GOPAS

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 plaint-text 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

GOPAS

2

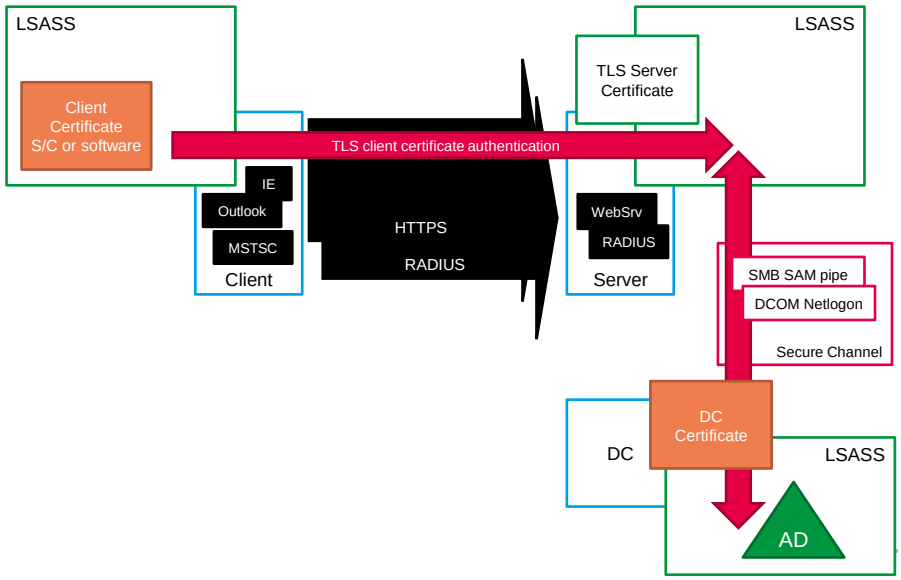
Two certificate authentications

- 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, ...

