

# Analyzing and Executing ADCS Attack Paths with BloodHound

x33fcon 2024

Permalink to this deck: [bit.ly/4edZokL](https://bit.ly/4edZokL)



Jonas Bülow Knudsen  
Product Architect @ SpecterOps  
[@Jonas\\_B\\_K](#)



Andy Robbins  
Principal Product Architect @ SpecterOps  
[@\\_wald0](#)

# Agenda

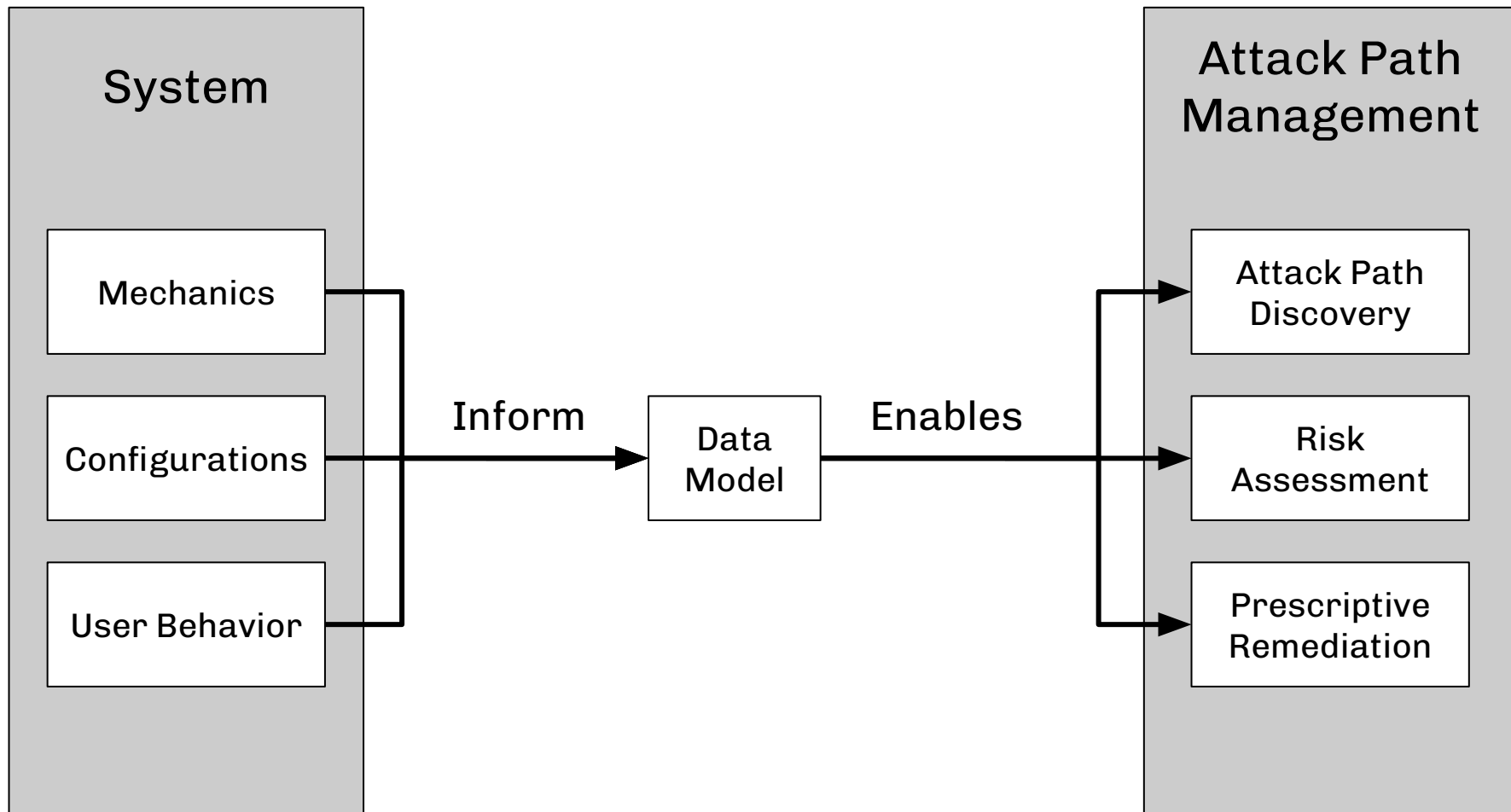
- How we model ADCS in BloodHound
- ADCS Attack Path discovery and execution
- Remediation Strategies and Practical Examples
- Conclusion

# Agenda

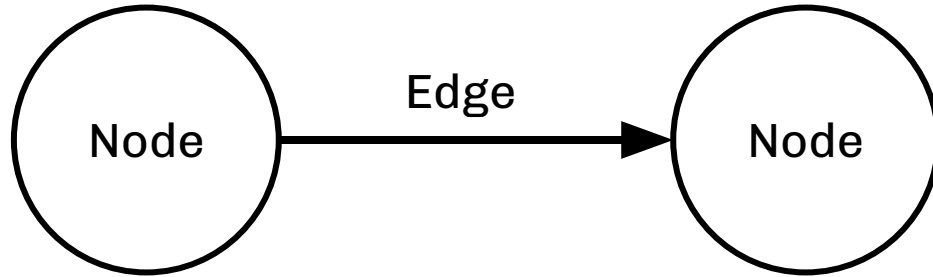
- How we model ADCS in BloodHound
  - The model's place, primitives, and purpose
  - Data sources and initial model
  - Post-processing to enrich the model
- ADCS Attack Path discovery and execution
- Remediation Strategies and Practical Examples
- Conclusion

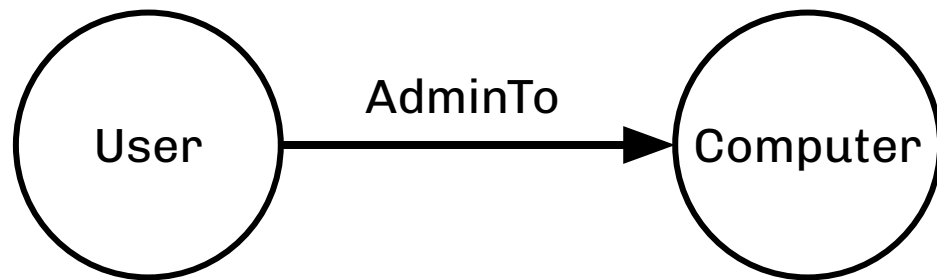
# Agenda

- How we model ADCS in BloodHound
  - The model's place, primitives, and purpose
  - Data sources and initial model
  - Post-processing to enrich the model
- ADCS Attack Path discovery and execution
- Remediation Strategies and Practical Examples
- Conclusion

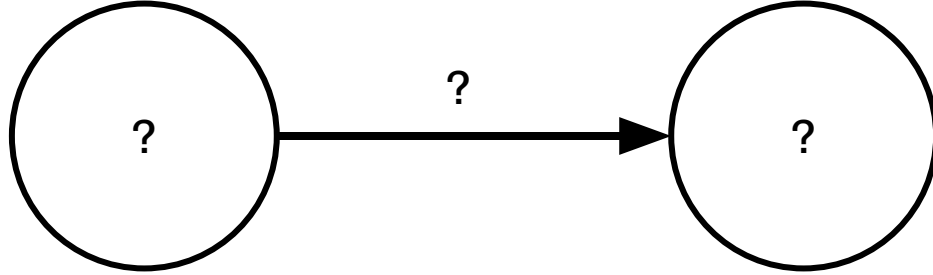


# Two primitive building blocks:

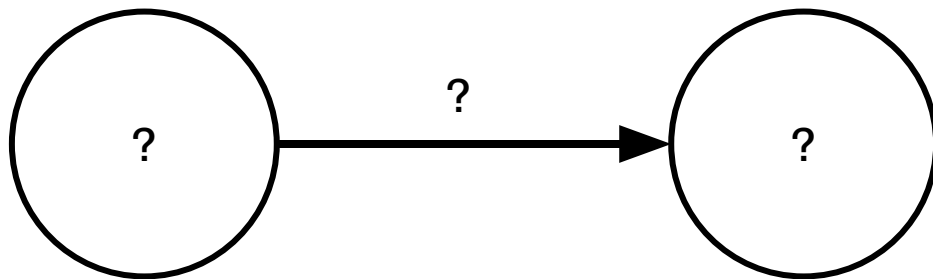




# How can we encode ESC1 into the graph?



# How can we encode ESC1 into the graph?



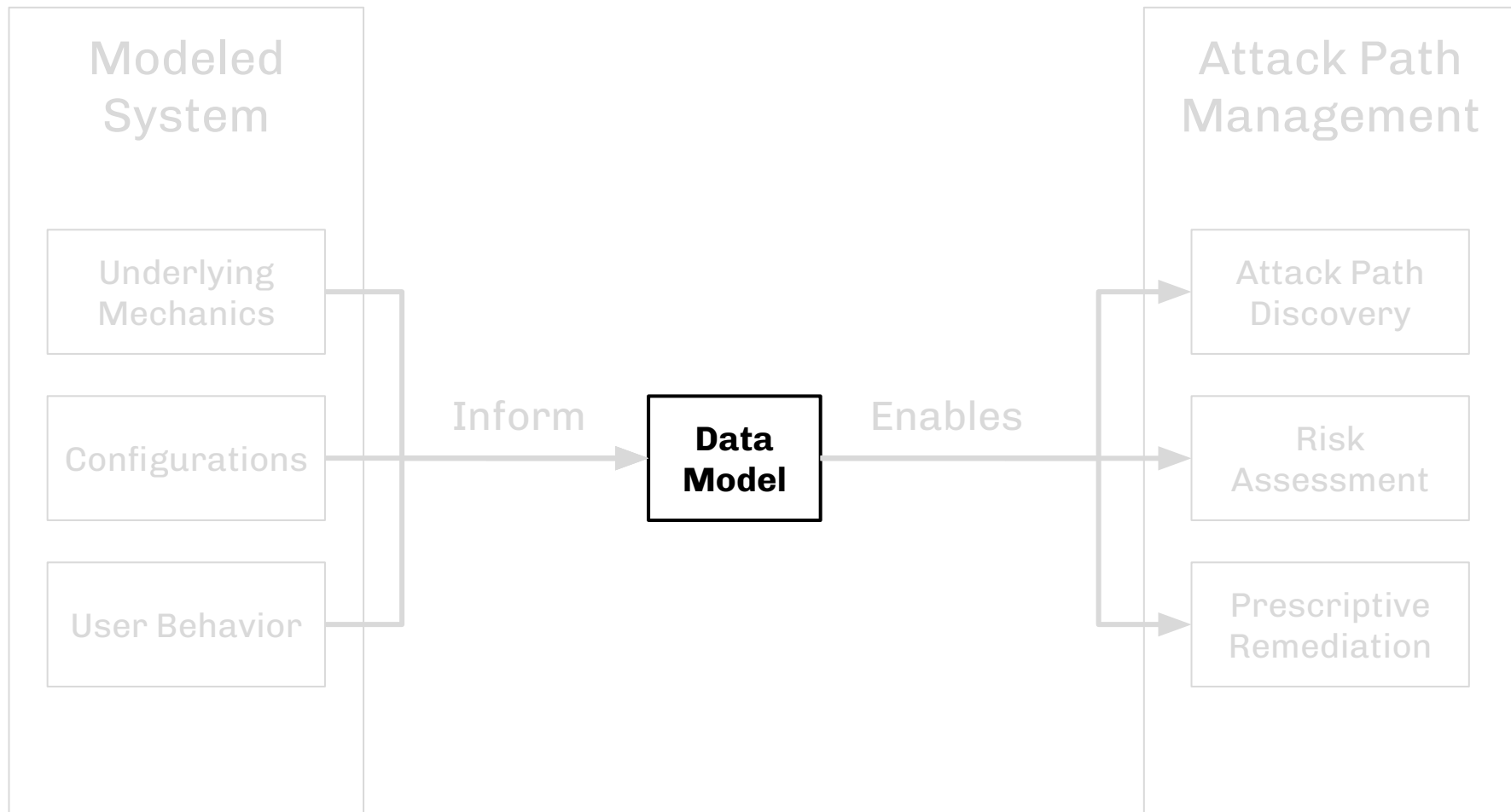
And:

- Enable simple discovery of ADCS-based attack paths
- Enable per-object auditing and analysis
- Comply with the existing data model and UX
- Maintain accuracy and performance of the application

# Put simply:

How do we get BloodHound to accurately, reliably, and quickly answer the following question:

**Which principals can perform ESC1?**



# Agenda

- **How we model ADCS in BloodHound**
  - The model's place, primitives, and purpose
  - **Data sources and initial model**
  - Post-processing to enrich the model
- ADCS Attack Path discovery and execution
- Remediation Strategies and Practical Examples
- Conclusion



Domain



Enterprise CA



Container



Root CA



Group



Cert Template



NT Auth Store



User



**Type:** Domain  
**Name:** ESC1.LOCAL  
**ObjectID:** S-1-5-21-1004336348-1177238915-682003330





Domain



Enterprise CA



Container



Root CA



Contains



Console1 - [Console Root\ADSI Edit\Configuration [ESC1-DC.ESC1.LOCAL] \CN=Configurat...

File Action View Favorites Window Help

Console Root

- ADSI Edit
  - Configuration [ESC1-DC.ESC1.LOCAL]
    - CN= Configuration,DC=ESC1,DC=LOCAL**
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=NTDS Quotas
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=AuthN Policy Configuration
        - CN=Claims Configuration
        - CN=Group Key Distribution Servi
        - CN=Microsoft SPP
        - CN=MsmqServices
        - CN=NetServices
      - CN=Public Key Services
        - CN=AIA
        - CN=CDP
        - CN=Certificate Templates
        - CN=Certification Authorities
        - CN=Enrollment Services
        - CN=KRA
        - CN=OID

Name	Class	Distinguish
CN=DisplaySpecifiers	container	CN=Display
CN=Extended-Rights	container	CN=Extend
CN=ForestUpdates	container	CN=Forest
CN=LostAndFoundC...	lostAndFound	CN=LostAr
CN=NTDS Quotas	msDS-QuotaContai...	CN=NTDS
CN=Partitions	crossRefContainer	CN=Partiti
CN=Physical Locations	physicalLocation	CN=Physic
CN=Services	container	CN=Service
CN=Sites	sitesContainer	CN=Sites,C
CN=WellKnown Secu...	container	CN=WellKr

**Type:**

Container

**Name:**

CONFIGURATION

**ObjectID:**

8CB1E5E9-0404-4710-B68A-E2A2512B04FB





Domain



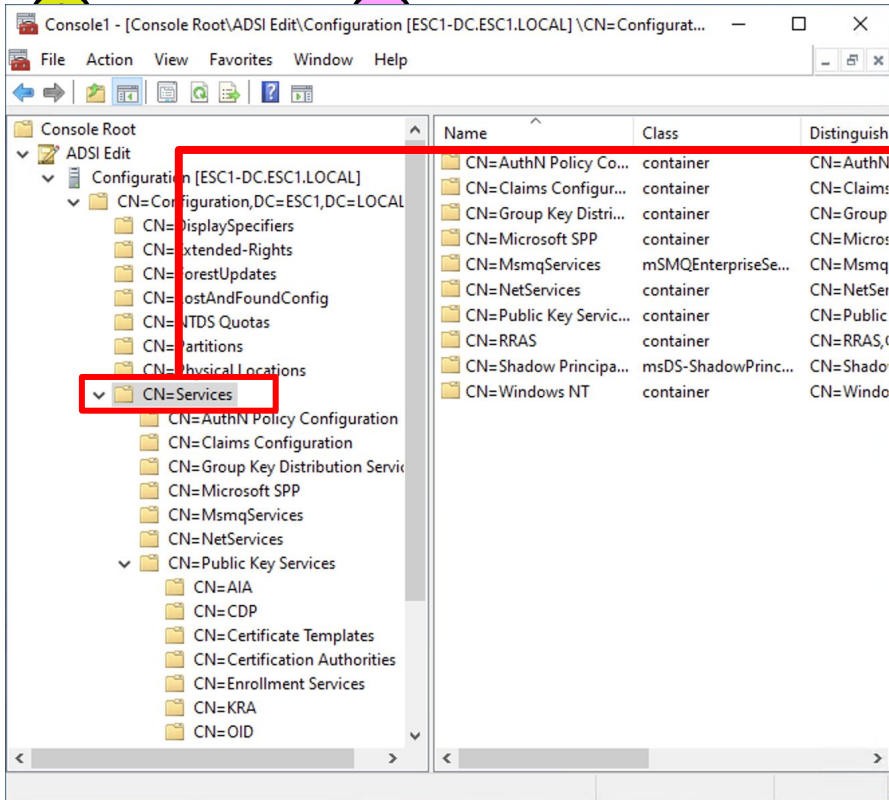
Enterprise CA



Container



Root CA



Contains



Contains



Type:

Container

Name:

SERVICES

ObjectID:

