



TLS Client Certificate and Smart Card Logon

Ing. Ondřej Ševeček | GOPAS a.s. |

MCSM:Directory2012 | MCM:Directory2008 | MVP:Enterprise Security | CEH:
Certified Ethical Hacker | CHFI: Computer Hacking Forensic Investigator |
CISA |

ondrej@sevecek.com | www.sevecek.com |

GOPAS: info@gopas.cz | www.gopas.cz | www.facebook.com/P.S.GOPAS

1

Motivation

- Limit use of **plaintext passwords**
 - hardware keyloggers
 - password sharing
 - remote access
 - long time access
- Work towards **Kerberos**
 - AES encryption
 - more secure delegation
 - Kerberos tickets **faster expiration** (down to 1 hour)
- Limit NTLM and pass-the-XXX attacks
 - **nothing else** can help you absolutely than **best practices**
 - or LSASS credentials in **Virtual Server Protection (VSP)** in Windows 10



2

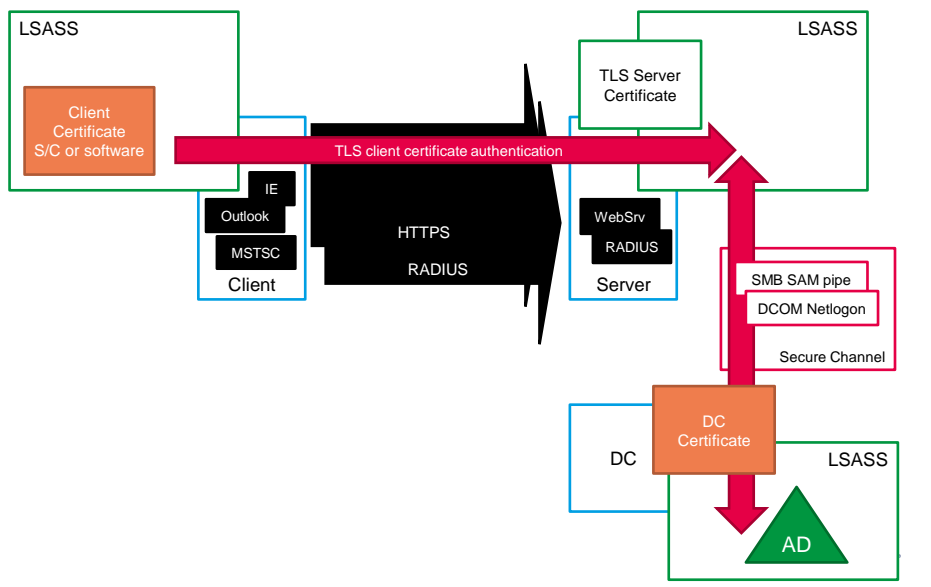
Two certificate authentications

- Interactive **Kerberos PKINIT** logon
 - produce Kerberos TGT with certificate private key pre-authentication
- TLS client certificate authentication (**SChannel**)
 - HTTPS, LDAPS, RADIUS EAP/PEAP
 - web, SSTP, RD Gateway, ADFS, WAP, VPN, WiFi, ...

