Certifikáty pro Secure Boot a co s nimi v roce 2026

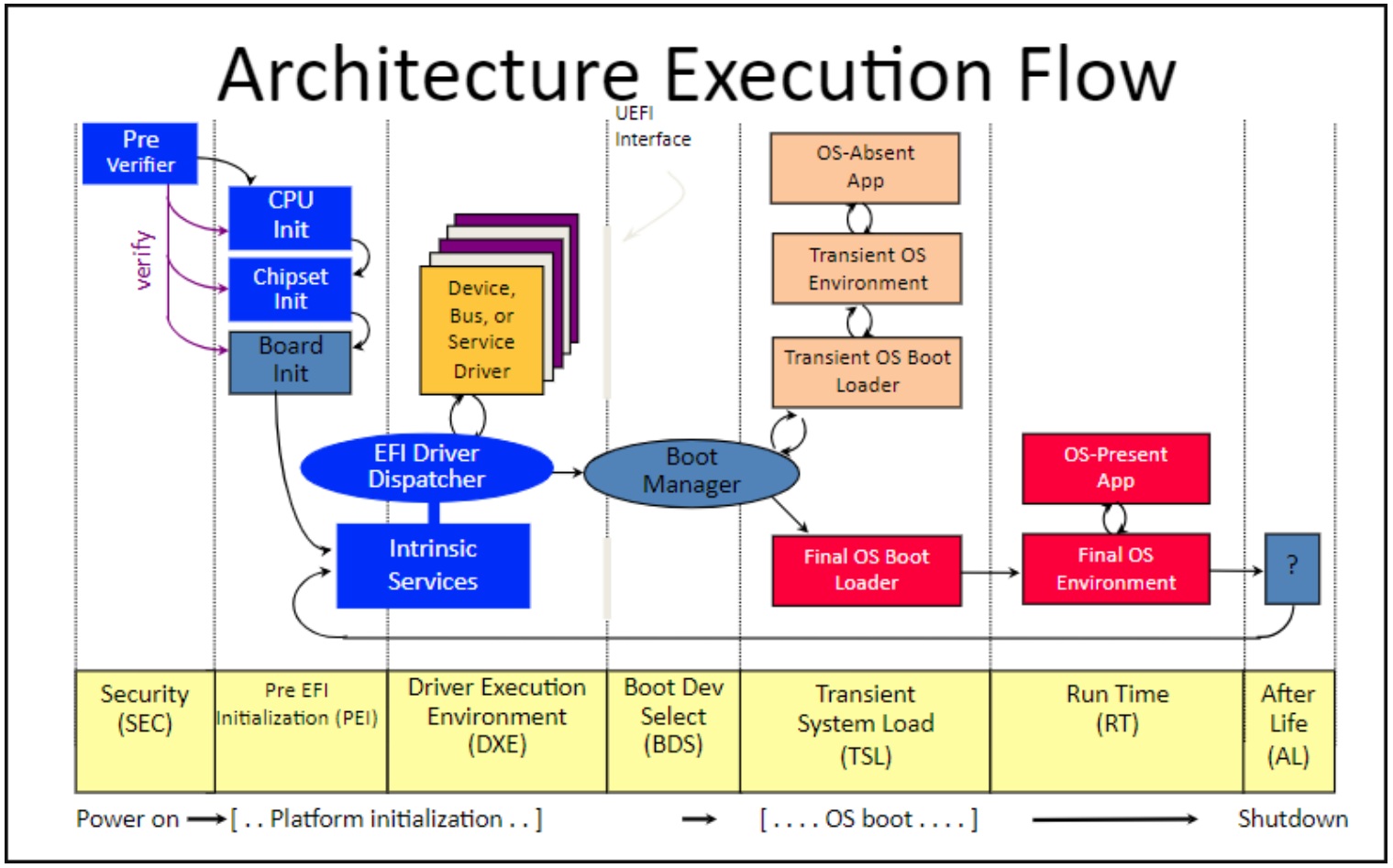
WUG Admin Day 2026

Jan Grundmann
Senior Consultant | grundmann@kpcs.cz
KPCS

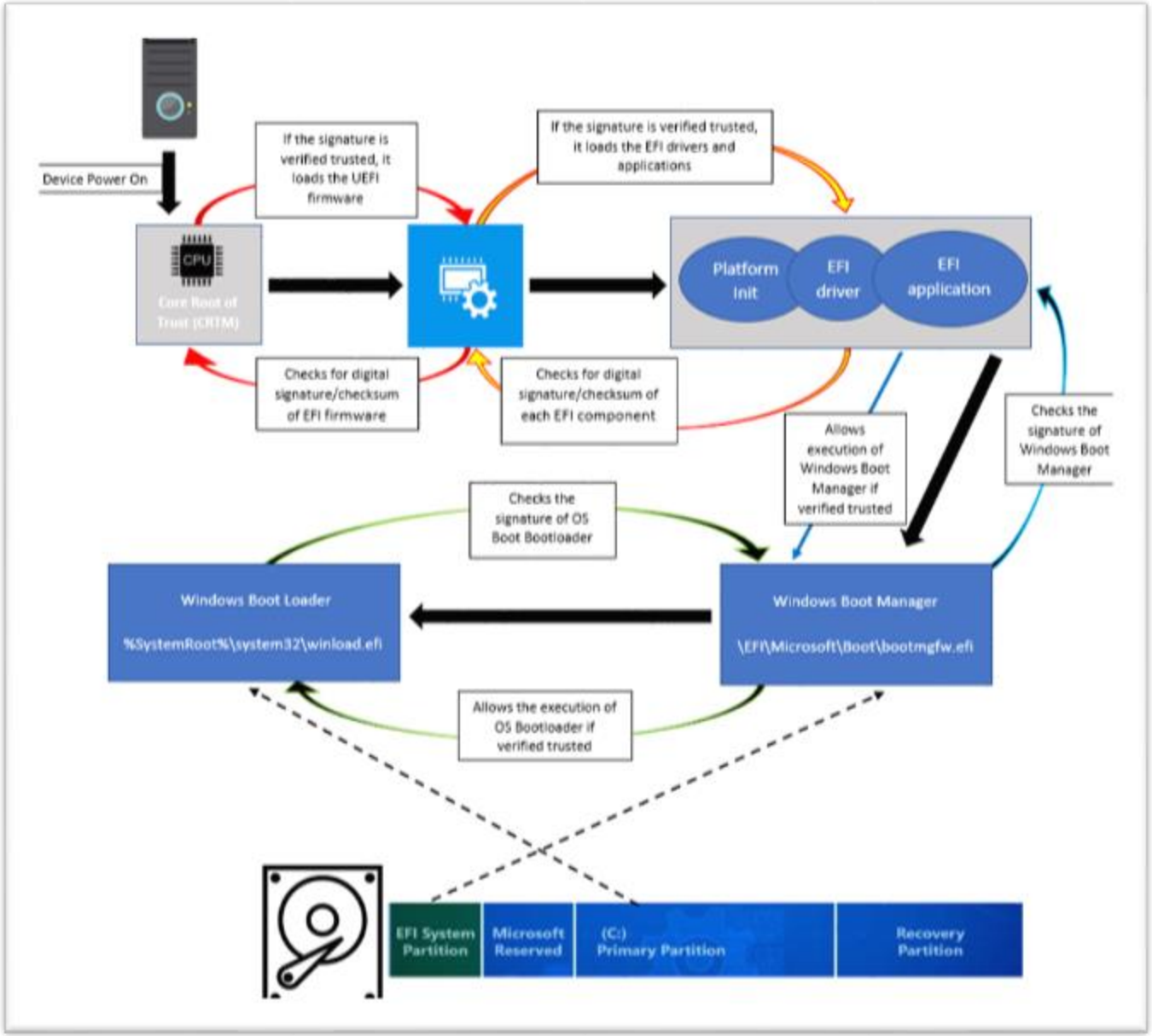
Intro

- Vyprší certifikáty
  - Bulvár: "… a vy už nenabootujete."
