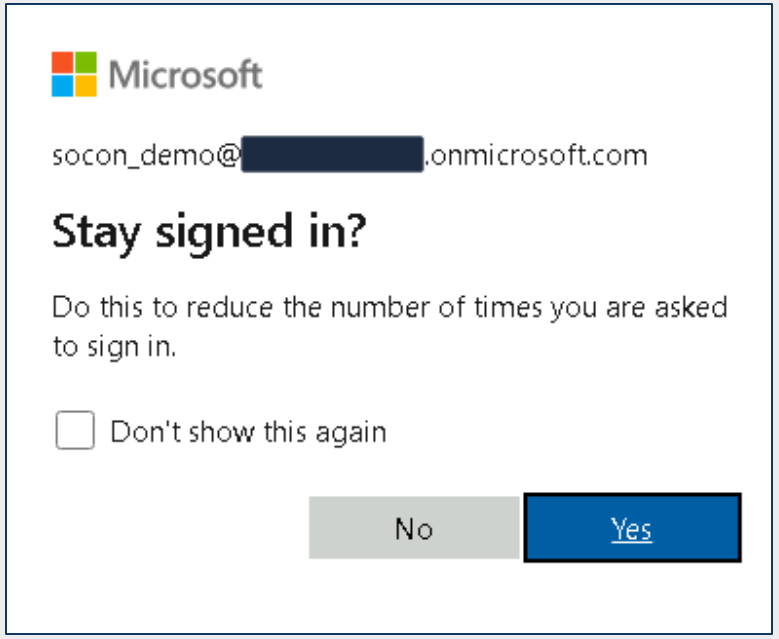
- Microsoft Authentication Method that allows users to authenticate directly against their Microsoft Entra ID tenants using X.509 certificates
- Part of Microsoft’s push to get customers to adopt phishing resistant authentication and move away from traditional federated authentication services (ex. ADFS)
- Works with Conditional Access Policies to enforce MFA



https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive







https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive

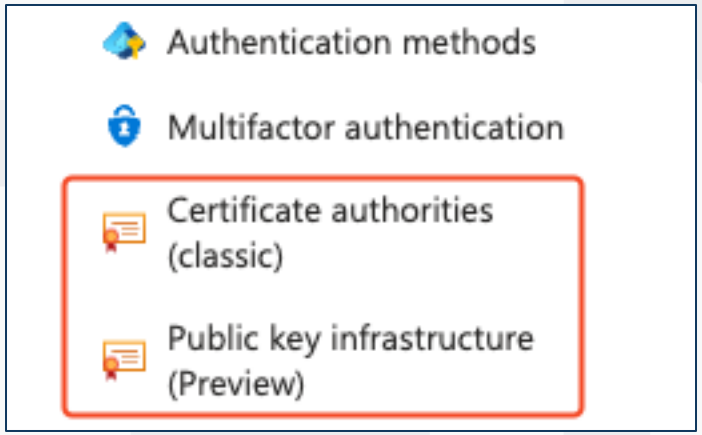
Microsoft CBA Components

- Certificate Authority Trust Store
  - Configure trusted CAs
- Username Binding Policies
  - Define mapping between certificates and Entra users
- Authentication Binding Policies
  - Determine strength of certificate authentication

https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-certificate-based-authentication

Certificate Authority Trust Store

- Microsoft Entra's trust store maintains certificate authorities that are trusted for certificate-based authentication
- Entra allows uploading root and subordinate CA certificates to establish an organization's chain of trust
- Each CA can define a certificate revocation list (CRL)
  - If CRL not configured, Microsoft Entra ID does not perform any CRL checking



PKIs | Deleted PKIs

Create PKI | Edit | Delete | Refresh | Edit columns | Got feedback?

Search | Add filter

1 PKI found

	Display name	Last operation status	Status details
☐	SOCON	Succeeded	

SOCON

Certificate Authorities

CAs | Deleted CAs

Upload CBA PKI | Add certificate authority | Edit | Delete | Refresh | Edit columns | Got feedback?

Search | Add filter

1 certificate authority found

	Name	Expired	Root cert	Issuer hints enabled	Thumbprint	CRL endpoint
☐	CN=snaplabs-DC-CA, DC=snaplabs, ...	No	Yes	Yes	FD600F39AA91E77[redacted]	

User Binding Policies

- Username binding policies specify how certificates are mapped to user identities in Entra
- There are two types of username binding policies:
  - High-Affinity Bindings
  - Low-Affinity Bindings
- Organizations can set up multiple username binding policy rules
  - Priority of rules depends on configuration order and authentication binding settings
  - Entra attempts to validate all configured username bindings until one results in a match

Username Binding Policies

Certificate Field	Entra User Attribute	Affinity Level
PrincipalName	userPrincipalName onPremisesUserPrincipalName certificateUserIds	Low-Affinity
RFC822Name	userPrincipalName onPremisesUserPrincipalName certificateUserIds	Low-Affinity
IssuerAndSubject (Preview)	certificateUserIds	Low-Affinity
Subject (Preview)	certificateUserIds	Low-Affinity
SKI	certificateUserIds	High-Affinity
SHA1PublicKey	certificateUserIds	High-Affinity
IssuerAndSerialNumber (Preview)	certificateUserIds	High-Affinity

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive

Enable and Target | **Configure**

Certificate revocation list (CRL) validation

This setting requires a CRL check for every certificate authority (CA). If the CRL distribution point is empty or not configured for your CAs, the authentication will fail. You can exempt certificate authorities from the CRL validation requirement.

Require CRL validation (recommended) ☐

Issuer Hints

Enable issuer hints to show only the valid certificates in the certificate picker during authentication. Learn more

Issuer Hints ☑

Authentication binding

The authentication binding policy helps determine the strength of your certificate-based authentication method policy as single-factor or multi-factor and low affinity or high affinity. Override default settings with special rules. Learn more

Protection Level ⓘ
- (●) Single-factor authentication
- ( ) Multi-factor authentication

Required Affinity Binding ⓘ
- (●) Low
- ( ) High

+ Add rule

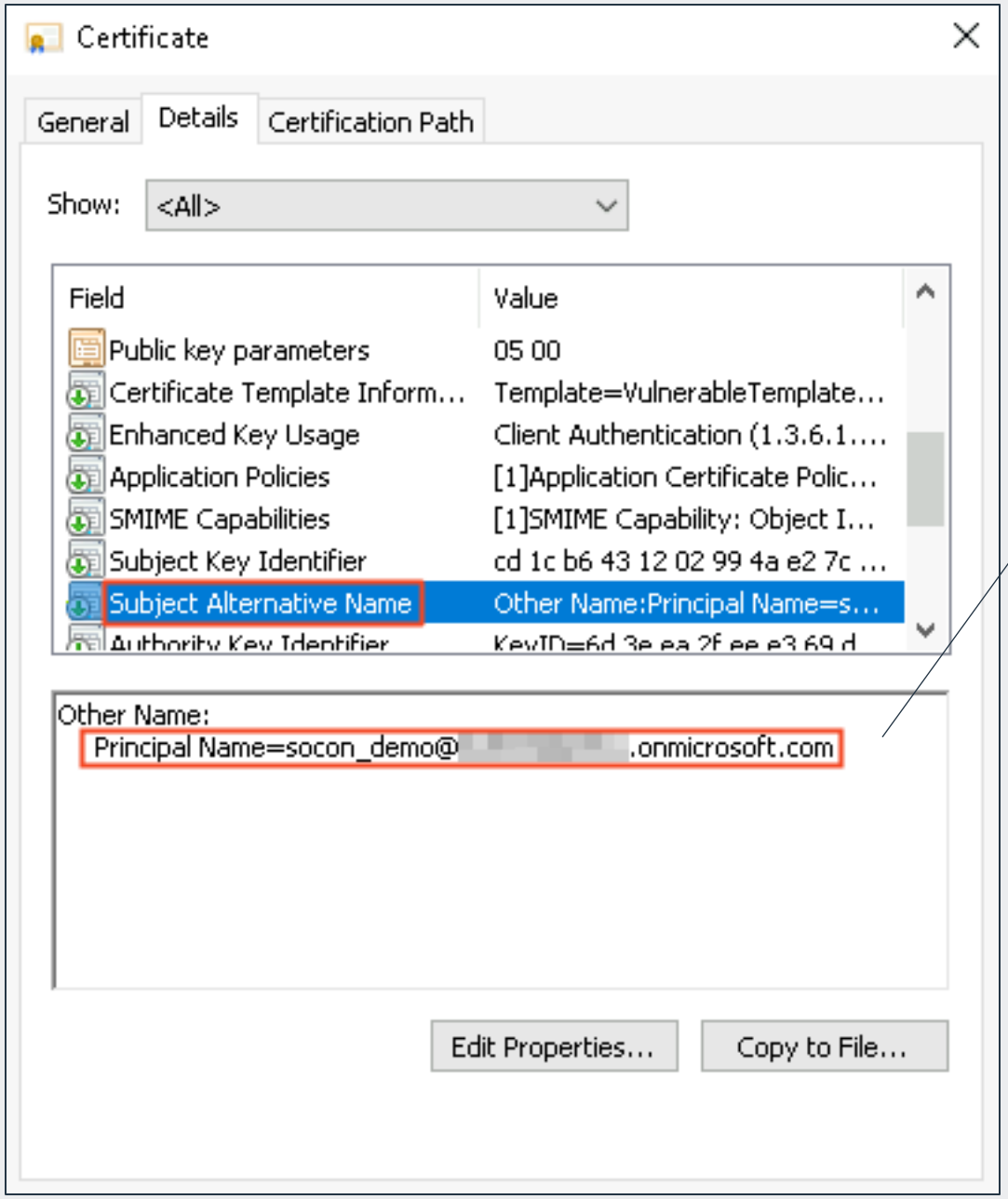
Certificate issuer	Policy OID	Authentication strength	Affinity binding
CN=snaplabs-DC-CA, DC=snaplabs, DC=local	N/A	Multi-factor	Low

