

Patch KB5014754

Ing. Bc. Martin Mikala
Bc. Jakub Kolařík
MONET+



KB5014754

- KB5014754: Certificate-based authentication changes on Windows domain controllers
- Vydán 10. května 2022
- různé verze OS Windows Server



Opravené zranitelnosti

- **kritická** zranitelnost CVE-2022-26923
- **kritická** zranitelnost CVE-2022-26931
- **kritická** zranitelnost CVE-2022-34691 (objevena až v srpnu)
- Eskalace privilegií v případě, že je použito přihlášení do Active Directory za použití certifikátu
- Doporučení instalovat patch co nejdříve

Dopad patche

- Certifikáty určené k autentizaci musí být nově lépe svázány s konkrétní identitou v AD
- Některé současné (stále platné) certifikáty nebude možno využít k autentizaci
- Přechodné období do 9. května 2023, kdy je možno využít "slabé" ztotožnění certifikátu (dle nastaveného módu operace AD serveru)

Módy operace

- Full Enforcement
 - preferovaný mód
 - silné ztotožnění
 - bude fungovat i po 9. květnu 2023
- Compatibility
 - silné i slabé ztotožnění
 - slabé ztotožnění je umožněno, ale logováno jako varování
 - **bude zrušeno k 9.květnu 2023**
- Disabled
 - neprobíhá ztotožnění ani logování
 - **bude zrušeno k 9.květnu 2023**

Praktické dopady

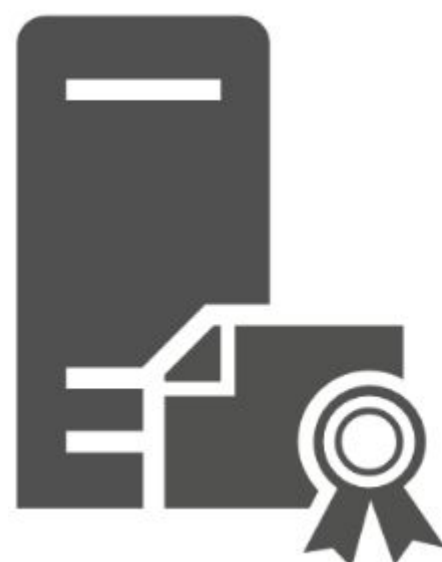
Proč se tím zabýváme?

Praktické dopady

- Pokud nebudou aplikována opatření popsaná v dalších slidech, v prostředí MS AD **přestane fungovat** (po aplikování Full Enforcement Mode):
 - Použití certifikátů pro autentizaci klienta opřenu o doménové mechanismy MS AD, např.:
 - Autentizace do operačního systému (např. funkcionality Smart Card Logon, 2FA)
 - Autentizace certifikátem na webové služby
- Prakticky ověřeno – PoC s nastavením Full Enforcement Mode
- **MS (DOMÉNA AD) BUDE NOVĚ VYŽADOVAT “AKTIVUM”, KTERÉMU BUDE DŮVĚŘOVAT**

Ztotožnění certifikátu

- **Na straně certifikátů** (doplnění SID do certifikátů)
- příklad SID S-1-5-21-661419251-832279228-3773173558-3765
- nekritické rozšíření OID 1.3.6.1.4.1.311.25.2 se zakódovanou hodnotou SID držitele certifikátu
- Jak řešit v rámci **MS AD Certificate Services**?



Active Directory
Certificate Services

Ztotožnění certifikátu

Superseded Templates Extensions Security Server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:

Fully distinguished 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)

* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

Ztotožnění certifikátu

- Šablona certifikátu s nastavením Subject Name - **Build from this Active Directory Information**
 - CA automaticky doplní rozšíření do certifikátu s hodnotou SID držitele certifikátu
 - Pravděpodobně většina uživatelských certifikátů v organizacích
- Šablona certifikátu s nastavením Subject Name - **Supply in the Request**
 - Je nutné zakódovat rozšíření do žádosti o certifikát (PKCS#10)
 - Využíváno pro možnost zakódování specifických informací do certifikátu, které nejsou v AD dostupné - typicky větší organizace

