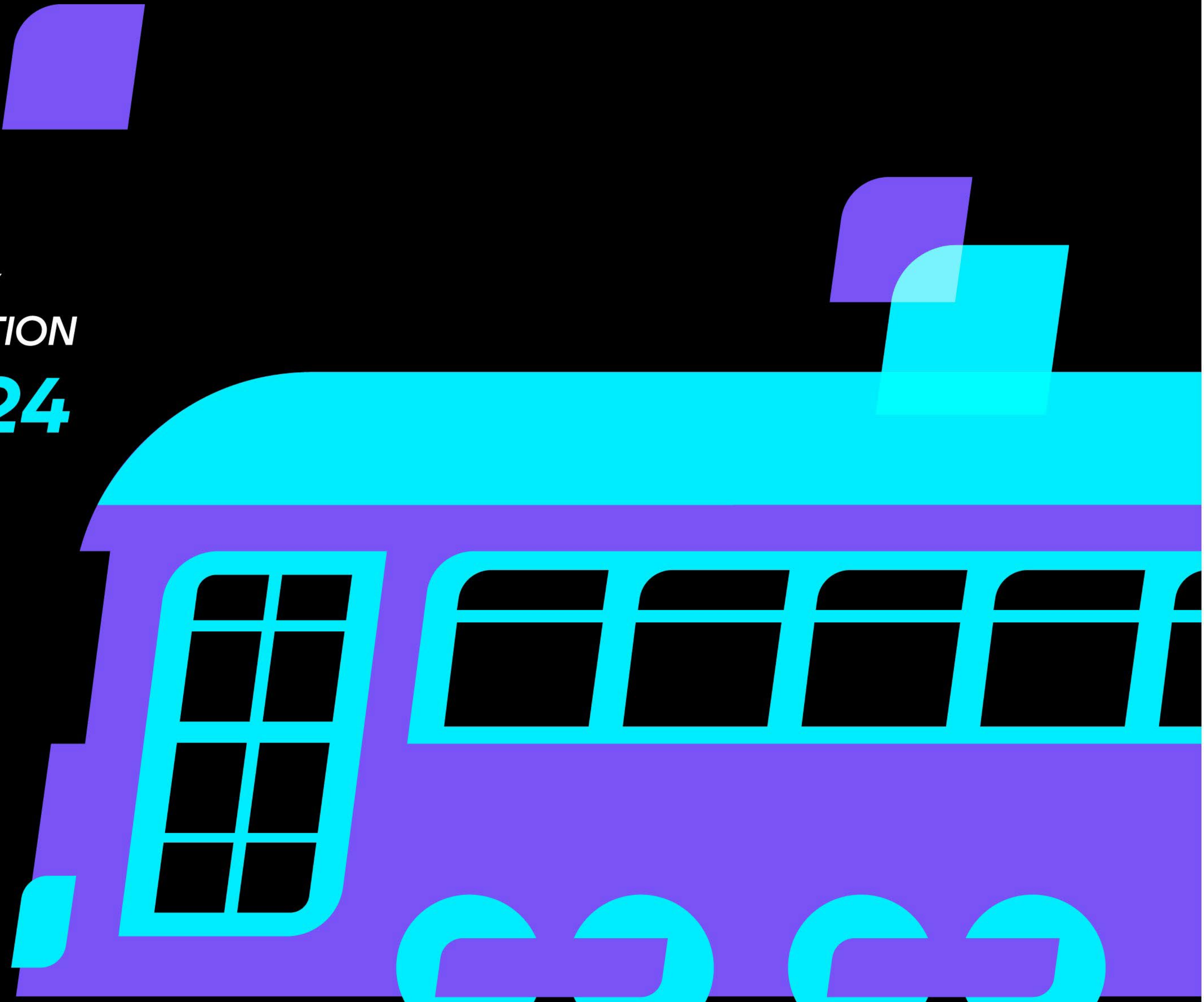
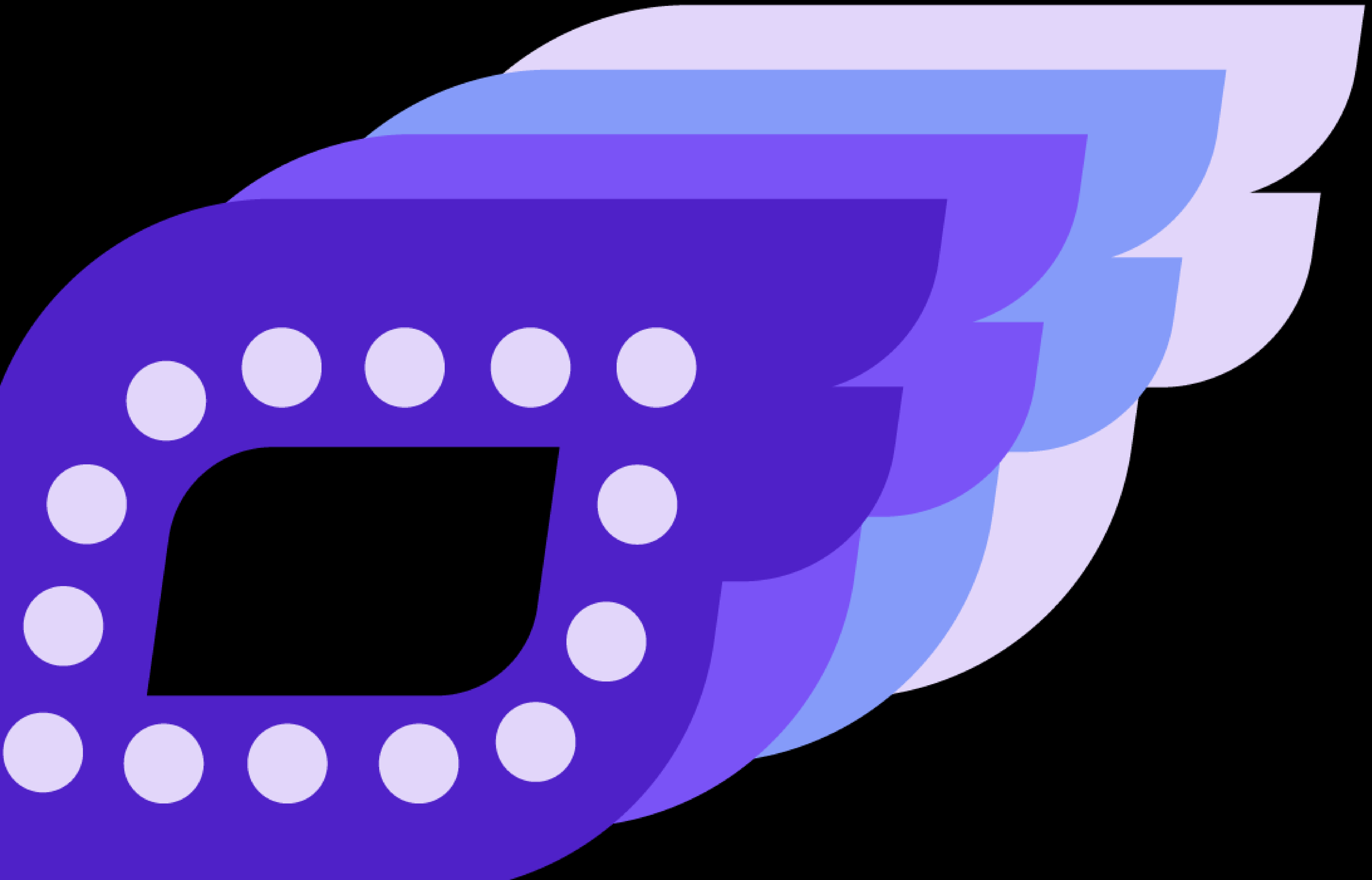
HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS



HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS



When your Enterprise PKI becomes one of your enemies

Christoffer Andersson

Principal Advisor – Epical

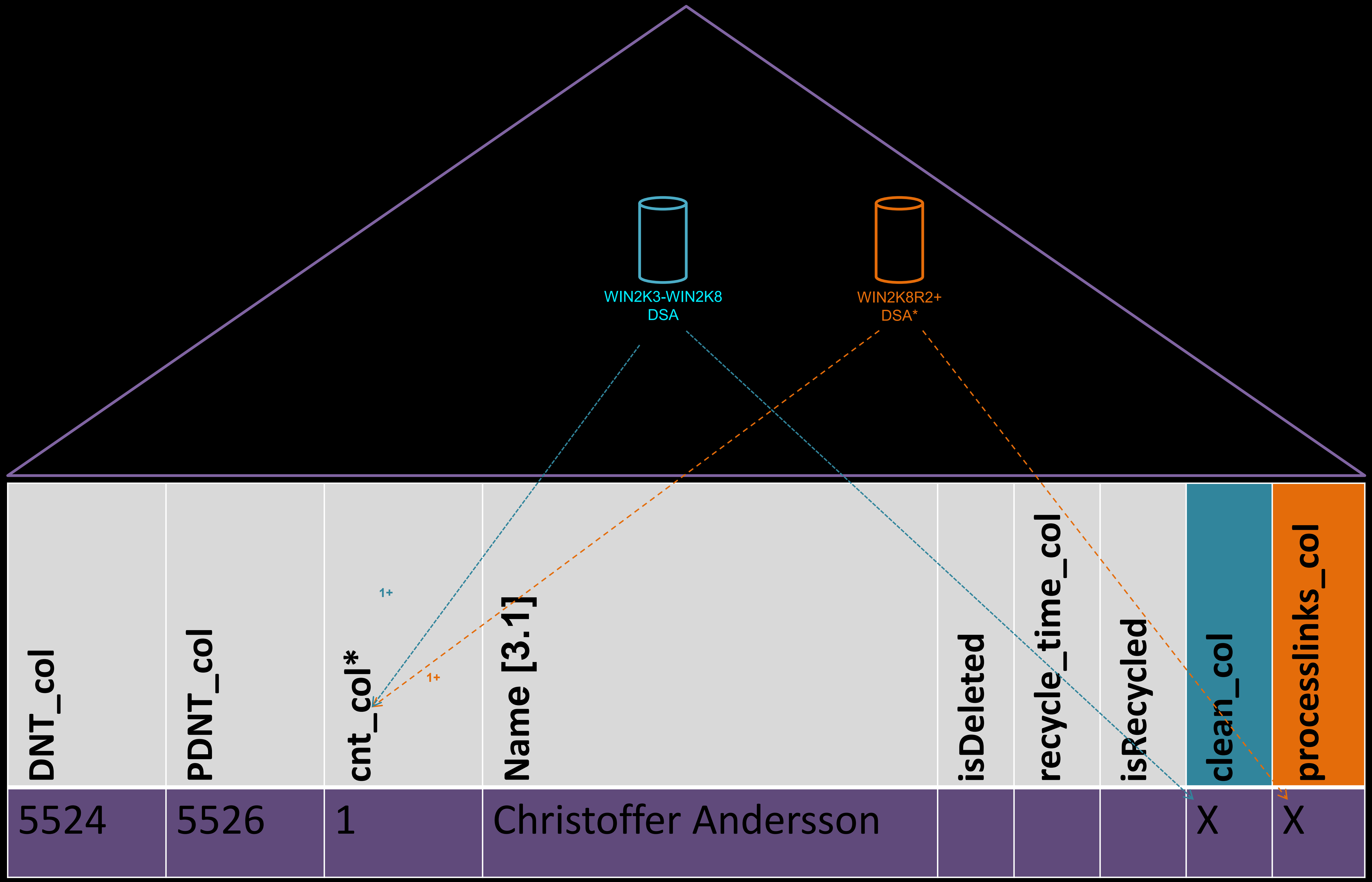
Who am I – Christoffer Andersson

- 38 years old from Sweden – Directory Services/AD Geek at source code level
- Principal Advisor at Epical Sweden – Previously Enfo Sweden
- Former Microsoft Most Valuable Professional (MVP) in Directory Services (2004-2011)
- Microsoft Most Valuable Researcher (MVR 2023)
- Working with Active Directory, PKI and Security for Critical Infrastructure daily

What you might know me from?

Delayed Link Processing

- Semantics
  - 10,000 links are processed in a single transaction, if there is more links – Delayed link processing is taking place
- Operations:
  - Remove forward links
  - Remove backward links
  - Deactivate links
  - Activate links
  - Authoritative restore (touch metadata)



DNT_col	PDNT_col	cnt_col*	Name [3.1]	isDeleted	recycle_time_col	isRecycled	clean_col	processlinks_col
5524	5526	1	Christoffer Andersson				X	X

The link cleaner and the delayed link processing mechanism uses prevents the object they are working on – from being physically deleted before they are done by increasing the ‘cnt_col’ with + 1. and decreasing it with -1. once there is no more work left to perform.

So, you have an ’Enterprise’ CA?

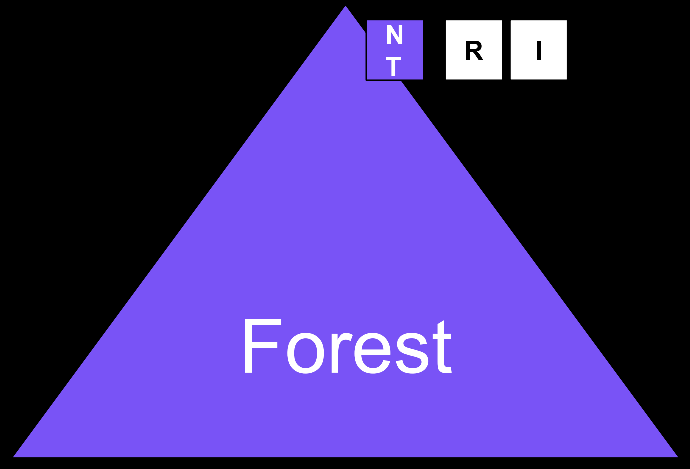
- It was created by first establishing CP (Certificate Policy) and Certificate Practice Statement (CPS) a ceremony was held, and the private key was generated in a HSM?

- Or someone/something needed a certificate? And a next, next finish CA was established?

Trusted for Authentication against AD?

NTAuth

- Trusted in NTAuth
- UPN
- Verify chain on DCs/KDCs
- Verify chain on Clients
- Contain SID Extension or SID in SAN (Only 2019 KDCs+)



SChannel

- Subject/Issuer certificate mapping
- Issuer certificate mapping
- UPN certificate mapping
- S4U2Self certificate mapping (NTAuth + SID)
- S4U2Self explicit certificate mapping (AltSecID)

AltSecID

- Verify chain on DCs/KDCs
- Verify chain on Clients
- ‘altSecurityIdentities’
  - X509IssuerSubject
  - X509SubjectOnly
  - X509RFC822
  - X509IssuerSerialNumber
  - X509SKI
  - X509SHA1PublicKey

* Strong Certificate Binding Enforcement

Let’s have a look at NTAuth

- CN=NTAuth,CN=Public Key Services,CN=Services,DC=Configuration,DC=X
  - cACertificate

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates\NTAuth\Certificates
  - <Thumbprint>

- Group Policy Autoenrollment CSE
  - Supposed to cache the content from AD to the Registry on each domain joined machine within the forest (Including DCs).

- The easy way: Get-EnterpriseCertificateStore
  https://github.com/CarlSorqvist/PsCertTools

Who validates against NTAuth?

- KDC/PKINIT unless altSecIDs
- LDAP-STARTTLS
- Enrollment of templates that have private key archival enabled
- NPS - Schannel
- IIS – Schannel
- ADFS? Yep regardless of altSecIDs
- …

How is a check against NTAuth performed?

- If we’re online we’re taking a trip to CN=NTAuth,CN=Public Key Services,CN=Services,DC=Configuration,DC=X right?

- Nope – We’re calling into crypt32.dll?CertVerifyCertificateChainPolicy with the ‘CERT_CHAIN_POLICY_NT_AUTH’ flag

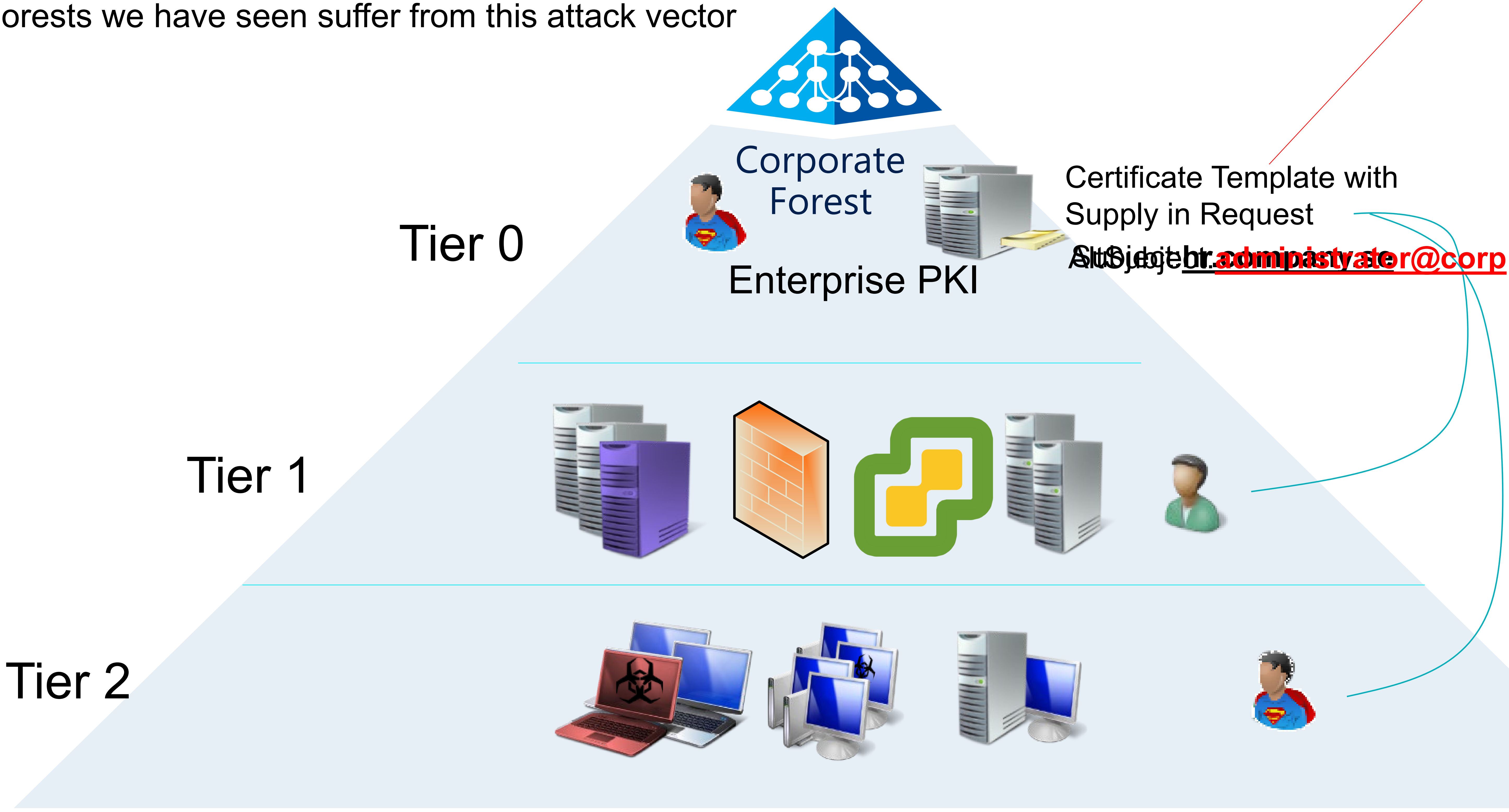
```
BOOL CertVerifyCertificateChainPolicy( [in] LPCSTR pszPolicyOID,
[in] PCCERT_CHAIN_CONTEXT pChainContext, [in]
PCERT_CHAIN_POLICY_PARA pPolicyPara, [in, out]
PCERT_CHAIN_POLICY_STATUS pPolicyStatus );
```

