

CQURE LIVE WEBINAR:

Breaking Trust: **A Handful of Ways to Compromise** **a Microsoft Certification Authority (CA)**

Tuesday, June 17th, 2025

7 PM CEST | 1 PM EDT | 10 AM PDT

Breaking Trust:

A Handful of Ways to Compromise a Microsoft Certification Authority (CA)

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cquire.us

X @PaulaCquire @CQUREAcademy

www.cquireacademy.com



Breaking Trust:

A Handful of Ways to Compromise a Microsoft Certification Authority (CA)

Peter Kloep

CQURE: Cybersecurity Expert, Principal IT Architect

CQURE Academy: Trainer

X @cquireacademy.com

www.cquireacademy.com



CQURE

What does **CQURE** do?

1. Consulting Services:

- a) Extensive IT Security Audits and Penetration Tests of all kinds
- b) Configuration Audit and Architecture
- c) Design Social Engineering Tests
- d) Advanced Troubleshooting and Debugging
- e) Emergency Response Services

2. R&D & CQLabs Tools & Hacks Publications.

3. Trainings & Seminars:

- a) Offline (mainly via our partners worldwide)
- b) Online (you will hear more about it at the end of this webinar, so stay with us!)



To ensure **good quality** of your experience:

1. If you have **problems with watching the webinar**, try re-logging into Zoom session.
2. If the **streaming on Zoom breaks** for any reason, please observe the chat for news from our Team – we should be back shortly.
3. If there is a connection or software problem, please check your email inbox for instructions.
4. Should the problems persist, please let us know in the comment section or via email – **info@cquireacademy.com**.
5. We will be answering your questions at the end of the webinar during the **Q&A session**, so write them down in the chat!

What to expect today:

1. A presentation and technical demos from our Experts
2. Tips on how you can learn with us
3. Live Q&A!
4. You will get access to the tools we will be using here!

Time for **the challenge!**

Which key is used in a Public Key Infrastructure to prove that a message or data packet is sent from the sender and has not been modified in transit?

To answer, scan the QR or go to:

<https://cquireacademy.com/webinar25/>



Agenda

01

Common vulnerabilities

„Insecure by default“ vs. „Bad planning“

02

Insecure Configuration

Missing hardening

03

Top „Backdoors“

ESCs an PetitPotam

04

Secure Design

How to design a more secure
CA-Infrastructure



05

Q&A

Time to ask your questions

#1. Common Vulnerabilities



CVE-2025-33073 :: Narrative

Windows SMB Client Elevation of Privilege Vulnerability

Released: Jun 10, 2025

More details:

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-33073>

[GitHub - mverschu/CVE-2025-33073: PoC Exploit for the NTLM reflection SMB flaw.](#)

CVE-2025-33073 :: Attack Vectors

Way No 1:

To add DNS record, which indicates our machine -> listening with **impacked** and performing a relay (PetitPotam or PrinterBug) to this machine with special DNS – authentication to “ourselves” + dumping SAM

Way No 2:

Starting responder with llmnr poisoning -> listening with **impacked** and performing a relay to vulnerable machine -> Coercer attack with point a concrete DNS that does not exist, but LLMNR poisoning can indicate that it supposed to go to us – relay + dumping SAM Relay