778E7398-3790-4053-8B08-0D480C5FB730





Domain



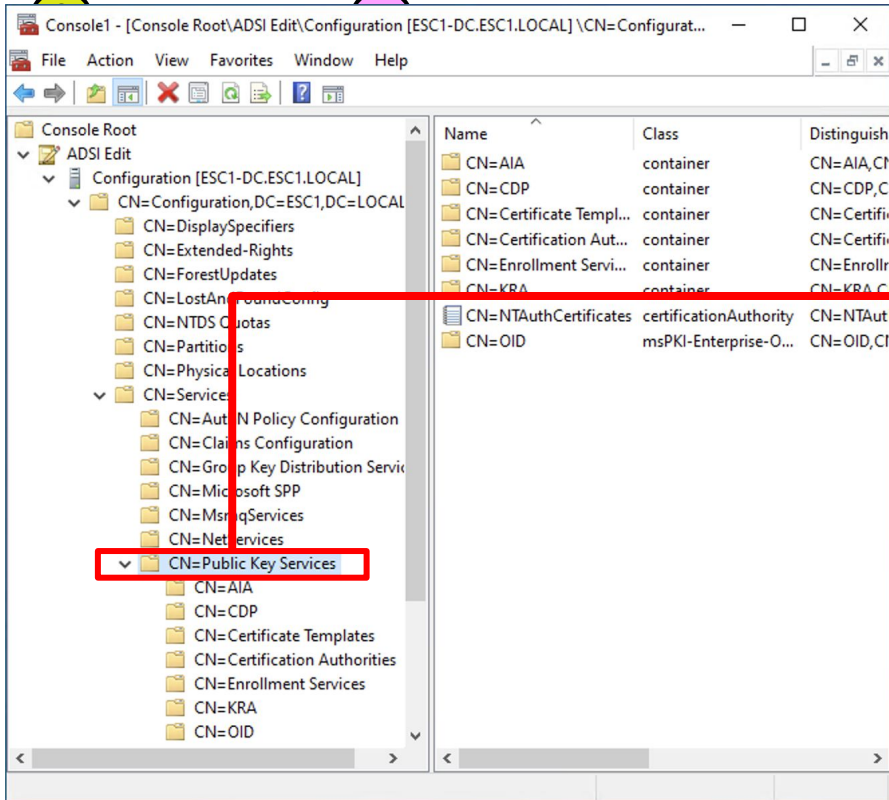
Enterprise CA



Container



Root CA



Contains



Contains



Contains



**Type:** Container

**Name:** PUBLIC KEY SERVICES

**ObjectID:** A18A3A99-3E4C-46DD-9C90-E5542FA4EC84





Domain



Enterprise CA



Container



Root CA



Group



Cert Template



NT Auth Store



User



Contains



Contains



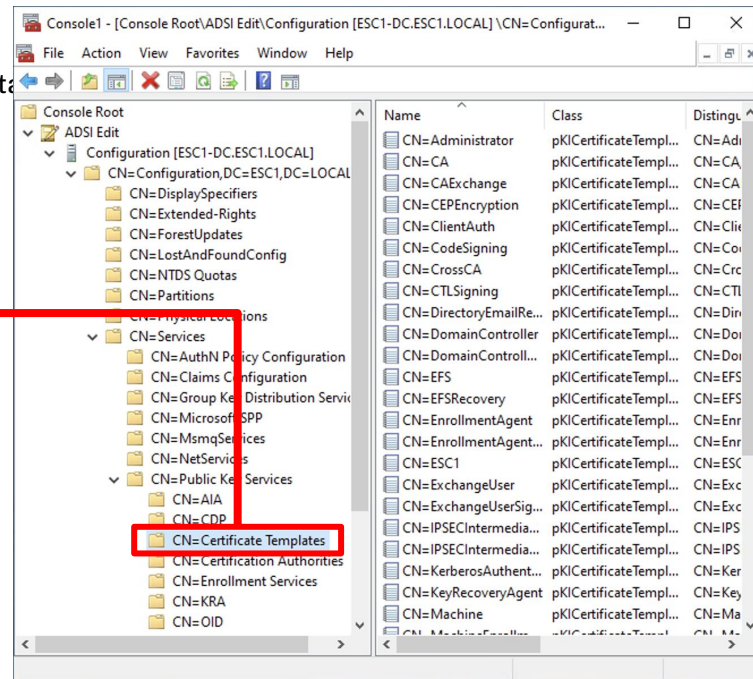
Contains



Contains



**Type:** Container  
**Name:** CERTIFICATE TEMPLATES  
**ObjectID:** 95D1A36E-7782-4CC5-823C-F5994359DDC0





Domain



Enterprise CA



Container



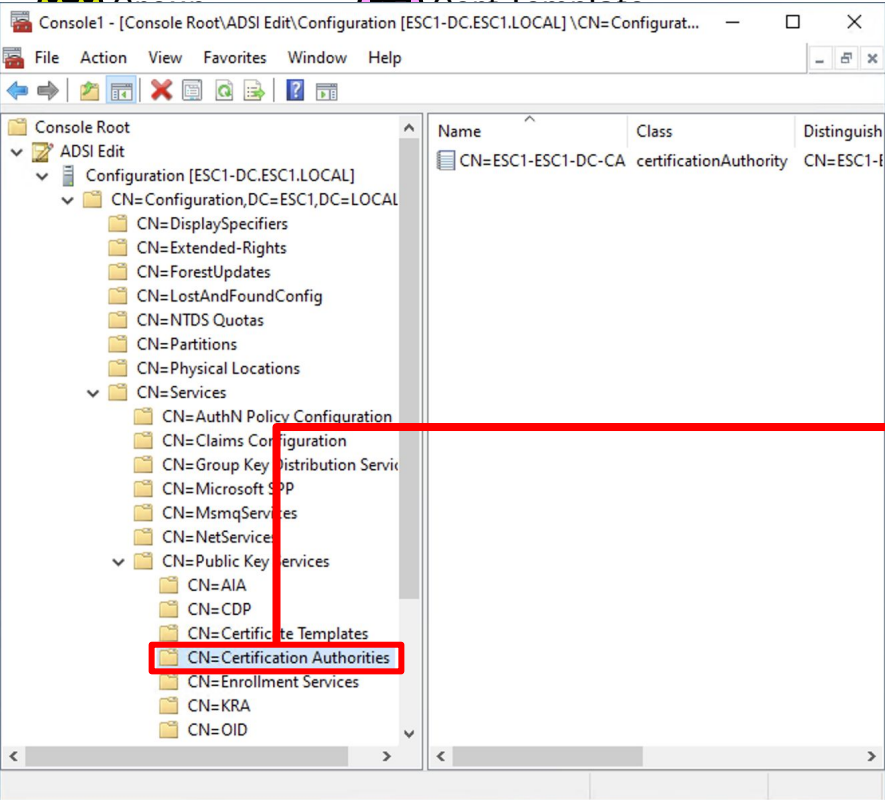
Root CA



Certificate Template



Certificate Template



Contains



Contains




Contains



Contains



<b>Type:</b>	Container	
<b>Name:</b>	CERTIFICATION AUTHORITIES	
<b>ObjectID:</b>	242AB0E0-13D1-4517-BEB0-07E504802B6B	



Domain



Enterprise CA



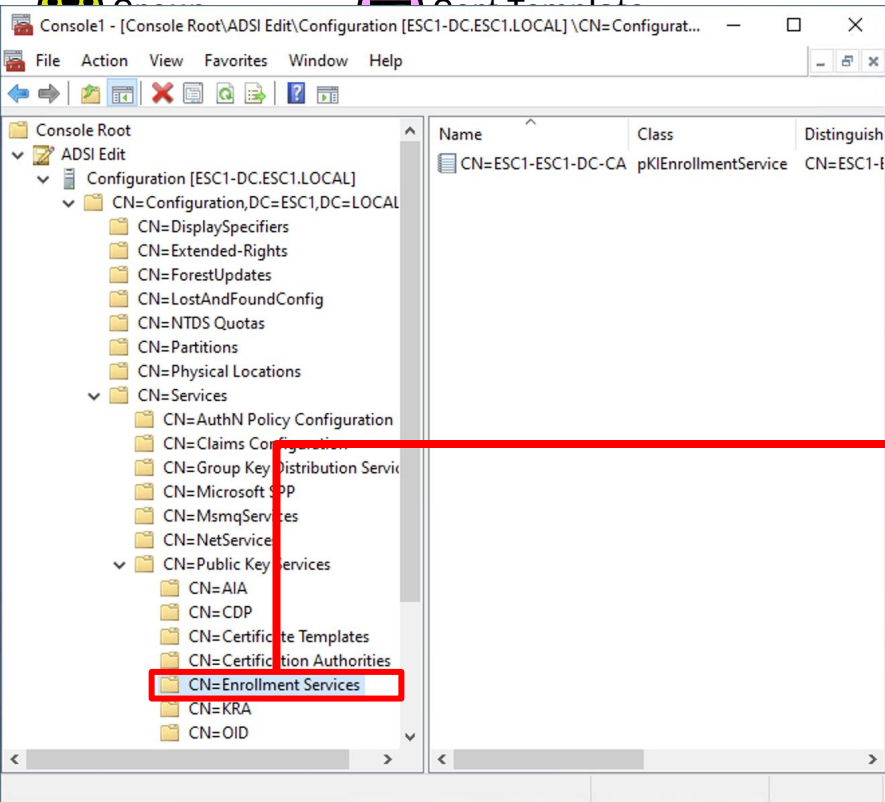
Container



Root CA



Certificate Template



Contains



Contains



Contains



Contains



Contains



**Type:**

Container

**Name:**

ENROLLMENT SERVICES

**ObjectID:**

22F8BB5D-B81E-4856-96A9-A6448386EB23





Domain



Enterprise CA



Container



Root CA



Certificate



Certificate

Console1 - [Console Root\ADSI Edit\Configuration [ESC1-DC.ESC1.LOCAL]\CN=Configurat...

File Action View Favorites Window Help

Console Root

- ADSI Edit
  - Configuration [ESC1-DC.ESC1.LOCAL]
    - CN=Configuration,DC=ESC1,DC=LOCAL
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=NTDS Quotas
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=AuthN Policy Configuration
        - CN=Claims Configuration
        - CN=Group Key Distribution Service
        - CN=Microsoft SPP
        - CN=MsmqServices
        - CN=NetServices
        - CN=Public Key Services
          - CN=AIA
          - CN=CDP
          - CN=Certificate Templates
          - CN=Certification Authorities
          - CN=Enrollment Services
          - CN=KRA
          - CN=OID

Name	Class	Distinguish
CN=AIA	container	CN=AIA,CN=...
CN=CDP	container	CN=CDP,CN=...
CN=Certificate Templ...	container	CN=Certifi...
CN=Certification Aut...	container	CN=Certifi...
CN=Enrollment Servi...	container	CN=Enrollr...
CN=KRA	container	CN=KRA,CN=...
CN=NTAuthCertificates	certificationAuthority	CN=NTAut...
CN=OID	msPKI-Enterprise-O...	CN=OID,CN=...



Contains



Contains



Contains



Contains



Contains

Contains

**Type:** NTAAuthStore

**Name:** NTAAuthCertificates

**ObjectID:** 722A8BB3-AEF5-49C7-9C8C-C1C97A219007

**caCerts:** [ ]



Domain



Enterprise CA



Container



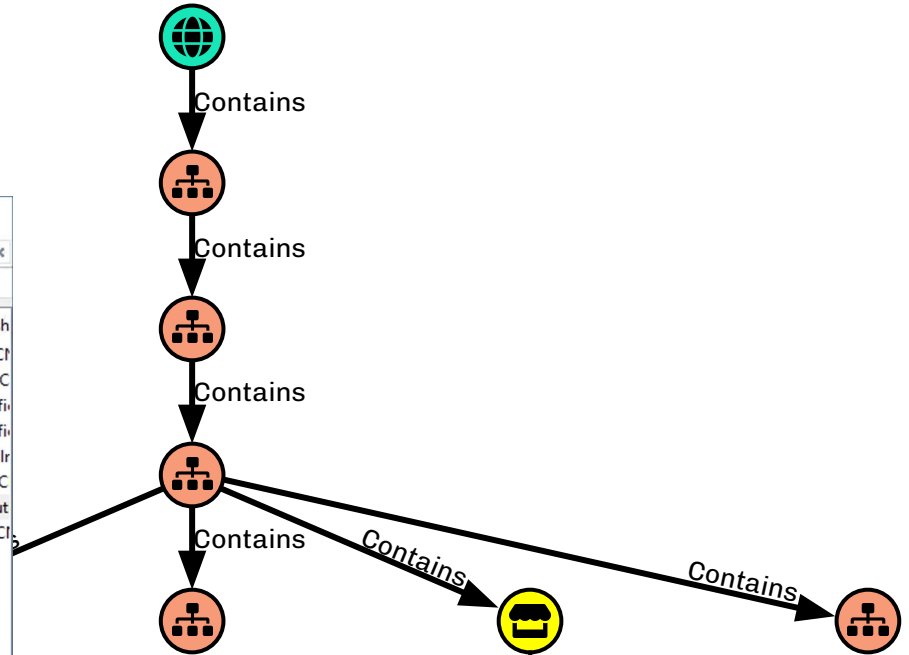
Root CA



Certificate



Certificate Template



**Type:** NTAAuthStore  
**Name:** NTAAuthCertificates  
**ObjectID:** 722A8BB3-AEF5-49C7-9C8C-C1C97A219007  
**caCerts:** [ ]



Console1 - [Console Root\ADSI Edit\Configuration [ESC1-DC.ESC1.LOCAL]\CN=Configurat...

File Action View Favorites Window Help

Console Root

- ADSI Edit
  - Configuration [ESC1-DC.ESC1.LOCAL]
    - CN=Configuration,DC=ESC1,D
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=NTDS Quotas
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=AuthN Policy Conf
        - CN=Claims Configurati
        - CN=Group Key Distribut
        - CN=Microsoft SPP
        - CN=MsmqServices
        - CN=NetServices
        - CN=Public Key Services
          - CN=AIA
          - CN=CDP
          - CN=Certificate Temp
          - CN=Certification Au
          - CN=Enrollment Serv
          - CN=KRA
          - CN=OID

CN=NTAuthCertificates Properties

Attribute Editor Security

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
authorityRevocationList	
cACertificate	\30\82\03\69\30\82\02\51\A0\03\02\01
cACertificateDN	<not set>
cAConnect	<not set>
cAUsages	<not set>
cAWEURL	<not set>
certificateRevocation...	
certificateTemplates	<not set>
cn	NTAuthCertificates
cRLObj	<not set>
crossCertificatePair	<not set>
currentParentCA	<not set>

Edit OK Cancel Apply Help



Domain



Enterprise CA



Container



Root CA



Certificate



Certificate Template



Contains



Contains



Contains



Contains



Contains

Contains

Contains



Type:

NTAuthStore

Name:

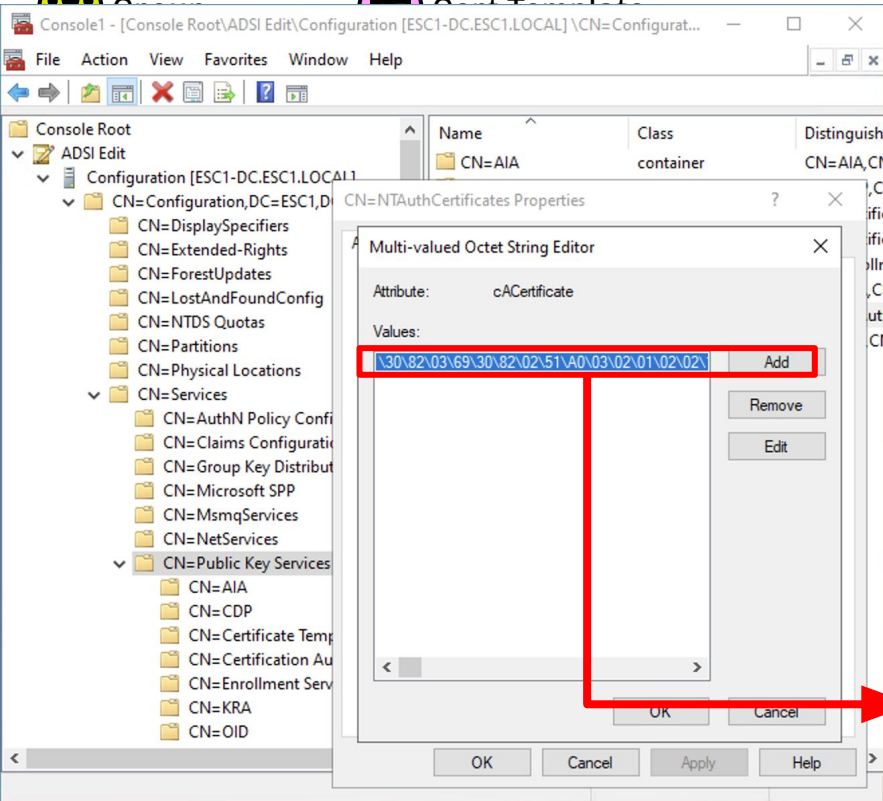
NTAuthCertificates

ObjectID:

722A8BB3-AEF5-49C7-9C8C-C1C97A219007

caCerts:

[ 5F0143662A7EA16E8DB90E44D0F1F1FC87B...]





Domain



Enterprise CA



Container



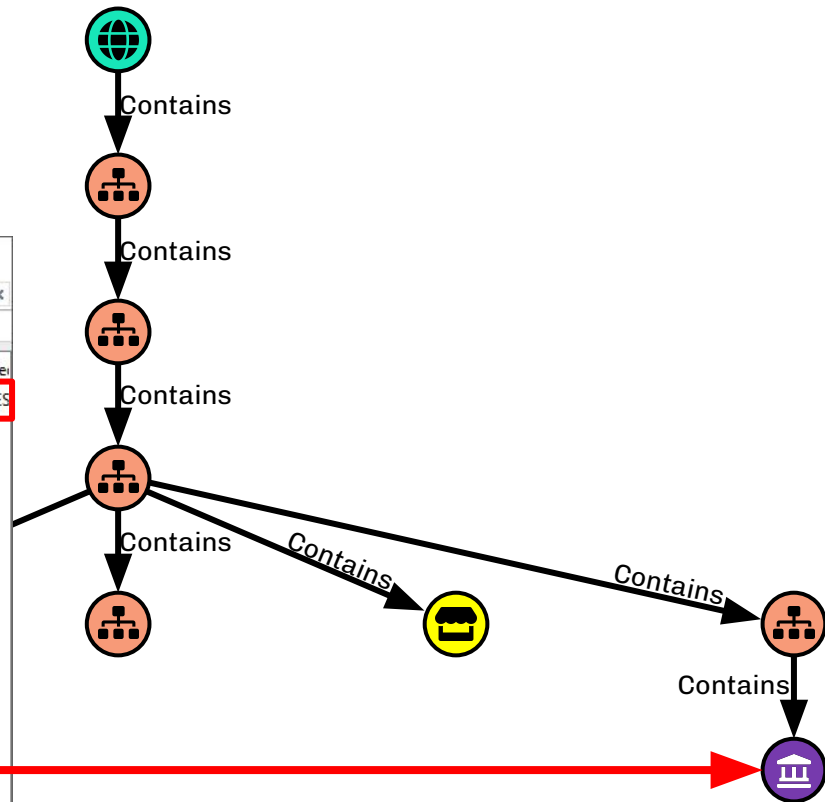
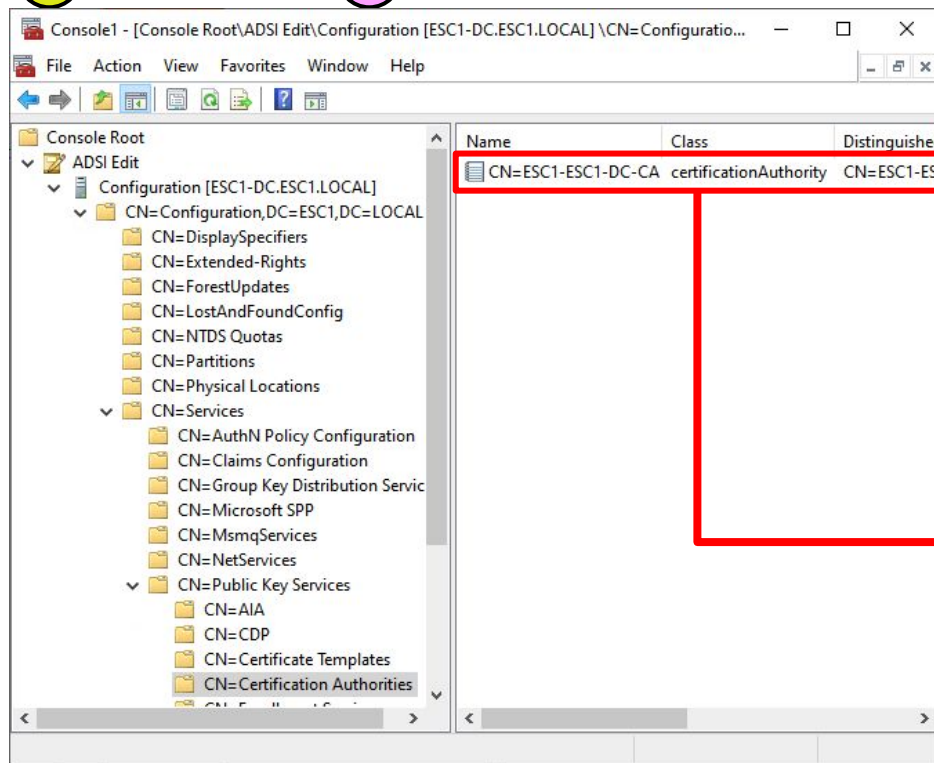
Root CA



Group



Cert Template





Domain



Enterprise CA



Container



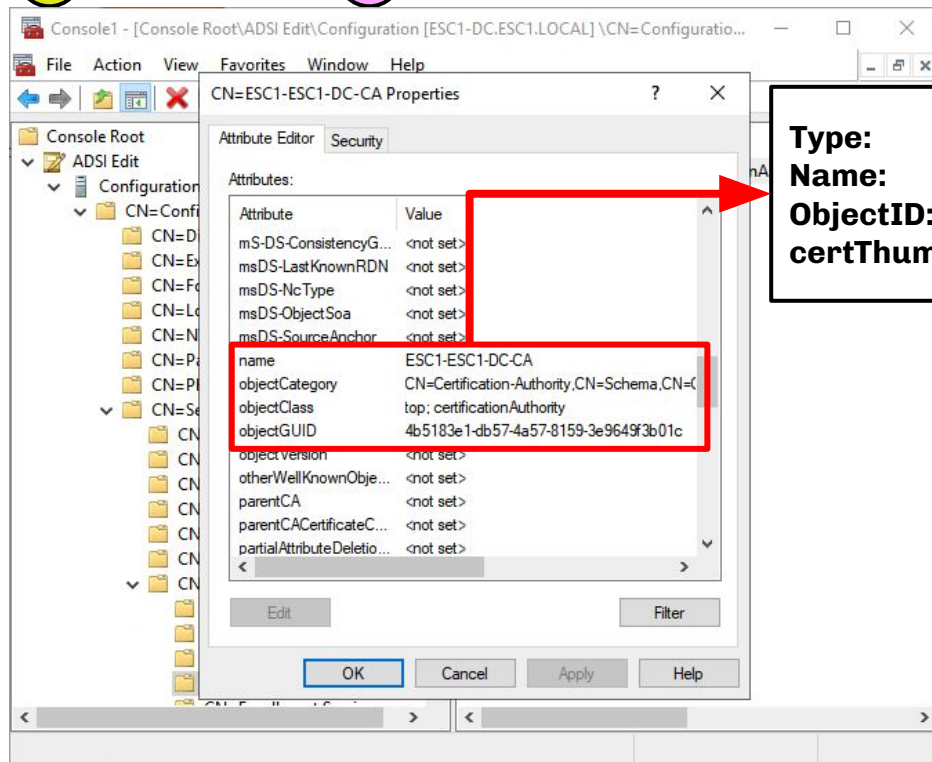
Root CA



Group



Cert Template



Contains



Contains

**Type:** RootCA  
**Name:** ESC1-ESC1-DC-CA  
**ObjectID:** 4B5183E1-DB57-4A57-8159-3E9649F3B01C  
**certThumbprint:**



Contains



Contains

Contains



Contains





Domain



Enterprise CA



Container



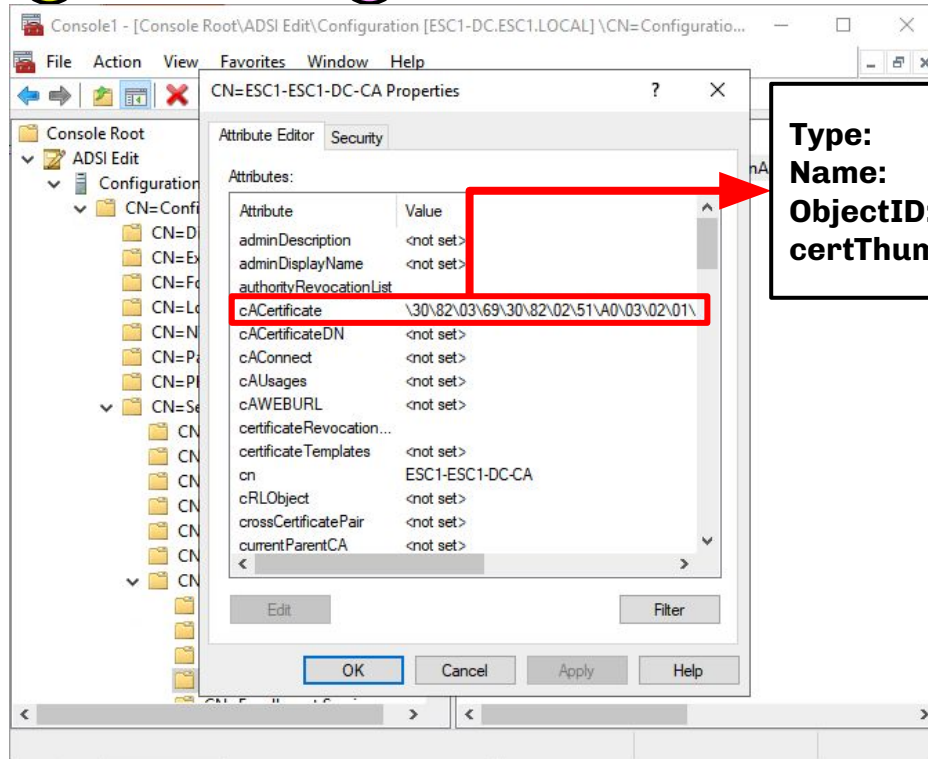
Root CA



Group



Cert Template



**Type:** RootCA  
**Name:** ESC1-ESC1-DC-CA  
**ObjectID:** 4B5183E1-DB57-4A57-8159-3E9649F3B01C  
**certThumbprint:** 5F0143662A7EA16E8DB90E44D0F1F1FC87B1E...