GOPAS

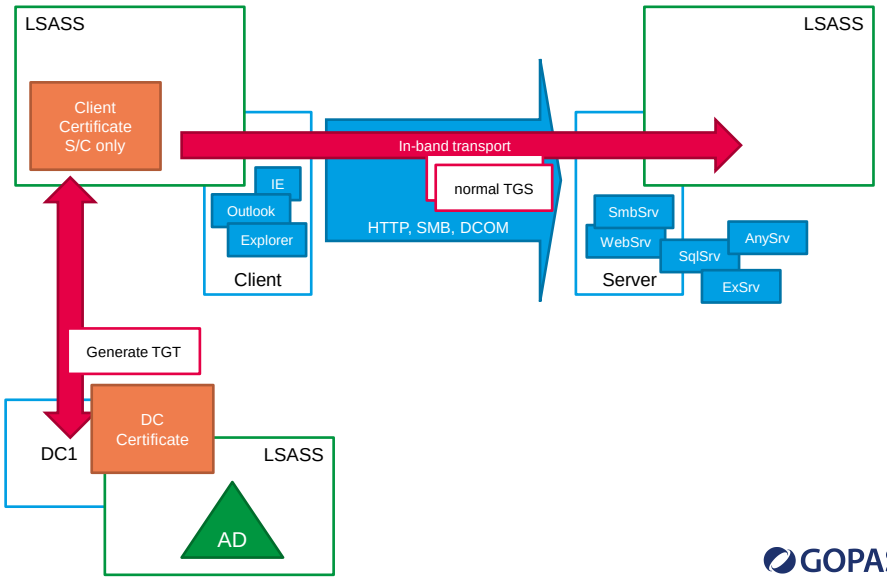
3

SChannel TLS client certificate authentication



4

Kerberos PKINIT



GOPAS

5

Technical requirements

- PKI
- CAs
- DC certificates
- user logon certificates

GOPAS

6

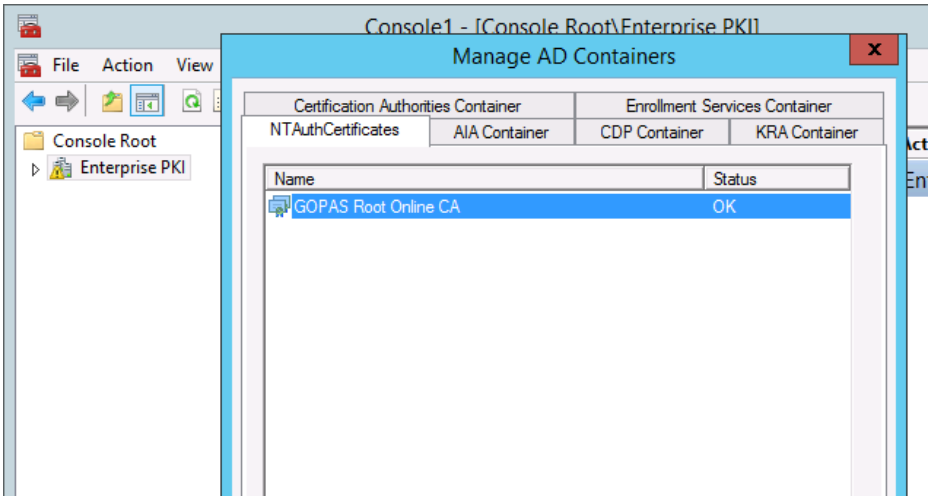
CA requirements

- Trusted root CA
- NTAuth 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

GOPAS

7

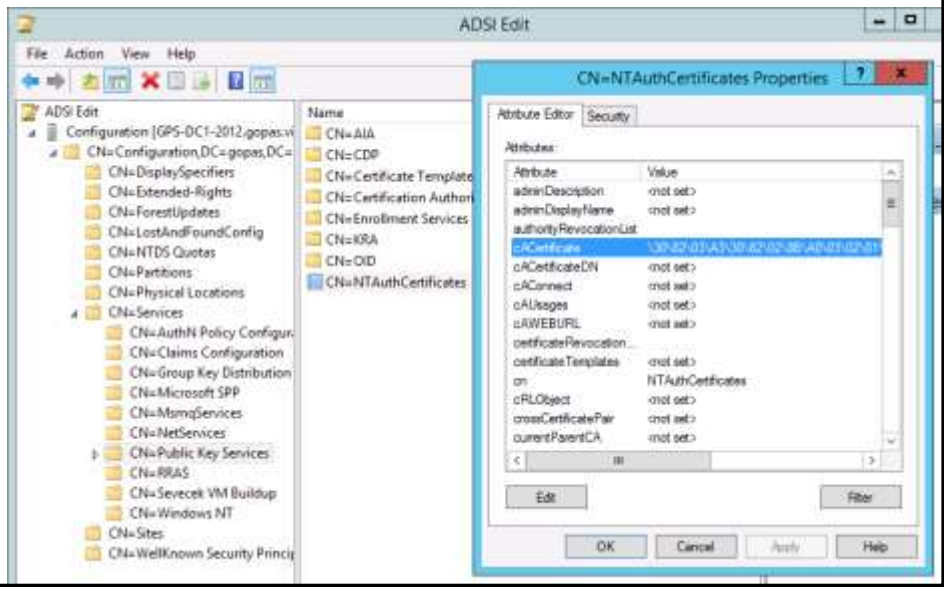
Verify NTAuth CAs for a forest using Enteprise PKI console



