Der Kampf gegen Goldene Zertifikate

30. DFN-Konferenz „Sicherheit in vernetzten Systemen“
Hamburg, 09.02.2023

Hans-Joachim Knobloch

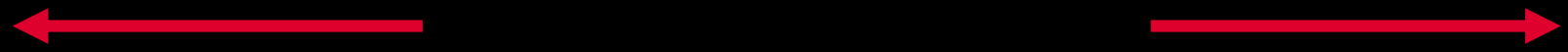
secorvo
security consulting

Einige PKI-Begriffe - kurz und knapp

OID – ASN.1 Object Identifier

- Zahlenfolge als weltweit eindeutige Kennung für *irgendwas*
- Wie DNS, nur von links nach rechts – „registrierte Domain“ ≈ „Präfix“

microsoft.com. ≈ 1.3.6.1.4.1.311



- Inhaber des Präfixes bestimmt, für welches *irgendwas* ein OID steht

1.3.6.1.4.1.311.20.2.2 = Zertifikat für Smartcard Anmeldung

Zertifikatserweiterungen

- Baukasten, um zusätzliche Informationen in Zertifikaten unterzubringen, die in der Anwendung wichtig und/oder nützlich sein können
- Eingestellte Erweiterungen sind untrennbarer Bestandteil des Zertifikats
- Per OID identifiziert → jeder Präfix-Inhaber kann neue Erweiterungen definieren

1.3.6.1.4.1.8861.42.3.8 = Zertifikat gilt nur jeden dritten Dienstag im Monat

- *Merke*:
  Nicht jede Anwendung „versteht“ jede Zertifikatserweiterung
  Nicht jede Zertifizierungsstelle (CA) „kann“ jede Zertifikatserweiterung

Nachfolgend relevante Zertifikatserweiterungen

EKU

Extended Key Usage

- *Für welche Zwecke ist das Zertifikat gedacht?*
- Zweck = OID

  Smartcard Logon

  Client Authentication (TLS)

  1.3.6.1.5.5.7.3.2

  Any Purpose

  2.5.29.37.0

  … und viele andere mehr

SAN

Subject Alternative Name

- *Welche Namen hat der Inhaber außerhalb des Directories?*
- Diverse Namensformen

  DNS-Name

  E-Mail-Adresse

  Windows Kontoname (UPN)

  … und andere mehr

SKI

Subject Key Identifier

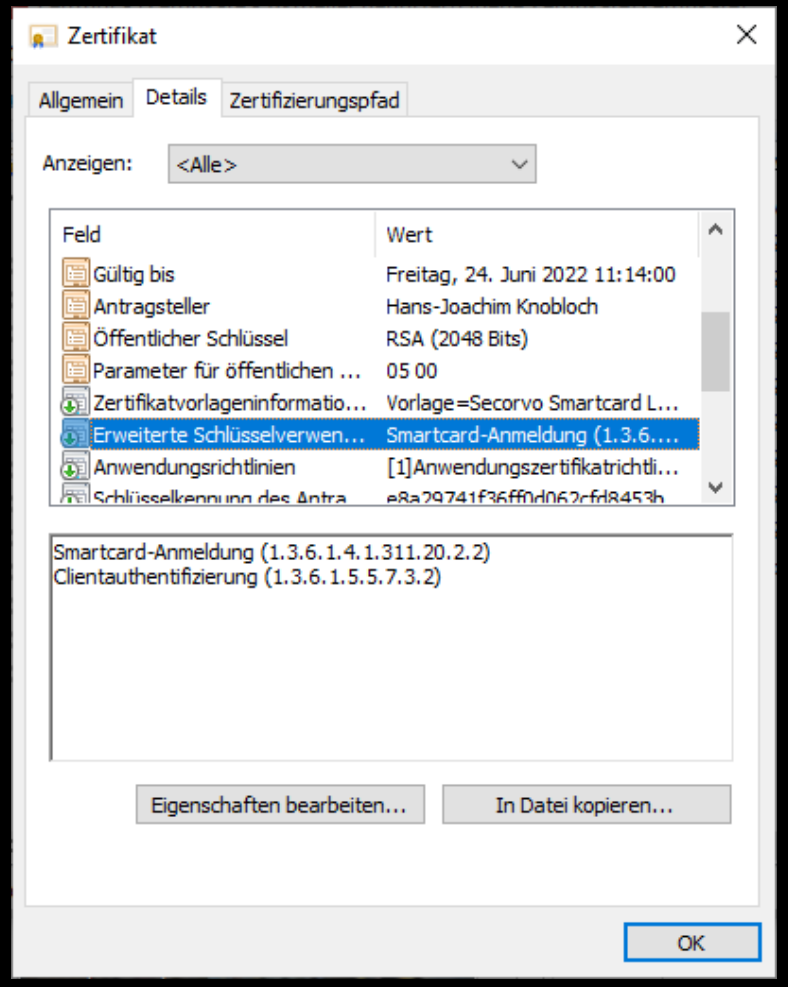
- Kurz-Kennzeichnung des Public Keys im Zertifikat
- Konvention: SHA-1 Hash als Fingerprint des Keys

  Aber:

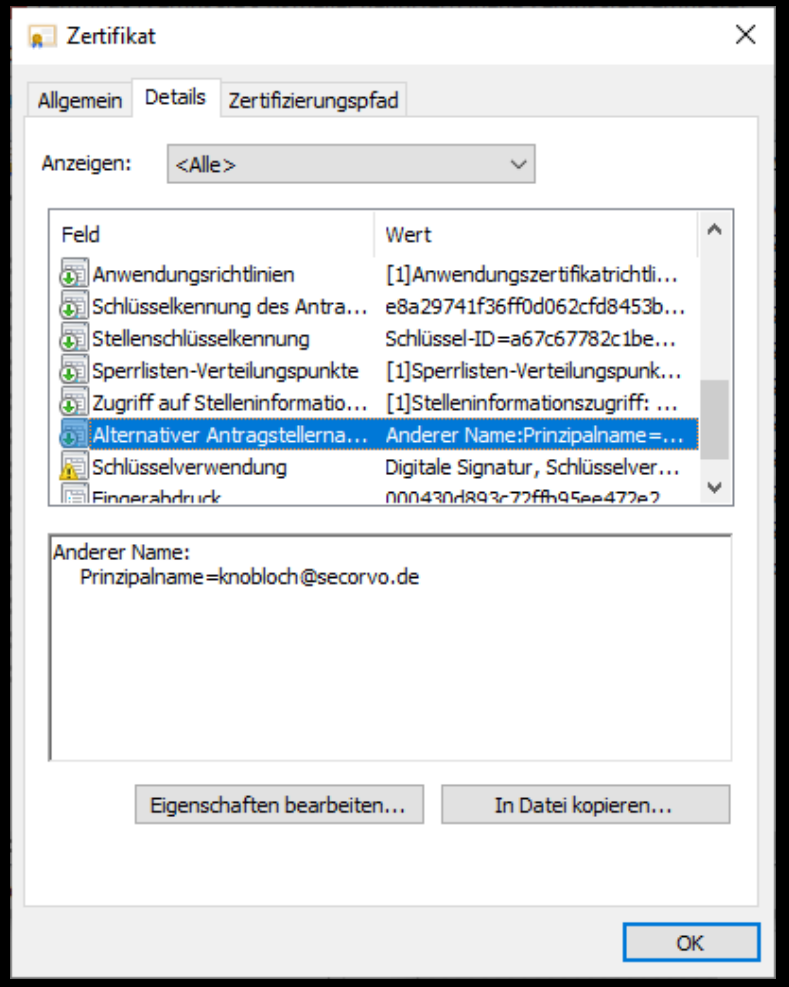
  Das ist nur Konvention, die CA könnte auch „Anton“ oder „Egon“ einstellen

Beispiel

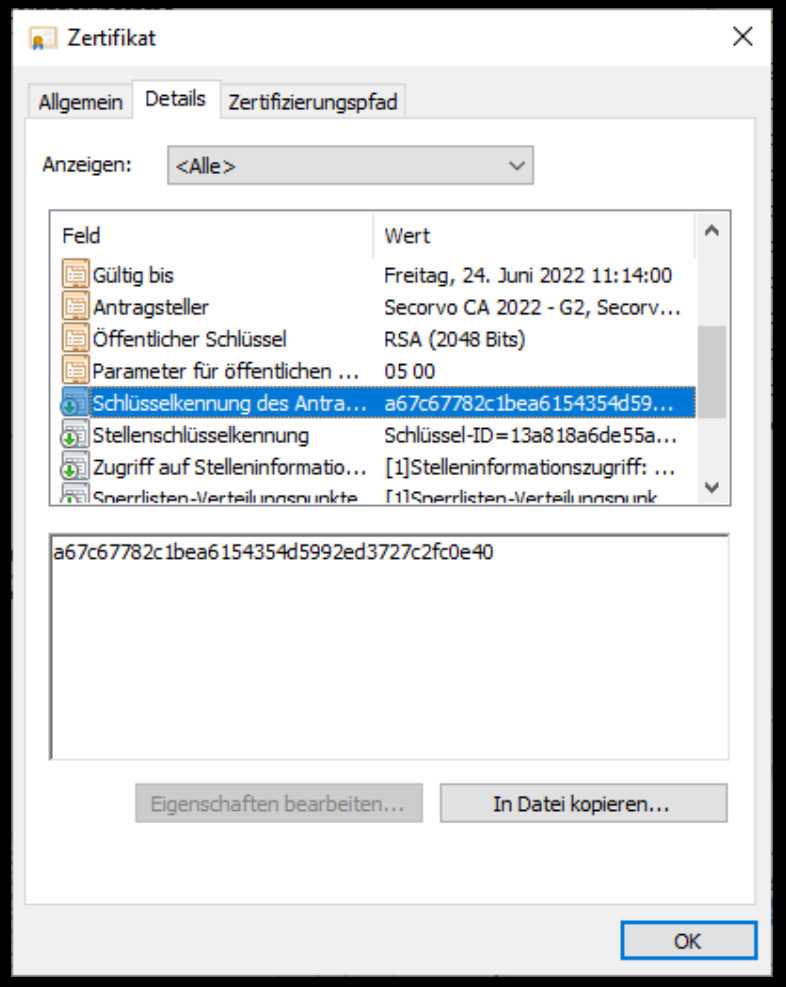
EKU



SAN



SKI

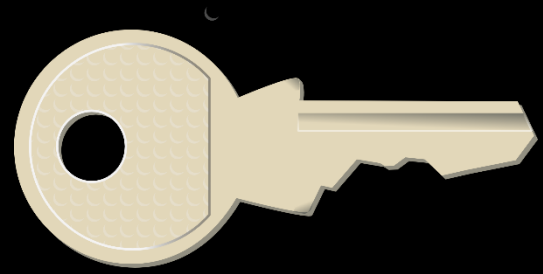


Kerberos und PKI

Zwei Dinge braucht man für Kerberos

Kerberos Ticket - eine Art von „Symmetric Key Zertifikat“

- In der Regel kurzfristig gültig, typisch acht Stunden



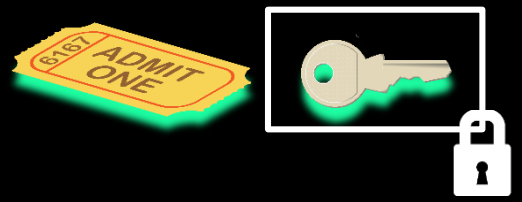
Passender Symmetrischer Schlüssel dazu

- Für jedes Ticket neu „geschnippt“

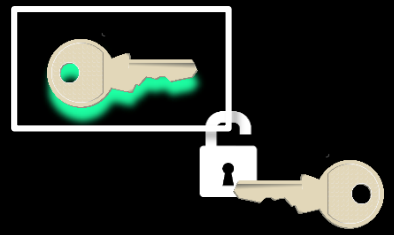
Wie kommt man an sein Ticket? – Regelfall

Logon Session Ticket a.k.a Ticket Granting Ticket

Kerberos
Ticket Granting Service
(AD Domain Controller)