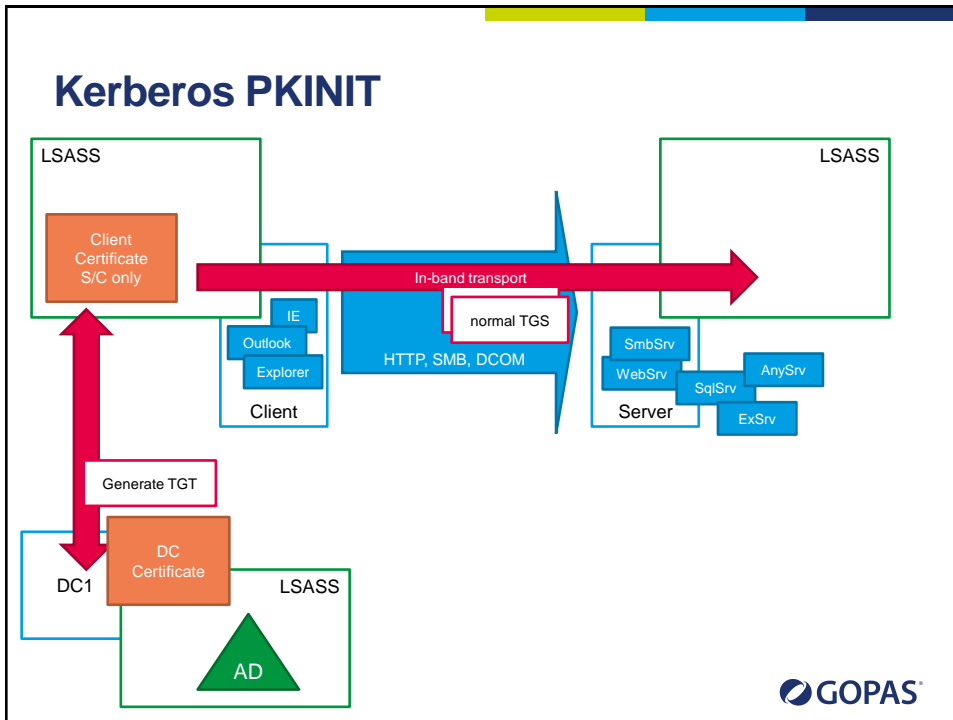


3

SChannel TLS client certificate authentication



4



5

Technical requirements

- PKI
- CAs
- DC certificates
- user logon certificates

6

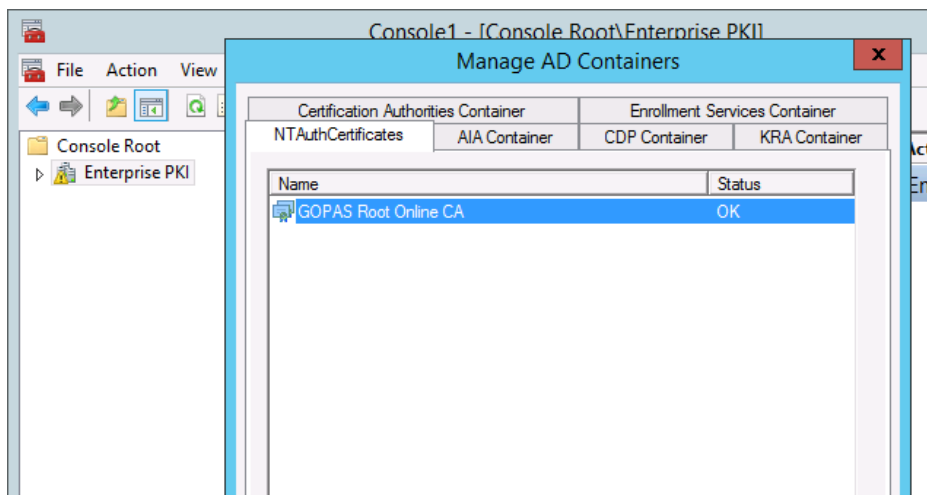
CA requirements

- Trusted root CA
- NTAAuth trusted **issuing** CA
 - enterprise (AD integrated) ADCS CAs by default
 - **CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=x**
 - **HKLM\Software\Microsoft\EnterpriseCertificates\NTAuth\Certificates**
 - ♦ #thumbprint#
- CRL valid (OCSP)
 - up-to-date, available, ideally anonymous HTTP



