BLOODHOUND
ENTERPRISE

ADCS Attack Paths in BloodHound

December 2023

Andy Robbins, Principal Product Architect

Jonas Bülow Knudsen, Product Architect

Who are we

Andy Robbins

Principal Product Architect
Co-Creator of BloodHound

Jonas Bülow Knudsen

Product Architect

Agenda

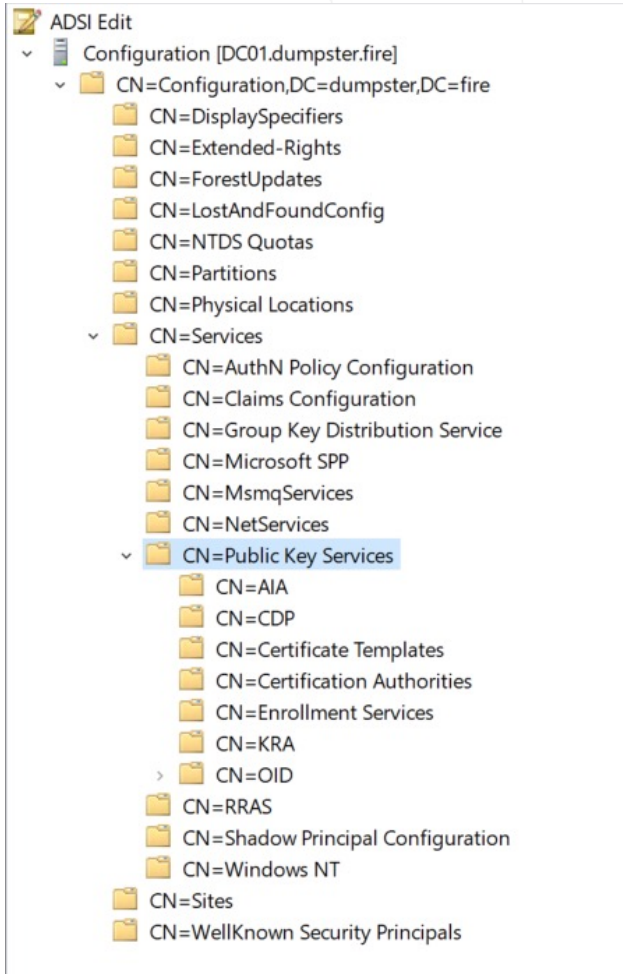
- What is ADCS
- ADCS Components in BloodHound
- Demo Time!
- ADCS in BloodHound Enterprise
- Acknowledgements

What is ADCS

Active Directory Certificate Services (ADCS)

What is ADCS

- Provides scalable Public Key Infrastructure (PKI)
- Used for issuing and managing digital certificates
- Located in the Public Key Services container

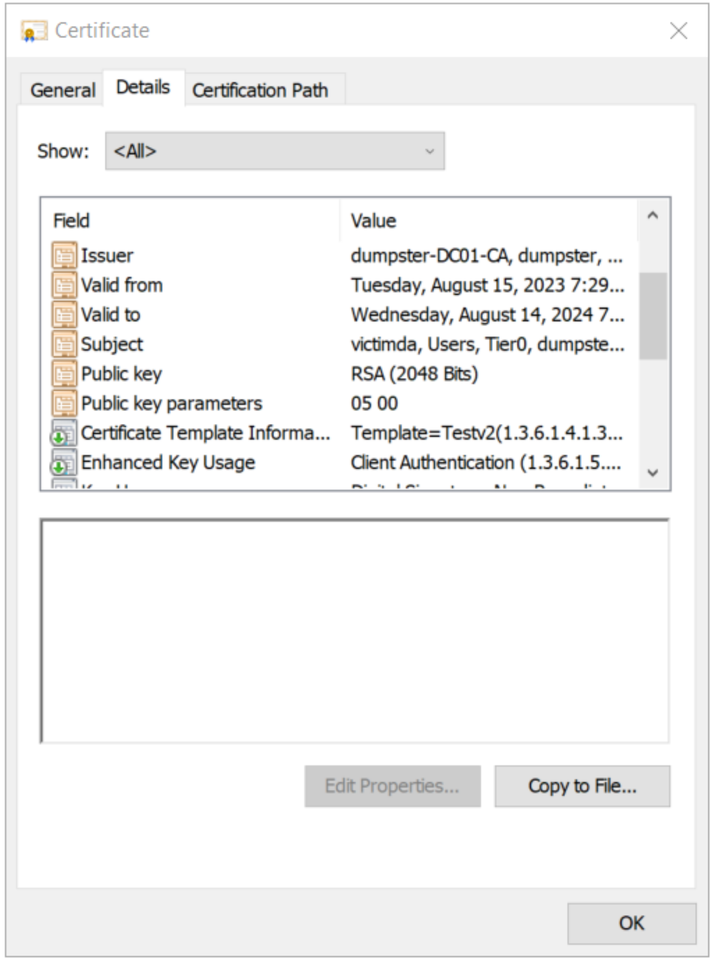


```
ADSI Edit
⌄ Configuration [DC01.dumpster.fire]
  ⌄ CN=Configuration,DC=dumpster,DC=fire
      CN=DisplaySpecifiers
      CN=Extended-Rights
      CN=ForestUpdates
      CN=LostAndFoundConfig
      CN=NTDS Quotas
      CN=Partitions
      CN=Physical Locations
    ⌄ CN=Services
        CN=AuthN Policy 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
```

Digital certificate

What is ADCS

- Asymmetric cryptography (public and private key pair)
- Bound to a "Subject"
- Used for encryption, signing, and authentication
- Holds a certificate chain



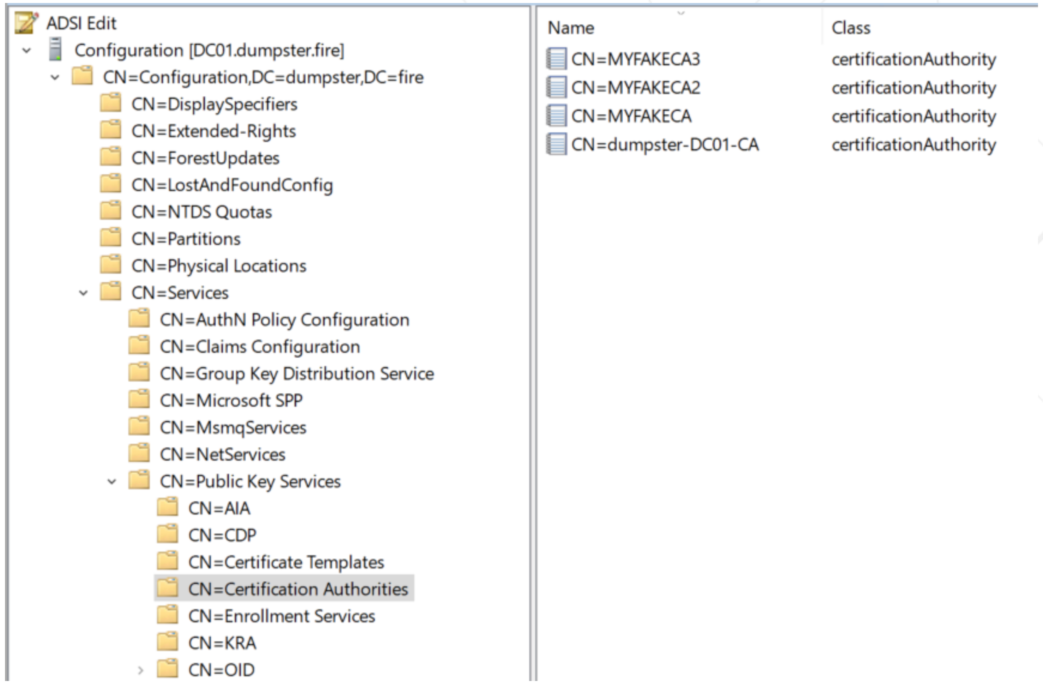
Show: <All>

Field	Value
Issuer	dumpster-DC01-CA, dumpster, ...
Valid from	Tuesday, August 15, 2023 7:29...
Valid to	Wednesday, August 14, 2024 7...
Subject	victimda, Users, Tier0, dumpste...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Certificate Template Informa...	Template=Testv2(1.3.6.1.4.1.3...
Enhanced Key Usage	Client Authentication (1.3.6.1.5....