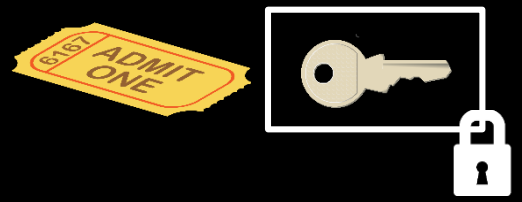


Service Ticket



Wie kommt man an sein Logon-Ticket? – Regelfall

Benutzername



Logon Session Ticket

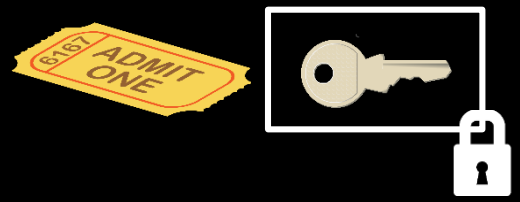
Entschlüsseln mit Hash
des Benutzerpassworts

Kerberos
Logon Service
(AD Domain Controller)

Wie kommt man an sein Logon-Ticket? – PKInit

Zertifikat, über das Benutzername ersichtlich wird

Kerberos
Logon Service
(AD Domain Controller)



Logon Session Ticket

Entschlüsseln mit
Private Key zum Zertifikat

Wie kommt man an sein Logon-Ticket? – PKInit

- PKInit wird genutzt für Smartcard Logon am Active Directory

- *Aber*:
  Es ist ein verbreitetes Missverständnis, dass der Private Key dabei immer unauslesbar auf einer Smartcard gespeichert sein muss

- PKInit wird u. a. genutzt von…
  - Windows Hello (in manchen Betriebsmodi „unter der Motorhaube“)
  - Mimikatz und weiteren „Hacker-Tools“

Welche Zertifikate akzeptiert der AD Domain Controller?

Gültig

- Zertifikatskette zu vertrauenswürdiger Root-CA
- Nicht abgelaufen
- Nicht gesperrt

Passende EKU

… eine davon genügt

- Smartcard Logon
- PKINIT Key Purpose Client Auth
- Client Authentication
- Any Purpose

CA dazu berechtigt

… in fast allen Fällen

- CA-Zertifikat der ausstellenden CA (nicht der Root-CA) im AD „NTAuth“ Container
- Bei Microsoft Enterprise CAs wird das bei der Installation automatisch dort eingestellt

Certificate Mapping im Active Directory

Certificate Mapping

Zertifikat! → Benutzername?

Implicit Mapping Identifikation des Benutzers steht direkt im Zertifikat

Explicit Mapping Information zum Zertifikat wird als Post-It an das betreffende Benutzer- oder Computerkonto im AD angeheftet

Implicit Mapping Methoden

- Windows Kontoname (UPN) in der SAN-Erweiterung

- DNS-Name des Computers, wie er im AD eingetragen ist, in der SAN-Erweiterung

Explicit Mapping Methoden

- Nutzt Directory-Attribut *altSecurityIdentities*
- Information, die *altSecurityIdentities* eingestellt werden kann (alternativ)
  - Subject Distinguished Name (DN) des Zertifikats
  - E-Mail-Adresse (RFC822Name) in der SAN-Erweiterung des Zertifikats
  - Issuer DN und Subject DN des Zertifikats
  - Issuer DN und Seriennummer des Zertifikats
  - Inhalt der SKI-Erweiterung des Zertifikats
  - Hashwert des Public Keys im Zertifikat

Explicit Mapping Methoden

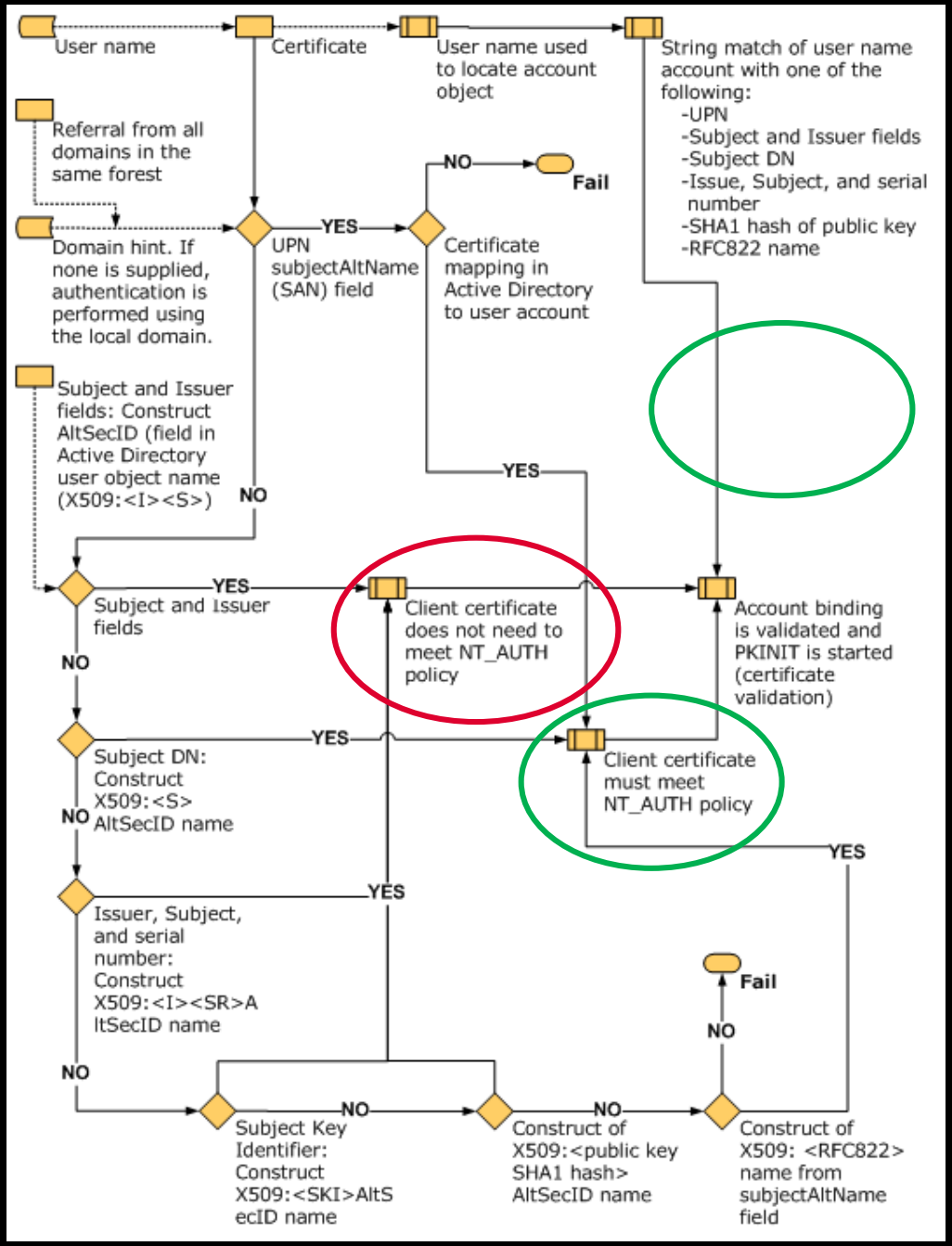
- Nutzt Directory-Attribut *altSecurityIdentities*
- Information, die *altSecurityIdentities* eingestellt werden kann (alternativ)
  - Subject Distinguished Name (DN) des Zertifikats
  - E-Mail-Adresse (RFC822Name) in der SAN-Erweiterung des Zertifikats
  - Issuer DN und Subject DN des Zertifikats
  - Issuer DN und Seriennummer des Zertifikats
  - Inhalt der SKI-Erweiterung des Zertifikats
  - Hashwert des Public Keys im Zertifikat

