SPECTEROPS

Defending Against ADCS Domain Escalation Techniques

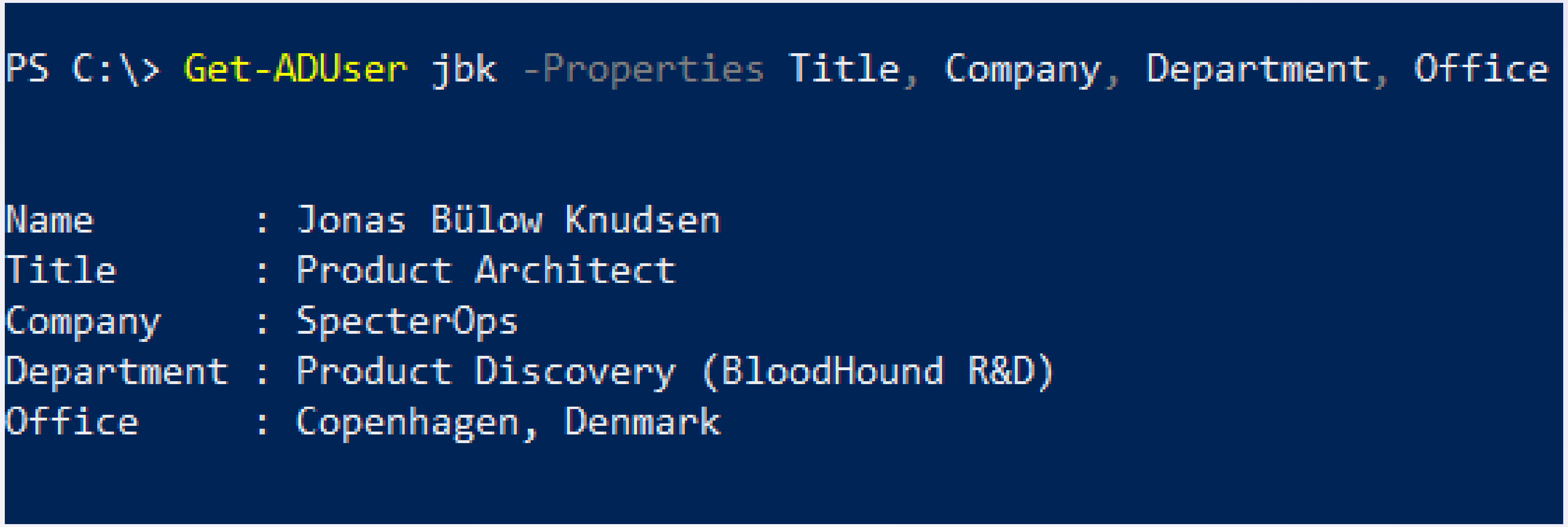
Span Cyber Security Arena – Nov, 2024

Jonas Bülow Knudsen

Agenda

- ADCS introduction
- ADCS domain escalation techniques
- Auditing and remediation

Whoami



```
PS C:\> Get-ADUser jbk -Properties Title, Company, Department, Office


Name       : Jonas Bülow Knudsen
Title      : Product Architect
Company    : SpecterOps
Department : Product Discovery (BloodHound R&D)
Office     : Copenhagen, Denmark
```

@Jonas_B_K

@JonasBK

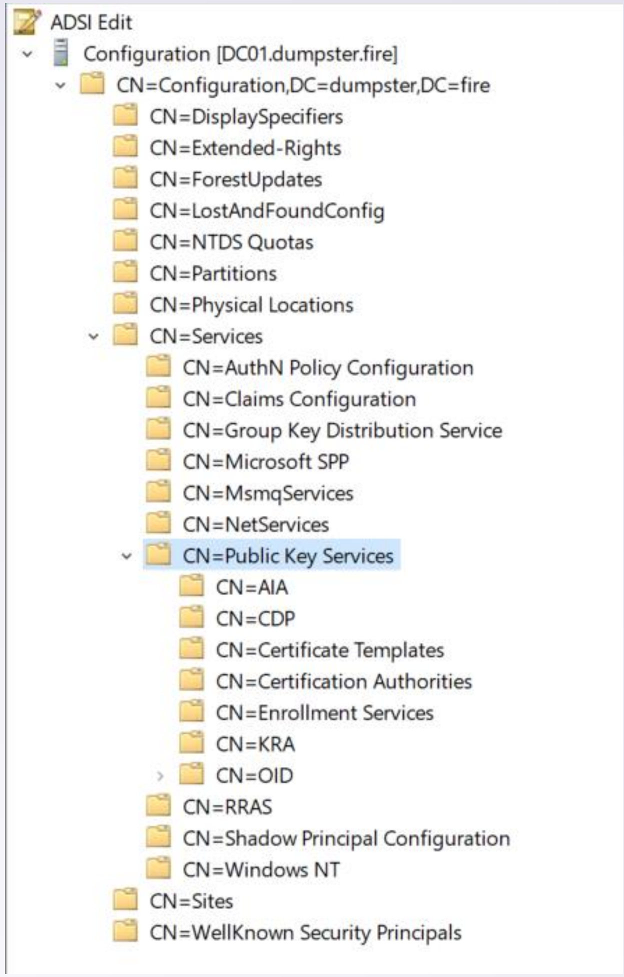
@Jonas-BK

ADCS introduction

Active Directory Certificate Services (ADCS)

ADCS introduction

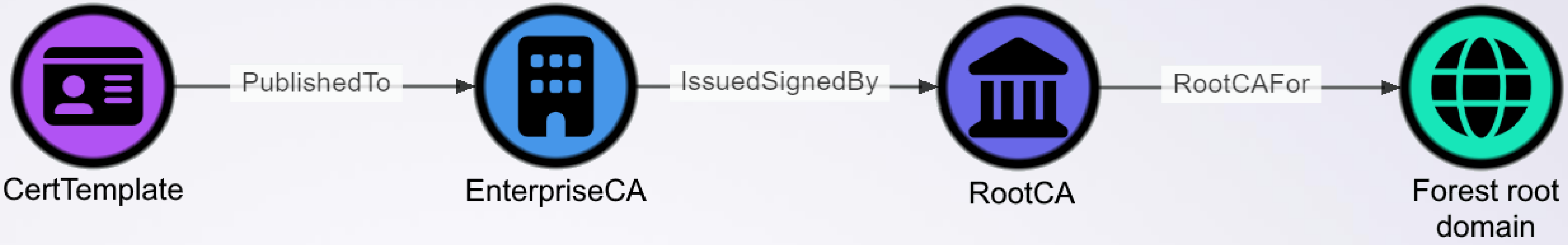
- Scalable Public Key Infrastructure (PKI)
- Issuing and managing digital certificates
- Public Key Services container



```
ADSI Edit
  Configuration [DC01.dumpster.fire]
    CN=Configuration,DC=dumpster,DC=fire
      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
        CN=RRAS
        CN=Shadow Principal Configuration
        CN=Windows NT
      CN=Sites
      CN=WellKnown Security Principals
```

ADCS components

ADCS introduction



ADCS domain escalation techniques

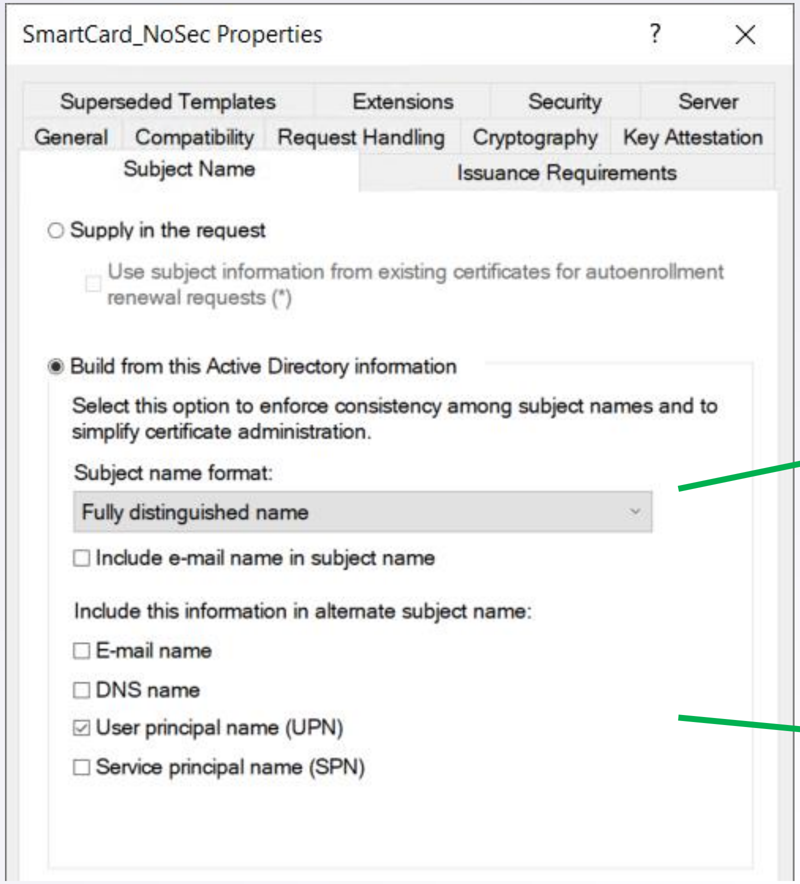
Background

ADCS domain escalation techniques

- 2021: Certified Pre-Owned ADCS whitepaper
    - Eight domain escalation techniques (ESC1 - ESC8)
- Since then
    - Almost guaranteed attack path to full domain compromise
    - More escalation techniques (ESC9 - ESC15)
    - Limited security improvements from Microsoft

Subject Name and Subject Alternative Name (SAN)

ADCS domain escalation techniques



SmartCard_NoSec Properties

○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

□ Include e-mail name in subject name

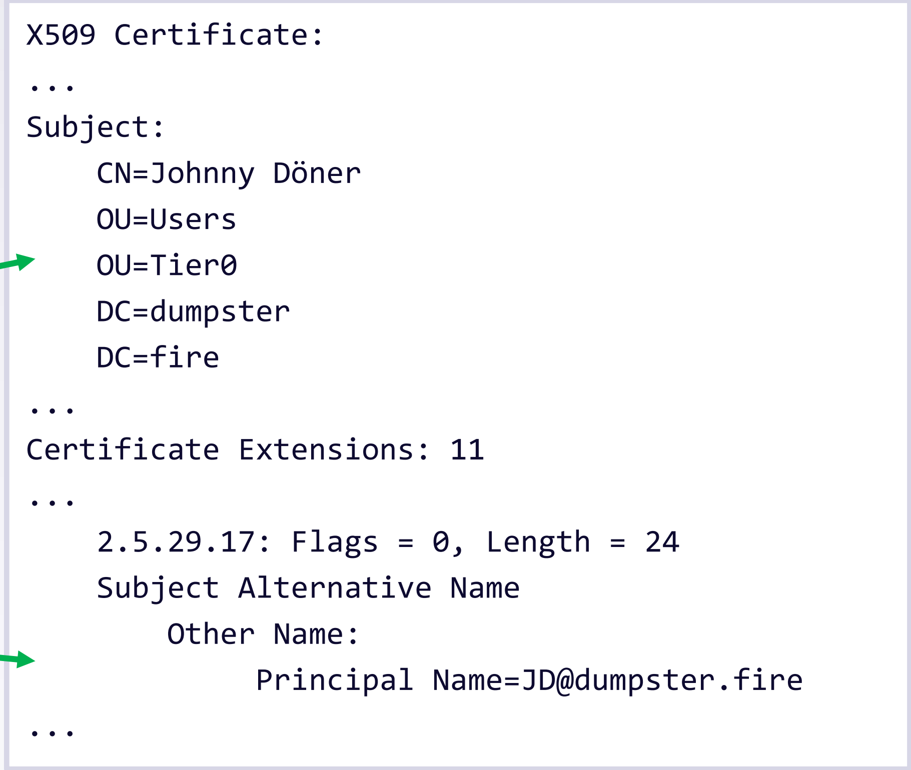
Include this information in alternate subject name:

□ E-mail name

□ DNS name

☑ User principal name (UPN)

□ Service principal name (SPN)

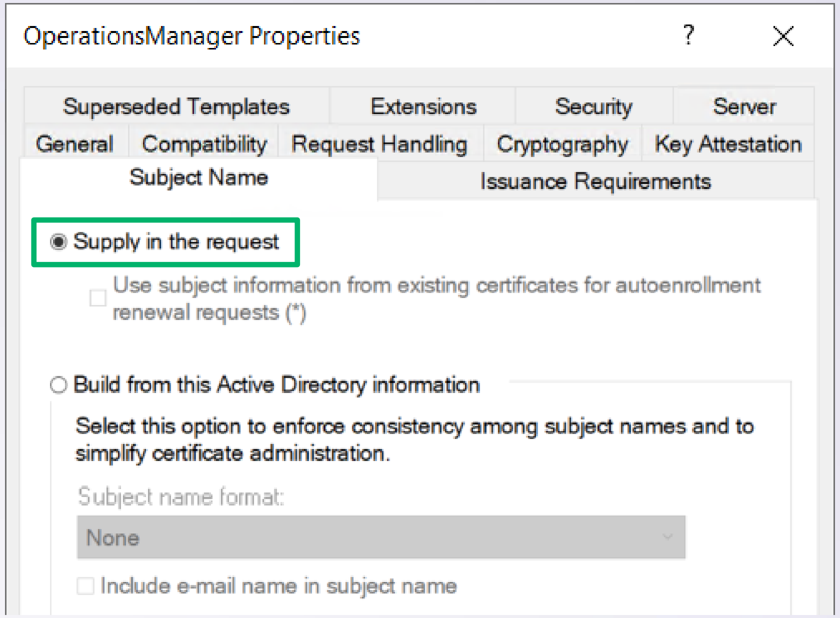


```
X509 Certificate:
...
Subject:
    CN=Johnny Döner
    OU=Users
    OU=Tier0
    DC=dumpster
    DC=fire
...
Certificate Extensions: 11
...
    2.5.29.17: Flags = 0, Length = 24
    Subject Alternative Name
        Other Name:
             Principal Name=JD@dumpster.fire
...
```

ESC1 Enrollee Supplies Subject

ADCS domain escalation techniques

- Special flag: `ENROLLEE_SUPPLIES_SUBJECT`
- Specify the certificate Subject Name and SAN in the request
- Enroll certificates as anyone 🔥



