Secure Boot: wymiana certyfikatów 2011 → 2023

Typ: procedura

Dotyczy: Windows 11 23H2–26H1, Windows 10 22H2, Windows Server; sprzęt UEFI z Secure Boot, maszyny Hyper-V

Czas: ~30 min pracy na maszynę pilotażową plus do 48 godzin i co najmniej jeden restart

Efekt: maszyny mają w firmware nowe urzędy z 2023 roku (KEK, Windows UEFI CA 2023, Microsoft UEFI CA 2023 i Option ROM UEFI CA 2023) i uruchamiają się przez boot manager podpisany Windows UEFI CA 2023; w rejestrze `UEFICA2023Status` = `Updated`, w dzienniku System zdarzenie 1808. Nośniki serwisowe są odtworzone, a odwołanie starego urzędu PCA 2011 w DBX jest świadomie zaplanowane, nie przypadkowe.

Skróty użyte na tej stronie (28)

Skrót	Co znaczy
AD	Active Directory: katalog kont, komputerów i zasad w domenie Windows
ADMX	szablony administracyjne zasad grupy w formacie XML
AVD	Azure Virtual Desktop: pulpity i aplikacje Windows uruchamiane w chmurze Azure
BIOS	Basic Input/Output System: oprogramowanie płyty głównej; potocznie także firmware UEFI
CA	Certificate Authority: urząd certyfikacji, który podpisuje inne certyfikaty
CFR	Controlled Feature Rollout: stopniowe włączanie funkcji partiami urządzeń
CSV	Comma-Separated Values: tabela w pliku tekstowym, kolumny rozdzielone przecinkami
DB	baza sygnatur dozwolonych w Secure Boot (zmienna UEFI db)
DBX	baza sygnatur zakazanych w Secure Boot, czyli lista odwołań (zmienna UEFI dbx)
EFI	Extensible Firmware Interface: poprzednik nazwy UEFI; partycja EFI trzyma programy rozruchowe
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
KB	Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008)
KEK	Key Exchange Key: klucz UEFI autoryzujący zmiany baz DB i DBX
MDM	Mobile Device Management: zdalne zarządzanie urządzeniami, np. przez Intune

Skrót	Co znaczy
MDT	Microsoft Deployment Toolkit: darmowe narzędzie do wdrażania obrazów Windows
OEM	Original Equipment Manufacturer: producent sprzętu
PC	Personal Computer: komputer osobisty
PCA	Production Certificate Authority: urząd podpisujący produkcyjne pliki rozruchowe Windows
PK	Platform Key: główny klucz Secure Boot, należący do producenta sprzętu
PXE	Preboot Execution Environment: rozruch komputera z sieci
ROM	Read-Only Memory: pamięć stała; Option ROM to firmware karty rozszerzeń
SCCM	System Center Configuration Manager: dziś Configuration Manager, lokalne zarządzanie flotą
SVN	Security Version Number: numer wersji bezpieczeństwa blokujący powrót do starszych plików
UEFI	Unified Extensible Firmware Interface: współczesny firmware płyty głównej
WDS	Windows Deployment Services: rola serwera do instalacji Windows przez sieć
WinCS	mechanizm konfiguracji Windows, który Microsoft wymienia obok rejestru, GPO i Intune jako ścieżkę IT-managed
WinPE	Windows Preinstallation Environment: minimalny Windows do instalacji i napraw
WinRM	Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting

Fiszka

□□ TYLKO ODCZYT

Czy Secure Boot jest w ogóle włączony: Confirm-SecureBootUEFI

```
Confirm-SecureBootUEFI
```

`True` — Secure Boot działa i wymiana certyfikatów ma sens. `False` — Secure Boot jest wyłączony w firmware: wtedy w rejestrze nie ma wartości serwisowych, w dzienniku nie ma zdarzeń, a aktualizacja się po prostu nie zaczyna. Błąd zamiast wyniku oznacza zwykle maszynę uruchomioną w trybie zgodności BIOS albo sesję bez uprawnień administratora.

□□ **BIOS** = Basic Input/Output System: oprogramowanie płyty głównej; potocznie także firmware UEFI

□□ TYLKO ODCZYT

Stan wymiany certyfikatów w rejestrze

```
# polecenie pomocnicze; nazwy wartości z dokumentacji Microsoftu
$sb  = 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot'
$srv = Get-ItemProperty "$sb\Servicing" -ErrorAction SilentlyContinue
[pscustomobject]@{
    AvailableUpdates     = '0x{0:X}' -f [int](Get-ItemProperty $sb -ErrorAction
SilentlyContinue).AvailableUpdates
    UEFICA2023Status     = $srv.UEFICA2023Status
    UEFICA2023Error      = $srv.UEFICA2023Error
    UEFICA2023ErrorEvent = $srv.UEFICA2023ErrorEvent
}
```

`AvailableUpdates` to maska bitowa zleceń: `0x5944` — „wdroż wszystkie potrzebne certyfikaty i przejdź na boot manager podpisany PCA2023”, po pierwszym przebiegu zadania wartość spada do `0x4100` (czas na ręczny restart), a po restarcie i ponownym przebiegu — do `0x4000`, na której procedura testowa Microsoftu się kończy; `0` — nic nie zlecono. O zakończeniu wymiany rozstrzyga `UEFICA2023Status` = `Updated` i zdarzenie 1808, a nie spadek `AvailableUpdates` do zera. `UEFICA2023Status` przyjmuje wartości `NotStarted`, `InProgress` i `Updated`; `UEFICA2023Error` równe 0 oznacza sukces, a `UEFICA2023ErrorEvent` podaje numer zdarzenia błędu, które trzeba sprawdzić w tabeli na końcu strony.