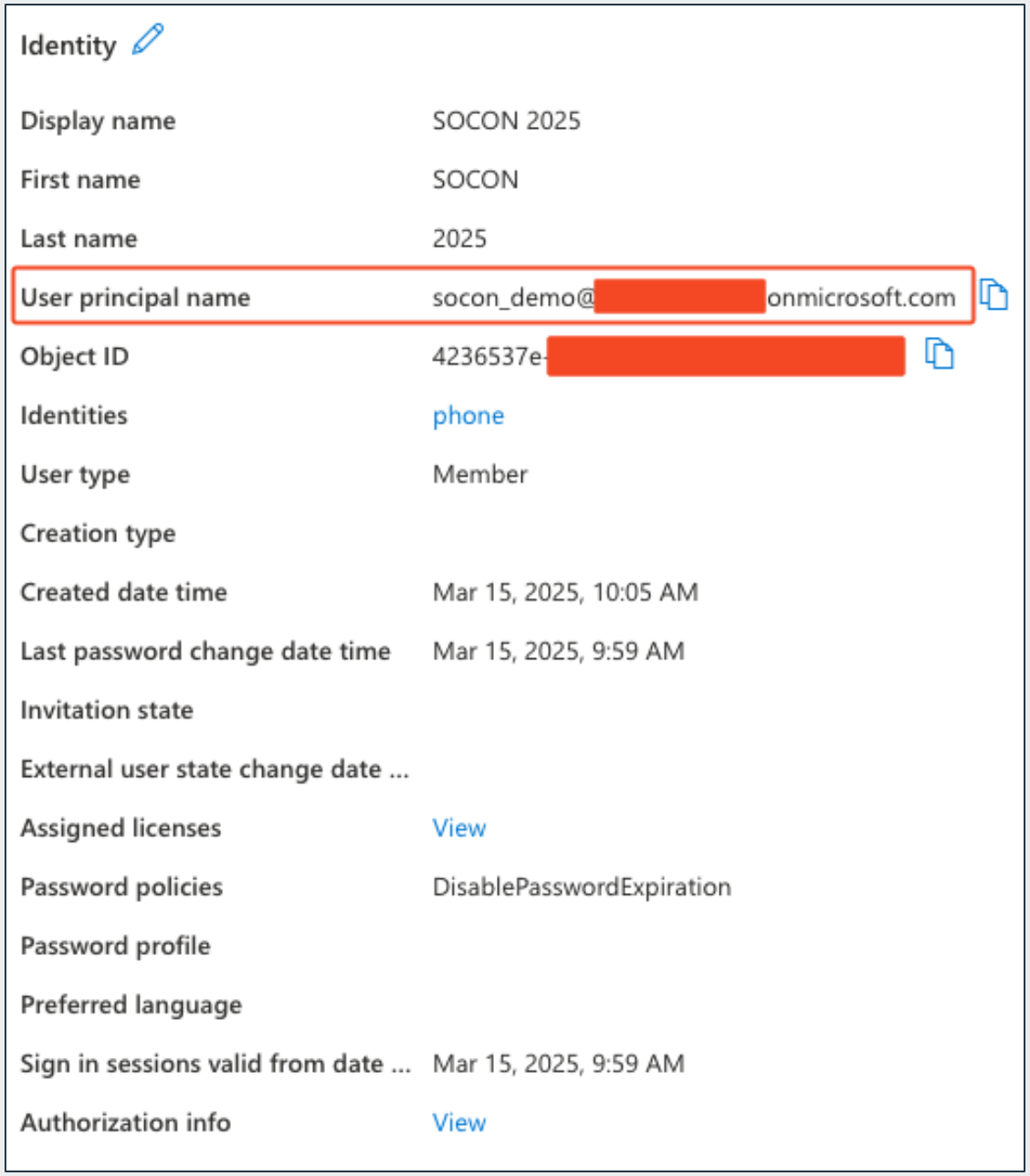
Username binding

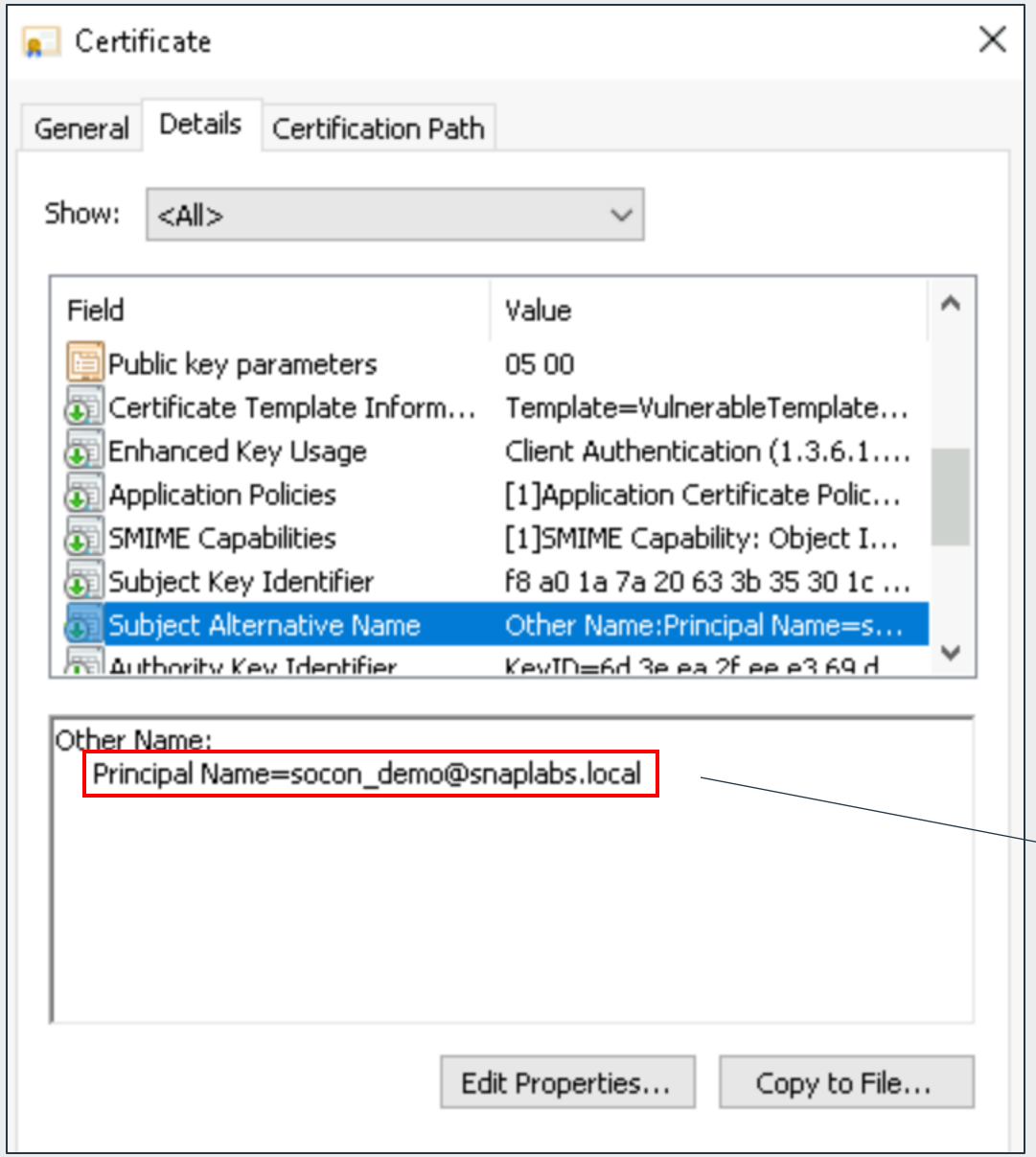
Select one of the X.509 certificates fields to bind with one of the user attributes in the cloud. Learn more