- Seit den Microsoft-Patches vom Mai 2022 in „stark“ und „schwach“ eingeteilt

… in *fast* allen Fällen NTAuth

- Auf die „NTAuth“-Bedingung wird verzichtet…
  - … wenn die ausstellende CA explizit genannt ist
  - … wenn (vermeintlich) der Public Key direkt referenziert wird

Quelle: https://docs.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-certificate-requirements-and-enumeration



Goldene Tickets und Goldene Zertifikate

Goldenes Ticket (Kerberos)

Logon Ticket für ein Konto mit hohen Rechten (Administrator, Domain Controller ö. ä.), möglichst lange gültig

Passender Symmetrischer Schlüssel dazu in der Hand des Angreifers

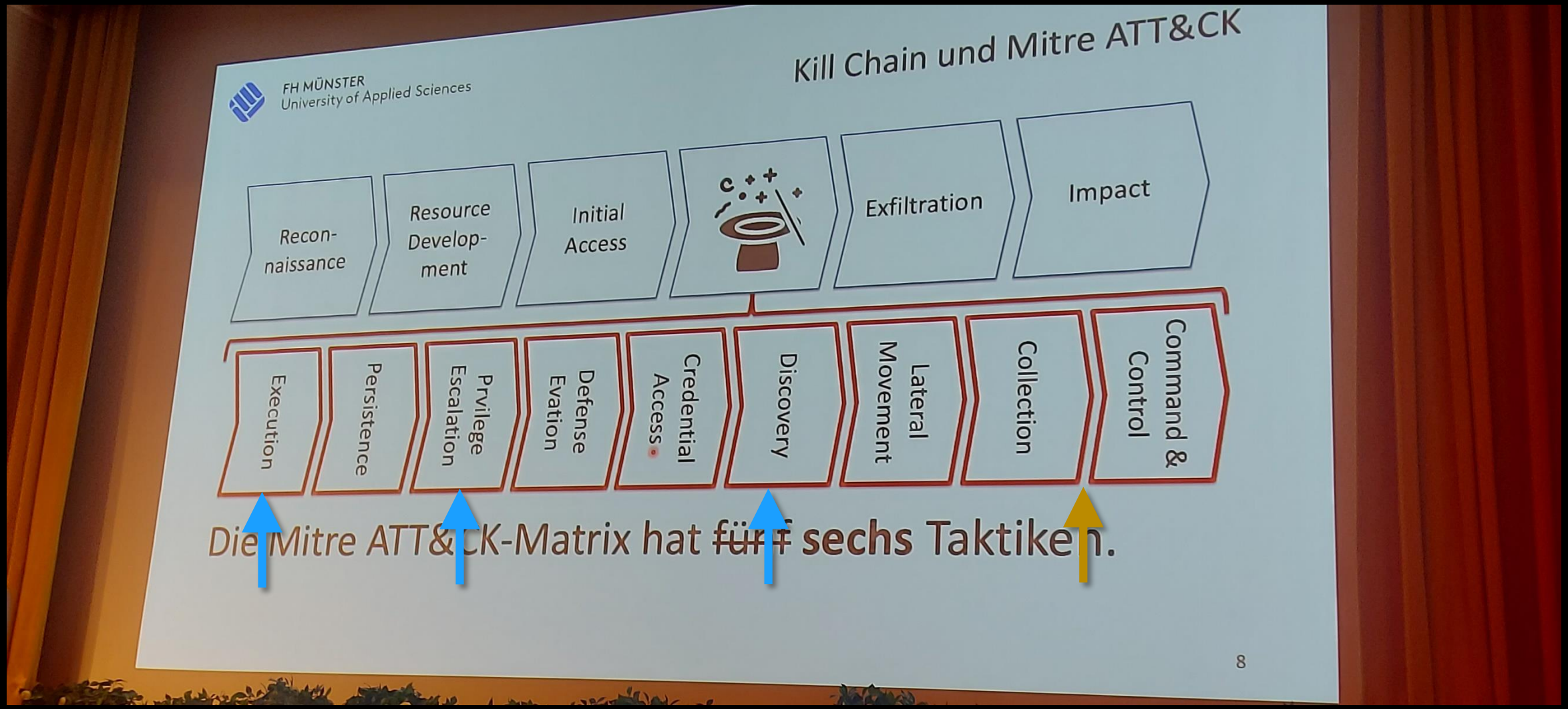
Goldenes Zertifikat

„PKInit-fähiges“ Zertifikat für ein Konto mit hohen Rechten (Administrator, Domain Controller ö. ä.)