OperationsManager Properties

● Supply in the request

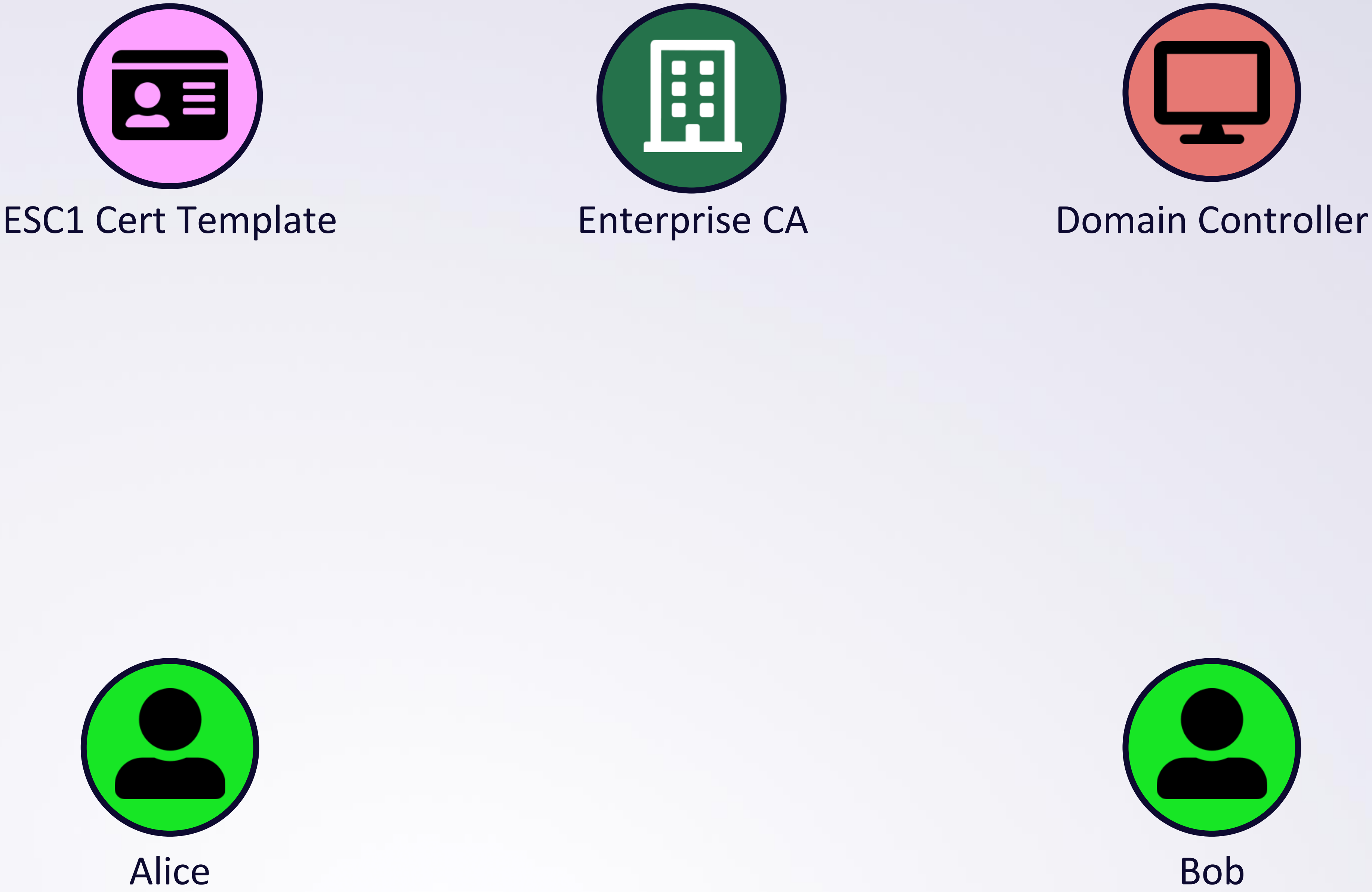
□ Use subject information from existing certificates for autoenrollment renewal requests (*)

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: None

□ Include e-mail name in subject name



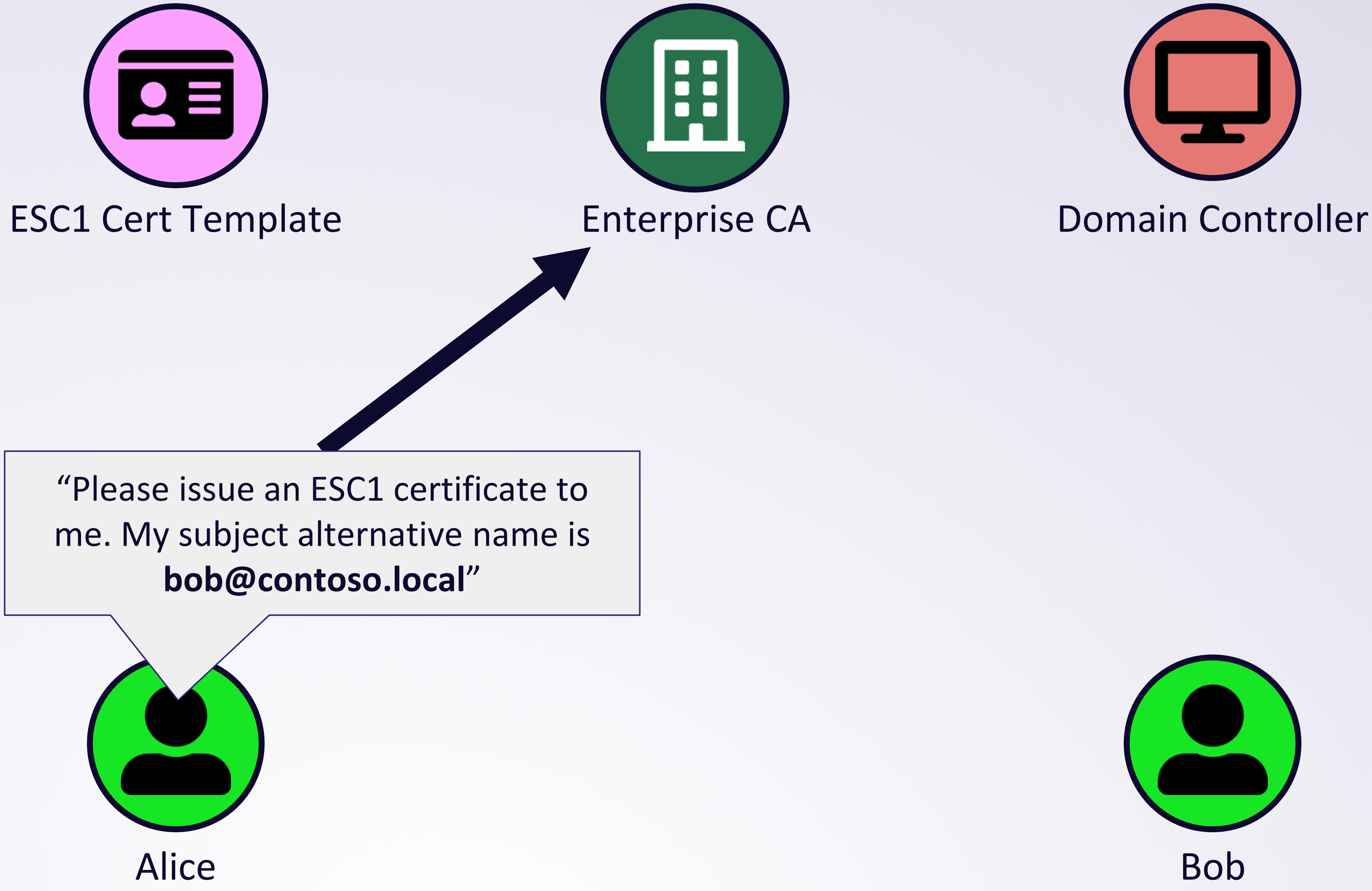
ESC1 Cert Template

Enterprise CA

Domain Controller

Alice

Bob



ESC1 Cert Template

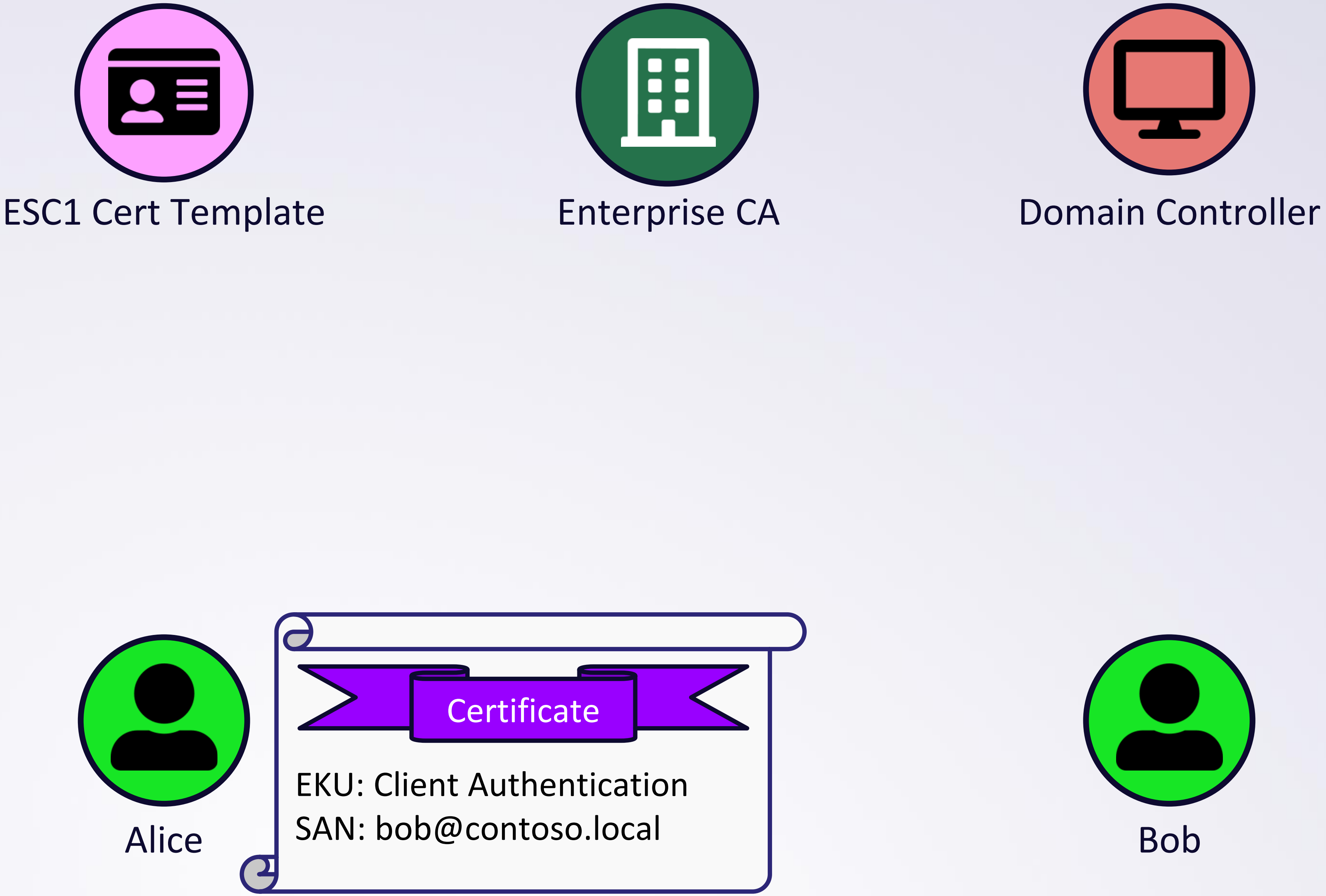
Enterprise CA

Domain Controller

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

Alice

Bob



ESC1 Cert Template

Enterprise CA

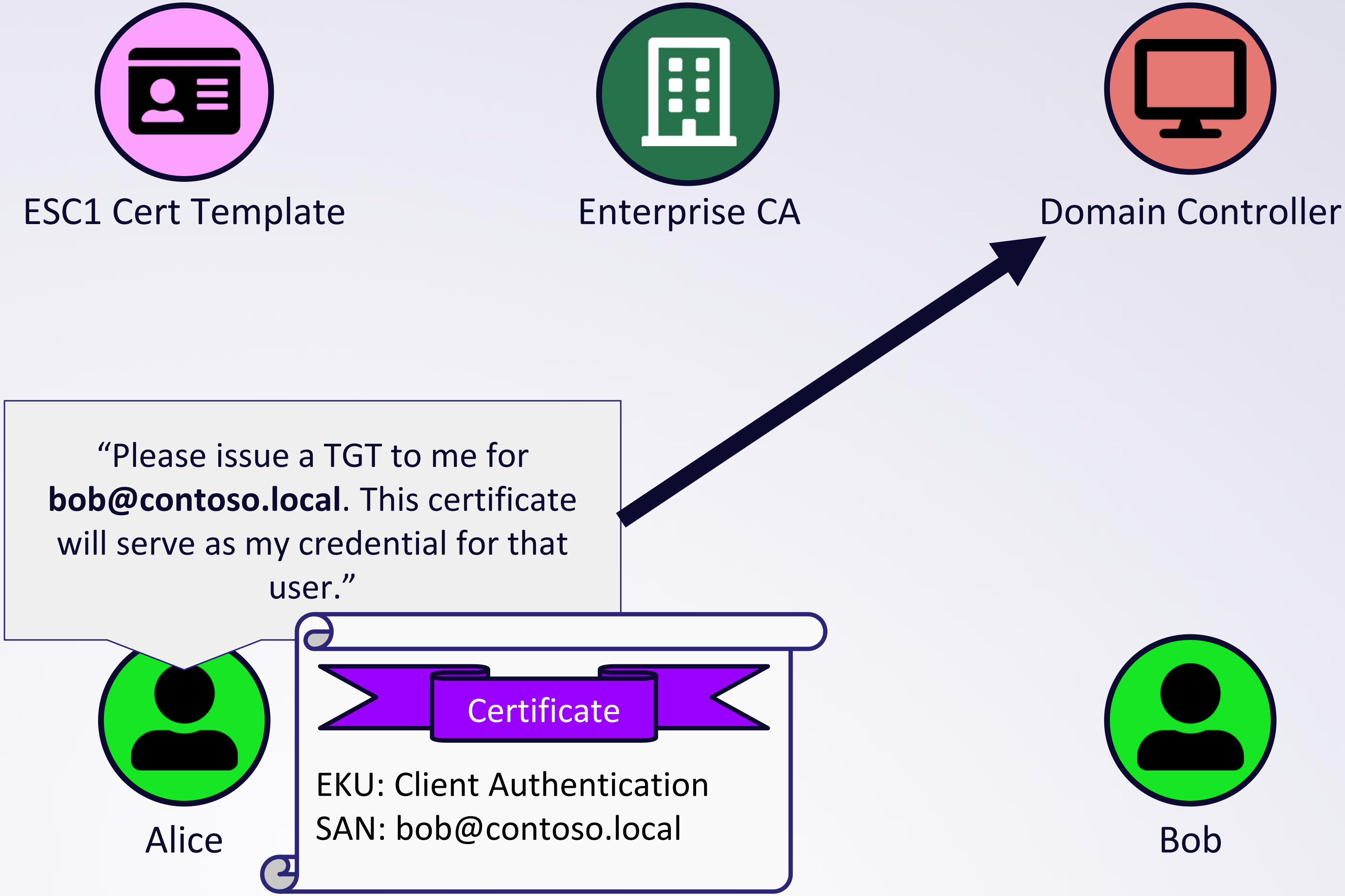
Domain Controller

Alice

Certificate

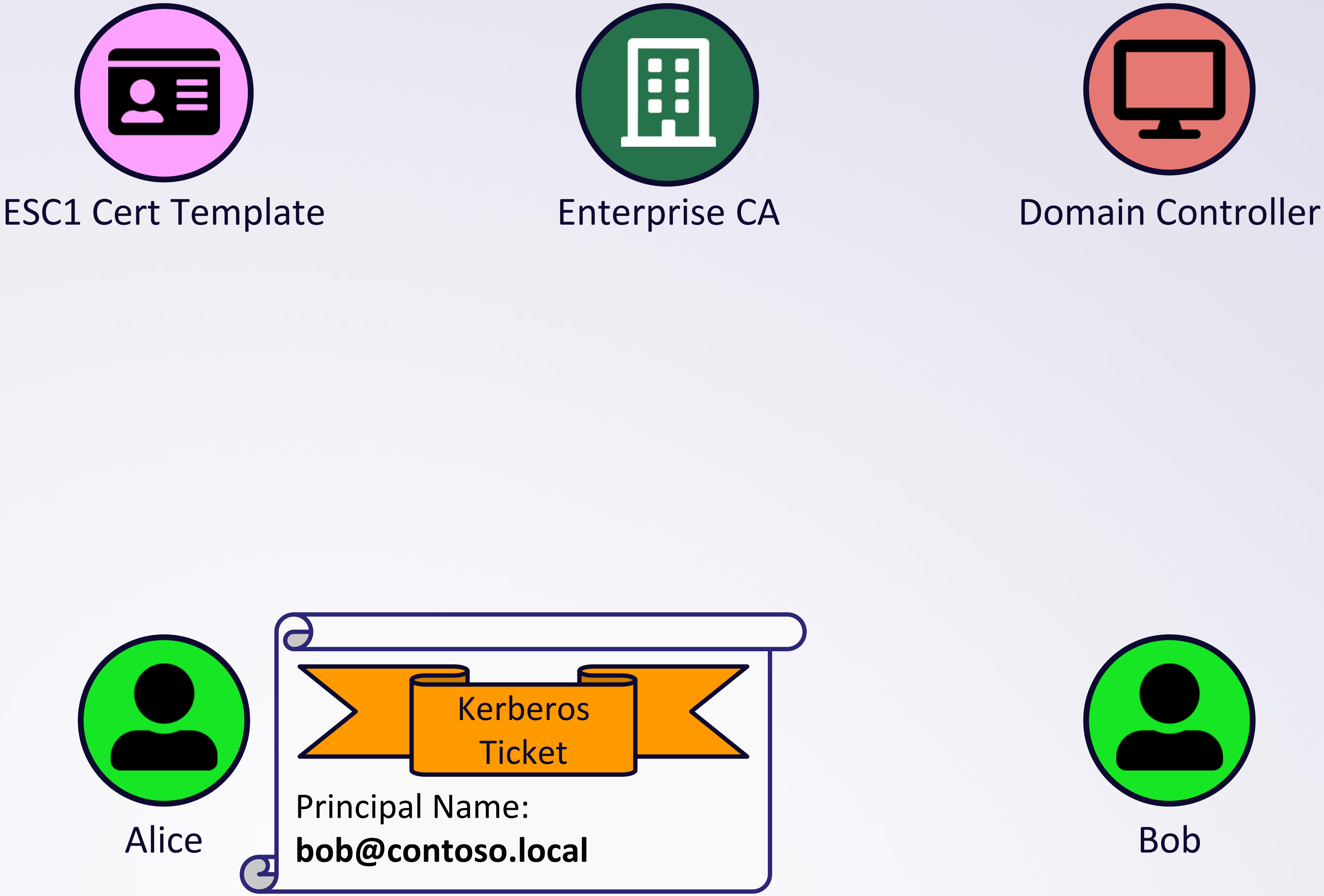
EKU: Client Authentication
SAN: bob@contoso.local