CVE-2025-33073

Prep. by Krystian Tyton



**What about bad
planning?**



Planning a CA-infrastructure

Planning and defining processes consumes 80% of a PKI project

Missing guards / protections might lead to compromise

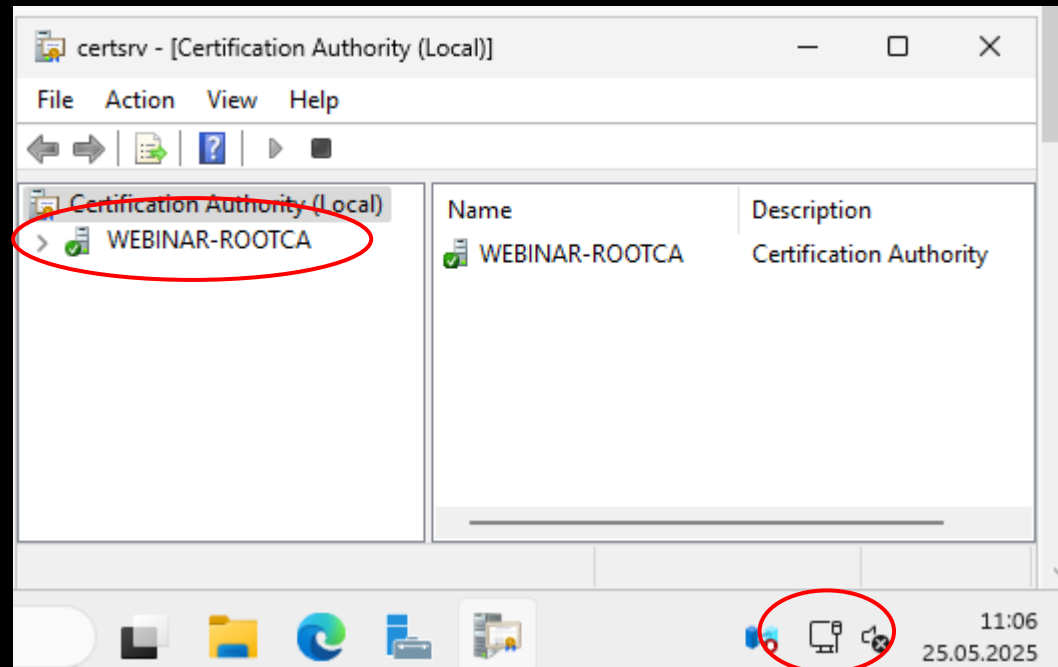
Hardening is crucial

Limit Access to the CA-systems

An infrastructure built 5 years ago might not be “state of the art” today

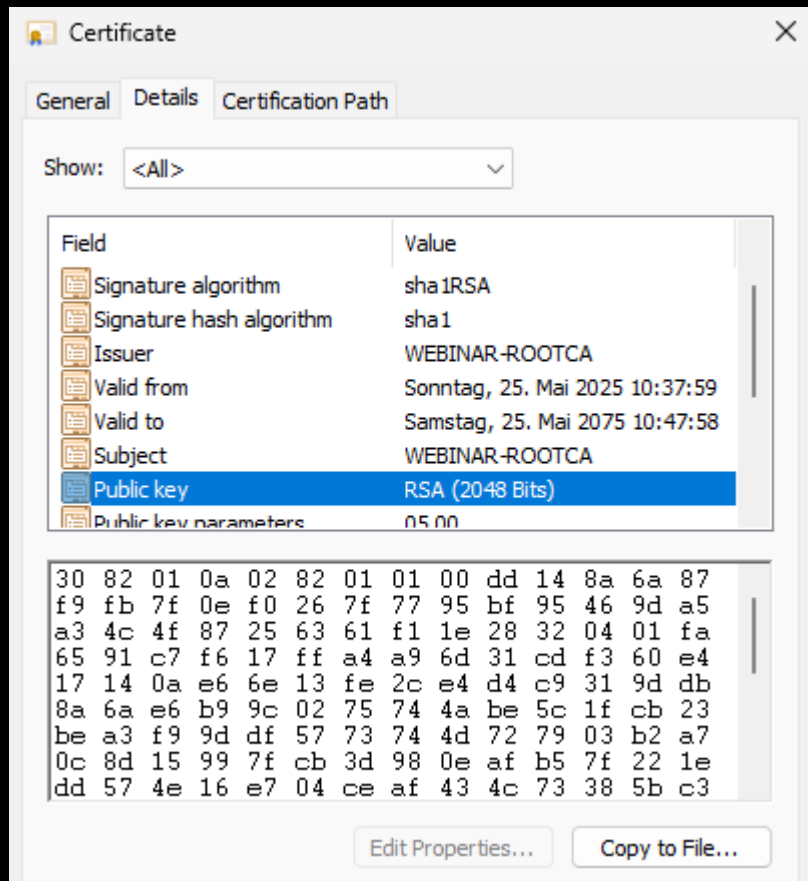
Planning a CA-infrastructure

Creating a multi-tier CA-infrastructure is common / good practice.
An offline CA is always OFFLINE!

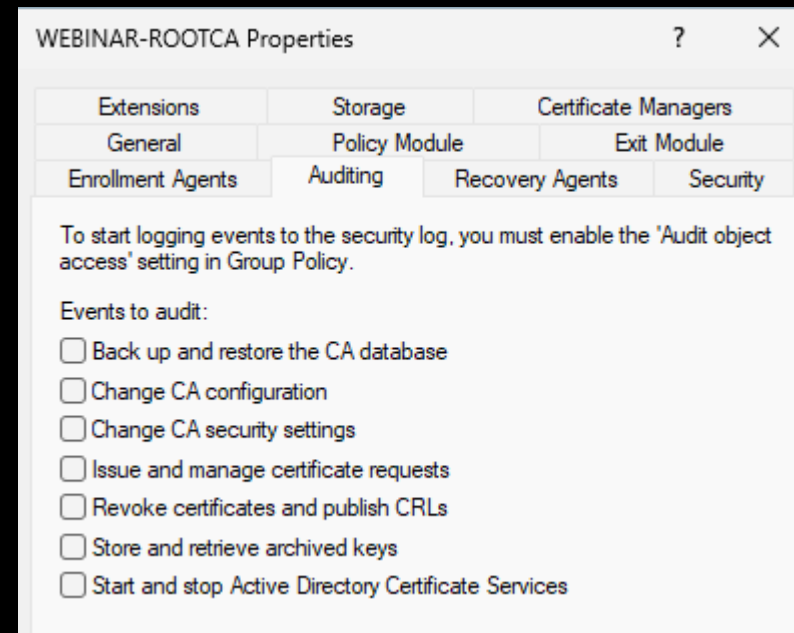


Design / Default (weak ciphers / auditing)

CA-Certificates:



No Auditing:



Windows-Components of a **CA-infrastructure**

One or more Certification Authorities

Revocation-Server (CRL and/or OCSP)

Proxy (CEP / CES)

Management-Server (with enrollment-Tools)

