TPM and certificate logon

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory | MVP:Enterprise Security | CEH | CHFI | CISA |
ondrej@sevecek.com | www.sevecek.com |

moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť
GLAB008 - capture the flag 2 - hackni si podnikovou síť
GOC175 - implementace bezpečnosti
GOC169 - ISO 27001
GOC172 - Kerberos troubleshooting
GOC161 - Cryptography

Agenda

- Why not passwords?
- Why two-factor authentication?
- What is TPM and how it is 1.5 authentication?
- AD CS installation quickly
- DC certificates
- TPM virtual smart card
- Can users obtain logon certificates by themselves?
- Registration authority for issuing TPM logon certificates
- TPM attestation

Passwords

- Easily compromised
  - hardware keyloggers
  - software keyloggers
  - surveillance cameras
- Very long validity
  - can be used from anywhere without user knowing
  - no incident investigation when compromised
- Bad quality
  - lockout vs. availability vs. DoS

Multifactor authentication

- know
  - password
  - PIN
- have
  - card
  - phone
  - notebook
- be
  - biometrics

1.5 authentication

- biometrics on mobile phones
- TPM module on laptops

- must have the device
- must not allow others to the device

Certificate logon with TPM

- bound to the device
- certificate using strong keys
- incident investigation

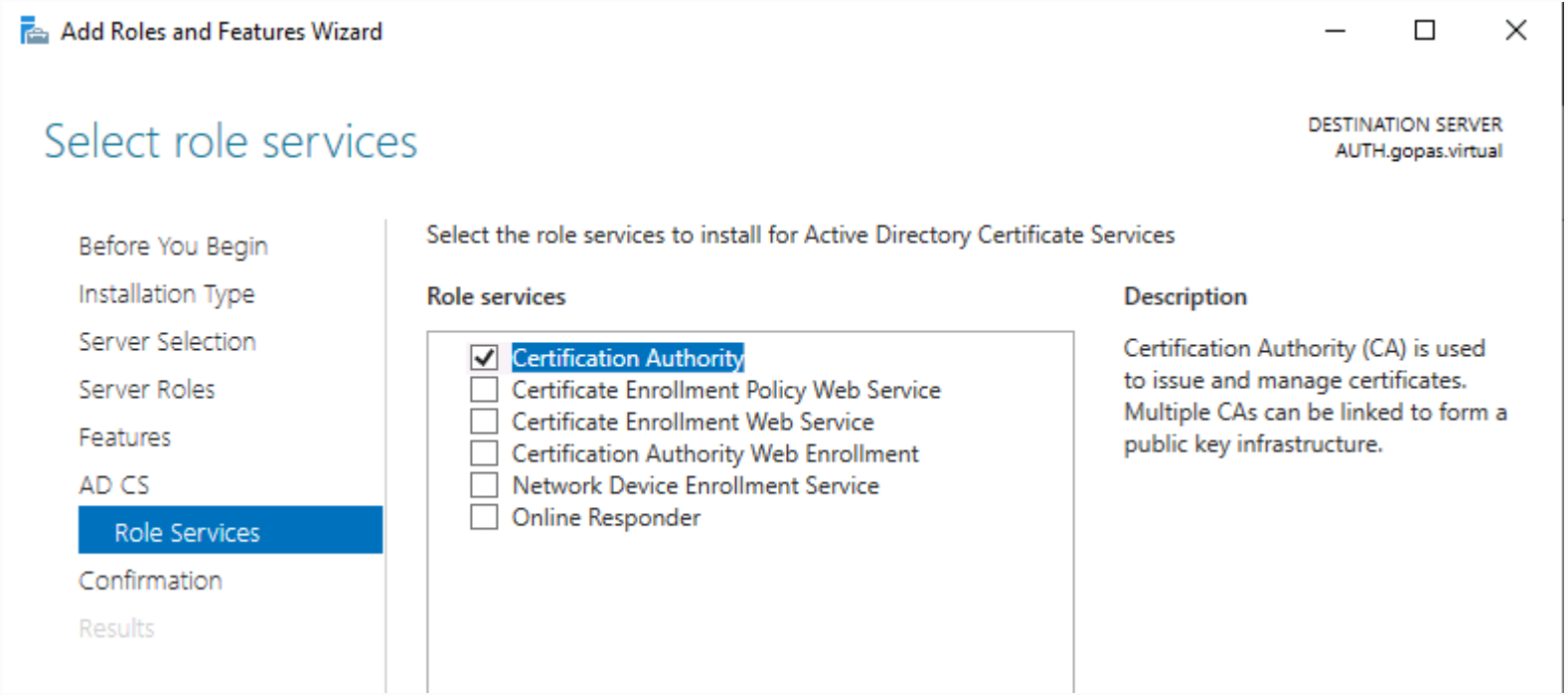
Certificate logon

- Active Directory
  - AD CS
  - DC certificates
  - user logon certificates
  - RA certificates
  - usage
    - CTRL-ALT-DEL
    - RDP
    - HTTPS
    - VPN
    - ADFS vs. Office365
    - Outlook, ActiveSync
- AAD and Office365
  - CA trusted - Get-AzureADTrustedCertificateAuthority
  - individual certificates mapped to user accounts in AAD