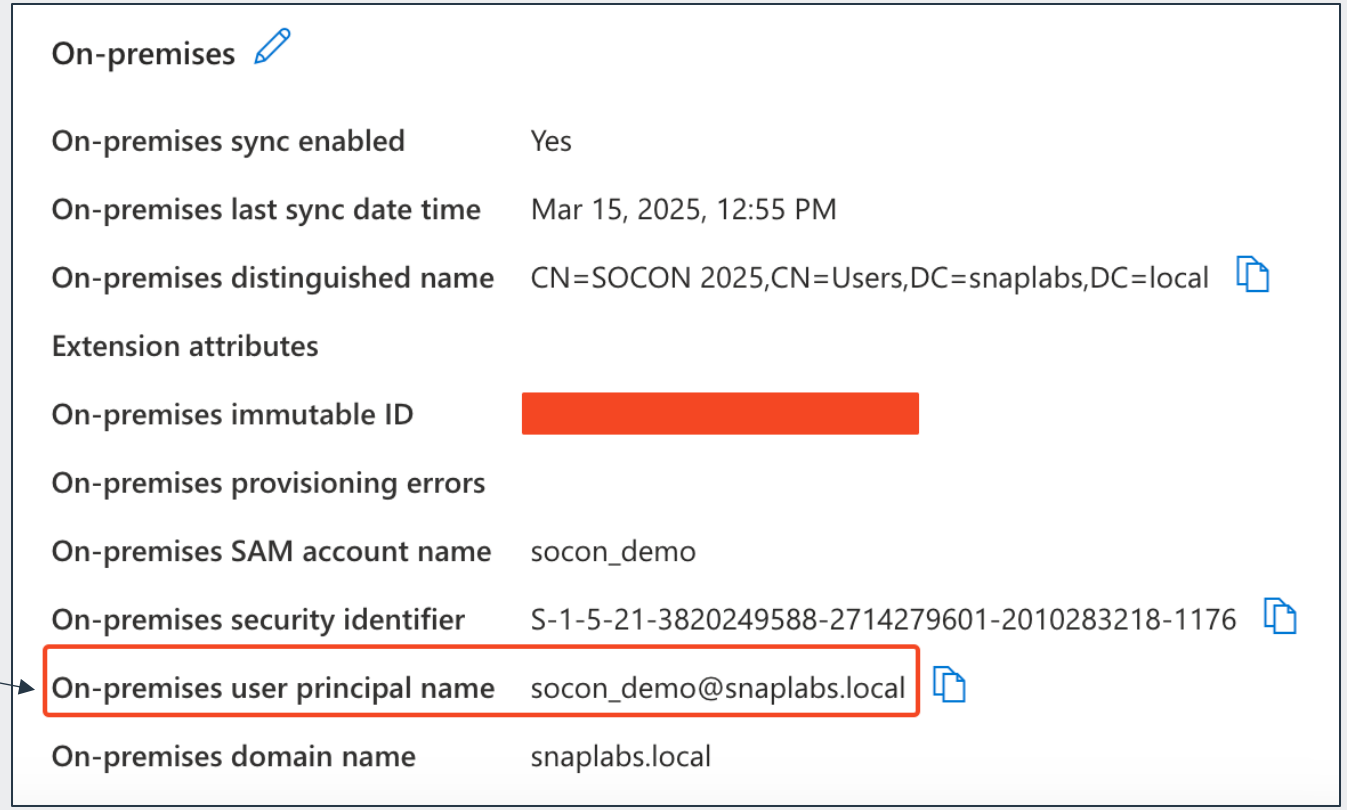
+ Add rule

Certificate field	Affinity binding	User attribute
PrincipalName	Low	userPrincipalName
SKI	High	CertificateUserIDs


Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Public key parameters
05 00
Certificate Template Inform...
Template=VulnerableTemplate...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Application Policies
[1]Application Certificate Polic...
SMIME Capabilities
[1]SMIME Capability: Object I...
Subject Key Identifier
cd 1c b6 43 12 02 99 4a e2 7c ...
Subject Alternative Name
Other Name:Principal Name=s...
Other Name:
Principal Name=socon_demo@[redacted].onmicrosoft.com
Edit Properties...
Copy to File...


Identity
Display name
SOCON 2025
First name
SOCON
Last name
2025
User principal name
socon_demo@[redacted]onmicrosoft.com
Object ID
4236537e-[redacted]
Identities
phone
User type
Member
Creation type
Created date time
Mar 15, 2025, 10:05 AM
Last password change date time
Mar 15, 2025, 9:59 AM
Invitation state
External user state change date ...
Assigned licenses
View
Password policies
DisablePasswordExpiration
Password profile
Preferred language
Sign in sessions valid from date ...
Mar 15, 2025, 9:59 AM
Authorization info
View


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Public key parameters
05 00
Certificate Template Inform...
Template=VulnerableTemplate...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Application Policies
[1]Application Certificate Polic...
SMIME Capabilities
[1]SMIME Capability: Object I...
Subject Key Identifier
f8 a0 1a 7a 20 63 3b 35 30 1c ...
Subject Alternative Name
Other Name:Principal Name=s...
Other Name:
Principal Name=socon_demo@snaplabs.local
Edit Properties...
Copy to File...


On-premises
On-premises sync enabled
Yes
On-premises last sync date time
Mar 15, 2025, 12:55 PM
On-premises distinguished name
CN=SOCON 2025,CN=Users,DC=snaplabs,DC=local
Extension attributes
On-premises immutable ID
On-premises provisioning errors
On-premises SAM account name
socon_demo
On-premises security identifier
S-1-5-21-3820249588-2714279601-2010283218-1176
On-premises user principal name
socon_demo@snaplabs.local
On-premises domain name
snaplabs.local

Authentication Binding Policies

- Determines the strength of the certificate-based authentication
- Comprised of tenant-level protections and binding rule policies
  - Binding rules map certificate attributes to protection levels
  - Ex. Issuer / Policy Object ID (OID)
- Default tenant-level protections:
  - Protection Level: Single-Factor Authentication
  - Affinity Binding: Low Affinity

Enable and Target | **Configure**

Certificate revocation list (CRL) validation

This setting requires a CRL check for every certificate authority (CA). If the CRL distribution point is empty or not configured for your CAs, the authentication will fail. You can exempt certificate authorities from the CRL validation requirement.

Require CRL validation (recommended) ☐

Issuer Hints

Enable issuer hints to show only the valid certificates in the certificate picker during authentication. Learn more

Issuer Hints ☑

Authentication binding

The authentication binding policy helps determine the strength of your certificate-based authentication method policy as single-factor or multi-factor and low affinity or high affinity. Override default settings with special rules. Learn more

Protection Level ⓘ
- (●) Single-factor authentication
- ( ) Multi-factor authentication

Required Affinity Binding ⓘ
- (●) Low
- ( ) High

+ Add rule

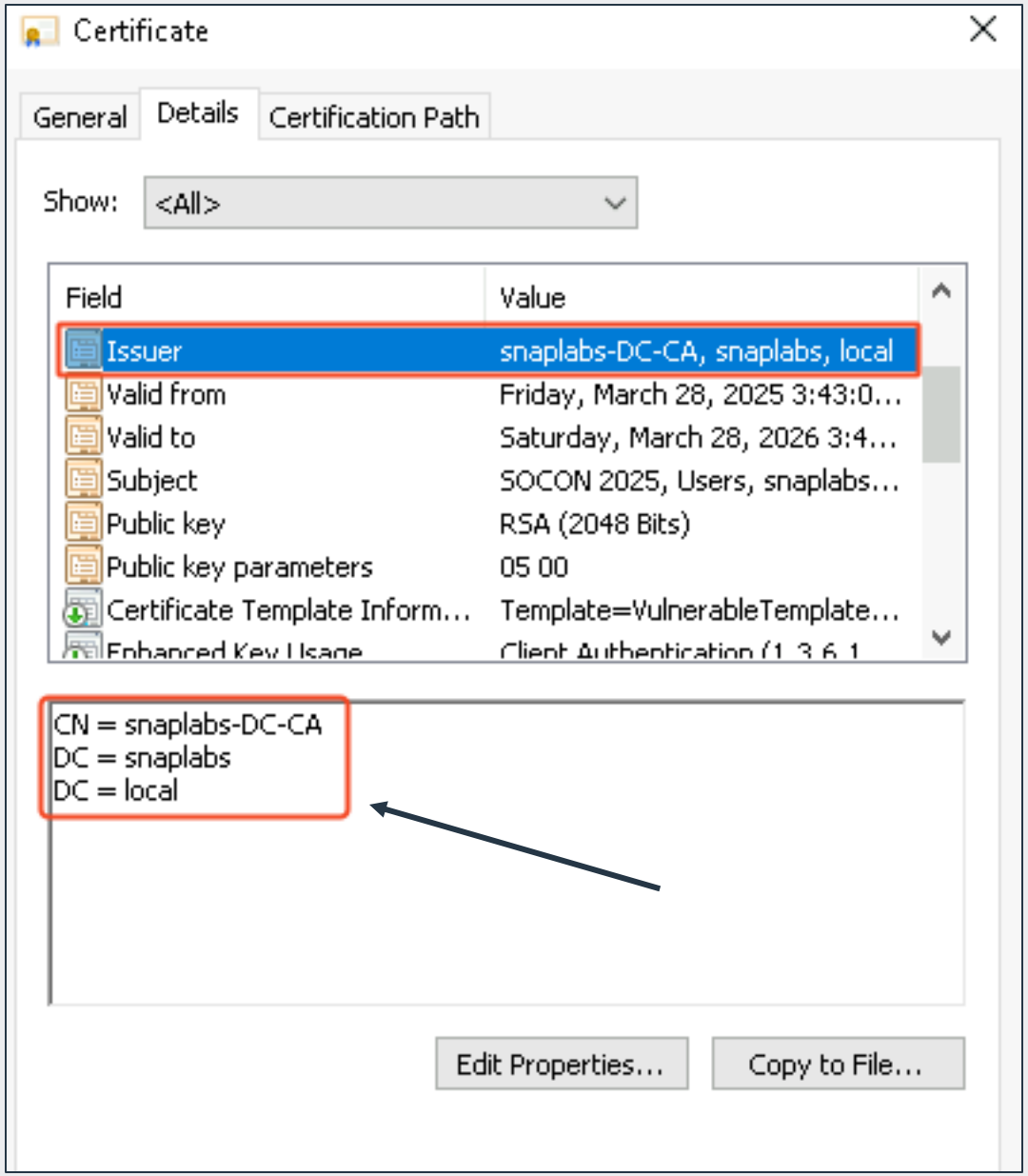
Certificate issuer	Policy OID	Authentication strength	Affinity binding
CN=snaplabs-DC-CA, DC=snaplabs, DC=local	N/A	Multi-factor	Low