Passender Private Key dazu in der Hand des Angreifers

Angriffe und Angriffsmöglichkeiten

… and here the magic happens …



Petit Potam Angriff

- Veröffentlicht im Juli 2021
- Generelle Voraussetzungen
  - AD-integrierte MS Enterprise CA mit CA Web Enrollment Oberfläche
- Ausgenutzte Schwachstelle: NTLM-Relaying (Man-in-the-Middle)
  - CA Web Enrollment läuft unter dem Internet Information Server (IIS) als Webserver
  - IIS akzeptiert standardmäßig Anmeldung per Kerberos oder NTLM
- Voraussetzungen des Angreifers
  - Angreifer verbindet sein eigenes System mit einem internen Netz, von dem aus er sowohl einen Domain Controller als auch den CA Web Enrollment Server erreichen kann

Petit Potam Ablauf

1. Angreifer installiert auf seinem System ein NTLM-Relay, das die Anmeldung eines anderen Systems als Man-in-the-Middle an das CA Web Enrollment weiterleitet
2. Angreifer triggert über eine Encrypted File System (EFS) Anfrage an den Domain Controller, das dieser sich bei seinem NTLM-Relay authentifiziert
3. NTLM Relay meldet sich als Domain Controller beim CA Web Enrollment an
4. Angreifer generiert sich ein Schüsselpaar und einen Zertifikatsrequest, über den er über das CA Web Enrollment ein Domain Controller Zertifikat bekommt
   - EKU OIDs: u. a. ClientAuthentication
   - SAN: DNS-Name des Domain Controllers

→ Goldenes Zertifikat

Certifried Angriff

- Entdeckt Ende 2021, Responsible Disclosure im Mai 2022
- Generelle Voraussetzungen
  - AD-integrierte MS Enterprise CA die Computerzertifikate für Windows-Arbeitsplätze ausstellt (bspw. für 802.1X-Anmeldung am WLAN und/oder LAN)
  - Praktisch immer wird dabei der Name im Zertifikat dem AD-Computer-Eintrag entnommen
- Ausgenutzte Schwachstelle: Attribut *dNSHostName* im AD-Computer-Account
  - Aus diesem Attribut wird der DNS-Name direkt in das Computerzertifikat übernommen
  - Keine Prüfung auf AD-weite Eindeutigkeit des gesetzten Wertes (zumindest vor dem Patch…)
  - Schreibrechte u. a. für SELF (Computerkonto) und CREATOR/OWNER (Domain-Join-Benutzer)
- Voraussetzungen des Angreifers
  - Angreifer ist bspw. lokaler Administrator eines Windows-Arbeitsplatzes
  - Weitere Wege möglich: via Domain Join im Self-Service oder lokale Rechte-Erweiterung

Certifried Ablauf

1. Angreifer nutzt als lokaler Administrator das Systemkonto des lokalen Computers
2. Angreifer überschreibt damit das AD-Attribut *dNSHostName* des lokalen Computers mit dem DNS-Namen eines Domain Controllers
3. Angreifer wartet ab oder triggert, dass der lokale Computer ein neues Computerzertifikat bekommt
4. Der Computer unter Kontrolle des Angreifers bekommt ein neues Computerzertifikat für einen Schlüssel im lokalen Keystore
   - Schlüsselverwendung: typischerweise ClientAuthentication (für IEEE 802.1X etc.)
   - SAN: DNS-Name des Domain Controllers

→ Goldenes Zertifikat

Was könnte noch schiefgehen? – Ansatzmöglichkeiten

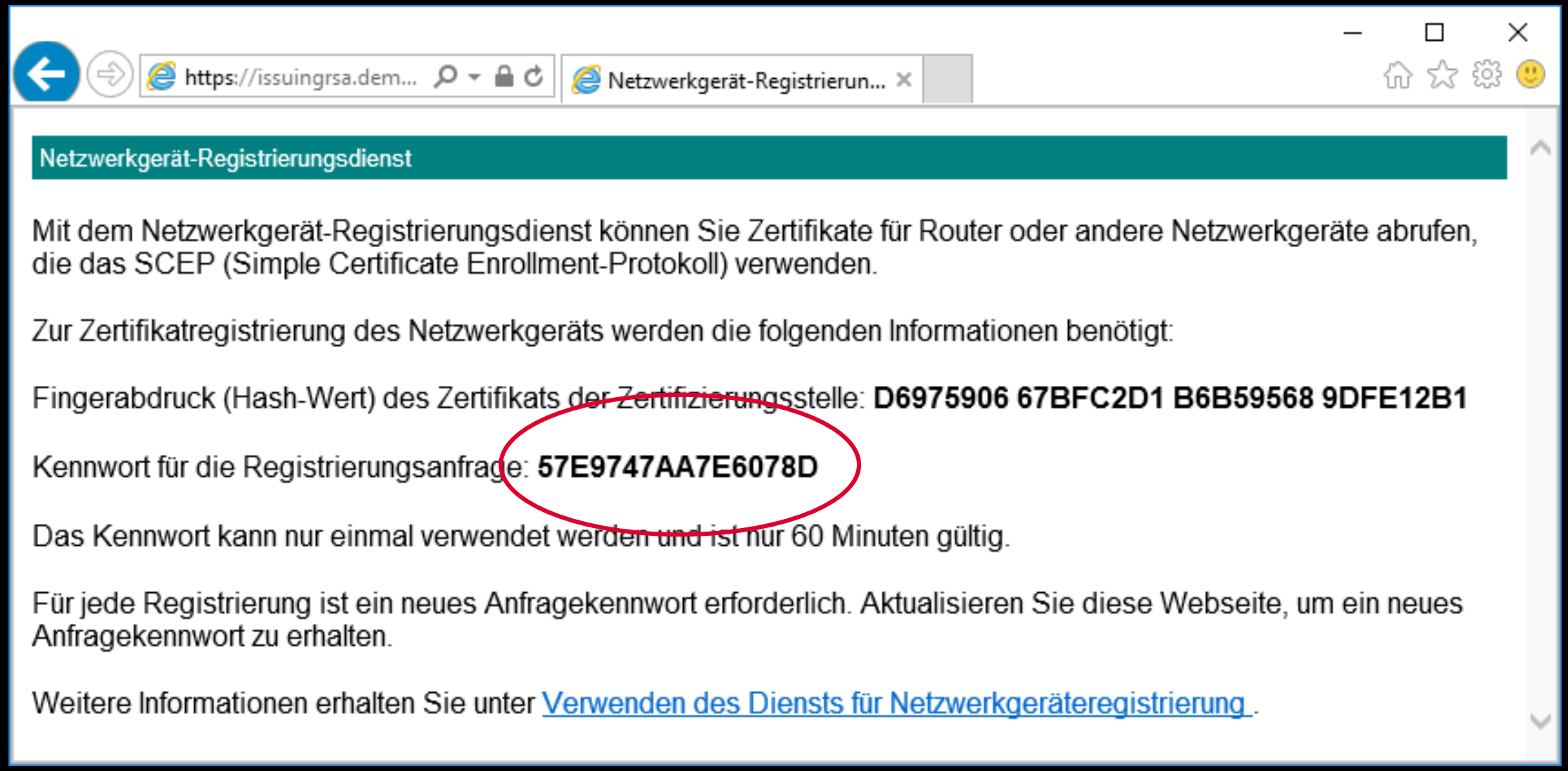
- Microsoft Certificate Enrollment Web Services – CEP / CES
  - Laufen wie das Web Enrollment als Anwendung im IIS
  - Anmeldeoptionen:
    - Clientzertifikat
    - Passwort
    - „Kerberos“
      In Wirklichkeit SPNEGO Negotiation = Kerberos oder NTLM
  - Ergo ebenfalls anfällig für NTLM-Relaying