Contains



Contains



Contains

Contains



Contains

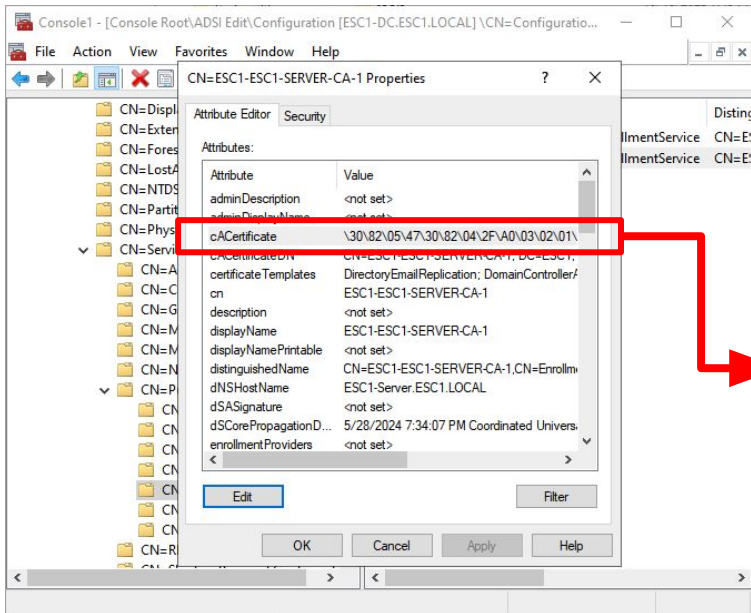


Contains

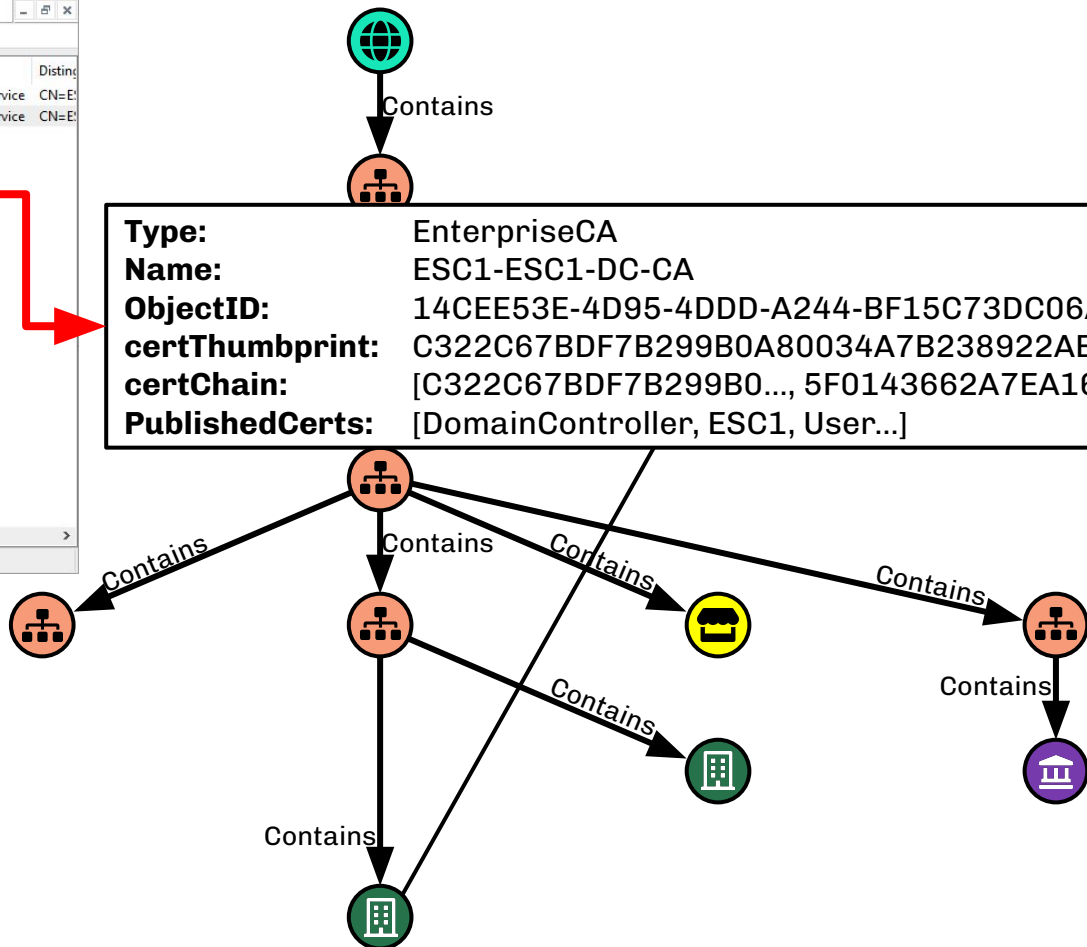


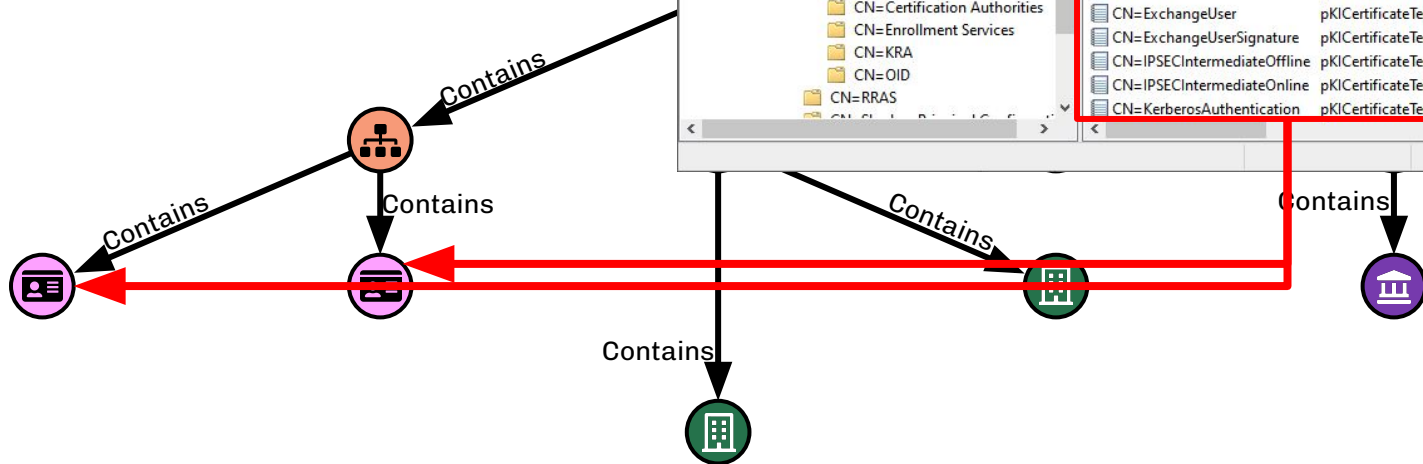
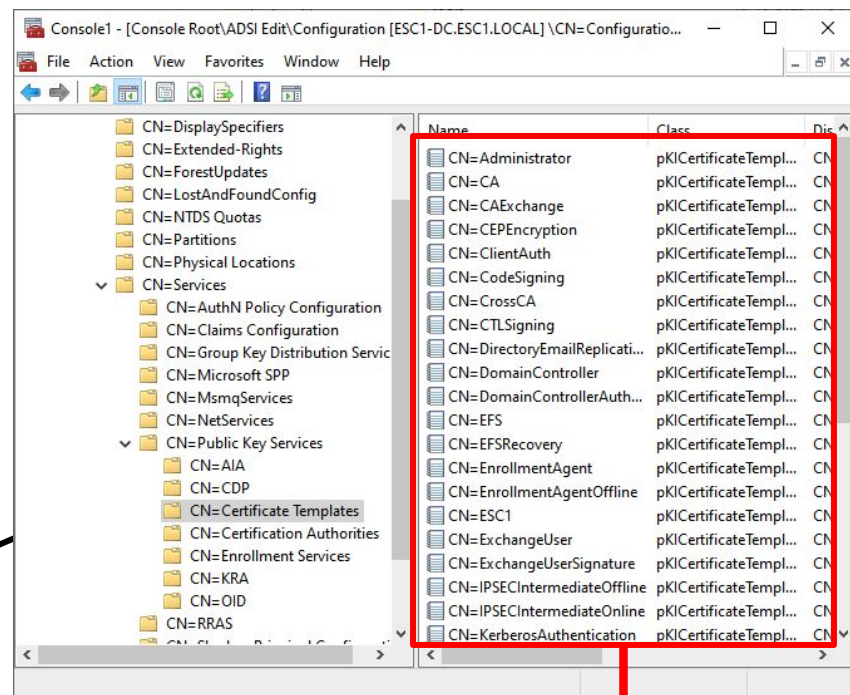


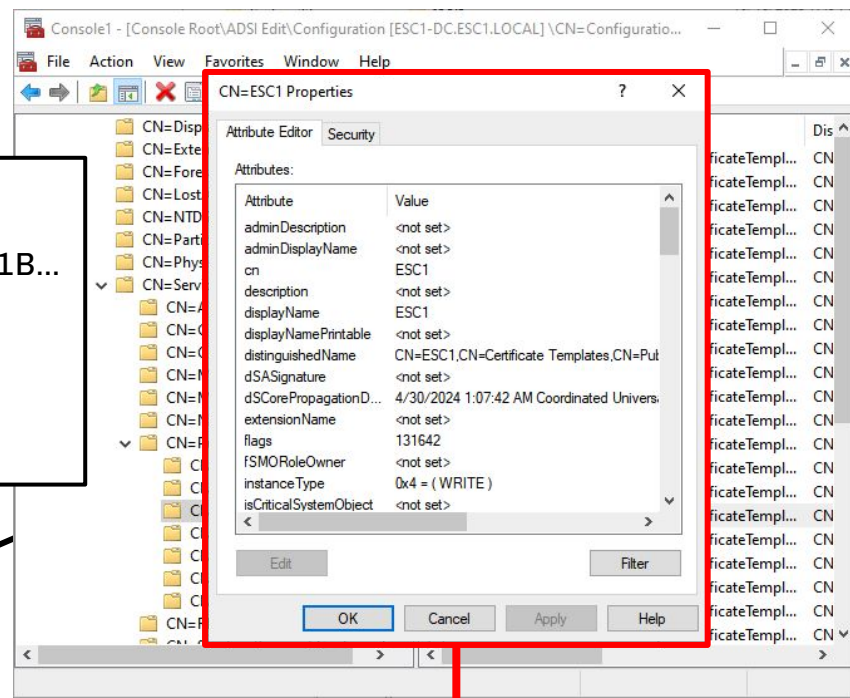
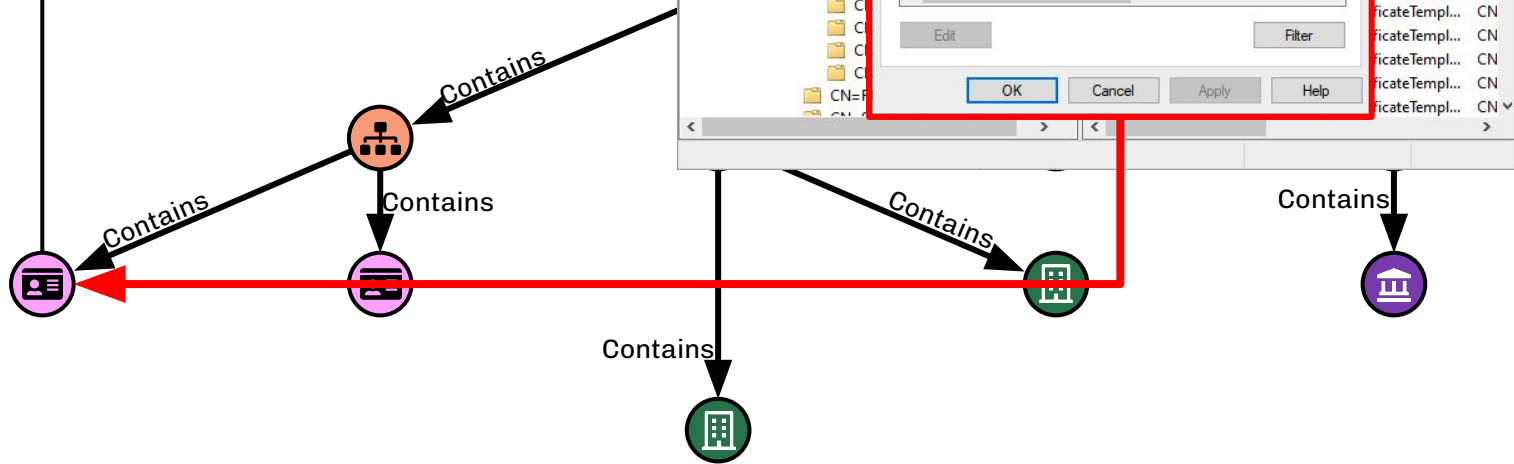
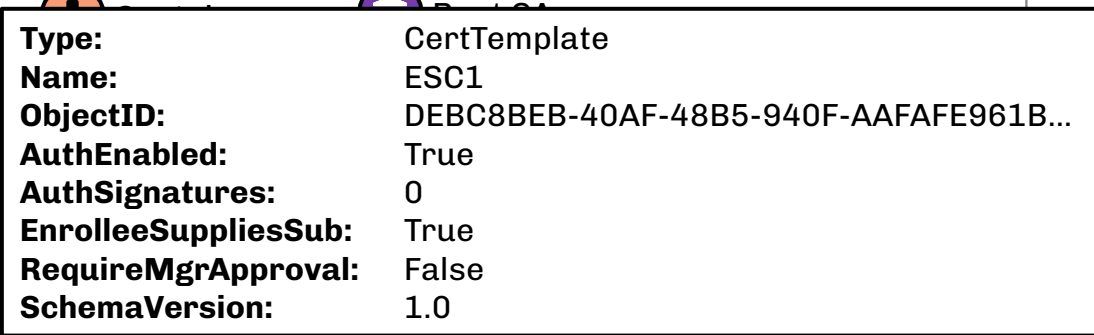




**Type:** EnterpriseCA  
**Name:** ESC1-ESC1-DC-CA  
**ObjectID:** 14CEE53E-4D95-4DDD-A244-BF15C73DC06A  
**certThumbprint:** C322C67BDF7B299B0A80034A7B238922AB1E1...  
**certChain:** [C322C67BDF7B299B0..., 5F0143662A7EA16E...]  
**PublishedCerts:** [DomainController, ESC1, User...]