Group Policies

Backup

Agents on CA-Servers

**Hey Raccoons? Some
questions? ;)**



#2. Insecure Configuration

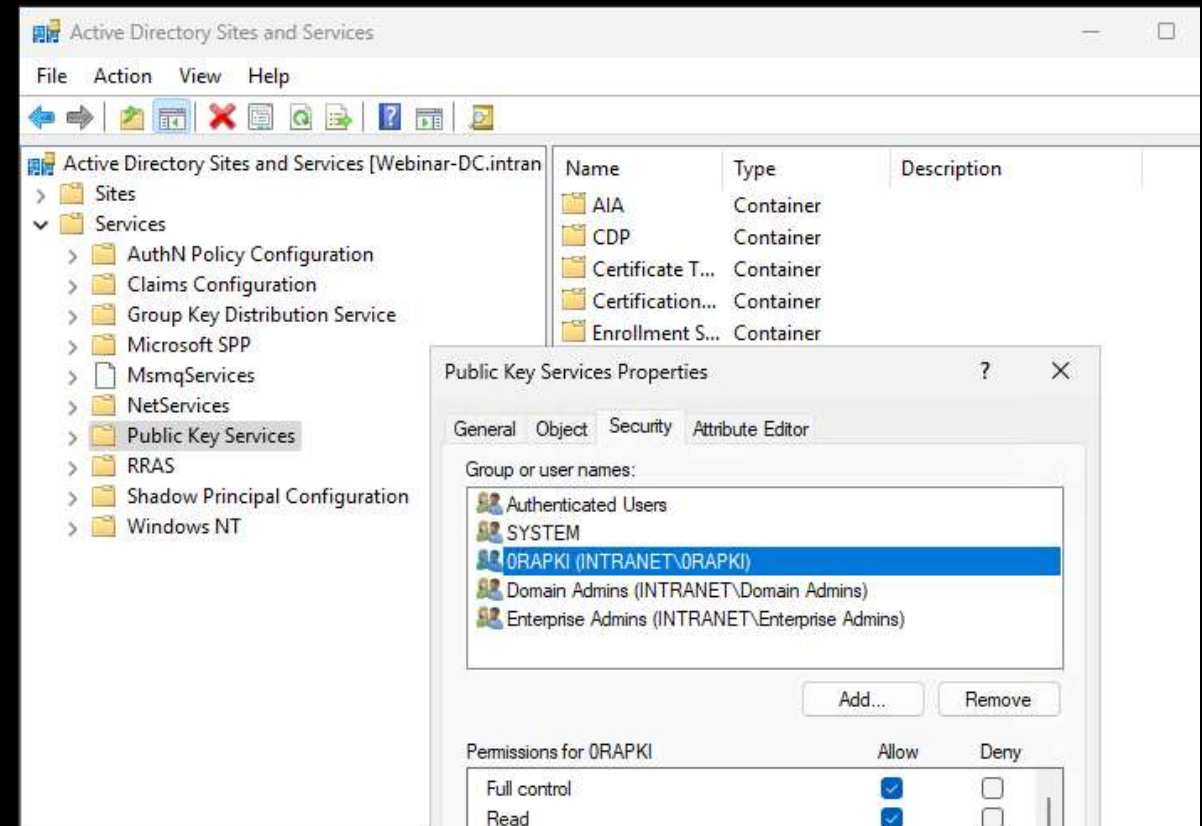


Insecure Configuration (security)

Missing Hardening:



No permission delegation:



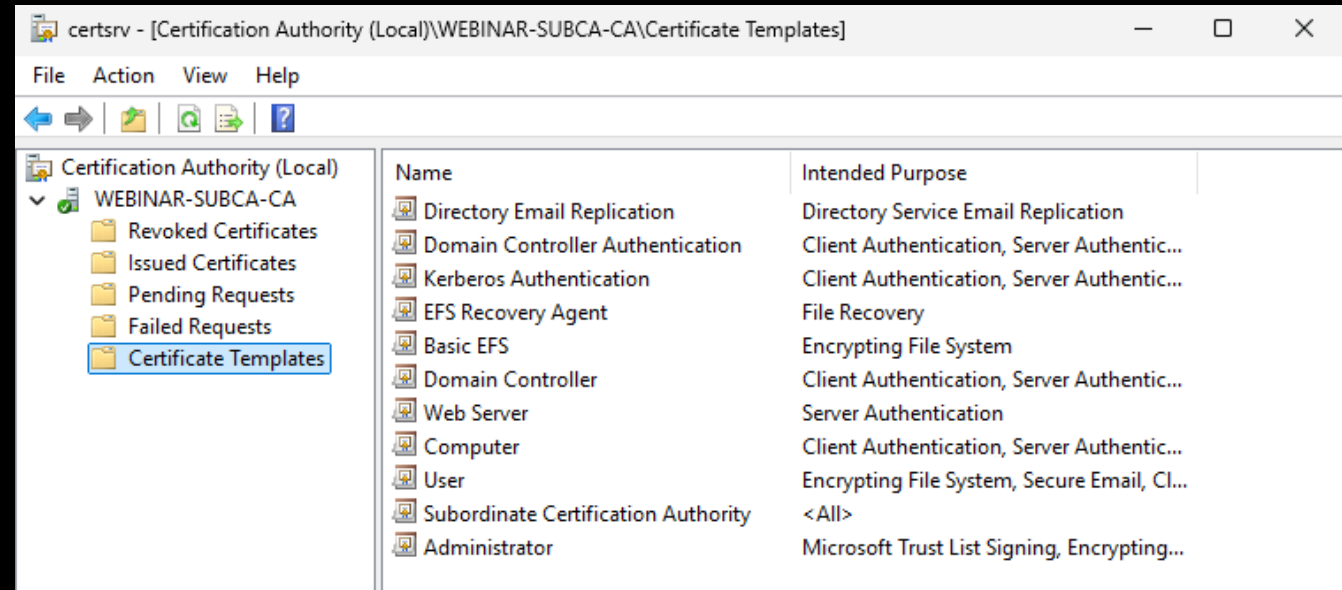
Insecure Configuration (defaults)