- Easy way - PowerShell: Test-Certificate -Cert $cert -Policy NTAUTH

HKLM\SOFTWARE\Microsoft\
EnterpriseCertificates\NTAuth\Certificates

Forest Compromise and Tier Lateral movement using PKI

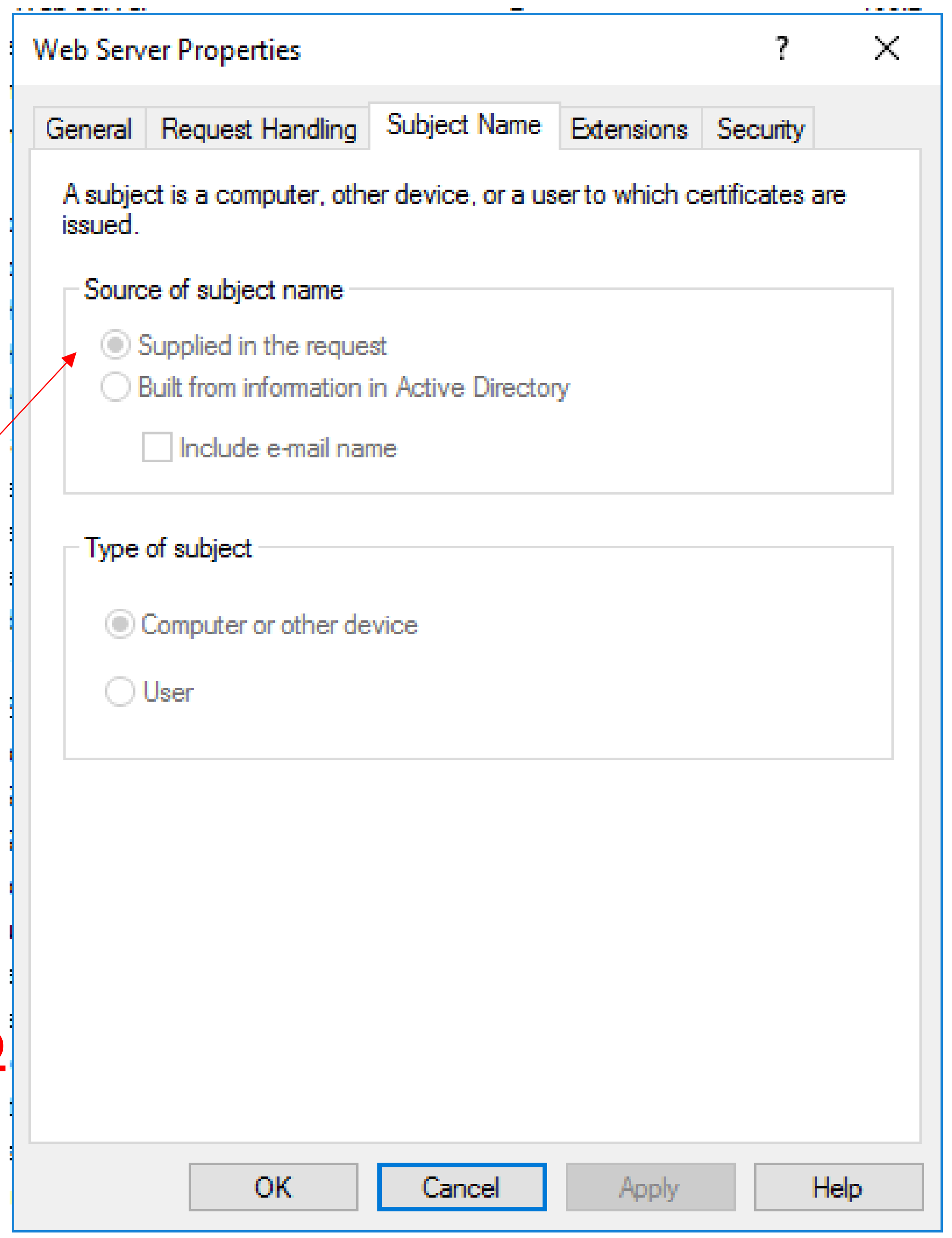
93% of all Forests we have seen suffer from this attack vector



Certificate Template with Supply in Request

Subject: dr.company.se

AltSubject: administrator@corp



A subject is a computer, other device, or a user to which certificates are issued.

Source of subject name

● Supplied in the request

○ Built from information in Active Directory

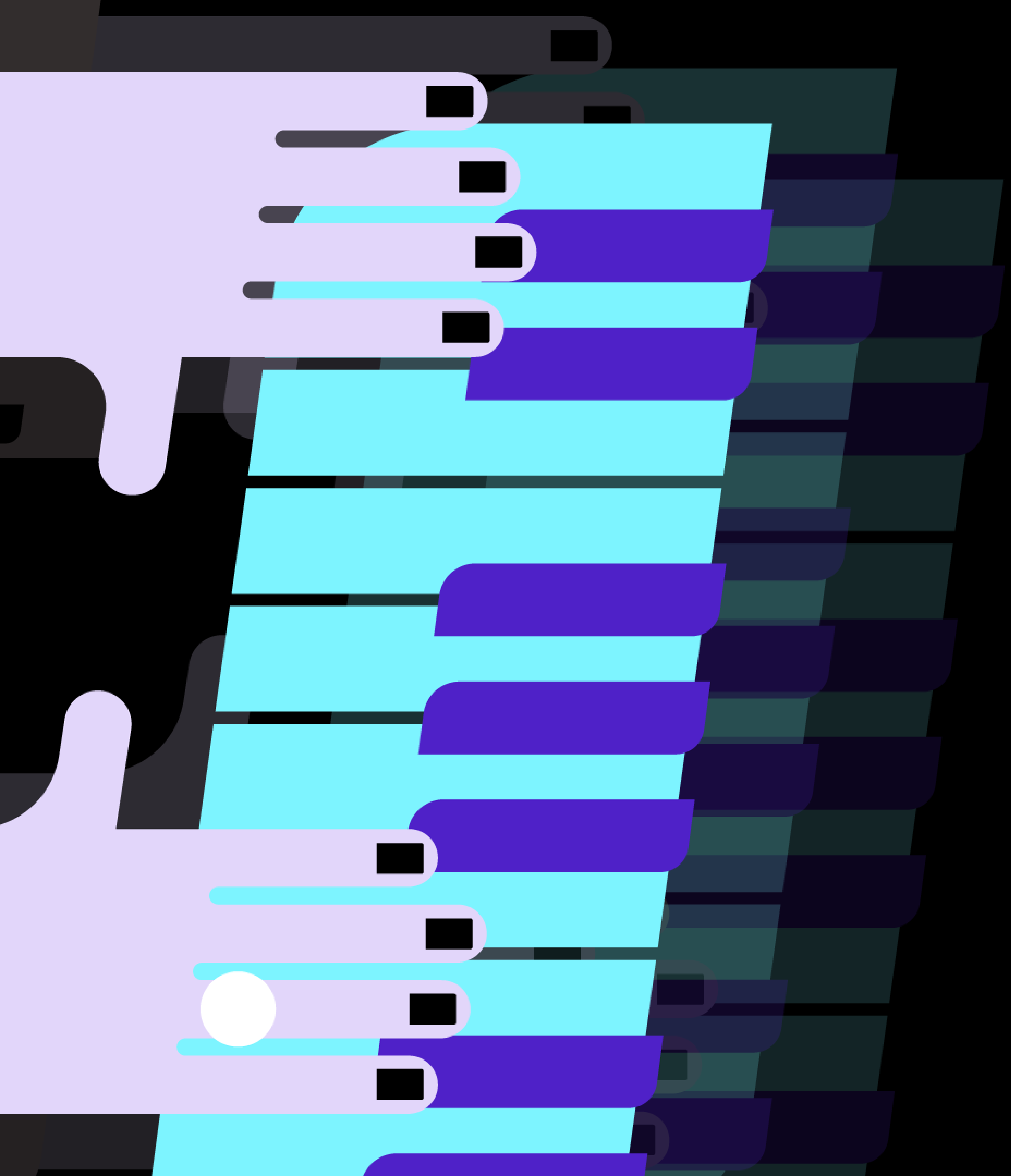
□ Include e-mail name

Type of subject

● Computer or other device

○ User

Game over!
Forest Compromised from Tier 2 account



HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Demo

Supply in the request

KDC – Strong Certificate Binding Enforcement

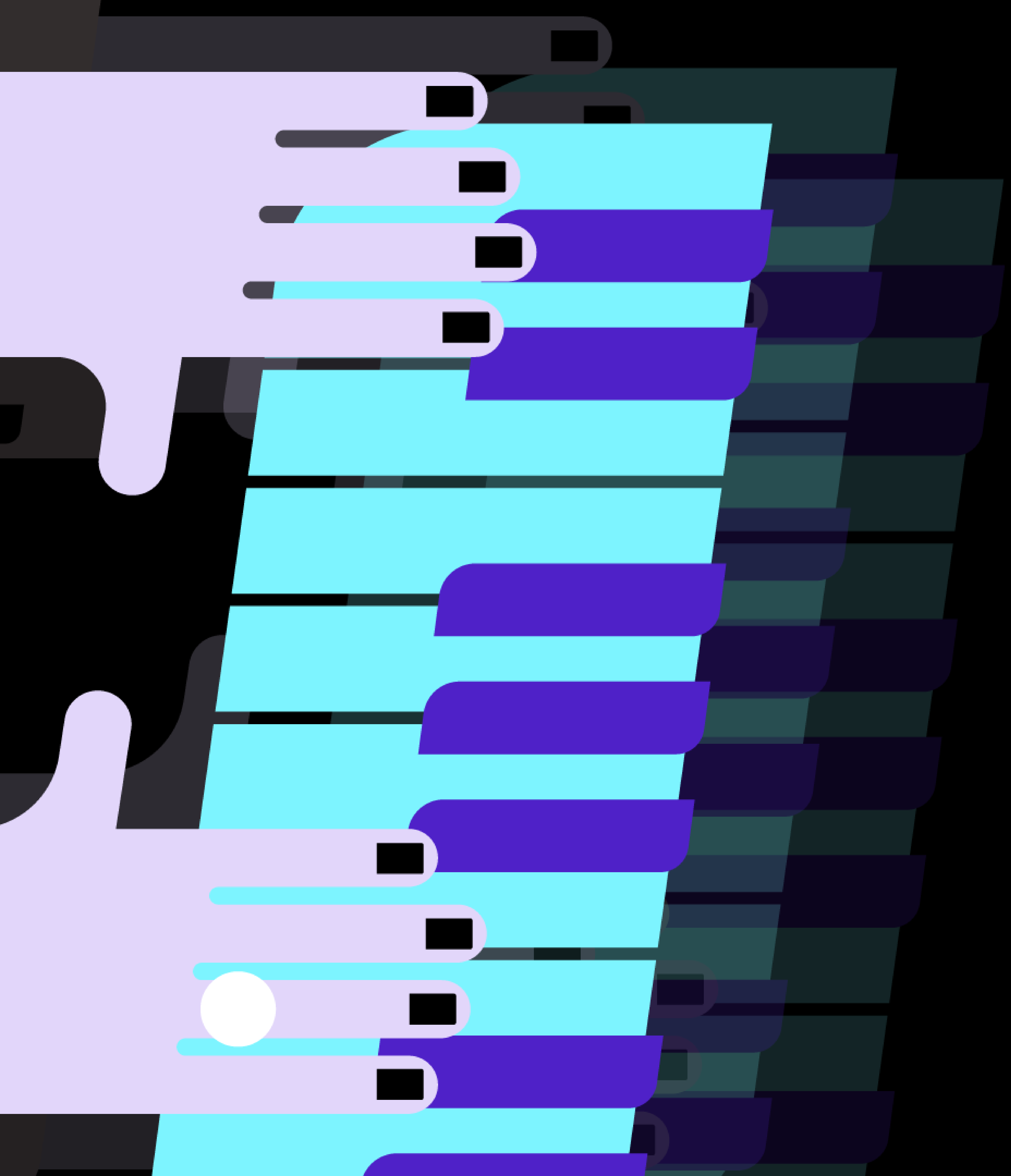
KDC changes (CVE-2022–26923)