GOPAS

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

GOPAS

10

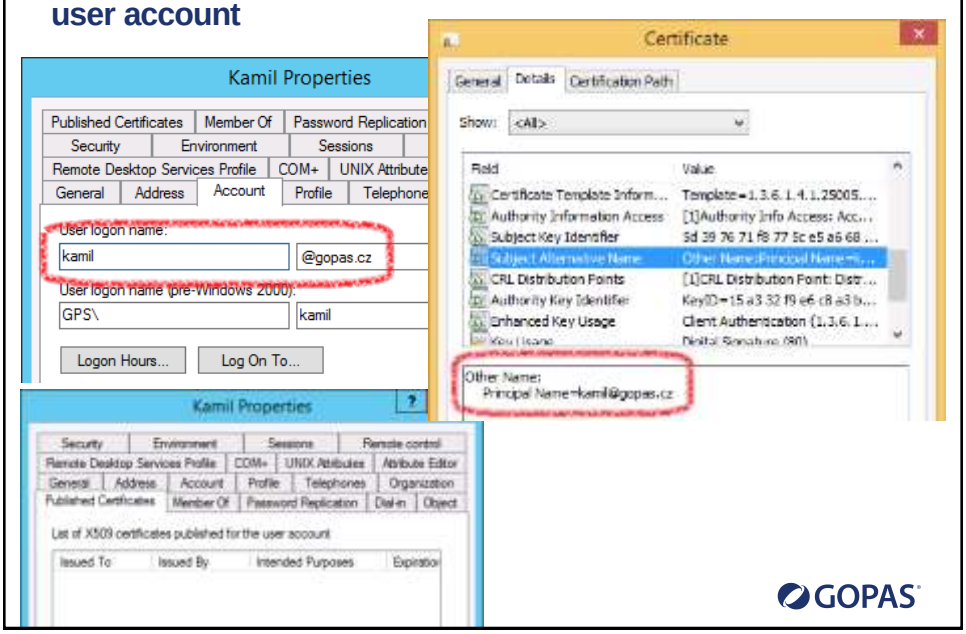
Client certificate requirements

- 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

GOPAS

11

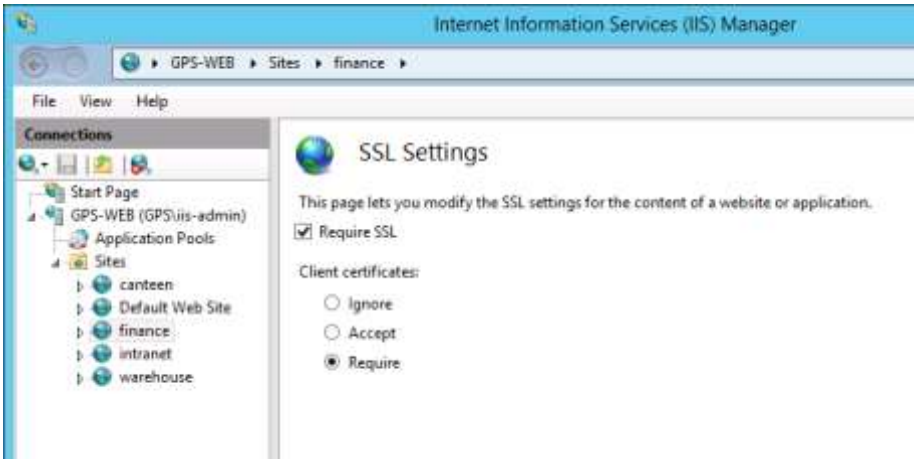
Client certificate SAN vs. Published Certificates on domain user account



GOPAS

12

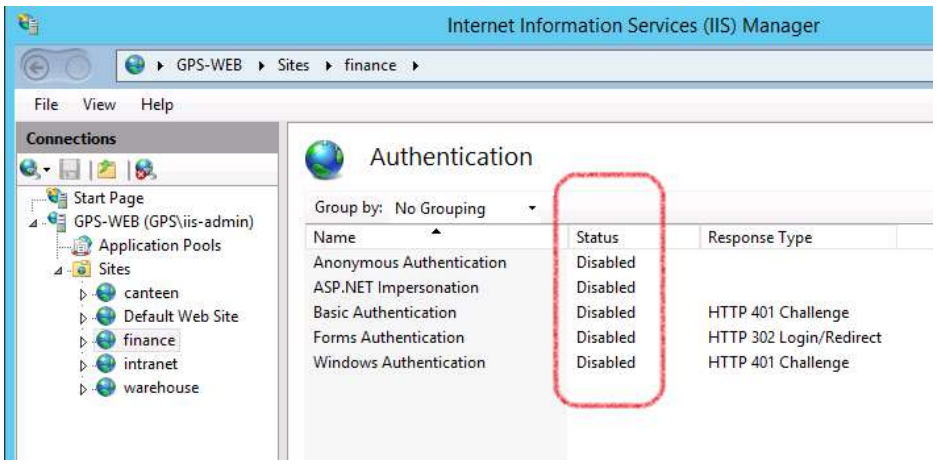
IIS TLS client certificate authentication #1
Enforce TLS and require client certificates



GOPAS

13

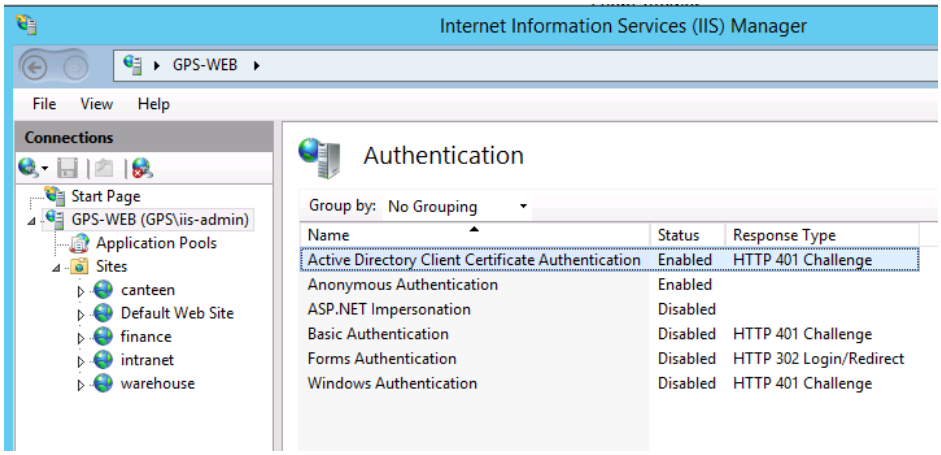
IIS TLS client certificate authentication #2
Disable all HTTP authentication methods