Missing CAPolicy:

```
[BasicConstraintsExtension]
PathLength=1
Critical=Yes
```

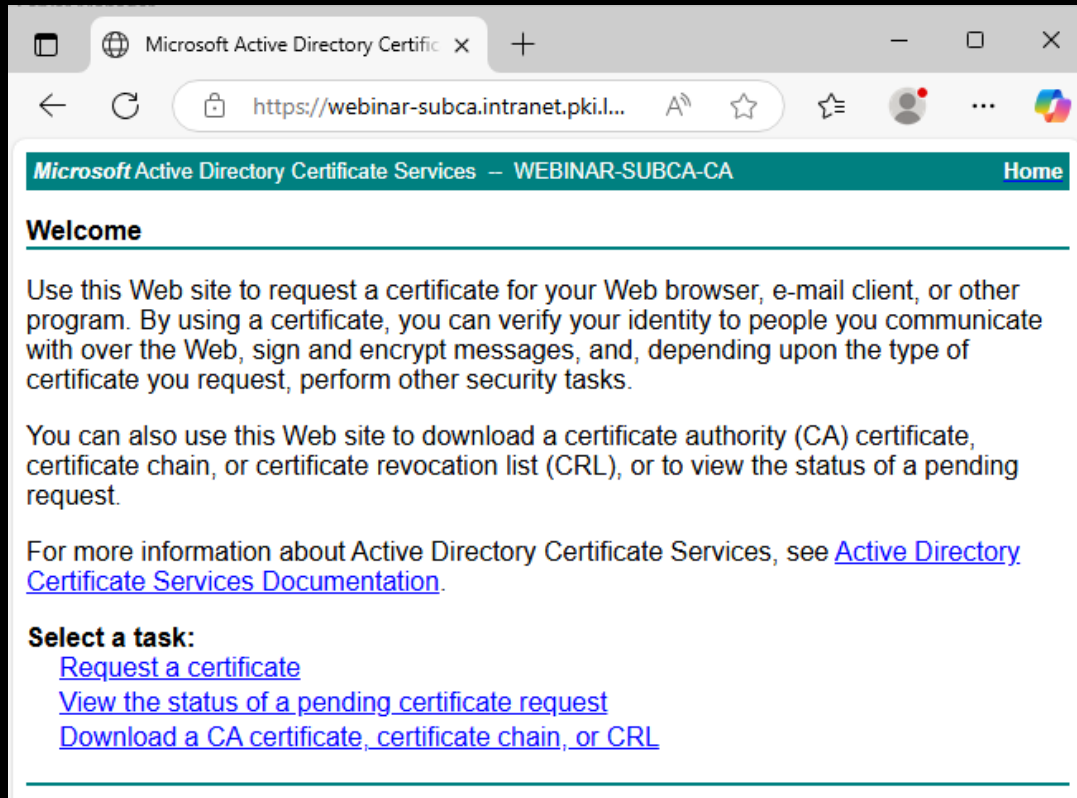
```
[Strings]
szOID_NAME_CONSTRAINTS = "2.5.29.30"
[Extensions]
Critical = %szOID_NAME_CONSTRAINTS%
%szOID_NAME_CONSTRAINTS% = "{text}"
_continue_ = "SubTree=Include&"
_continue_ = "DNS = .pki.lab.de&"
_continue_ = "DIRECTORYNAME = CN=pki.lab.de&"
_continue_ = "SubTree=Exclude&"
_continue_ = "DNS = *.pki.lab.de&"
```

Default installation:



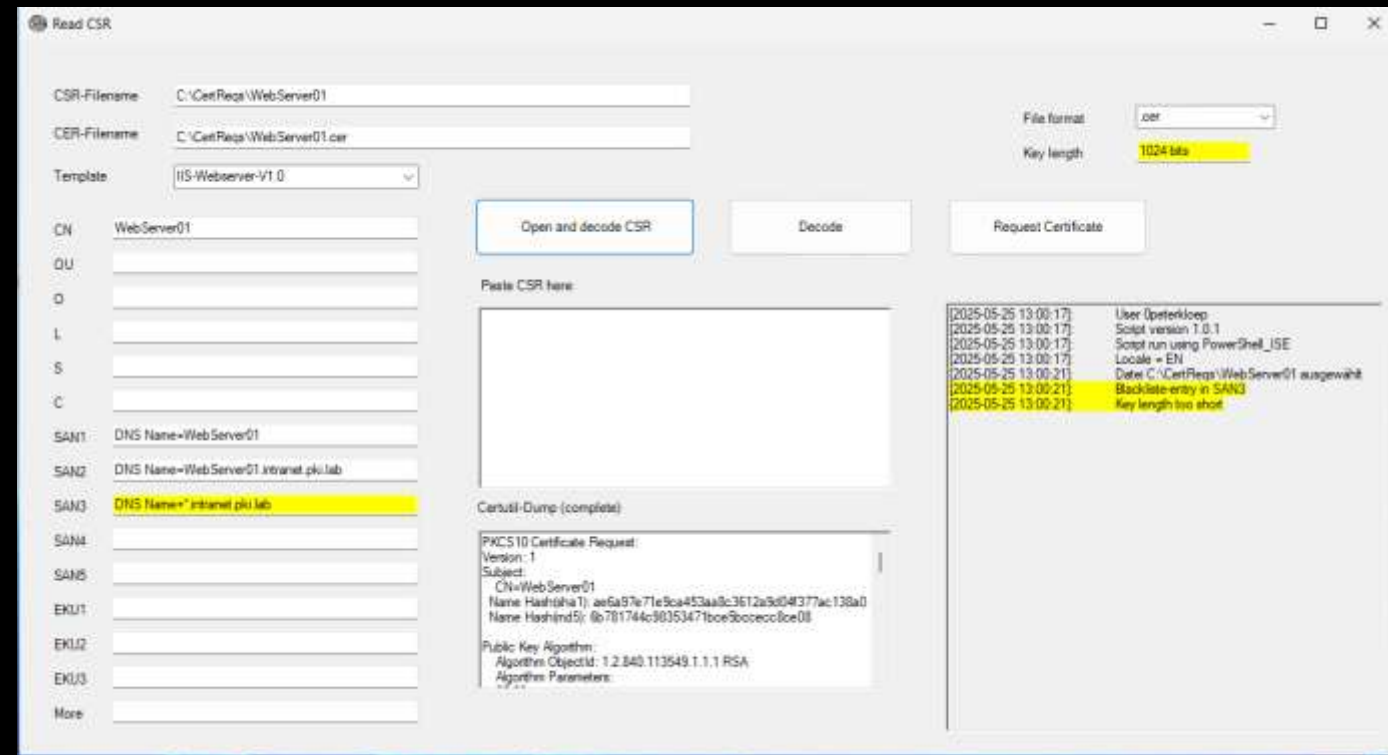
Insecure Configuration (deprecated features)

Legacy Tools:



The screenshot shows a web browser window with the URL `https://webinar-subca.intranet.pki.l...`. The page title is "Microsoft Active Directory Certificate Services – WEBINAR-SUBCA-CA". The main content area has a "Welcome" heading and a paragraph explaining the site's purpose: "Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks." Below this, it states: "You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request." A link is provided: "For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#)." At the bottom, under "Select a task:", there are three links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

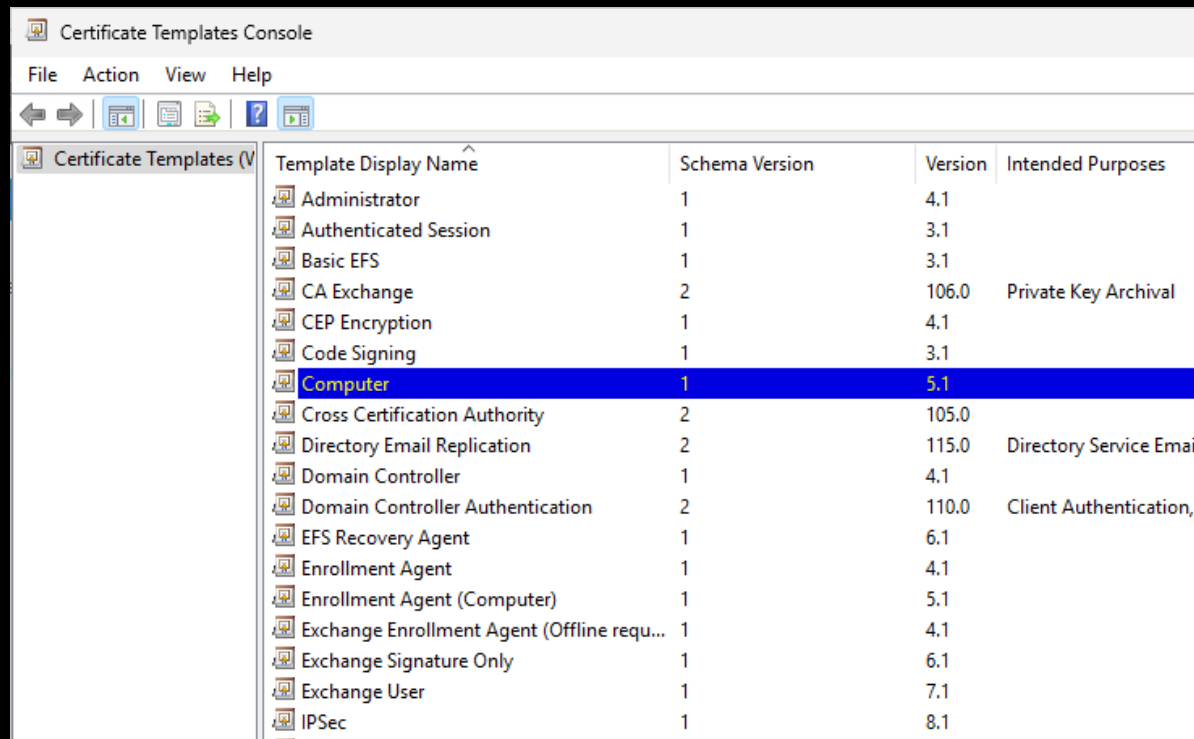
Better option:



The screenshot shows a "Read CSR" application window. It has several input fields: "CSR-Filename" (C:\CertReqs\WebServer01), "CER-Filename" (C:\CertReqs\WebServer01.cer), and "Template" (IIS-Webserver-V1.0). There are three buttons: "Open and decode CSR", "Decode", and "Request Certificate". Below the input fields, there are sections for "CN", "OU", "O", "L", "S", "C", "SAN1", "SAN2", "SAN3", "SAN4", "SAN5", "EKU1", "EKU2", "EKU3", and "More". The "SAN3" field is highlighted in yellow and contains the text "DNS Name=*.intranet.pki.lab". To the right of the input fields, there are two buttons: "Open and decode CSR" and "Decode". Below these buttons, there is a "Paste CSR here:" label and a text area. To the right of the text area, there is a "File format" dropdown menu set to ".cer" and a "Key length" field set to "1024 bits". Below the text area, there is a "Certificate Dump (complete)" section showing a PKCS10 Certificate Request. The dump includes fields like "Version: 1", "Subject: CN=WebServer01", "Name Hash(ha1): ae6a97e71e9ca453aa8c3612a9d04377ac138a0", "Name Hash(md5): 6b781744c98153471bce930eccc0ce08", "Public Key Algorithm: Algorithm ObjectID: 1.2.840.113549.1.1.1 RSA", and "Algorithm Parameters: ...". On the far right, there is a log window showing a series of timestamps and messages, including "User: Opeterkloop", "Script version: 1.0.1", "Script run using PowerShell_ISE", "Locale = EN", "Date: C:\CertReqs\WebServer01 ausgewählt", "Backdate entry in SAN3", and "Key length too short".

Insecure Configuration (templates)

Template Version:




The screenshot shows the 'Certificate Templates Console' window. The 'Certificate Templates (V)' tree on the left has 'Computer' selected. The main pane displays a table of certificate templates.


Template Display Name	Schema Version	Version	Intended Purposes
Administrator	1	4.1	
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Key Archival
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Service Email
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication,
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	


Template Permissions:


Subject Name		Server		Issuance Requirements	
Compatibility	General	Request Handling	Cryptography	Key Attestation	
Superseded Templates			Extensions		Security


Group or user names:

 Authenticated Users

 ORAPKI (INTRANET\ORAPKI)

 Domain Admins (INTRANET\Domain Admins)

 Domain Computers (INTRANET\Domain Computers)

 Enterprise Admins (INTRANET\Enterprise Admins)

Add...

Remove

Permissions for Domain Computers	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Insecure Configuration (templates)

Common misunderstanding:

Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation
Purpose: Signature and encryption				
<input type="checkbox"/> Delete revoked or expired certificates (do not archive)				
<input type="checkbox"/> Include symmetric algorithms allowed by the subject				
<input type="checkbox"/> Archive subject's encryption private key				
<input type="checkbox"/> Authorize additional service accounts to access the private key (*)				
Key Permissions...				
<input type="checkbox"/> Allow private key to be exported				
<input type="checkbox"/> Renew with the same key				
<input type="checkbox"/> For automatic renewal of smart card certificates, use the existing key if a new key cannot be created				

Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation
Purpose: Signature and encryption				
<input type="checkbox"/> Delete revoked or expired certificates (do not archive)				
<input type="checkbox"/> Include symmetric algorithms allowed by the subject				
<input checked="" type="checkbox"/> Archive subject's encryption private key				
<input type="checkbox"/> Authorize additional service accounts to access the private key (*)				
Key Permissions...				

**g0t Qu3stion\$?
(remember g0tmi1k?)**



#3. Top „Backdoors“



Escalation Attacks against AD CS (ESC)

ESC1: Misconfigured Certificate Template (Account with enroll permission, Requestor supplied in the request, ClientAuthentication, no Manager Approval)

➔ Requestor can supply SAN (e.g. administrator@pki.lab) and can authenticate using the cert (fixed in 2025-02)

ESC2: Similar to ESC1, but "Any Purpose" as EKU

➔ Requestor can supply SAN (e.g. administrator@pki.lab) and can authenticate using the cert (fixed in 2025-02)

Escalation Attacks against AD CS (ESC)

ESC3: Misconfigured Certificate Template for Enrollment Agent

➔ Requestor can request other certificates for different users (e.g. administrator@pki.lab) and can authenticate using the cert.

ESC4: Write-Permission on CA templates for non-Admins

➔ Lead to ESC1-3 vulnerability

Escalation Attacks against AD CS (ESC)

ESC5: Misconfigured Permission in Active Directory

➔ Attacker can modify trusted CAs and or can control computer settings.

ESC6: If the EDITF_ATTRIBUTESUBJECTALTNAME2 is enabled on the CA

➔ Lead to ESC1-3 vulnerability

Escalation Attacks against AD CS (ESC)

ESC7: Wrong permission on CA: Non-Admin (CertManager) have Manage CA permission

→ Attacker can modify CA registry which leads to ESC6.

ESC8: NTLM replay attack against web service (Certsrv / CEP / CES). Also called PetitPotam

→ Forge Certificate for DomainController to authenticate as DC

Escalation Attacks against AD CS (ESC)

ESC9: If StrongCertificateBindingEnforcement is not enabled (enabled by 2025-02) and attacker has permission on user account
→ leads to ESC1-3.