Bob



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

EKU: Client Authentication
SAN: bob@contoso.local



ESC1 Cert Template

Enterprise CA

Domain Controller

Alice

Kerberos Ticket

Principal Name:
bob@contoso.local

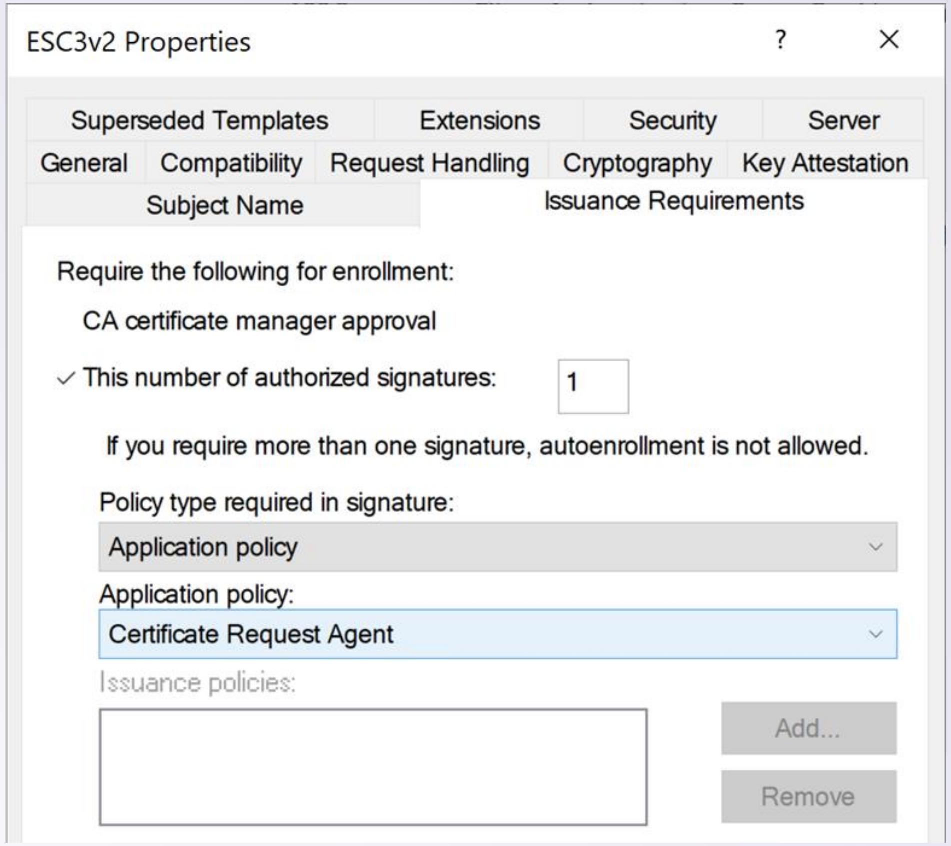
Bob

BloodHound ESC1 demo by Andy Robbins: https://drive.google.com/file/d/1N45L48ZFe0L4vqZGKvoX2nMBP1ohkw-r/view?usp=drive_link

ESC3 – Another impersonation abuse

ADCS domain escalation techniques

- Certificate Request Agent EKU → 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



Require the following for enrollment:

CA certificate manager approval

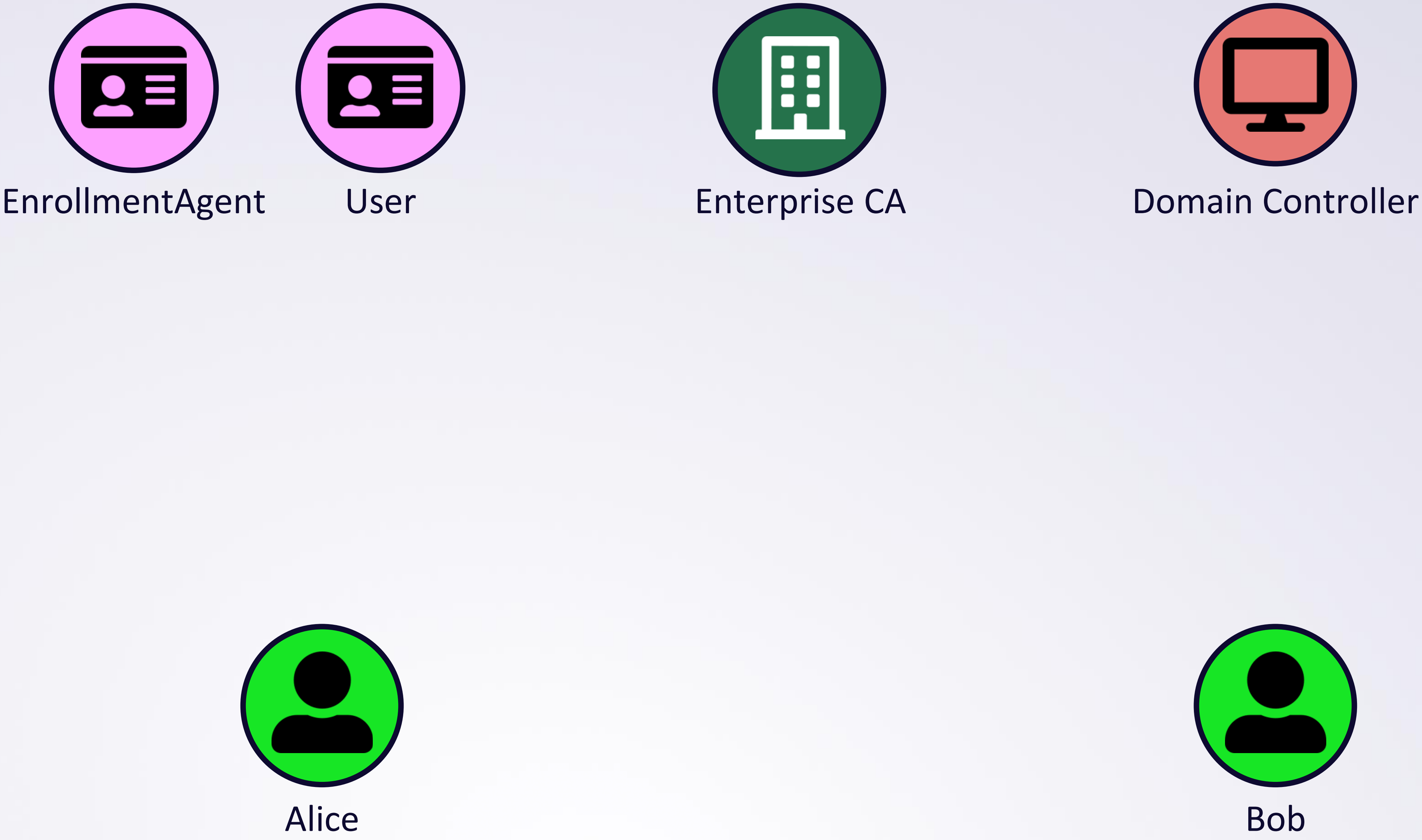
✓ This number of authorized signatures: 1

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:



EnrollmentAgent

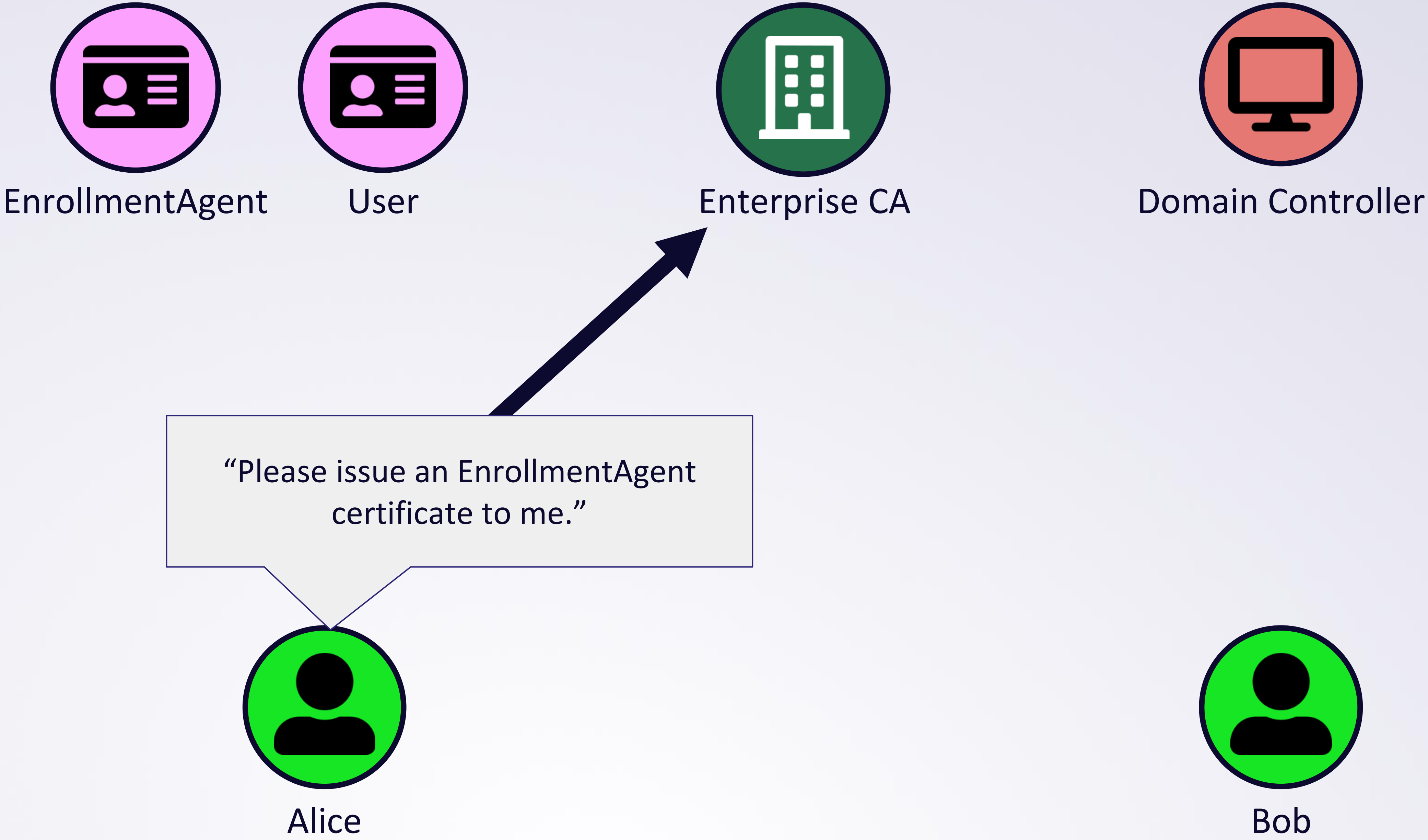
User

Enterprise CA

Domain Controller

Alice

Bob



EnrollmentAgent

User

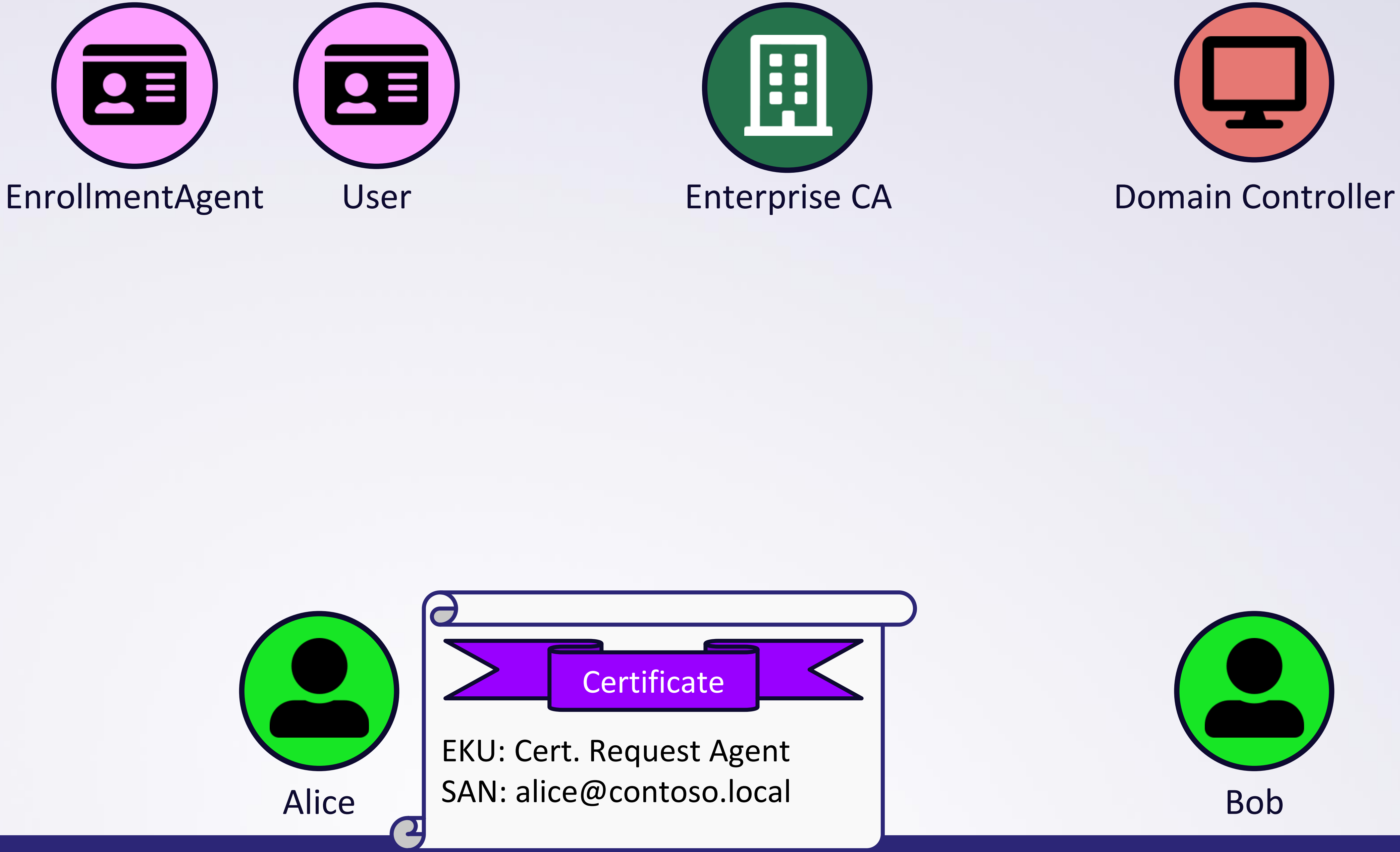
Enterprise CA

Domain Controller

“Please issue an EnrollmentAgent certificate to me.”