ADCS components – RootCA

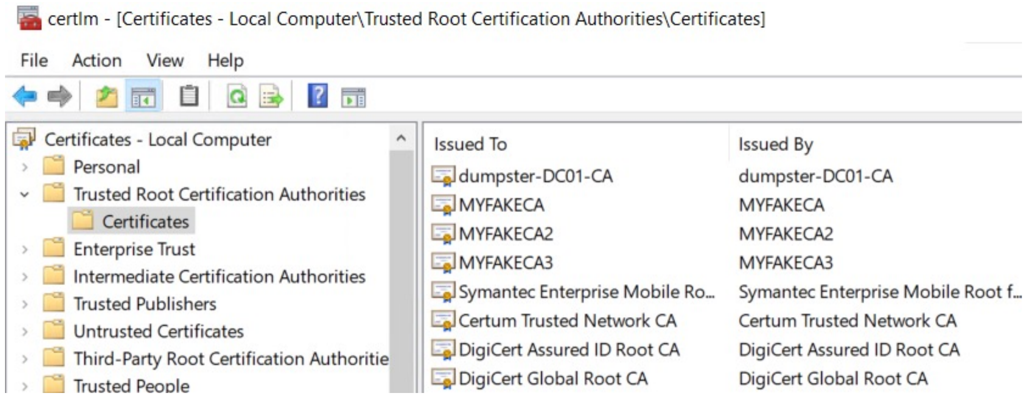
What is ADCS

- Root Certificate Authority
- Self-signed certificate (no issuer)
- Trusted by all computers in the forest
- Issues Enterprise CA certificates



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

Name	Class
CN=MYFAKECA3	certificationAuthority
CN=MYFAKECA2	certificationAuthority
CN=MYFAKECA	certificationAuthority
CN=dumpster-DC01-CA	certificationAuthority



certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]

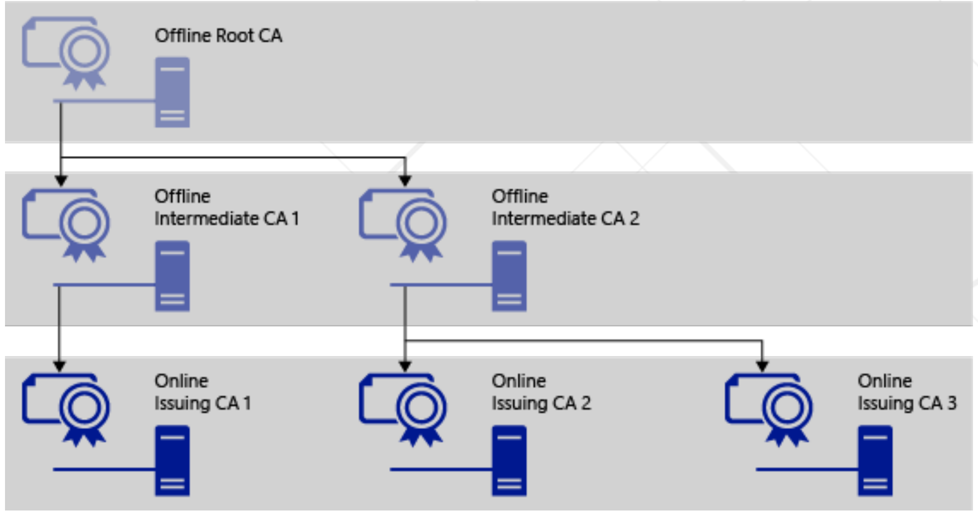
- Certificates - Local Computer
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authoritie
  - Trusted People

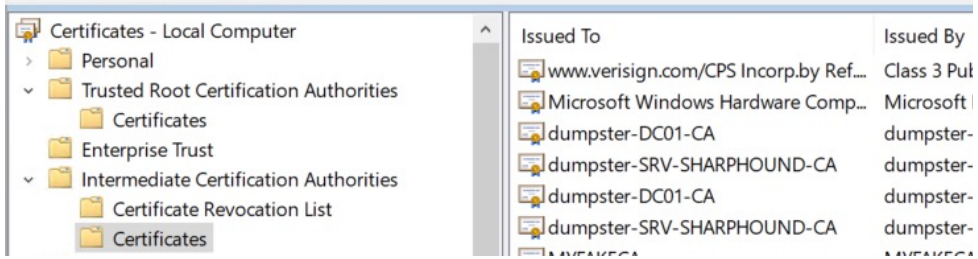
Issued To	Issued By
dumpster-DC01-CA	dumpster-DC01-CA
MYFAKECA	MYFAKECA
MYFAKECA2	MYFAKECA2
MYFAKECA3	MYFAKECA3
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...
Certum Trusted Network CA	Certum Trusted Network CA
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Global Root CA	DigiCert Global Root CA

ADCS components – EnterpriseCA

What is ADCS

- Aka enrollment service
- Certificate chains up to a RootCA
- Intermediate CAs and Issuing CAs = EnterpriseCAs
- Located in the “Enrollment Services” container
- Trusted by all computers in the forest



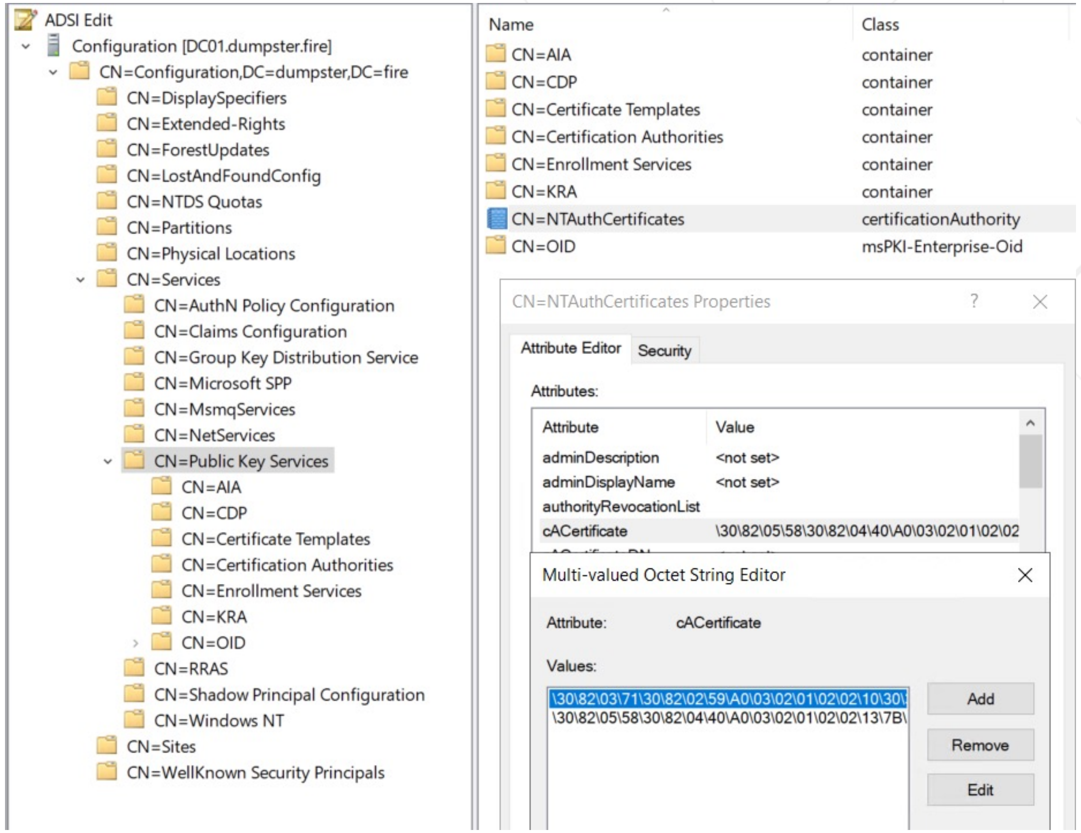

Certificates - Local Computer
- Personal
- Trusted Root Certification Authorities
  - Certificates
- Enterprise Trust
- Intermediate Certification Authorities
  - Certificate Revocation List
  - Certificates

Issued To	Issued By
www.verisign.com/CPS Incorp.by Ref...	Class 3 Pul
Microsoft Windows Hardware Comp...	Microsoft
dumpster-DC01-CA	dumpster-
dumpster-SRV-SHARPHOUND-CA	dumpster-
dumpster-DC01-CA	dumpster-
dumpster-SRV-SHARPHOUND-CA	dumpster-

ADCS components – NTAuthStore

What is ADCS

- EnterpriseCA must be trusted for NT authentication
- NTAuthCertificates object (aka NTAuth store)
- Replicated to the local NTAuth store on DCs



```
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
```

Name	Class
CN=AIA	container
CN=CDP	container
CN=Certificate Templates	container
CN=Certification Authorities	container
CN=Enrollment Services	container
CN=KRA	container
CN=NTAuthCertificates	certificationAuthority
CN=OID	msPKI-Enterprise-Oid

CN=NTAuthCertificates Properties

Attributes:

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
authorityRevocationList	
cACertificate	\30\82\05\58\30\82\04\40\A0\03\02\01\02\02