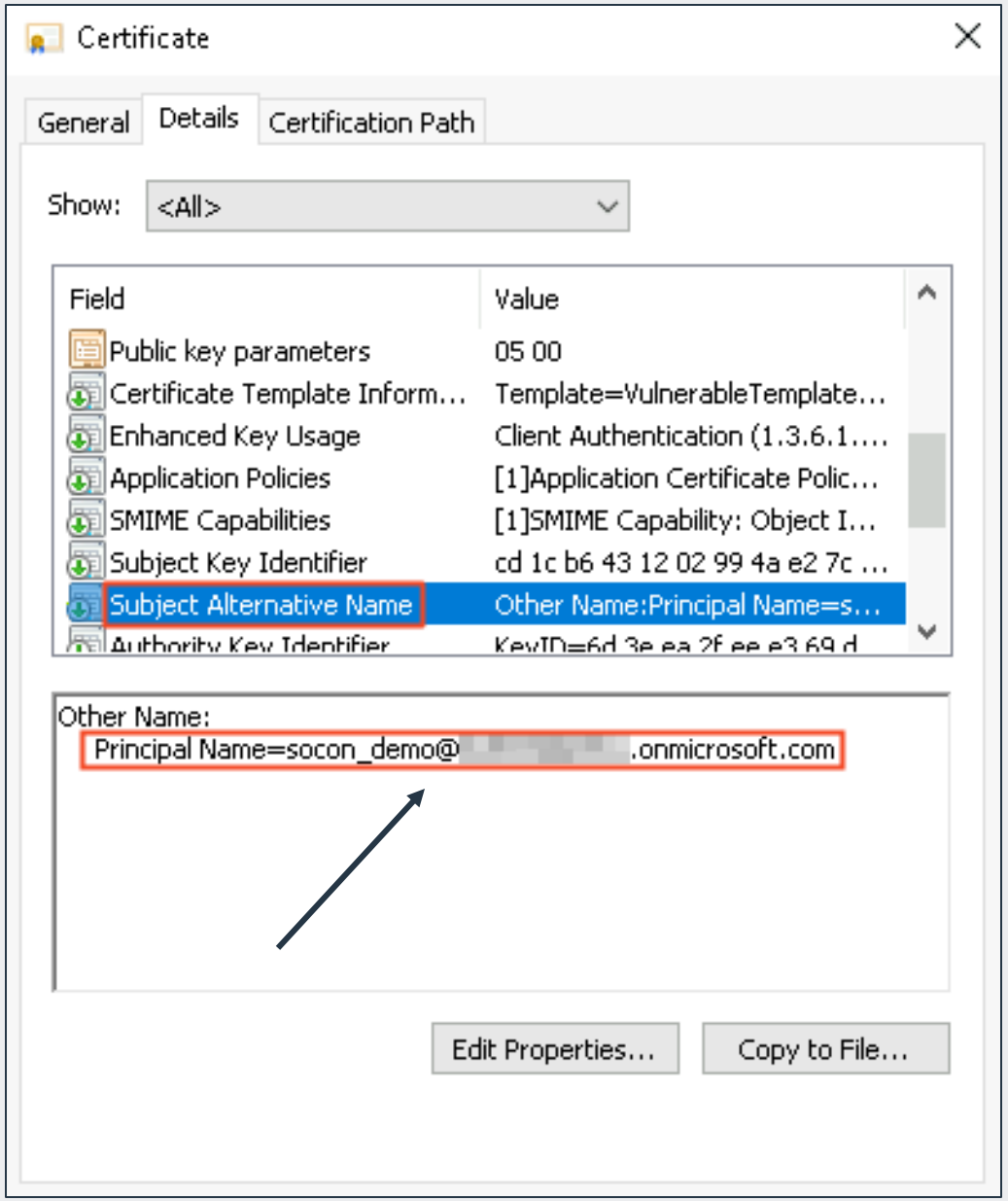
Username binding

Select one of the X.509 certificates fields to bind with one of the user attributes in the cloud. Learn more

+ Add rule

Certificate field	Affinity binding	User attribute
PrincipalName	Low	userPrincipalName
SKI	High	CertificateUserIDs

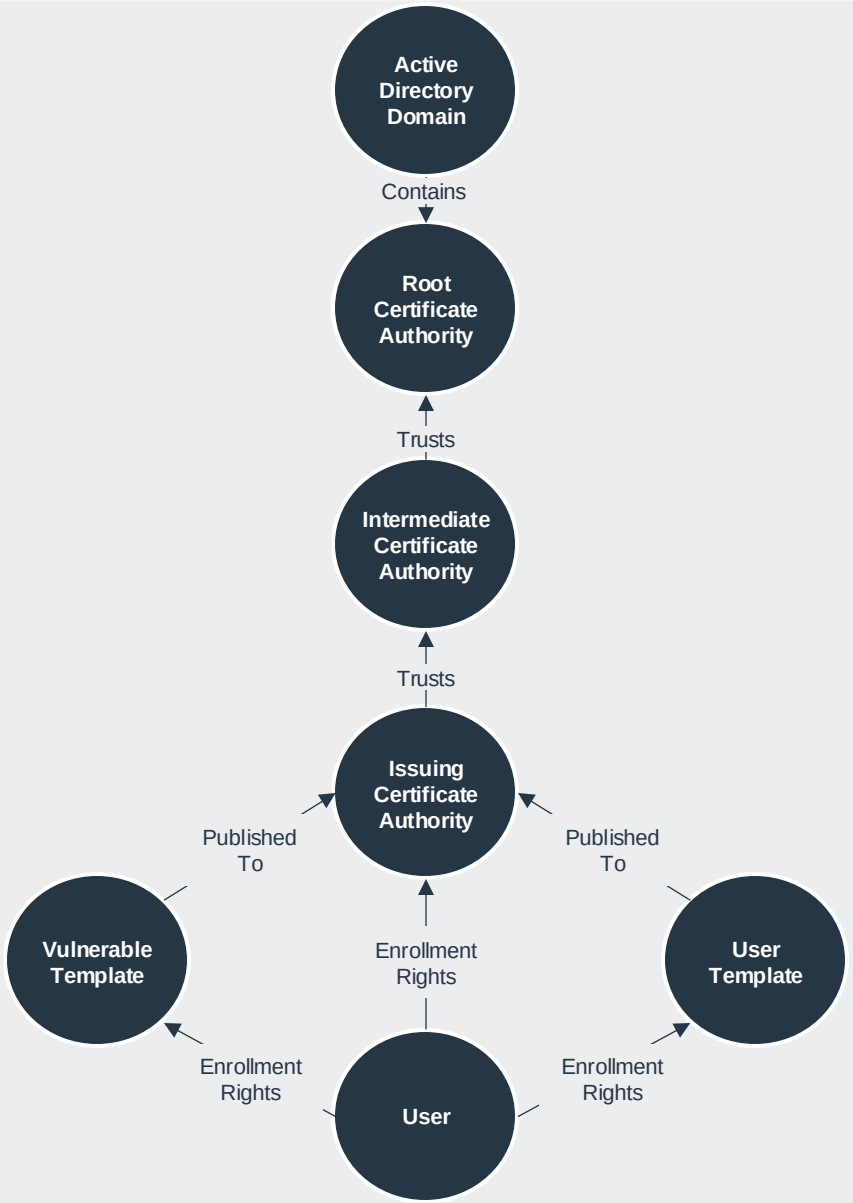

Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Issuer
snaplabs-DC-CA, snaplabs, local
Valid from
Friday, March 28, 2025 3:43:0...
Valid to
Saturday, March 28, 2026 3:4...
Subject
SOCON 2025, Users, snaplabs...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Inform...
Template=VulnerableTemplate...
CN = snaplabs-DC-CA
DC = snaplabs
DC = local
Edit Properties...
Copy to File...