Zakódování v žádosti

1.3.6.1.4.1.311.25.2: Flags = 0, Length = 41

```
0000 30 3f a0 3d 06 0a 2b 06 01 04 01 82 37 19 02 01 0?.=...+.....7...
0010 a0 2f 04 2d 53 2d 31 2d 35 2d 32 31 2d 31 36 31 ./.-S-1-5-21-161
0020 33 31 32 39 34 33 34 2d 33 32 31 31 32 38 36 33 3129434-32112863
0030 30 2d 31 36 32 30 34 39 39 36 36 35 2d 32 31 38 0-1620499665-218
0040 36 6
```

```
0000: 30 3f ; SEQUENCE (3f Bytes)|
0002: a0 3d ; OPTIONAL[0] (3d Bytes)
0004: 06 0a ; OBJECT_ID (a Bytes)
0006: | 2b 06 01 04 01 82 37 19 02 01
| ; 1.3.6.1.4.1.311.25.2.1
0010: a0 2f ; OPTIONAL[0] (2f Bytes)
0012: 04 2d ; OCTET_STRING (2d Bytes)
0014: 53 2d 31 2d 35 2d 32 31 2d 31 36 31 33 31 32 39 ; S-1-5-21-1613129
0024: 34 33 34 2d 33 32 31 31 32 38 36 33 30 2d 31 36 ; 434-321128630-16
0034: 32 30 34 39 39 36 36 35 2d 32 31 38 36 ; 20499665-2186
```


ACEx - Automated Certificate Exchange

Certifikáty bude třeba převydat

Aktualizace certifikátů



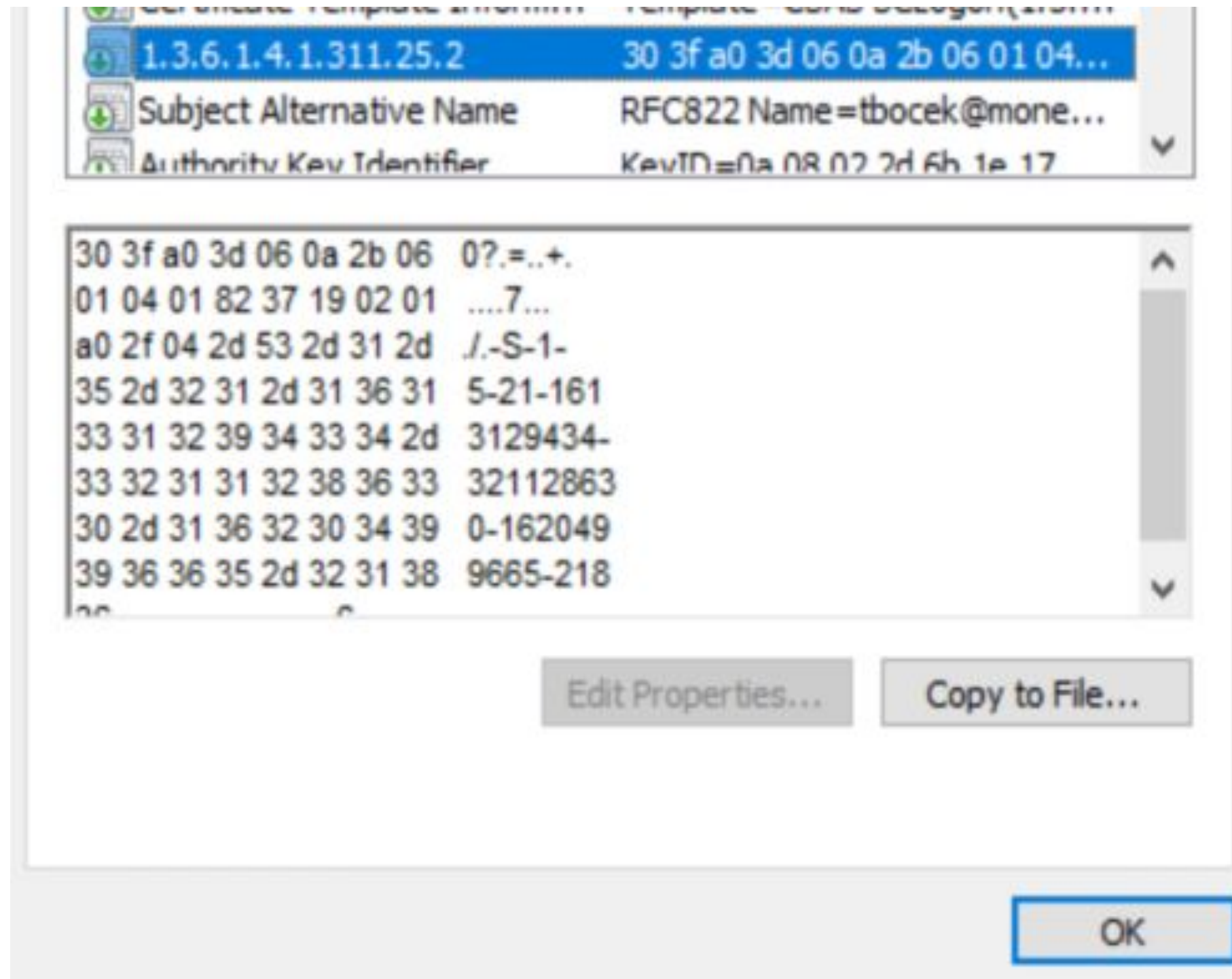
- Je třeba aktualizovat certifikáty uživatele CMSCSI \jkolarik
- Ponechte čipovou kartou 9203801209151324 ve čtečce
- Proces aktualizace spusťte tlačítkem Aktualizovat