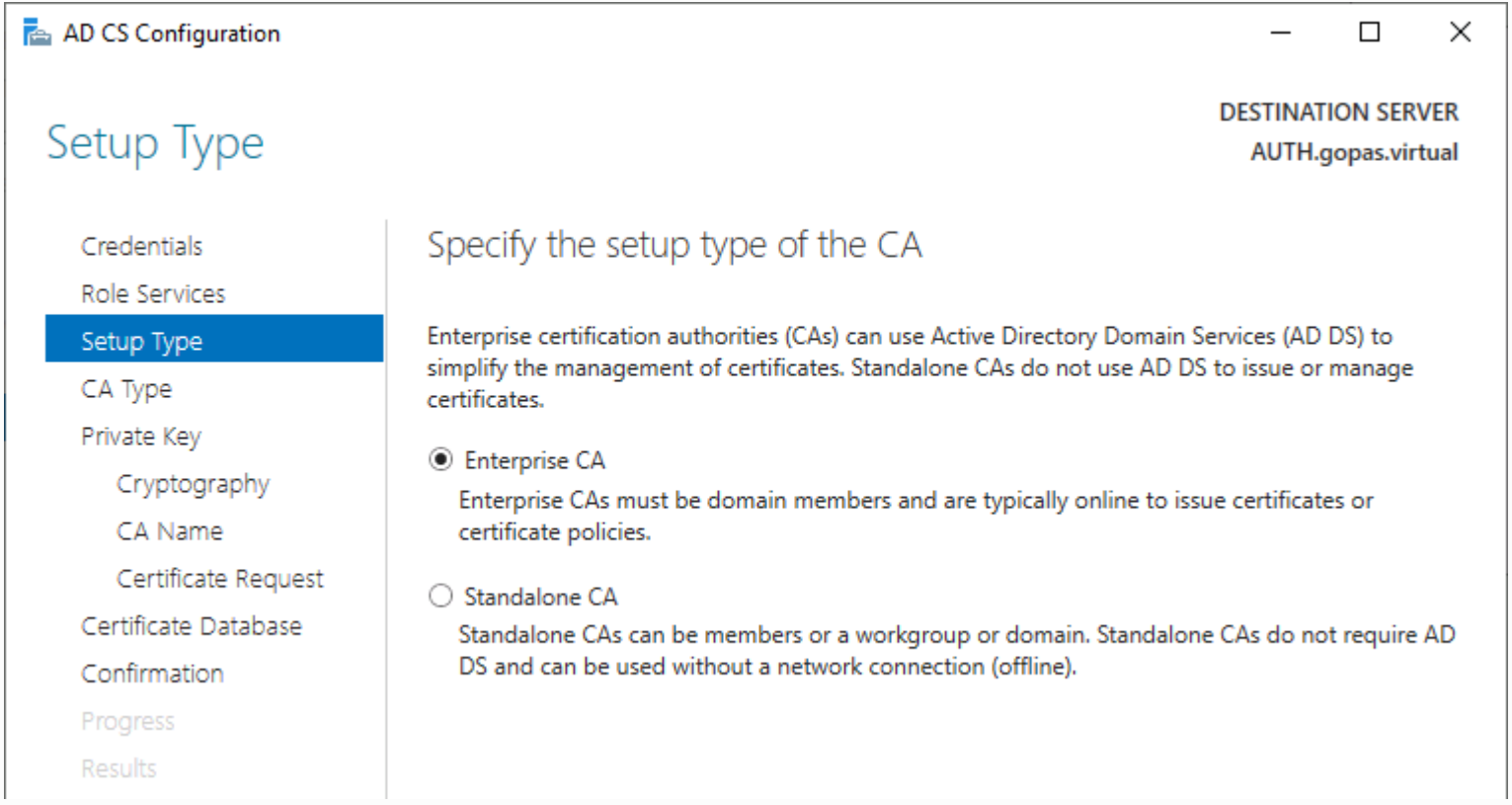
AD CS installation

- keep it safe
  - install on a DC guarantees security
    - Domain Admins
    - physical security