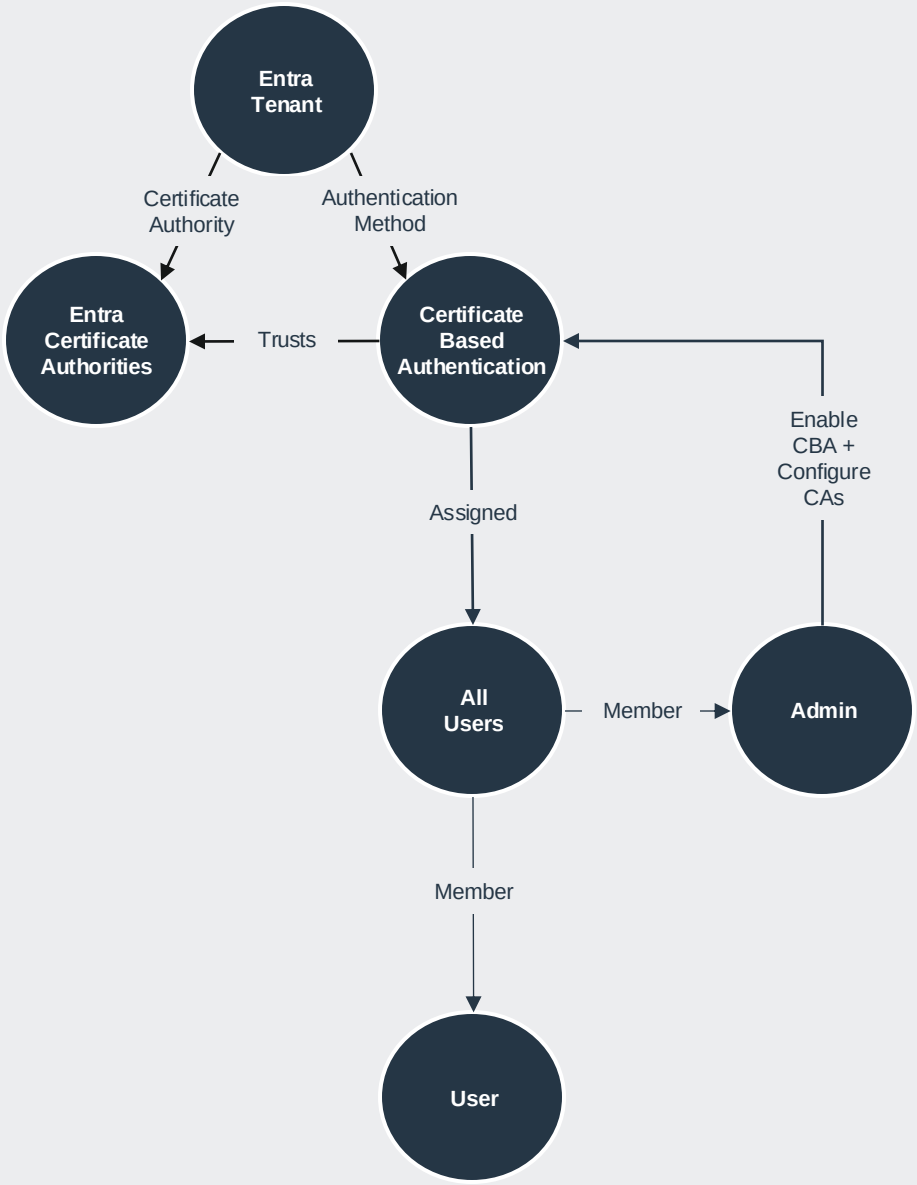

Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Public key parameters
05 00
Certificate Template Inform...
Template=VulnerableTemplate...
Enhanced Key Usage
Client Authentication (1.3.6.1....
Application Policies
[1]Application Certificate Polic...
SMIME Capabilities
[1]SMIME Capability: Object I...
Subject Key Identifier
cd 1c b6 43 12 02 99 4a e2 7c ...
Subject Alternative Name
Other Name:Principal Name=s...
Other Name:
Principal Name=socon_demo@ .onmicrosoft.com
Edit Properties...
Copy to File...

Active Directory

Boundary

Entra



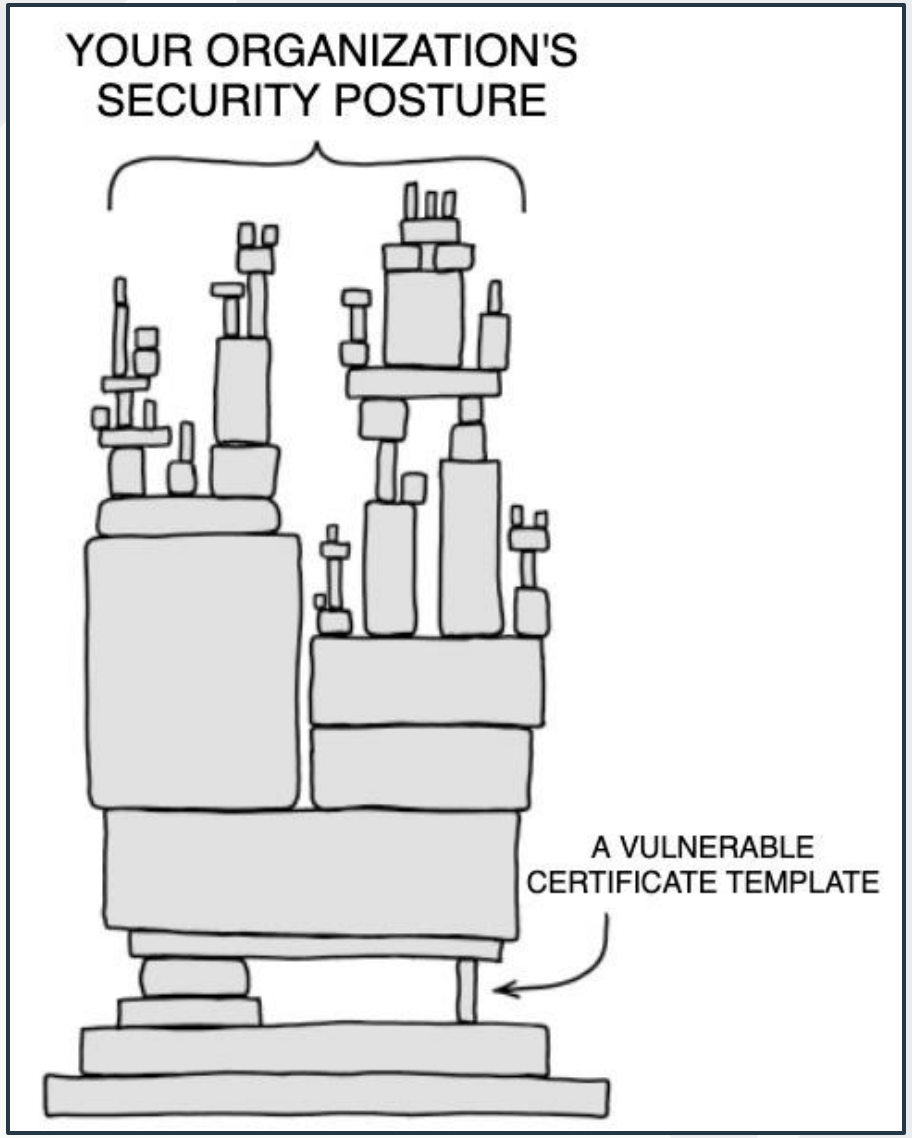


Crossing The Bridge

Pivoting From Active Directory to Entra

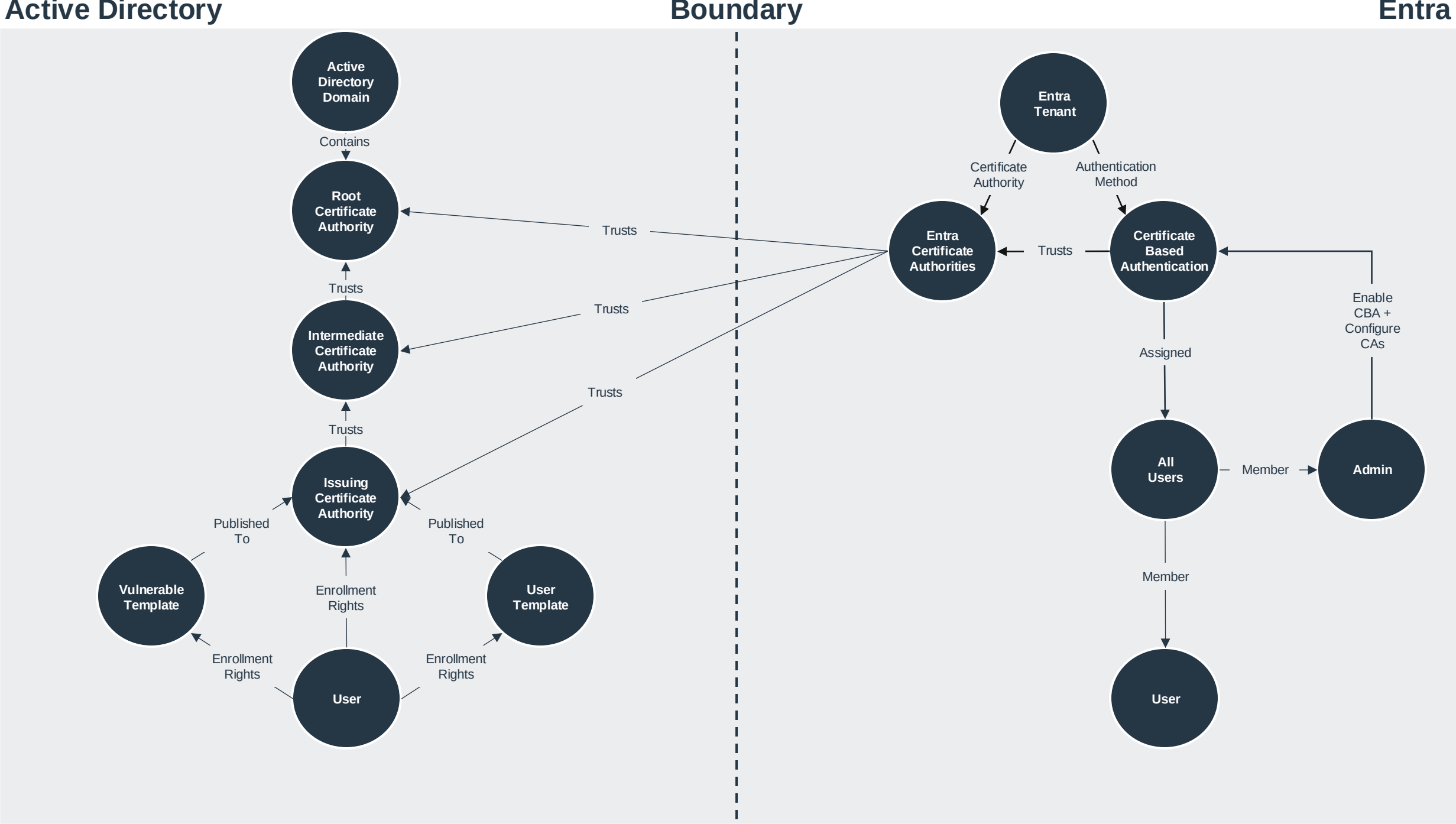
Hybrid Configurations

- Organizations often extend on-premises infrastructure through hybrid trust relationships and federation configurations
  - Entra Connect
  - Okta Synchronization
- Many organizations configuring Entra CBA trust existing on-premises ADCS infrastructure
  - Allowing on-premises security misconfigurations to impact cloud identities and resources



