

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

PLATINUM PARTNER



GOLD PARTNER

DEVCON HALL SHOWIT HALL



SILVER PARTNER

PROFINIT
NÁSKOK DÍKY ZNALOSTEM

GENERAL PARTNER



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

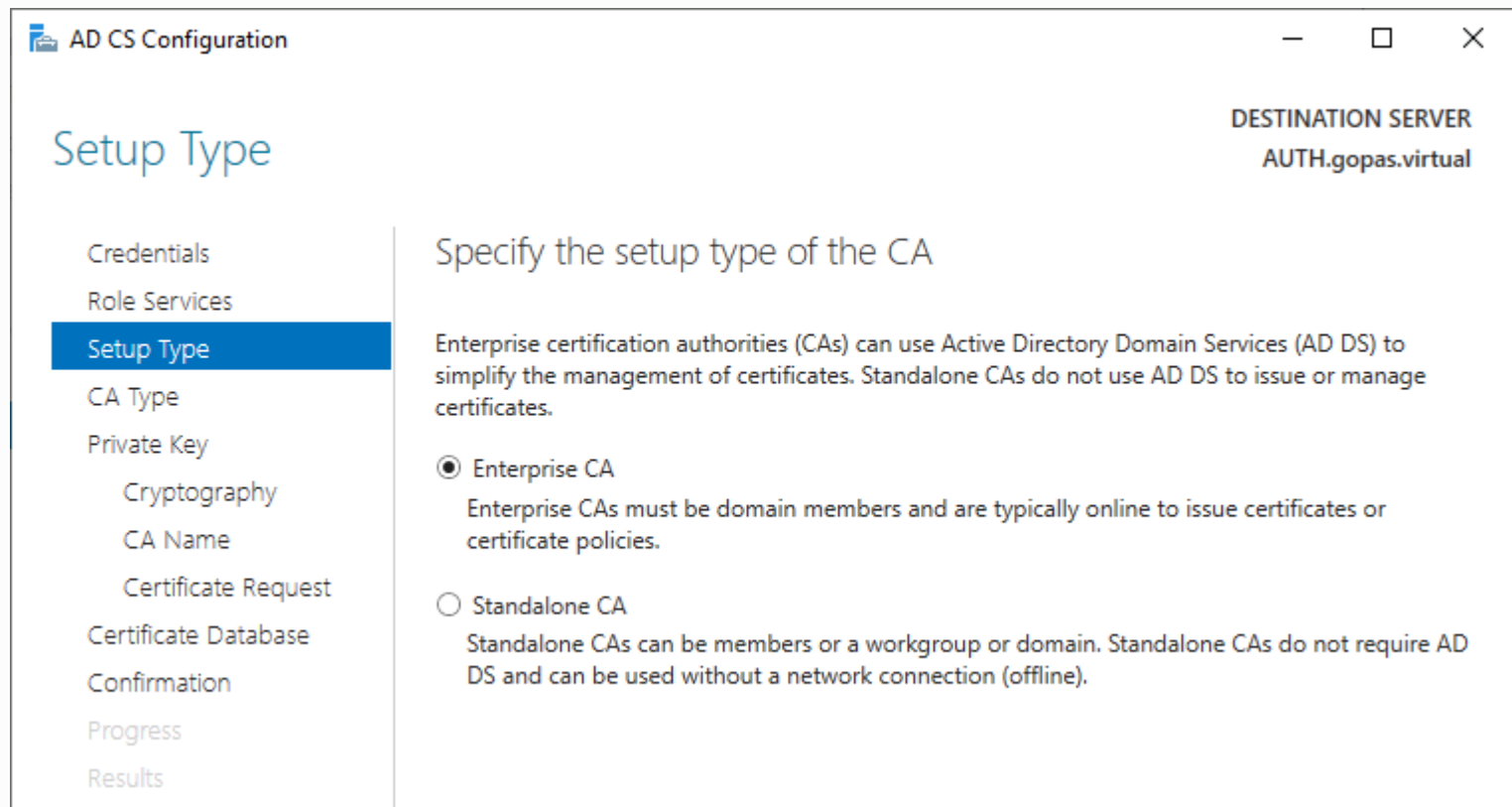
AD CS installation

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

Simplest AD CS installation

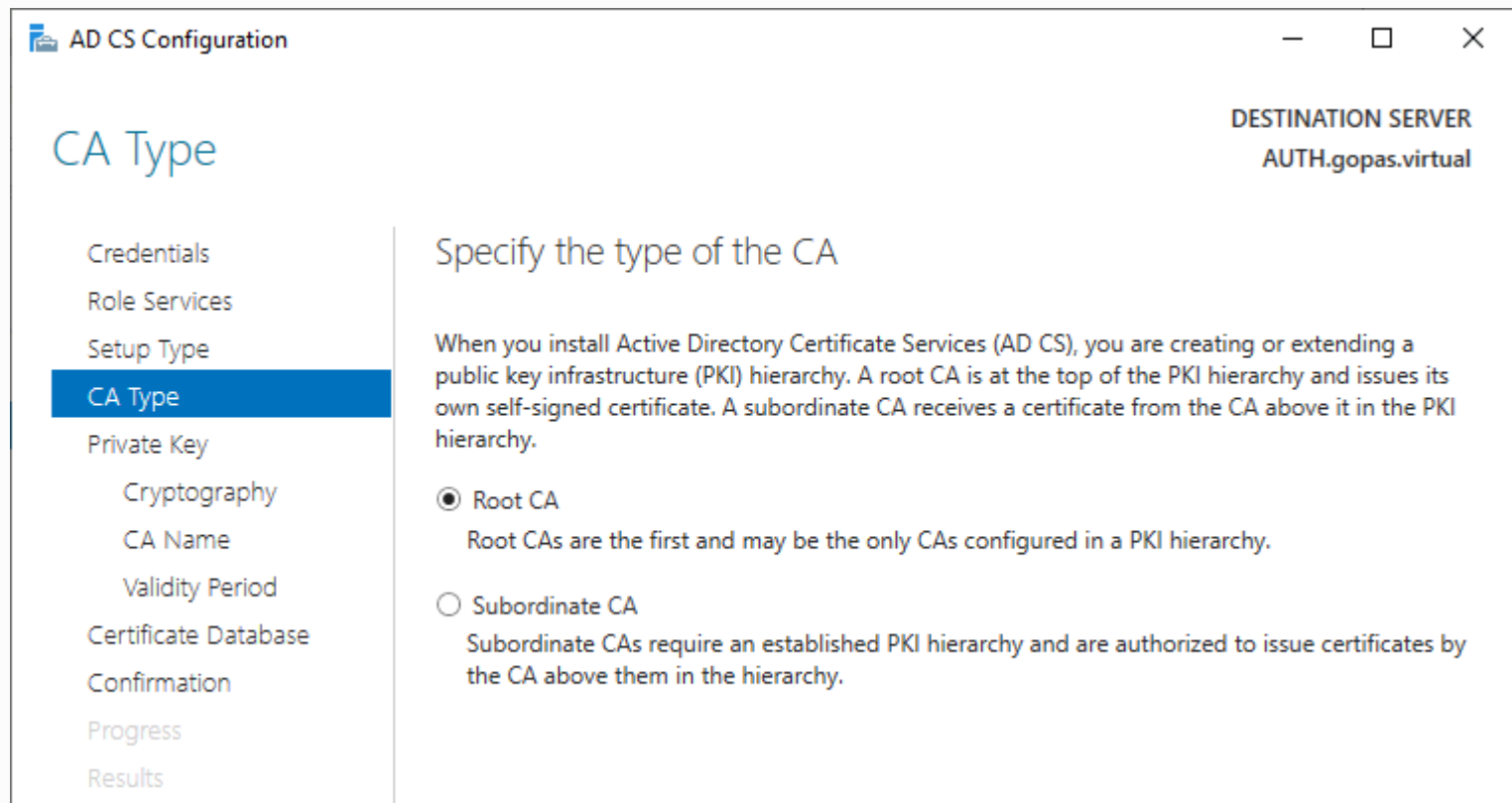
The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select role services'. In the top right corner, it says 'DESTINATION SERVER AUTH.gopas.virtual'. On the left, a navigation pane lists the steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services' (highlighted), 'Confirmation', and 'Results'. The main area is titled 'Select the role services to install for Active Directory Certificate Services'. Under the 'Role services' section, there is a list of services with checkboxes: 'Certification Authority' (checked), 'Certificate Enrollment Policy Web Service', 'Certificate Enrollment Web Service', 'Certification Authority Web Enrollment', 'Network Device Enrollment Service', and 'Online Responder'. To the right, under the 'Description' section, it states: 'Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.'

Simplest AD CS installation



The screenshot shows the 'AD CS Configuration' wizard window. The title bar includes the text 'AD CS Configuration' and standard window controls. The main heading is 'Setup Type'. On the right side, it displays 'DESTINATION SERVER AUTH.gopas.virtual'. A left-hand navigation pane lists the following steps: 'Credentials', 'Role Services', 'Setup Type' (highlighted in blue), 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Certificate Request', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Specify the setup type of the CA' and contains the following text: 'Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.' Below this text are two radio button options: 'Enterprise CA' (which is selected) and 'Standalone CA'. The 'Enterprise CA' option includes the subtext: 'Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.' The 'Standalone CA' option includes the subtext: 'Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).'