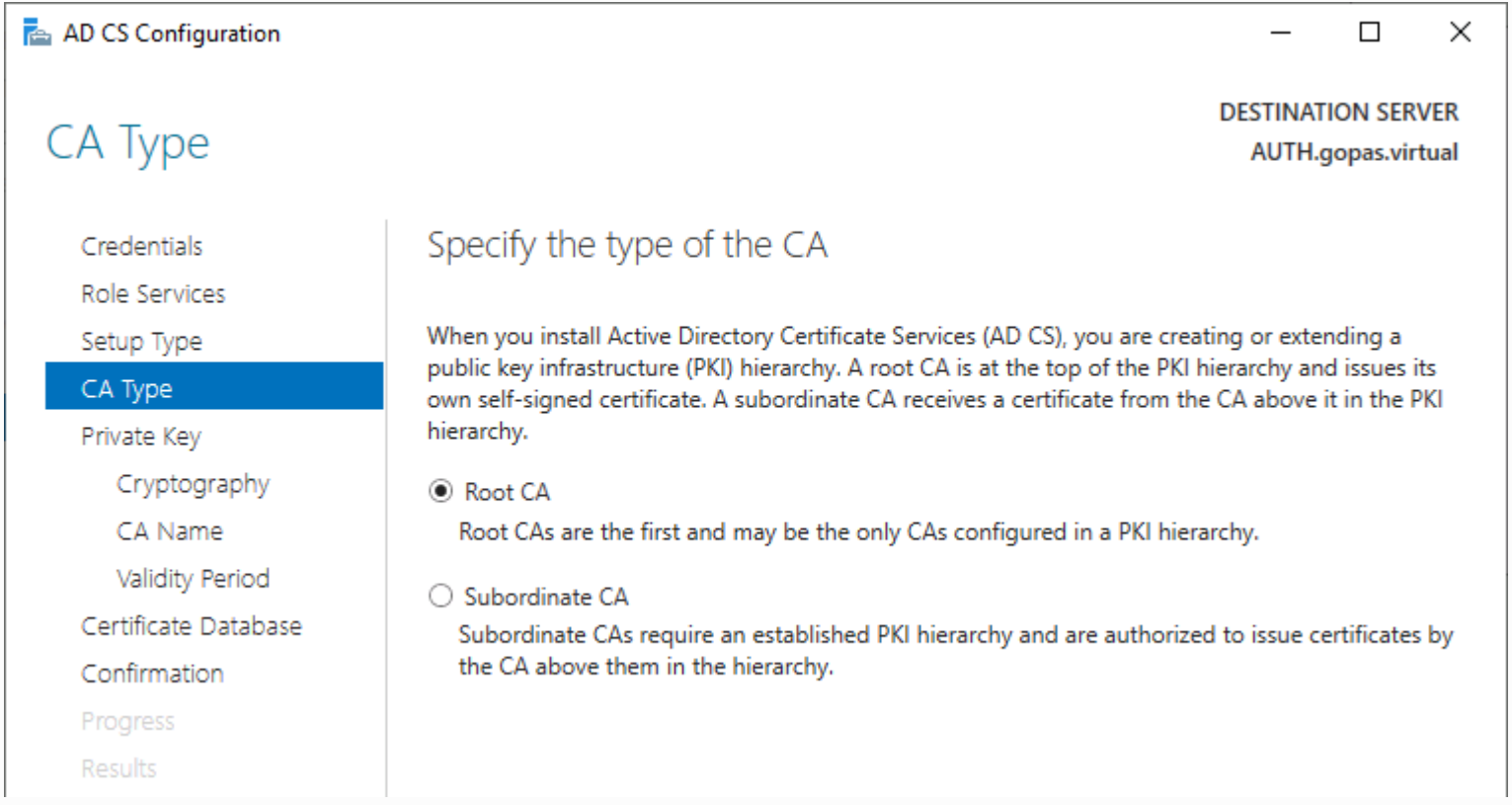
Simplest AD CS installation



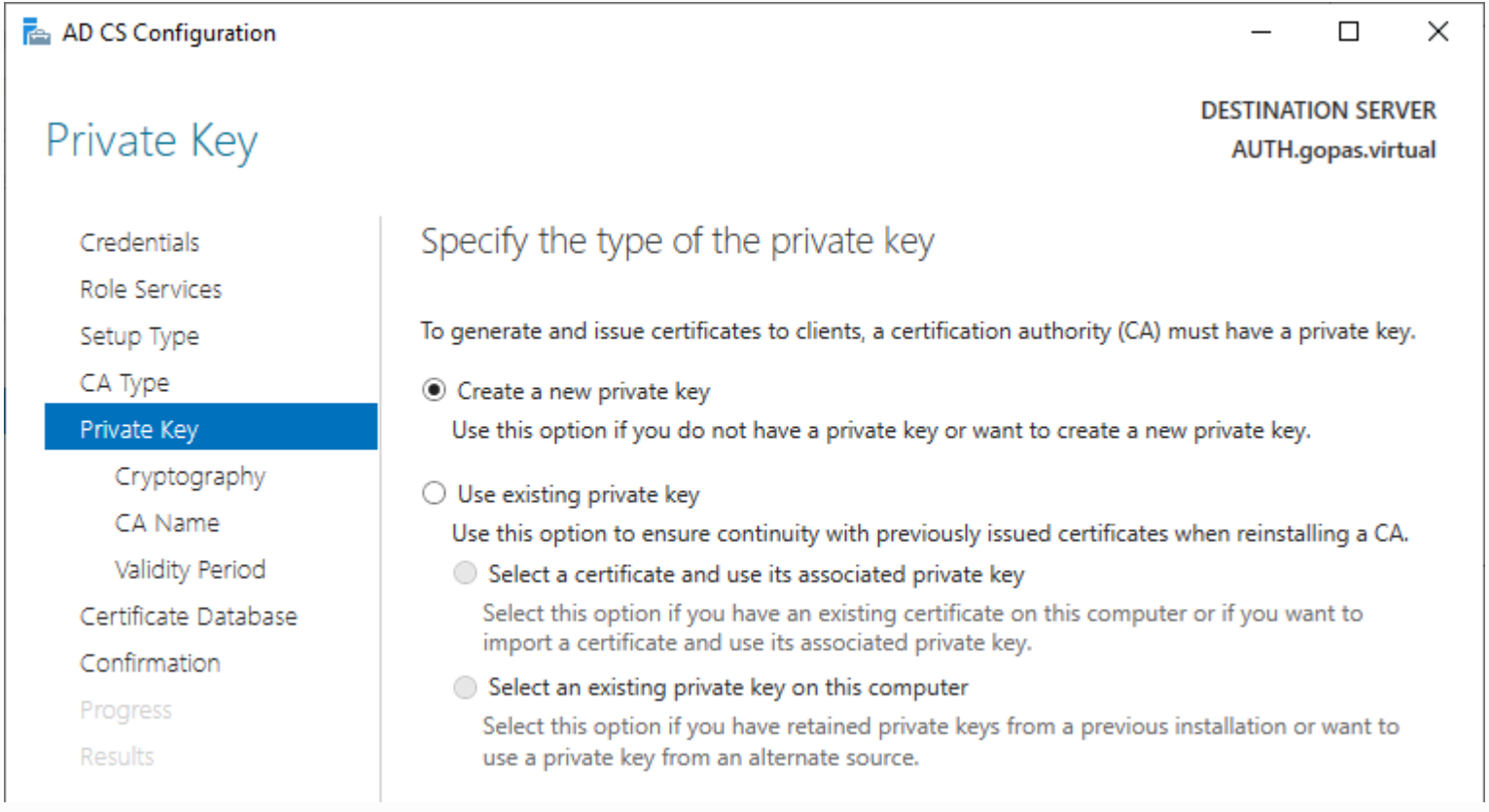
Simplest AD CS installation



Simplest AD CS installation

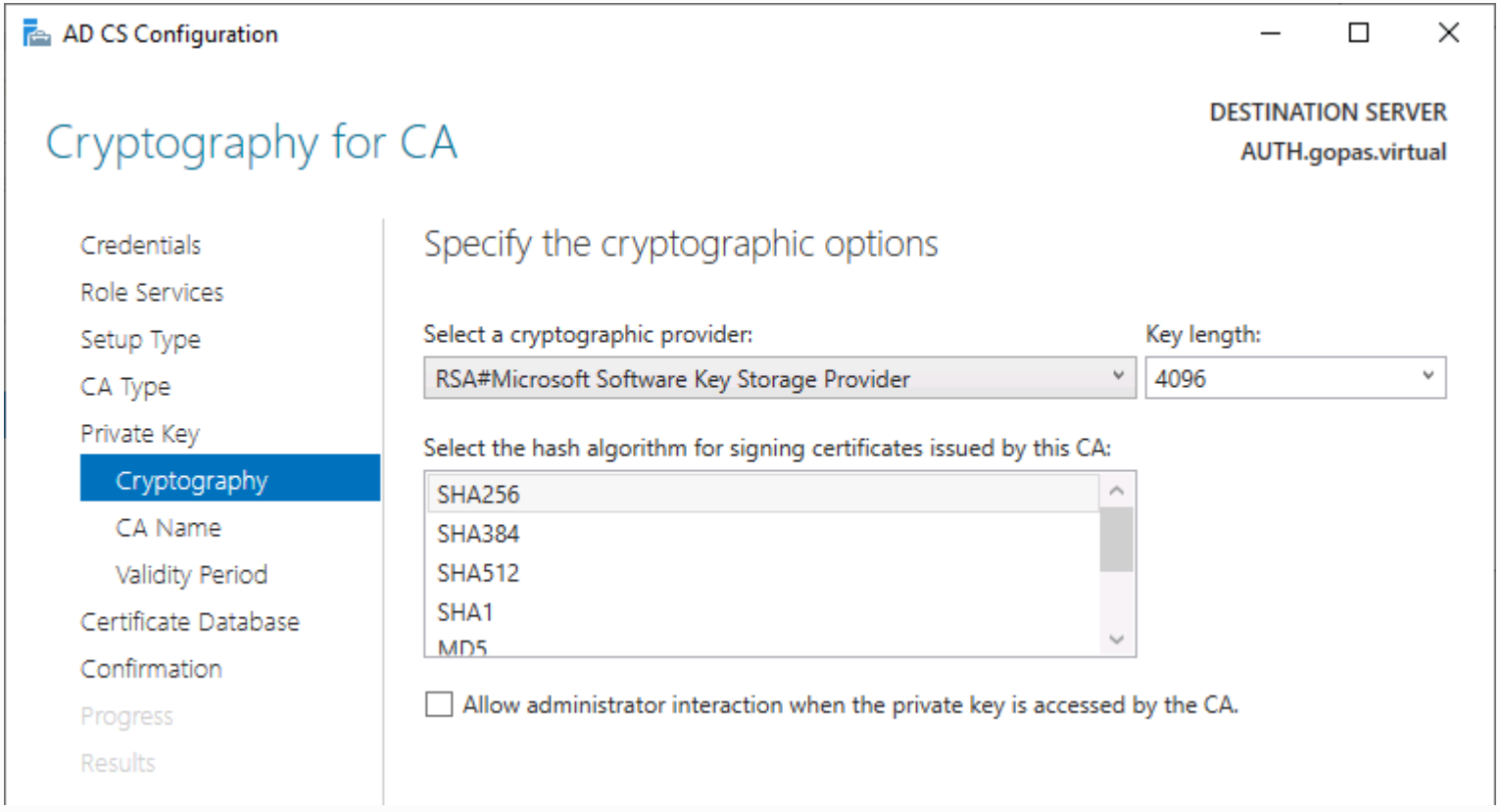


Simplest AD CS installation

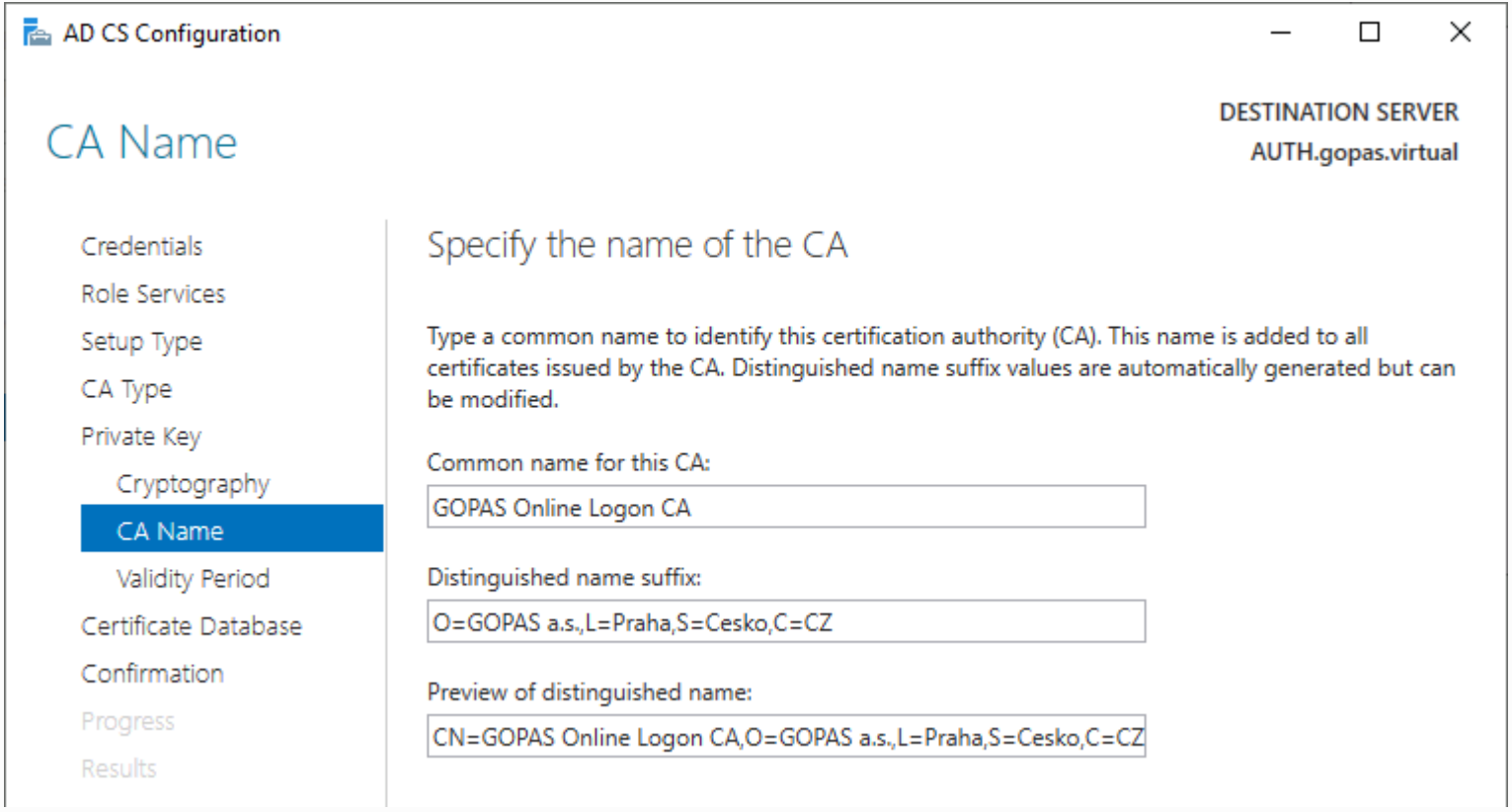