-  Domain
-  Container
-  Group
-  NT Authority

Group 1 Properties

Object Security Attribute Editor

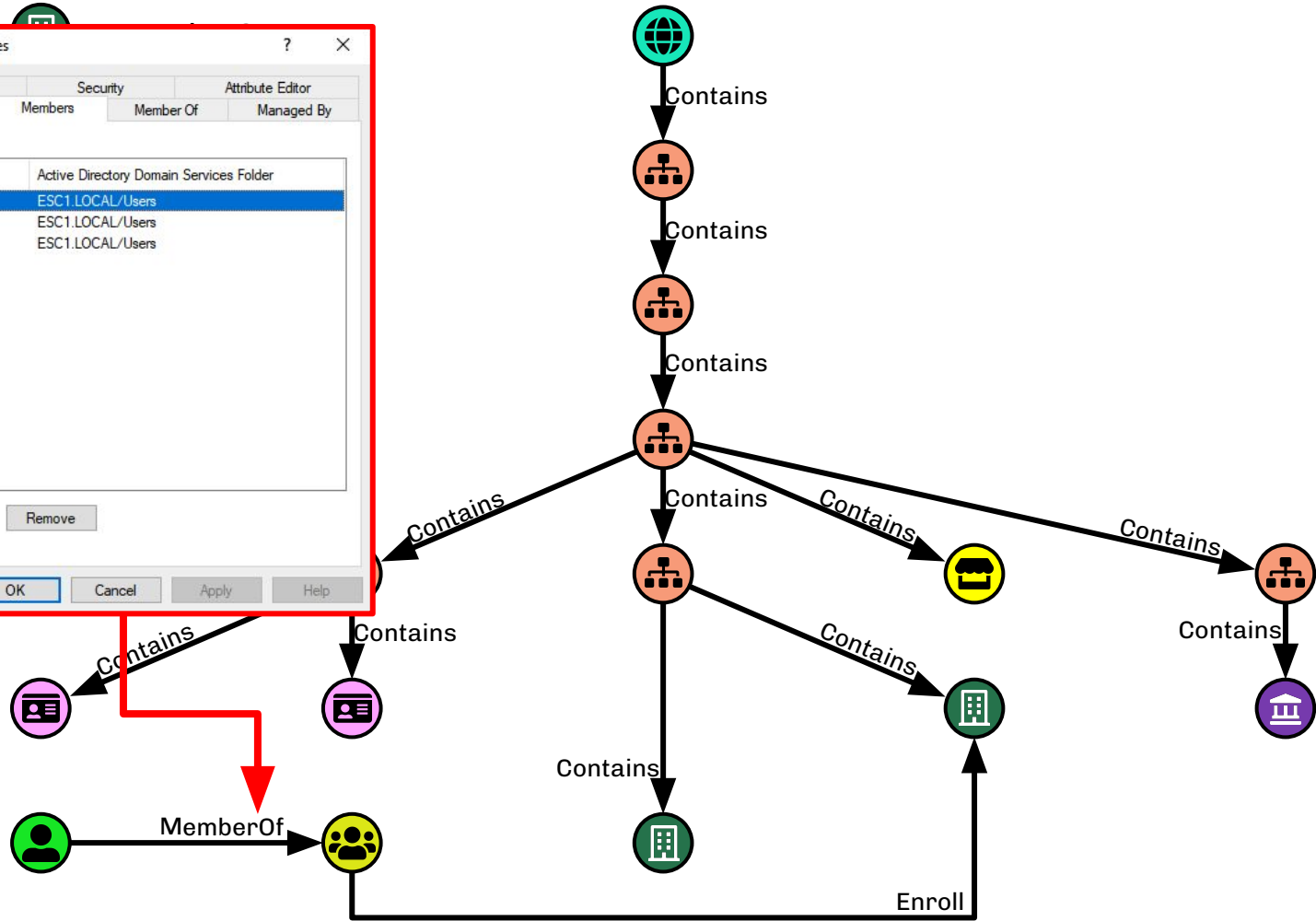
General Members Member Of Managed By

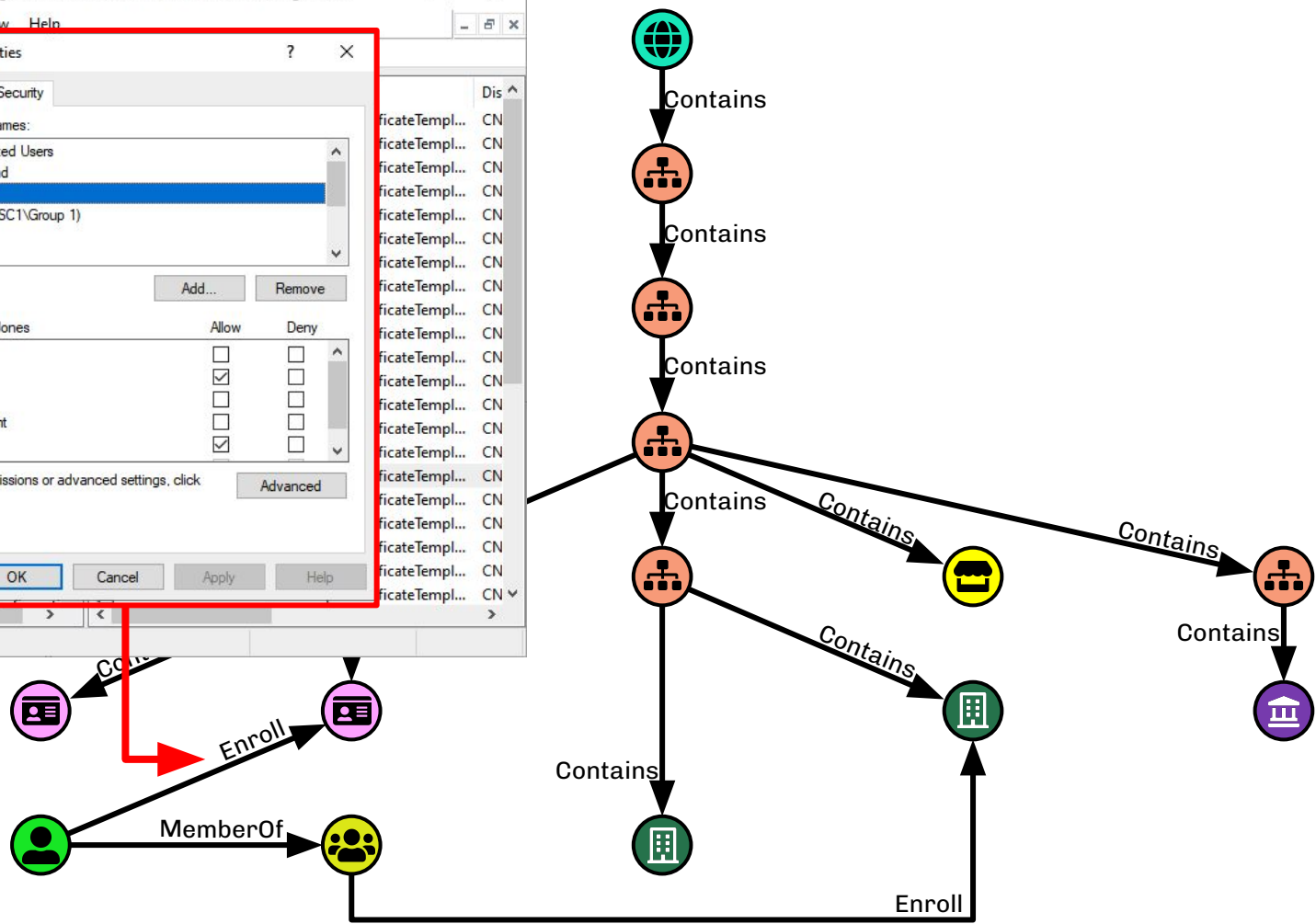
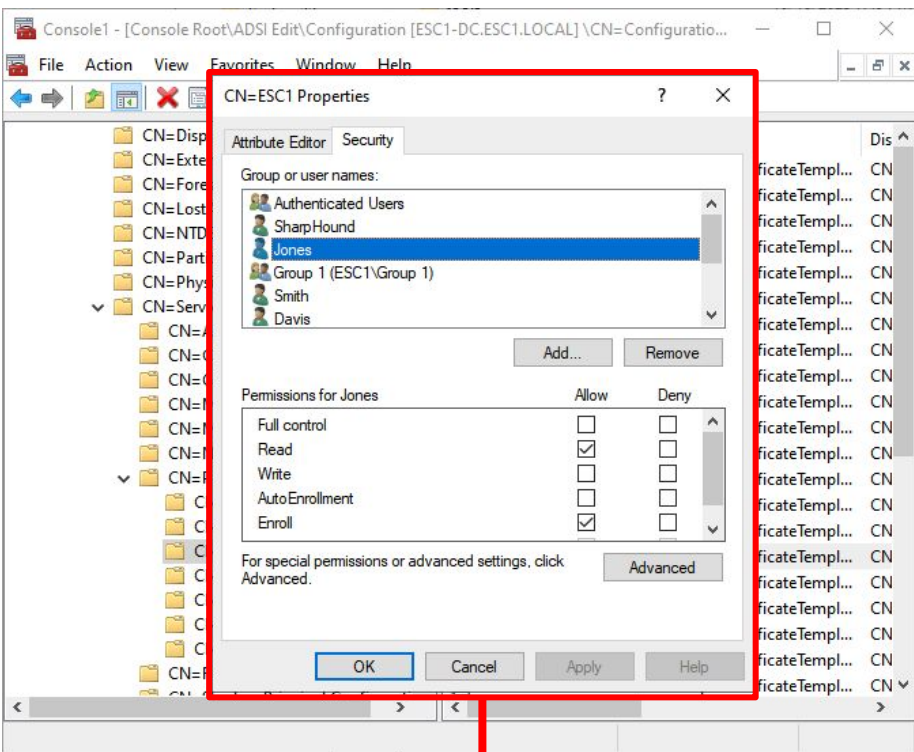
Members:

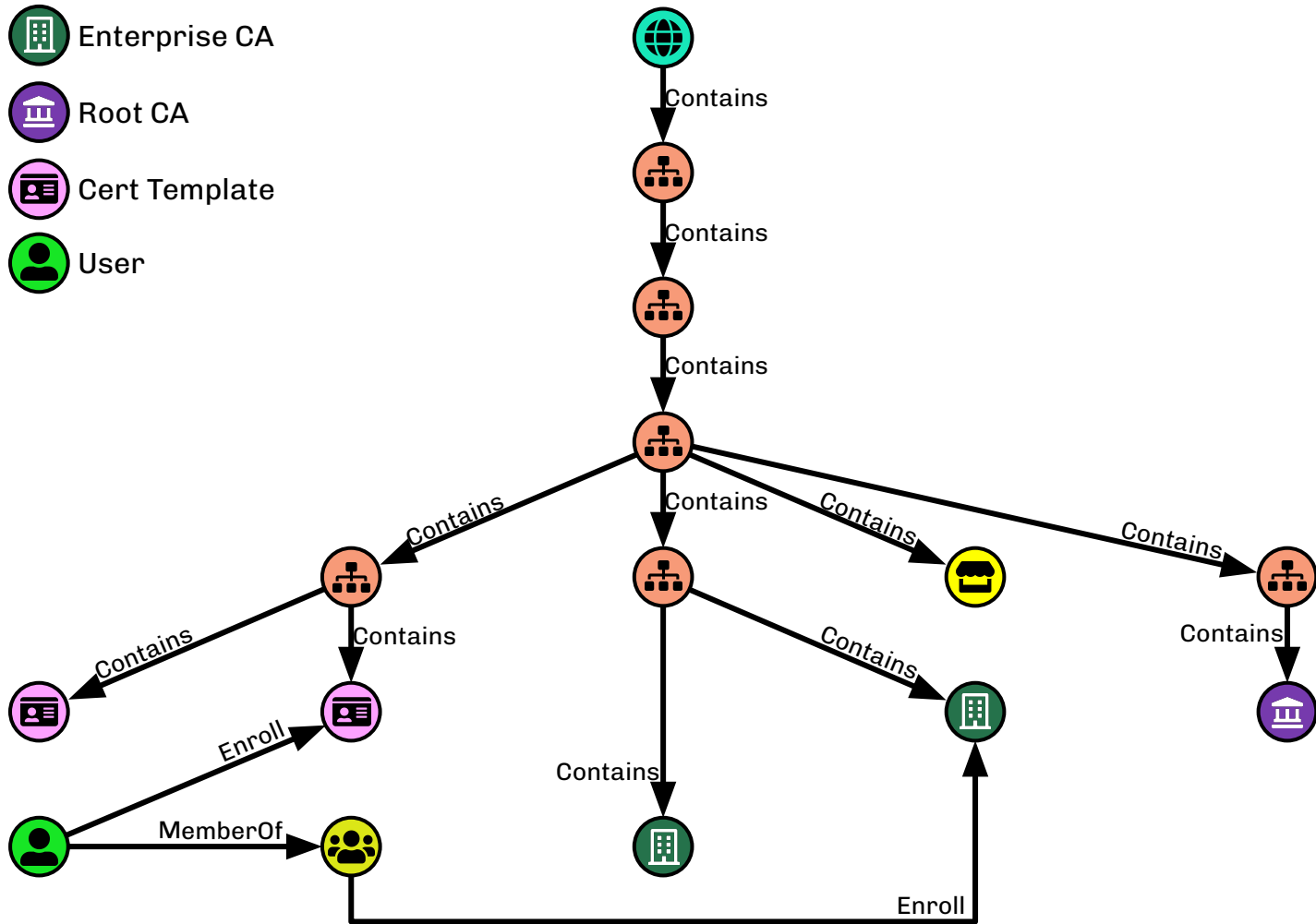
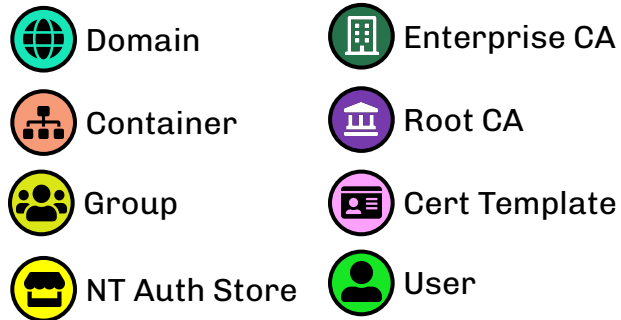
Name	Active Directory Domain Services Folder
Garcia	ESC1.LOCAL/Users
Group 2	ESC1.LOCAL/Users
Jones	ESC1.LOCAL/Users

Add... Remove

OK Cancel Apply Help

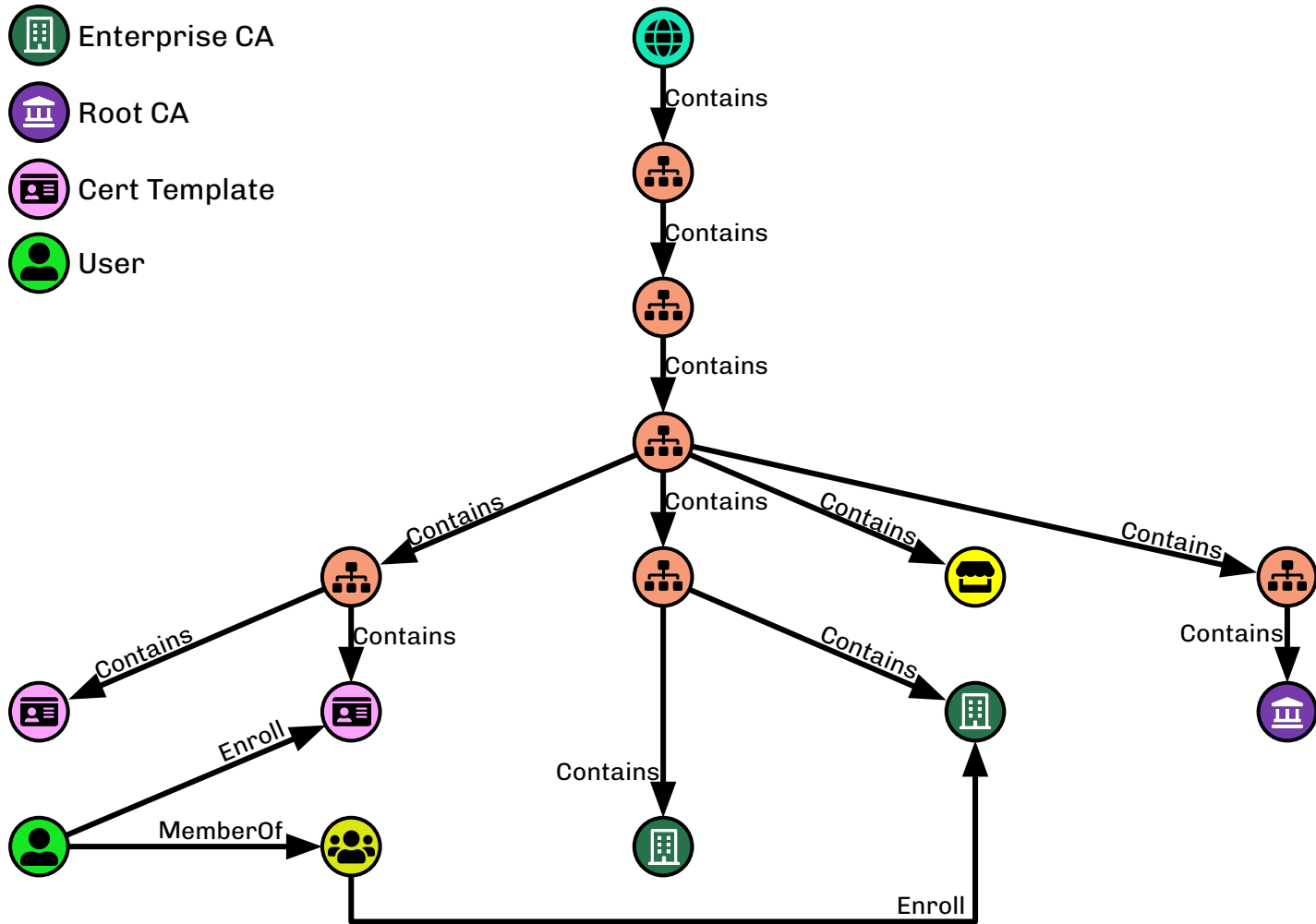
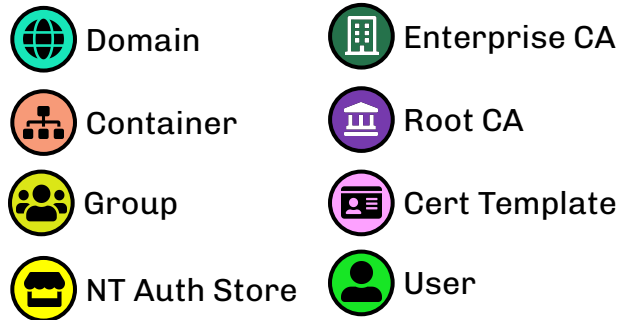


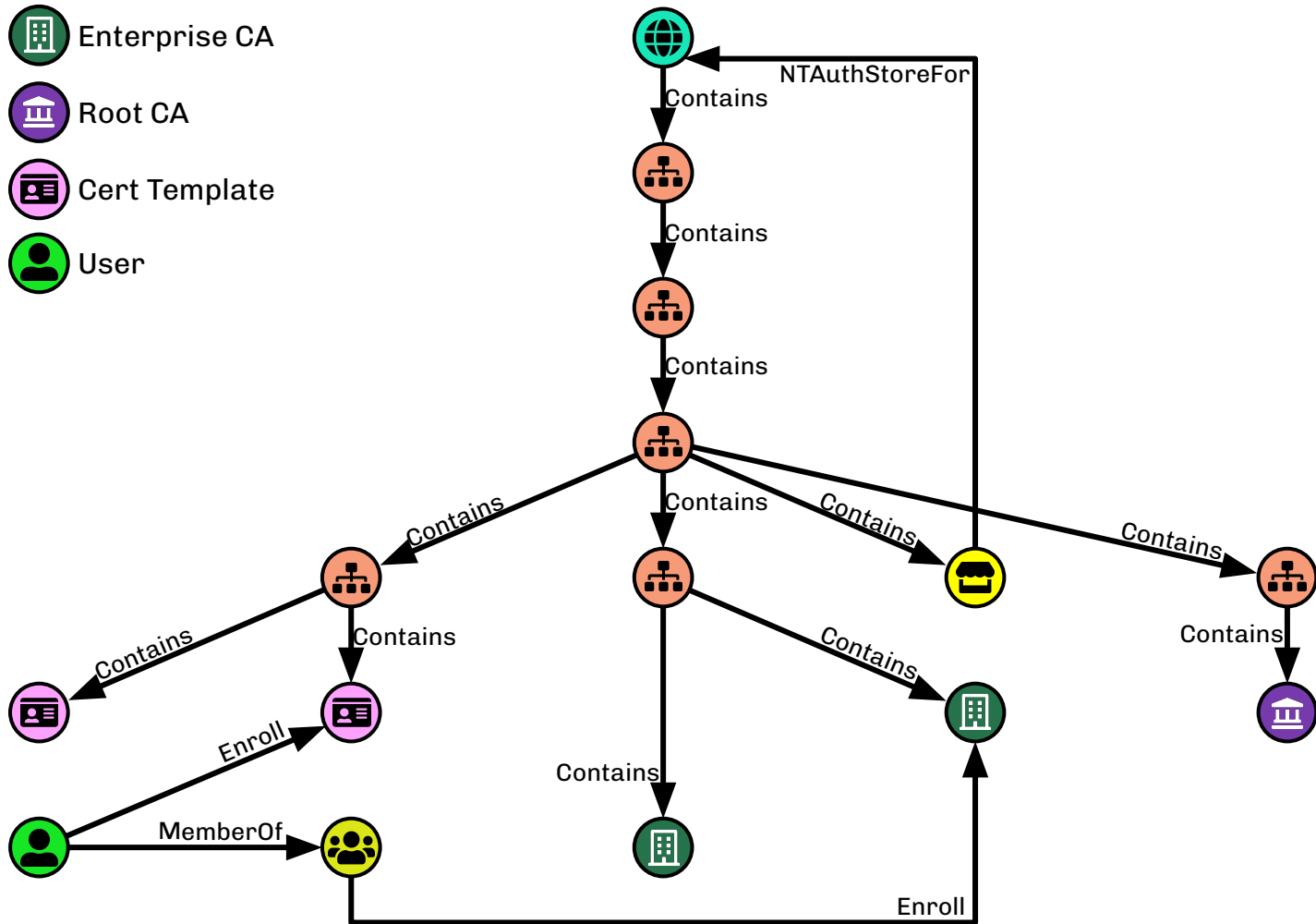
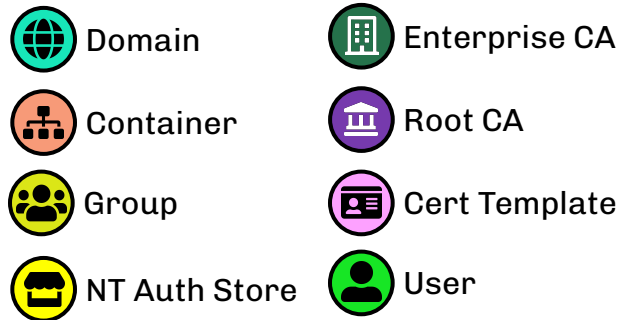