Simplest AD CS installation



The screenshot shows the 'AD CS Configuration' window. On the left is a navigation pane with the following items: Credentials, Role Services, Setup Type, CA Type (highlighted in blue), Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the type of the CA'. It contains a paragraph explaining that installing AD CS creates or extends a PKI hierarchy, with a root CA at the top and subordinate CAs below. Two radio buttons are present: 'Root CA' (selected) and 'Subordinate CA'. The 'DESTINATION SERVER' is listed as 'AUTH.gopas.virtual'.

AD CS Configuration

DESTINATION SERVER
AUTH.gopas.virtual

CA Type

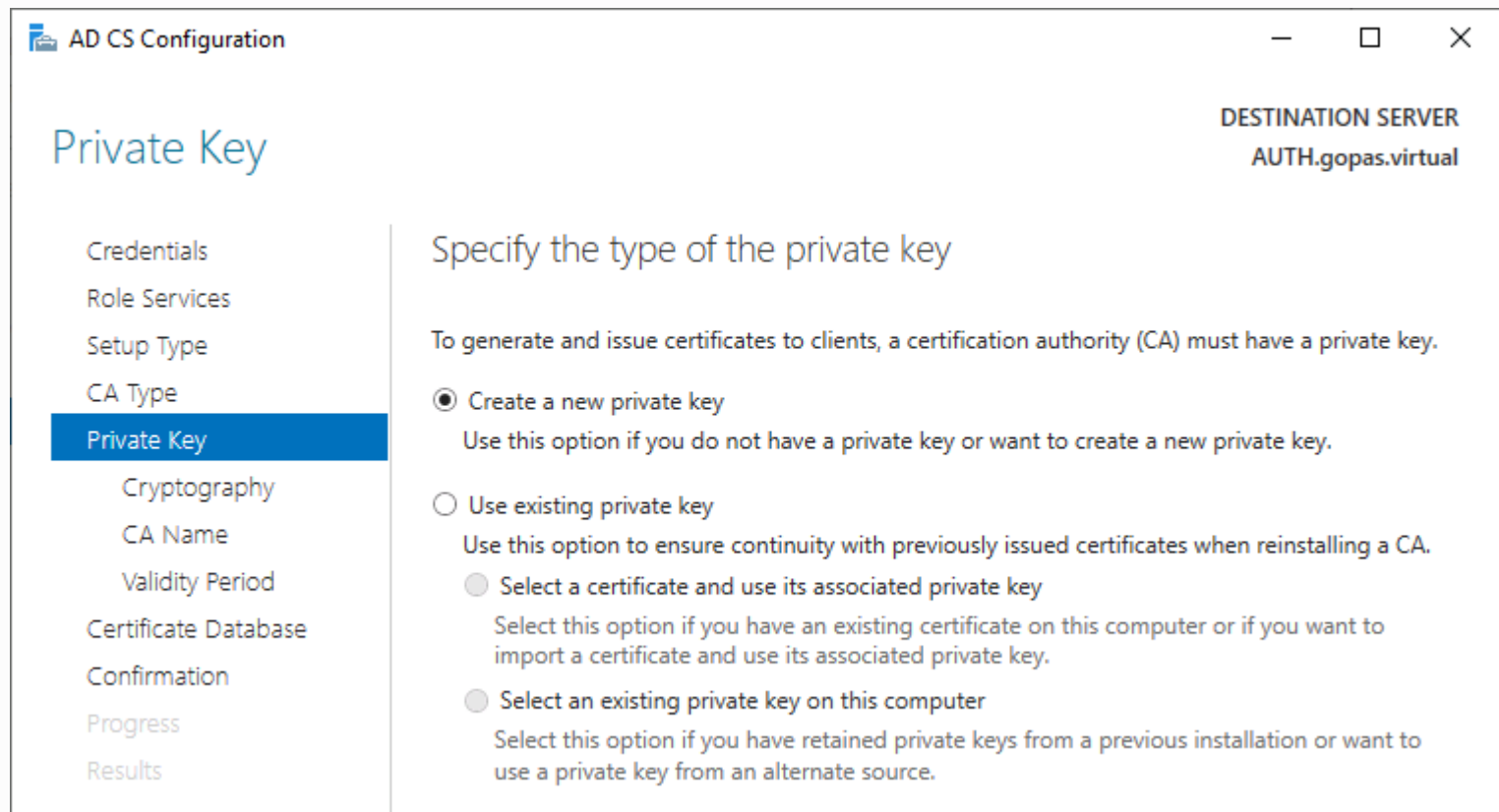
- Credentials
- Role Services
- Setup Type
- CA Type**
- Private Key
 - Cryptography
 - CA Name
 - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

- Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
- Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

Simplest AD CS installation



The screenshot shows the 'AD CS Configuration' console window. The title bar includes the application name and standard window controls. On the right side, the 'DESTINATION SERVER' is identified as 'AUTH.gopas.virtual'. The left-hand navigation pane lists several steps: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key' (which is highlighted in blue), 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Specify the type of the private key'. Below this title, a descriptive paragraph states: 'To generate and issue certificates to clients, a certification authority (CA) must have a private key.' Three radio button options are provided: 1. 'Create a new private key' (selected), with the instruction: 'Use this option if you do not have a private key or want to create a new private key.' 2. 'Use existing private key', with the instruction: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' 3. 'Select an existing private key on this computer', with the instruction: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.'