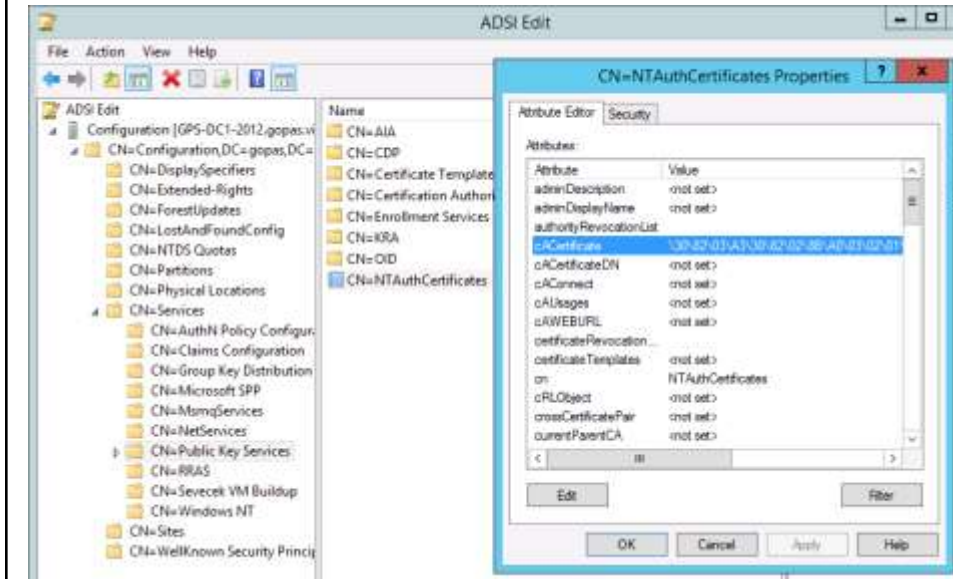
7

Verify NTAAuth CAs for a forest using Enterprise PKI console



8

NTAuthCertificates object (CN=Public Key Services,CN=Services,CN=Configuration)



9

DC certificate requirements (2003+)

- EKU (default template Kerberos Authentication)
 - Server Authentication
 - Client Authentication
 - Smart Card Logon
 - Kerberos Authentication
- SAN
 - DNS domain name
 - NetBIOS domain name
- CRL valid (or OCSP)
 - up-to-date, available, ideally anonymous HTTP
 - from client's perspective
 - certutil -urlfetch -verify
 - certutil -url

10

Client certificate requirements

- Stored in smart card in case of Kerberos PKINIT
 - EKU = Smart Card Logon
- Stored in S/C or software provider in case of TLS client certificate logon
 - EKU = Client Authentication
- SAN
 - user principal name (UPN)
 - manually mapped SAN or subject
- CRL valid (or OCSP)
 - up-to-date, available, ideally anonymous HTTP
 - from DC's perspective
 - certutil -urlfetch -verify
 - certutil -url



11

Client certificate SAN vs. Published Certificates on domain user account

The image shows two overlapping windows. The background window is 'Kamil Properties' with the 'Account' tab selected. The 'User logon name' field is highlighted with a red dashed box and contains 'kamil' and '@gopas.cz'. The foreground window is 'Certificate' with the 'Details' tab selected. The 'Subject Alternative Name' field is highlighted with a blue selection bar and contains 'Other Name: Principal Name=kamil@gopas.cz', which is also circled with a red dashed box. Other certificate details visible include Certificate Template Information, Authority Information Access, Subject Key Identifier, CRL Distribution Points, Authority Key Identifier, Enhanced Key Usage, and Key Usage.