- Default: Compatibility Mode (StrongCertificateBindingEnforcement:1) (Allowed until: September 10, 2025)
  - Certificate SID extension
  - altSecurityIdentities

X509IssuerSerialNumber	"X509:<I>IssuerName<SR>1234567890"	Strong
X509SKI	"X509:<SKI>123456789abcdef"	Strong
X509SHA1PublicKey	"X509:<SHA1-PUKEY>123456789abcdef"	Strong

  - altSubjectName (Only 25246 KDC and later, now reverse integrated to Windows Server 2019)
    - URL=tag:microsoft.com,2022-09-14:sid:<value>
  - Computer/User account pre-dates 'NotBefore' in certificate
    - HKLM\SYSTEM\CurrentControlSet\Services\Kdc\CertificateBackdatingCompensation – 3600 = 1h
- Full Enforcement Mode (StrongCertificateBindingEnforcement:2) (Planned: February 11, 2025)
  - Certificate SID extension
  - altSecurityIdentities

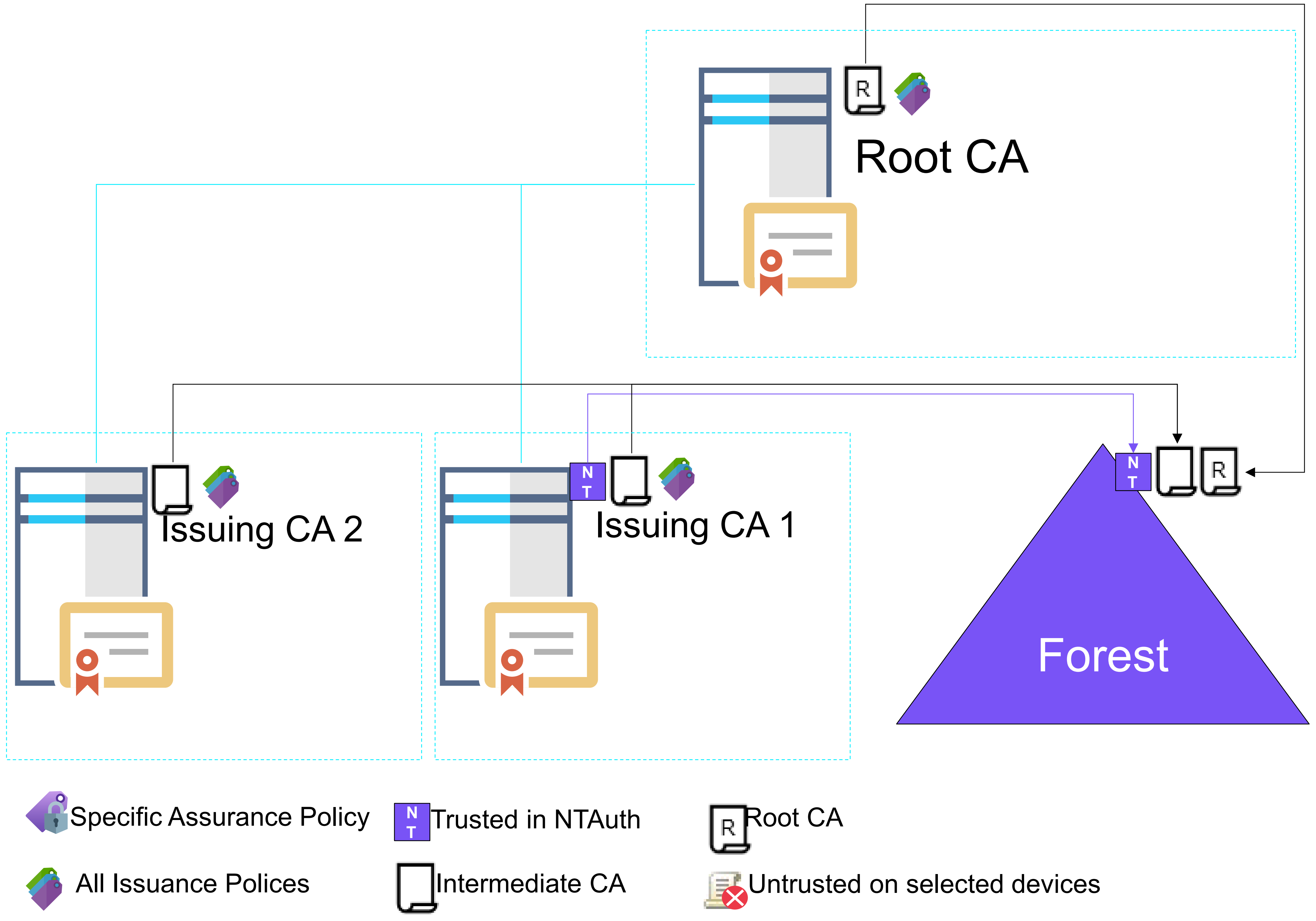
Troubleshooting tips: KDC maintains cache of all successful authentications, restart is required to clear the cache



Demo

Supply in the request with StrongCertificateBindingEnforcement

Supply in the request abuse - Mitigations

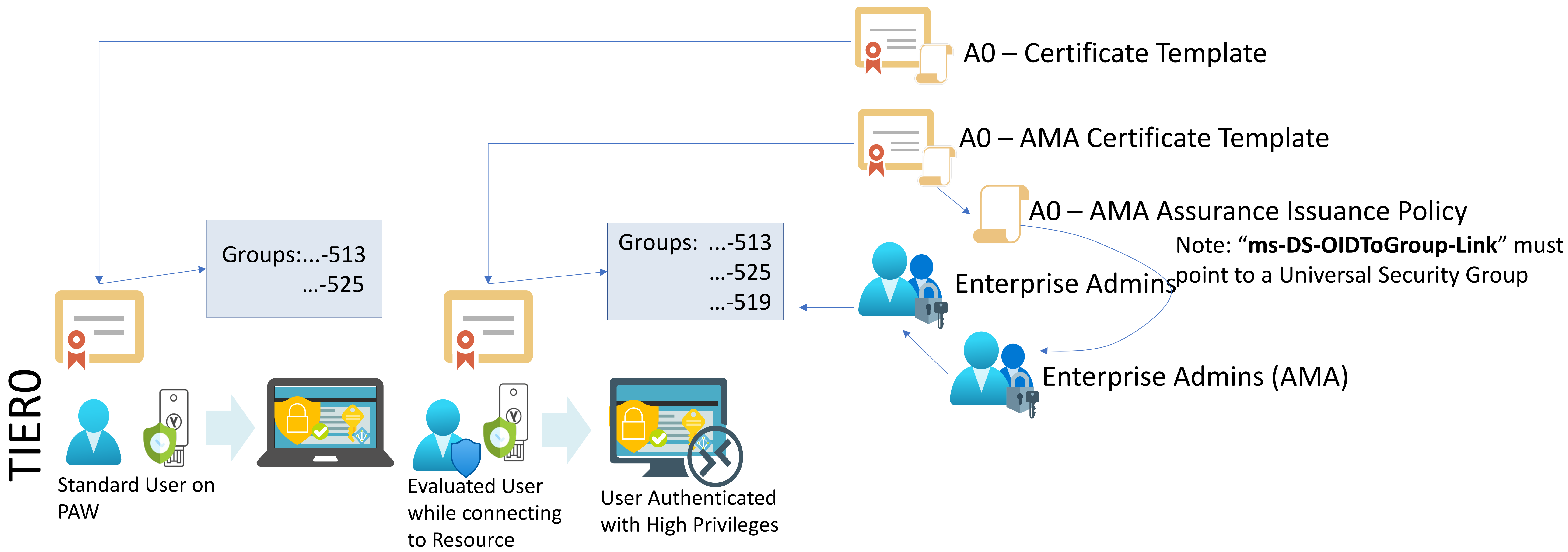


- Consider at least two CAs – both managed from T0
  - Issuing CA1 - Enterprise CA
    - Trusted in NTAuth
    - Can only have templates with "build from active directory" published
  - Issuing CA2 – Enterprise CA
    - Untrusted from NTAuth (remember you need to do this every time you renew the CA cert/key)
    - Should have the following extensions blocked
      - DisableExtensionList +1.3.6.1.4.1.311.25.2 (SID)
      - DisableExtensionList +1.3.6.1.4.1.311.21.10 (App Policies)
    - Templates configured for 'Supply in the request' should have '0x00080000' in 'msPKI-Enrollment-Flag'

Tip: https://github.com/CarlSorqvist/PsCertTools/tree/main/NTAuthGuard

Key take away: KDC changes for CVE-2022–26923 only protect against those attack vectors not misconfigured templates

Authentication Mechanism Assurance (AMA)


A0 – Certificate Template
A0 – AMA Certificate Template
A0 – AMA Assurance Issuance Policy
Groups:...-513
...-525
Groups: ...-513
...-525
...-519
Enterprise Admins
Enterprise Admins (AMA)
TIER0
Standard User on PAW
Evaluated User while connecting to Resource
User Authenticated with High Privileges