AD CS Configuration

DESTINATION SERVER
AUTH.gopas.virtual

Private Key

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key**
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

- Create a new private key
Use this option if you do not have a private key or want to create a new private key.
- Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
 - Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
 - Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

Simplest AD CS installation

The screenshot shows the 'AD CS Configuration' console window. The title bar reads 'AD CS Configuration' and the window is maximized. The main heading is 'Cryptography for CA'. On the right, it indicates the 'DESTINATION SERVER' as 'AUTH.gopas.virtual'. A left-hand navigation pane lists several steps: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography' (which is highlighted in blue), 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Specify the cryptographic options'. It contains two sections: 'Select a cryptographic provider:' with a dropdown menu set to 'RSA#Microsoft Software Key Storage Provider', and 'Key length:' with a dropdown menu set to '4096'. Below this is 'Select the hash algorithm for signing certificates issued by this CA:' with a list box containing 'SHA256', 'SHA384', 'SHA512', 'SHA1', and 'MD5'. At the bottom, there is an unchecked checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.'

AD CS Configuration

DESTINATION SERVER
AUTH.gopas.virtual

Cryptography for CA

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography**
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

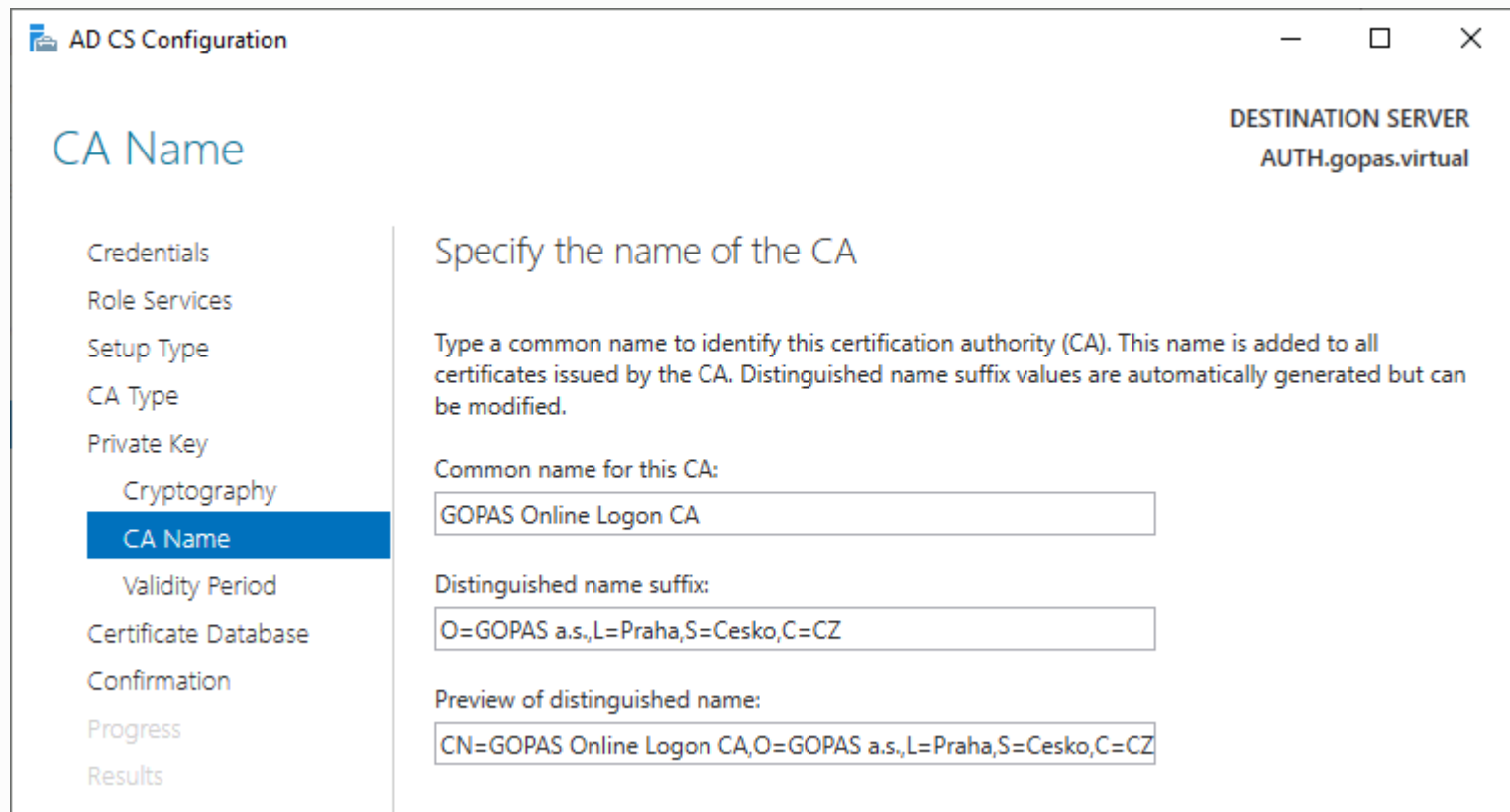
Key length: 4096

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

Allow administrator interaction when the private key is accessed by the CA.