Multi-valued Octet String Editor

Attribute: cACertificate

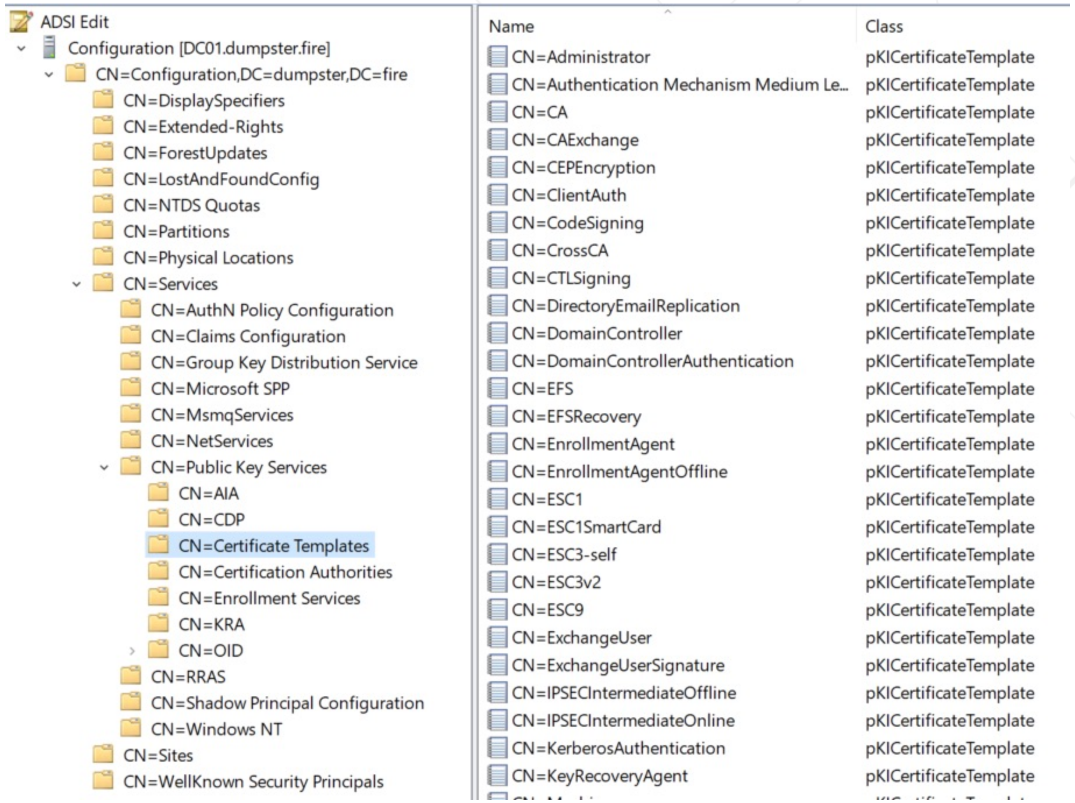
Values:

```
\30\82\03\71\30\82\02\59\A0\03\02\01\02\02\10\30\
\30\82\05\58\30\82\04\40\A0\03\02\01\02\02\13\7B\
```

ADCS components – CertTemplate

What is ADCS

- Used for certificate enrollment requests
- Holds characteristics of a certificate
  - Certificate usage
  - Validity period
  - And more..
- Published by EnterpriseCAs



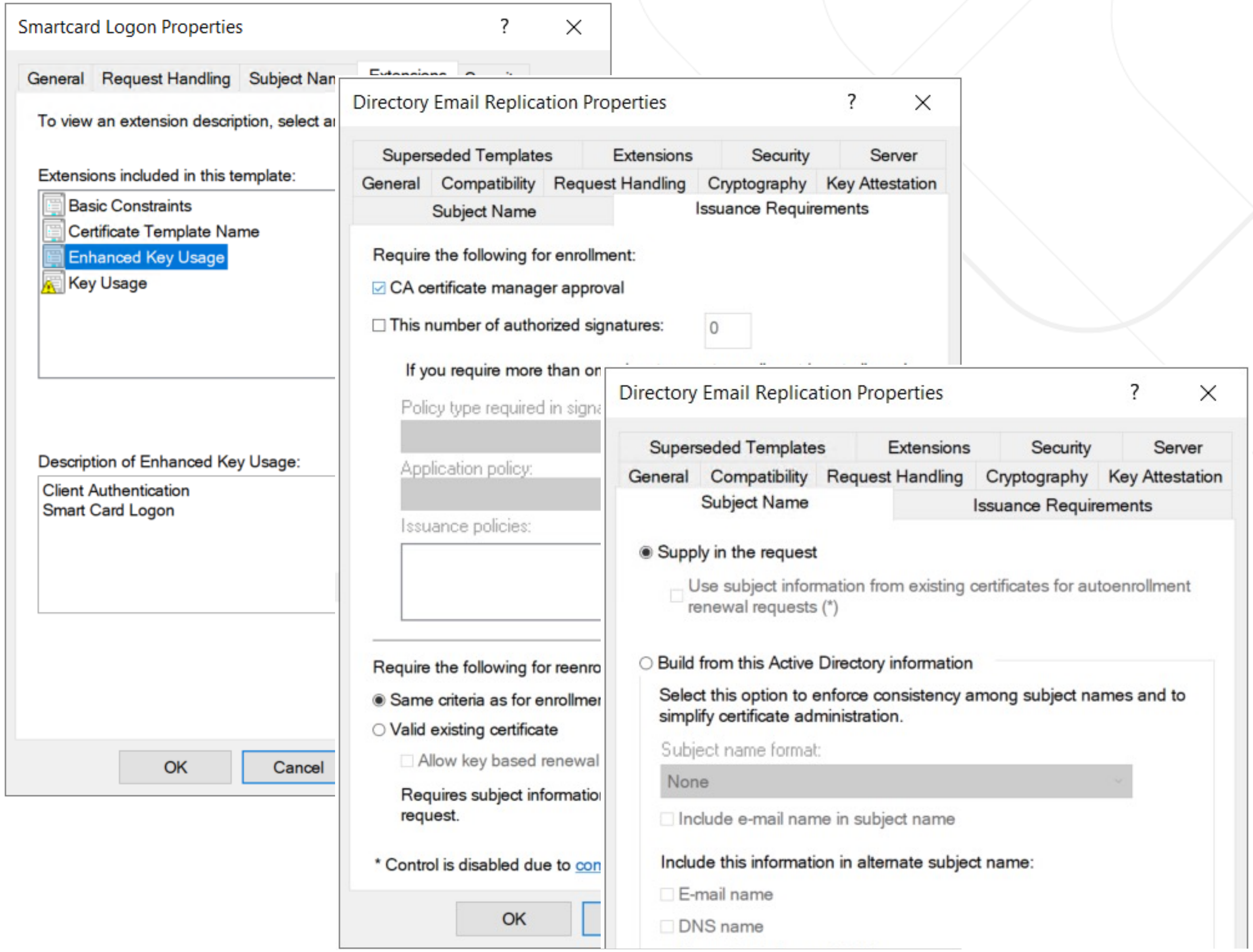
```
ADSI Edit
  Configuration [DC01.dumpster.fire]
    CN=Configuration,DC=dumpster,DC=fire
      CN=DisplaySpecifiers
      CN=Extended-Rights
      CN=ForestUpdates
      CN=LostAndFoundConfig
      CN=NTDS Quotas
      CN=Partitions
      CN=Physical Locations
      CN=Services
        CN=AuthN Policy 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
```

Name	Class
CN=Administrator	pKICertificateTemplate
CN=Authentication Mechanism Medium Le...	pKICertificateTemplate
CN=CA	pKICertificateTemplate
CN=CAExchange	pKICertificateTemplate
CN=CEPEncryption	pKICertificateTemplate
CN=ClientAuth	pKICertificateTemplate
CN=CodeSigning	pKICertificateTemplate
CN=CrossCA	pKICertificateTemplate
CN=CTLSigning	pKICertificateTemplate
CN=DirectoryEmailReplication	pKICertificateTemplate
CN=DomainController	pKICertificateTemplate
CN=DomainControllerAuthentication	pKICertificateTemplate
CN=EFS	pKICertificateTemplate
CN=EFSRecovery	pKICertificateTemplate
CN=EnrollmentAgent	pKICertificateTemplate
CN=EnrollmentAgentOffline	pKICertificateTemplate
CN=ESC1	pKICertificateTemplate
CN=ESC1SmartCard	pKICertificateTemplate
CN=ESC3-self	pKICertificateTemplate
CN=ESC3v2	pKICertificateTemplate
CN=ESC9	pKICertificateTemplate
CN=ExchangeUser	pKICertificateTemplate
CN=ExchangeUserSignature	pKICertificateTemplate
CN=IPSECIntermediateOffline	pKICertificateTemplate
CN=IPSECIntermediateOnline	pKICertificateTemplate
CN=KerberosAuthentication	pKICertificateTemplate
CN=KeyRecoveryAgent	pKICertificateTemplate

ADCS components – CertTemplate

What is ADCS

- Enhanced Key Usage (EKU)
    - Client Authentication (1.3.6.1.5.5.7.3.2)
    - PKINIT Client Authentication (1.3.6.1.5.2.3.4)
    - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
    - Any Purpose (2.5.29.37.0)
    - SubCA (no EKUs)
- Issuance requirements
    - Manager approval
    - Authorized signatures
- ENROLLEE_SUPPLIES_SUBJECT flag
    - Enroll as anyone 🔥



To view an extension description, select ar

Extensions included in this template:

- Basic Constraints
- Certificate Template Name
- Enhanced Key Usage
- Key Usage

Description of Enhanced Key Usage:

Client Authentication
Smart Card Logon

Require the following for enrollment:

☑ CA certificate manager approval

☐ This number of authorized signatures: 0

If you require more than on

Policy type required in signa

Application policy:

Issuance policies:

Require the following for reenro

● Same criteria as for enrollmer

○ Valid existing certificate

☐ Allow key based renewal

Requires subject informatio request.