  - Řetězové maily: " … a pokud nepošlete tuto zprávu 5 přátelům, bude váš počítač hacknut."
  - Realita: " … a nic." *(moc zásadního se nestane)*
    - Nepůjde patchovat Secure Boot

Jak bootuje počítač?

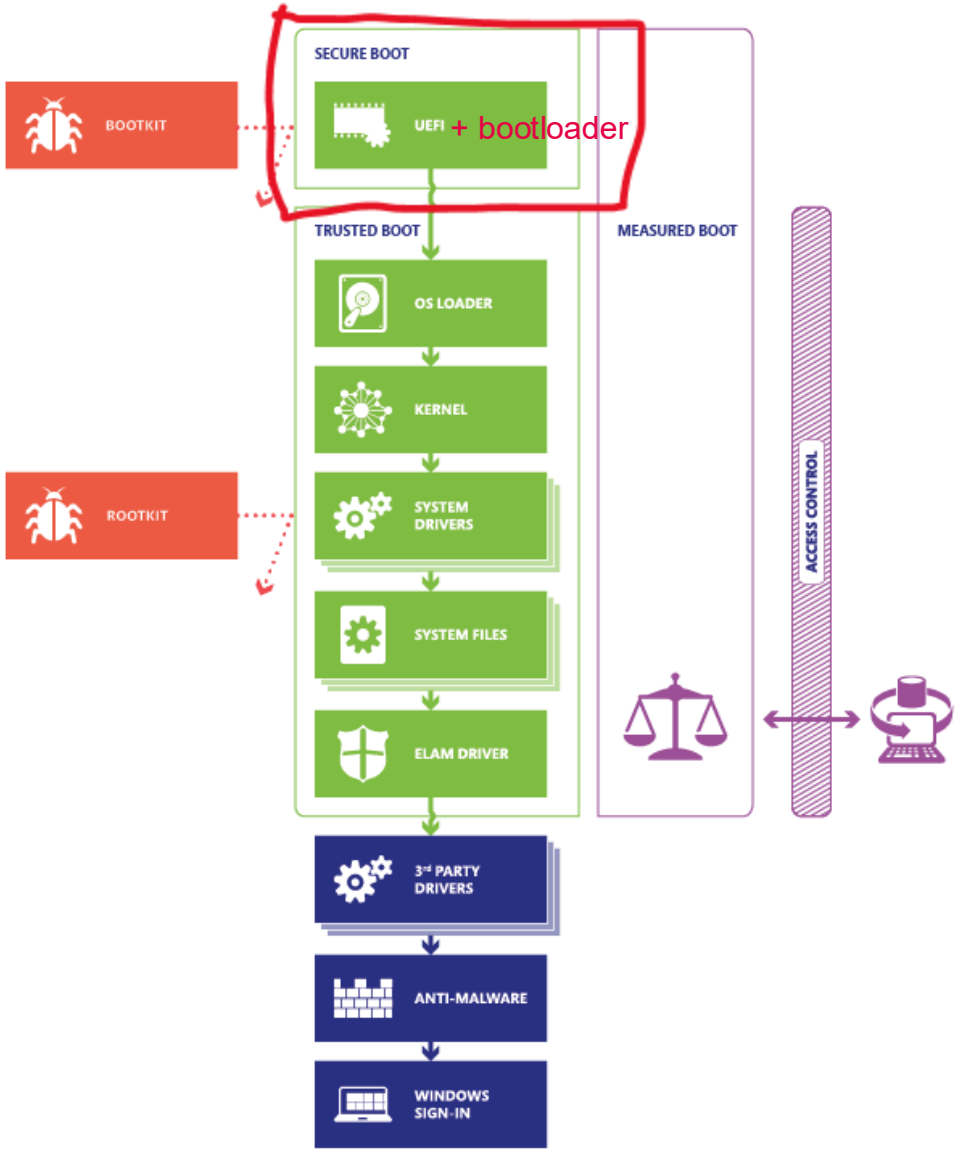


Co je to ten Secure Boot?