Simplest AD CS installation



The screenshot shows the 'AD CS Configuration' wizard window. The title bar includes the application icon, the text 'AD CS Configuration', and standard window controls (minimize, maximize, close). In the top right corner, the text 'DESTINATION SERVER AUTH.gopas.virtual' is displayed. On the left side, there is a vertical navigation pane with the following items: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name' (highlighted in blue), 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area of the wizard is titled 'Specify the name of the CA'. Below this title, there is a descriptive paragraph: 'Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' There are three input fields: 'Common name for this CA:' with the value 'GOPAS Online Logon CA'; 'Distinguished name suffix:' with the value 'O=GOPAS a.s.,L=Praha,S=Cesko,C=CZ'; and 'Preview of distinguished name:' with the value 'CN=GOPAS Online Logon CA,O=GOPAS a.s.,L=Praha,S=Cesko,C=CZ'.

AD CS Configuration

DESTINATION SERVER
AUTH.gopas.virtual

CA Name

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the name of the CA

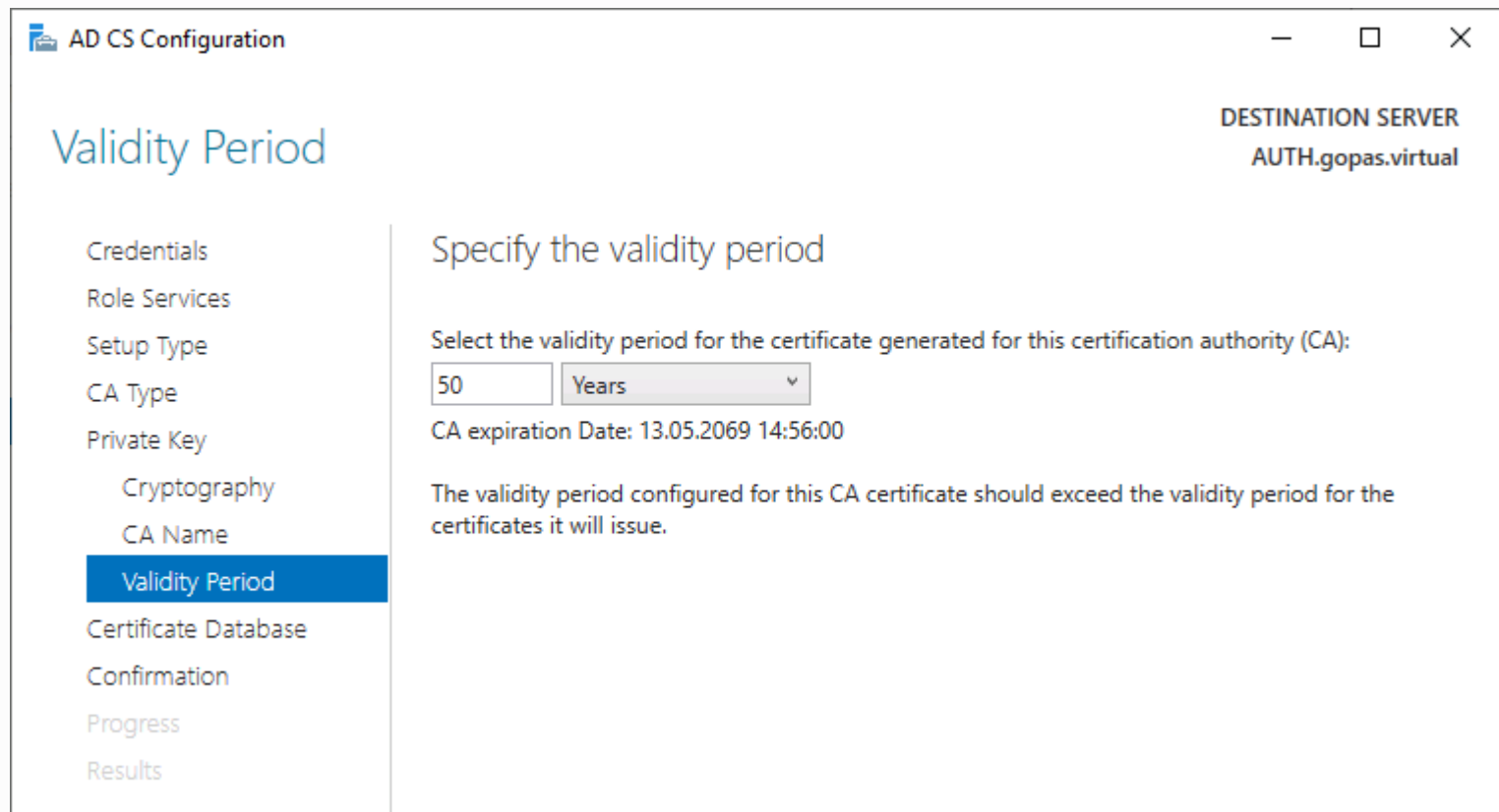
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