* Control is disabled due to con

● 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

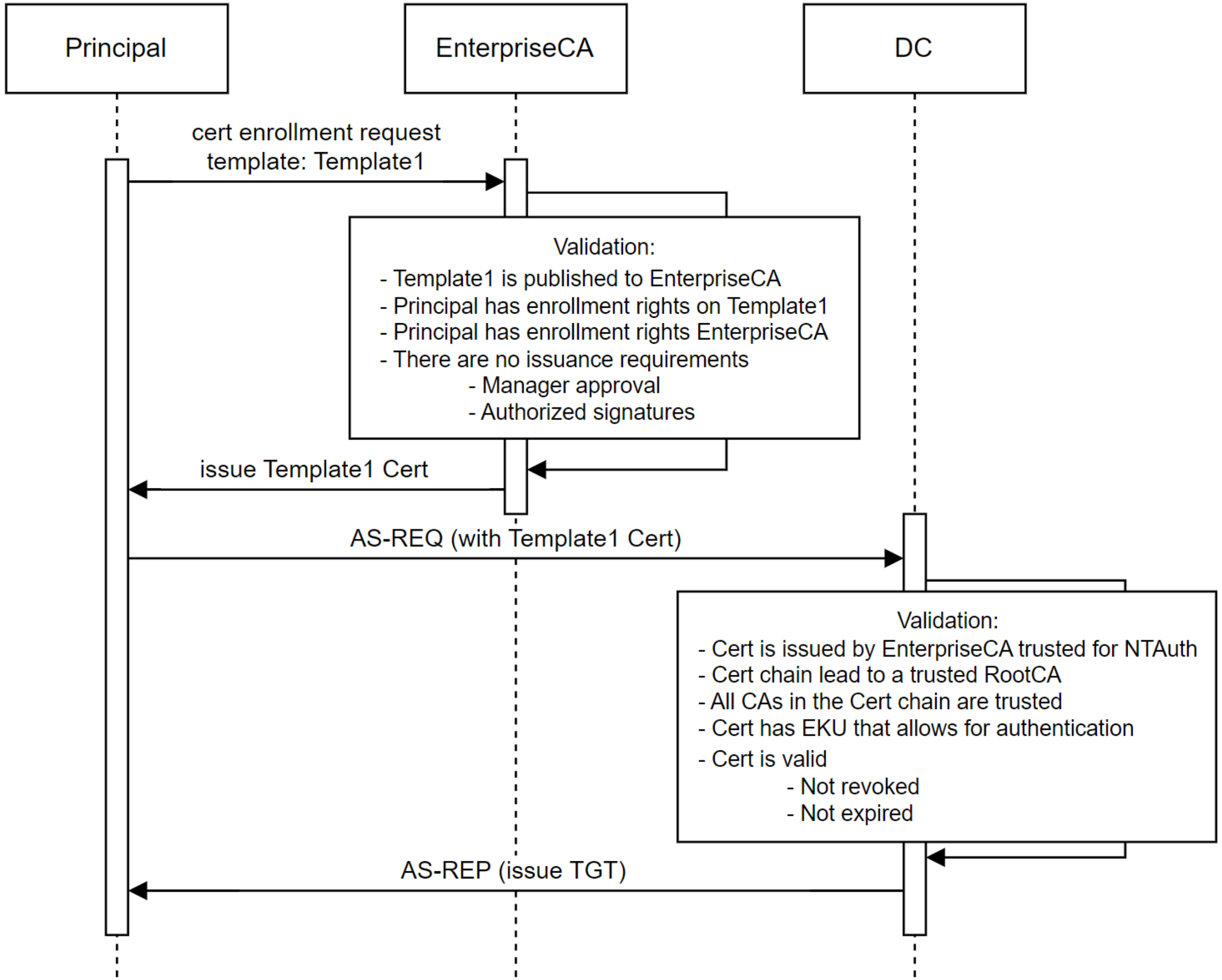
Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

Enrollment and authentication process (simplified)

What is ADCS



Validation:

- Template1 is published to EnterpriseCA
- Principal has enrollment rights on Template1
- Principal has enrollment rights EnterpriseCA
- There are no issuance requirements
  - Manager approval
  - Authorized signatures

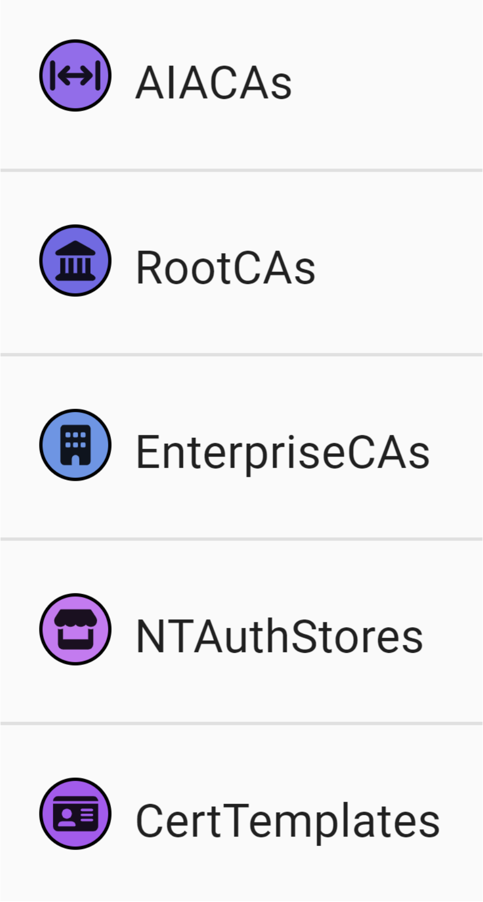
Validation:

- Cert is issued by EnterpriseCA trusted for NTAuth
- Cert chain lead to a trusted RootCA
- All CAs in the Cert chain are trusted
- Cert has EKU that allows for authentication
- Cert is valid
  - Not revoked
  - Not expired