GOPAS
POCITACOVA.SKOLA.CZ

Simplest AD CS installation

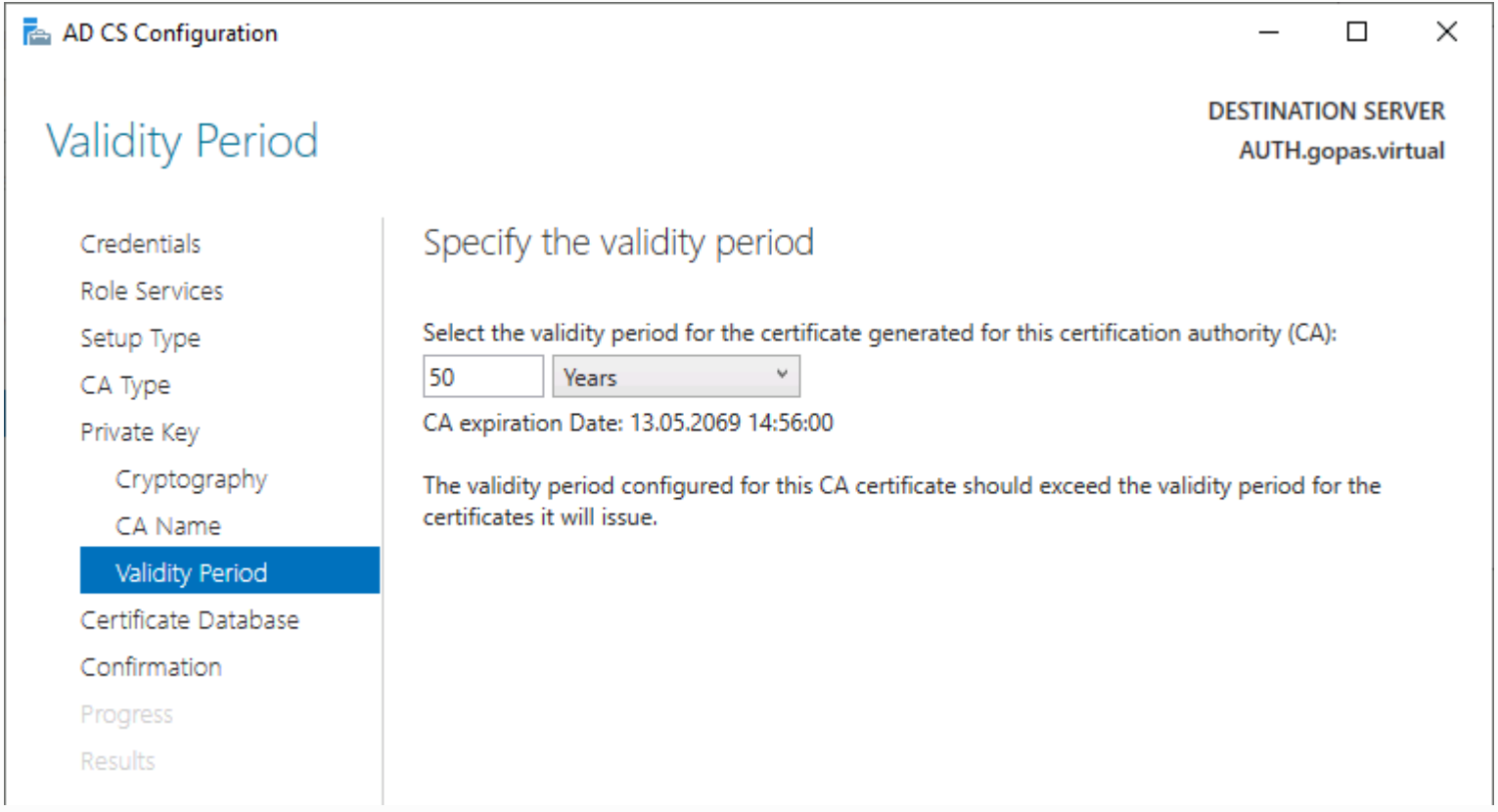


Simplest AD CS installation

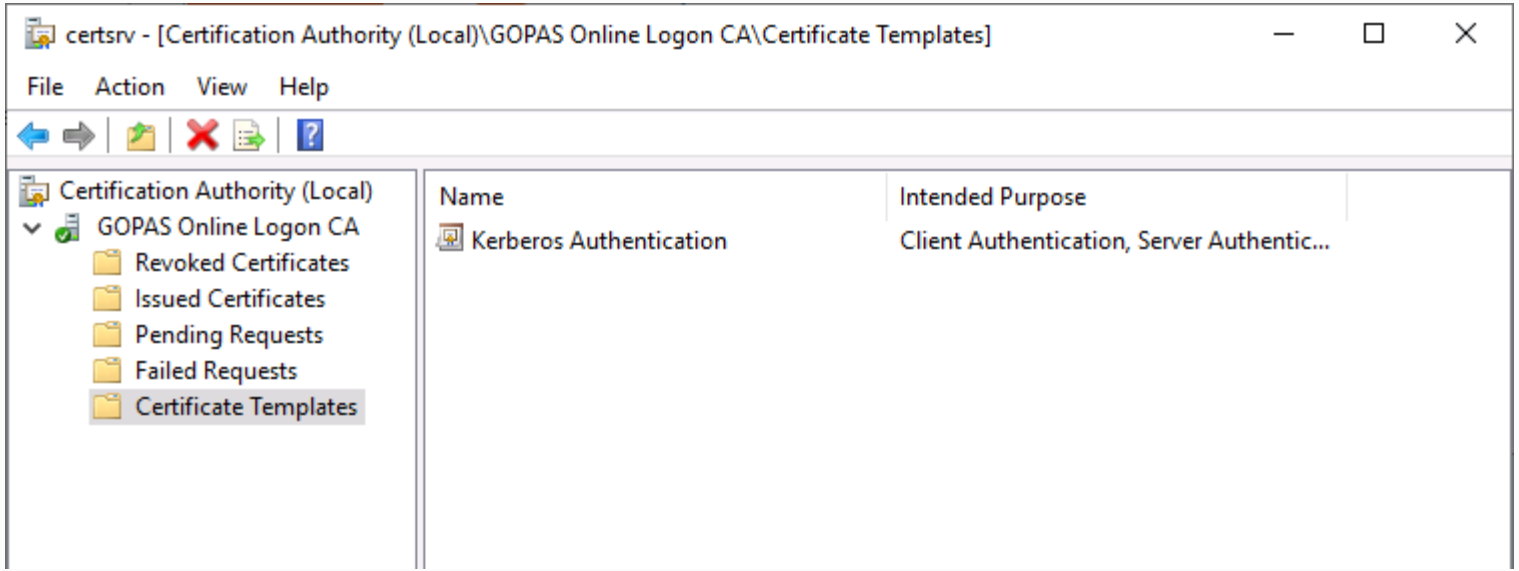


GOPAS
POCITACOVA.SKOLA.CZ

Simplest AD CS installation



Simplest DC certificates with auto-enrollment