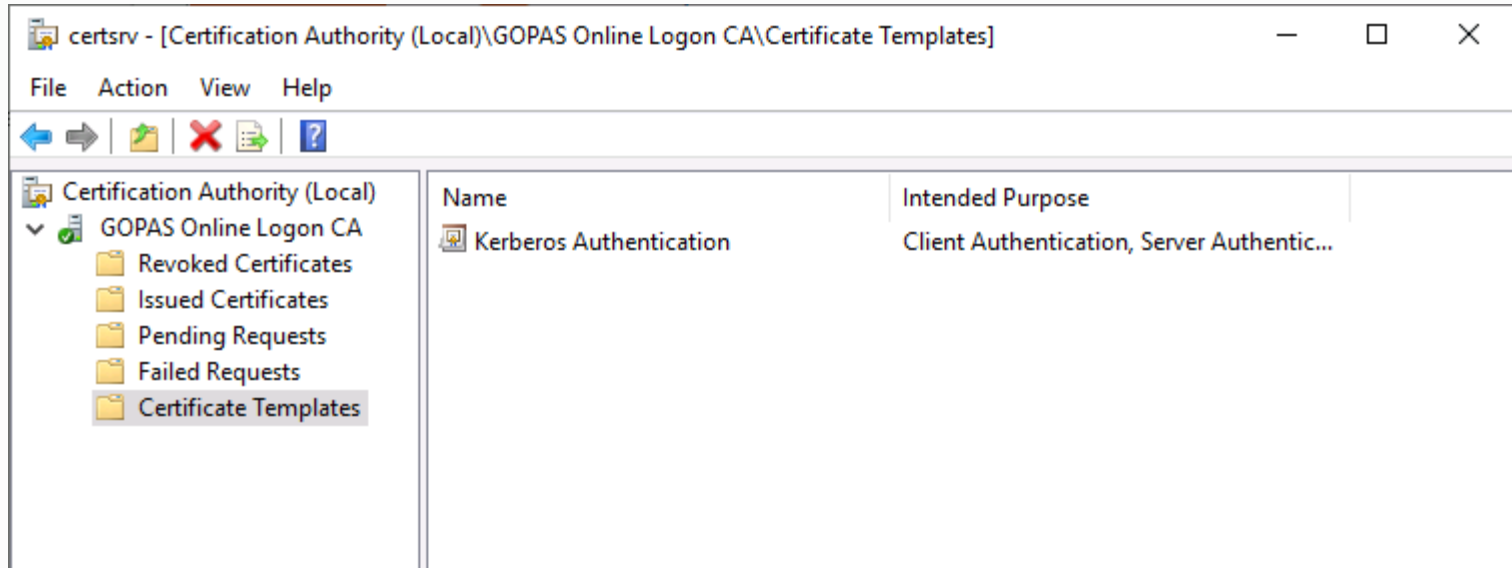
Preview of distinguished name:

Simplest AD CS installation



The screenshot shows the 'AD CS Configuration' wizard window. The title bar reads 'AD CS Configuration' and includes standard window controls. On the right side, it displays 'DESTINATION SERVER AUTH.gopas.virtual'. The main heading is 'Validity Period'. A left-hand navigation pane lists several steps: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Validity Period' (which is highlighted in blue), 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Specify the validity period' and contains the following text: 'Select the validity period for the certificate generated for this certification authority (CA):'. Below this is a form with a text input field containing '50' and a dropdown menu set to 'Years'. Underneath the form, it shows 'CA expiration Date: 13.05.2069 14:56:00'. At the bottom, a warning message states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.'