GOPAS

14

IIS TLS client certificate authentication #3
Install Active Directory Client Certificate Authentication
Enable AD mapper server-wide

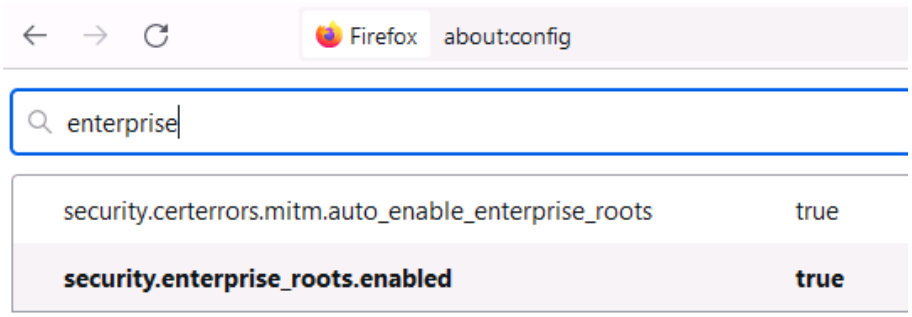


GOPAS

15

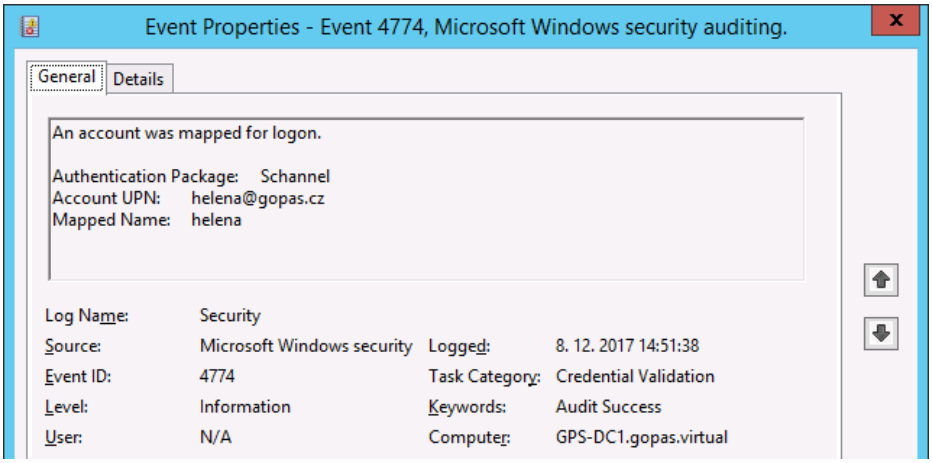
Firefox does not see Windows certificates by default