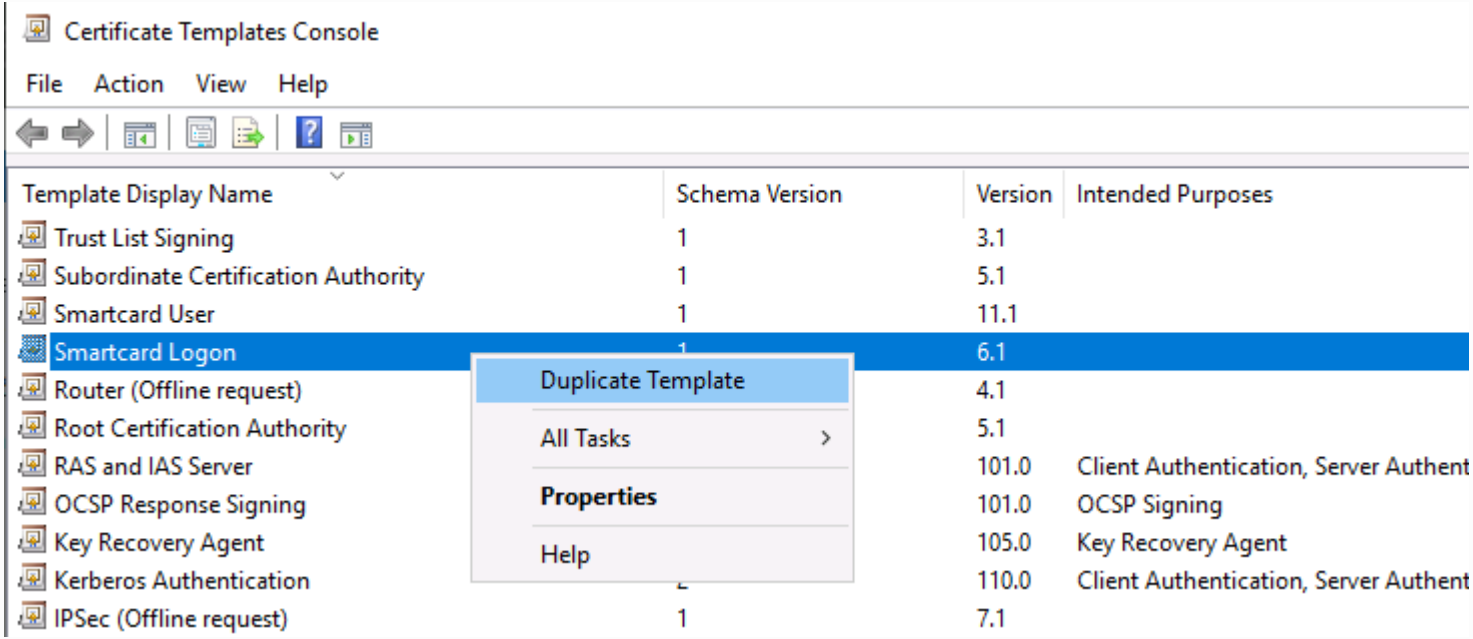
TPM virtual smart card

- TPMVSCMGR
  - create /name ... /pinpolicy minlen 4 uppercase ALLOWED lowercase ALLOWED digits ALLOWED ... /generate
- PUK
  - user knows
- AdminKey
  - 48 digits
  - admin PIN reset by computing a challenge