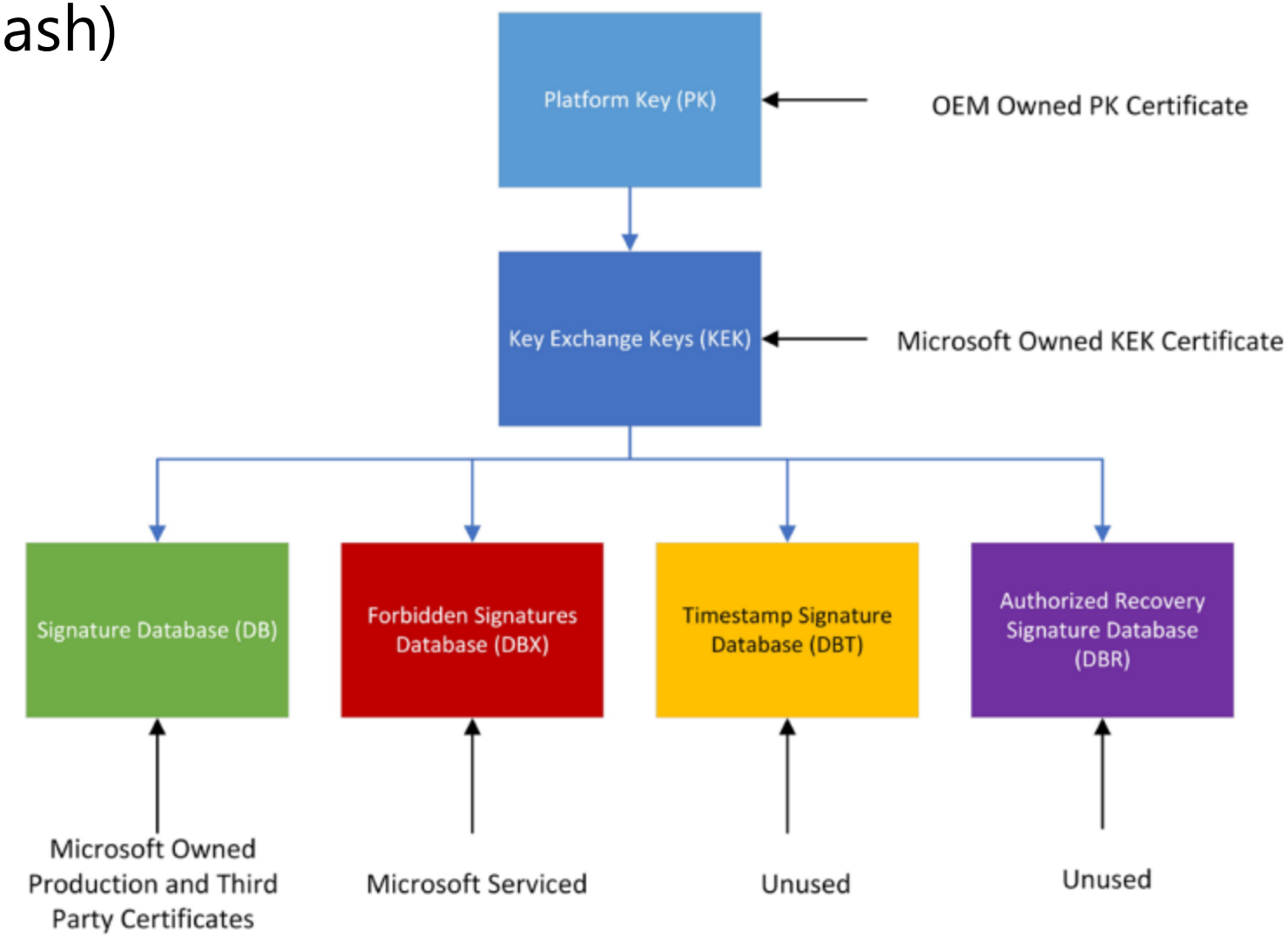
Co je to ten Secure Boot?

- Secure boot je bezpečnostní řešení, které chrání komponenty v rámci UEFI (před bootem OS)
- Microsoft ještě rozeznává Trusted Boot, což je ochrana bootu OS
- Secure Boot + Trusted Boot = Measured Boot
- Bootloader \EFI\Microsoft\Boot\bootmgfw.efi
- OS loader \Windows\System32\winload.efi



A jak to zabezpečí?

- Validace kódu (signed, hash)
- Čemu věříme?
  - UEFI proměnným



Příklad

- PK: Dell

```
PS C:\WINDOWS\system32> Get-UEFICertificate.ps1


Type            : PK
Description     : Platform Key
Index           : 1
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 70564dce-9afc-4ee3-85fc-949649d7e45c
CertificateSize : 929
Subject         : CN=Dell Inc. Platform Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Issuer          : CN=Dell Inc. Platform Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Thumbprint      : 44D641CACA0809002398B4877B8E982ED26F7B76
Issued          : 6/1/2016 10:20:07 PM
Expires         : 6/1/2031 10:30:06 PM
SerialNumber    : 50A1BD858AE7B6BC402DCA78CDD268A1
ParseError      :
RawData         : {48, 130, 3, 157...}
```

Příklad

- KEK: Dell, Microsoft

```
Type            : KEK
Description     : Key Exchange Key
Index           : 1
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 70564dce-9afc-4ee3-85fc-949649d7e45c
CertificateSize : 966
Subject         : CN=Dell Inc. Key Exchange Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Issuer          : CN=Dell Inc. Platform Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Thumbprint      : D4884608AEA442433CF06E5A2164BFF8D3D310D6
Issued          : 6/1/2016 10:22:48 PM
Expires         : 6/1/2023 10:32:47 PM
SerialNumber    : 279BAD52BF5DABB24C367742F4EBACCD
ParseError      :
RawData         : {48, 130, 3, 194...}

Type            : KEK
Description     : Key Exchange Key
Index           : 2
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1516
Subject         : CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer          : CN=Microsoft Corporation Third Party Marketplace Root, O=Microsoft Corporation, L=Redmond,
                  S=Washington, C=US
Thumbprint      : 31590BFD89C9D74ED087DFAC66334B3931254B30
Issued          : 6/24/2011 10:41:29 PM
Expires         : 6/24/2026 10:51:29 PM
SerialNumber    : 610AD188000000000003
ParseError      :
RawData         : {48, 130, 5, 232...}
```