ⓘ Important

Make sure the PKI is secure and can't be easily compromised. In the event of a compromise, the attacker can create and sign client certificates and compromise any user in the tenant, both users whom are synchronized from on-premises and cloud-only users. However, a strong key protection strategy, along with other physical and logical controls, such as HSM activation cards or tokens for the secure storage of artifacts, can provide defense-in-depth to prevent external attackers or ins
the integrity of the PKI. For more information, see Securing PKI.


Active Directory
Boundary
Entra
Active Directory Domain
Contains
Root Certificate Authority
Trusts
Intermediate Certificate Authority
Trusts
Issuing Certificate Authority
Trusts
Trusts
Trusts
Published To
Published To
Vulnerable Template
User Template
Enrollment Rights
Enrollment Rights
Enrollment Rights
User
Entra Tenant
Certificate Authority
Authentication Method
Entra Certificate Authorities
Trusts
Certificate Based Authentication
Enable CBA + Configure CAs
Assigned
All Users
Member
Admin
Member
User

Enable and Target | **Configure**

Certificate revocation list (CRL) validation

This setting requires a CRL check for every certificate authority (CA). If the CRL distribution point is empty or not configured for your CAs, the authentication will fail. You can exempt certificate authorities from the CRL validation requirement.

Require CRL validation (recommended) ☐

Issuer Hints

Enable issuer hints to show only the valid certificates in the certificate picker during authentication. Learn more

Issuer Hints ☑

Authentication binding

The authentication binding policy helps determine the strength of your certificate-based authentication method policy as single-factor or multi-factor and low affinity or high affinity. Override default settings with special rules. Learn more

Protection Level ⓘ
- (●) Single-factor authentication
- ( ) Multi-factor authentication

Required Affinity Binding ⓘ
- (●) Low
- ( ) High

+ Add rule

Certificate issuer	Policy OID	Authentication strength	Affinity binding
CN=snaplabs-DC-CA, DC=snaplabs, DC=local	N/A	Multi-factor	Low

Username binding

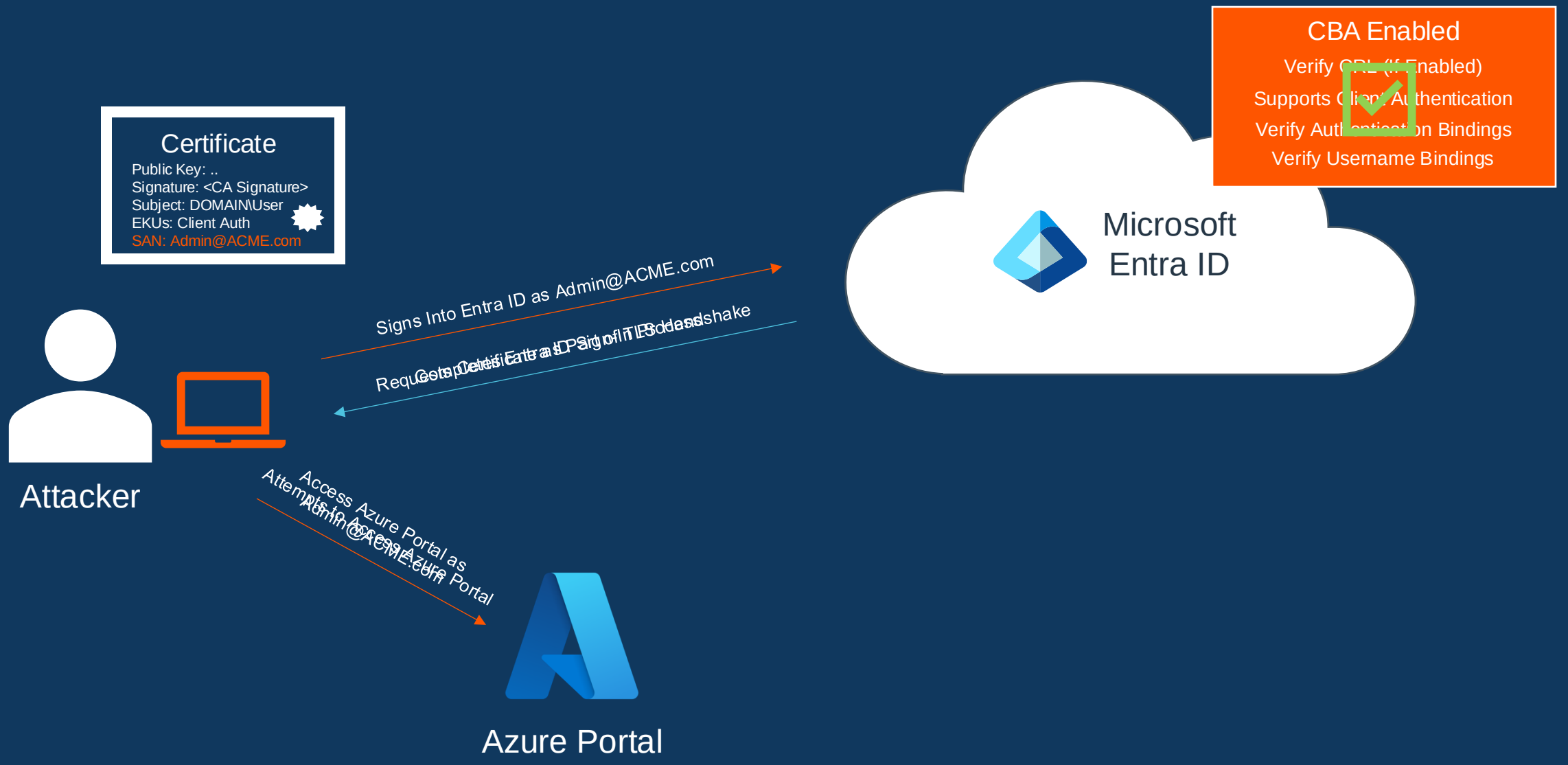
Select one of the X.509 certificates fields to bind with one of the user attributes in the cloud. Learn more

+ Add rule

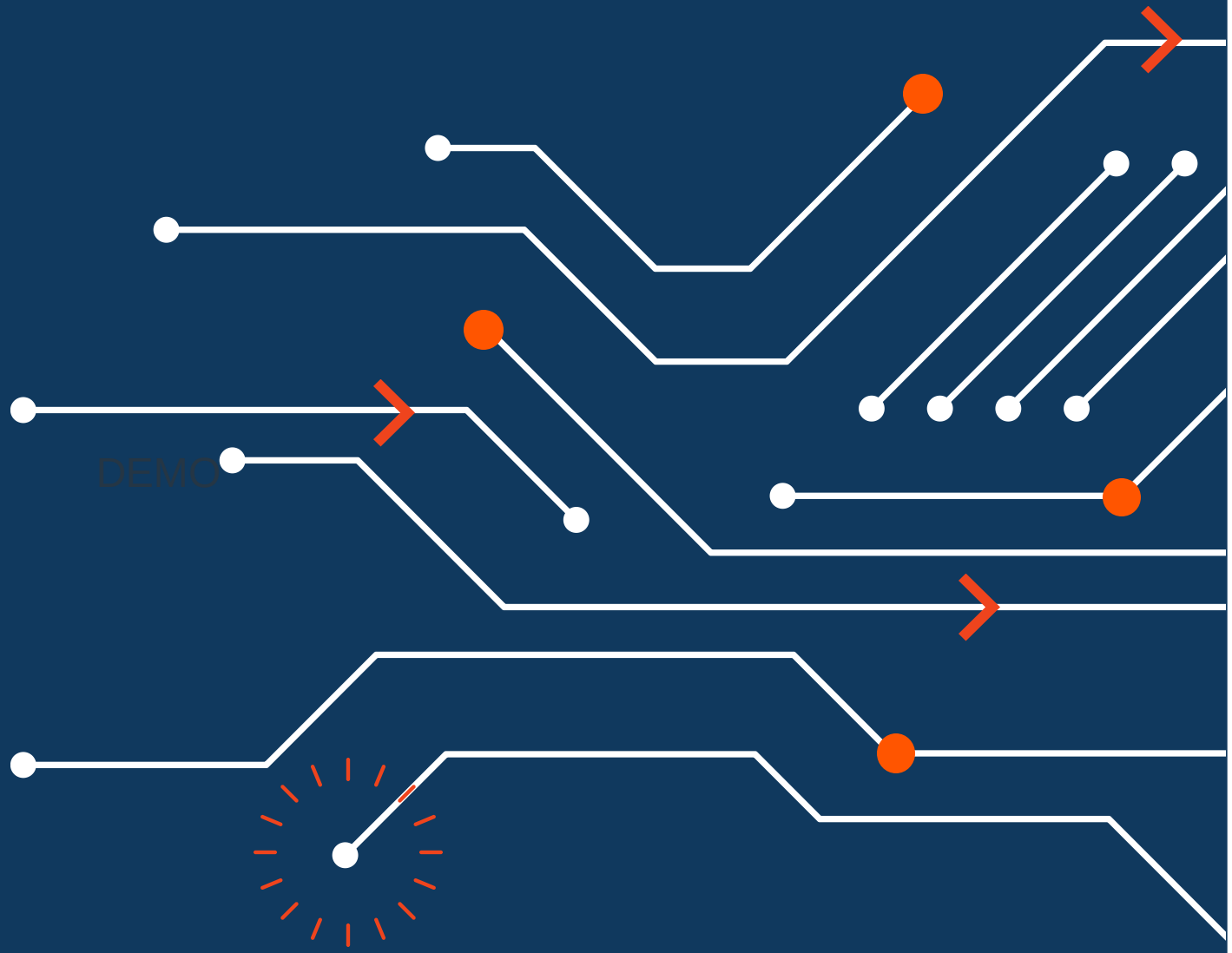
Certificate field	Affinity binding	User attribute
PrincipalName	Low	userPrincipalName
SKI	High	CertificateUserIDs