ADCS components in BloodHound

New node types

ADCS components in BloodHound



AIACAs

RootCAs

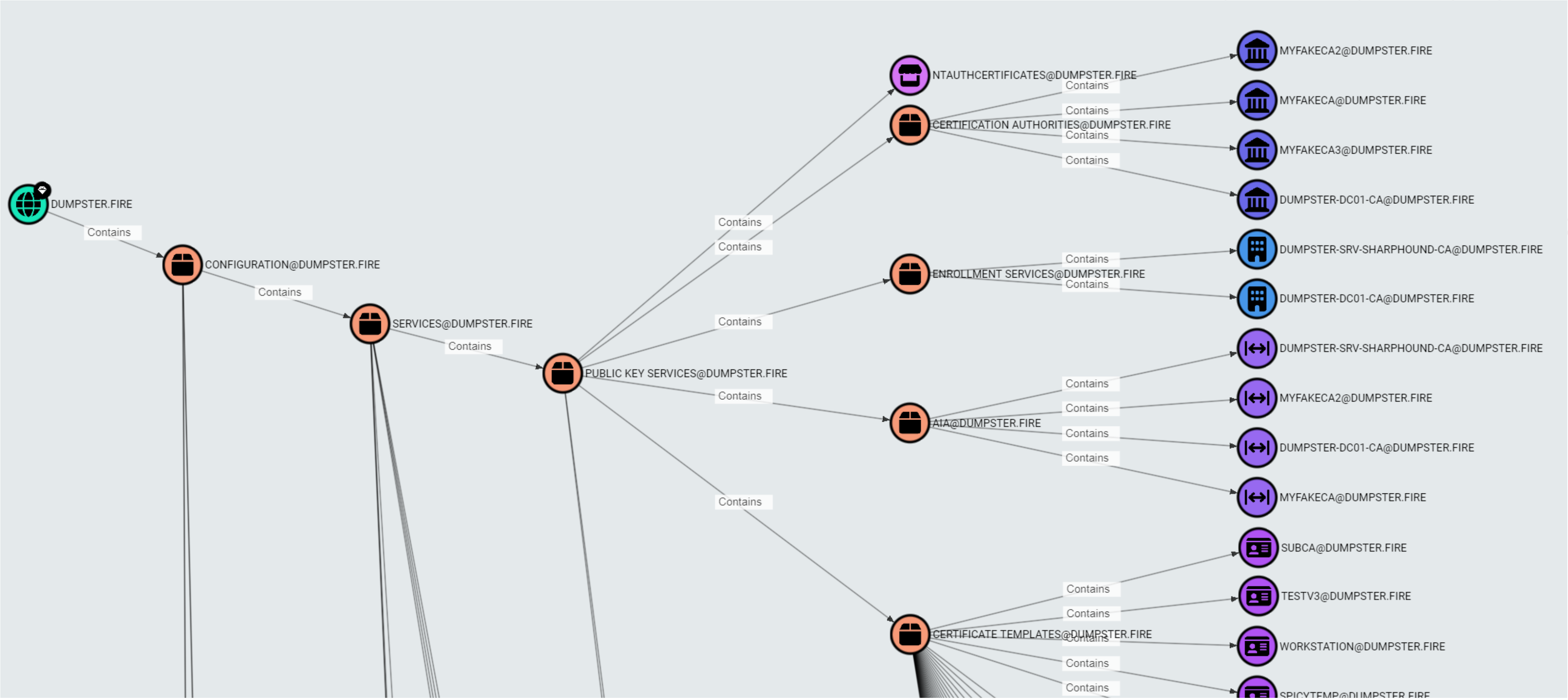
EnterpriseCAs

NTAuthStores

CertTemplates

New node types

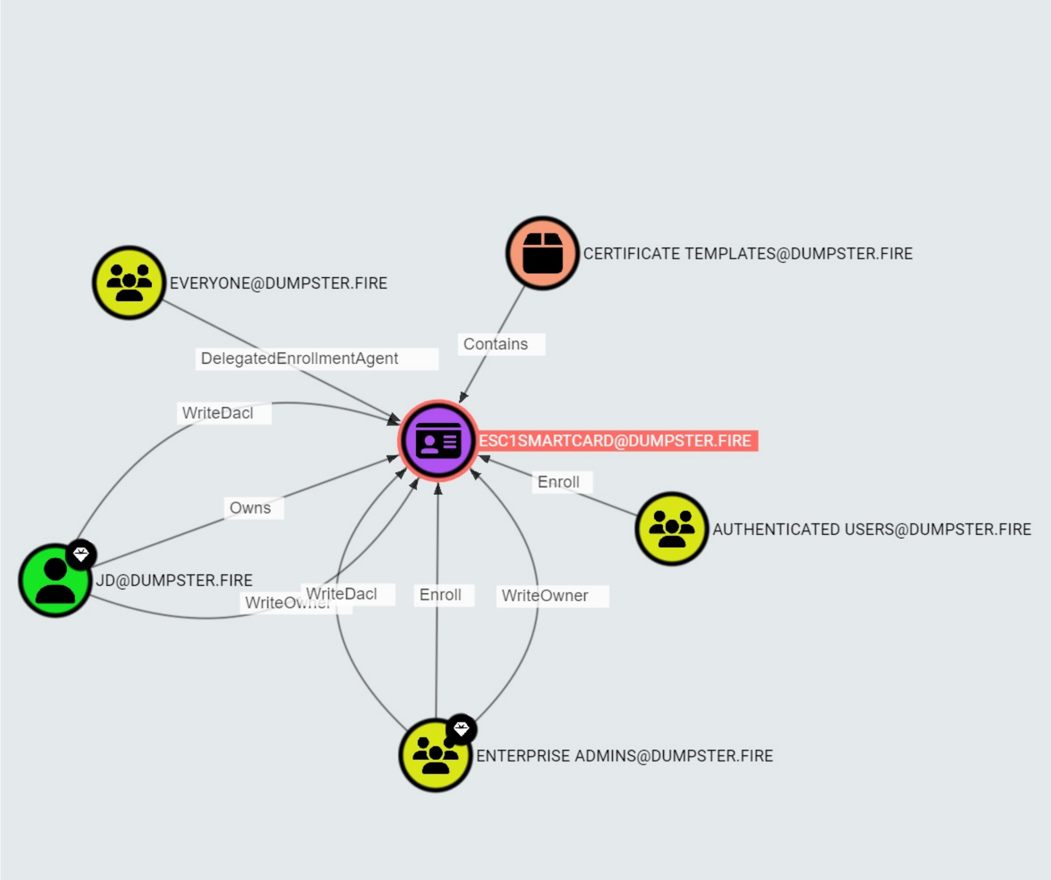
ADCS components in BloodHound

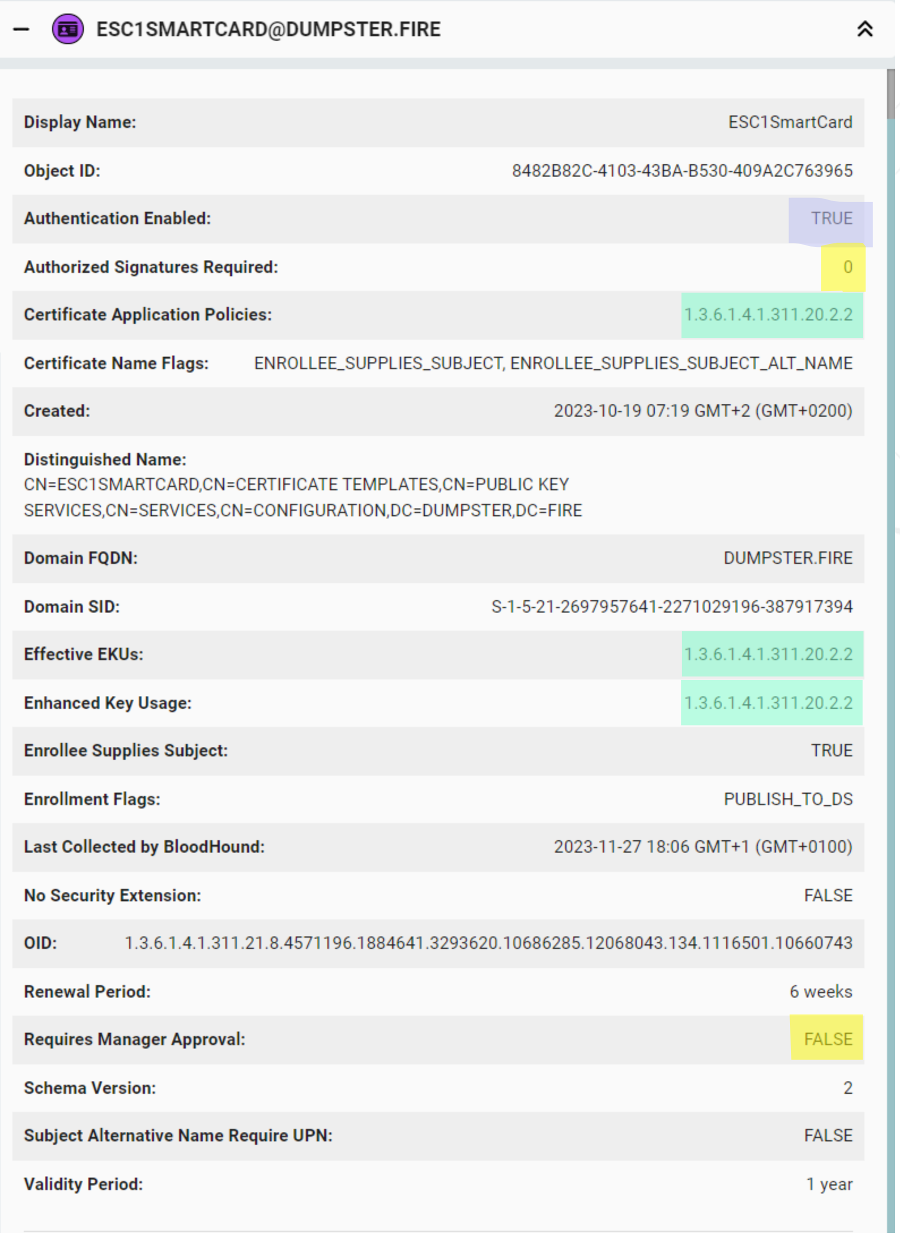


DUMPSTER.FIRE
Contains
CONFIGURATION@DUMPSTER.FIRE
Contains
SERVICES@DUMPSTER.FIRE
Contains
PUBLIC KEY SERVICES@DUMPSTER.FIRE
Contains
Contains
Contains
Contains
Contains
NTAUTHCERTIFICATES@DUMPSTER.FIRE
CERTIFICATION AUTHORITIES@DUMPSTER.FIRE
ENROLLMENT SERVICES@DUMPSTER.FIRE
AIA@DUMPSTER.FIRE
CERTIFICATE TEMPLATES@DUMPSTER.FIRE
Contains
MYFAKECA2@DUMPSTER.FIRE
MYFAKECA@DUMPSTER.FIRE
MYFAKECA3@DUMPSTER.FIRE
DUMPSTER-DC01-CA@DUMPSTER.FIRE
DUMPSTER-SRV-SHARPHOUND-CA@DUMPSTER.FIRE
DUMPSTER-DC01-CA@DUMPSTER.FIRE
DUMPSTER-SRV-SHARPHOUND-CA@DUMPSTER.FIRE
MYFAKECA2@DUMPSTER.FIRE
DUMPSTER-DC01-CA@DUMPSTER.FIRE
MYFAKECA@DUMPSTER.FIRE
SUBCA@DUMPSTER.FIRE
TESTV3@DUMPSTER.FIRE
WORKSTATION@DUMPSTER.FIRE
SPICYTEMP@DUMPSTER.FIRE

New node types

ADCS components in BloodHound


CERTIFICATE TEMPLATES@DUMPSTER.FIRE
EVERYONE@DUMPSTER.FIRE
Contains
DelegatedEnrollmentAgent
WriteDacl
ESC1SMARTCARD@DUMPSTER.FIRE
Enroll
Owns
AUTHENTICATED USERS@DUMPSTER.FIRE
JD@DUMPSTER.FIRE
WriteOwner
WriteDacl
Enroll
WriteOwner
ENTERPRISE ADMINS@DUMPSTER.FIRE


ESC1SMARTCARD@DUMPSTER.FIRE

Display Name:	ESC1SmartCard
Object ID:	8482B82C-4103-43BA-B530-409A2C763965
Authentication Enabled:	TRUE
Authorized Signatures Required:	0
Certificate Application Policies:	1.3.6.1.4.1.311.20.2.2
Certificate Name Flags:	ENROLLEE_SUPPLIES_SUBJECT, ENROLLEE_SUPPLIES_SUBJECT_ALT_NAME
Created:	2023-10-19 07:19 GMT+2 (GMT+0200)
Distinguished Name:	CN=ESC1SMARTCARD,CN=CERTIFICATE TEMPLATES,CN=PUBLIC KEY SERVICES,CN=SERVICES,CN=CONFIGURATION,DC=DUMPSTER,DC=FIRE
Domain FQDN:	DUMPSTER.FIRE
Domain SID:	S-1-5-21-2697957641-2271029196-387917394
Effective EKUs:	1.3.6.1.4.1.311.20.2.2
Enhanced Key Usage:	1.3.6.1.4.1.311.20.2.2
Enrollee Supplies Subject:	TRUE
Enrollment Flags:	PUBLISH_TO_DS
Last Collected by BloodHound:	2023-11-27 18:06 GMT+1 (GMT+0100)
No Security Extension:	FALSE
OID:	1.3.6.1.4.1.311.21.8.4571196.1884641.3293620.10686285.12068043.134.1116501.10660743
Renewal Period:	6 weeks
Requires Manager Approval:	FALSE
Schema Version:	2
Subject Alternative Name Require UPN:	FALSE
Validity Period:	1 year

New non-traversable edges

ADCS components in BloodHound

- RootCAFor
- EnterpriseCAFor
- NTAuthStoreFor
- PublishedTo
- ManageCertificates
- ManageCA
- DCFor
- CanAbuseUPNCertMapping
- CanAbuseWeakCertBinding

- Enroll
- HostsCAService
- WritePKIEnrollmentFlag
- WritePKINameFlag
- IssuedSignedBy
- EnrollOnBehalfOf
- DelegatedEnrollmentAgent
- TrustedForNTAuth

What is a non-traversable edge?