Příklad

- DB: 2x Dell, 2x Microsoft

```
ype            : DB
escription     : Signature Database
ndex           : 1
ignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
wnerGuid       : 70564dce-9afc-4ee3-85fc-949649d7e45c
ertificateSize : 936
ubject         : CN=Dell Bios DB Key, O=Dell Inc., L=Round Rock, S=TX, C=USA
ssuer          : CN=Dell Bios Key Exchange Key, O=Dell Inc., L=Round Rock, S=TX, C=USA
humbprint      : F118703532B370164B6C3872C018DD68A9FE8A2D
ssued          : 8/10/2018 1:04:36 AM
xpires         : 8/10/2028 1:14:36 AM
erialNumber    : 1D6D9590D4808C8E4F82A0089A16FE39
arseError      :
awData         : {48, 130, 3, 164...}

ype            : DB
escription     : Signature Database
ndex           : 2
ignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
wnerGuid       : 70564dce-9afc-4ee3-85fc-949649d7e45c
ertificateSize : 951
ubject         : CN=Dell Bios FW Aux Authority 2018, O=Dell Inc., L=Round Rock, S=TX, C=USA
ssuer          : CN=Dell Bios Key Exchange Key, O=Dell Inc., L=Round Rock, S=TX, C=USA
humbprint      : 094CCEC85BBAA160B8EE0296BEA24FD7C3A3EB08
ssued          : 12/11/2018 10:59:23 PM
xpires         : 12/11/2028 11:09:23 PM
erialNumber    : 22584D1F857B55BC4CE1E6F0BDF7BE08
arseError      :
awData         : {48, 130, 3, 179...}
```

```
Type            : DB
Description     : Signature Database
Index           : 3
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1499
Subject         : CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L
Issuer          : CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporatio
Thumbprint      : 580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D
Issued          : 10/19/2011 8:41:42 PM
Expires         : 10/19/2026 8:51:42 PM
SerialNumber    : 6107765600000000008
ParseError      :
RawData         : {48, 130, 5, 215...}
```

```
Type            : DB
Description     : Signature Database
Index           : 4
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1556
Subject         : CN=Microsoft Corporation UEFI CA 2011, O=Microsoft Corporation, L=Redmond
Issuer          : CN=Microsoft Corporation Third Party Marketplace Root, O=Microsoft Corpor
                  S=Washington, C=US
Thumbprint      : 46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3
Issued          : 6/27/2011 11:22:45 PM
Expires         : 6/27/2026 11:32:45 PM
SerialNumber    : 6108D3C4000000000004
ParseError      :
RawData         : {48, 130, 6, 16...}
```

Problém

- "Microsoft Corporation KEK CA 2011" vyprší 24.6.2026.
  - pak MS nepůjde aktualizovat DB/DBX
- "Microsoft Windows Production PCA 2011" vyprší 19.10.2026.
  - pak nepůjde podepsat žádná 1st party MS Secure Boot komponenta, hlavně bootloader (Windows Boot Manager)
- "Microsoft UEFI CA 2011" vyprší 27.6.2026.
  - pak nepůjde podepsat 3rd party Secure Boot komponenty (Linux Shim, …)
  - bifurkace

Problém

- CVE-2026-21265

Co s tím?

- následovat MS playbook
  - ...který říká, že to MS nasadí
  - ", ale ..."

Secure Boot Certificate updates: Guidance for IT professionals and organizations

▶ *Applies To*

Original Published Date: June 26, 2025

KB ID: 5062713

This article has guidance for:

Organizations (enterprise, small business, and education) with IT-managed Windows devices and updates.

Note: If you are an individual who owns a personal Windows device, please go to the article Windows devices for home users, businesses, and schools with Microsoft-managed updates.

Co se může stát?

- že to nasazení neproběhne úspěšně
  - UEFI neumí Secure Boot config update (většinou u KEK)
  - OEM neautorizoval update MS KEK (podpisem PK)
    - ztráta přístupu k PK
    - nereagoval na výzvu od MS
    - OEM out of business

- "A může se to stát i mně?"

Jak si stojí moje portfolio?

1) Mám UEFI, co nedělá problémy?
   - hurá za OEM

2) Doručí(il) mi MS nové certifikáty?
   - musím si udělat inventuru

Inventura

- Event Log – System - "TPM-WMI" - id 1801 a 1808
- Registry
  - HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot "AvailableUpdates"
    - řídící prvek skrze bitmask (dword)
    - 0 (nebo nepřítomnost) -> nic se neděje
    - nenulové číselné hodnoty -> něco se děje
  - .\Servicing "UEFICA2023Status"
    - lidsky srozumitelný string NotStarted/InProgress/Updated
    - tamtéž "UEFICA2023Error" - detail případné chyby
    - tamtéž "WindowsUEFICA2023Capable" - prý nepoužívat

A co dál?

- 3 cesty nasazení
  - hands off
    1) MS doručí díky "high confidence bucket"
    2) MS doručí díky "controlled feature rollout"
  - hands on
    3) orchestruju sám

- Proč ne OEM?

1) "high confidence bucket"

- Default
  - "HighConfidenceOptOut" na 1
- bucket podle variant hw/sw
- postupné nasazování a sledování skrze diagnostic data (cizí), pokud úspěch, nasazujeme pro celý bucket v rámci CU
- neprůhledné

2) "controlled feature rollout"

- "MicrosoftUpdateManagedOptIn" na 1
- musím mít zapnutá diagnostic data
- není jasný rozdíl od "high confidence bucket"
  - Zřejmě bude docházet k aplikaci dynamičtěji i mimo CU
- neprůhledné

3) udělej si sám

- "AvailableUpdates" - "0" -> "0x5944"

- Scheduled task " \Microsoft\Windows\PI\Secure-Boot-Update"
  - Startuje co 12 hodin