Alice

Bob



EnrollmentAgent

User

Enterprise CA

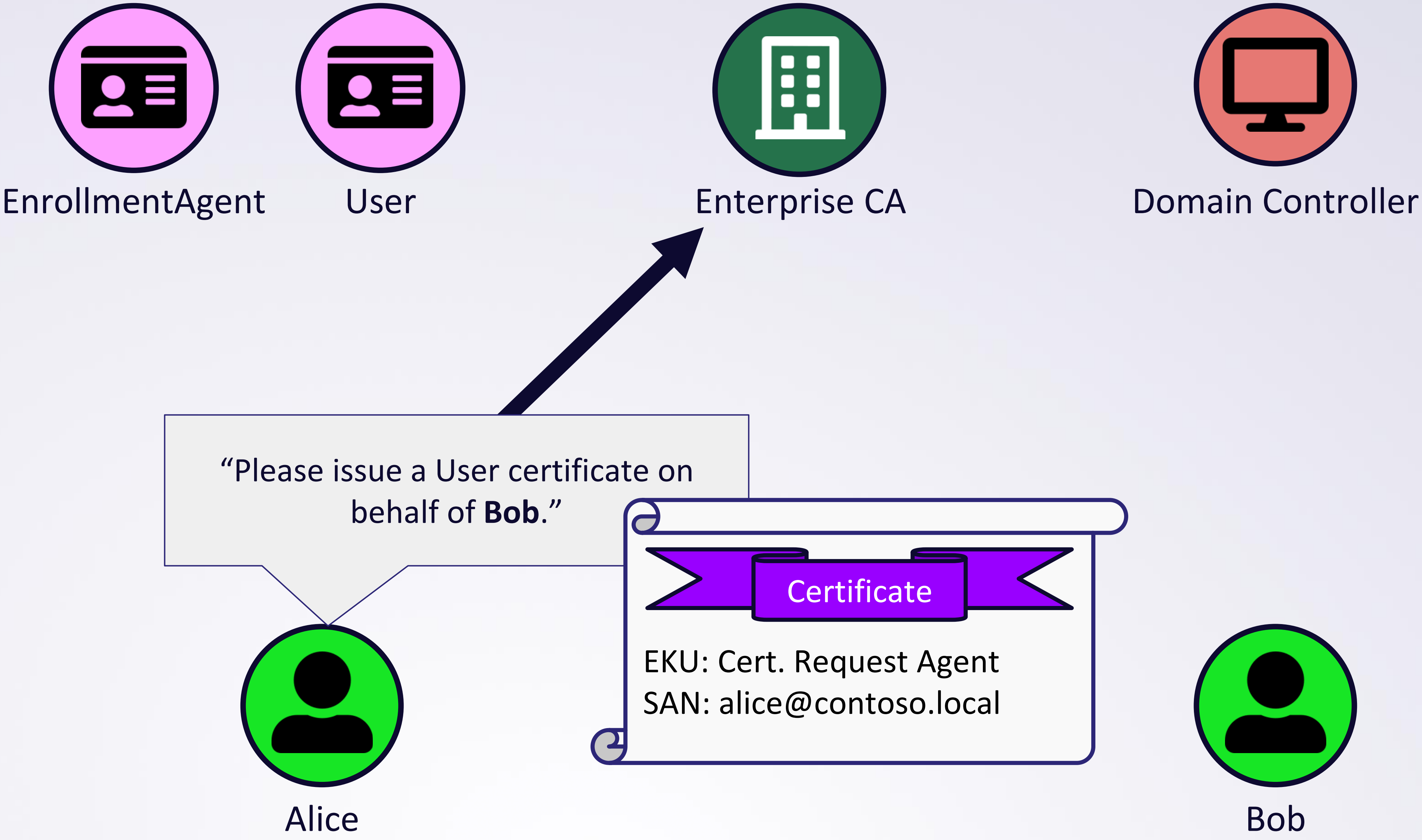
Domain Controller

Alice

Certificate

EKU: Cert. Request Agent
SAN: alice@contoso.local

Bob



EnrollmentAgent

User

Enterprise CA

Domain Controller

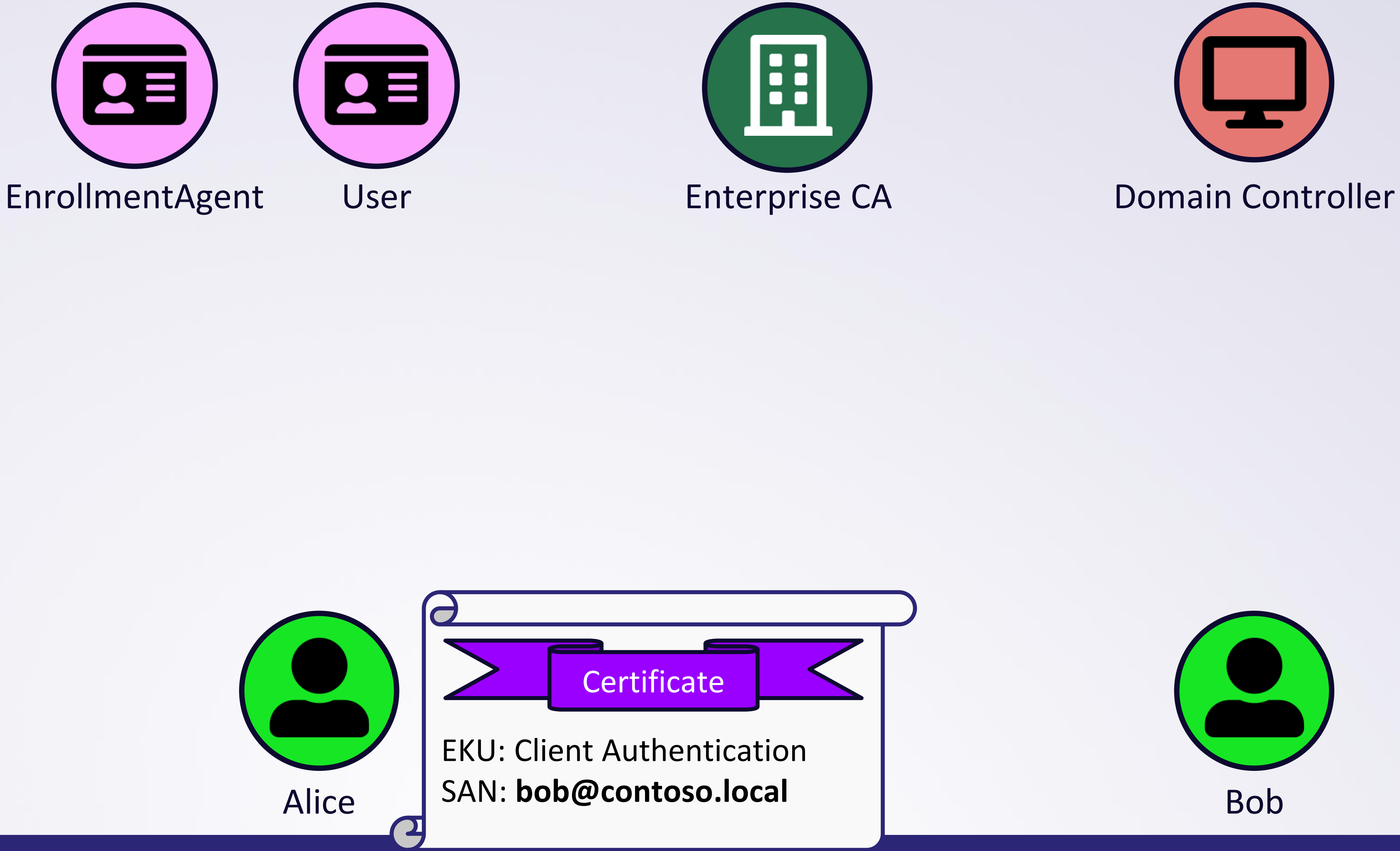
“Please issue a User certificate on behalf of **Bob**.”

Certificate

EKU: Cert. Request Agent
SAN: alice@contoso.local

Alice

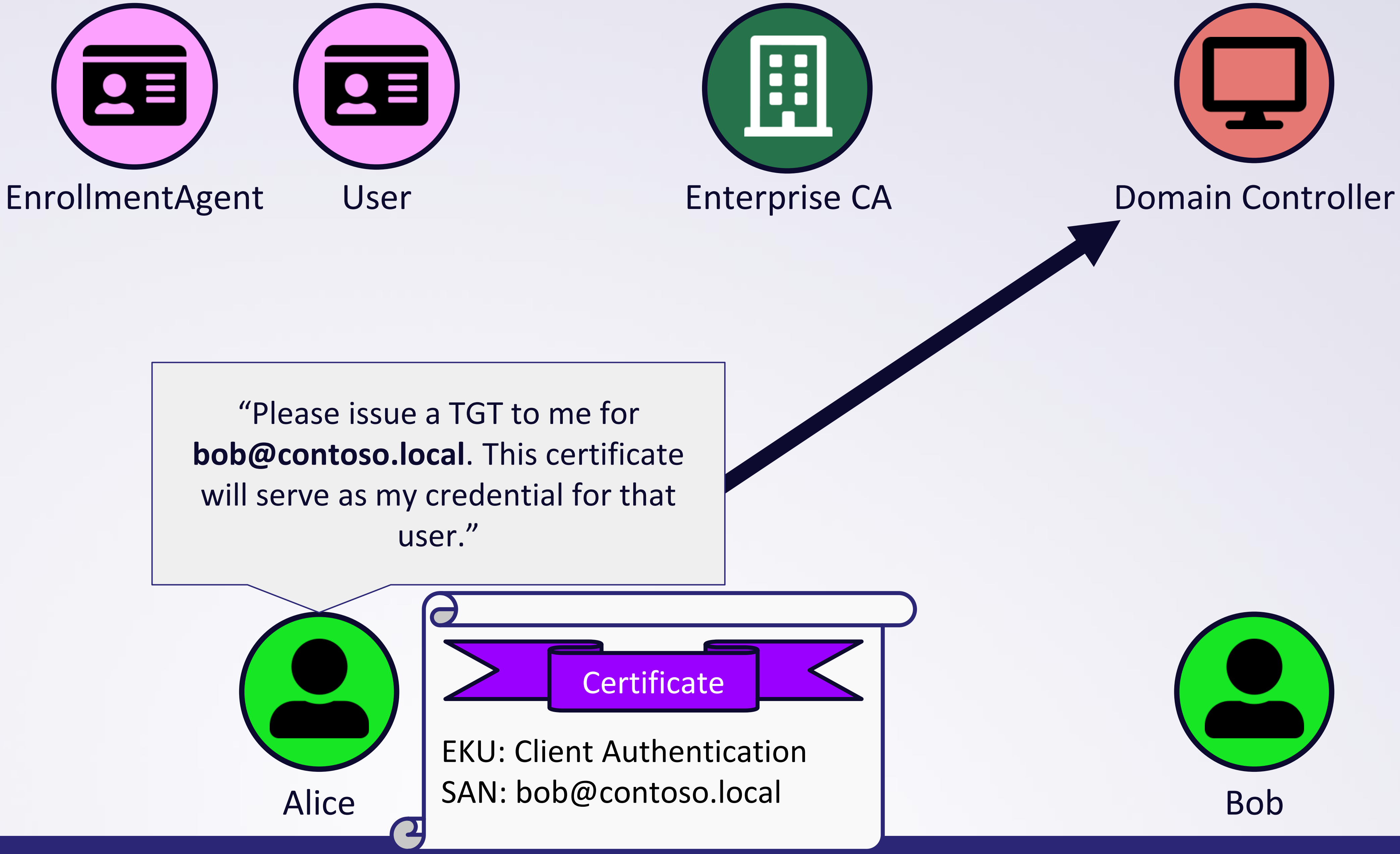
Bob



Certificate

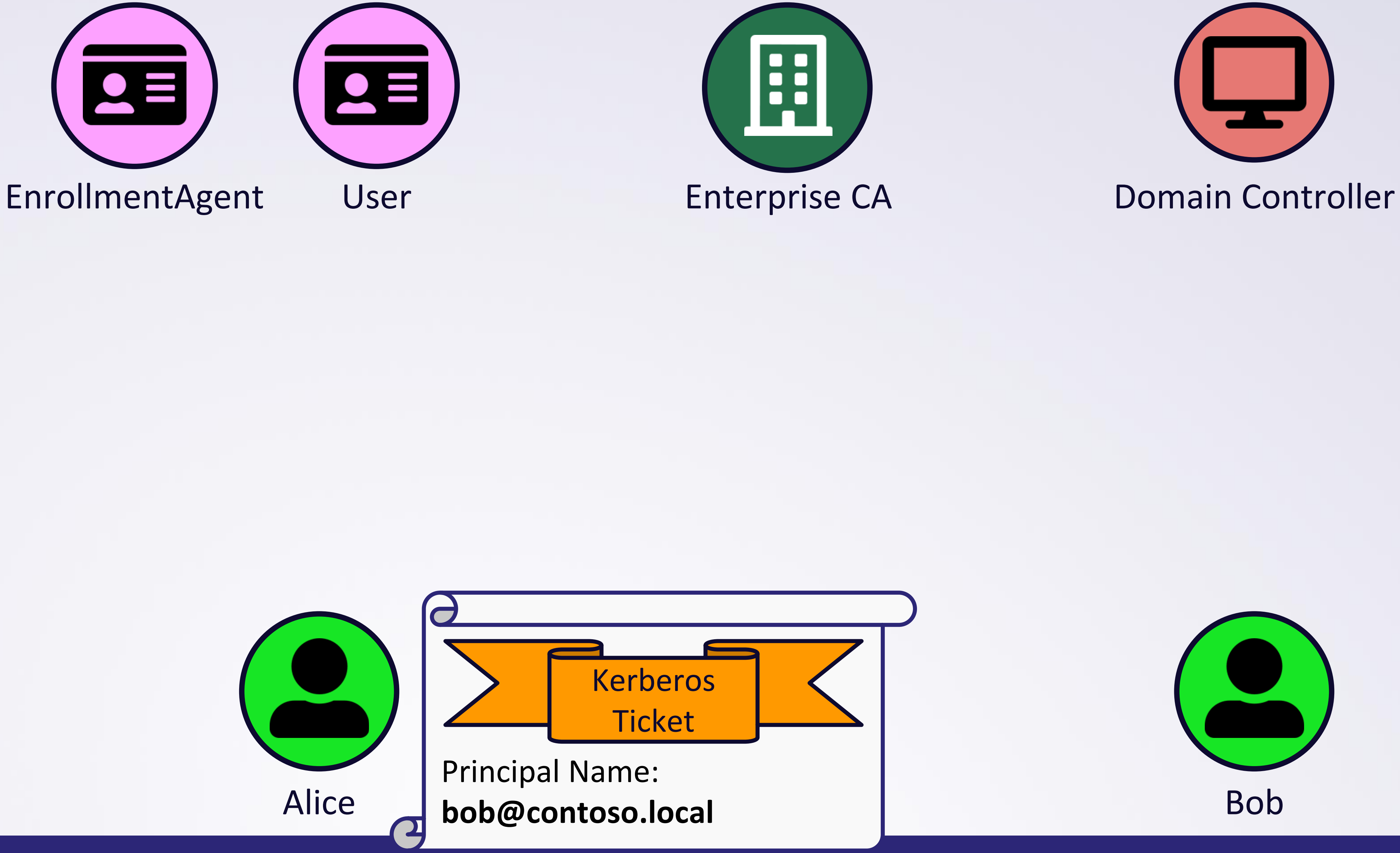
EKU: Client Authentication

SAN: **bob@contoso.local**



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

EKU: Client Authentication
SAN: bob@contoso.local



EnrollmentAgent

User

Enterprise CA

Domain Controller

Alice

Kerberos Ticket

Principal Name:

bob@contoso.local

Bob

ADCS domain escalation requirements

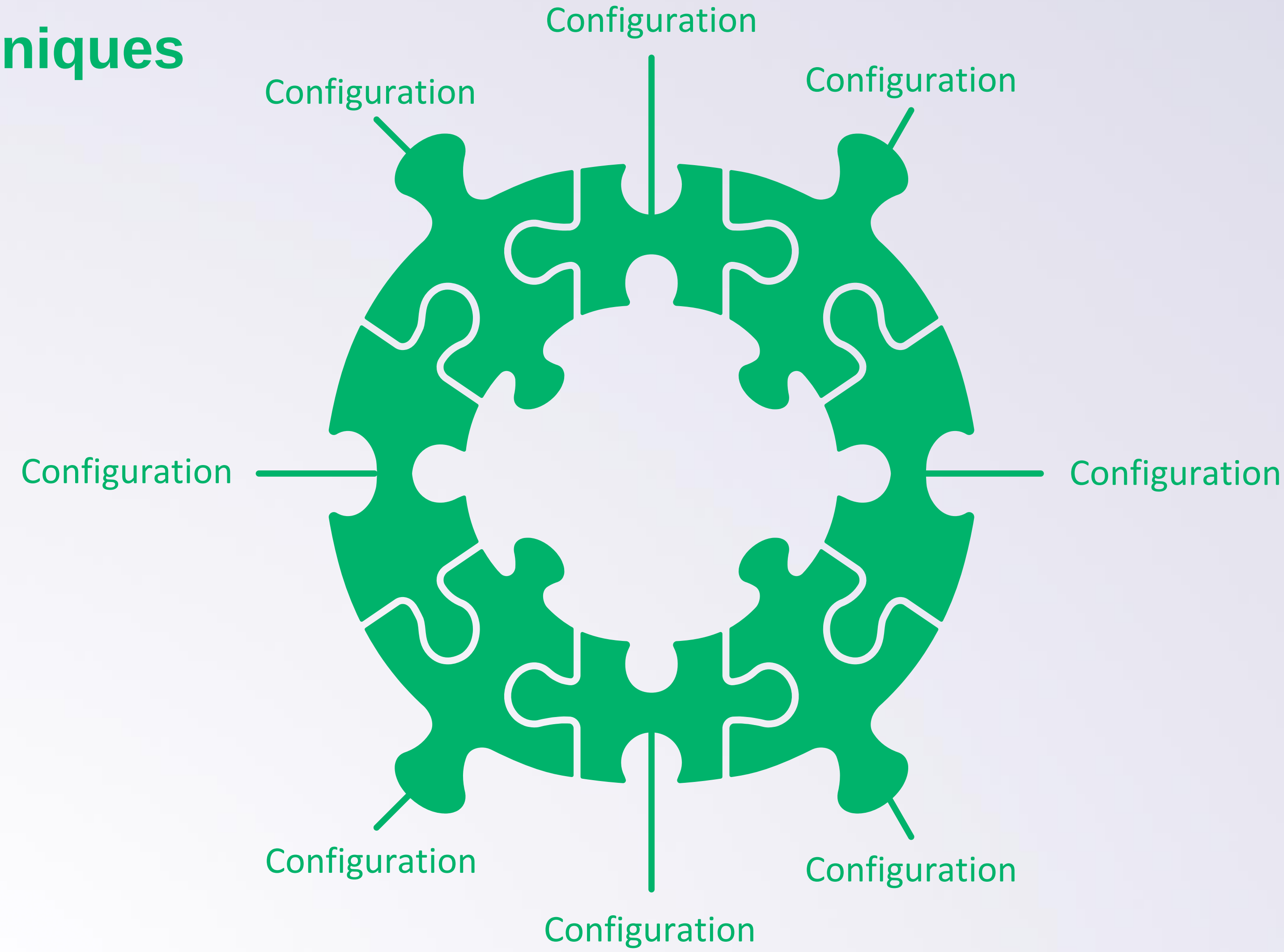
ADCS domain escalation techniques

ESC1 requirements for certificate template:

1. Enrollment rights
2. ENROLLEE_SUPPLIES_SUBJECT flag
3. EKUs that enable domain authentication
4. Manager approval disabled
5. No authorized signatures required
6. Published to an enterprise CA

ESC1 requirements for enterprise CA:

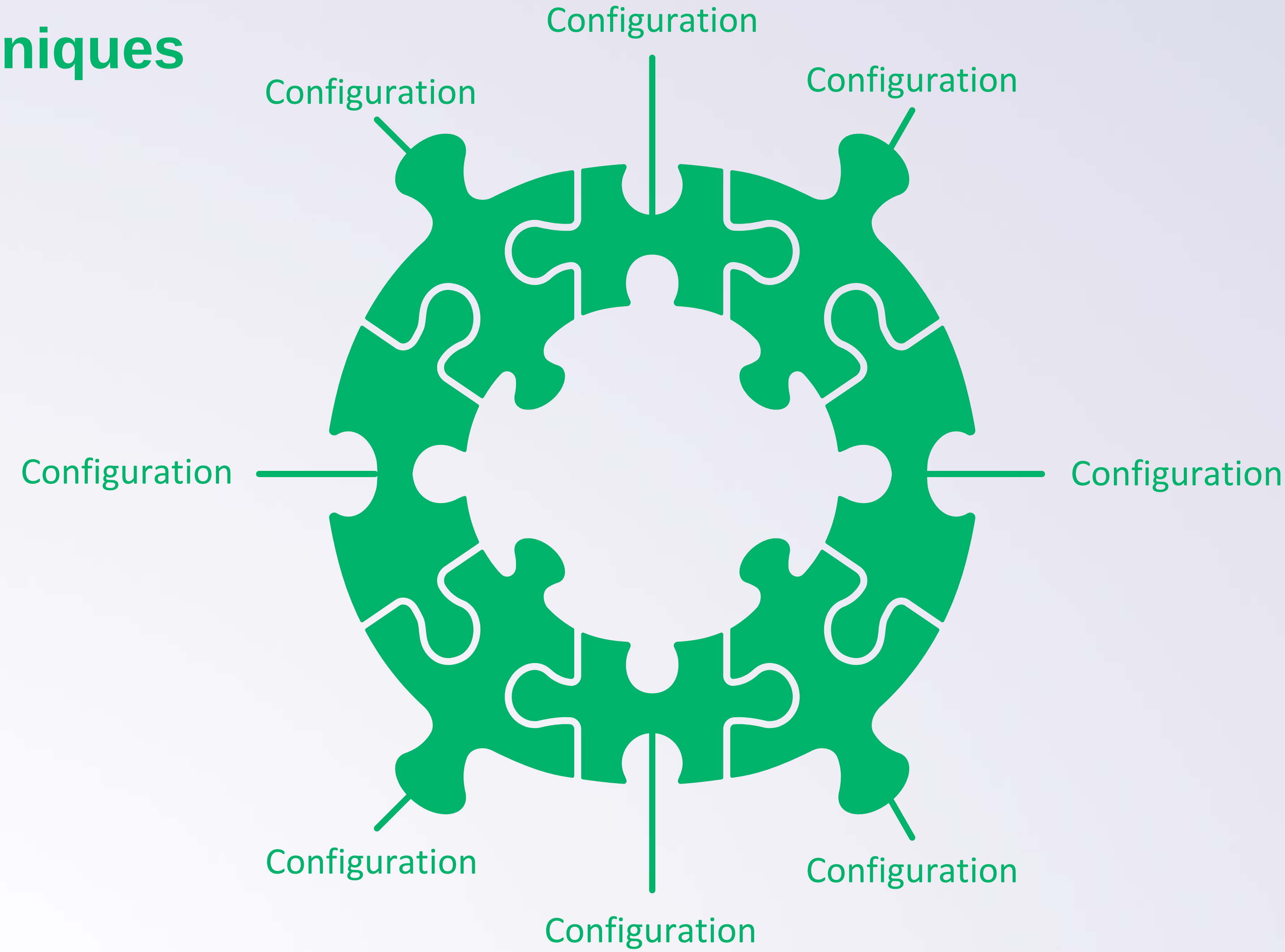
1. Enrollment rights
2. Trusted for NT authentication
3. CA certificate chain is trusted