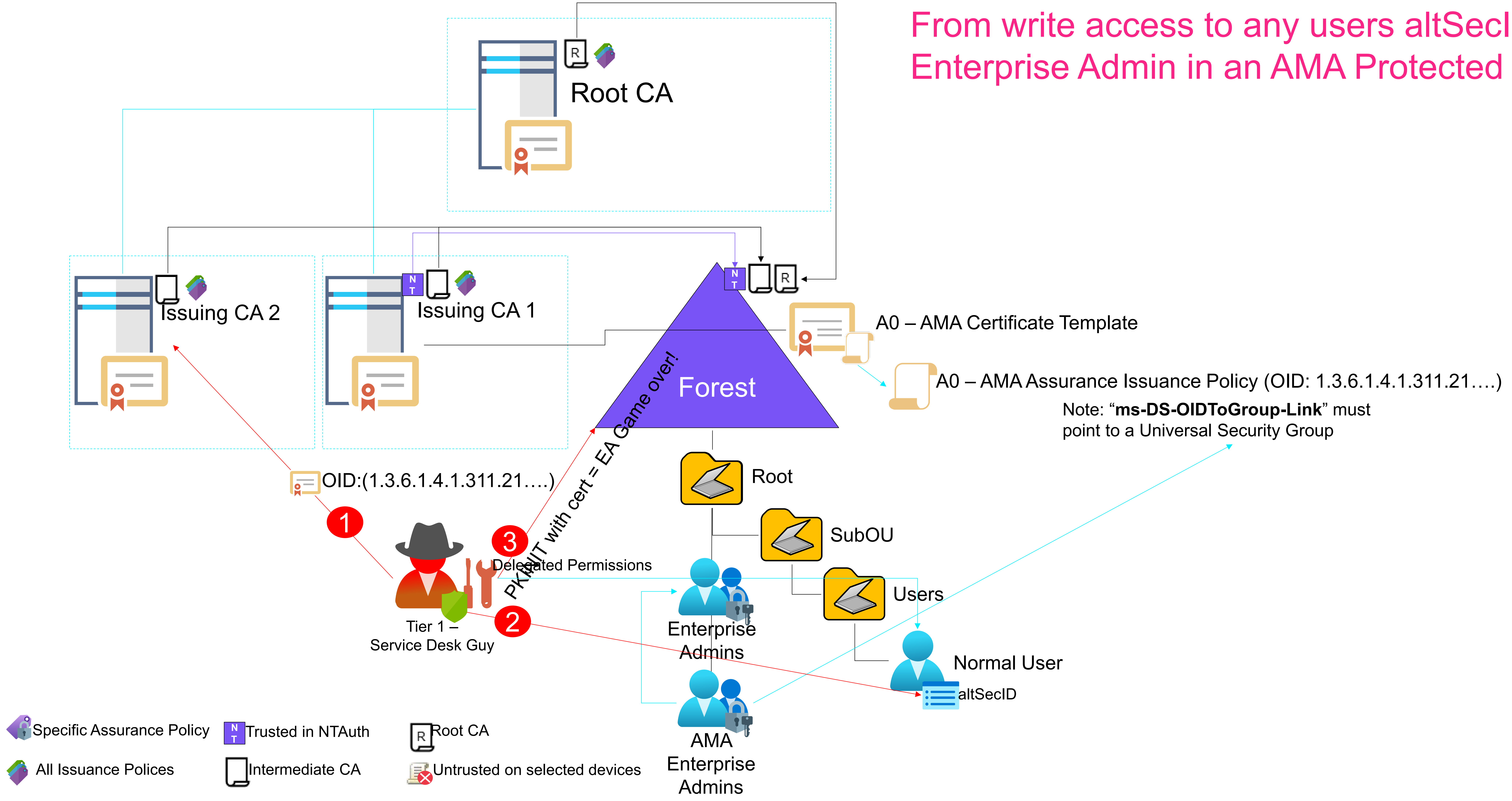
Note: "**ms-DS-OIDToGroup-Link**" must point to a Universal Security Group

Mitigates PtH – You-re welcome to grab my hash – you only get AMA if authenticated with the AMA cert, PIN only released by pressing Yubikey

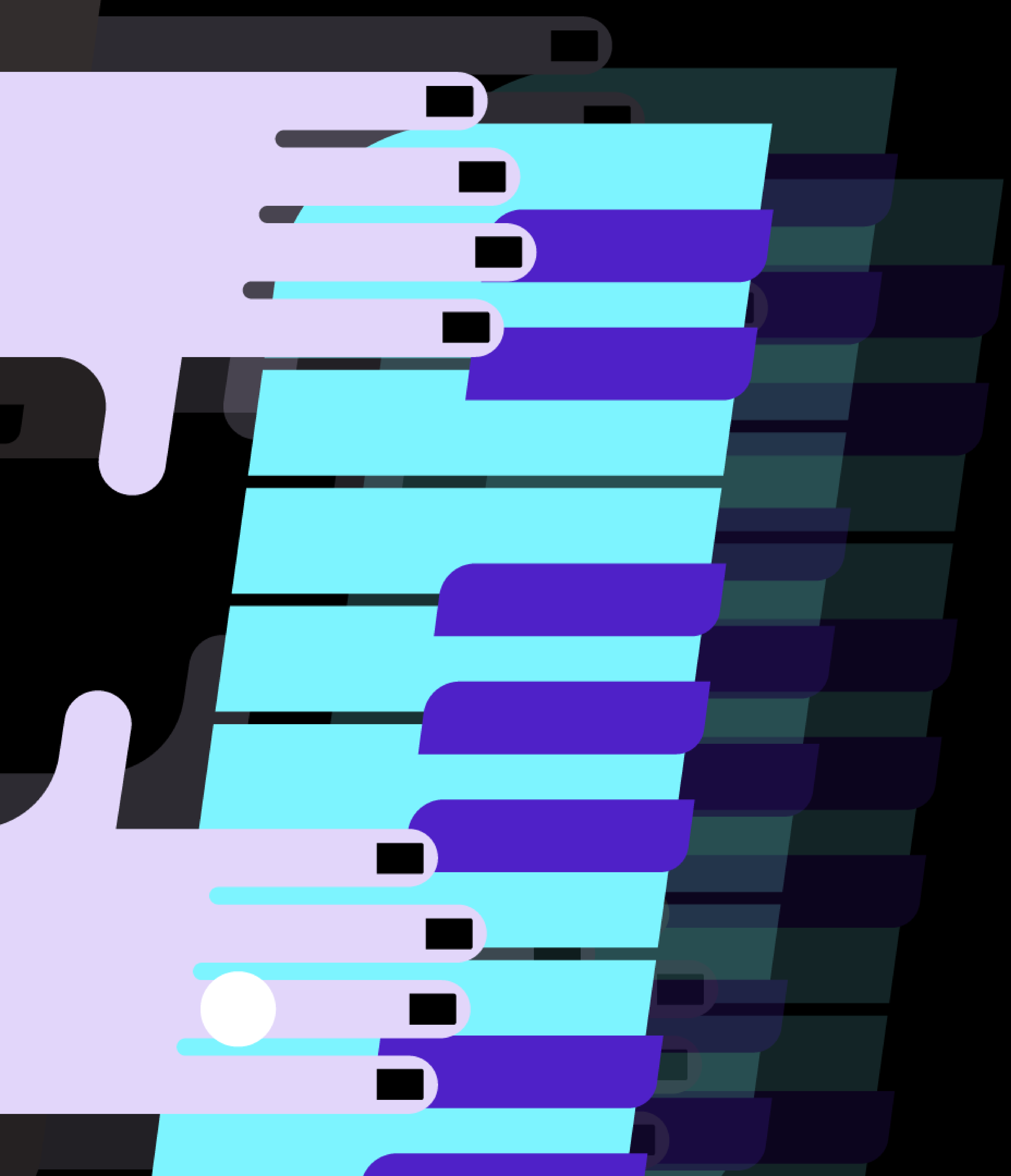
Federal Identity, Credential, and Access Management (FICAM) program – recommends using AMA: https://www.idmanagement.gov/implement/scl-windows/

PKINIT– altSecurityIdentities + AMA ☹

From write access to any users altSecID to Enterprise Admin in an AMA Protected Forest



R
Root CA
Issuing CA 2
N T
Issuing CA 1
N T
R
Forest
A0 – AMA Certificate Template
A0 – AMA Assurance Issuance Policy (OID: 1.3.6.1.4.1.311.21….)
Note: “**ms-DS-OIDToGroup-Link**” must point to a Universal Security Group
OID:(1.3.6.1.4.1.311.21….)
1
2
3
PKINIT with cert = EA Game over!
Delegated Permissions
Tier 1 – Service Desk Guy
Root
SubOU
Users
Enterprise Admins
Normal User
altSecID
AMA Enterprise Admins
Specific Assurance Policy
All Issuance Polices
N T
Trusted in NTAuth
Intermediate CA
R
Root CA
Untrusted on selected devices