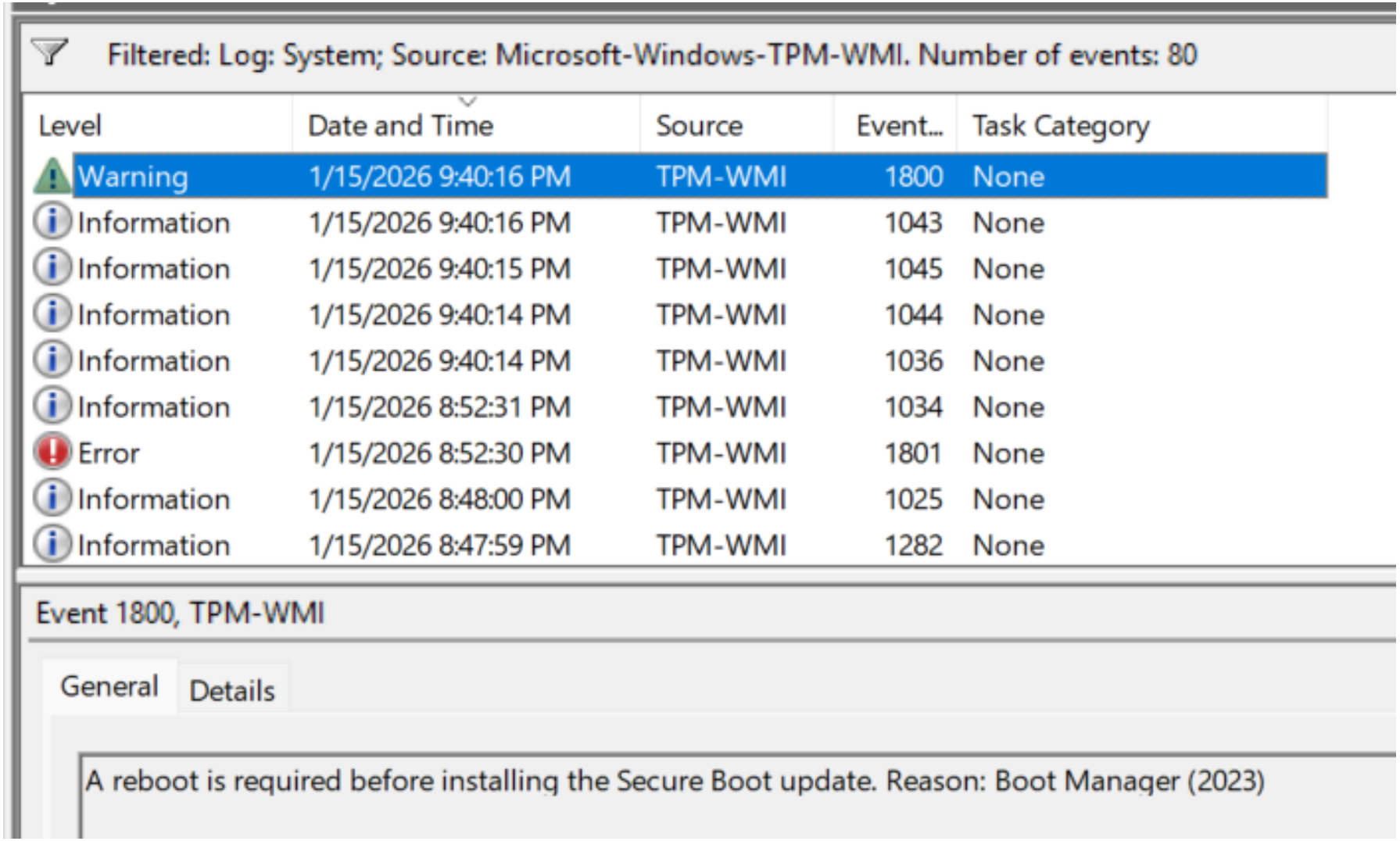
3) udělej si sám

1) reg add HKLM\SYSTEM\CurrentControlSet\Control\SecureBoot /t REG_DWORD /v AvailableUpdates /d 0x5944 /f

2) schtasks /run /tn "Secure-Boot-Update"

3) shutdown /r /t 0

3) udělej si sám



3) udělej si sám

```
Type            : KEK
Description     : Key Exchange Key
Index           : 1
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 70564dce-9afc-4ee3-85fc-949649d7e45c
CertificateSize : 966
Subject         : CN=Dell Inc. Key Exchange Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Issuer          : CN=Dell Inc. Platform Key, O=Dell Inc., L=Round Rock, S=Texas, C=US
Thumbprint      : D4884608AEA442433CF06E5A2164BFF8D3D310D6
Issued          : 6/1/2016 10:22:48 PM
Expires         : 6/1/2023 10:32:47 PM
SerialNumber    : 279BAD52BF5DABB24C367742F4EBACCD
ParseError      :
RawData         : {48, 130, 3, 194...}

Type            : KEK
Description     : Key Exchange Key
Index           : 2
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1516
Subject         : CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer          : CN=Microsoft Corporation Third Party Marketplace Root, O=Microsoft Corporation, L=Redmond,
                  S=Washington, C=US
Thumbprint      : 31590BFD89C9D74ED087DFAC66334B3931254B30
Issued          : 6/24/2011 10:41:29 PM
Expires         : 6/24/2026 10:51:29 PM
SerialNumber    : 610AD188000000000003
ParseError      :
RawData         : {48, 130, 5, 232...}

Type            : KEK
Description     : Key Exchange Key
Index           : 3
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1462
Subject         : CN=Microsoft Corporation KEK 2K CA 2023, O=Microsoft Corporation, C=US
Issuer          : CN=Microsoft RSA Devices Root CA 2021, O=Microsoft Corporation, C=US
Thumbprint      : 459AB6FB5E284D272D5E3E6ABC8ED663829D632B
Issued          : 3/2/2023 9:21:35 PM
Expires         : 3/2/2038 9:31:35 PM
SerialNumber    : 330000001314168B616D82824B000000000013
ParseError      :
RawData         : {48, 130, 5, 178...}
```