ESC10: StrongCertificateBindingEnforcement is configured insecure and the attacker can use SAN entry to authenticate as Computer (DC)
→ Forge Certificate for DomainController to authenticate as DC and gain access to critical data

Escalation Attacks against AD CS (ESC)

ESC11: NTLM replay attack if RPC encryption is not enforced

→ leads to ESC1-3.

ESC12: CAs Private key compromise with Yubikey HSM

→ Access Key („Password“) is stored in registry and can be used to recover key. Sign new certs.

Escalation Attacks against AD CS (ESC)

ESC13: If msDS-OldToGroupLink is used and accounts have enroll permission on the template they are a member of the group without being a member in AD

ESC14: use altSecurityIdentities with explicit certificate mapping.

Escalation Attacks against AD CS (ESC)

ESC15: Misuses Application Policies in V1-Templates when subject name is supplied in the request

ESC16: CA is configured not to add SID to certificates which might bypass StrongCertificateMapping (if not required by DomainControllers)

PetitPotam



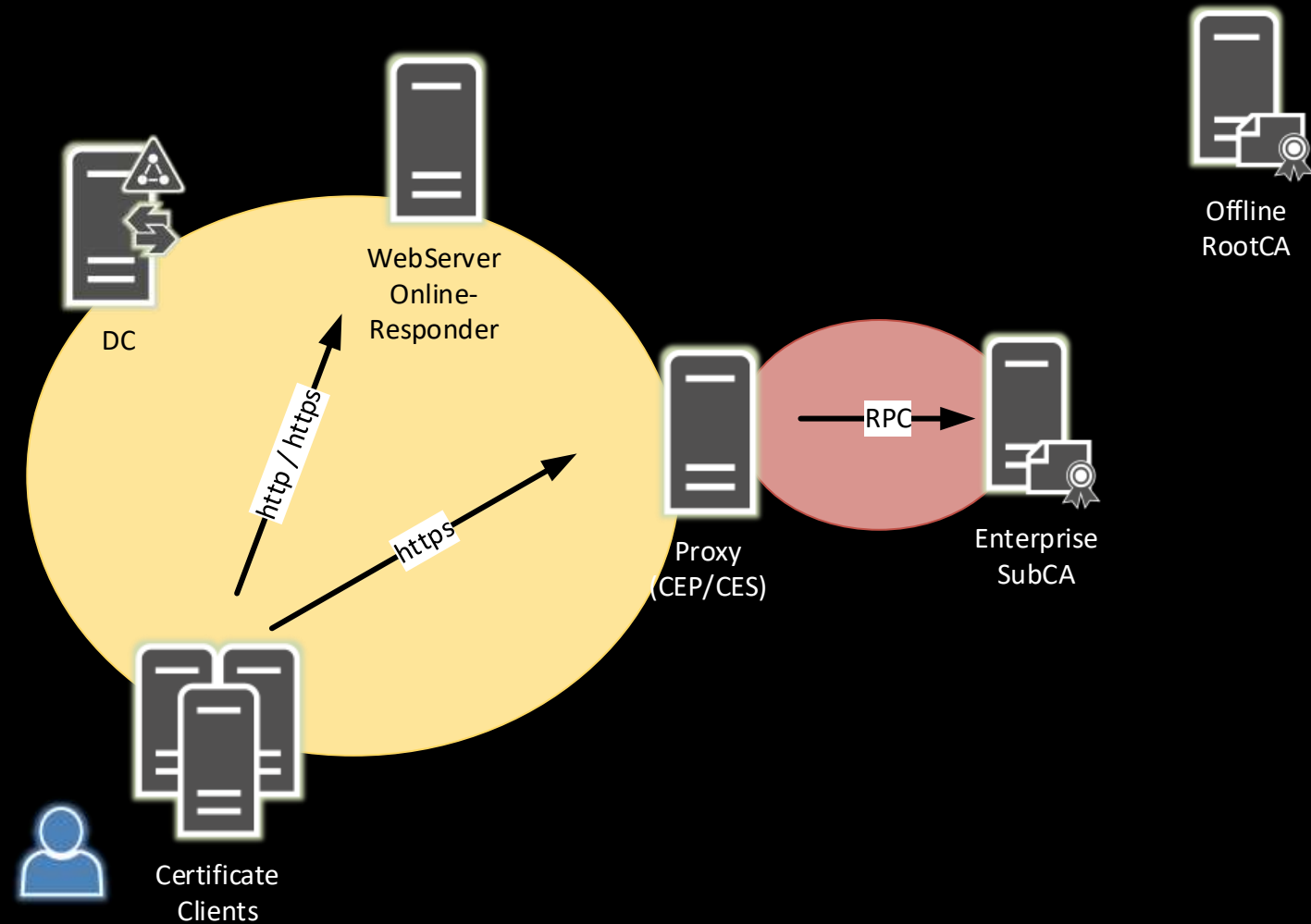
Maybe questions?



#4. Secure Design



How it can look like?



Security considerations

1. Apply all Tier0 protections
2. Restrict Access
3. Limit network connection
4. Audit Services and Configuration changes
5. Do your housekeeping (Patching / Updates)

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

#5. Permissions for Templates



Auditing

[GitHub - GhostPack/Certify: Active Directory certificate abuse.](#)

Certify is a C# tool to enumerate and abuse misconfigurations in Active Directory Certificate Services (AD CS).

[@harmj0y](#) and [@tifkin](#) are the primary authors of Certify and the the associated AD CS research

Do You want to **Enhance** Your
Windows Security Knowledge?