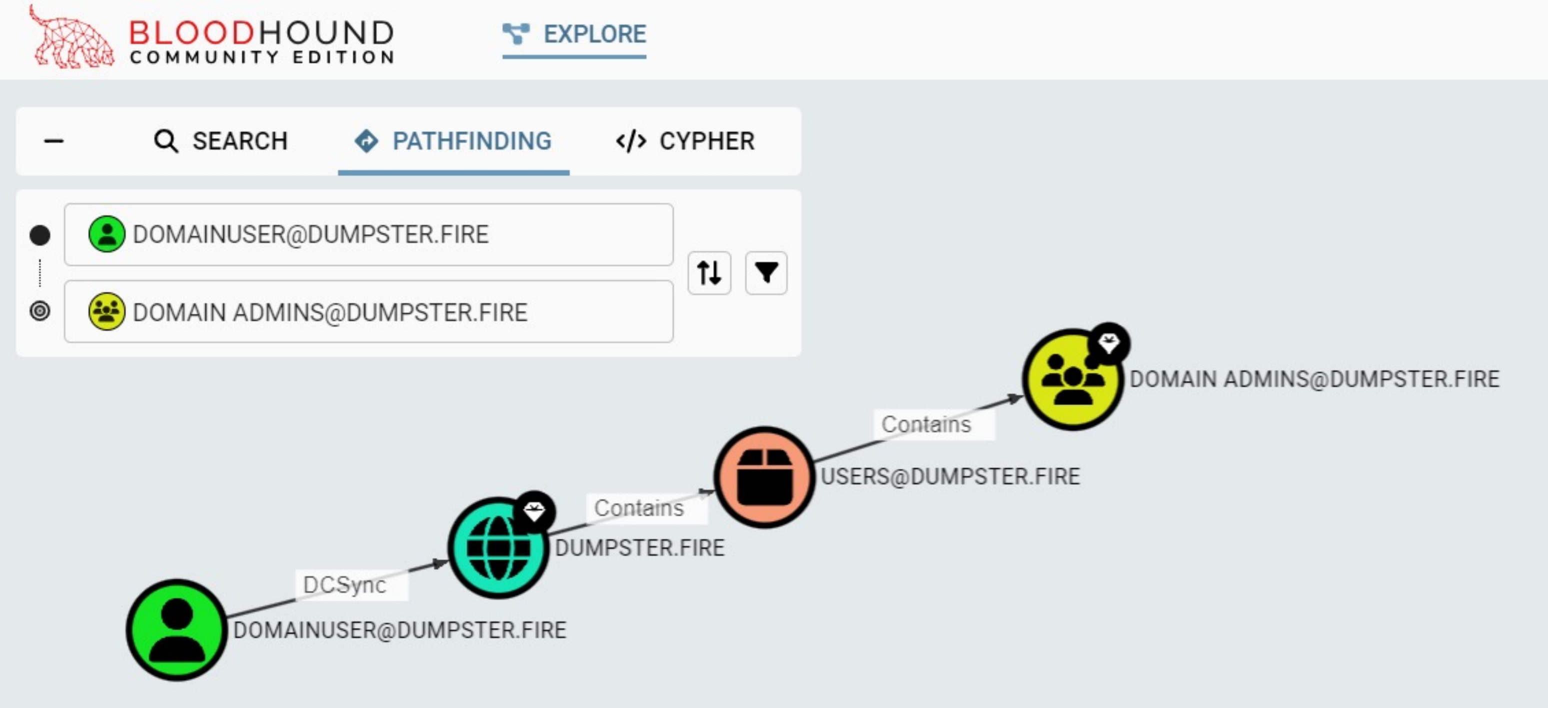
ADCS components in BloodHound

- Privileges and relationships that are not abusable on their own
- Excluded from path-finding
- Used to construct abusable (traversable) edges
- Example: GetChanges + GetChangesAll = DCSync

What is a non-traversable edge?

ADCS components in BloodHound

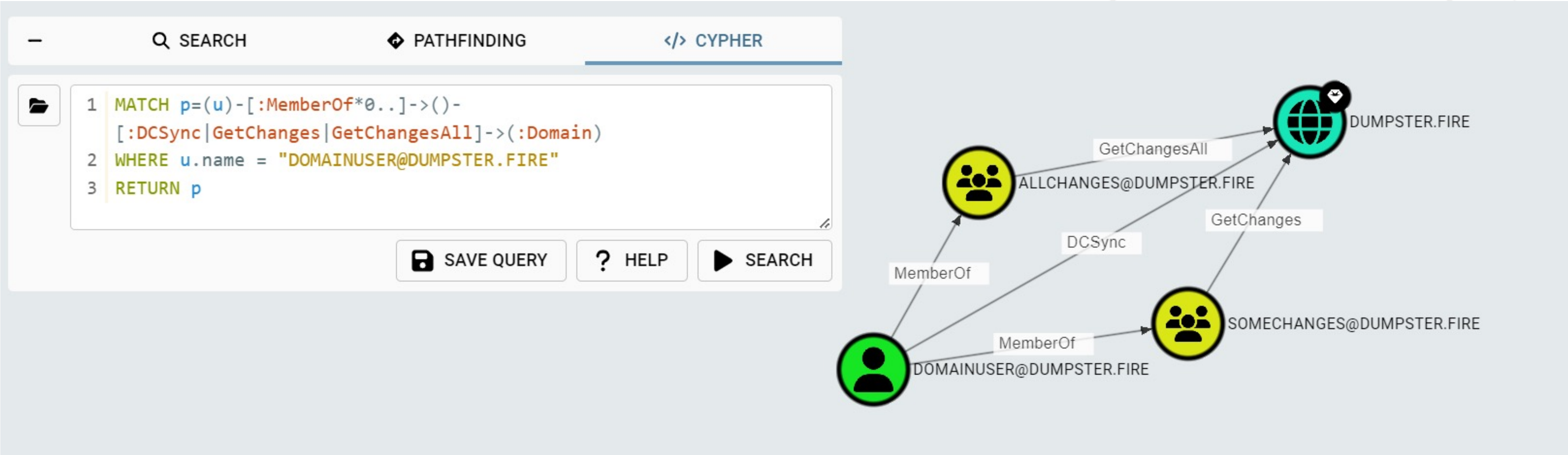
- Example: GetChanges + GetChangesAll = DCSync



What is a non-traversable edge?

ADCS components in BloodHound

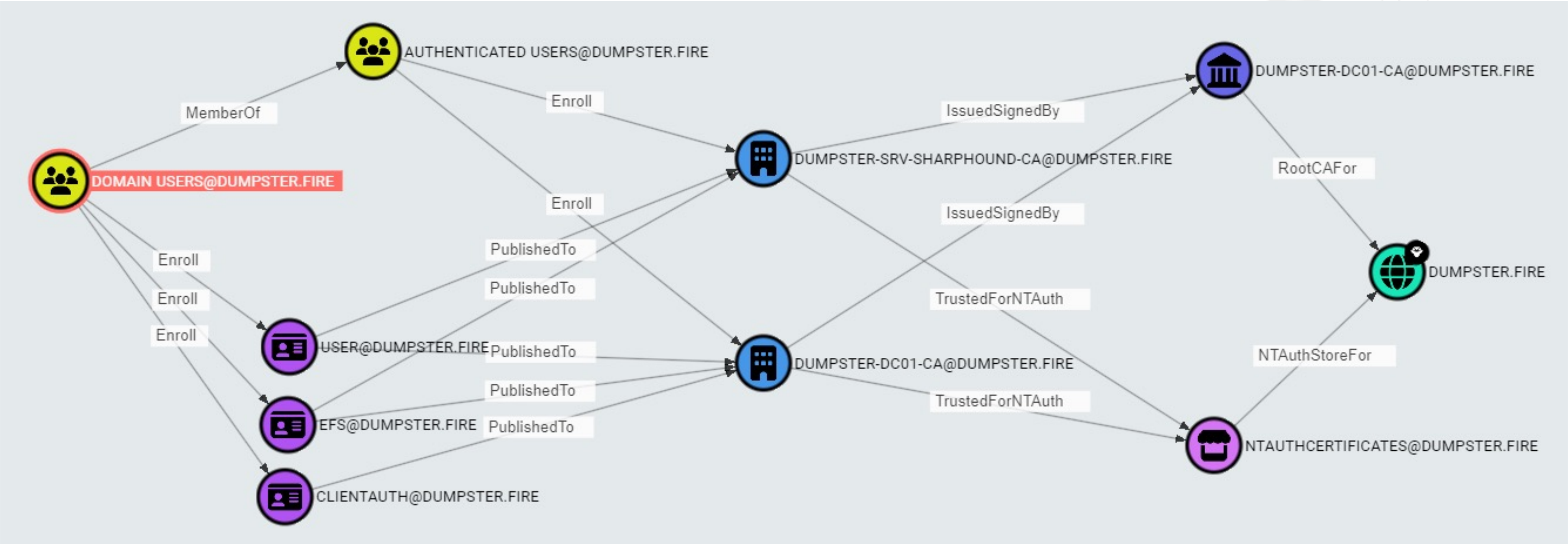
- Example: GetChanges + GetChangesAll = DCSync



```
MATCH p=(u)-[:MemberOf*0..]->()-[:DCSync|GetChanges|GetChangesAll]->(:Domain)
WHERE u.name = "DOMAINUSER@DUMPSTER.FIRE"
RETURN p
```