HYBRID IDENTITY PROTECTION conf24

NEW ORLEANS

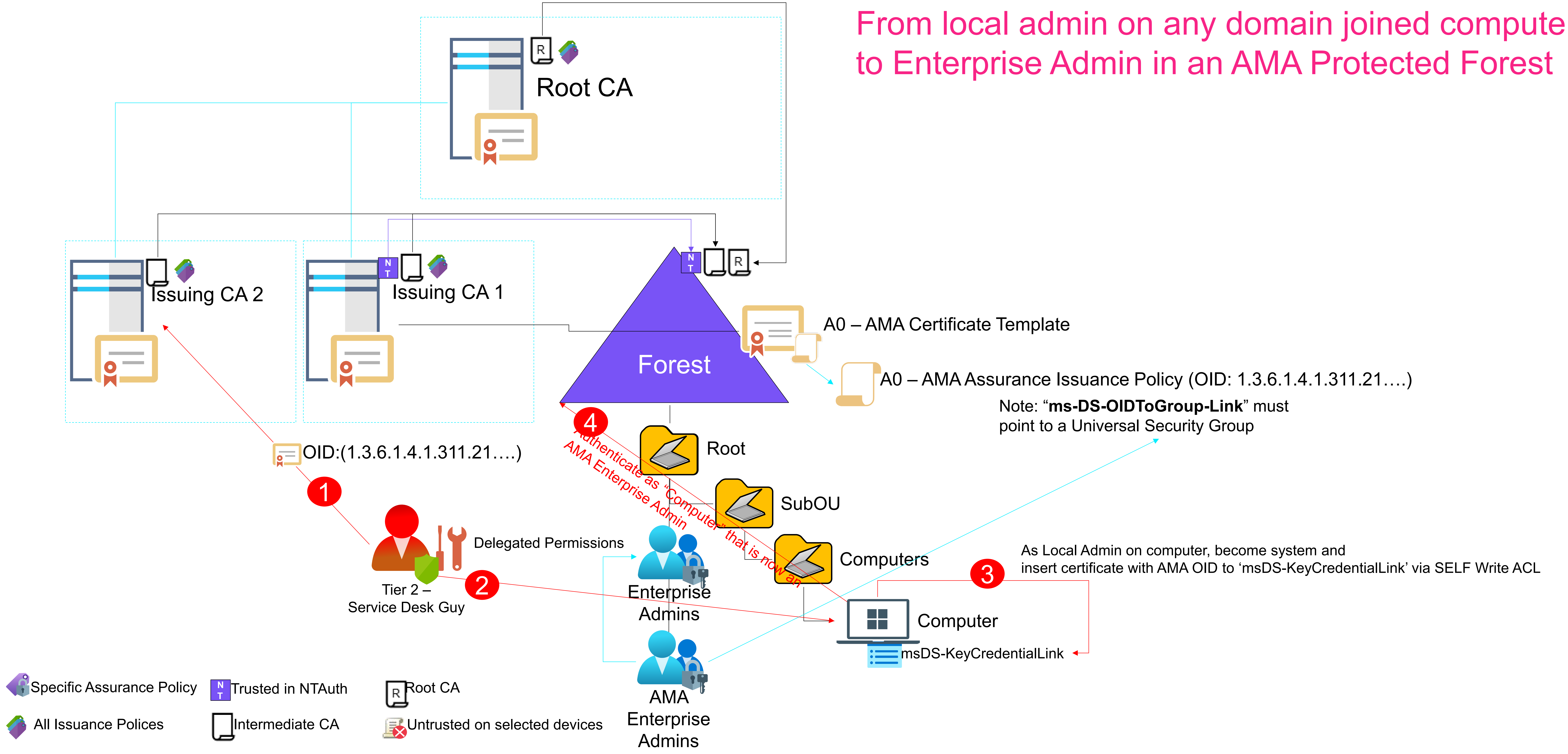
Demo

altSecID + AMA

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

PKINIT– NTAuth + KCL + AMA ☹

From local admin on any domain joined computer to Enterprise Admin in an AMA Protected Forest



Root CA

Issuing CA 2

Issuing CA 1

Forest

A0 – AMA Certificate Template

A0 – AMA Assurance Issuance Policy (OID: 1.3.6.1.4.1.311.21….)

Note: “**ms-DS-OIDToGroup-Link**” must point to a Universal Security Group

OID:(1.3.6.1.4.1.311.21….)

1

Delegated Permissions

Tier 2 –
Service Desk Guy

2

4 Authenticate as “Computer” that is now an AMA Enterprise Admin

Root

SubOU

Computers

Enterprise Admins

AMA Enterprise Admins

3 As Local Admin on computer, become system and insert certificate with AMA OID to ‘msDS-KeyCredentialLink’ via SELF Write ACL