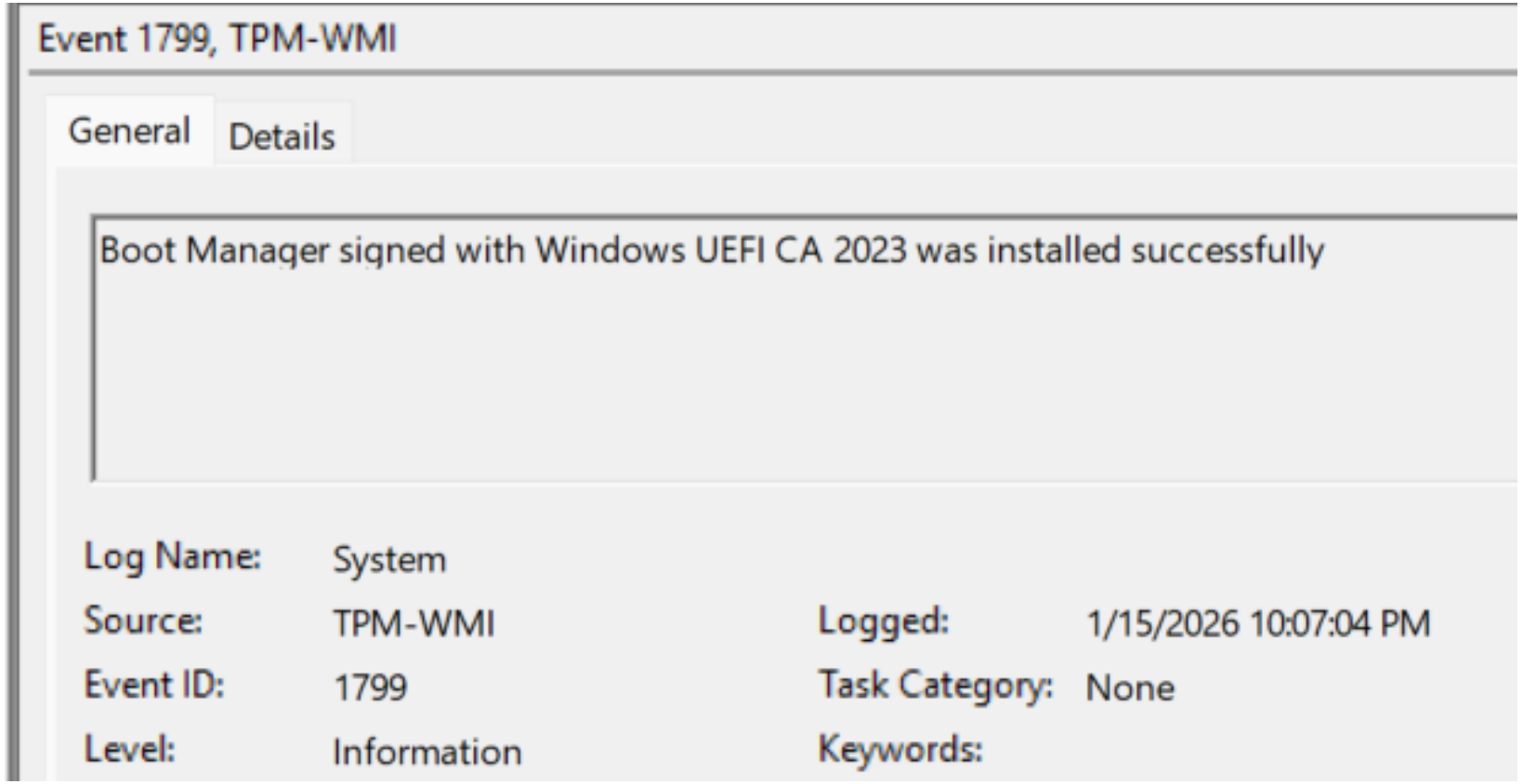
3) udělej si sám

```
Type            : DB
Description     : Signature Database
Index           : 5
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1454
Subject         : CN=Windows UEFI CA 2023, O=Microsoft Corporation, C=US
Issuer          : CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Thumbprint      : 45A0FA32604773C82433C3B7D59E7466B3AC0C67
Issued          : 6/13/2023 8:58:29 PM
Expires         : 6/13/2035 9:08:29 PM
SerialNumber    : 330000001A888B9800562284C100000000001A
ParseError      :
RawData         : {48, 130, 5, 170...}

Type            : DB
Description     : Signature Database
Index           : 6
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1459
Subject         : CN=Microsoft Option ROM UEFI CA 2023, O=Microsoft Corporation, C=US
Issuer          : CN=Microsoft RSA Devices Root CA 2021, O=Microsoft Corporation, C=US
Thumbprint      : 3FB39E2B8BD183BF9E4594E72183CA60AFCD4277
Issued          : 10/26/2023 9:02:20 PM
Expires         : 10/26/2038 9:12:20 PM
SerialNumber    : 3300000017B3EC4D8F01E27005000000000017
ParseError      :
RawData         : {48, 130, 5, 175...}

Type            : DB
Description     : Signature Database
Index           : 7
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1448
Subject         : CN=Microsoft UEFI CA 2023, O=Microsoft Corporation, C=US
Issuer          : CN=Microsoft RSA Devices Root CA 2021, O=Microsoft Corporation, C=US
Thumbprint      : B5EEB4A6706048073F0ED296E7F580A790B59EAA
Issued          : 6/13/2023 9:21:47 PM
Expires         : 6/13/2038 9:31:47 PM
SerialNumber    : 3300000001636BF36899F1575CC000000000016
ParseError      :
RawData         : {48, 130, 5, 164...}
```