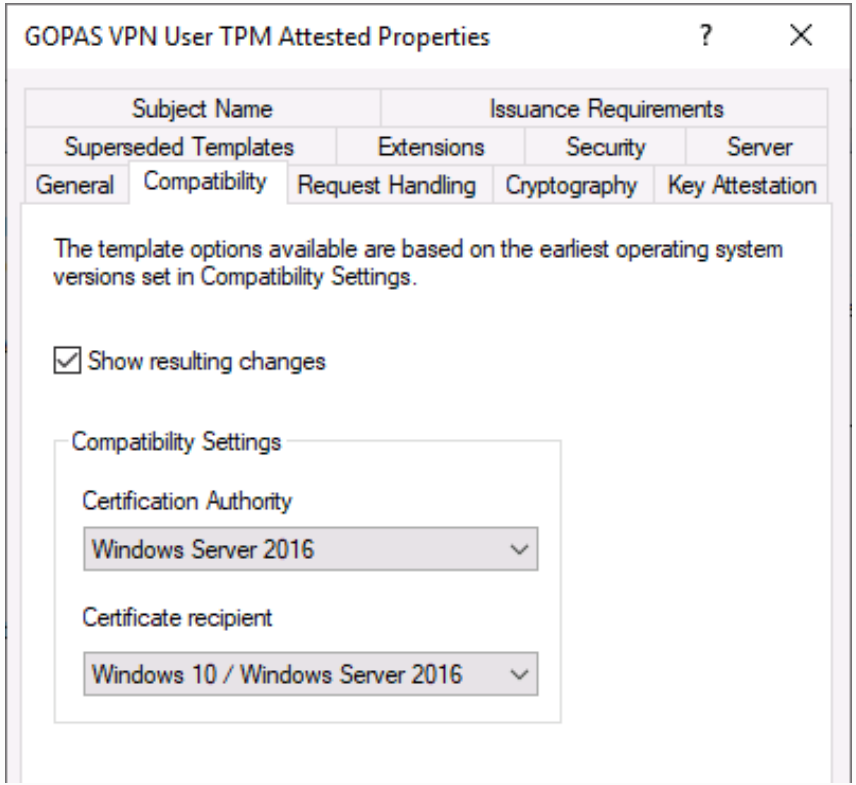
Issuing logon certificates

- Self service
  - free "duplication" and renewal
  - no attestation
- Attestation by workstation admins
- Attestation by TPM key hash
  - machine certificates for 802.1x VPN and WiFi