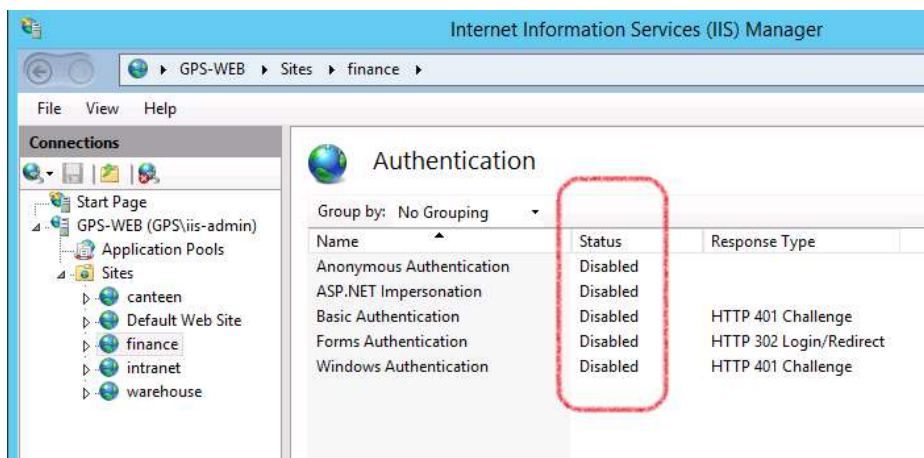
12

IIS TLS client certificate authentication #1 Enforce TLS and require client certificates



13

IIS TLS client certificate authentication #2 Disable all HTTP authentication methods

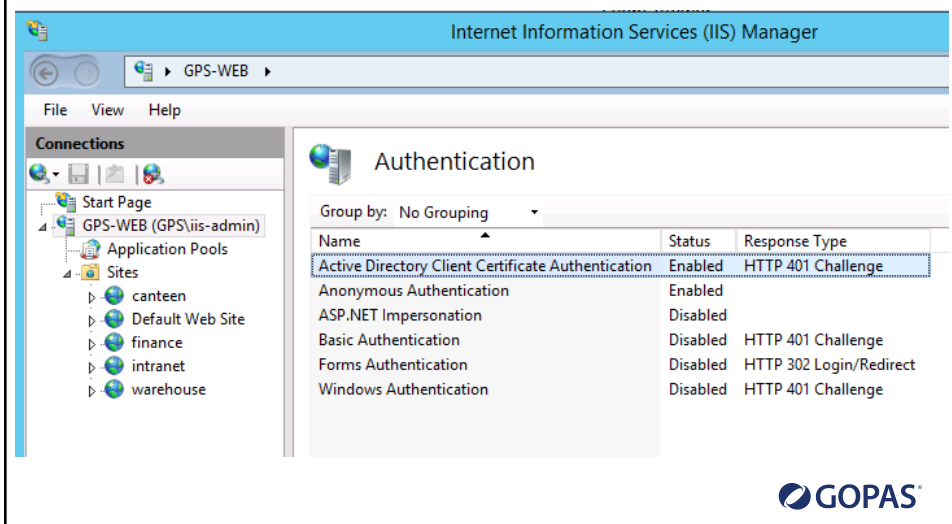


14

IIS TLS client certificate authentication #3

Install Active Directory Client Certificate Authentication

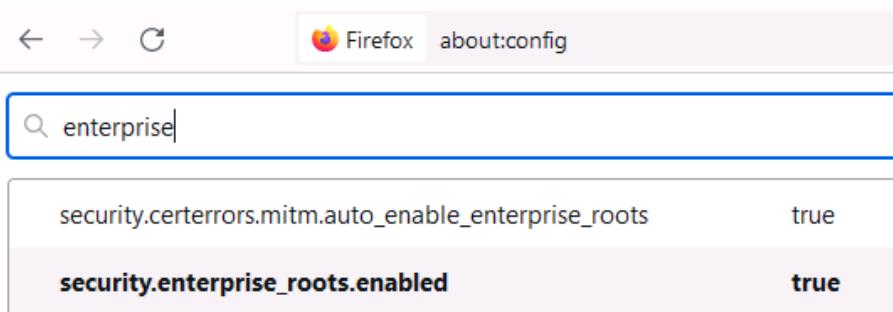
Enable AD mapper server-wide



15

Firefox does not see Windows certificates by default

- `about:config`
 - `security.enterprise_roots_enabled`



16

Schannel authentication events on DCs



Event Properties - Event 4774, Microsoft Windows security auditing.