Simplest DC certificates with auto-enrollment



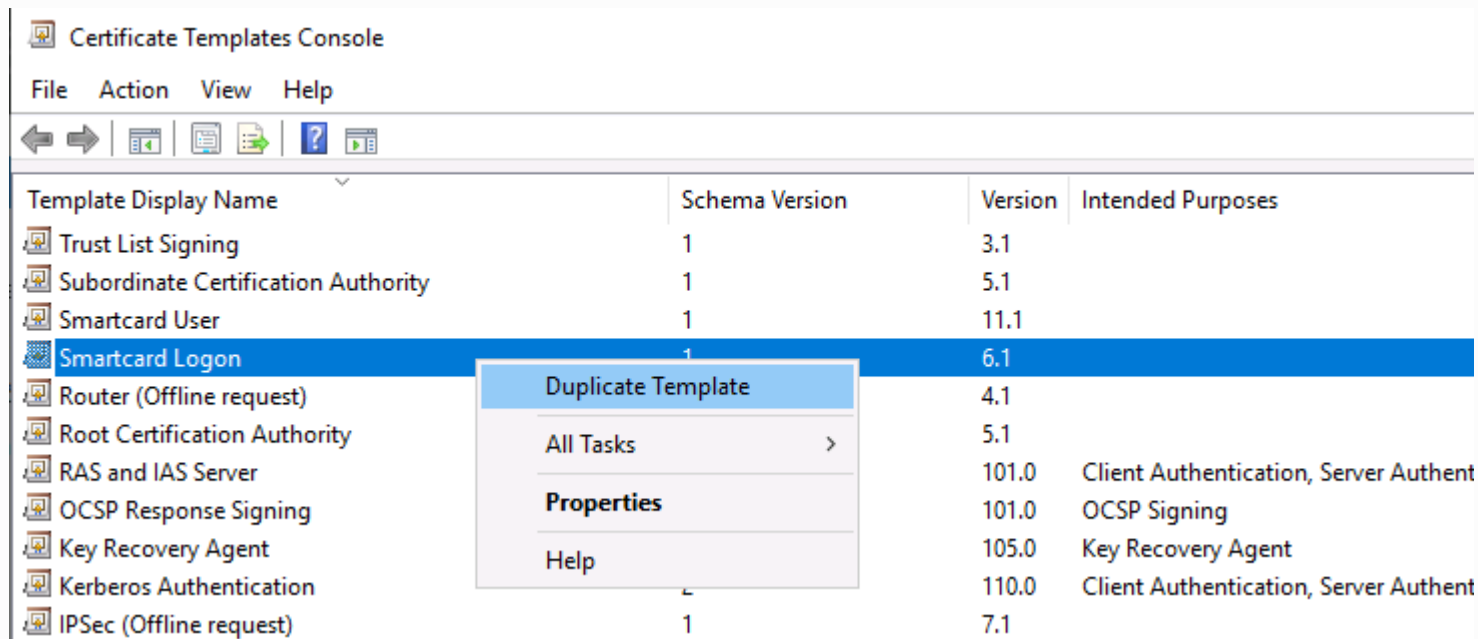
TPM virtual smart card

- 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



The screenshot shows the Certificate Templates Console window. The 'Smartcard Logon' template is selected, and a context menu is open over it. The context menu options are: Duplicate Template, All Tasks, Properties, and Help.

Template Display Name	Schema Version	Version	Intended Purposes
Trust List Signing	1	3.1	
Subordinate Certification Authority	1	5.1	
Smartcard User	1	11.1	
Smartcard Logon	1	6.1	
Router (Offline request)		4.1	
Root Certification Authority		5.1	
RAS and IAS Server		101.0	Client Authentication, Server Authent
OCSP Response Signing		101.0	OCSP Signing
Key Recovery Agent		105.0	Key Recovery Agent
Kerberos Authentication		110.0	Client Authentication, Server Authent
IPSec (Offline request)	1	7.1	

Simple user logon certificate template

GOPAS VPN User TPM Attested Properties ? X

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

The template options available are based on the earliest operating system versions set in Compatibility Settings.

Show resulting changes

Compatibility Settings

Certification Authority
Windows Server 2016

Certificate recipient
Windows 10 / Windows Server 2016

Simple user logon certificate template

GOPS TPM Logon Properties

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

Provider Category:

Algorithm name:

Minimum key size:

Choose which cryptographic providers can be used for requests

Requests can use any provider available on the subject's computer

Requests must use one of the following providers:

Providers:

- Microsoft Smart Card Key Storage Provider
- Microsoft Software Key Storage Provider
- Microsoft Platform Crypto Provider

Simple user logon certificate template

GOPAS VPN User TPM Attested Properties ? X

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

Template display name:
GOPAS VPN User TPM Attested

Template name:
GOPASVPNUserTPMAttested

Validity period: 3 months

Renewal period: 2 weeks

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

Simple user logon certificate template

GOPAS VPN User TPM Attested Properties ? X

Superseded Templates	Extensions	Security	Server	
General	Compatibility	Request Handling	Cryptography	Key Attestation

Subject Name Issuance Requirements

Supply in the request

Use subject information from existing certificates for autoenrollment renewal requests

Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Common name

Include e-mail name in subject name

Include this information in alternate subject name:

E-mail name

DNS name

User principal name (UPN)

Service principal name (SPN)

Simple user logon certificate template

GOPAS VPN User TPM Attested Properties

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- Employees (GPS\Employees)
- PKI Admins (GPS\PKI Admins)

Add... Remove

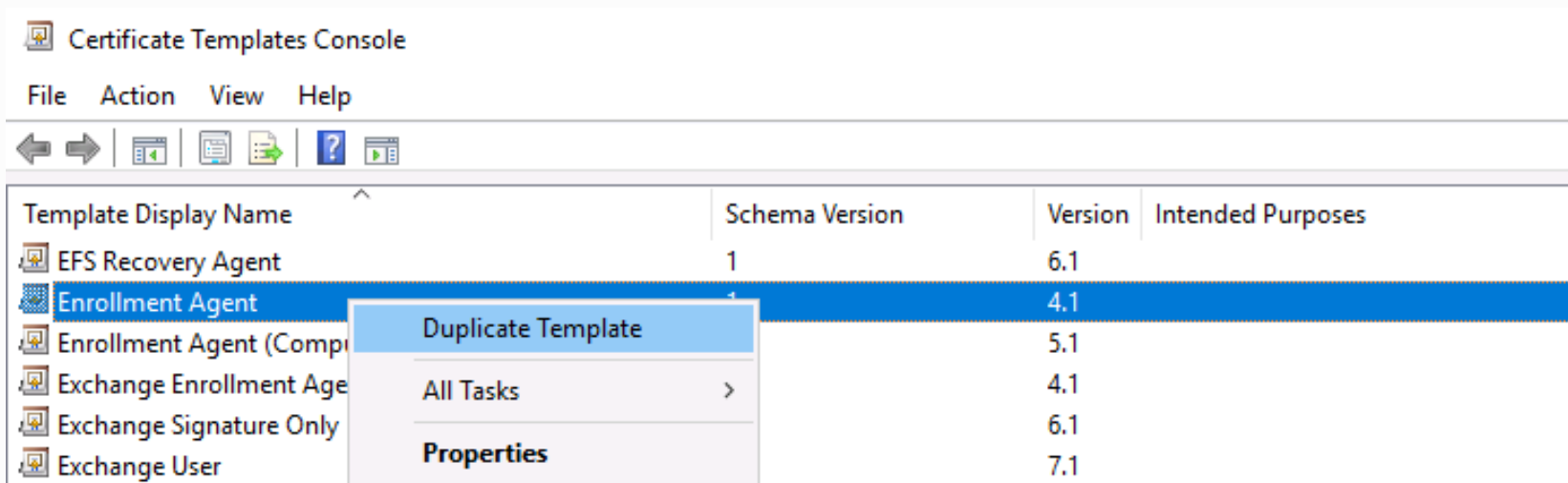
Permissions for Employees

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

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



The screenshot shows the Certificate Templates Console window. The title bar reads "Certificate Templates Console". The menu bar includes "File", "Action", "View", and "Help". Below the menu bar is a toolbar with icons for navigation and help. The main area displays a table of certificate templates. The "Enrollment Agent" template is selected, and a context menu is open over it, showing options: "Duplicate Template", "All Tasks", and "Properties".

Template Display Name	Schema Version	Version	Intended Purposes
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Compu...		5.1	
Exchange Enrollment Age...		4.1	
Exchange Signature Only		6.1	
Exchange User		7.1	

RA certificate for workstation admins

GOPAS TPM Enrollment Agent Properties ? X

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

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

Requests can use any provider available on the subject's computer

Requests must use one of the following providers:

Providers:

- Microsoft Base Smart Card Crypto Provider
- Microsoft Base Cryptographic Provider v1.0
- Microsoft Enhanced Cryptographic Provider v1.0
- Microsoft Enhanced RSA and AES Cryptographic Provider
- Microsoft Strong Cryptographic Provider

Request hash: Determined by CSP

Use alternate signature format

RA certificate for workstation admins

GOPAS TPM Enrollment Agent Properties

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- PKI Admins (GPS\PKI Admins)
- WKS Admins (GPS\WKS Admins)**

Add... Remove

Permissions for WKS Admins

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

User certificate requiring the RA signature

GOPS TPM Logon Properties ? X

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy

Application policy:

Certificate Request Agent

Issuance policies:

Add... Remove

Require the following for reenrollment:

Same criteria as for enrollment

Valid existing certificate

Allow key based renewal

Requires subject information to be provided within the certificate request.

TPM attestation for machine certificates

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

TPM attestation for machine certificates

GOPAS VPN User TPM Attested Properties

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

Key Attestation

None

Required, if client is capable

Required

Perform attestation based on:

User credentials

Hardware certificate

Hardware key

Issuance policies for key attested certificates

Include issuance policies for enforced attestation types

Perform attestation only (do not include issuance policies)

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