Computer

msDS-KeyCredentialLink

Specific Assurance Policy

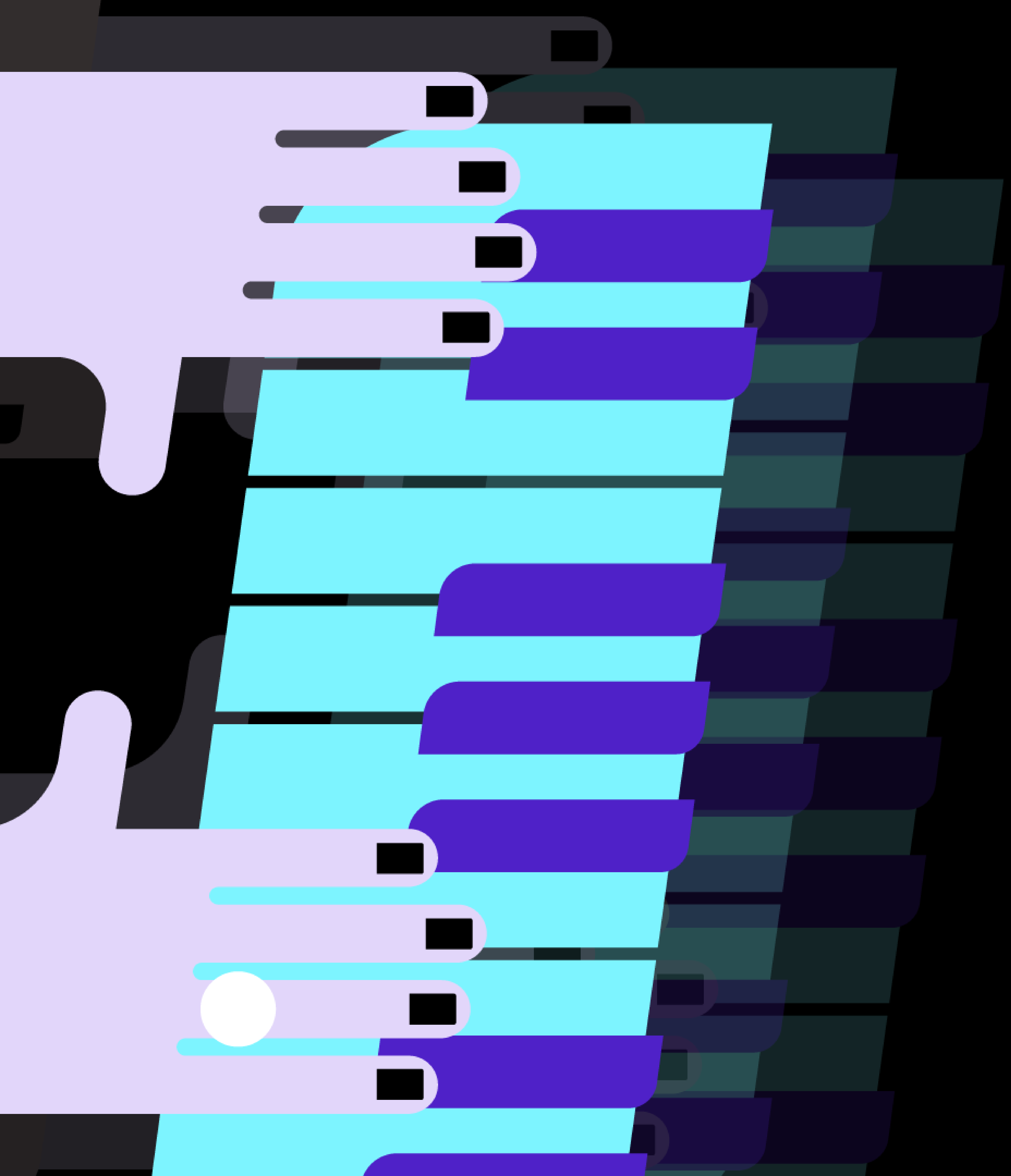
All Issuance Polices

Trusted in NTAuth

Intermediate CA

Root CA

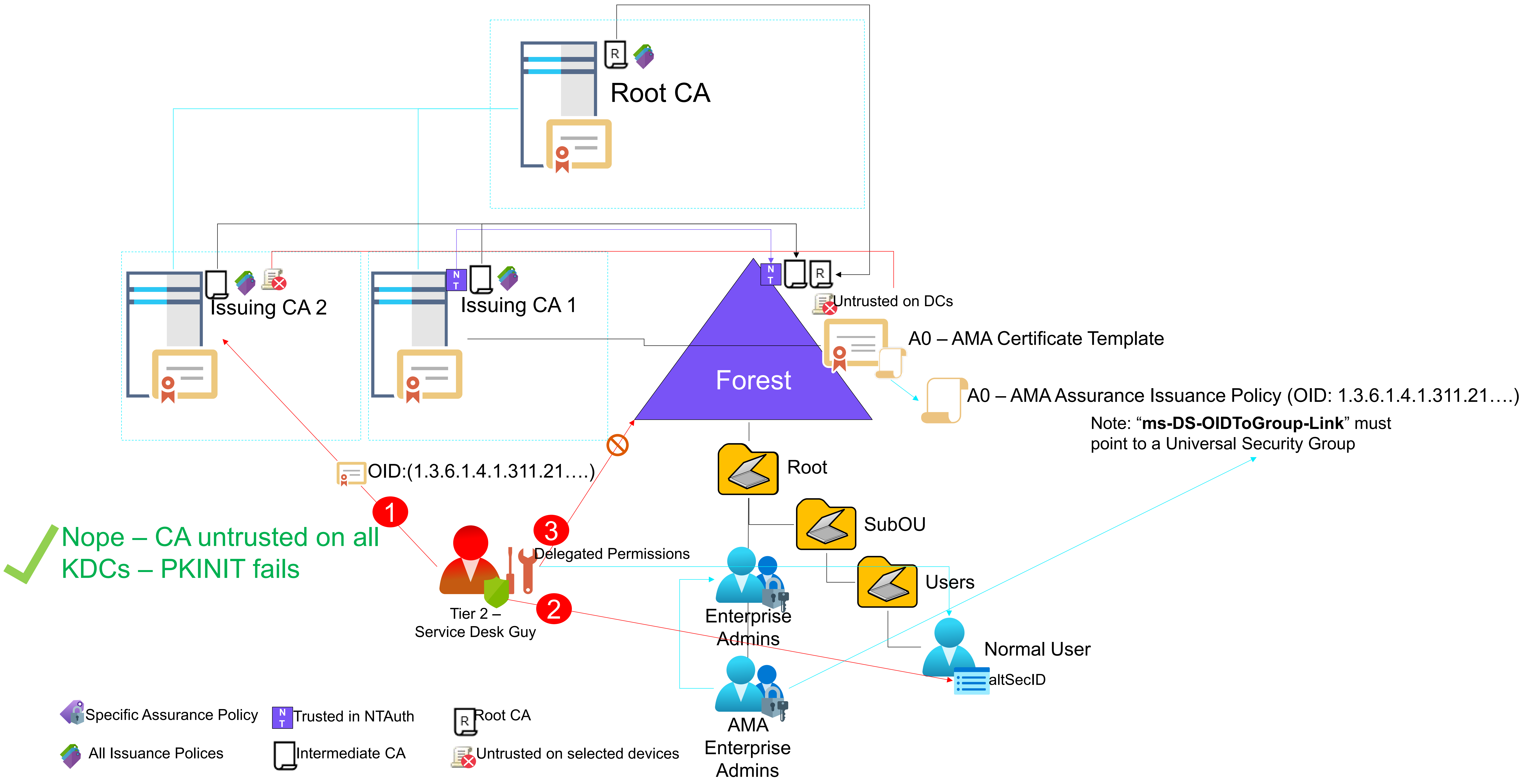
Untrusted on selected devices



Demo

KCL + AMA

PKINIT– AMA/Policy Abuse Mitigation 1

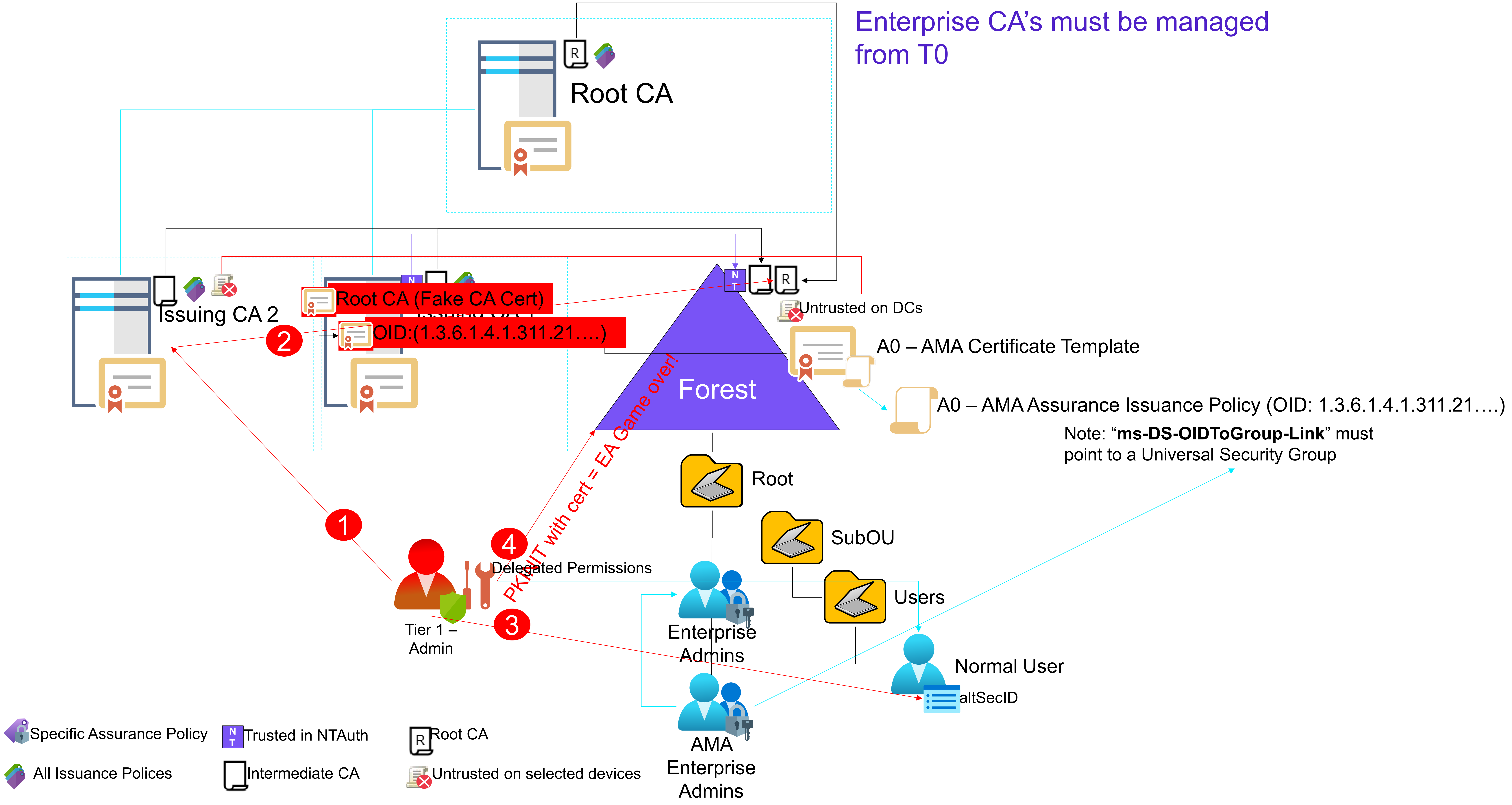


Note: “**ms-DS-OIDToGroup-Link**” must point to a Universal Security Group

✓ Nope – CA untrusted on all KDCs – PKINIT fails

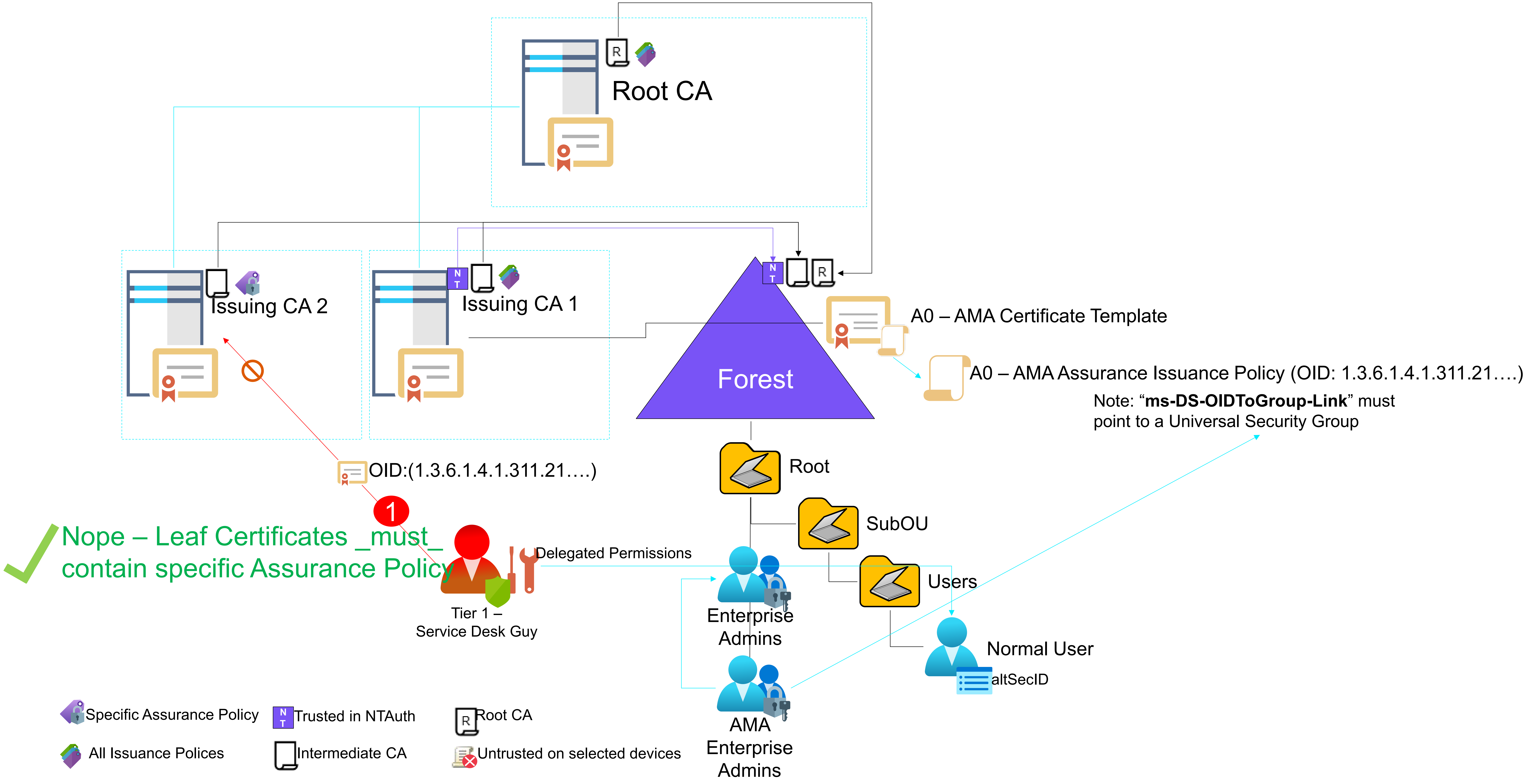
PKINIT– altSecurityIdentities + AMA + Cert Publishers ☹