- about:config
  - security.enterprise_roots_enabled



16

Schannel authentication events on DCs



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

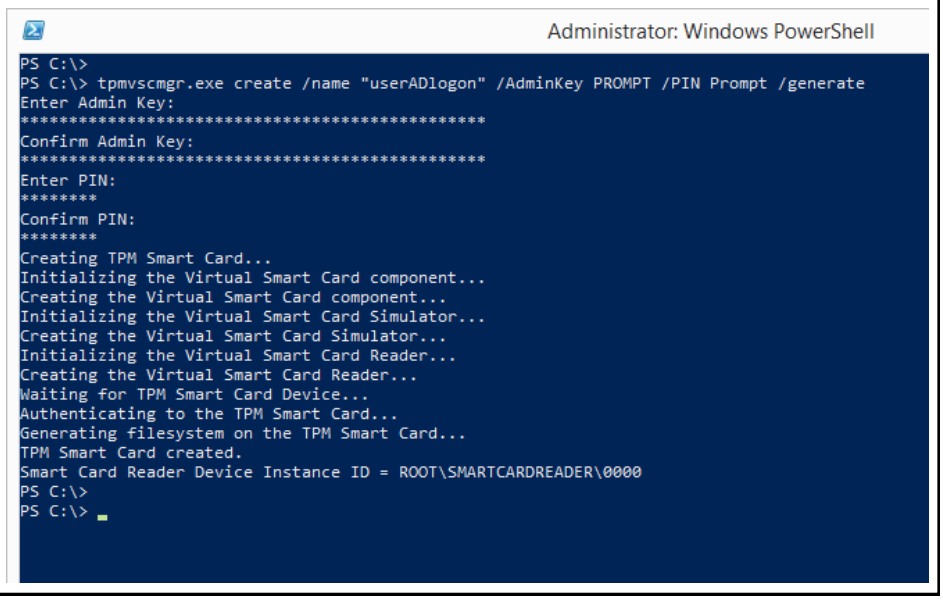
Hardware drivers

- "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

GOPAS

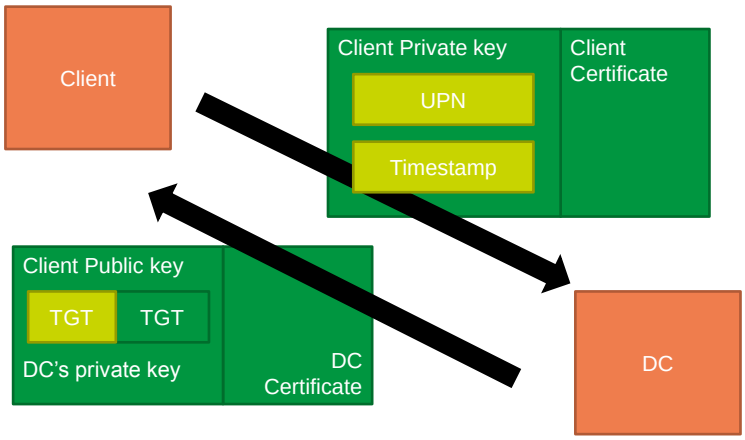
19

TPM virtual smart-card



20

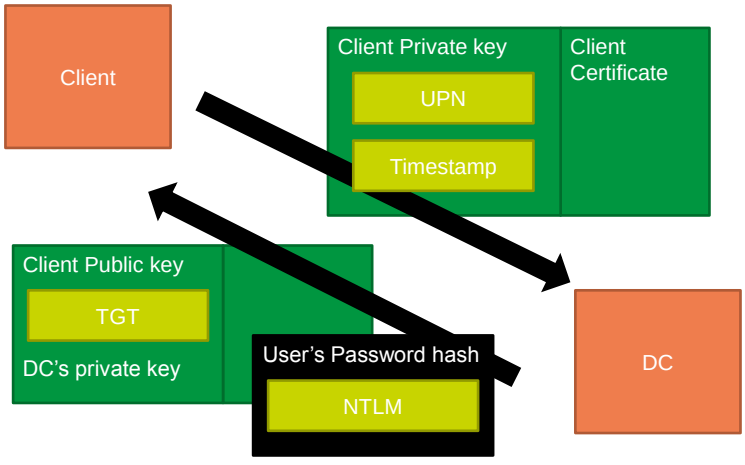
Smart card logon (PKINIT)



GOPAS

21

NTLM credentials in PAC



GOPAS

22

Auditing

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

GOPAS

23

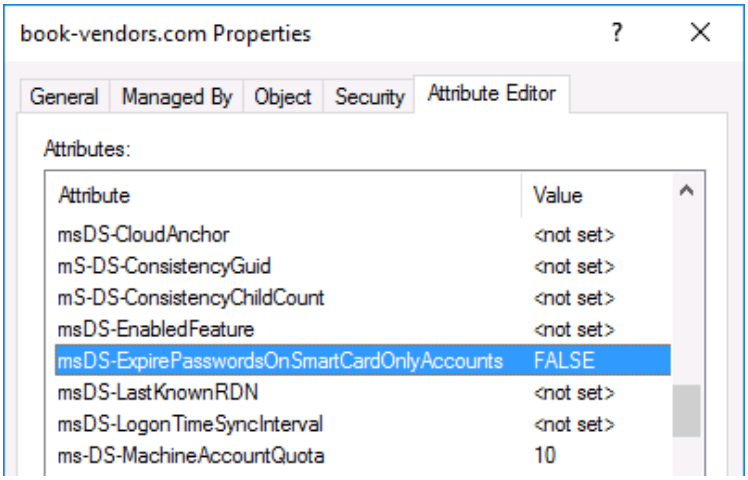
Require S/C for interactive logon

- 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

GOPAS

24

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



GOPAS

25

S/C removal behavior

- Log-off
- Lock-out and/or RDP disconnect

- Smart Card Removal Policy service must be enabled
  - GPO

GOPAS

26