Was könnte noch schiefgehen? – Ansatzmöglichkeiten

- Network Device Enrollment Service (NDES)
  - Microsoft-Implementierung des Simple Certificate Enrollment Protocol (SCEP)
  - Häufig genutzt von Mobile Device Management Systemen (MDM), um die verwalteten Mobilgeräte mit Zertifikaten auszustatten
  - Läuft ebenfalls als Anwendung im IIS, ergo anfällig für NTLM-Relaying

  Und mehr…
  - Zur Zertifikatsbeantragung genügt ein Einmalpasswort („SCEP-Challenge“)
  - Namen im Zertifikat werden aus dem Zertifikatsantrag übernommen
  - Abgefangene SCEP-Challenge ist potenziell Gutschein für ein Goldenes Zertifikat
  - Es gibt Schutzmechanismen dagegen, aber die werden oft nicht verwendet oder sind technisch nicht umsetzbar

NDES SCEP-Challenge – Abruf per Browser



Was könnte noch schiefgehen? – Ansatzmöglichkeiten

- Missbrauch des Explicit Mapping
  - Zum Beispiel bei unsicherer Vergabe von Schreibrechten im AD (im Default sicher):
    - Eintragen des eigenen Angreifer-Zertifikats
  - Zum Beispiel bei konfiguriertem Explicit Mapping mit SKI:
    - Unterschieben eines eigenen Root-Zertifikats des Angreifers
    - Ausstellen eines zweiten Zertifikats mit derselben SKI-Erweiterung unter diesem Root-Zertifikat

Microsofts Gegenmaßnahmen

Reaktionen auf Petit Potam

- Domain Controller lässt sich nicht mehr (so leicht) zu einer NTLM-Authentifikation verführen
- NTLM-Relaying – ist eher ein Feature (kann nicht einfach behoben werden)
- Empfehlung: NTLM möglichst weitgehend deaktivieren

Warum macht Microsoft das nicht schon längst in Standardeinstellung?
Weil dann vieles, das man vielleicht braucht, nicht mehr funktioniert.

Reaktion auf Certifried – KB5014754 – Mai 2022 Patchday

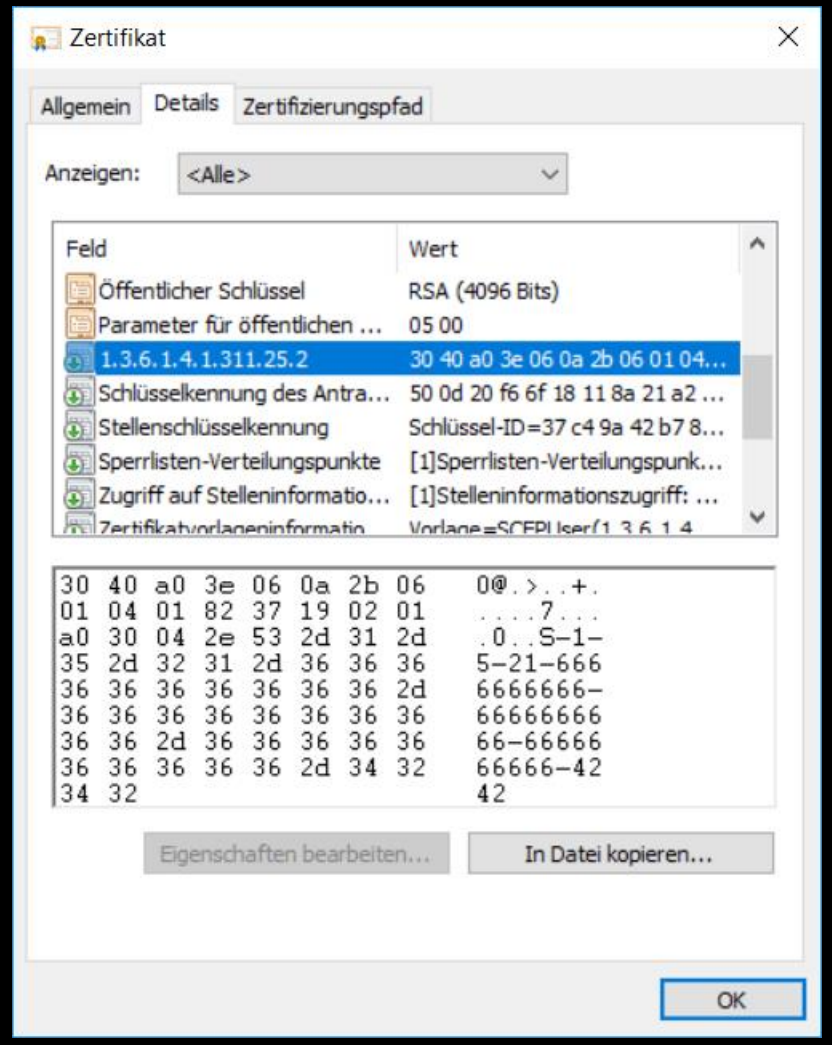
- Patches für
  - Domain Controller / Kerberos KDC
  - AD Certificate Services („Microsoft CA“)
  - SChannel Subsystem (Windows TLS Library)
- Änderungen
  - Beschreiben des *dNSHostName* Attributs: Host-Anteil muss gleich AD-Computername sein
  - Certificate Mapping Methoden (implizit und explizit) in „stark“ und „schwach“ unterteilt
  - Neue Zertifikatserweiterung mit AD Security Identifier
- Folgepatch für Mai *frühestens November* 2023 angekündigt
  - Dann akzeptieren Domain Controller nur noch „starke“ Mapping-Methoden
  - Komponenten wie der Network Policy Server (RADIUS) schon ab Mai 2022 kann aber vorläufig noch auf altes Verhalten zurückgestellt werden