Abusing Misconfigured Certificate Template

Authenticating With Admin Certificate



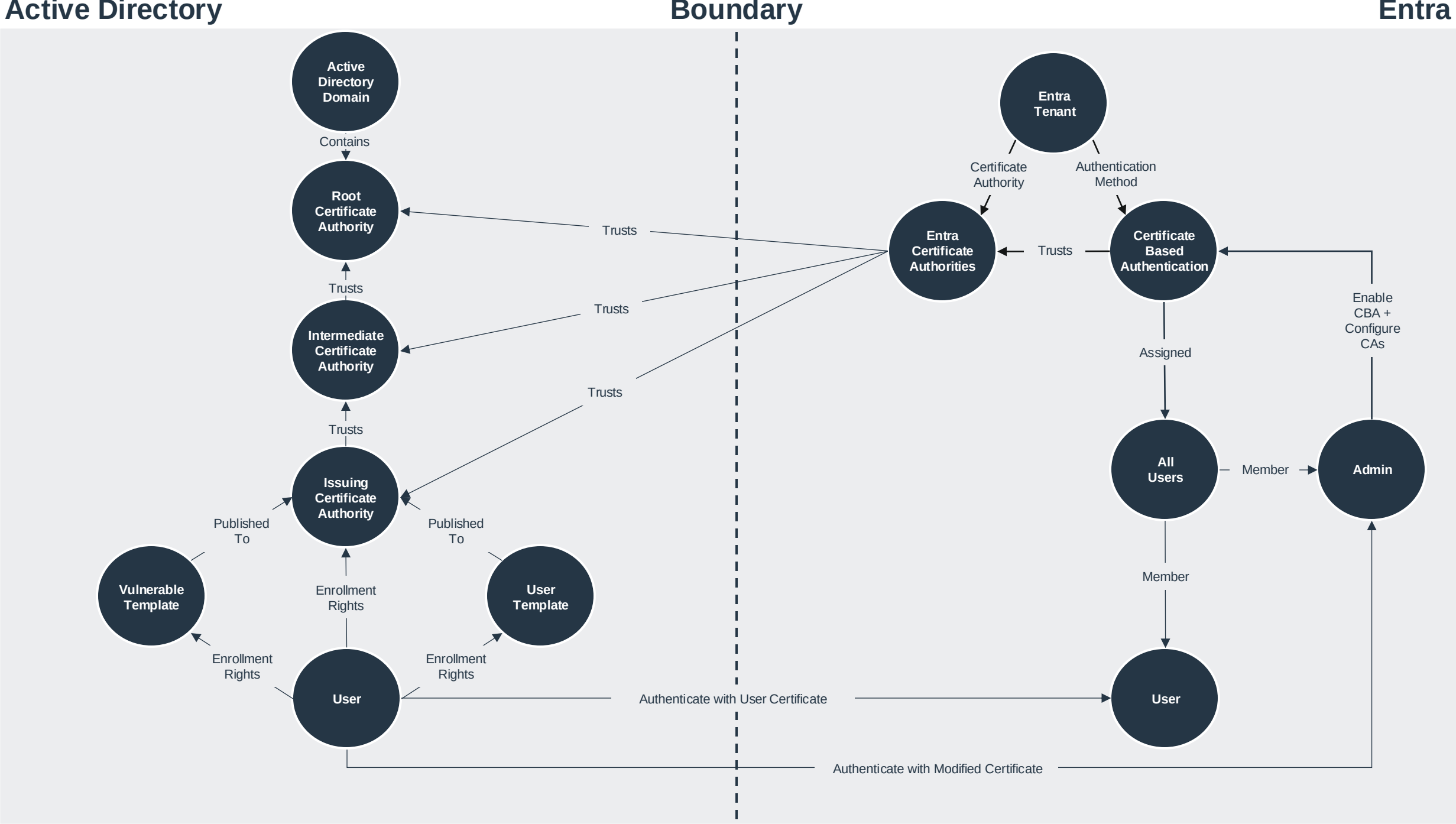
DEMO



C:\Users\domain_admin\Downloads - PowerShell 5.1 (6136)

```
C:\Users\domain_admin\Downloads> .\Certify.exe request /ca:dc.snaplabs.local\snaplabs-DC-CA /altname:"socon_demo@[redacted]onmicrosoft.com" /su
```

1:47 AM
3/30/2025


Active Directory
Boundary
Entra
Active Directory Domain
Contains
Root Certificate Authority
Trusts
Intermediate Certificate Authority
Trusts
Issuing Certificate Authority
Trusts
Trusts
Trusts
Published To
Published To
Vulnerable Template
User Template
Enrollment Rights
Enrollment Rights
Enrollment Rights
User
Authenticate with User Certificate
Authenticate with Modified Certificate
Entra Tenant
Certificate Authority
Authentication Method
Entra Certificate Authorities
Trusts
Certificate Based Authentication
Enable CBA + Configure CAs
Assigned
All Users
Member
Admin
Member
User

Reconnaissance Tips

- Attackers can passively enumerate whether users have CBA enabled via the GetCredentialType endpoint
  - HasCertAuth Field in Response
  - CertAuthUrl Field in Response
- Several open-source tools already include this information in output
  - Ex. AADInternals, AADOutsider-py


```
{
    "Username": "socon_demo@[redacted].onmicrosoft.com",
    "Display": "socon_demo@[redacted].onmicrosoft.com",
    "IfExistsResult": 0,
    "IsUnmanaged": false,
    "ThrottleStatus": 0,
    "Credentials": {
        "PrefCredential": 15,
        "HasPassword": true,
        "HasCertAuth": true,
        "RemoteNgcParams": null,
        "FidoParams": null,
        "QrCodePinParams": null,
        "SasParams": null,
        "CertAuthParams": {
            "CertAuthUrl": "https://t43e[redacted].certauth.login.microsoft
        },
        "GoogleParams": null,
        "FacebookParams": null,
        "OtcNotAutoSent": false
    },
    "DfpProperties": {},
    "EstsProperties": {
        "DesktopSsoEnabled": true,
        "UserTenantBranding": null,
        "DomainType": 3
    },
    "FlowToken": "[redacted]
    "IsSignupDisallowed": true,
    "apiCanary": "[redacted]
```

Persistence Tips

- If CRL validation is not required in CBA, then certificates revoked on the ADCS Certificate Authority will still be able to authenticate to Entra ID
- Maintain access to Entra ID even when access in AD is revoked
- Common configuration for organizations trusting ADCS Certificate Authorities