ADCS domain escalation requirements

ADCS domain escalation techniques

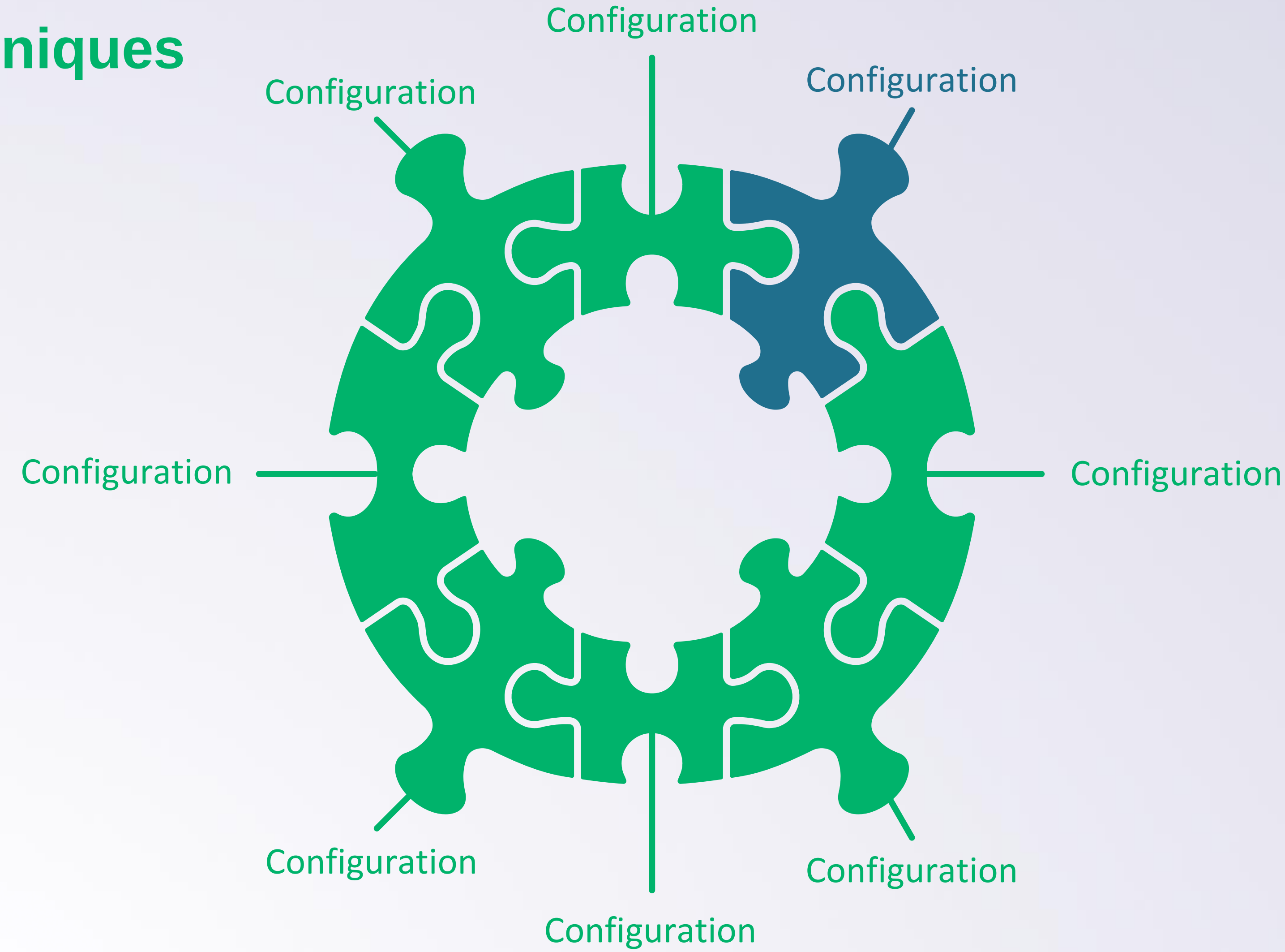
ESC1 =



ADCS domain escalation requirements

ADCS domain escalation techniques

ESC3 =

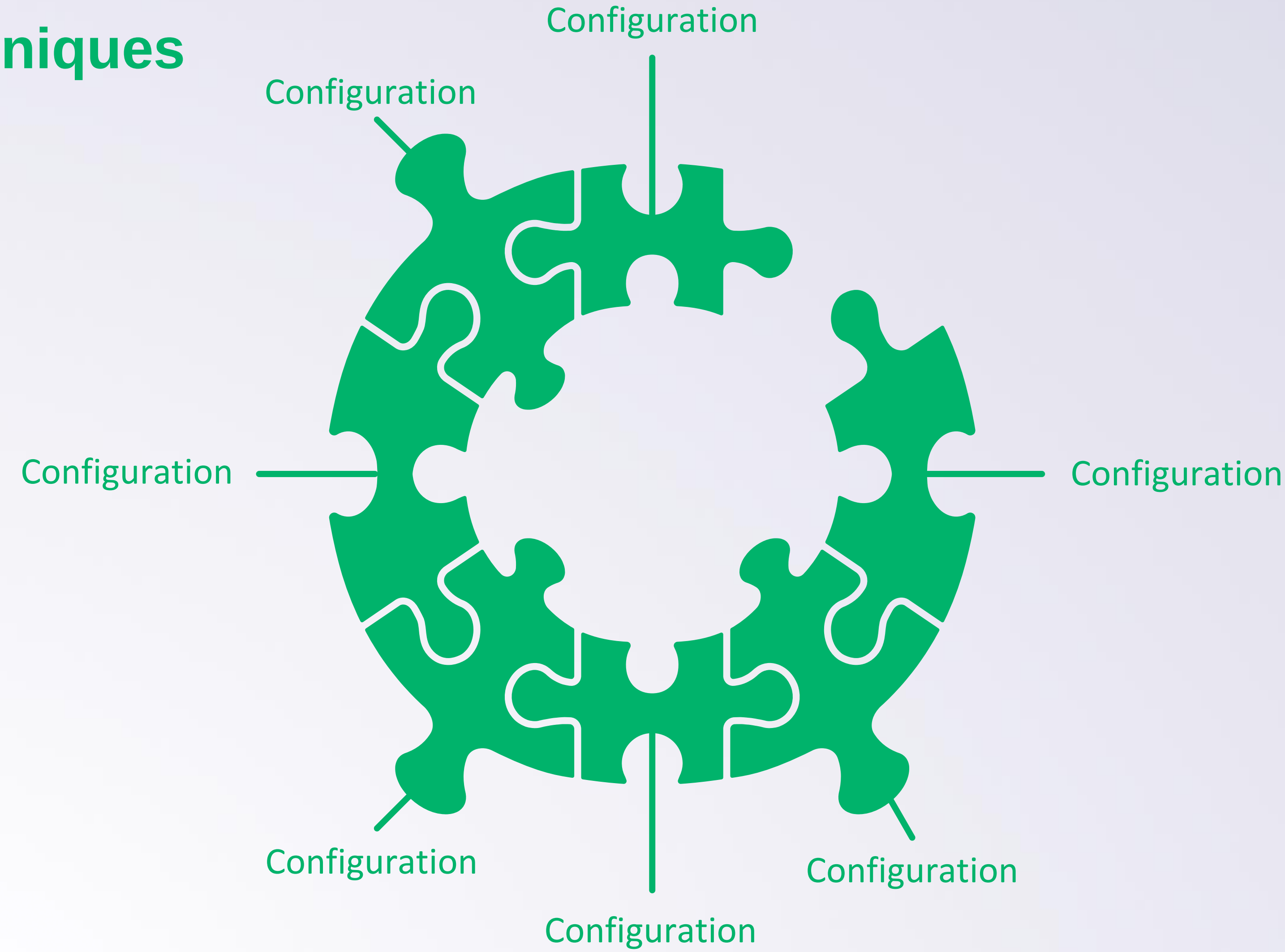


ADCS domain escalation requirements

ADCS domain escalation techniques

ESC1
ESC3

≠

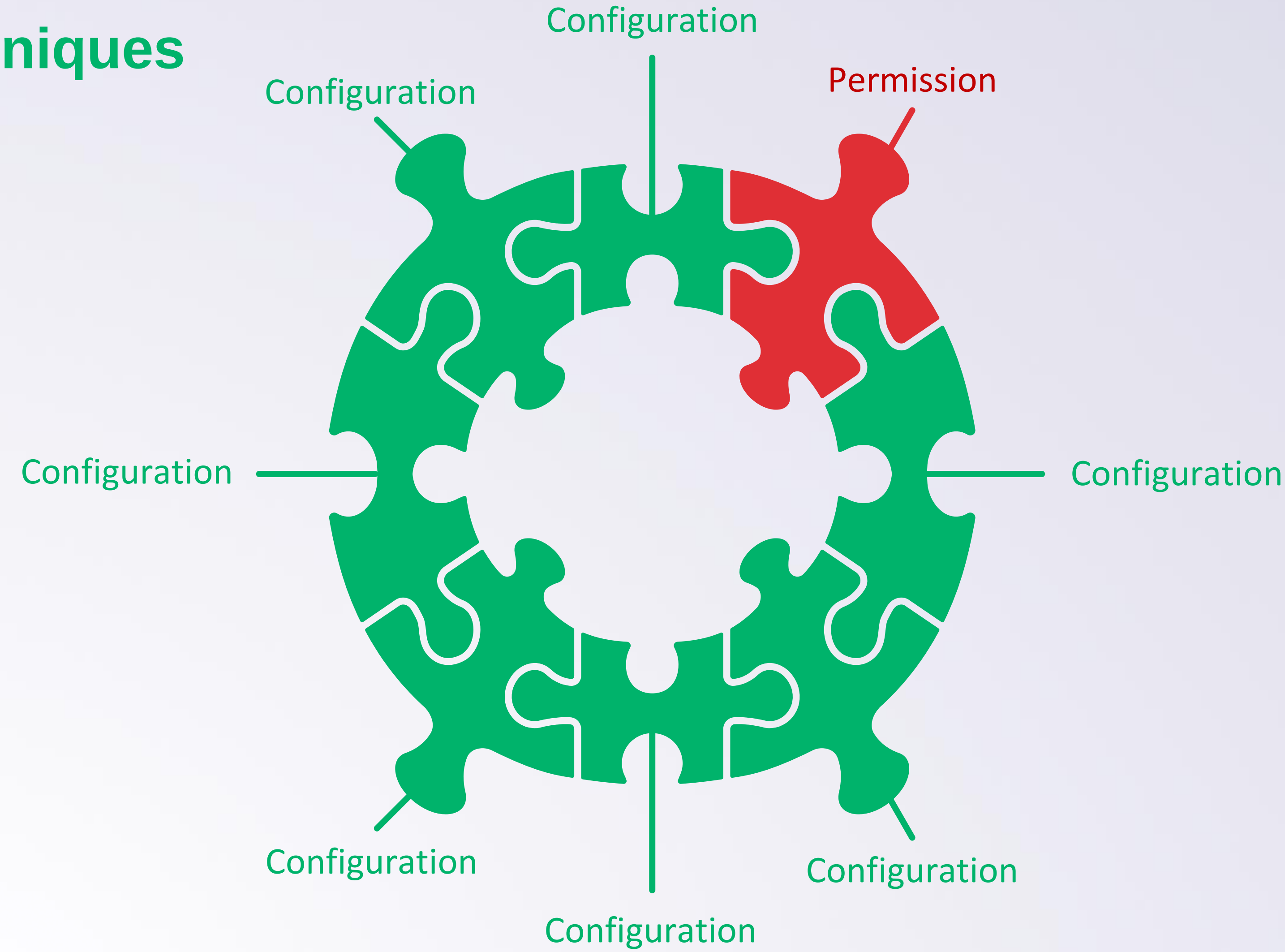


ADCS domain escalation requirements

ADCS domain escalation techniques

ESC4
ESC5
ESC7

=



Permissions to enable an escalation

ADCS domain escalation techniques

Technique	Control
ESC4	Control over certificate template
ESC5	Control over ADCS AD objects
ESC7	Control over CA service

Overview

ADCS domain escalation techniques

Escalation technique	Abuse
ESC1, ESC3	Template enables impersonation
ESC4, ESC5, ESC7	Control over ADCS objects

Overview

ADCS domain escalation techniques

Escalation technique	Abuse
ESC1, ESC3, ESC2, ESC13, ESC15	Template enables impersonation
ESC4, ESC5, ESC7, ESC12	Control over ADCS objects
ESC6	CA enables impersonation
ESC9, ESC10, ESC14b, c, d	Weak certificate mapping
ESC8	Relay authentication to HTTP
ESC11	Relay authentication to RPC
ESC14a	Control over explicit mappings on target

More resources

ADCS domain escalation techniques

Original blogposts

- ESC1-ESC8
- ESC9-ESC10
- ESC11
- ESC12
- ESC13
- ESC14
- ESC15

Follow-up blogposts

- ESC1-ESC10
- ESC1
- ESC3
- ESC5
- ESC6, ESC9, ESC10
- ESC7

Auditing and remediation

“We do not need to audit ADCS because.. “

Auditing and remediation

- “.. we have XDR”
  - How can it tell if a certificate enrollment/authentication is bad?
  - Prevention > detection
- “.. we had a pentest/red team”
  - Consultants are limited to time, tools, knowledge
  - How can they tell what permissions are legit?
- “.. we already did it”
  - More escalations has been published
  - Your environment changes

- You should probably audit ADCS

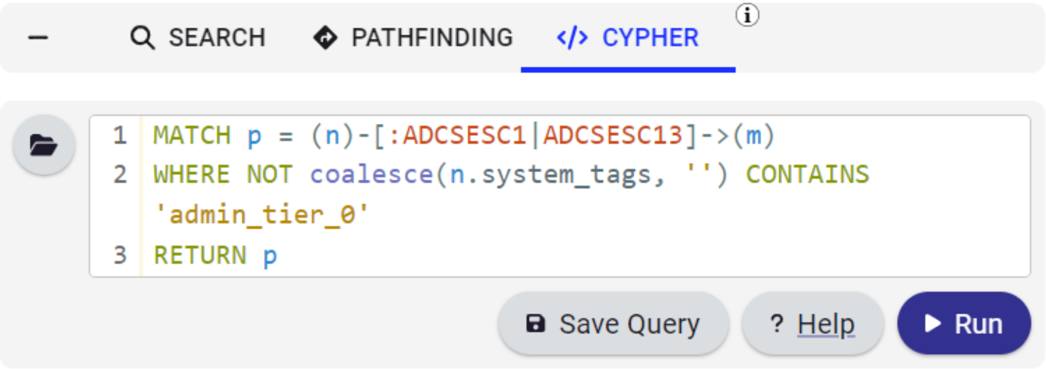
Overview

Auditing and remediation

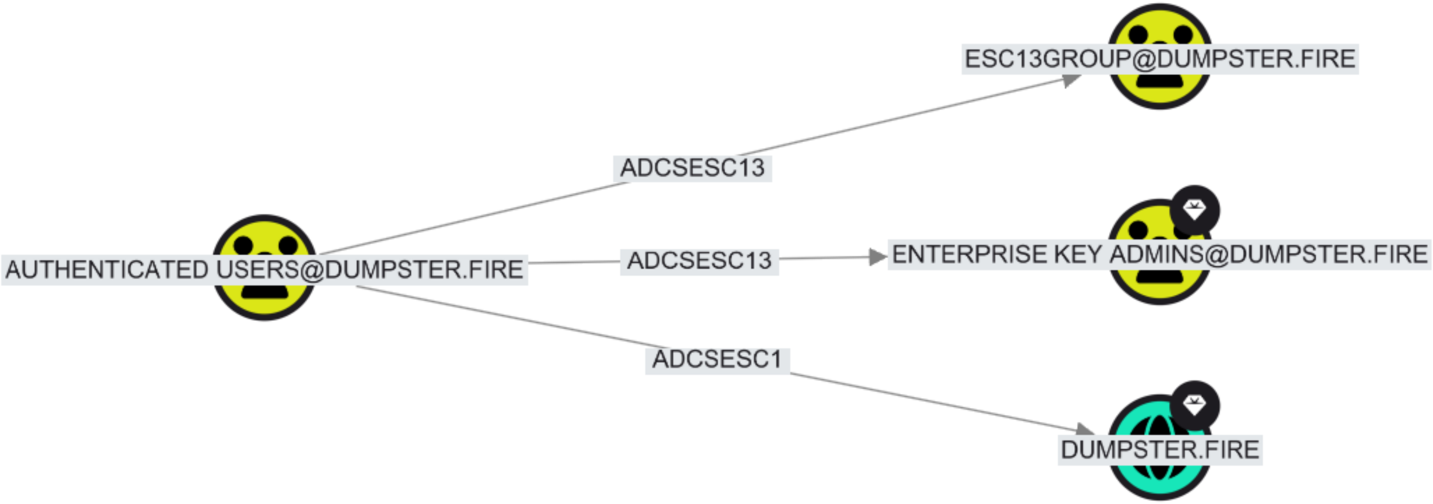
Escalation technique	Abuse	Audit tool	Remediation
ESC1, ESC13, ESC15	Template enables impersonation	BloodHound	Restrict enrollment rights to Tier Zero
ESC2, ESC3	Template enables impersonation	BloodHound	Restrict enrollment agents
ESC4, ESC5, ESC7, ESC12	Control over ADCS objects	BloodHound	Restrict control of ADCS objects to Tier Zero
ESC6	CA enables impersonation	BloodHound	Turn off `ATTRIBUTESUBJECTALTNAME2`
ESC9, ESC10, ESC14b, c, d	Weak certificate mapping	BloodHound	Enforce strong certificate mapping
ESC8	Relay authentication to HTTP	PingCastle	Enforce HTTPS + EPA
ESC11	Relay authentication to RPC	Certipy	Enforce ICPR encryption
ESC14a	Control over explicit mappings on target	PowerShell	Restrict write access to AltSecurityIdentities

ESC1/13: Template enables impersonation

Auditing



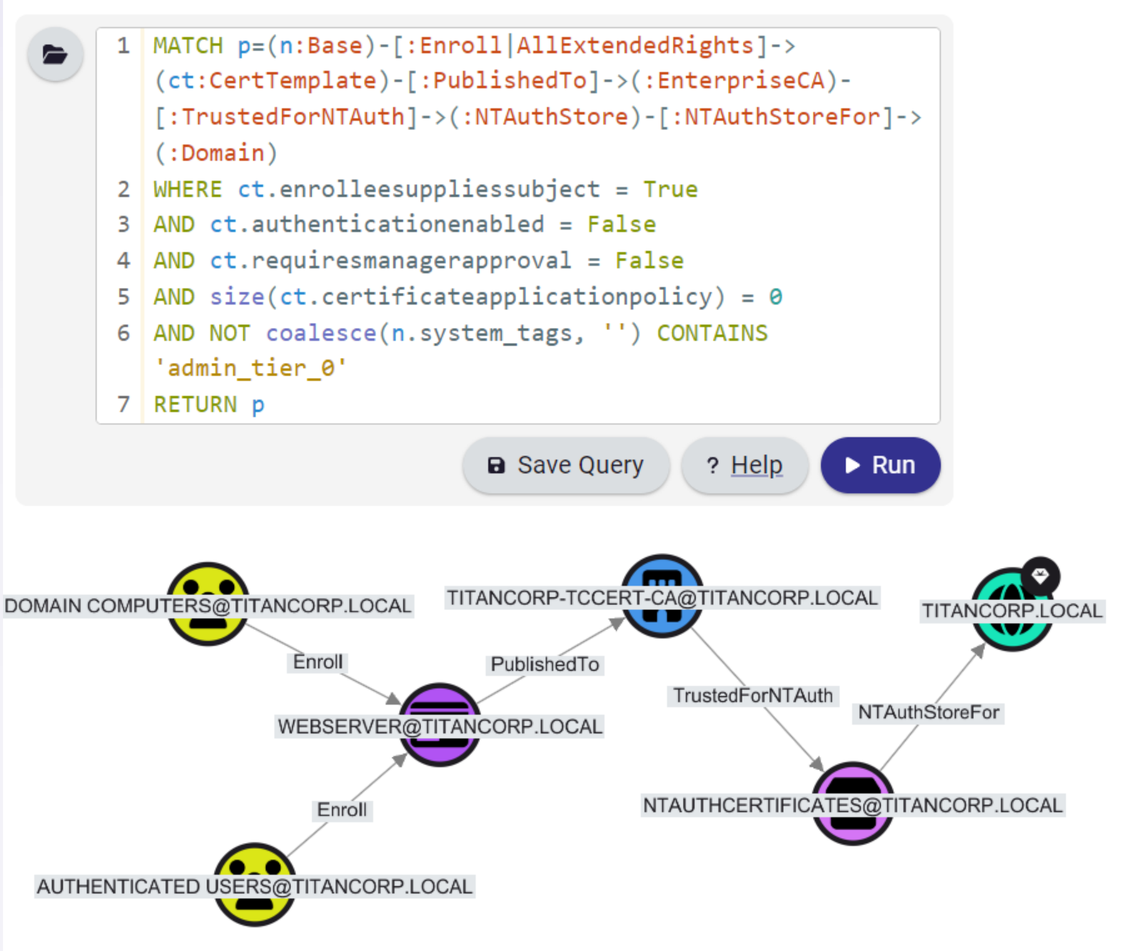
```
MATCH p = (n)-[:ADCSESC1|ADCSESC13]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS
'admin_tier_0'
RETURN p
```


ESC13GROUP@DUMPSTER.FIRE
ADCSESC13
AUTHENTICATED USERS@DUMPSTER.FIRE
ADCSESC13
ENTERPRISE KEY ADMINS@DUMPSTER.FIRE
ADCSESC1
DUMPSTER.FIRE

```
MATCH p = (n)-[:ADCSESC1|ADCSESC13]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS 'admin_tier_0’
RETURN p
```

ESC15: Template enables impersonation

Auditing



```
MATCH p=(n:Base)-[:Enroll|AllExtendedRights]->(ct:CertTemplate)-[:PublishedTo]->(:EnterpriseCA)-[:TrustedForNTAuth]->(:NTAuthStore)-[:NTAuthStoreFor]->(:Domain)
WHERE ct.enrolleesuppliessubject = True
AND ct.authenticationenabled = False
AND ct.requiresmanagerapproval = False
AND size(ct.certificateapplicationpolicy) = 0
AND NOT coalesce(n.system_tags, '') CONTAINS 'admin_tier_0'
RETURN p
```