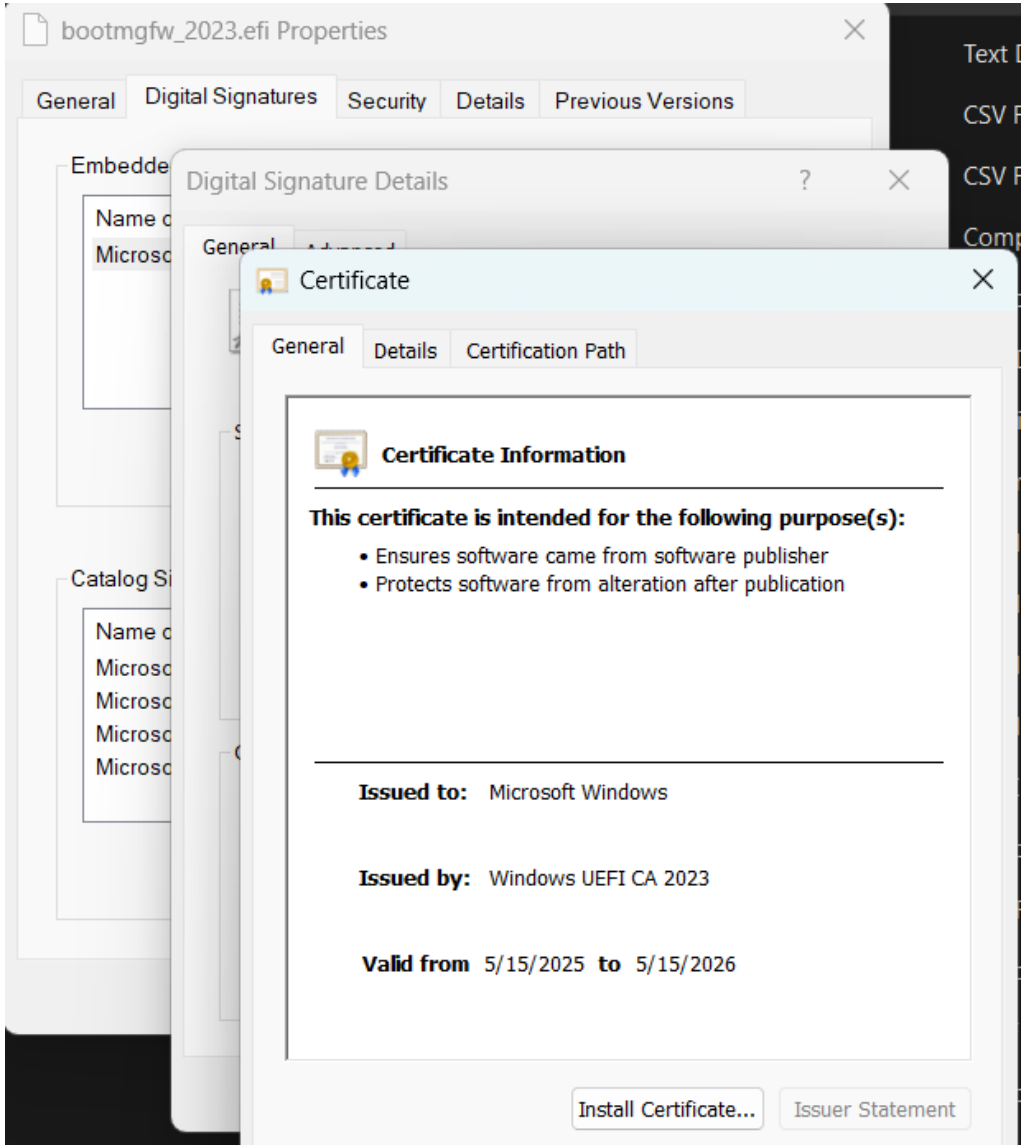
3) udělej si sám

1) reg add HKLM\SYSTEM\CurrentControlSet\Control\SecureBoot /t REG_DWORD /v AvailableUpdates /d 0x5944 /f
2) schtasks /run /tn "Secure-Boot-Update"
   - 0x5944 -> 0x4100
3) shutdown /r /t 0
4) schtasks /run /tn "Secure-Boot-Update"

3) udělej si sám



3) udělej si sám



3) udělej si sám

Name	Type	Data
(Default)	REG_SZ	(value not set)
BucketHash	REG_SZ	a6fc8dc52656bdd6cb911c4bd8f848771b172b7d0ba5d8f33dcb3f06943c97ad
ConfidenceLevel	REG_SZ	
UEFICA2023Status	REG_SZ	Updated
WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

3) udělej si sám

1) reg add HKLM\SYSTEM\CurrentControlSet\Control\SecureBoot /t REG_DWORD /v AvailableUpdates /d 0x5944 /f
2) schtasks /run /tn "Secure-Boot-Update"
   - 0x5944 -> 0x4100
3) shutdown /r /t 0
4) schtasks /run /tn "Secure-Boot-Update"
   - 0x4100 -> 0x4000
5) party

3) udělej si sám - device mgmt nástroje

- GPO: Computer Configuration->Administrative Templates->Windows Components->Secure Boot
- Secure Boot CLI: WinCsFlags.exe (/query | /apply)
- Intune: settings catalog "Secure Boot"
  - 0x82B00006 rejected by licensing
    - Pro (včetně Pro ->Enterprise)

3) udělej si sám - device mgmt nástroje

- GPO: Computer C[illegible] A[illegible] Templates->Windows Com
- Secure Boot CLI:
- Intune: settings
  - 0x82B00006
    - Pro (včetně

Known Issues

Microsoft Intune Error Code 65000 on Pro editions of Windows

Symptoms

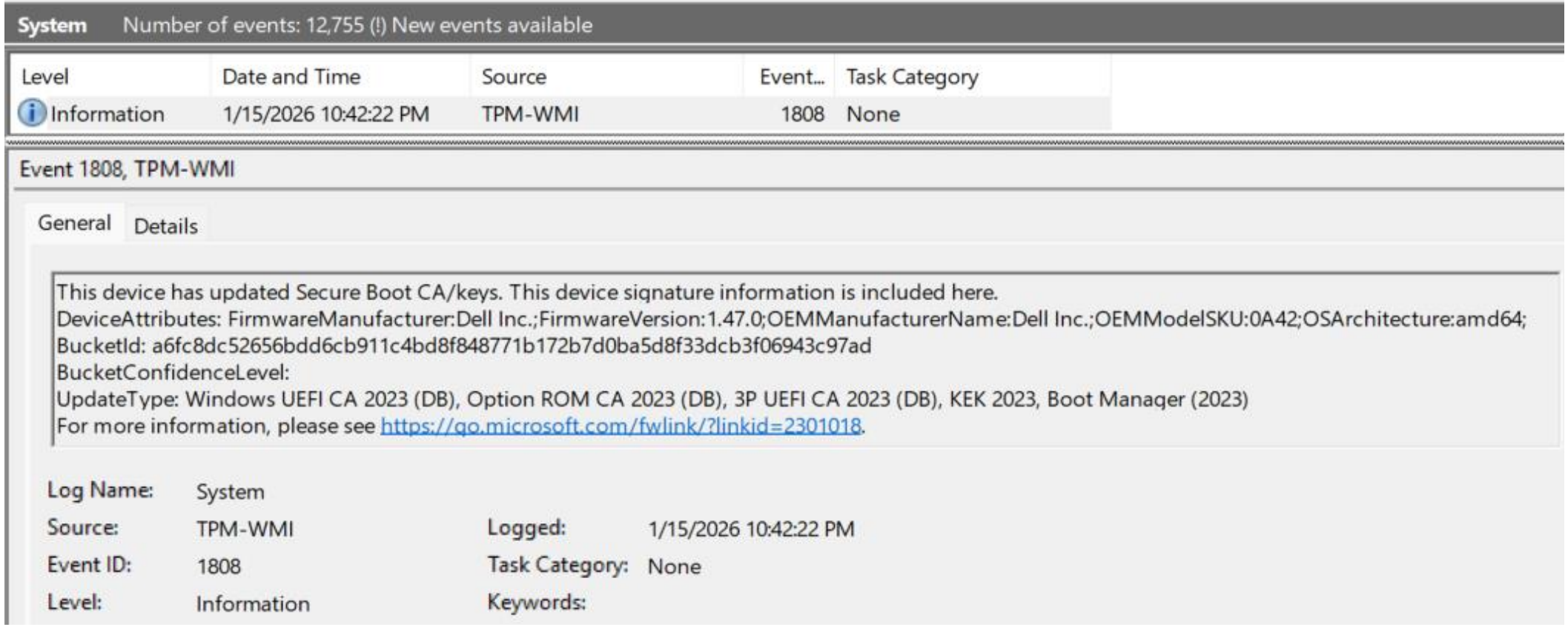
Secure Boot configuration settings deployed through Microsoft Intune Mobile Device Management (MDM) are currently blocked on Pro editions of Windows 10 and Windows 11.