Defensive Strategies

Protecting Your Organizations

Hardening

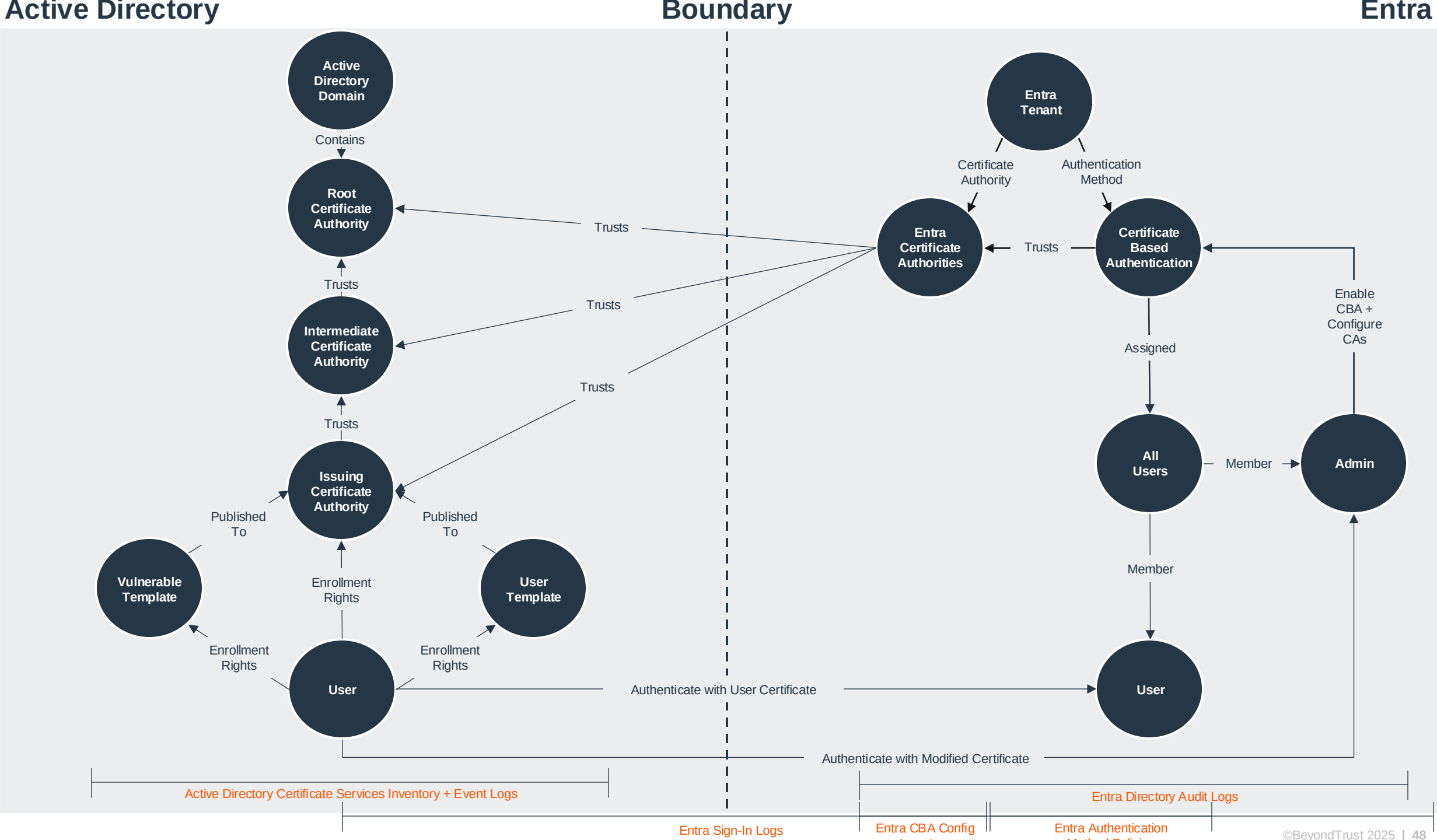
DEMO

Hardening Entra CBA

- Enforce High-Affinity Bindings
  - Use mapping types based on non-reusable identifiers
    - Ex. Subject Key Identifiers or SHA1 Public Key
- Implement Strict CRL Validation
  - Ensure trusted CAs regularly publish updated CRLs
- Configure Authentication Binding Policies carefully
  - Use combination of Issuer + Policy OID for highest security
- Manage trust relationships
  - Only trust CAs that follow best practices
  - Use Conditional Access Policies to add additional protections/enforcements

Detections

DEMO


Active Directory
Boundary
Entra
Active Directory Domain
Contains
Root Certificate Authority
Trusts
Intermediate Certificate Authority
Trusts
Issuing Certificate Authority
Trusts
Trusts
Trusts
Published To
Published To
Vulnerable Template
User Template
Enrollment Rights
Enrollment Rights
Enrollment Rights
User
Authenticate with User Certificate
Entra Tenant
Certificate Authority
Authentication Method
Entra Certificate Authorities
Trusts
Certificate Based Authentication
Enable CBA + Configure CAs
Assigned
All Users
Member
Admin
Member
User
Authenticate with Modified Certificate
Active Directory Certificate Services Inventory + Event Logs
Entra Directory Audit Logs
Entra Sign-In Logs
Entra CBA Config
Entra Authentication

Detections

- Goal: Correlate suspicious ADCS certificate enrollment with certificate-based authentication to Entra
- Available Telemetry:
  - Active Directory:
    - Event ID 4886: Certificate Requested
    - Event ID 4887: Certificate Issued
  - Entra ID:
    - Entra Sign-In Logs
- Additional Context:
  - ADCS LDAP Configurations
  - Entra CBA + CA Configurations

ADCS Event Logs

Event Code	Description	Interesting Attributes

4886	Certificate Services received a certificate request	**System Logs:**
		• Computer: Enrollment Server
		Event Data Logs:
		• Attributes:
		  • CCM: Source Computer (Not always present)
		  • CDC: Enrollment Server (Not always present)
		  • RMD: Source Computer (Not always present)
		  • Certificate Template: Certificate template enrolled (Not always present)
		  • SAN: Alternative SAN specified in ticket (Not always present)
		• Request ID: (Potential correlation with 4887 events)
		• Requester: Source User / Computer Account (Useful for source identification)

4887	Certificate Services approved a certificate request and issued a certificate	**System Logs:**
		• Computer: Enrollment Server
		Event Data Logs:
		• **Subject Key Identifier (Unique identification of certificate)**
		• **Subject: Distinguished name of the subject of the certificate (Not always present)**
		• **Attributes:**
		  • **CCM: Source Computer (Not always present)**
		  • **CDC: Enrollment Server (Not always present)**
		  • **RMD: Source Computer (Not always present)**
		  • **Certificate Template: Certificate Template Enrolled (Not always present)**
		  • **SAN: Alternative SAN Specified in Ticket (Not always present)**
		• Request ID: (Potential correlation with 4886 events)
		• Requester: Source User / Computer Account (Useful for source identification)
		• Disposition: Possibly status of the certificate enrollment
		  • 0 → Request Did Not Complete
		  • 1 → Failed
		  • 2 → Denied
		  • 3 → Issued
		  • 4 → Issued Separately
		  • 5 → Taken Under Submission
		  • 6 → Revoked

Entra Sign-In Logs

Event Type	Description	Interesting Attributes

Entra Sign-In Logs	Microsoft Entra logs all sign-ins into an Entra ID tenant, which includes your internal apps and resources	• Date
		• Authentication Requirement
		• Status (Interrupted / Successful)
		• Username / User ID
		• Target Application / Application ID
		• Resource / Resource ID
		• Client App
		• User Agent
		• IP Address
		• IsInteractive
		• Device
		  • Browser
		  • Operating System
		  • Managed / Joined
		  • Device ID (Could be used to correlate on AD side)
		• **Authentication Details**
		  • **Authentication Method: X.509 Certificate**
		  • **Succeeded: True / False**
		• **Additional Details**
		  • **User Certificate Subject**
		  • **User Certificate Issuer**
		  • **User Certificate Serial Number**
		  • **User Certificate Thumbprint**
		  • **User Certificate Valid From (Possibly key off this for enrollment)**
		  • **User Certificate Expiration (Possibly key off this for enrollment)**
		  • **User Certificate Binding Identifier (Could key off this if modified SAN is shown, but not always the case)**
		  • **User Certificate Binding**
		  • **User Certificate Affinity Mode (Low / High Affinity)**

Problems in Correlation

- Active Directory Certificate Services event logging is inconsistent
  - Valuable fields do not always populate in logs
  - Tested against multiple tools (ex. Certify, Certipy, Built-In Certificate Manager)
- Available logs do not allow for robust cross-domain event correlation
  - Difficult to obtain high affinity that certificate requested in AD is the same certificate being used to authenticate to Entra

Alternative Telemetry Solutions

- Exit modules in ADCS offer powerful opportunities to enhance security monitoring and event telemetry
- Exit modules are customizable components that execute when specific CA operations occur
  - Ex. Certificate Issuance, etc.
- Exit modules can view certificate properties and extensions, as well as view request attributes and properties
- Defenders could leverage exit modules to enrich existing Windows event logs or write custom events with necessary fields
  - Ex. Populate Serial Number, Alternative SANs, etc.

Future Research

- Emerging Cloud Capabilities
  - Microsoft Cloud PKI
  - Entra ID External Authentication Method (EAM)
- NDES + SCEP
- Services Leveraging Certificate-Based Authentication
  - ADFS
  - Okta

Takeaways

- Security issues transcend domain boundaries in hybrid environments
- Implement detection and response strategies that can track and correlate activities across on-premises, cloud, and SaaS environments to identify sophisticated attack chains
- Phishing-resistant and passwordless authentication methods provide significant security benefits, but aren't invulnerable
  - Understanding their specific limitations is critical for comprehensive security

Additional Resources

- https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831740(v=ws.11)
- https://posts.specterops.io/passwordless-persistence-and-privilege-escalation-in-azure-98a01310be3f
- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication-technical-deep-dive
- https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-certificate-based-authentication
- https://goodworkaround.com/2022/02/15/digging-into-azure-ad-certificate-based-authentication/
- https://www.gradenegger.eu/en/a-policy-module-to-help-you-to-build-your-business-introduction-of-the-tamemycerts-policy-module/
- https://nach0focht.wordpress.com/2014/01/05/exit-modules/

Thank You!

beyondtrust.com