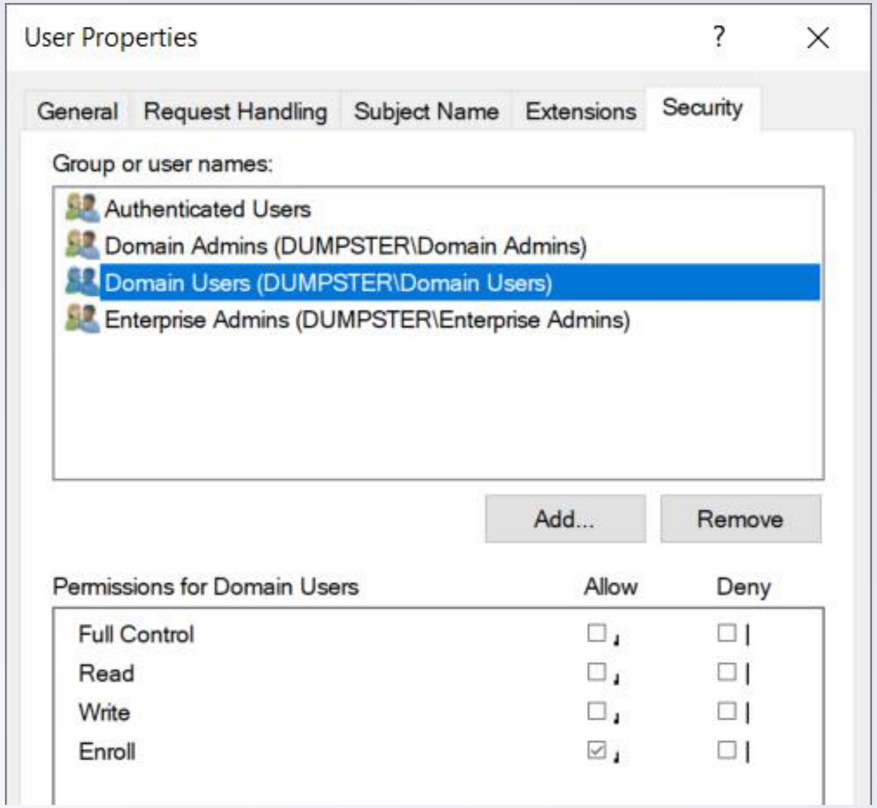
Save Query
? Help
▶ Run
DOMAIN COMPUTERS@TITANCORP.LOCAL
Enroll
WEBSERVER@TITANCORP.LOCAL
Enroll
AUTHENTICATED USERS@TITANCORP.LOCAL
PublishedTo
TITANCORP-TCCERT-CA@TITANCORP.LOCAL
TrustedForNTAuth
NTAUTHCERTIFICATES@TITANCORP.LOCAL
NTAuthStoreFor
TITANCORP.LOCAL

```
MATCH p=(n:Base)-
[:Enroll|AllExtendedRights]-
>(ct:CertTemplate)-[:PublishedTo]-
>(:EnterpriseCA)-
[:TrustedForNTAuth]->(:NTAuthStore)-
[:NTAuthStoreFor]->(:Domain)
WHERE ct.enrolleesuppliessubject =
True
AND ct.authenticationenabled = False
AND ct.requiresmanagerapproval =
False
AND
size(ct.certificateapplicationpolicy
) = 0
AND NOT coalesce(n.system_tags, '')
CONTAINS 'admin_tier_0’
RETURN p
```

ESC1/13/15: Restrict enrollment rights to Tier Zero

Remediation

- Only Tier Zero users should be allowed to impersonate others
- Alternative: Enrollment agents



User Properties

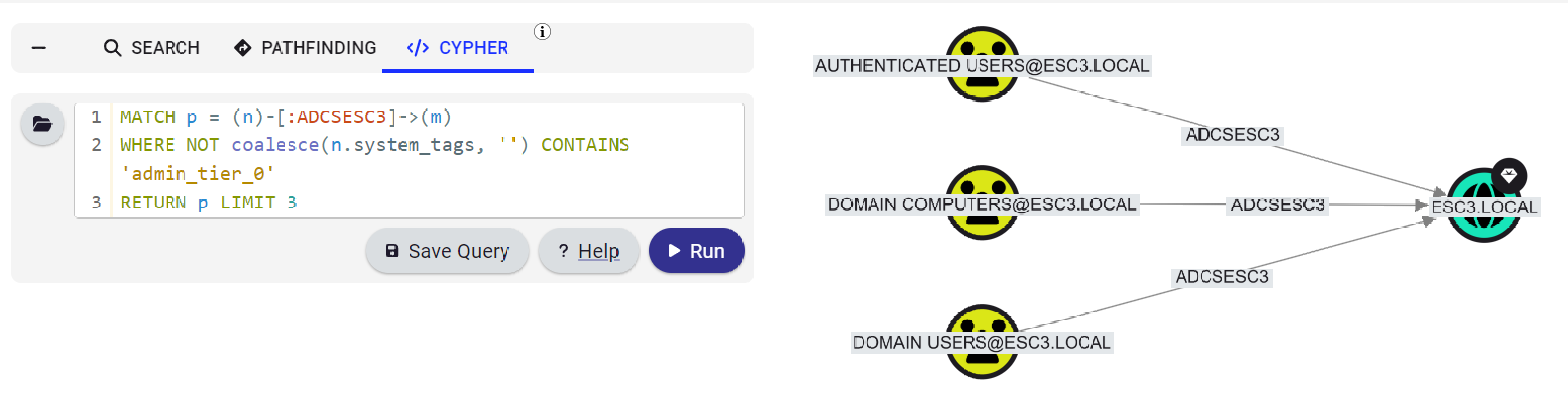
Group or user names:

- Authenticated Users
- Domain Admins (DUMPSTER\Domain Admins)
- Domain Users (DUMPSTER\Domain Users)
- Enterprise Admins (DUMPSTER\Enterprise Admins)

Permissions for Domain Users	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Enroll	☑	□

ESC2/3: Template enables impersonation

Auditing



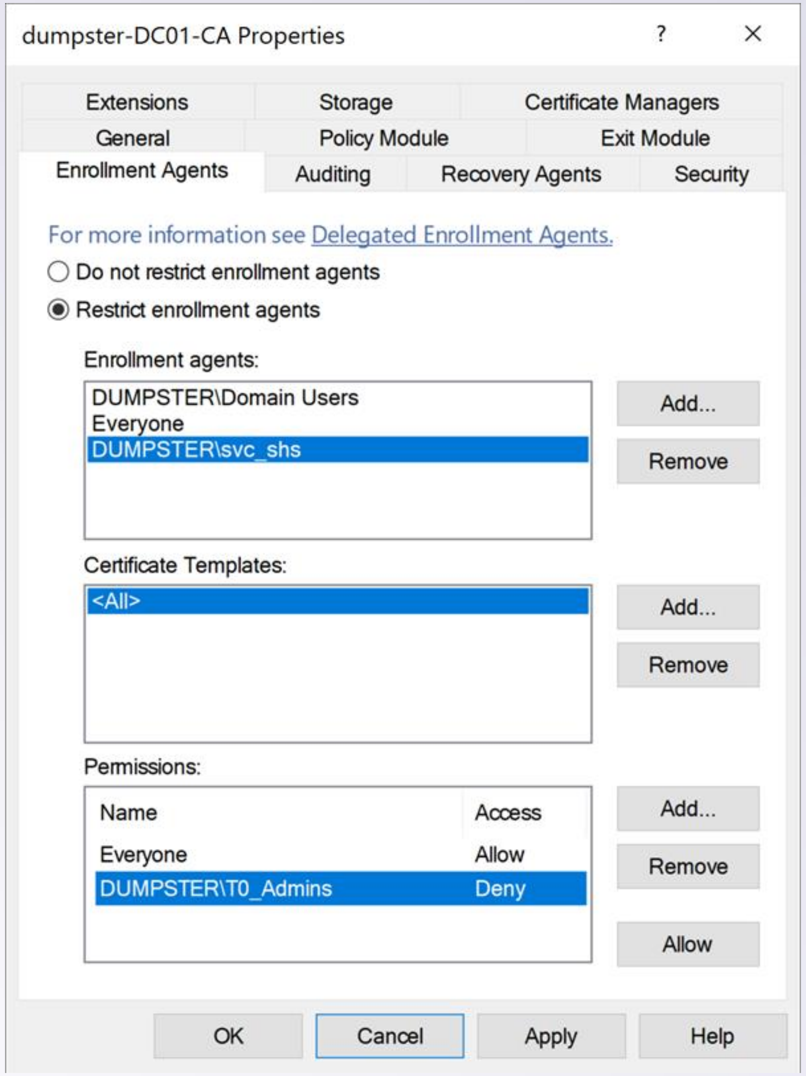
```
MATCH p = (n)-[:ADCSESC3]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS
'admin_tier_0'
RETURN p LIMIT 3
```

```
MATCH p = (n)-[:ADCSESC3]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS 'admin_tier_0’
RETURN p
```

ESC2/3: Restrict enrollment agents

Remediation

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



dumpster-DC01-CA Properties

For more information see Delegated Enrollment Agents.

○ Do not restrict enrollment agents

● Restrict enrollment agents

Enrollment agents:

DUMPSTER\Domain Users
Everyone
DUMPSTER\svc_shs

Certificate Templates:

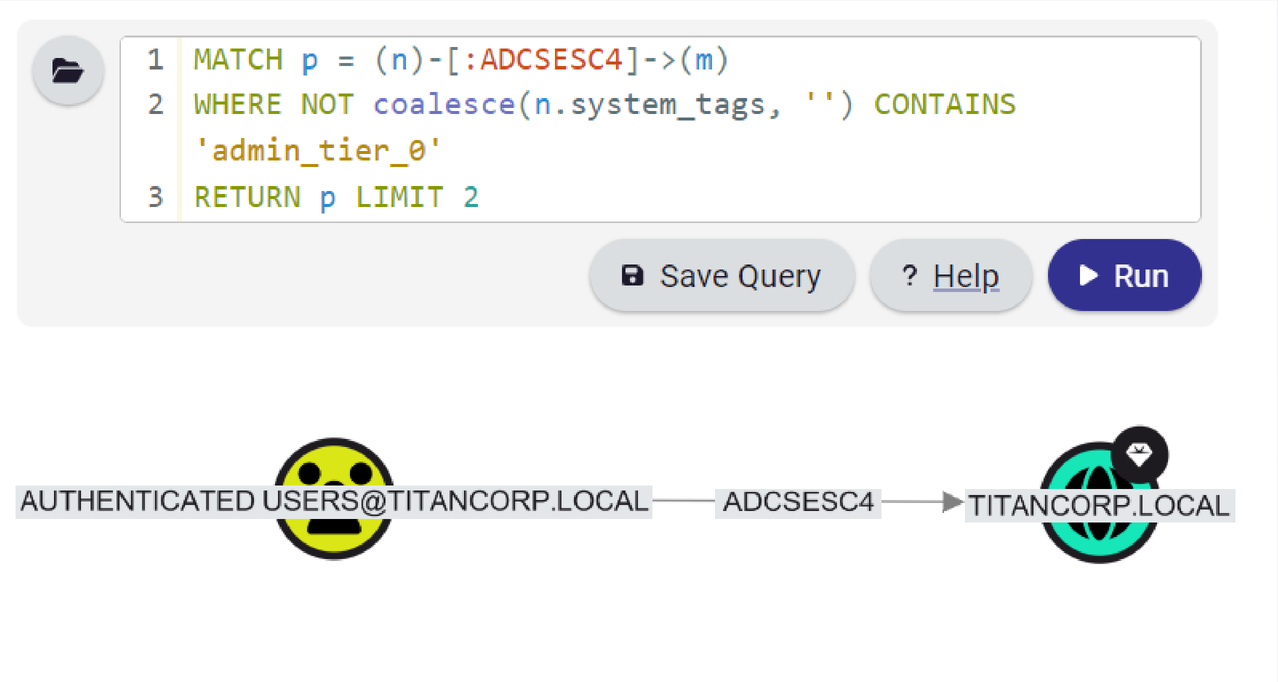
<All>

Permissions:

Name	Access
Everyone	Allow
DUMPSTER\T0_Admins	Deny

ESC4: Control over ADCS objects

Auditing

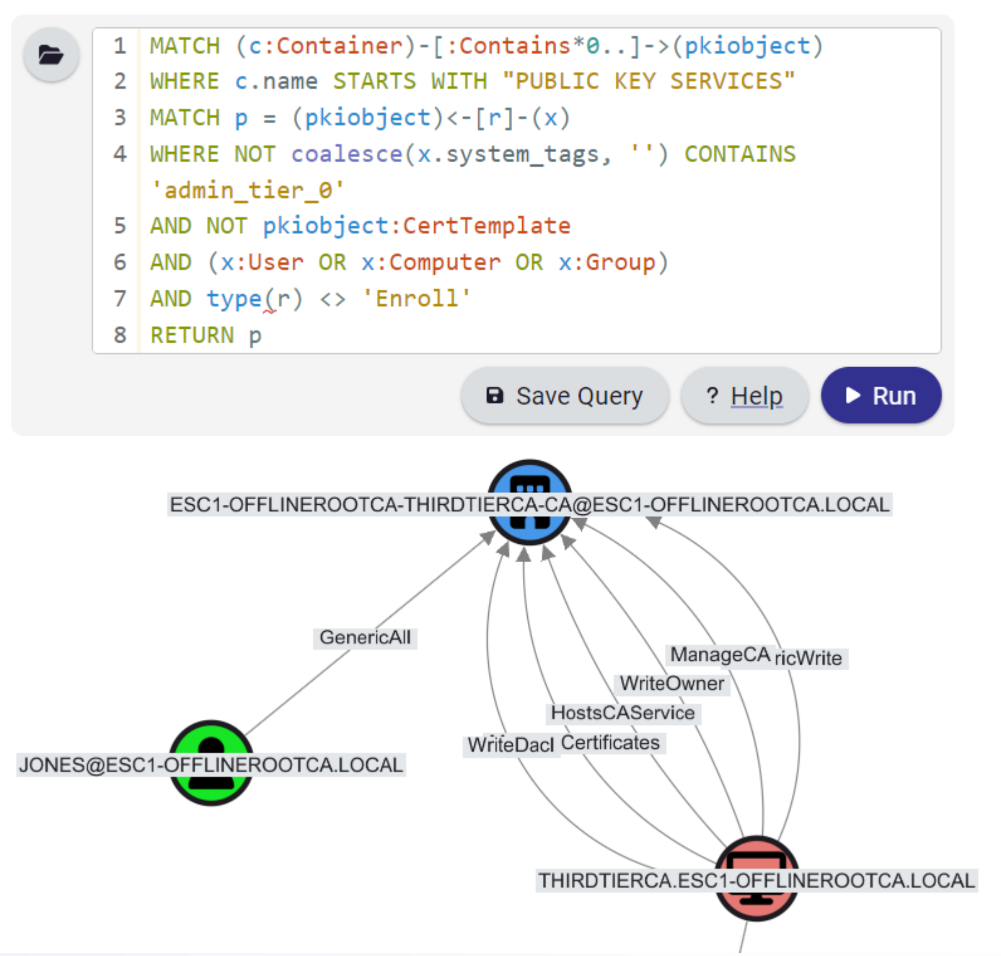


```
MATCH p = (n)-[:ADCSESC4]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS
'admin_tier_0'
RETURN p LIMIT 2
```

```
MATCH p = (n)-[:ADCSESC4]->(m)
WHERE NOT coalesce(n.system_tags,
'') CONTAINS 'admin_tier_0’
RETURN p
```

ESC5/7/12: Control over ADCS objects

Auditing



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

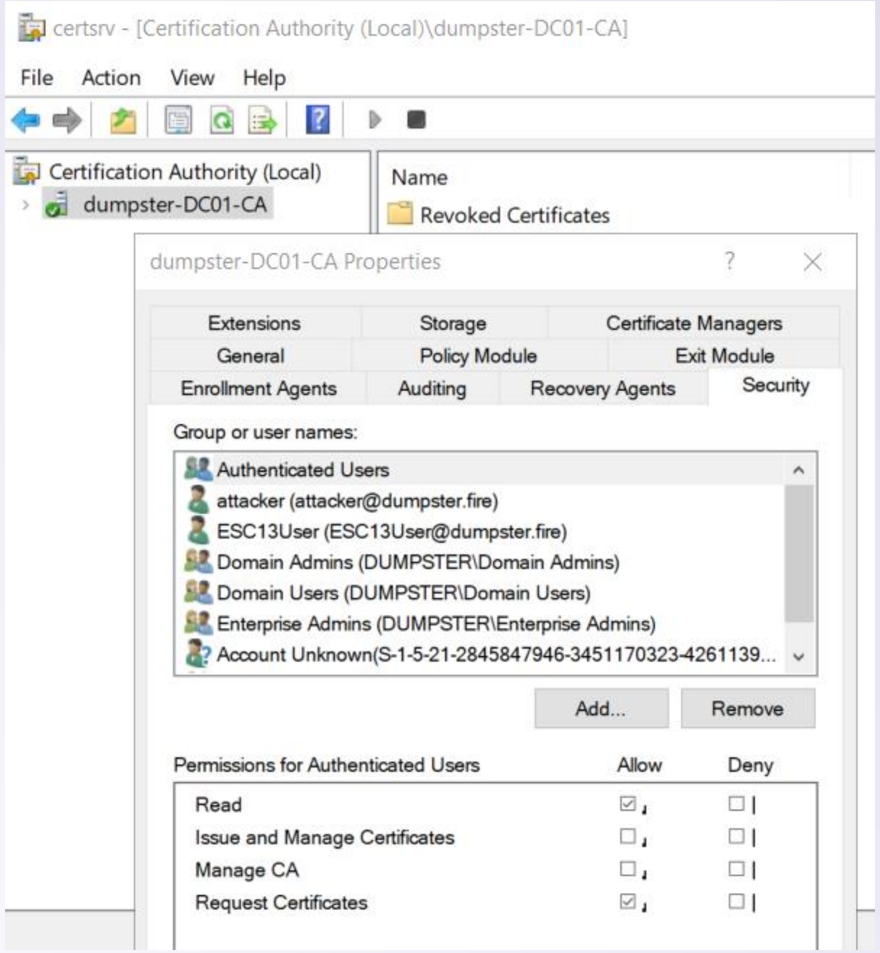
Save Query
? Help
Run
ESC1-OFFLINEROOTCA-THIRDTIERCA-CA@ESC1-OFFLINEROOTCA.LOCAL
GenericAll
JONES@ESC1-OFFLINEROOTCA.LOCAL
ManageCA
ricWrite
WriteOwner
HostsCAService
WriteDacl
Certificates
THIRDTIERCA.ESC1-OFFLINEROOTCA.LOCAL