General Details

An account was mapped for logon.

Authentication Package: Schannel
 Account UPN: helena@gopas.cz
 Mapped Name: helena

Log Name: Security
 Source: Microsoft Windows security Logged: 8. 12. 2017 14:51:38
 Event ID: 4774 Task Category: Credential Validation
 Level: Information Keywords: Audit Success
 User: N/A Computer: GPS-DC1.gopas.virtual

GOPAS

17

Hardware requirements

- Smart card + reader
- Smart card in a reader = token
- USB, PCMCIA

- TPM on motherboard

- Smart card is not a USB flash drive
 - crypto CPU separate from OS
 - performs crypto-operations under PIN protection
 - crypto-memory cannot be "just read"

GOPAS

18

Hardware drivers

- "bus" drivers for reader
- crypto-provider for the chip
 - Cryptographic Services Provider (CSP)
 - mini-driver DLL for Base Smart Card CSP or Smart Card KSP
- certutil -csplist
- certutil -scinfo



19

TPM virtual smart-card

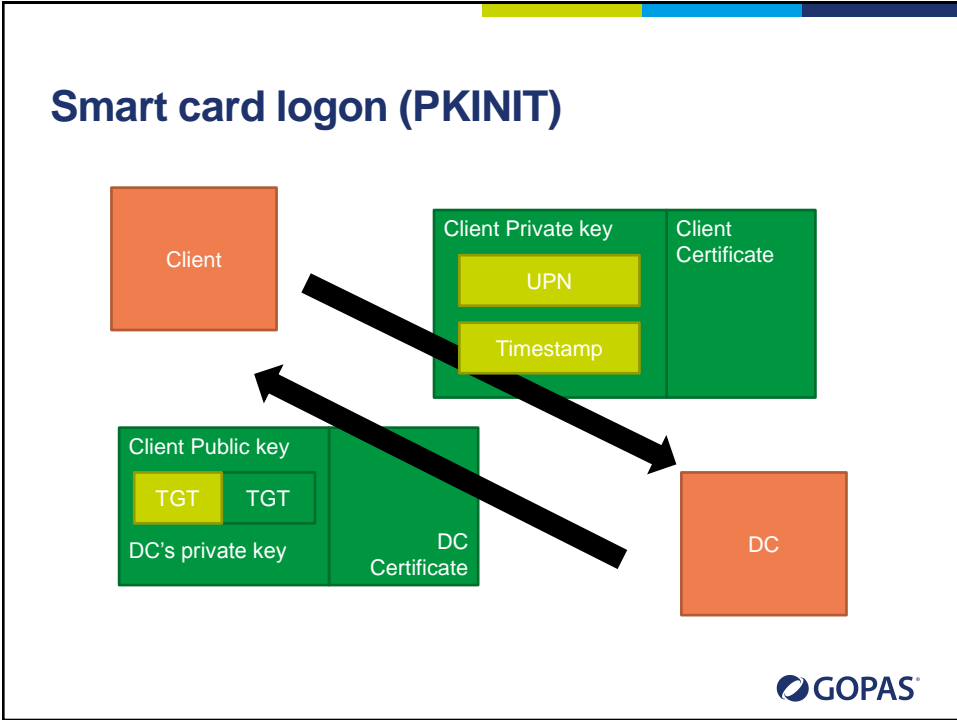
```

Administrator: Windows PowerShell

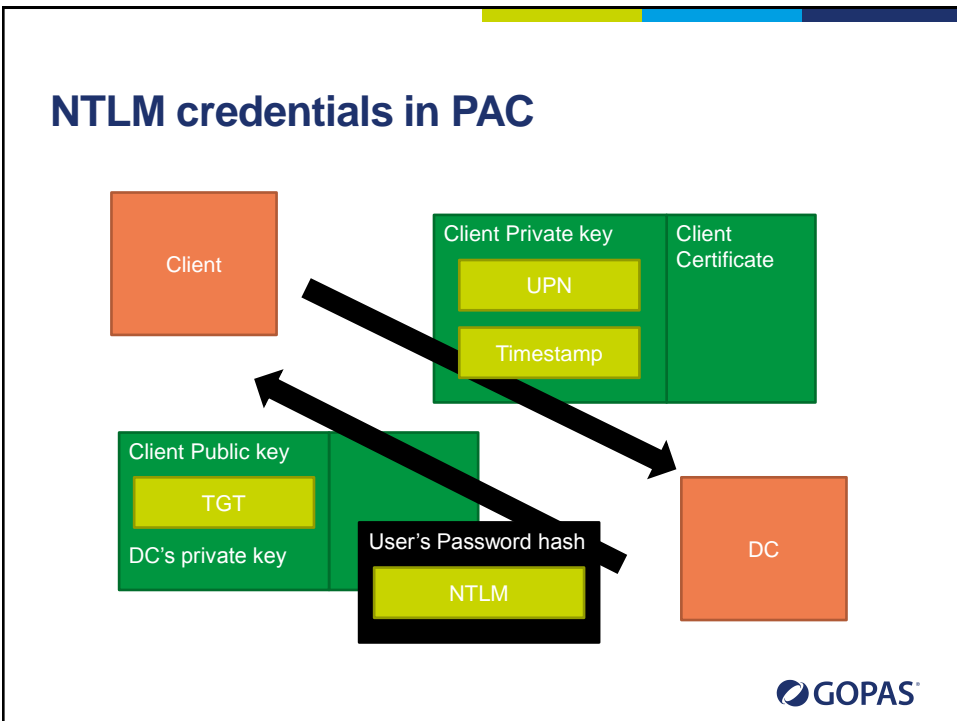
PS C:\>
PS C:\> tpmvscmgr.exe create /name "userADlogon" /AdminKey PROMPT /PIN Prompt /generate
Enter Admin Key:
*****
Confirm Admin Key:
*****
Enter PIN:
*****
Confirm PIN:
*****
Creating TPM Smart Card...
Initializing the Virtual Smart Card component...
Creating the Virtual Smart Card component...