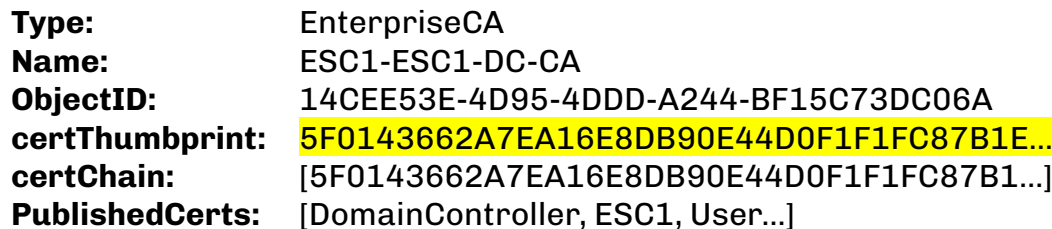
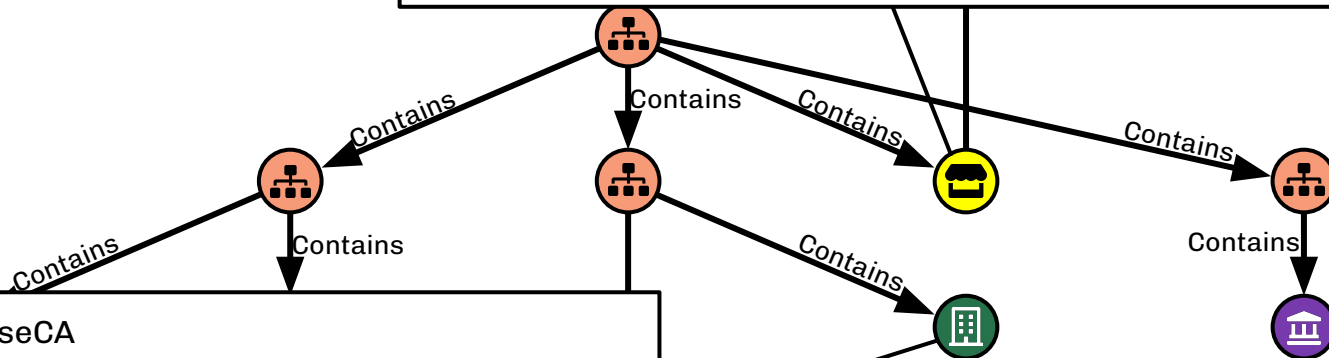
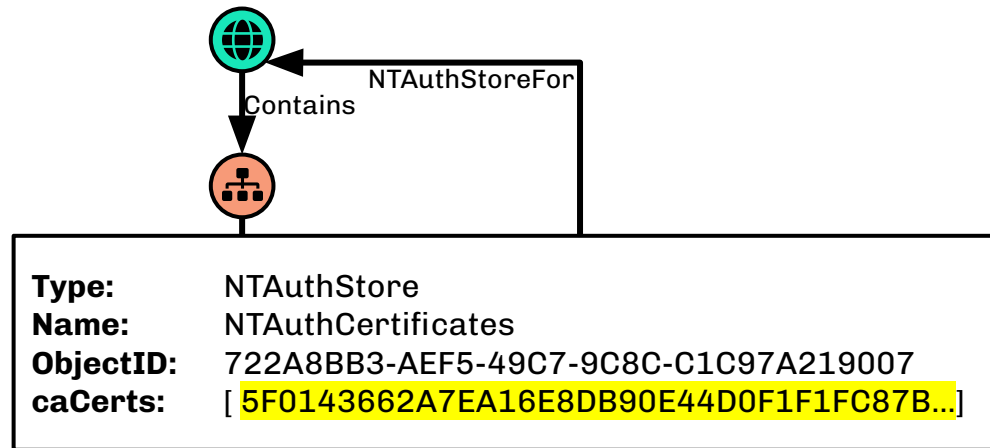
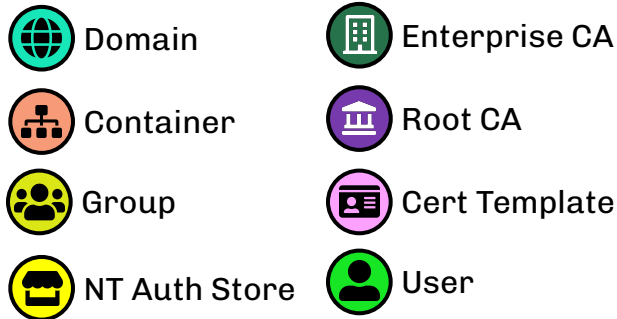


# Agenda

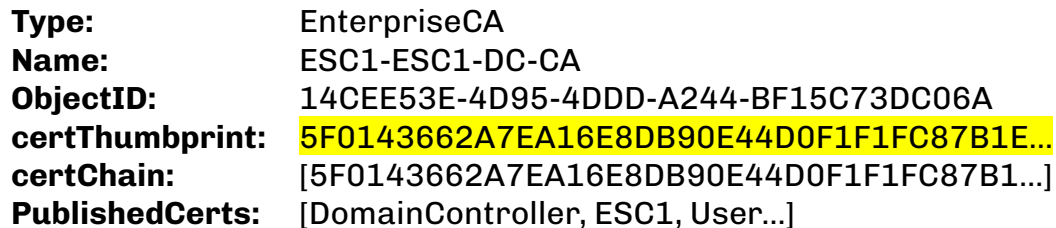
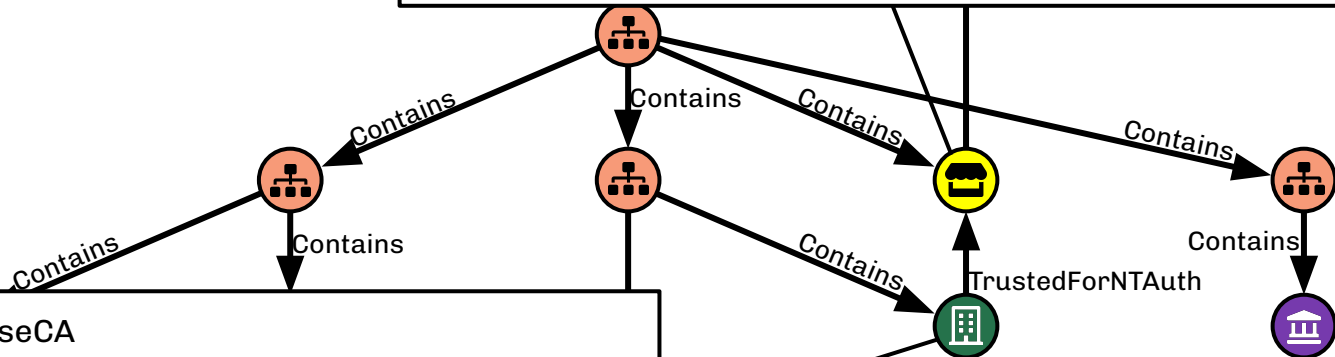
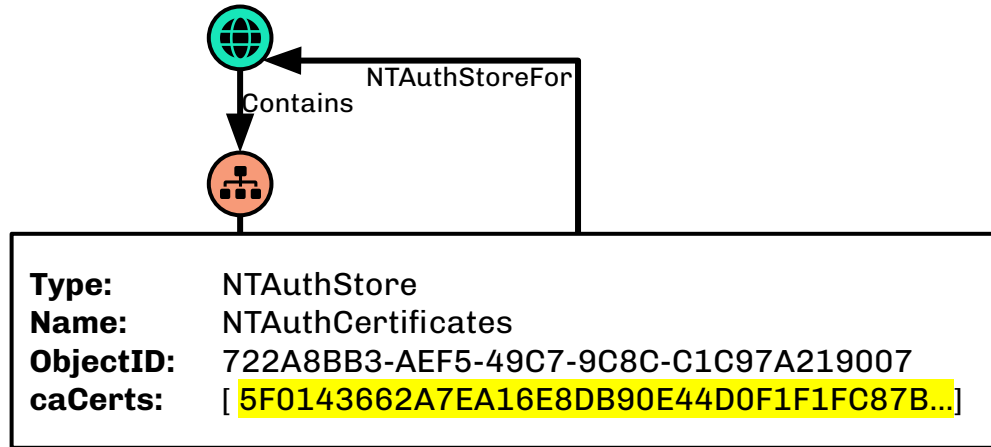
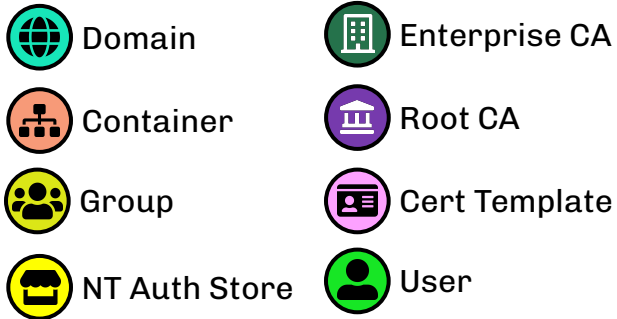
- **How we model ADCS in BloodHound**
  - The model's place, primitives, and purpose
  - Data sources and initial model
  - **Post-processing to enrich the model**
- ADCS Attack Path discovery and execution
- Remediation Strategies and Practical Examples
- Conclusion







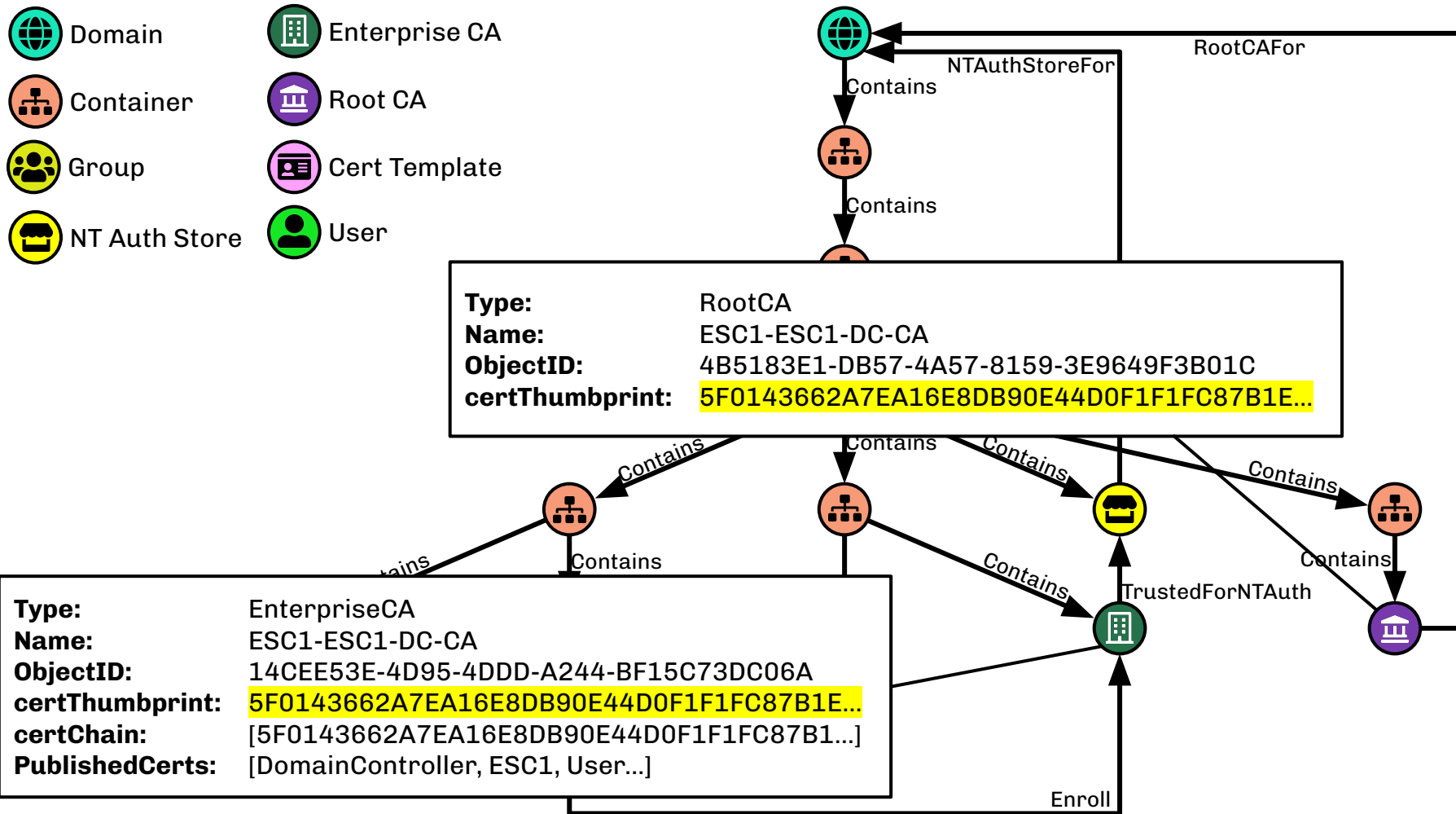
Enroll

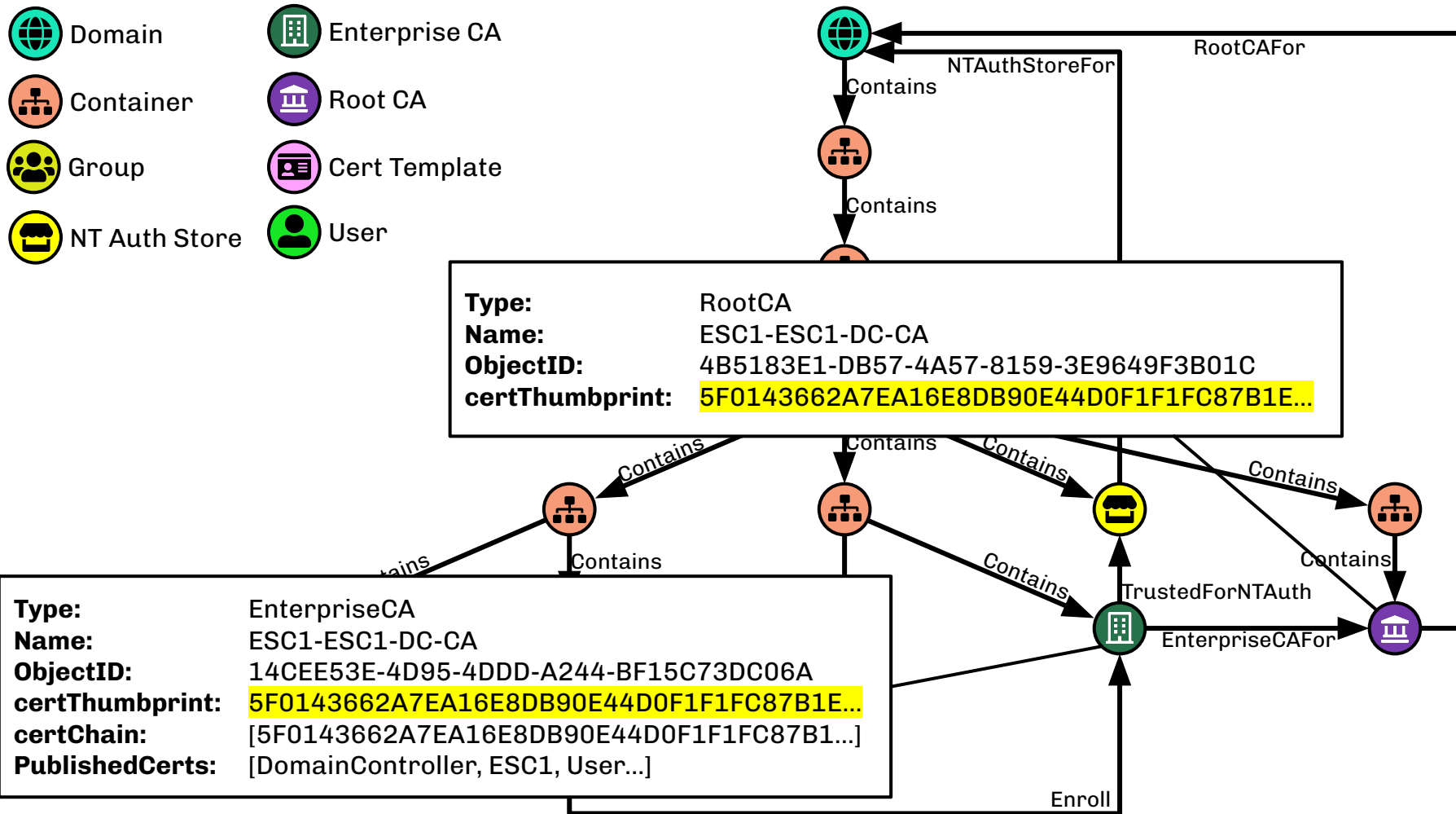


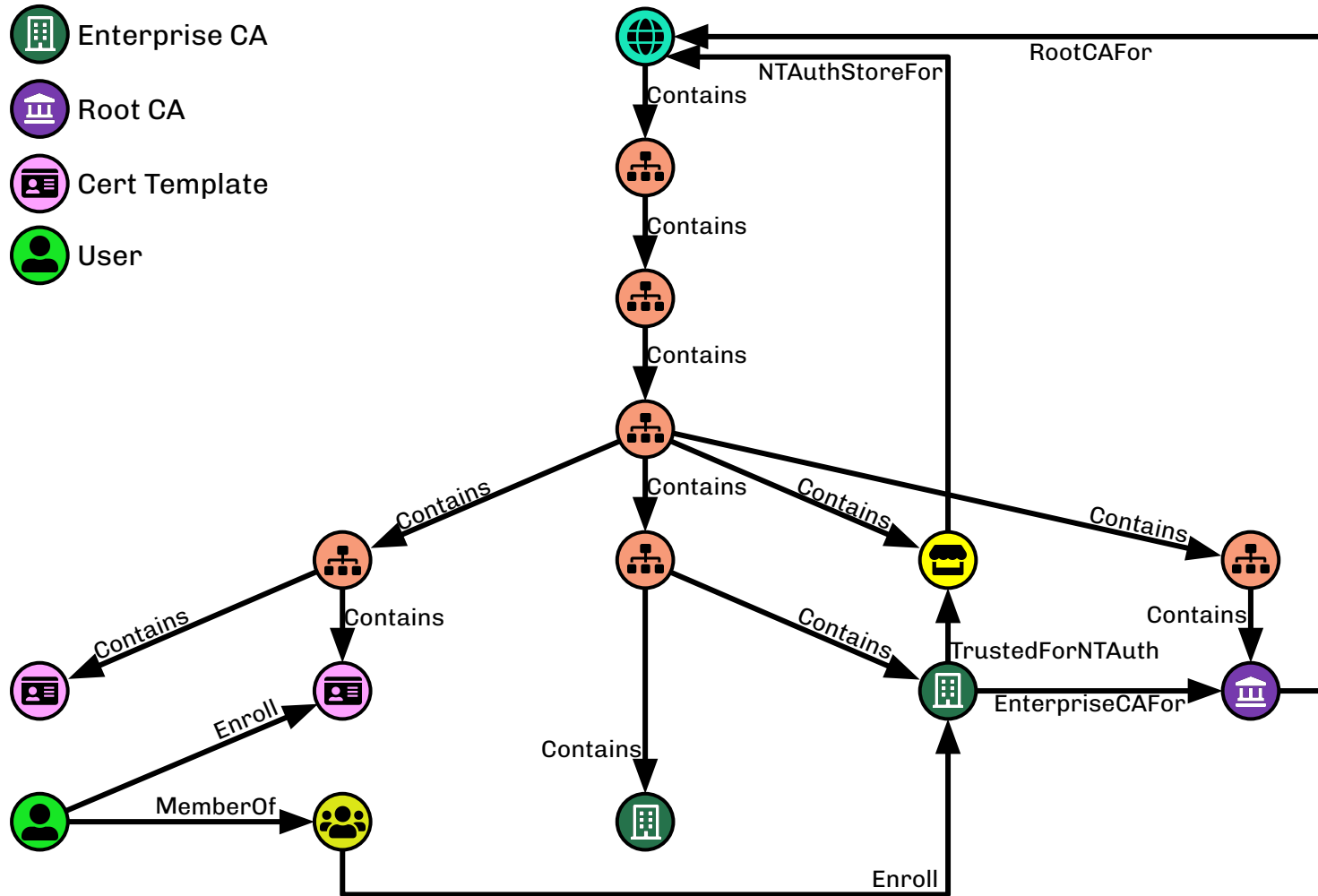
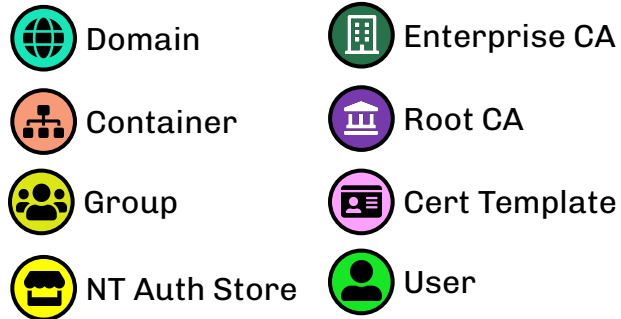
Enroll