Enterprise CA’s must be managed from T0



Note: “**ms-DS-OIDToGroup-Link**” must point to a Universal Security Group

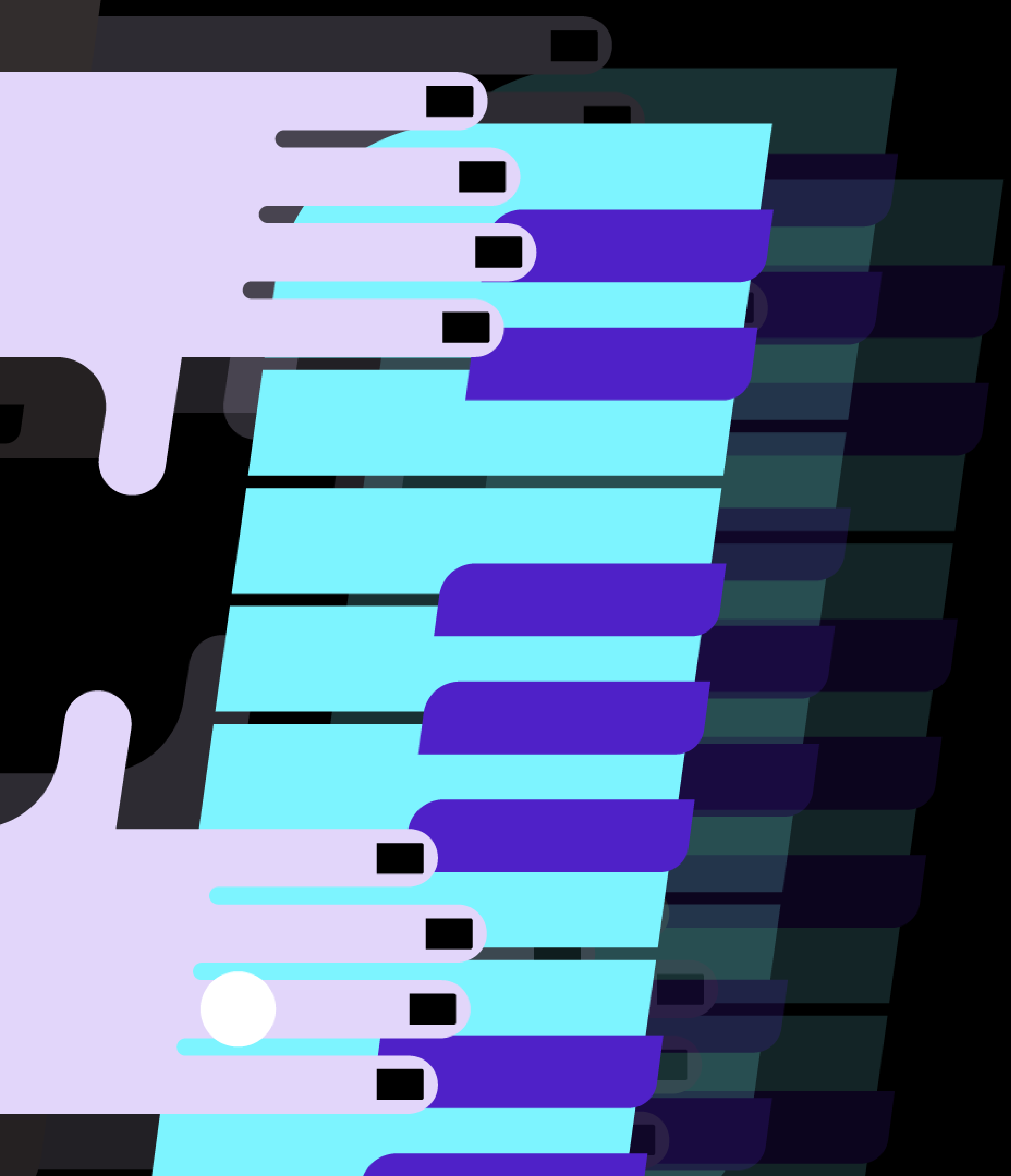
PKINIT– AMA/Policy Abuse Mitigation 2



Note: “**ms-DS-OIDToGroup-Link**” must point to a Universal Security Group

✓ Nope – Leaf Certificates _must_ contain specific Assurance Policy

Specific Assurance Policy	N T Trusted in NTAuth	R Root CA
All Issuance Polices	Intermediate CA	Untrusted on selected devices



HYBRID IDENTITY PROTECTION conf24

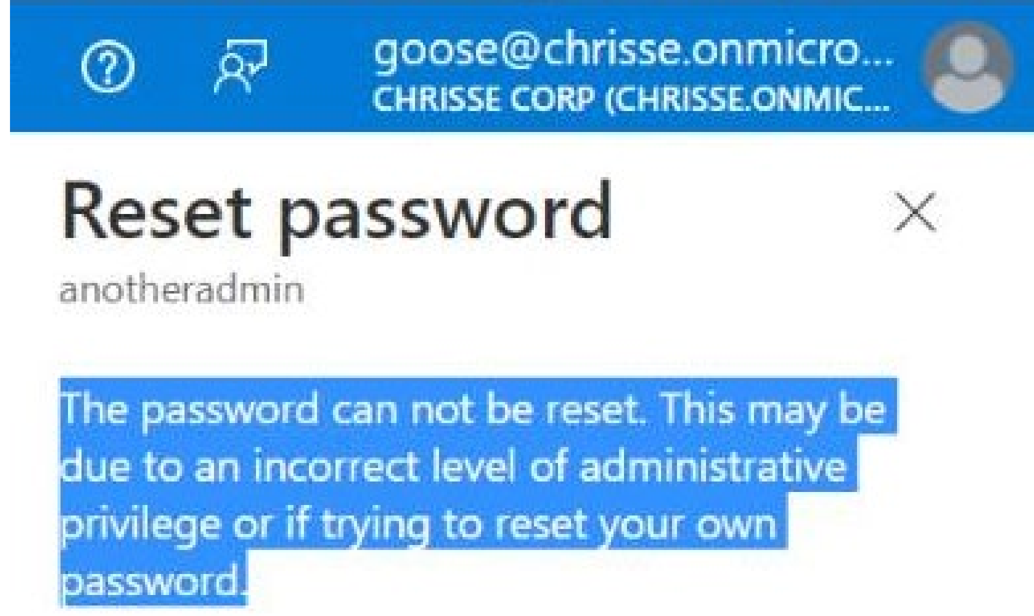
NEW ORLEANS

Entra ID

Certificate Based Authentication (CBA)

Entra ID – Certificate Based Authentication (CBA)

- certificateUserIds
  - PrincipalName
  - RFC822Name
  - SKI
  - SHA1PublicKey
  - IssuerAndSerialNumber (preview)
  - IssuerAndSubject (preview)
  - Subject (preview)



Reset password

anotheradmin

The password can not be reset. This may be due to an incorrect level of administrative privilege or if trying to reset your own password.

Entra ID - Privilege Escalation from User Administrator to Global Administrator using CBA

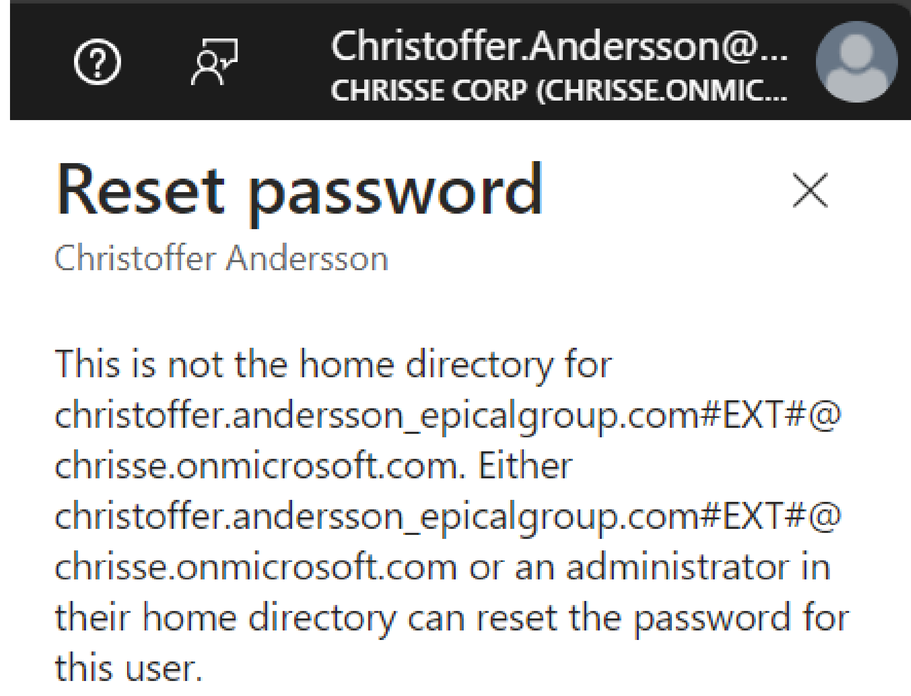
1. Let's say CBA is enabled on the Azure AD tenant with a Trusted Certificate Authority X.

2. A user granted the ‘User Administrator’ role authenticate to the Azure AD tenant and obtain (1) one certificate from the Trusted Certificate Authority X

3. Then updates the AuthorizationInfo on an existing Global Administrator account, more specifically adding one entry to ‘certificateUserIds’ that specifies the ‘’subject key identifier” of the certificate previously obtained from the Trusted Certificate Authority X in the format of X509:<SKI>612c391c06a2b36f0e5410fd4cc897c15f3f4a0d

4. It is now possible to use the certificate obtained from the Trusted Certificate Authority X to logon to Azure using CBA as the Global Administrator account.

Impersonation of any Guest/Federated from external tenant in own Entra ID tenant using CBA



Christoffer.Andersson@...
CHRISSE CORP (CHRISSE.ONMIC...

Reset password

Christoffer Andersson

This is not the home directory for christoffer.andersson_epicalgroup.com#EXT#@chrisse.onmicrosoft.com. Either christoffer.andersson_epicalgroup.com#EXT#@chrisse.onmicrosoft.com or an administrator in their home directory can reset the password for this user.

1. Let's say CBA is enabled on the Azure AD tenant with a Trusted Certificate Authority X.
2. A user granted ‘User Administrator’ or ‘Global Administrator’ role authenticate to the Azure AD tenant and obtain (1) certificate from the Trusted Certificate Authority X
3. Then updates the AuthorizationInfo on any guest/federated account, more specifically adding one entry to ‘certificateUserIds’ where he specifies the ‘’subject key identifier” of the certificate previously obtained from the Trusted Certificate Authority X also known as SKI in the format of X509:<SKI>612c391c06a2b36f0e5410fd4cc897c15f3f4a0d – this update is surprisingly allowed on guest accounts and federated accounts that origins form any other Azure AD tenants
4. It is now possible to use the certificate obtained from the Trusted Certificate Authority X to logon to Azure using CBA and you get authenticated as username_externalfederateddomain#EXT#@yourdomain.onmicrosoft.com.

Microsoft Security Response Center (MSRC)

- Thanks for working with me on those issues – and rolling out fixes globally
- Entra ID - Privilege Escalation from User Administrator to Global Administrator using CBA
  - 2023-01-20: We confirmed the behavior you reported.
  - US$10000.00 bounty award under the Azure Bounty Program.
- Impersonation of any Guest/Federated from external tenant in own Entra ID tenant using CBA
  - 2023-02-03: We confirmed the behavior you reported.
  - US$10000.00 bounty award under the Azure Bounty Program.
- Global fixes rolled out – 2023-03-24
- Awarded Microsoft Most Valuable Researcher (MVR 2023)

Thank you!

Christoffer Andersson

Principal Advisor – Epical Sweden
christoffer.andersson@epicalgroup.com
http://www.epicalgroup.com

Blog: http://blog.chrisse.se – DS Geek Blog

Credits

- CertRequestTools – Carl Sörqvist: https://github.com/CarlSorqvist/PsCertTools/tree/main/CertReqTools
- Rubeus - @harmj0y https://github.com/GhostPack/Rubeus
- Whisker - Elad Shamir https://github.com/eladshamir/Whisker

Rubeus and Whisker was modified to take a certificate directly from a cert store rather than PFX.

Questions?