Initializing the Virtual Smart Card Simulator...
Creating the Virtual Smart Card Simulator...
Initializing the Virtual Smart Card Reader...
Creating the Virtual Smart Card Reader...
Waiting for TPM Smart Card Device...
Authenticating to the TPM Smart Card...
Generating filesystem on the TPM Smart Card...
TPM Smart Card created.
Smart Card Reader Device Instance ID = ROOT\SMARTCARDREADER\0000
PS C:\>
PS C:\>

```

20



21



22

Auditing

- Account logon
 - Kerberos Authentication Service
 - ♦ ID: 4771
 - ♦ Pre-authentication type: 15



23

Require S/C for interactive logon

- **Interactive** logon only
 - pre-authentication generate TGT
- Per user account in AD
 - userAccountControl = 262144 (0x40000)
 - GUI randomizes password
- Per computer by GPO
 - all users on the computer



24

Expired passwords prevent S/C logon as well 2016+ msDS-ExpirePasswordsOnSmartCardOnlyAccounts

Attribute	Value
msDS-CloudAnchor	<not set>
mS-DS-ConsistencyGuid	<not set>
mS-DS-ConsistencyChildCount	<not set>
msDS-EnabledFeature	<not set>
msDS-ExpirePasswordsOnSmartCardOnlyAccounts	FALSE
msDS-LastKnownRDN	<not set>
msDS-Logon Time Sync Interval	<not set>
ms-DS-MachineAccountQuota	10

25

S/C removal behavior

- Log-off
- Lock-out and/or RDP disconnect
- Smart Card Removal Policy service must be enabled
 - GPO

26