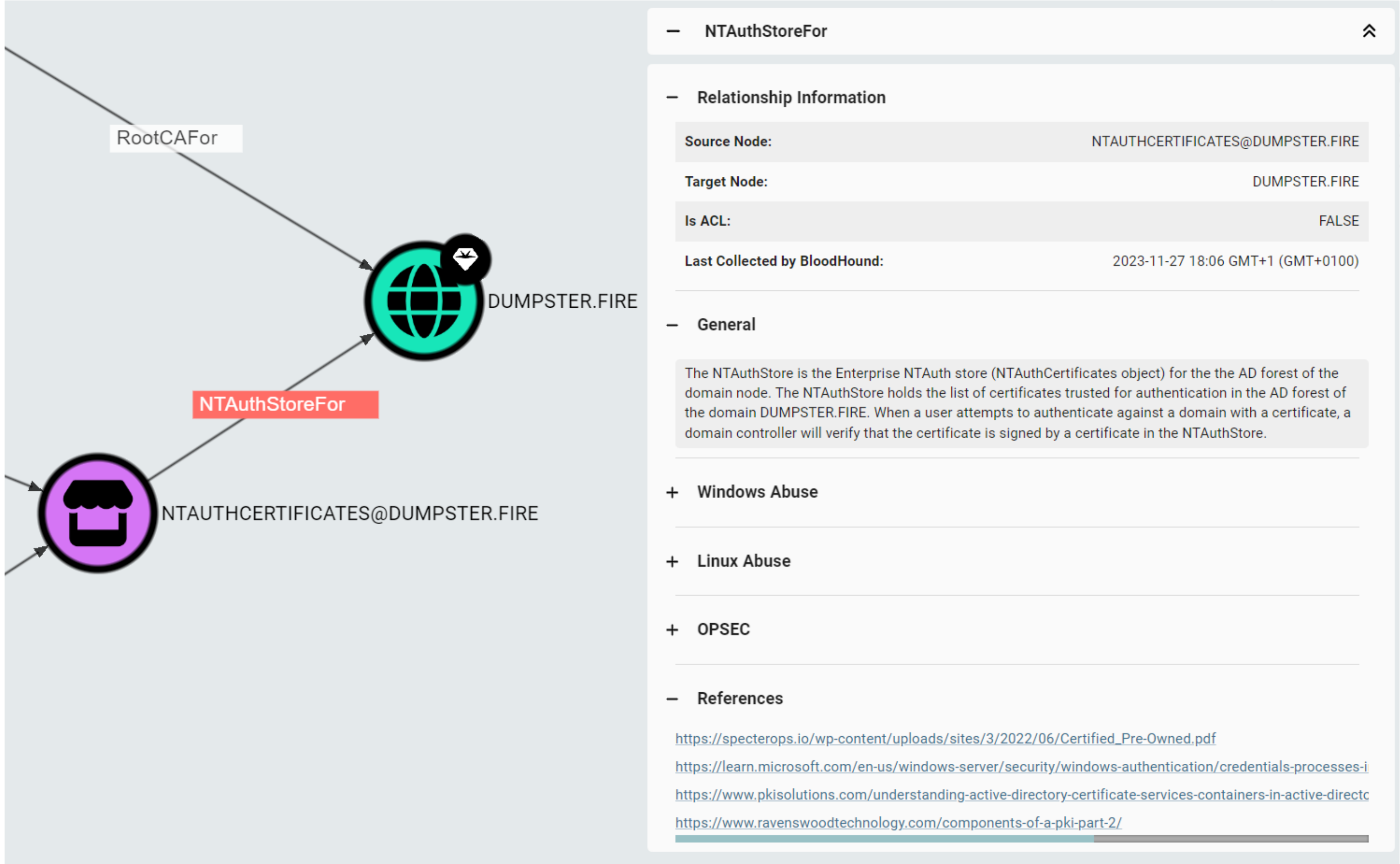
New non-traversable edges

ADCS components in BloodHound



New non-traversable edges

ADCS attack paths in BloodHound



NTAuthStoreFor

Relationship Information

Source Node:	NTAUTHCERTIFICATES@DUMPSTER.FIRE
Target Node:	DUMPSTER.FIRE
Is ACL:	FALSE
Last Collected by BloodHound:	2023-11-27 18:06 GMT+1 (GMT+0100)

General

The NTAuthStore is the Enterprise NTAuth store (NTAuthCertificates object) for the the AD forest of the domain node. The NTAuthStore holds the list of certificates trusted for authentication in the AD forest of the domain DUMPSTER.FIRE. When a user attempts to authenticate against a domain with a certificate, a domain controller will verify that the certificate is signed by a certificate in the NTAuthStore.

+ Windows Abuse

+ Linux Abuse

+ OPSEC

References

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf
https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-i
https://www.pkisolutions.com/understanding-active-directory-certificate-services-containers-in-active-directc
https://www.ravenswoodtechnology.com/components-of-a-pki-part-2/

Demo Time!

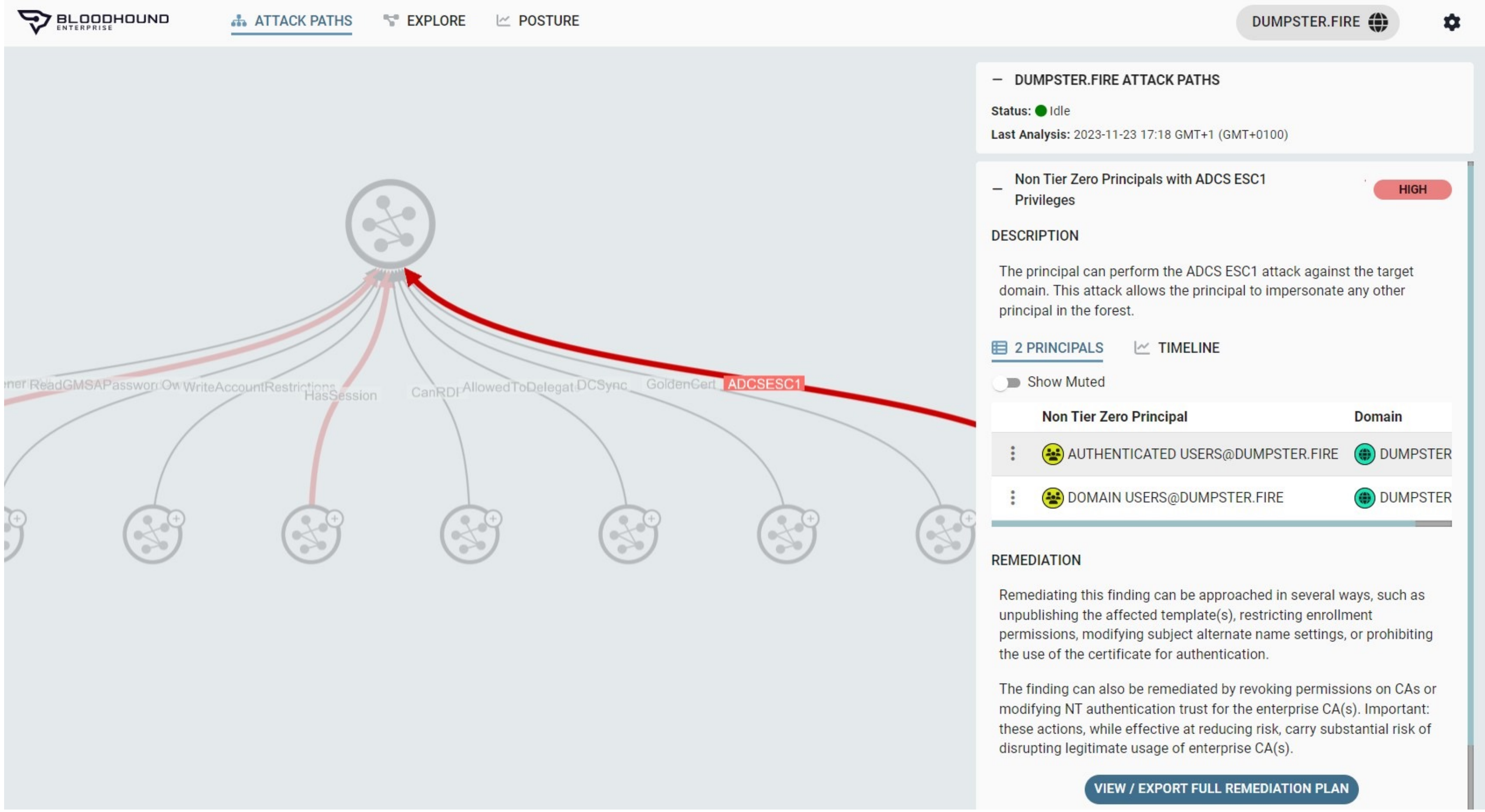
ADCS ESC1

- **Status:** we're very close to shipping this.
- Let's get into the demo!