Reaktion auf Certifried – KB5014754 – Mai 2022 Patchday

- Insgesamt eher unausgegoren…
  - Microsoft-CAs mit den Mai 2022 Patches schreiben die SID-Erweiterung in alle neu erstellten Zertifikate, bei denen der Inhabername aus dem AD übernommen wird
  - Potenzielle Sicherheitslücke (entdeckt durch Uwe Gradenegger):
    Bei Zertifikaten, für die der Inhabername aus dem Zertifikatsantrag übernommen wird, wird auch eine evtl. vorhandene SID-Erweiterung ungeprüft übernommen
  - Verwendung der SID-Erweiterung kann in der Oberfläche nicht konfiguriert werden wie bei anderen Zertifikate – insbesondere nicht genauso deaktiviert

Man merkt, dass das ursprüngliche Entwickler-Team der Active Directory Certificate Services aufgelöst wurde und nicht mehr greifbar ist.

Neue Zertifikatserweiterung sz_NTDS_CA_SCURITY_EXT



Enthält den eindeutigen AD Security Identifier (SID) des AD-Kontos

Kann auch bspw. mit OpenSSL nachgebildet werden

```
RANDFILE = ./tmp/.rnd
[ req ]
default_bits = 4096
default_keyfile = .\tmp\scep_key.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
prompt = no
string_mask = nombstr
req_extensions = sid_ext
[ req_distinguished_name ]
CN = SID Extension Test
[ req_attributes ]
challengePassword = F494CB4805C3F8E4
[sid_ext]
1.3.6.1.4.1.311.25.2 = ASN1:SEQUENCE:ntds_ca_security
[ntds_ca_security]
extension_value = IMPLICIT:0,SEQUENCE:name_sid
[name_sid]
type = OID:1.3.6.1.4.1.311.25.2.1
value = EXPLICIT:0,FORMAT:ASCII,OCTETSTRING:S-1-5-21-6666666666-6666666666-6666666666-4242
```

Implicit Mapping Methoden – „stark“ und „schwach“

- Windows Kontoname (UPN) in der SAN-Erweiterung

- DNS-Name des Computers, wie er im AD eingetragen ist, in der SAN-Erweiterung

- SID in der neuen SID-Erweiterung

Handlungsbedarf und Empfehlungen

Wenn man Zertifikate zur AD-Anmeldung einsetzt…

- … und die über eine eigene MS Enterprise CA ausstellt
  - Falls noch nicht geschehen, den KB5014754 auf dem Issuing-CA-Server einspielen
  - Falls Anmeldezertifikate mit Gültigkeit über Oktober 2023 hinaus im Umlauf sind, anstoßen, dass diese ersetzt werden
    - Sehr einfach, wenn Windows Certificate Autoenrollment verwendet wird
    - Bei Zertifikaten für Mobilgeräte ist in der Regel ein *entsprechender Patch für das MDM* erforderlich, Hersteller/Lieferanten anfragen
- … und die über ein Drittprodukt oder eine Managed PKI bezieht
  - Beim Lieferanten/Dienstleister nachhaken, ob/ab wann die SID-Erweiterung unterstützt wird
  - Sicherstellen, dass bis November 2023 alle Anmeldezertifikate durch neue mit SID-Erweiterung ersetzt werden
- Alternativ: starkes explizites Mapping für alle Anmeldezertifikate konfigurieren
  - Keine fertige Tool-Unterstützung von Microsoft, nicht zu vernachlässigender Aufwand

PetitPotam Angriff

Angreifer

Enterprise-CA installiert?

ja

CA-Zertifikat in NTAuth?

ja

Web-Enrollment oder CES installiert?

Domain Controller Zertifikat o. ä.

NTLM-Relay

Goldenes Zertifikat

nein

nein

Certifried Angriff

Maschinen-zertifikate für Clients?

Lokale Administrator-Rechte?

dNSHostName überschreiben

Explicit Mapping für hochberechtigte Benutzer konfiguriert?

ja

Explicit Mapping?

Andere, anfällige Zertifikatvorlagen

nein

Versuche etwas anderes…

NDES installiert?

Goldene SCEP Challenge

Für den DC vertrauenswürdige CA unter Kontrolle?

Zertifikat mit manipuliertem Issuer DN oder SKI

PetitPotam Angriff

Angreifer

Enterprise-CA installiert?

ja

CA-Zertifikat in NTAuth?

ja

Web-Enrollment oder CES installiert?

Domain Controller Zertifikat o. ä.

NTLM deaktivieren

Goldenes Zertifikat

nein

nein

Certifried Angriff

Maschinen-zertifikate für Clients?

Lokale Administrator-Rechte?

dN… …iben

KB5014754 Patch

Explicit Mapping für hochberechtigte Benutzer konfiguriert?

ja

Explicit Mapping?

Andere, anfällige Zertifikatvorlagen

nein

Versuche etwas anderes…

NDES installiert?

Goldene SCEP Challenge

Für den DC vertrauenswürdige CA unter Kontrolle?