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

ESC4/5/7/12: Restrict control over ADCS objects

Remediation

- ADCS is Tier Zero
- No reason non-Tier Zero has control over ADCS objects
- Incl. control over CA computers



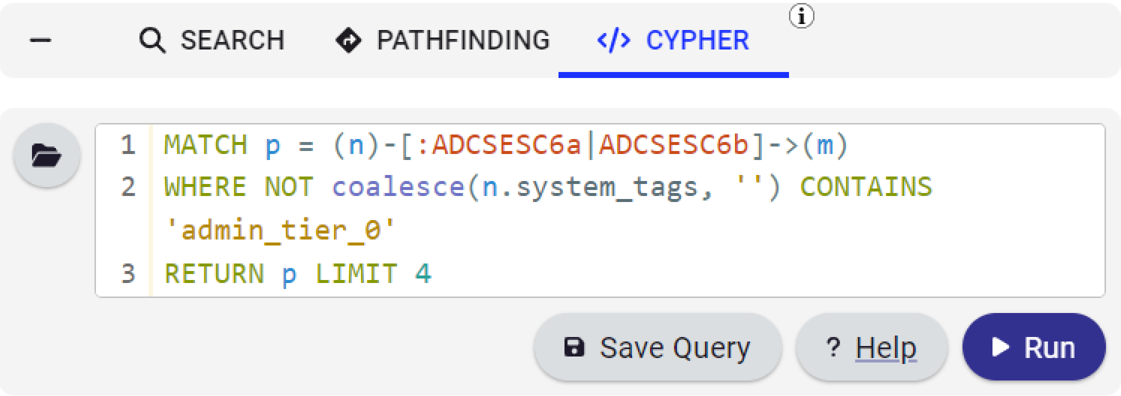
Group or user names:

Authenticated Users
attacker (attacker@dumpster.fire)
ESC13User (ESC13User@dumpster.fire)
Domain Admins (DUMPSTER\Domain Admins)
Domain Users (DUMPSTER\Domain Users)
Enterprise Admins (DUMPSTER\Enterprise Admins)
Account Unknown(S-1-5-21-2845847946-3451170323-4261139...

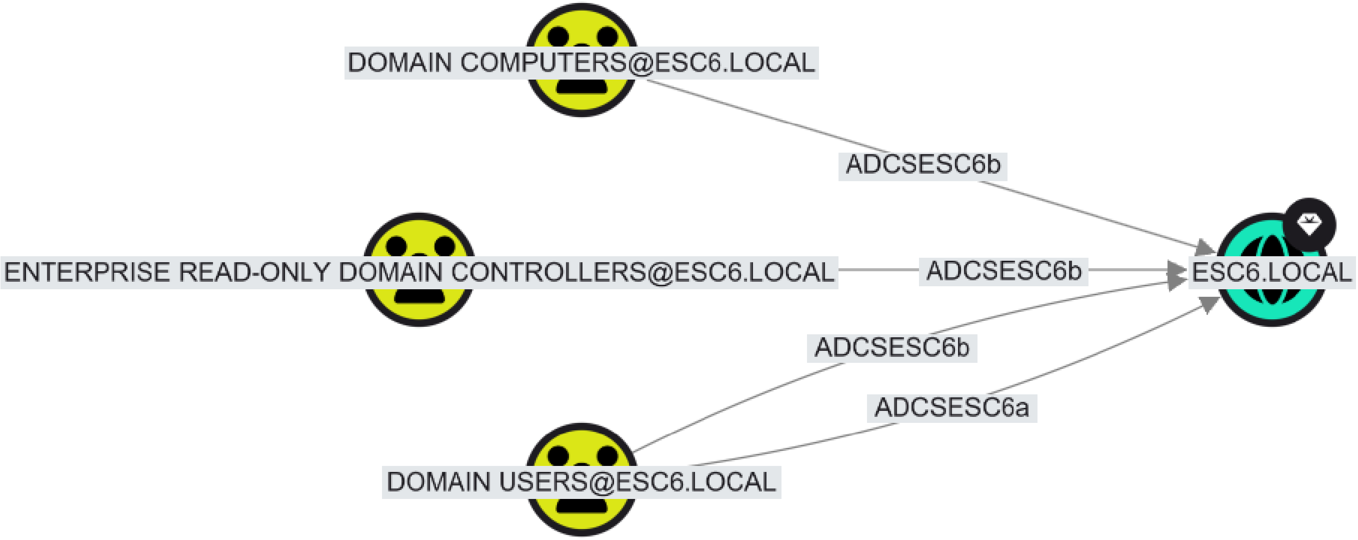
Permissions for Authenticated Users	Allow	Deny
Read	☑	□
Issue and Manage Certificates	□	□
Manage CA	□	□
Request Certificates	☑	□

ESC6: CA enables impersonation

Auditing



```
MATCH p = (n)-[:ADCSESC6a|ADCSESC6b]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS
'admin_tier_0'
RETURN p LIMIT 4
```


DOMAIN COMPUTERS@ESC6.LOCAL
ADCSESC6b
ENTERPRISE READ-ONLY DOMAIN CONTROLLERS@ESC6.LOCAL
ADCSESC6b
ESC6.LOCAL
ADCSESC6b
ADCSESC6a
DOMAIN USERS@ESC6.LOCAL

```
MATCH p = (n)-[:ADCSESC6a|ADCSESC6b]->(m)
WHERE NOT coalesce(n.system_tags, '') CONTAINS 'admin_tier_0'
RETURN p
```

ESC6: Turn off ATTRIBUTESUBJECTALTNAME2

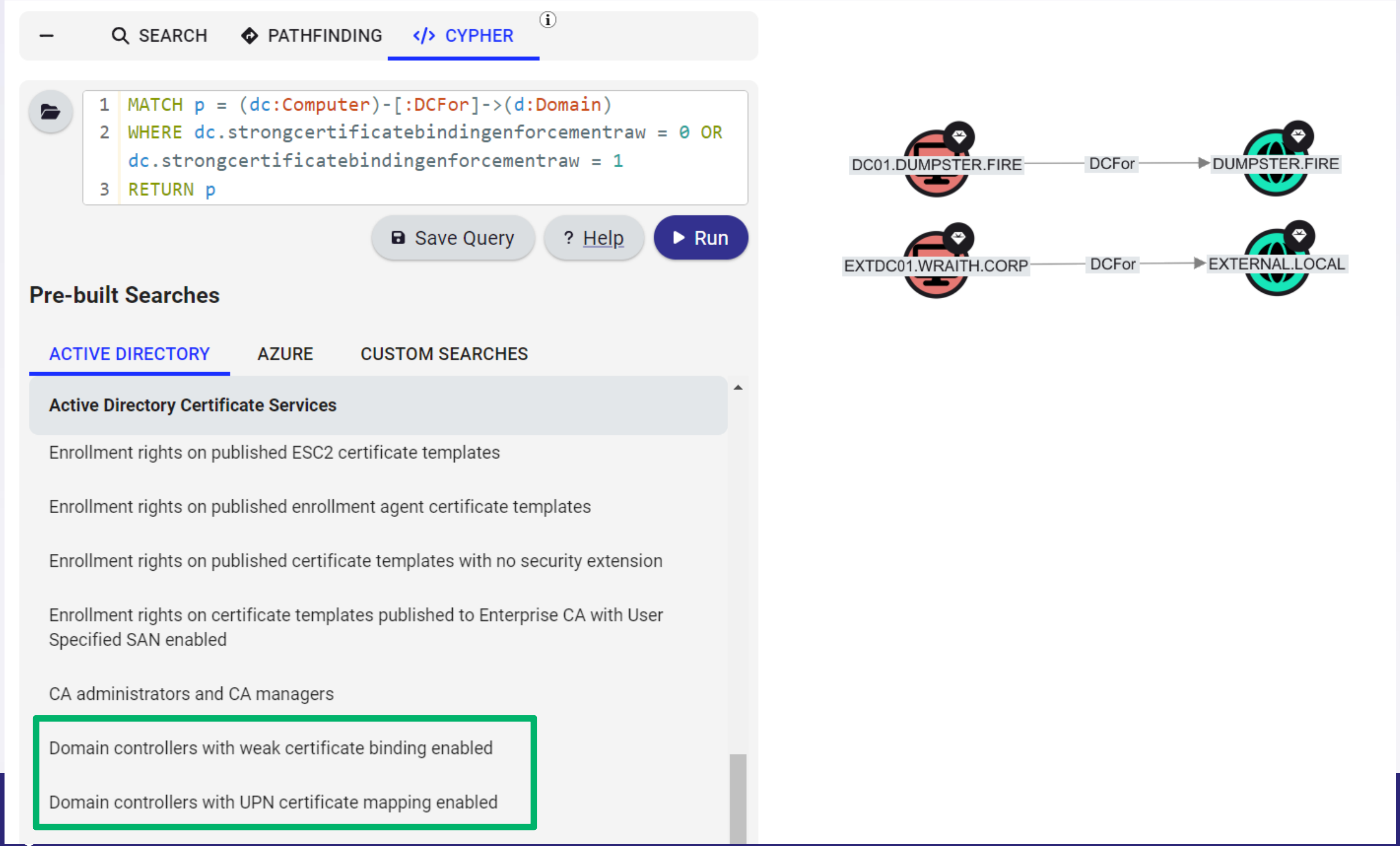
Remediation

Remove the `EDITF_ATTRIBUTESUBJECTALTNAME2` flag on a CA host:

```
certutil -config "CA_HOST\CA_NAME" -setreg
policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2
```

ESC9/10/14bcd: Weak certificate mapping

Auditing



```
MATCH p = (dc:Computer)-[:DCFor]->(d:Domain)
WHERE dc.strongcertificatebindingenforcementraw = 0 OR
dc.strongcertificatebindingenforcementraw = 1
RETURN p
```

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Active Directory Certificate Services

- Enrollment rights on published ESC2 certificate templates
- Enrollment rights on published enrollment agent certificate templates
- Enrollment rights on published certificate templates with no security extension
- Enrollment rights on certificate templates published to Enterprise CA with User Specified SAN enabled
- CA administrators and CA managers
- Domain controllers with weak certificate binding enabled
- Domain controllers with UPN certificate mapping enabled

- Audit requires admin access on DCs
- DCs vulnerable by default
- Read more: ADCS Attack Paths in BloodHound — Part 3

ESC9/10/14bcd: Enforce strong mapping

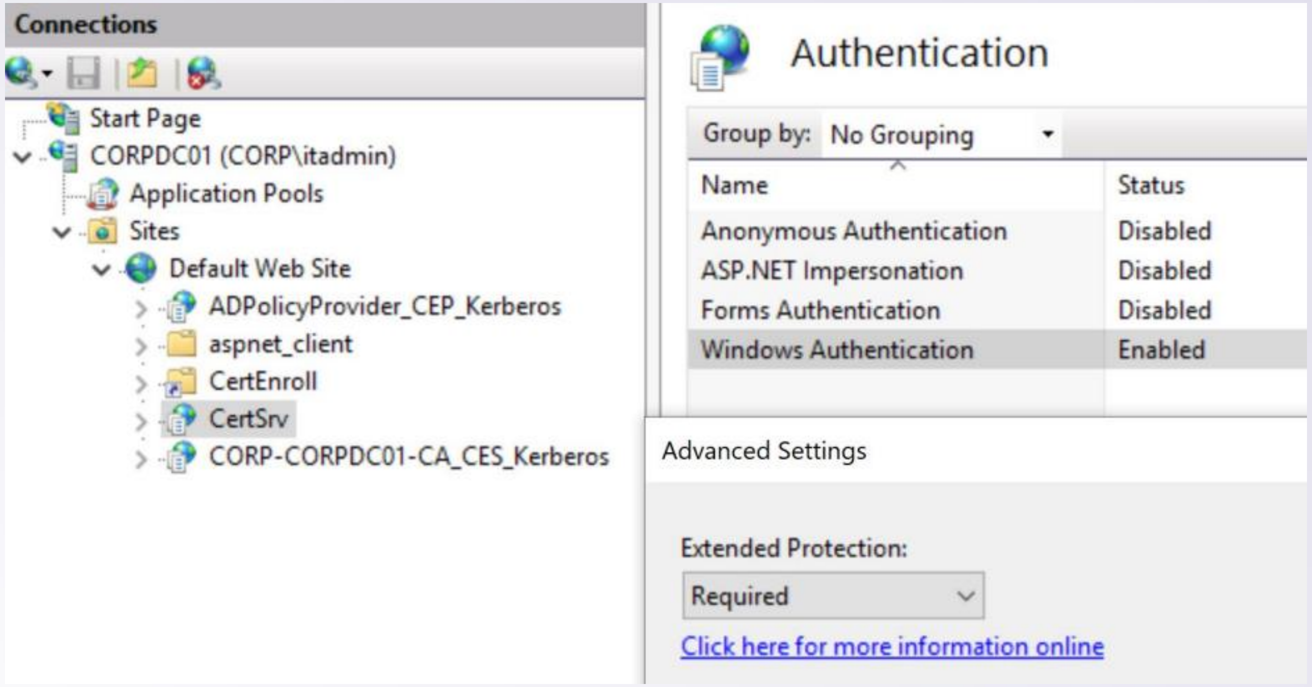
Remediation

- Controlled in registry on DCs
- Two settings:
  - Kerberos certificate mapping
  - Schannel certificate mapping
- Microsoft guidance: KB5014754: Certificate-based authentication changes on Windows domain controllers

ESC8: Relay authentication to HTTP

Auditing and remediation

- Audit: PingCastle
- Remediation (both)
  - HTTPS
  - Require Extended Protection for Authentication (EPA)



Name	Status
Anonymous Authentication	Disabled
ASP.NET Impersonation	Disabled
Forms Authentication	Disabled
Windows Authentication	Enabled

Advanced Settings

Extended Protection: Required

Click here for more information online

ESC11: Relay authentication to RPC

Auditing and remediation

- Audit: Certipy
- Remediation: Encryption on ICPR

```
certutil -setreg CA\InterfaceFlags
+IF_ENFORCEENCRYPTICERTREQUEST

net stop certsvc & net start certsvc
```

ESC14a: Control over explicit mappings on target

Auditing and remediation

- Attack:
  - 1) Add reference to attacker-controlled certificate in target’s AltSecurityIdentities
  - 2) Authenticate as target using certificate
- Audit: Get-WriteAltSecIDACEs.ps1
  - Explained in blog post: ESC14 Abuse Technique
- Remediation: Restrict write access to AltSecurityIdentities attribute

Remediation - It’s a balance

Controlled remediation

- Examine situation carefully
- Explore possible solutions
- Determine what could break
- Restore plan
- Phased implementation
- Document everything

Fast remediation

- Click, click, done!
- (screaming starts in the background)

Detection

Auditing and remediation

- Out of scope for today
- Great resource by Teymur Kheirkhabarov and Demyan Sokolin from BI.ZONE:
    - https://speakerdeck.com/heirhabarov/hunting-for-active-directory-certificate-services-abuse
- Track down if remediation will break something

SPECTEROPS

Thank you