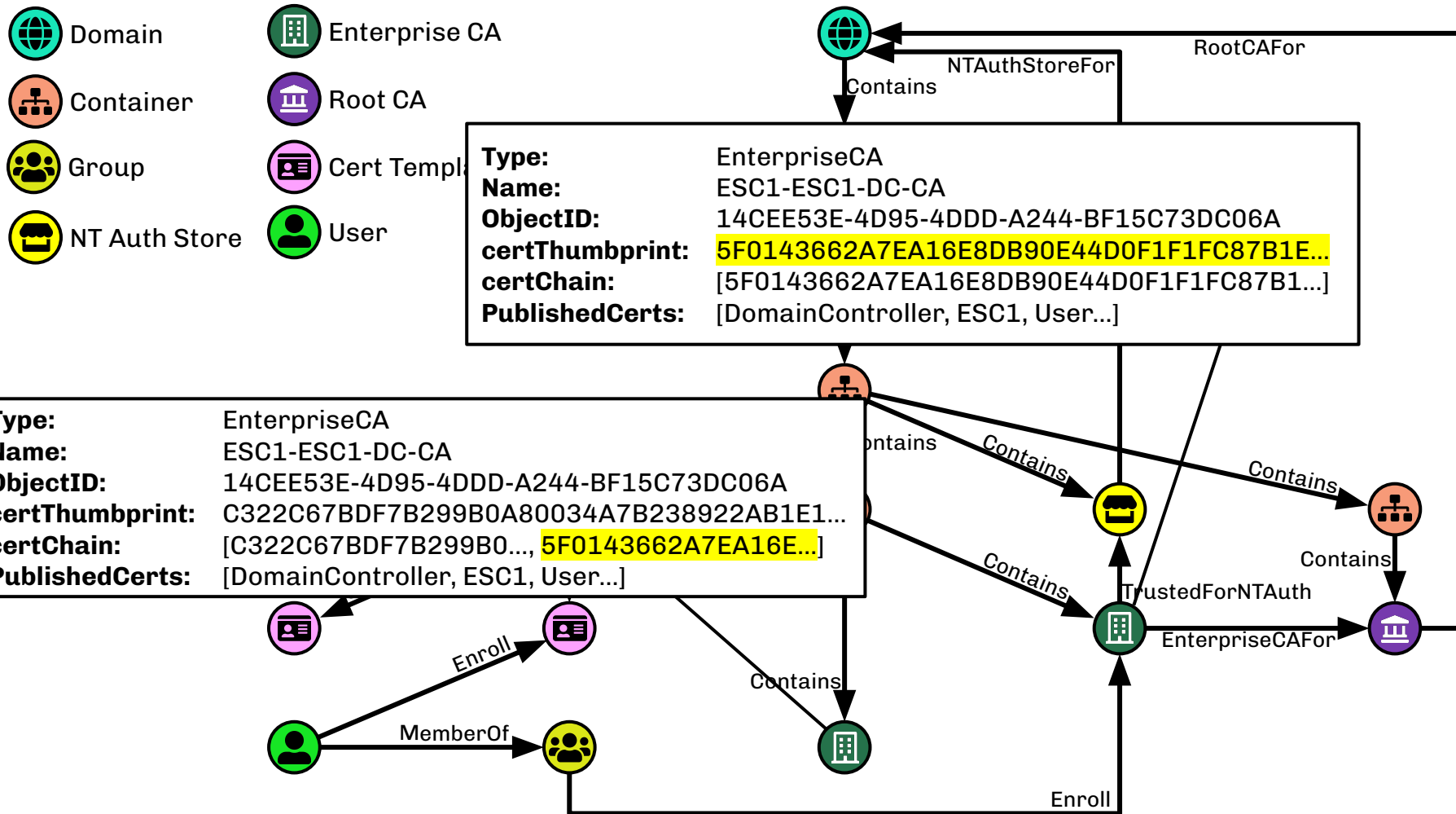














Domain



Enterprise CA



Container



Root CA



Group



Cert Template



NT Auth Store



User

**Type:** EnterpriseCA  
**Name:** ESC1-ESC1-DC-CA  
**ObjectID:** 14CEE53E-4D95-4DDD-A244-BF15C73DC06A  
**certThumbprint:** 5F0143662A7EA16E8DB90E44D0F1F1FC87B1E...  
**certChain:** [5F0143662A7EA16E8DB90E44D0F1F1FC87B1...]  
**PublishedCerts:** [DomainController, ESC1, User...]

**Type:** EnterpriseCA  
**Name:** ESC1-ESC1-DC-CA  
**ObjectID:** 14CEE53E-4D95-4DDD-A244-BF15C73DC06A  
**certThumbprint:** C322C67BDF7B299B0A80034A7B238922AB1E1...  
**certChain:** [C322C67BDF7B299B0..., 5F0143662A7EA16E...]  
**PublishedCerts:** [DomainController, ESC1, User...]



Enroll



MemberOf



Contains

NTAuthStoreFor

RootCAFor



Contains

Contains

Contains

Contains

Contains



Contains

IssuedSignedBy

Enroll

TrustedForNTAuth

EnterpriseCAFor







Domain



Enterprise



Container



Root CA



Group



Cert Template

**Type:**

EnterpriseCA

**Name:**

ESC1-ESC1-DC-CA

**ObjectID:**

14CEE53E-4D95-4DDD-A244-BF15C73DC06A

**certThumbprint:**

5F0143662A7EA16E8DB90E44D0F1F1FC87B1E...

**certChain:**

[5F0143662A7EA16E8DB90E44D0F1F1FC87B1...]

**PublishedCerts:**

[DomainController, **ESC1**, User...]

**Type:**

CertTemplate

**Name:**

**ESC1**

**ObjectID:**

DEBC8BEB-40AF-48B5-940F-AAFAFE961B...

**AuthEnabled:**

True

**AuthSignatures:**

0

**EnrolleeSuppliesSub:**

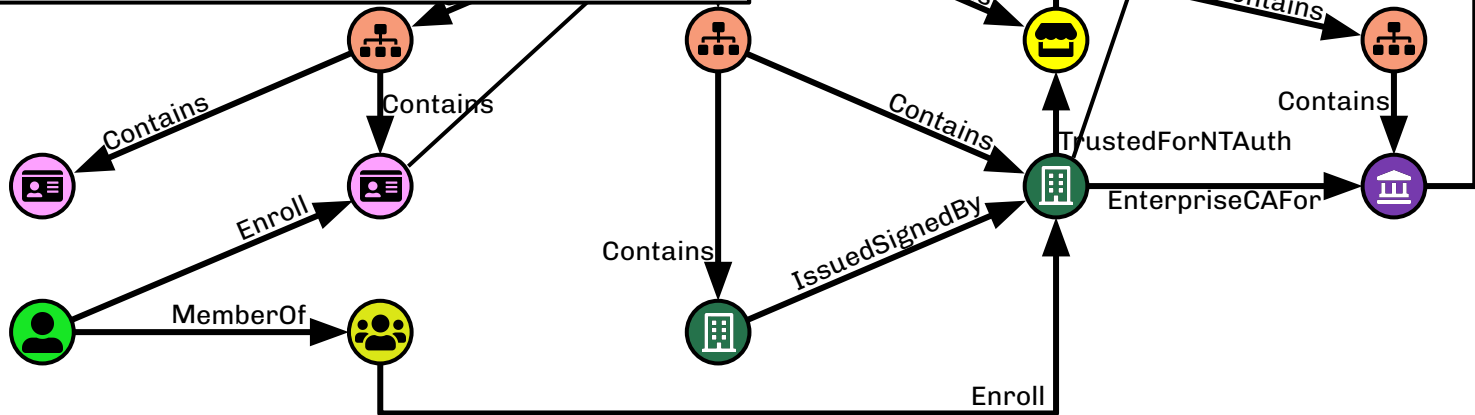
True

**RequireMgrApproval:**

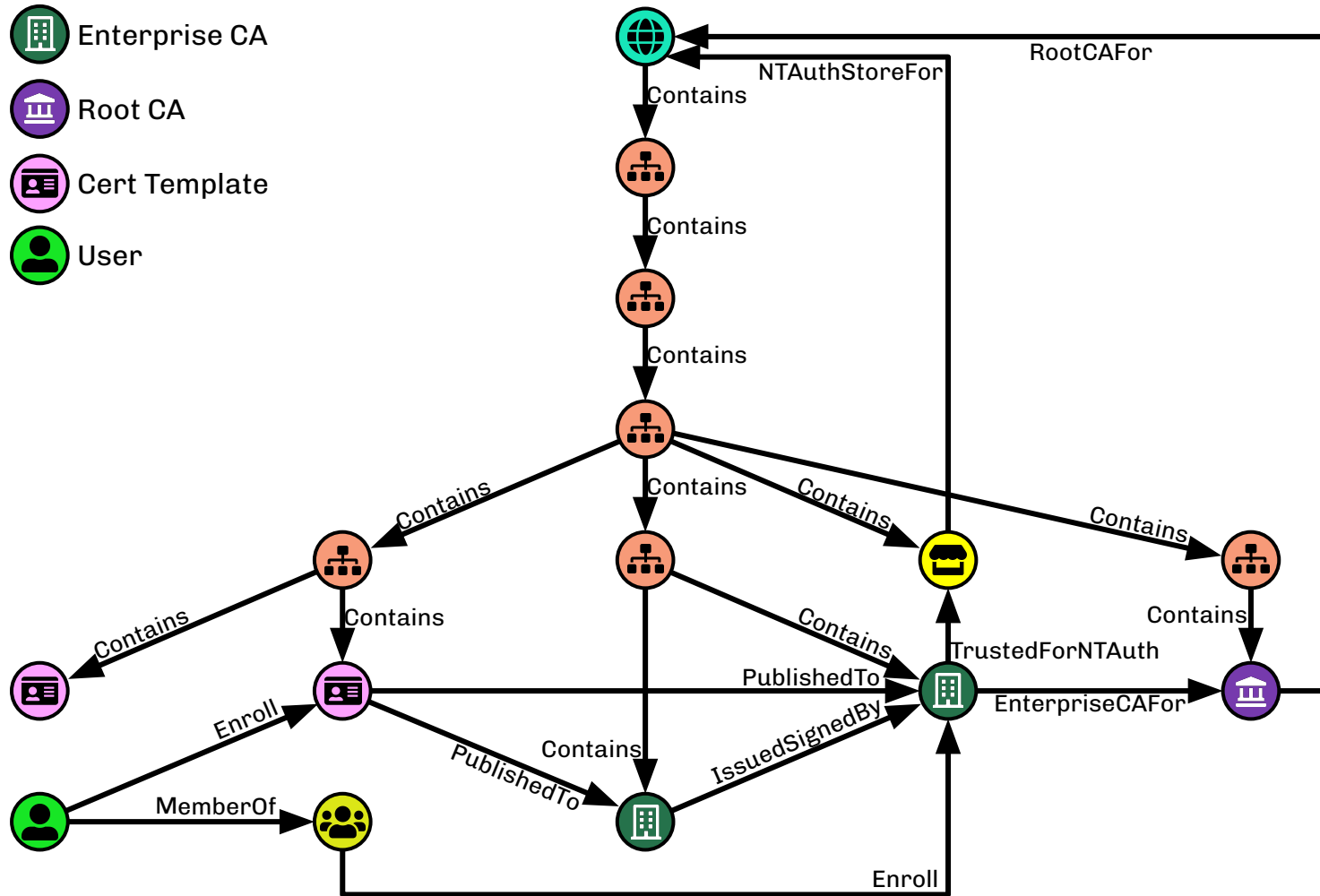
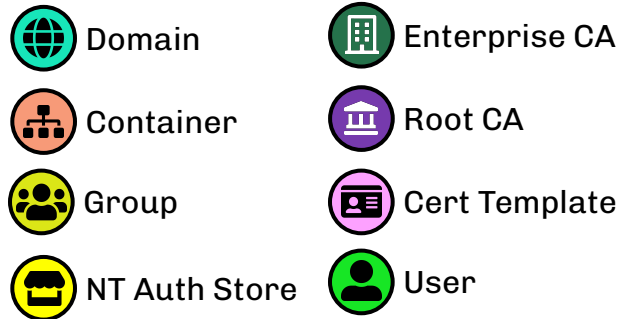
False

**SchemaVersion:**

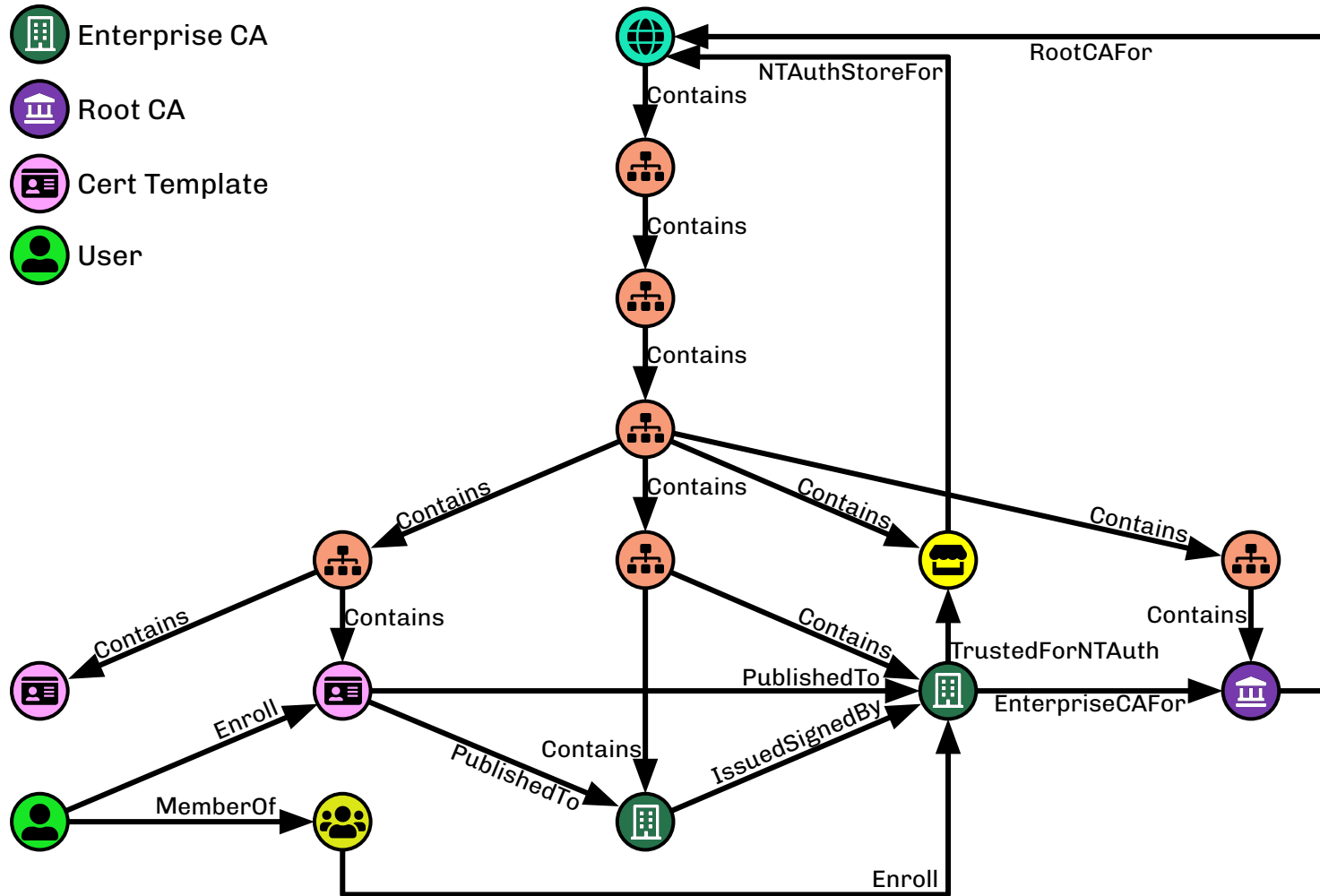
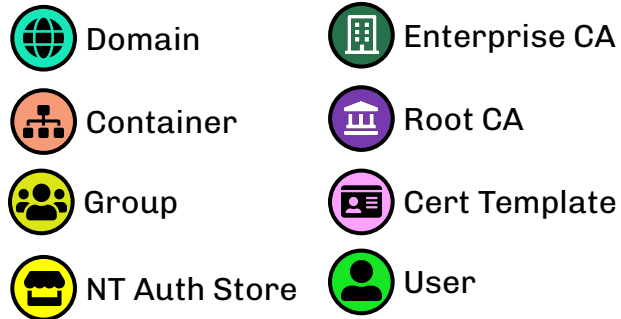
1.0



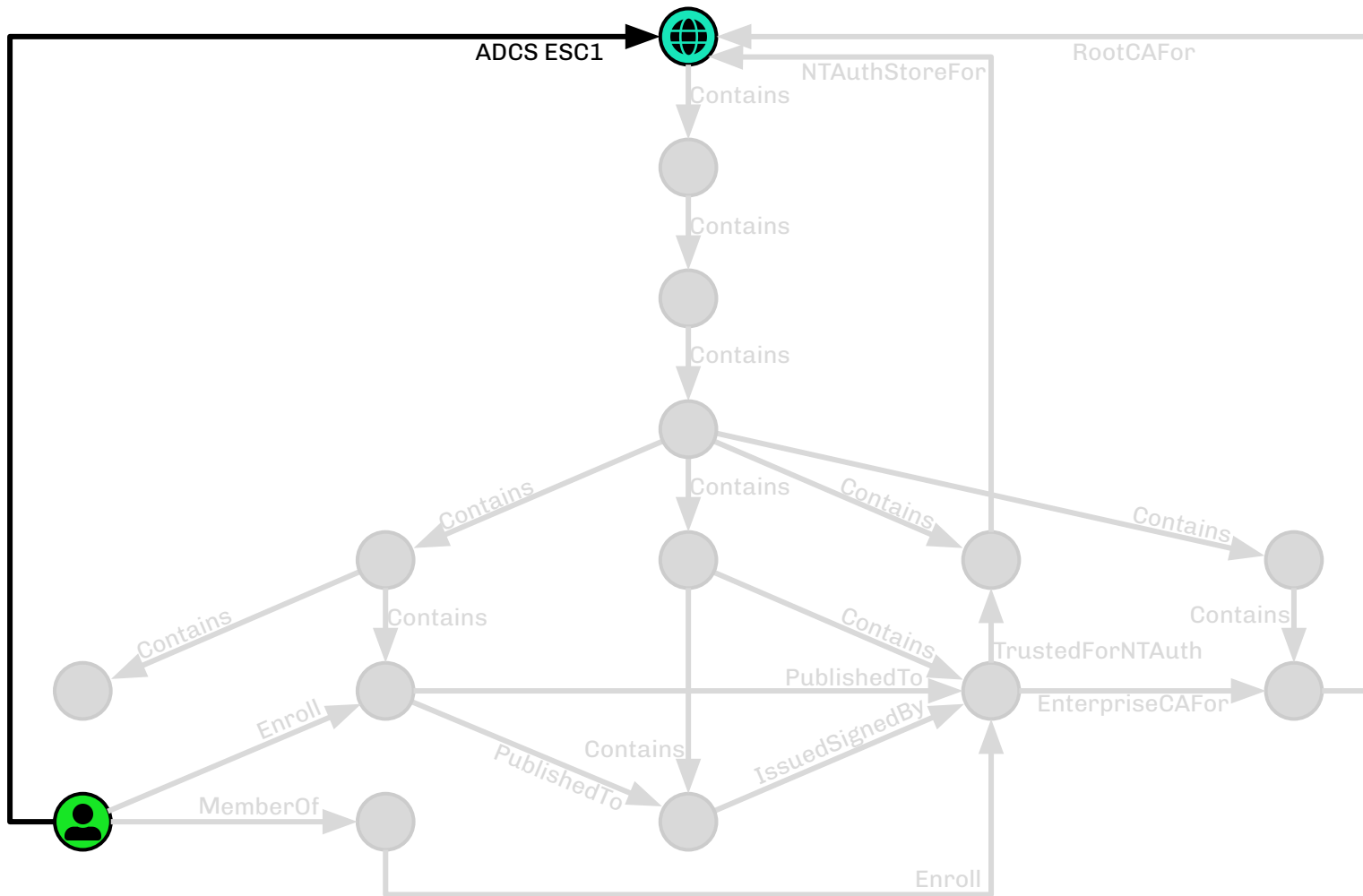




This model enables automatic  
identification of ADCS privilege  
escalation primitives



The diagram illustrates the structure of the Windows Certificate Store. It shows a hierarchy starting with **RootCAFor** (represented by a globe icon). Below it is **NTAuthStoreFor** (represented by a yellow bus icon). The **NTAuthStoreFor** contains a chain of certificates (represented by grey circles). One of these certificates is **TrustedForNTAuth** (represented by a green building icon). The **TrustedForNTAuth** contains a certificate **EnterpriseCAFor** (represented by a purple building icon). The **EnterpriseCAFor** contains a certificate **IssuedSignedBy** (represented by a grey circle). The **IssuedSignedBy** contains a certificate **Enroll** (represented by a grey circle). The **TrustedForNTAuth** is also **PublishedTo** the **EnterpriseCAFor**.