- Attempts to apply these policies result in Microsoft Intune Error Code 65000.
- Event logs might record POLICYMANAGER_E_AREAPOLICY_NOTAPPLICABLEINEDITION, indicating the feature is unavailable on this edition.

Workaround

The issue is under investigation, and additional information will be shared as soon as it becomes available.

3) udělej si sám



- hurá, jdeme domů

A co když …?

- Reinstaluju OS
- Resetuju UEFI
- Vypnu a zapnu Secure Boot

A co když …?

- Reinstaluju OS
  - OK. V UEFI mám staré i nové certifikáty.

A co k

- Reinsta
  - OK. V

```
Type            : DB
Description     : Signature Database
Index           : 4
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1556
Subject         : CN=Microsoft Corporation UEFI CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Issuer          : CN=Microsoft Corporation Third Party Marketplace Root, O=Microsoft Corporation, L=Redmond,
                  S=Washington, C=US
Thumbprint      : 46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3
Issued          : 6/27/2011 11:22:45 PM
Expires         : 6/27/2026 11:32:45 PM
SerialNumber    : 6108D3C4000000000004
ParseError      :
RawData         : {48, 130, 6, 16...}

Type            : DB
Description     : Signature Database
Index           : 5
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1454
Subject         : CN=Windows UEFI CA 2023, O=Microsoft Corporation, C=US
Issuer          : CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Thumbprint      : 45A0FA32604773C82433C3B7D59E7466B3AC0C67
Issued          : 6/13/2023 8:58:29 PM
Expires         : 6/13/2035 9:08:29 PM
SerialNumber    : 330000001A888B9800562284C100000000001A
ParseError      :
RawData         : {48, 130, 5, 170...}

Type            : DB
Description     : Signature Database
Index           : 6
SignatureType   : a5c059a1-94e4-4aa7-87b5-ab155c2bf072
OwnerGuid       : 77fa9abd-0359-4d32-bd60-28f4e78f784b
CertificateSize : 1459
Subject         : CN=Microsoft Option ROM UEFI CA 2023, O=Microsoft Corporation, C=US
Issuer          : CN=Microsoft RSA Devices Root CA 2021, O=Microsoft Corporation, C=US
Thumbprint      : 3FB39E2B8BD183BF9E4594E72183CA60AFCD4277
Issued          : 10/26/2023 9:02:20 PM
Expires         : 10/26/2038 9:12:20 PM
SerialNumber    : 3300000017B3EC4D8F01E27005000000000017
ParseError      :
RawData         : {48, 130, 5, 175...}
```

A co když …?

- Resetuju UEFI/vypnu a zapnu Secure Boot
  - Problém. OEM specific
  - Paralelní _default proměnné (např. DB_default)
    - UEFI managed (OS do nich nesahá, narozdíl od těch „aktiviních“)
    - MS detekuje stav a pokud chybí 2023 cert, do boot order přidává recovery bootloader SecureBootRecovery.efi
      - Automaticky při failu bootmgfw.efi aplikuje "Windows UEFI CA 2023" do DB

Bonus

- BlackLotus bootkit
  - chyba v bootloaderech (Windows Boot Manager) -> bypass Secure Boot
  - CVE-2022-21894, CVE-2023-24932, částečný fix 01/2022
  - zneužití skrze downgrade
    - **dbx** nemá kapacitu na hash revokaci
    - update na 2023 cert
    - revokace "Microsoft Windows Production PCA 2011" (**dbx**)
    - zavedení Secure Version Number pro WBM a zápis do UEFI
    - "AvailableUpdates"+"Secure-Boot-Update"+reboot
    - přestane fungovat cokoli, co neumí 2023
      - bootovací media (PXE boot, ISO, USB, ...)

```
$DBXSVN=([Regex]::Matches((((Get-SecureBootUEFI dbx).Bytes |% {'{0:x2}' -f $_}) -join
''),'01612b139dd5598843ab1c185c3cb2eb92.....')).Value | sort | select -last 1; if ($DBXSVN.Count) { 'SVN {0}.{1}' -f
[int]::Parse($DBXSVN.Substring(36,4),[System.Globalization.NumberStyles]::HexNumber),
[int]::Parse($DBXSVN.Substring(40,4),[System.Globalization.NumberStyles]::HexNumber) } else { 'No SVN.' }
```

Závěr

- Můžu nic nedělat a (asi) dobře to dopadne
- Měl bych mít přehled, jak to u nás MS jde
- V senzitivním prostředí chci nasazení řídit
- Když už to mám v ruce, můžu zkusit mitigaci BlackLotus

Q&A

Zdroje

- https://techcommunity.microsoft.com/blog/windows-itpro-blog/secure-boot-playbook-for-certificates-expiring-in-2026/4469235
- https://support.microsoft.com/en-us/topic/secure-boot-certificate-updates-guidance-for-it-professionals-and-organizations-e2b43f9f-b424-42df-bc6a-8476db65ab2f
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21265
- https://support.microsoft.com/en-us/topic/enterprise-deployment-guidance-for-cve-2023-24932-88b8f034-20b7-4a45-80cb-c6049b0f9967#id0ebbf=overview
- https://github.com/microsoft/secureboot_objects
- https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/
- https://www.linkedin.com/pulse/understanding-uefi-secure-boot-how-helps-windows-10-process-basu-roy
- https://uefi.org/sites/default/files/resources/Evolving%20the%20Secure%20Boot%20Ecosystem_Flick%20and%20Sutherland.pdf
- https://medium.com/@sekyourityblog/secure-boot-explained-every-system-boot-is-a-negotiation-of-trust-be32fb023439
- https://media.defense.gov/2023/Jun/22/2003245723/-1/-1/0/CSI_BlackLotus_Mitigation_Guide.PDF
- https://uefi.org/sites/default/files/resources/UEFI-Plugfest-WindowsBootEnvironment.pdf
- https://patchmypc.com/blog/intune-policy-rejected-by-licensing