Aktualizovat

Rozhodnout...

Podrobnosti...

Příklad SID v certifikátu



Dekódování SID z certifikátu v aplikaci Správce karty ProID+

Správce karty ProID

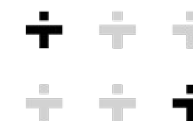
Soubor Zobrazení Nástroje Nápověda

- Alcor Micro USB Smart Card Reader 0
 - 9203803022182588
 - PIN
 - PUK
 - QPIN
 - SmartcardLogonUserRSA - 5ae85217-59e1-4
 - Kolařík Jakub**
 - imp20220823-ea5b2706-94d0-44b1-998c-26b
- Microsoft Virtual Smart Card 0

CERTIFIKÁT

Sériové číslo:	4700000336BA62A2F2AE6290CC000000000336
Platnost:	29.07.2022 11:10:17 - 25.06.2024 10:31:06
Vydal:	Monet Internal CA 01, monetplus, cz
Pro:	Kolařík Jakub, monetplus, cz, OU_VAU_Users, OU_VAU
Stav:	platný
Účel použití:	Ověření klienta Přihlášení pomocí čipové karty
Alternativní název:	UPN: jkolarik@monetplus.cz
SID:	S-1-5-21-661419251-832279228-3773173558-2414
Šablona:	Smartcard Logon User RSA
Otisk (SHA-1):	E4D7 4A08 F257 7569 6CC9 CE51 AFB0 6831 CDEB 7A9B

Více informací Export do souboru



Ztotožnění certifikátu

- **Na straně Active Directory**
 - Namapování certifikátů do altSecurityIdentities v AD
 - Slabé (např. emailová adresa)
 - Silné (např. vydavatel + SN certifikátu)

S čím vám rádi pomůžeme

Pro zákazníky MONET+ se servisní smlouvou:

- Budeme kontaktovat napřímo a navrhujeme řešení

Pro všechny ostatní organizace:

- Provedeme revizi PKI a certifikátů – **zdarma**
- Aplikujeme doporučené změny v souladu s legislativou a normami
- Navrhujeme nástroje pro automatizaci certifikátů



ProID

A modern office interior with a man on a phone, a man on stairs, and a man and woman talking.

Děkuji!

Potřebujete vyřešit kryptografii
ve vaší organizaci?

Kontaktujte nás.

www.proid.cz | info@proid.cz