ADCS in BloodHound Enterprise

New findings

ADCS attack paths in BloodHound



DUMPSTER.FIRE ATTACK PATHS

Status: ● Idle

Last Analysis: 2023-11-23 17:18 GMT+1 (GMT+0100)

Non Tier Zero Principals with ADCS ESC1 Privileges HIGH

DESCRIPTION

The principal can perform the ADCS ESC1 attack against the target domain. This attack allows the principal to impersonate any other principal in the forest.

2 PRINCIPALS TIMELINE

Show Muted

Non Tier Zero Principal	Domain
AUTHENTICATED USERS@DUMPSTER.FIRE	DUMPSTER
DOMAIN USERS@DUMPSTER.FIRE	DUMPSTER

REMEDIATION

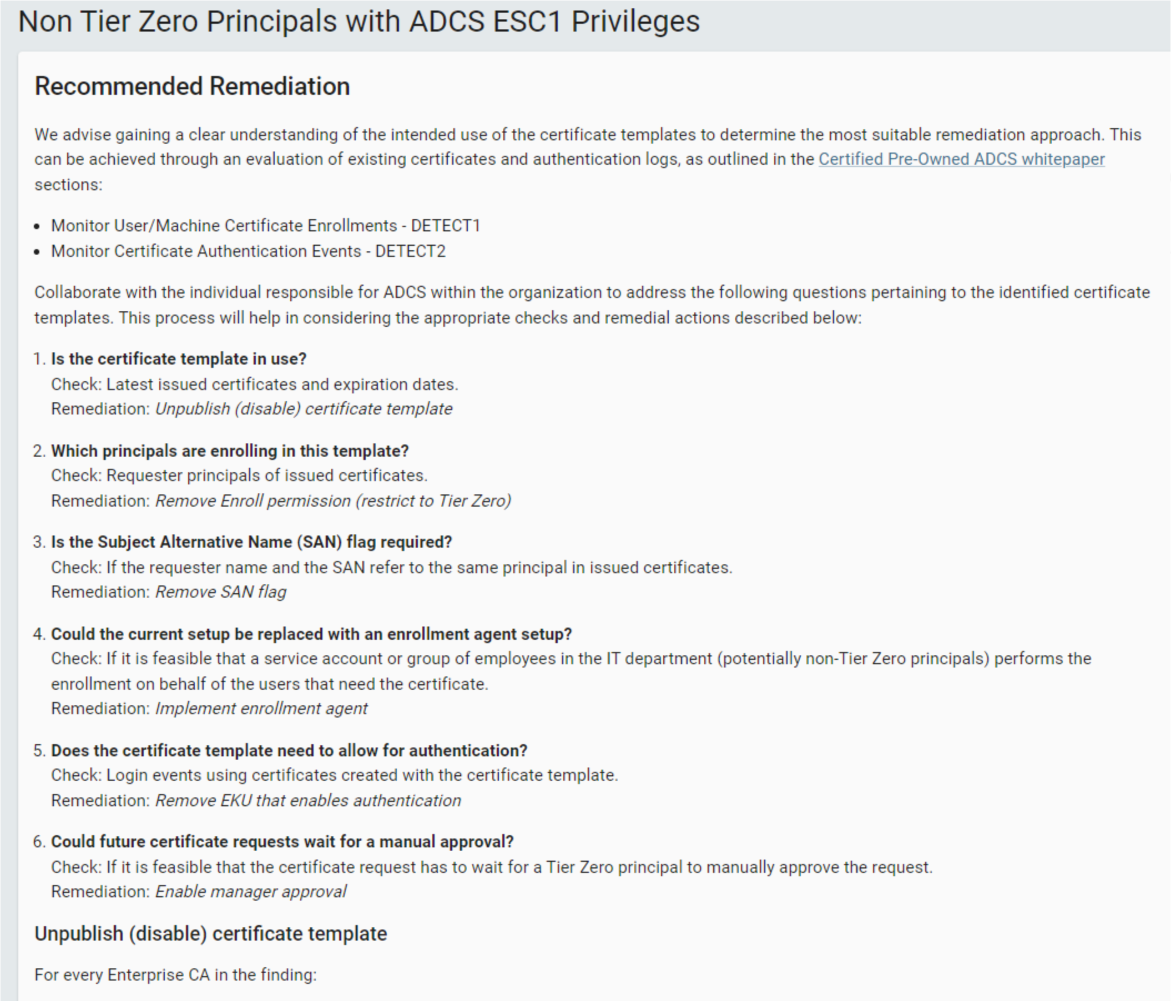
Remediating this finding can be approached in several ways, such as unpublishing the affected template(s), restricting enrollment permissions, modifying subject alternate name settings, or prohibiting the use of the certificate for authentication.

The finding can also be remediated by revoking permissions on CAs or modifying NT authentication trust for the enterprise CA(s). Important: these actions, while effective at reducing risk, carry substantial risk of disrupting legitimate usage of enterprise CA(s).

VIEW / EXPORT FULL REMEDIATION PLAN

New remediations

ADCS attack paths in BloodHound



Non Tier Zero Principals with ADCS ESC1 Privileges

Recommended Remediation

We advise gaining a clear understanding of the intended use of the certificate templates to determine the most suitable remediation approach. This can be achieved through an evaluation of existing certificates and authentication logs, as outlined in the Certified Pre-Owned ADCS whitepaper sections:

- Monitor User/Machine Certificate Enrollments - DETECT1
- Monitor Certificate Authentication Events - DETECT2

Collaborate with the individual responsible for ADCS within the organization to address the following questions pertaining to the identified certificate templates. This process will help in considering the appropriate checks and remedial actions described below:

1. **Is the certificate template in use?**
   Check: Latest issued certificates and expiration dates.
   Remediation: *Unpublish (disable) certificate template*
2. **Which principals are enrolling in this template?**
   Check: Requester principals of issued certificates.
   Remediation: *Remove Enroll permission (restrict to Tier Zero)*
3. **Is the Subject Alternative Name (SAN) flag required?**
   Check: If the requester name and the SAN refer to the same principal in issued certificates.
   Remediation: *Remove SAN flag*
4. **Could the current setup be replaced with an enrollment agent setup?**
   Check: If it is feasible that a service account or group of employees in the IT department (potentially non-Tier Zero principals) performs the enrollment on behalf of the users that need the certificate.
   Remediation: *Implement enrollment agent*
5. **Does the certificate template need to allow for authentication?**
   Check: Login events using certificates created with the certificate template.
   Remediation: *Remove EKU that enables authentication*
6. **Could future certificate requests wait for a manual approval?**
   Check: If it is feasible that the certificate request has to wait for a Tier Zero principal to manually approve the request.
   Remediation: *Enable manager approval*

Unpublish (disable) certificate template

For every Enterprise CA in the finding:

Acknowledgements

Acknowledgements

- Oliver Lyak – Offensive Expert @ Institute for Cyber Risk
- Jean Marsault – Manager @ Wavestone
- Benjamin Delpy – Creator of Mimikatz, Chef de Service d'ARCOS @ Banqe de France
- Christoph Falta
- Maciej Kosz - IT Security Officer @ Vattenfalland
- Mike Jankowski-Lorek – Cyber Security Architect @ CQURE
- Elke Stangl – Engineer @ punktwissen Proyer & Stangl OG
- Carl Sörqvist - Senior Consultant @ Bitoba
- Ceri Coburn – Red Team Operator & Offensive Security Dev @ Pen Test Partners
- Brad Hill – Software Engineer @ Meta
- Keyfactor Technical Team
- Mark Gamache – Principal Cryptography Engineer @ Salesforce
- Daniel Scheidt – Pentester @ Vorwerk Gruppe
- Vadims Podāns - PKI Consultant @ PKI Solutions Inc.
- Andrea Pierini – Senior Incident Response Consultant @ Semperis
- Charlie Clark – Senior Security Consultant @ MDSec
- Will Schroeder – Researcher @ SpecterOps
- Lee Christensen – Researcher @ SpecterOps
- BloodHound Enterprise Team @ SpecterOps

BLOODHOUND
ENTERPRISE

Thank you

Join us in the BloodHoundGang Slack: https://join.slack.com/t/bloodhoundhq/shared_invite/zt-28t90wqao-VC9uT~U2WPOtEup~aFH0Yw