# Agenda

- How we model ADCS in BloodHound
- **ADCS Attack Path discovery and execution**
  - **ESC1**
  - **ESC3**
  - **ESC4**
- Remediation Strategies and Practical Examples
- Conclusion

# Agenda

- How we model ADCS in BloodHound
- **ADCS Attack Path discovery and execution**
  - **ESC1**
  - ESC3
  - ESC4
- Remediation Strategies and Practical Examples
- Conclusion



ESC1 Cert Template



Enterprise CA



Domain Controller



Alice



Bob



ESC1 Cert Template



Enterprise CA



Domain Controller

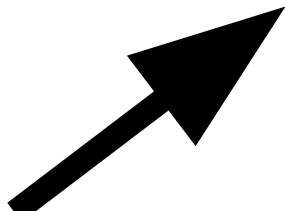
“Please issue an ESC1 certificate to me. My subject alternative name is **bob@contoso.local**”



Alice



Bob





ESC1 Cert Template



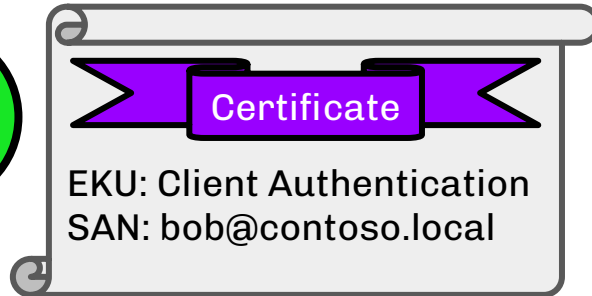
Enterprise CA



Domain Controller



Alice



Bob



ESC1 Cert Template



Enterprise CA

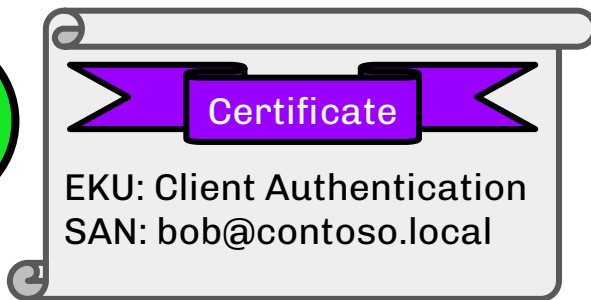


Domain Controller

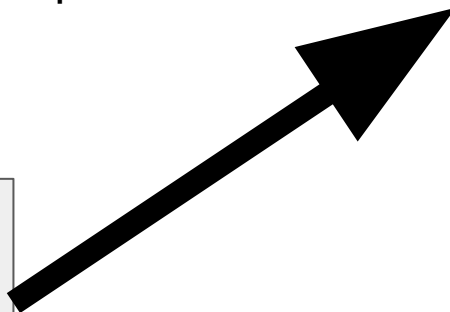
“Please issue a TGT to me for **bob@contoso.local**. This certificate will serve as my credential for that user.”



Alice



Bob

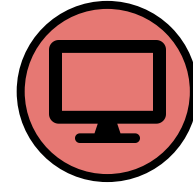




ESC1 Cert Template



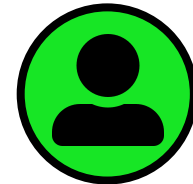
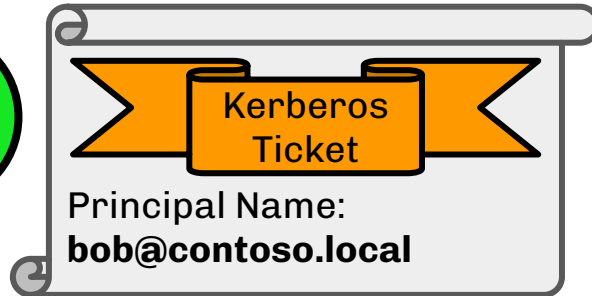
Enterprise CA



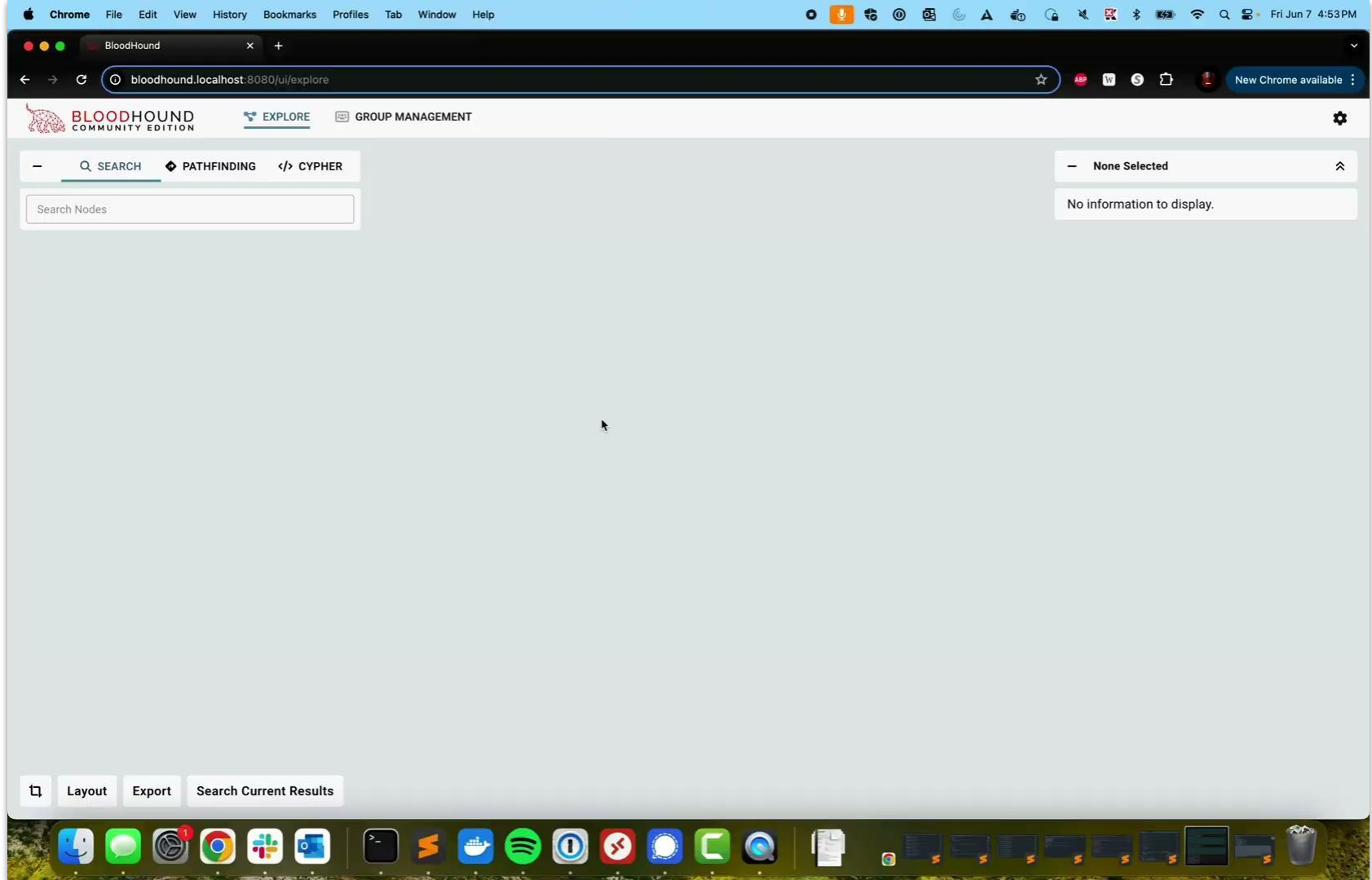
Domain Controller



Alice

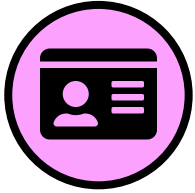


Bob



# Agenda

- How we model ADCS in BloodHound
- **ADCS Attack Path discovery and execution**
  - ESC1
  - **ESC3**
  - ESC4
- Remediation Strategies and Practical Examples
- Conclusion



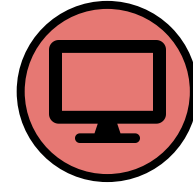
EnrollmentAgent



User



Enterprise CA



Domain Controller

## ESC3 - Abuse of Enrollment Agent Permissions



Alice



Bob



EnrollmentAgent



User



Enterprise CA



Domain Controller

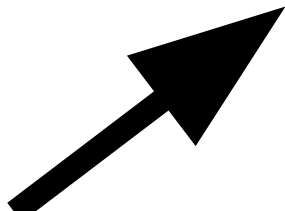
"Please issue an EnrollmentAgent  
certificate to me."



Alice



Bob





EnrollmentAgent



User



Enterprise CA



Domain Controller



Alice



Bob



EnrollmentAgent



User



Enterprise CA



Domain Controller

"Please issue an User certificate  
on behalf of **Bob**."



Alice



Bob



EnrollmentAgent



User



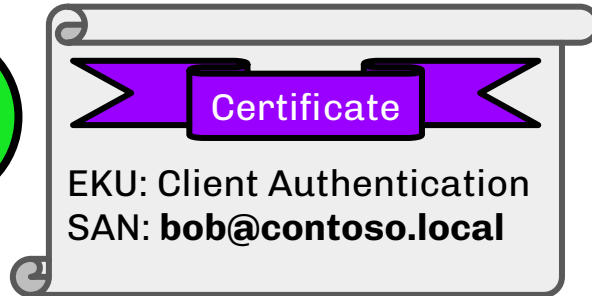
Enterprise CA



Domain Controller



Alice



Bob



EnrollmentAgent



User



Enterprise CA

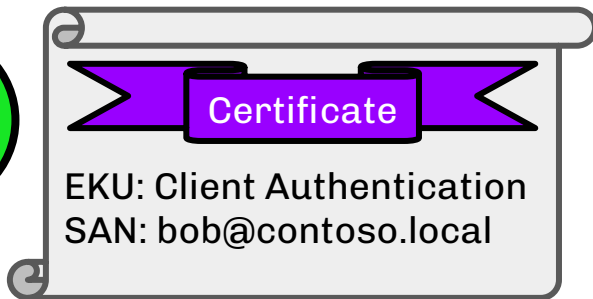


Domain Controller

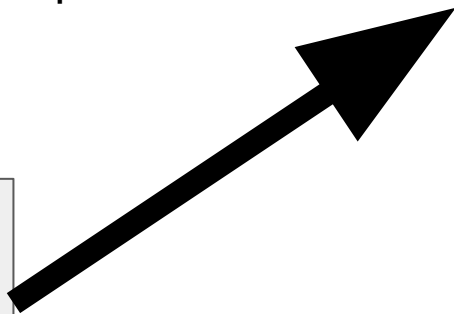
“Please issue a TGT to me for **bob@contoso.local**. This certificate will serve as my credential for that user.”



Alice



Bob





EnrollmentAgent



User



Enterprise CA



Domain Controller



Alice

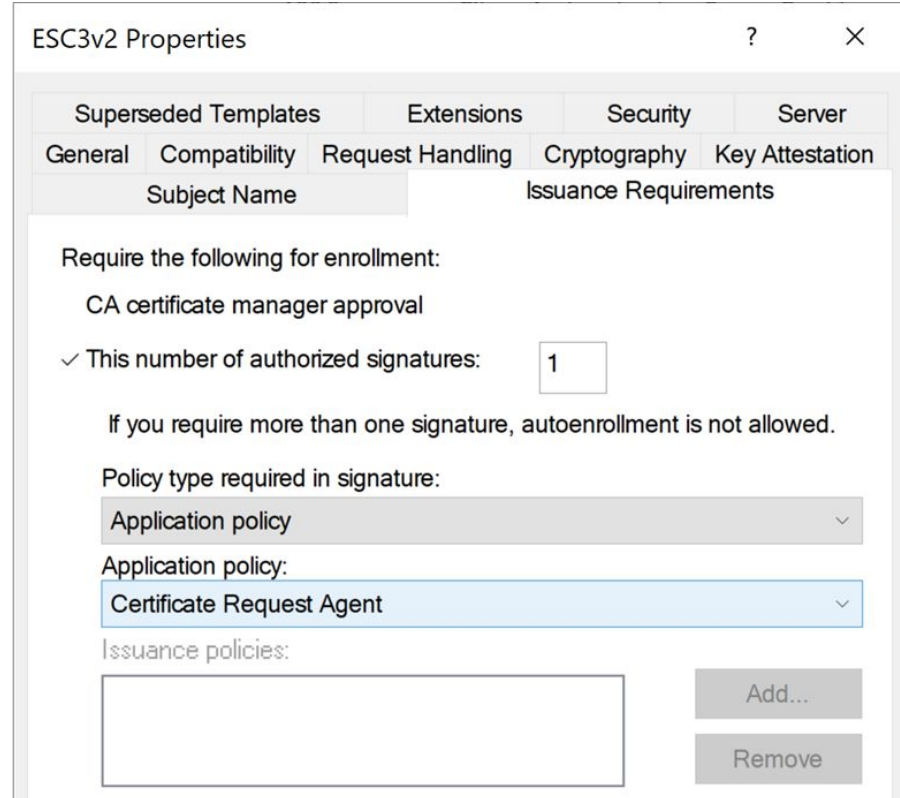


Bob

# ESC3 - What is an Enrollment Agent

- *Certificate Request Agent* EKU (1.3.6.1.4.1.311.20.2.1) → Enrollment Agent
- Can enroll on behalf of other principals in templates:
  - Schema version 1
  - Schema version 2+ with the Certificate Request Agent EKU required as Application Policy

<https://posts.specterops.io/adcs-attack-paths-in-bloodhound-part-2-ac7f925d1547>



ESC3v2 Properties

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Require the following for enrollment:

CA certificate manager approval

✓ This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy

Application policy:

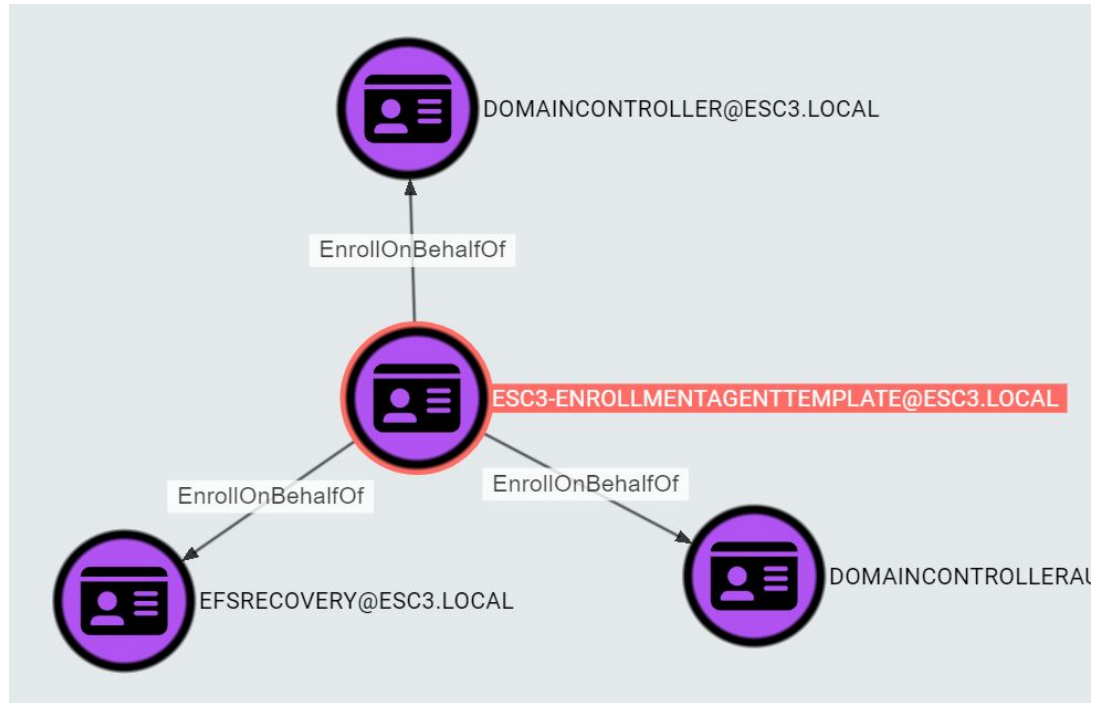
Certificate Request Agent

Issuance policies:

Add...

Remove

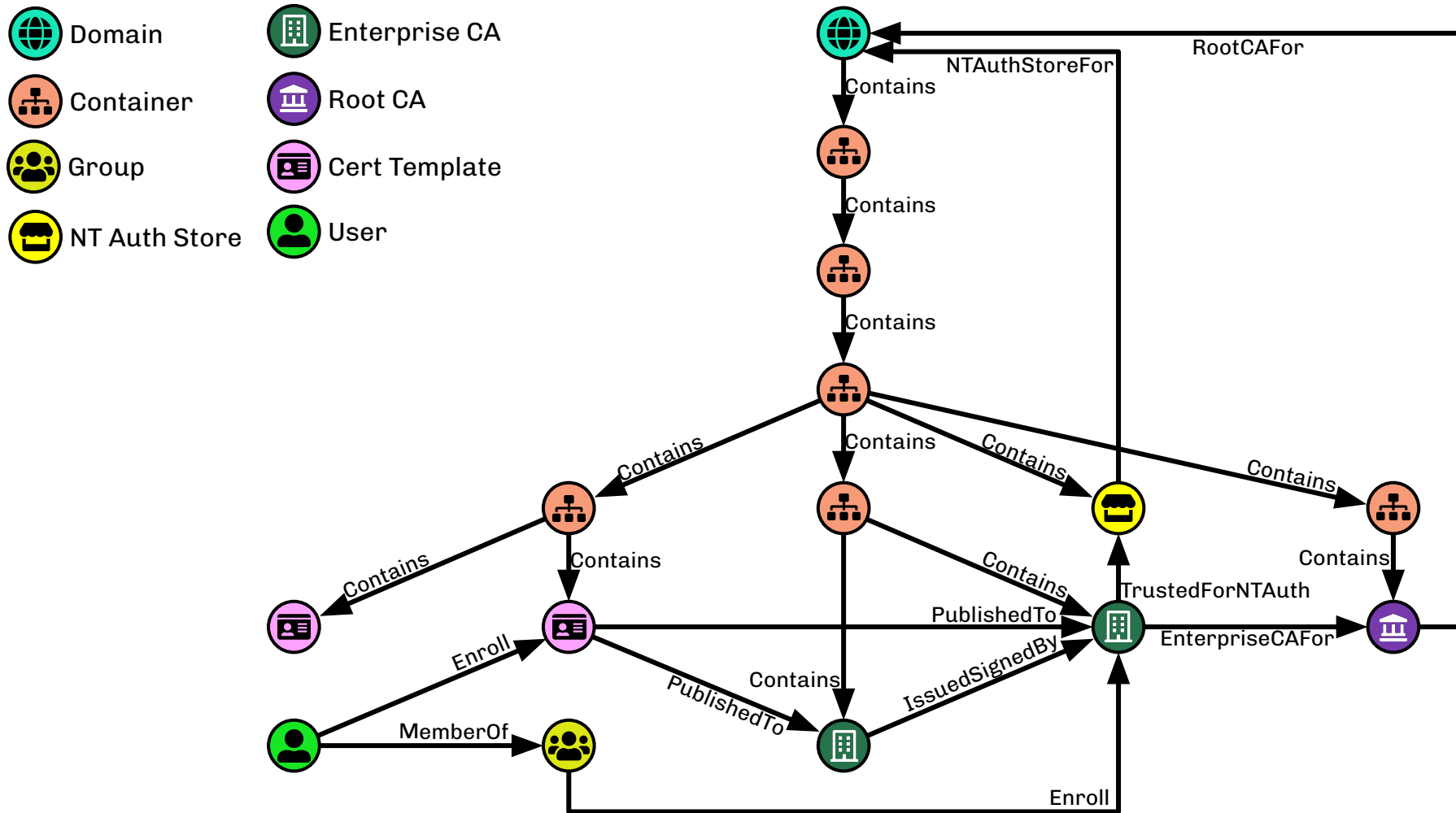
# ESC3 - Enrollment Agents in BloodHound