Zertifikat mit manipuliertem Issuer DN oder SKI

Weitere mögliche Schutzmaßnahmen

- Web Enrollment / Certificate Enrollment Web Services deaktivieren
- Einsatz von NTLM verbieten
  - Gut: für den CA-Server, besser: für alle Domain Controller, am besten: im gesamten AD
- NDES nicht verwenden
  - Manche MDM-Software kann Zertifikate auch ohne SCEP ausrollen
- NDES absichern durch ein NDES Policy Modul
  - Wo das geht: z. B. MS Intune – Wo man in die Röhre schaut: u. a. BlackBerry UEM
- Zertifikat der Issuing-CA aus dem NTAuth Container entfernen
- Einsatz eines CA Policy Moduls wie TameMyCerts von Uwe Gradenegger
  - Blacklisting von kritischen Namen in Zertifikaten

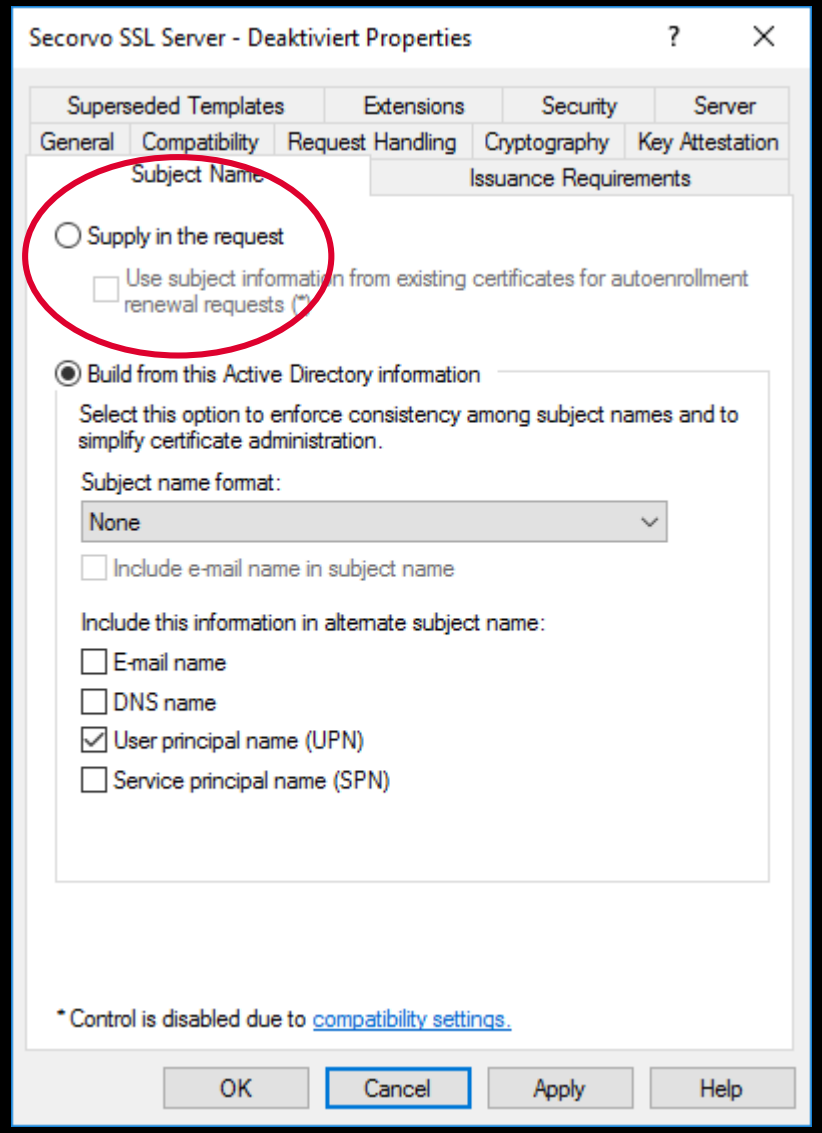
Weitere mögliche Schutzmaßnahmen

- Web Enrollment / Certificate Enrollment Web Services deaktivieren
- Einsatz von NTLM verbieten
  - Gut: für den CA-Server, besser: für alle Domain Controller, am besten: im gesamten AD
- NDES nicht verwenden
  - Manche MDM-Software kann Zertifikate auch ohne SCEP ausrollen
- NDES absichern durch ein NDES Policy Modul
  - Wo das geht: z. B. MS Intune – Wo man in die Röhre schaut: u. a. BlackBerry UEM
- Zertifikat der Issuing-CA aus dem NTAuth Container entfernen
- Einsatz eines CA Policy Moduls wie TameMyCerts von Uwe Gradenegger
  - Blacklisting von kritischen Namen in Zertifikaten

Meist geht einiges davon nicht, ohne benötigte Funktionalität zu verlieren

Auf weitere Einfallstore für potentielle Goldene Zertifikate prüfen

- „Offline“-Zertifikatstemplates mit „Subject Name: supply in the request“
  - Sparsam verwenden
  - Welche EKU OID werden verwendet?
  - Wer hat „Enroll“ Rechte zur Beantragung?
  - Im Zweifel durch einen Certificate Manager vor der Ausstellung manuell prüfen
  - Ggf. damit erstellte Zertifikate auf „kritische“ Namen (Domain Controller, AD-Administratoren, …) scannen
    - Zertifikatsdatenbank
    - Event-Log
    - Mails des SMTP-Exit-Moduls der Microsoft-CA



Auf weitere Einfallstore für potentielle Goldene Zertifikate prüfen

- Bei welchen AD-Konten ist Explicit Mapping konfiguriert?
  - Insbesondere eine der Varianten ohne NTAuth Policy Check
  - Bei der Gelegenheit auch gleich das Attribut *msDS-KeyMaterial*
    - Ab Windows Server 2016 ergänzt für Windows Hello for Business im Key Trust Mode
  - Wer hat Schreibrechte auf diese Attribute?
  - Wird das alles so (noch) benötigt?
  - *ldifde.exe* hilft

- Welche Trusted Root-CAs wurden auf Domain Controllern nachträglich ergänzt?
  - D. h. nicht von Microsoft über deren Root-CA-Programm geprüft und verteilt
  - *sigcheck64.exe* aus den Sysinternals Tools hilft


secorvo
security consulting
Ettlinger Str. 12-14
76137 Karlsruhe
Telefon +49 721 255171-0
Telefax +49 721 255171-100
info@secorvo.de
www.secorvo.de