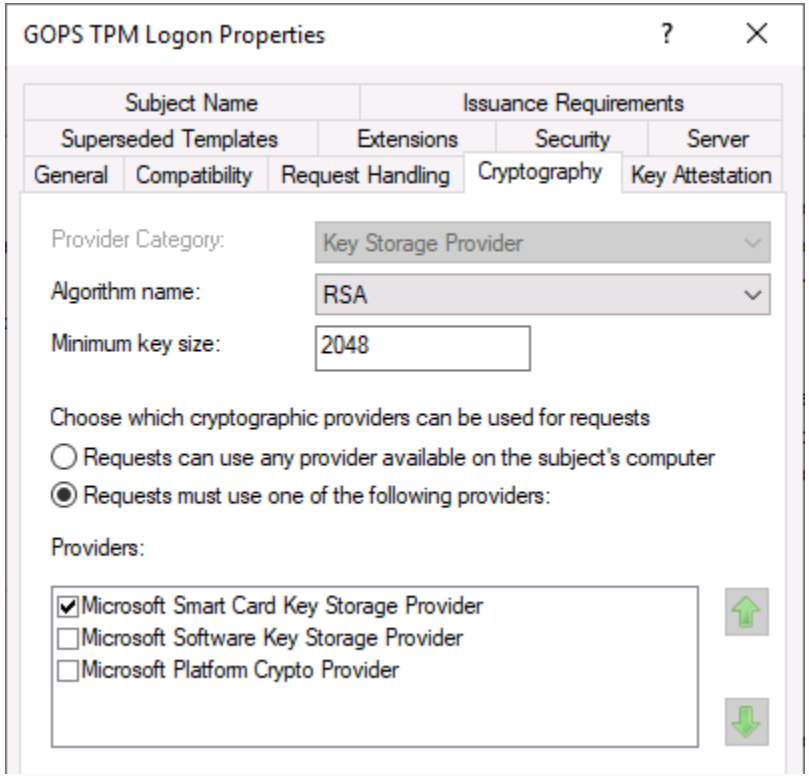
Simple user logon certificate template



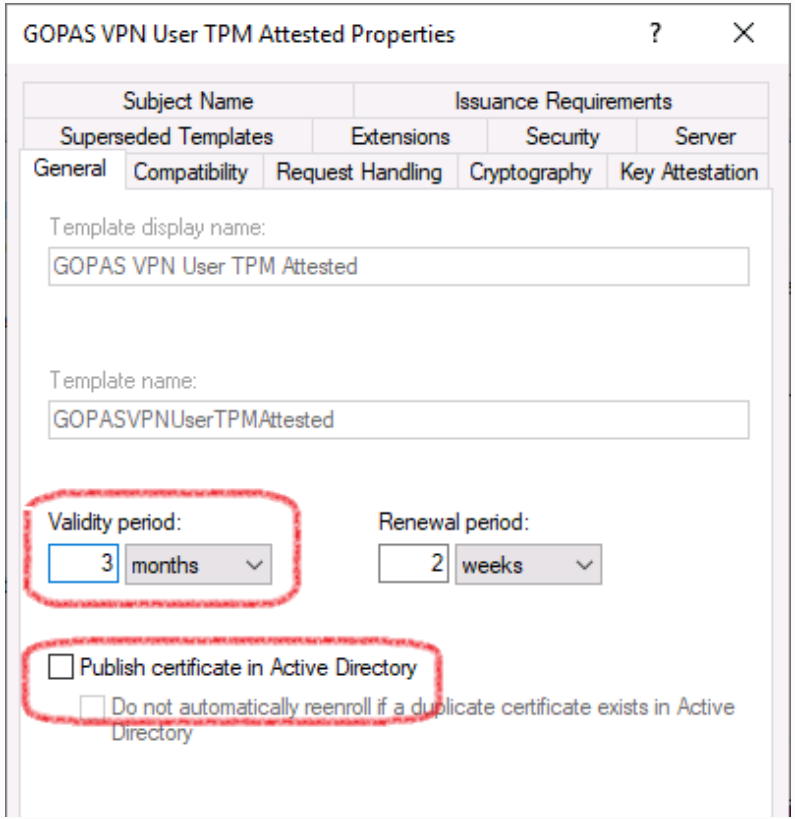
Simple user logon certificate template



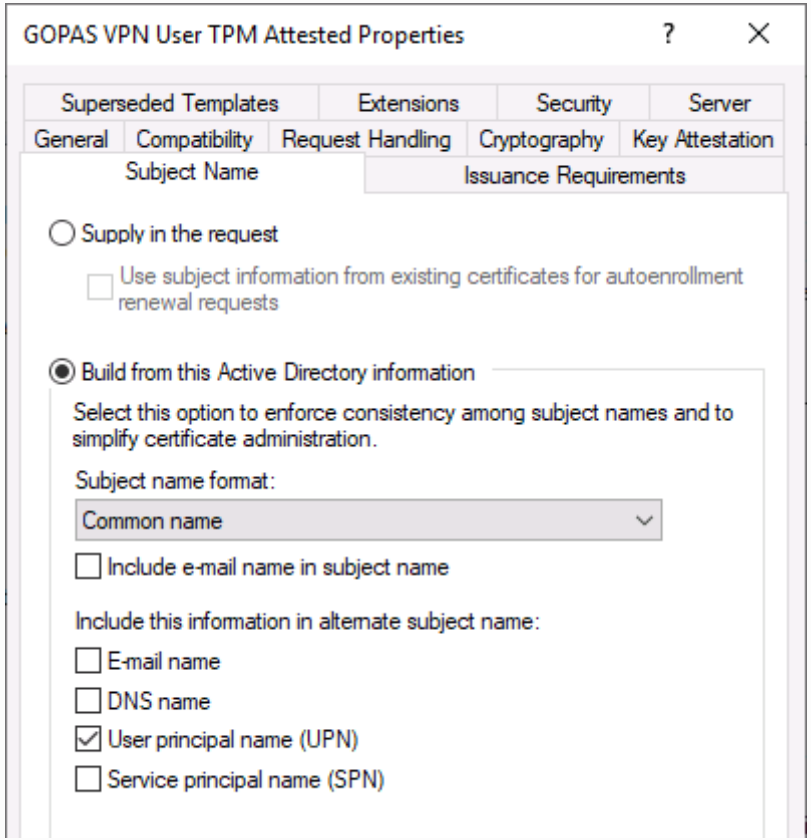
Simple user logon certificate template



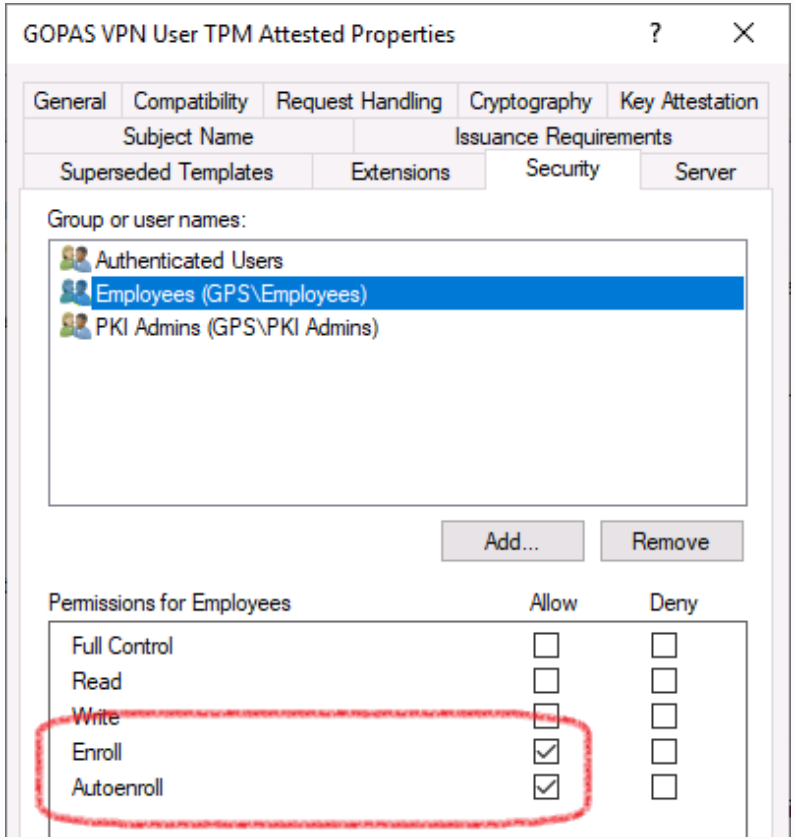
Simple user logon certificate template



Simple user logon certificate template



Simple user logon certificate template

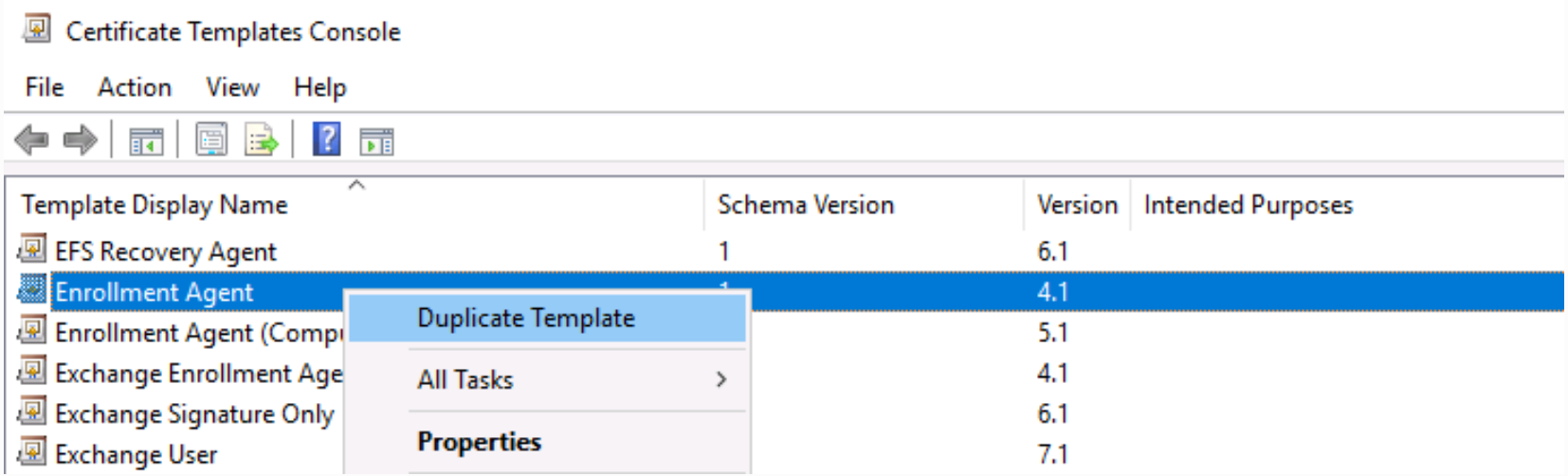


Attestation with RA

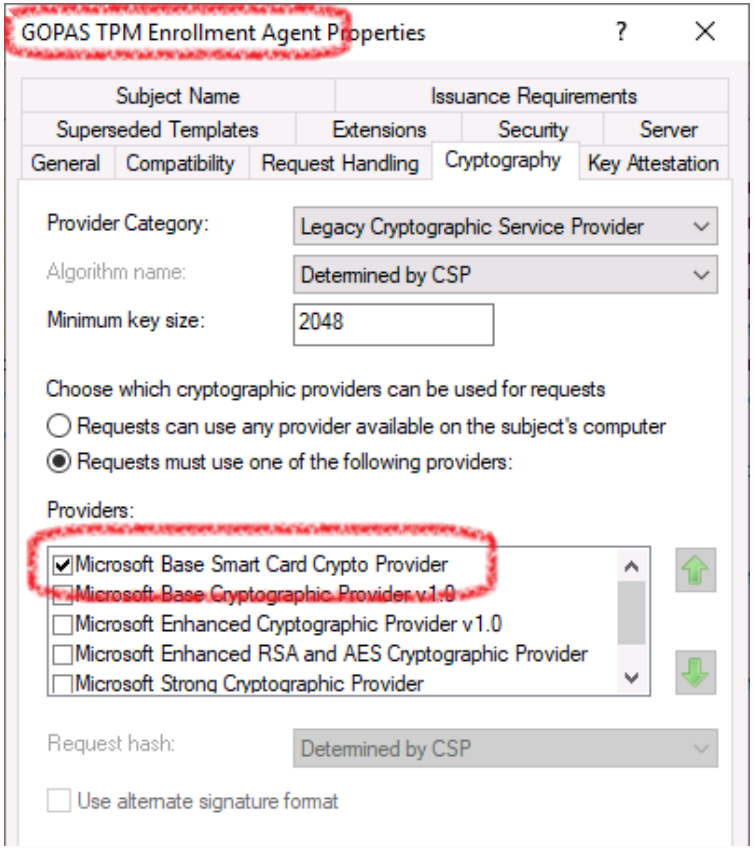
- Enrollment Agent = Registration Authority

- workstation admins issue certificates on behalf of the users
- using RA smart-card