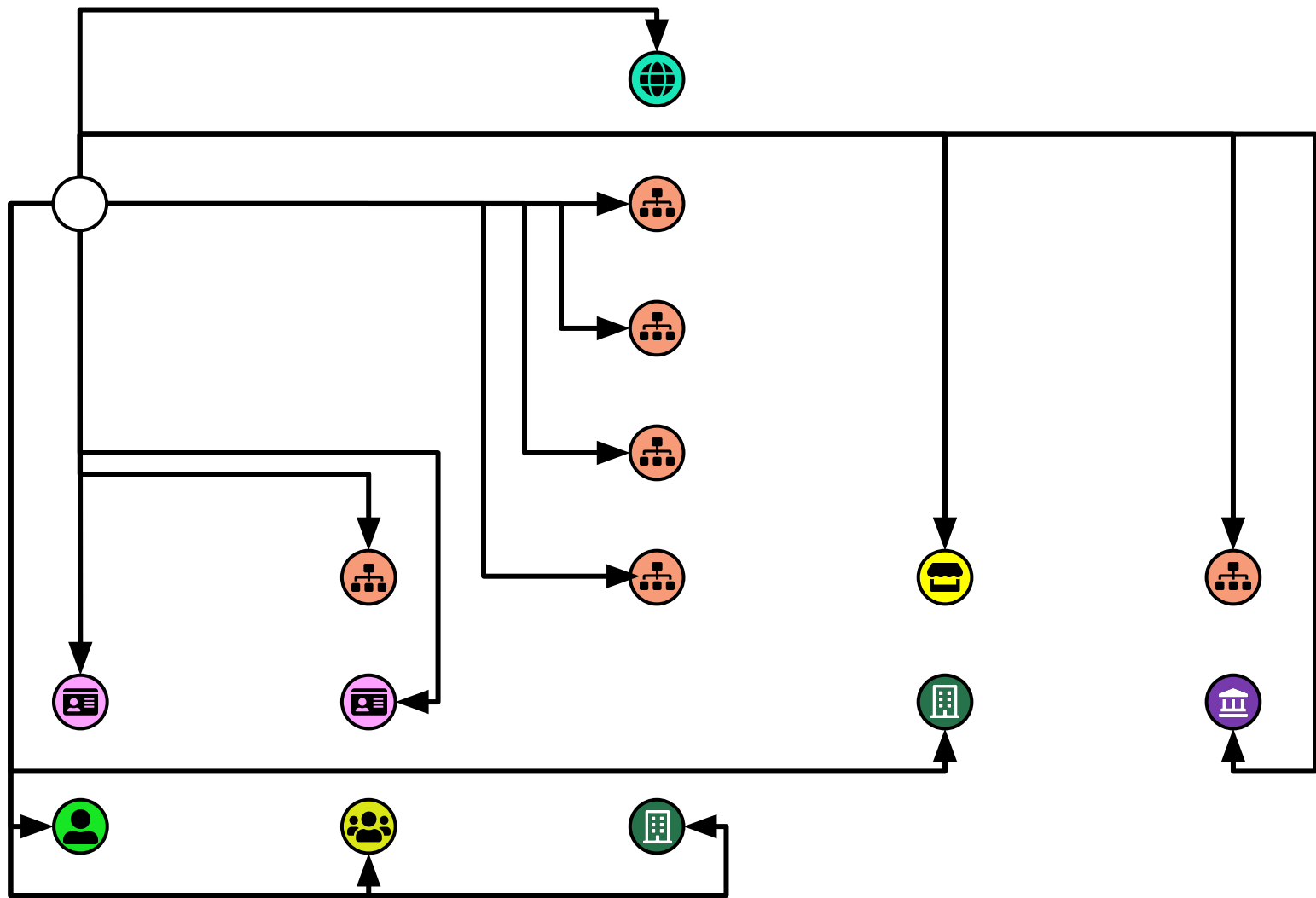


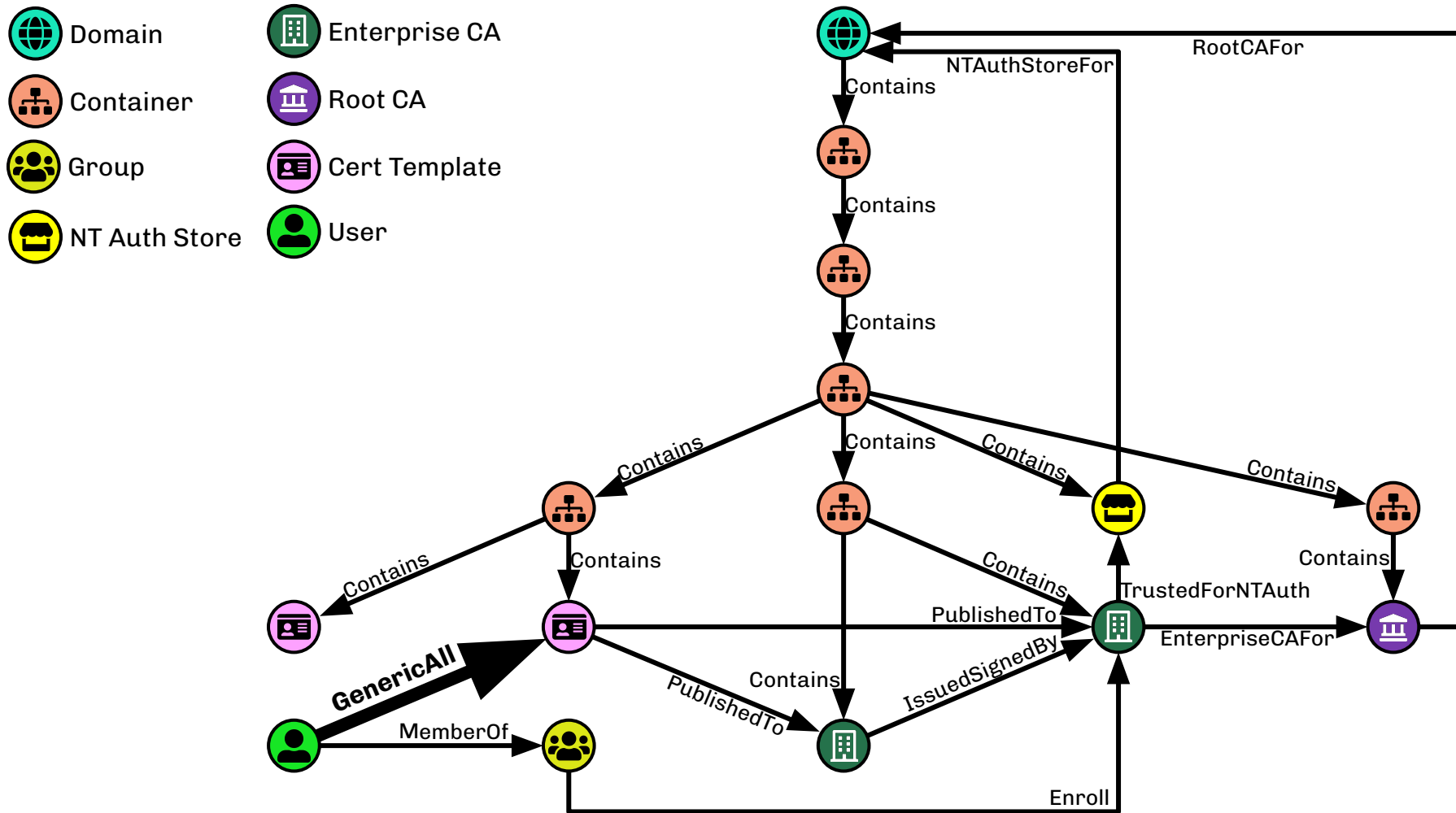
# Agenda

- How we model ADCS in BloodHound
- **ADCS Attack Path discovery and execution**
  - ESC1
  - ESC3
  - **ESC4**
- Remediation Strategies and Practical Examples
- Conclusion










**“That wouldn’t happen  
in the real world”**


“That wouldn’t happen  
in the real world”

**WRONG**

—

Q SEARCH

 PATHFINDING

 CYPHER

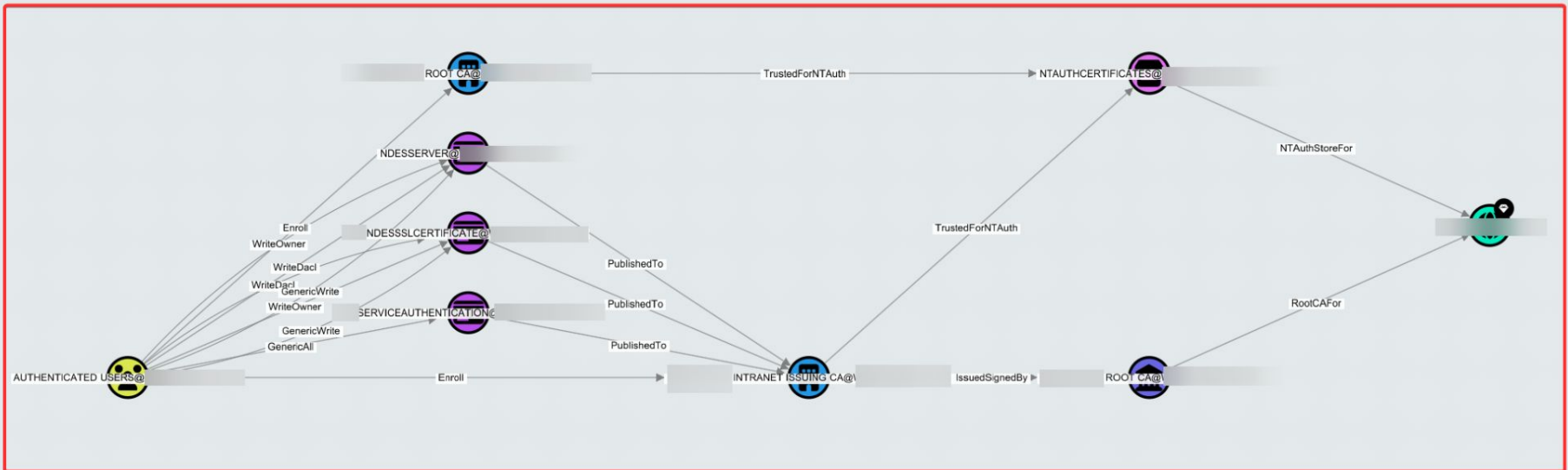
AUTHENTICATED USERS@

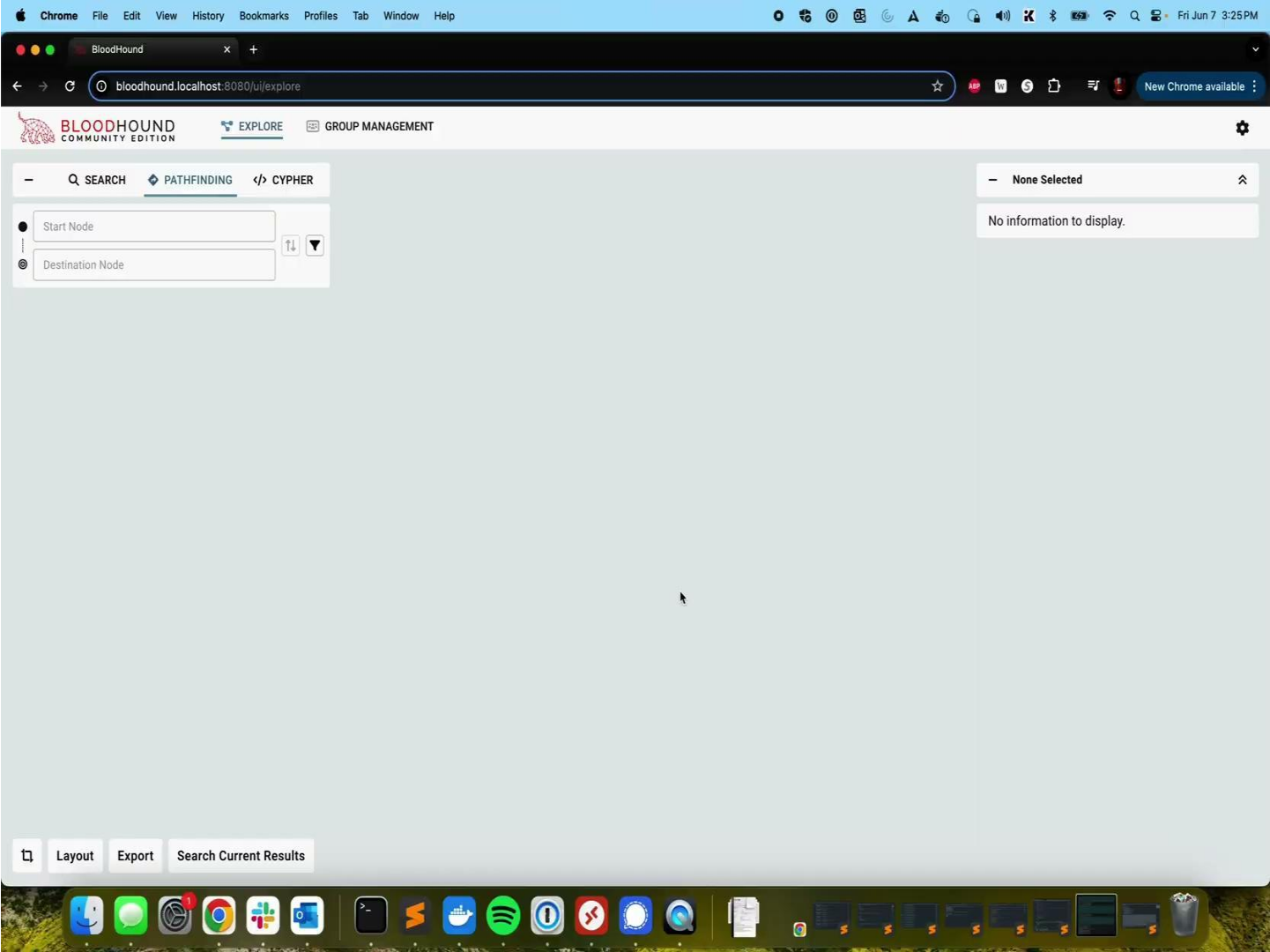
↕

▼

+ ADCSESC4

⌵








# Agenda

- How we model ADCS in BloodHound
- ADCS Attack Path discovery and execution
- **Remediation Strategies and Practical Examples**
- Conclusion


# Find non-Tier Zero principals with ADCSESCx edges

 **BLOODHOUND**  
COMMUNITY EDITION

 [EXPLORE](#)  [GROUP MANAGEMENT](#)

— [Q SEARCH](#) [◆ PATHFINDING](#) [</> CYPHER](#)

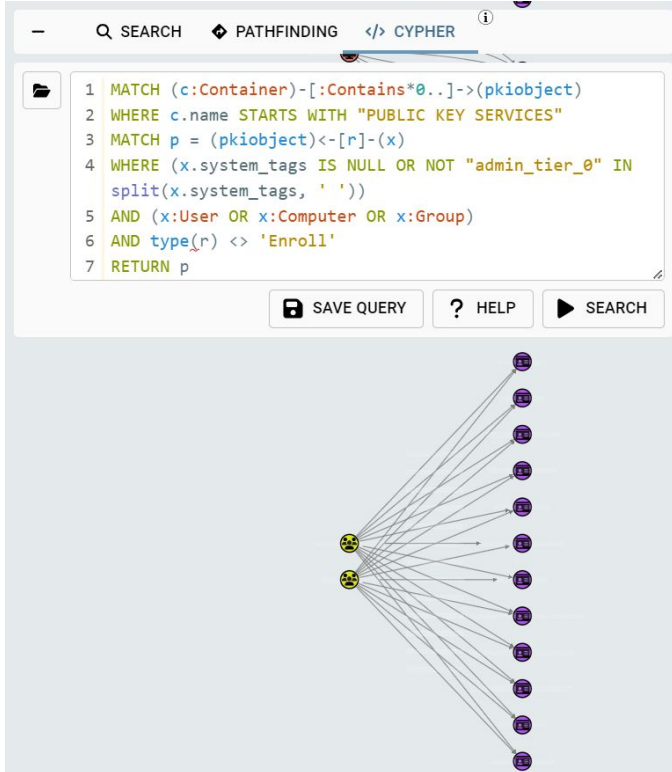
```
1 MATCH p = (n)-  
[:ADCSESC1|ADCSESC3|ADCSESC4|ADCSESC6a|ADCSESC6b|ADCSESC9a|ADCSESC9b|ADCSESC10a|ADCSESC10b|ADCSESC13]->(m)  
2 WHERE "admin_tier_0" IN split(m.system_tags, ' ')  
3 AND (n.system_tags IS NULL OR NOT "admin_tier_0" IN  
split(n.system_tags, ' '))  
4 RETURN p
```

 [SAVE QUERY](#) [? HELP](#) [▶ SEARCH](#)



```
MATCH p =  
(n) - [ :ADCSESC1|ADCSESC3|ADCSESC4|ADCSESC6a|ADCSESC6b|ADCSESC9a|ADCSESC9b|ADCSESC10a|ADCSESC10b|ADCSESC13] -> (m)  
WHERE "admin_tier_0" IN split(m.system_tags, ' ')  
AND (n.system_tags IS NULL OR NOT "admin_tier_0" IN split(n.system_tags, ' '))  
RETURN p
```

# Find non-Tier Zero principals with ADCS permissions



The screenshot shows a Cypher query editor interface. The query is as follows:

```
1 MATCH (c:Container)-[:Contains*0..]->(pkiobject)
2 WHERE c.name STARTS WITH "PUBLIC KEY SERVICES"
3 MATCH p = (pkiobject)<-[r]-(x)
4 WHERE (x.system_tags IS NULL OR NOT "admin_tier_0" IN
   split(x.system_tags, ' '))
5 AND (x:User OR x:Computer OR x:Group)
6 AND type(r) <> 'Enroll'
7 RETURN p
```

Below the query editor, there are buttons for "SAVE QUERY", "HELP", and "SEARCH". The results section displays a graph visualization with two nodes on the left (yellow icons) and a vertical column of 15 nodes on the right (purple icons). Arrows point from the left nodes to each of the right nodes.

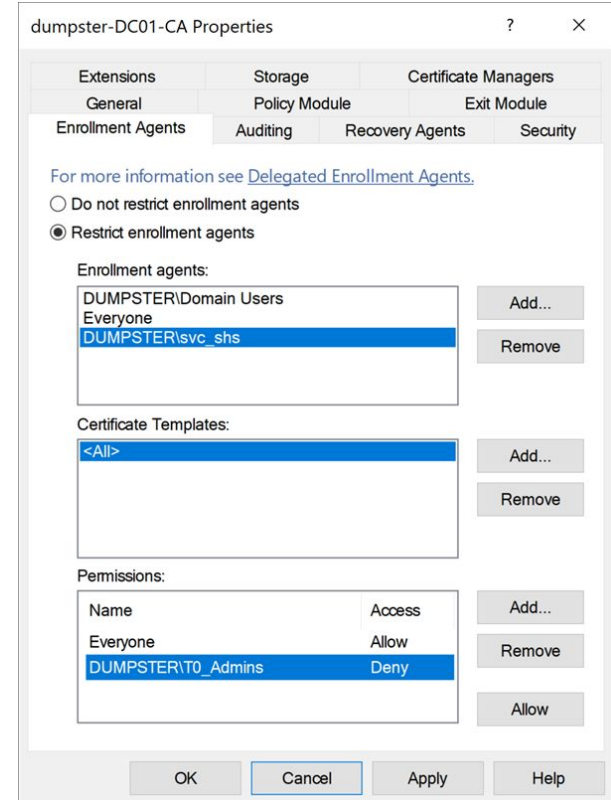
```
MATCH
(c:Container)-[:Contains*0..]->(pkiobject)
WHERE c.name STARTS WITH "PUBLIC KEY
SERVICES"
MATCH p = (pkiobject)<-[r]-(x)
WHERE (
x.system_tags IS NULL
OR NOT "admin_tier_0" IN
split(x.system_tags, ' ')
)
AND (x:User OR x:Computer OR x:Group)
AND type(r) <> 'Enroll'
RETURN p
```

# ESC1 Remediation

- ESC1: Enrollee Supplies Subject
- If you can, then either:
  - Limit enrollment rights to Tier Zero principals
  - Remove EKUs that enable domain authentication

# ESC1 Remediation

- Common scenario:  
Helpdesk (NOT Tier Zero) creates smart cards on behalf of others
- Solution: Enrollment agents - with restrictions
- Example:
  - Yubico - Setting up Smart Card Login for Enroll on Behalf of:  
<https://support.yubico.com/hc/en-us/articles/360015669119-Setting-up-Smart-Card-Login-for-Enroll-on-Behalf-of>



# ESC1 Remediation

Be careful - not all security vendors know what they are doing

## FIDO Security Keys

[Home](#) [Products](#) [Guides](#) [Compatible Service Catalog](#) [FAQ](#)

6. Under the **Security** tab, be sure the **Read** and **Enroll** ability is set for the user or group of users who will be setting up the smart cards for logon. The admin group is same as auto-enrollment settings.

Authenticated Users



Subject Name	Server	Issuance Requirements
Compatibility	General	Request Handling
Superseded Templates	Extensions	Cryptography
		Key Attestation
		Security

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (TEST\Domain Admins)
- Domain Users (TEST\Domain Users)
- Enterprise Admins (TEST\Enterprise Admins)

Add... Remove

Permissions for Authenticated Users	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced. Advanced

Enroll



(on agent template)



# Agenda

- How we model ADCS in BloodHound
- ADCS Attack Path discovery and execution
- Remediation Strategies and Practical Examples
- **Conclusion**

# Conclusion

- ADCS attack paths are highly complex
- BloodHound dramatically simplifies ADCS attack path discovery
- BloodHound CE is free and open source software:
  - <https://github.com/SpecterOps/BloodHound>
- Join us in the BloodHound Slack:
  - <https://ghst.ly/BHSlack>