ADVANCED WINDOWS SECURITY COURSE 2026



CQURE

Is *this* course for you?



Intermediate/Advanced



Ethical hacker



Brave Newbies

What's *Really at Stake* If You Don't Level Up?



Failed Security Audits



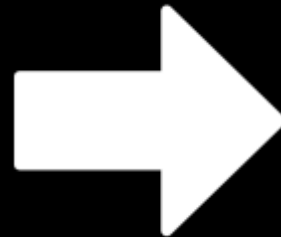
Successful Breaches



Career Stagnation



Budget Rejections



Become the Go-To Expert



Protect Company Assets

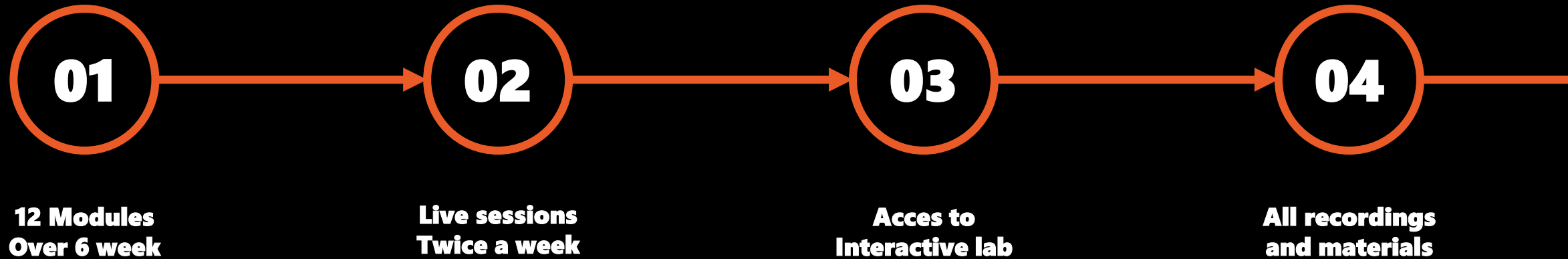


Unlock Career Growth



Build Executive Trust

What's inside **ADVANCED WINDOWS SECURITY COURSE 2026** ?



What's inside **ADVANCED WINDOWS SECURITY COURSE 2026** ?

05

**CQURE
Tools/Examples
Scripts**

06

**Discord
community**

07

**Final
certification**

You Could Do It Alone.

Or You Could Do It Right.

***Advanced Windows
Security Course is:***



Structured



Time efficient



Expert Led



Advanced Windows Security Course 2026



LIVE Trainings

You'll join our 2-hour long live classes on a special interactive platform – happening twice a week at 7PM CET (10 AM PST / 1 PM EST).



Action packed

You'll go through 12 modules in 6 weeks. We're not fluffing around, you've been warned.



Once a Year Only

We organize this course only once a year, in its last quarter. The 2026 edition is updated with latest trends, new tools, and challenges.



Extra Materials

We've prepared for you tools, slides, extra materials, and homework for each session.



12-month Access

You'll get a full year of online access to all the recordings counted from the first class.



The Training Lab

During the course, you'll have access to a special training platform where you can safely test your hacks.



Social & Network

You'll become a member of a closed Discord group, where you can not only share your challenges and geeky jokes, but also network.



CQURE Certificate – "Windows Security Master 2026"

You'll receive an official CQURE certificate "Windows Security Master 2026" after passing the final exam. Yes, there will be a final exam.



Interactive Classroom

After every class, you'll be able to ask questions.

PRE-SALE APPLICATION DISCOUNT FOR AWSC26

PRE-SALE PRICE

\$1899 **save \$1300**

Valid only till 30th June 2025



<https://cqu.re/awsc26>

APPLY NOW.
PAY LATER.

Available
BY APPLICATION
ONLY.

Here's How to Apply



Your Instructors



Paula Januszkiewicz

Founder & CEO, Microsoft Regional
Director, MVP, MCT



Sami Laiho

Windows OS Expert,
MVP



Peter Kloep

Cybersecurity Expert,
Principal IT Architect



Your Instructors



Marcin Krawczyk

Cloud & Cybersecurity Expert



Damian Widera

Data Platform MVP, MCT,
Software Engineer,
Cybersecurity Expert



Artur Kalinowski

Cybersecurity Expert

Your Instructors



Amr Thabet

Cybersecurity Expert



Przemysław Tomasiak

Cybersecurity Expert



Jan Marek

MVP, MCT, Microsoft
Security Specialist



Who are our alumni?



Milan Racko

IT Security Specialist



Kamil Więcek

Senior DevOps Expert

Ready to join?

APPLY NOW!



CQURE

PRE-SALE APPLICATION DISCOUNT FOR AWSC26

PRE-SALE PRICE

\$1899 **save \$1300**

Valid only till 30th June 2025



<https://cqu.re/awsc26>

APPLY NOW.
PAY LATER.

Available
BY APPLICATION
ONLY.

**CHALLENGE
WINNER**



Q&A Time!



**Visit our BLOG and discover more about
cybersecurity solutions & tools:**

<https://cquireacademy.com/blog>



DOWNLOAD THE TOOLS

<https://resources.cqureacademy.com/tools/>

Username: student

Password: CQUREAcademy#123!

If you want level up your Windows Cybersecurity Skills



JOIN OUR ONLINE TRAININGS