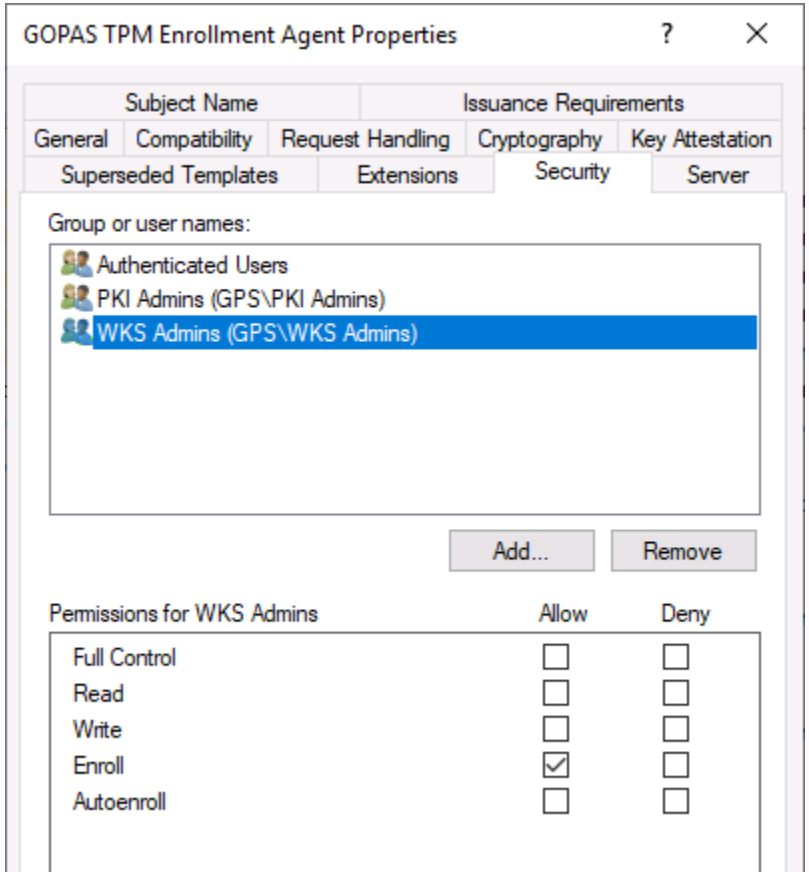
RA certificate for workstation admins



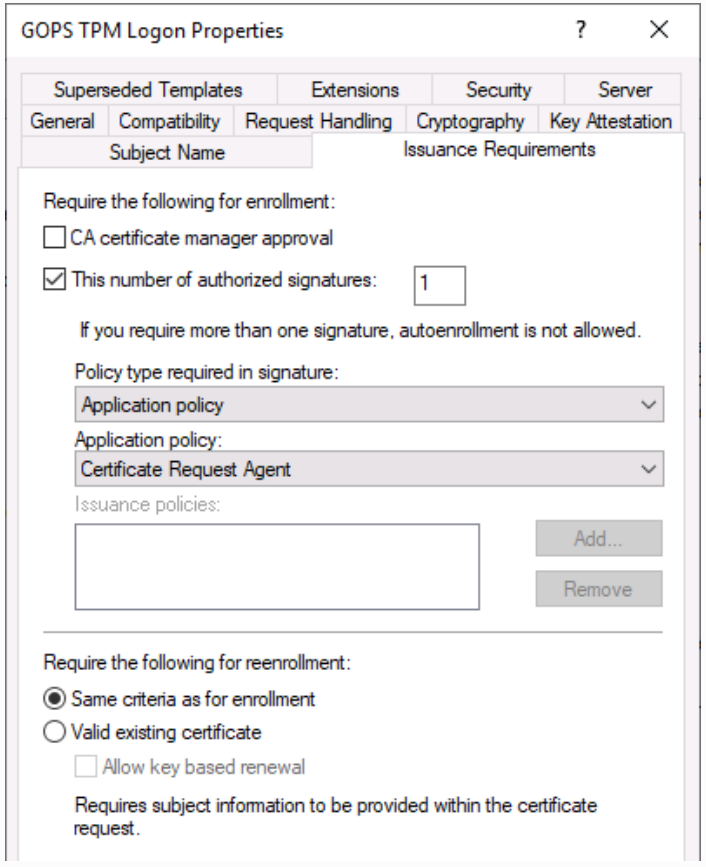
RA certificate for workstation admins



RA certificate for workstation admins



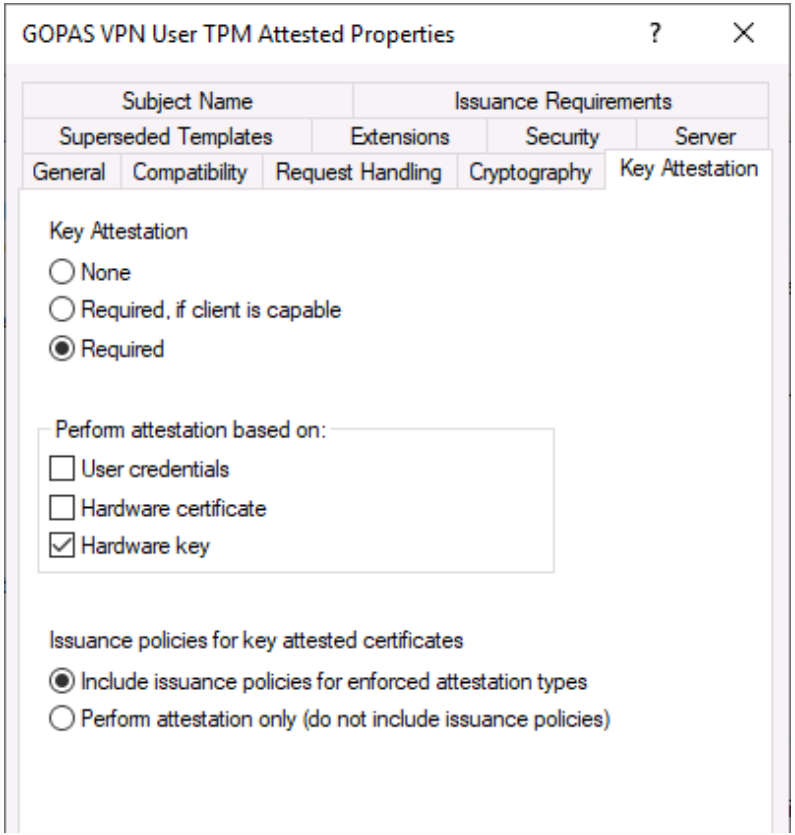
User certificate requiring the RA signature



TPM attestation for machine certificates

- Get-TpmEndorsementInfo -Hash sha256
- certutil.exe -setreg CA\EndorsementKeyListDirectories +"C:\TpmEndorsement"

TPM attestation for machine certificates



Summary

- Strong credentials bound to device

Děkuji za pozornost

moje kurzy v GOPASu
GLAB007 - capture the flag 1 - hackni si podnikovou síť GLAB008 - capture the flag 2 - hackni si podnikovou síť GOC175 - implementace bezpečnosti GOC169 - ISO 27001 GOC172 - Kerberos troubleshooting GOC161 - Cryptography

www.**gopas.cz**