Wartości `AvailableUpdatesPolicy`, `WindowsUEFICA2023Capable`, `BucketHash` i `ConfidenceLevel` tylko odczytujemy — Microsoft zastrzega, żeby ich nie zmieniać.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
AvailableUpdates     : 0x0
UEFICA2023Status     : Updated
UEFICA2023Error      : 0
UEFICA2023ErrorEvent :
```

TYLKO ODCZYT

Zdarzenia Secure Boot w dzienniku System (źródło TPM-WMI)

```
# polecenie pomocnicze; numery zdarzeń z dokumentacji Microsoftu
$id =
1032,1033,1034,1036,1037,1043,1044,1045,1795,1796,1797,1798,1799,1800,1801,1802,1803,180
8
Get-WinEvent -FilterHashtable @{ LogName = 'System'; ProviderName = '*TPM-WMI*'; Id =
```

```
$id } -MaxEvents 200 -ErrorAction SilentlyContinue |
    Select-Object TimeCreated, Id, LevelDisplayName, Message |
    Format-Table -Wrap
```

Filtrujemy po nazwie źródła zawierającej `TPM-WMI`, bo te same numery zdarzeń mogą w dzienniku System należeć do innych źródeł — i robimy to w samym zapytaniu (`ProviderName` w `-FilterHashtable` przyjmuje symbole wieloznaczne), żeby limit `-MaxEvents` liczył wyłącznie zdarzenia tego źródła. Stan docelowy to **1808** (informacja: urządzenie ma nowe urzędy i klucze w firmware). **1801** (błąd) — certyfikaty zaktualizowane, ale jeszcze niezastosowane w firmware. **1803** — brak KEK podpisanego kluczem PK producenta; tego nie naprawimy sami. Pełne znaczenie numerów jest w tabeli poniżej.

KEK = Key Exchange Key: klucz UEFI autoryzujący zmiany baz DB i DBX · **PK** = Platform Key: główny klucz Secure Boot, należący do producenta sprzętu

Zdarzenie	Znaczenie
1808 (informacja)	urządzenie ma nowe urzędy i klucze w firmware — stan docelowy
1801 (błąd)	certyfikaty zaktualizowane, ale jeszcze niezastosowane w firmware
1799	zainstalowano boot manager podpisany Windows UEFI CA 2023
1043 / 1045 / 1044	KEK zaktualizowany / UEFI CA 2023 w DB / Option ROM UEFI CA 2023 w DB
1036 / 1034 / 1037	aktualizacja DB / aktualizacja DBX / PCA 2011 dodany do DBX
1795 / 1796	firmware zwrócił błąd przy zapisie zmiennej / błąd, ponowienie przy restarcie
1797 / 1798	brak CA 2023 w DB / boot manager niepodpisany nowym urzędem — DBX zablokowany
1800	wymagany restart
1802	zablokowane przez znany błąd firmware — sprawdzić u producenta
1803	**brak KEK podpisanego kluczem PK producenta**
1032	konfiguracja BitLockera spowodowałaby odzyskiwanie
1033	wykryto potencjalnie odwołany boot manager na partycji EFI

TYLKO ODCZYT

Zawartość bazy DB: Get-SecureBootUEFI

```
# parametr -Decoded: aktualizacje zbiorcze z 14 IV 2026 i nowsze
Get-SecureBootUEFI -Name db -Decoded
```

```
# jednowierszowiec z poradników, nie z dokumentacji Microsoftu
[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows
UEFI CA 2023'
```

Parametr `-Decoded` dodano do `Get-SecureBootUEFI` w aktualizacjach zbiorczych z 14 kwietnia 2026 i późniejszych — tak podaje osobna strona pomocy Microsoftu z kwietnia 2026; referencja cmdletu na Microsoft Learn jeszcze go nie wymienia (udokumentowane są tam tylko `-Name` i `-OutputFilePath`). Zwraca certyfikaty z bazy w postaci czytelnej (Subject, Algorithm, ValidFrom, ValidTo), zamiast surowych bajtów. Na maszynie bez tej aktualizacji polecenie kończy się błędem nieznanego parametru — wtedy używamy drugiego polecenia: jednowierszowca z poradników, który nie jest przepisem Microsoftu, ale opiera się na udokumentowanej właściwości `Bytes` wyniku `Get-SecureBootUEFI`.

DB = baza sygnatur dozwolonych w Secure Boot (zmienna UEFI db)

TYLKO ODCZYT

Klucze odzyskiwania BitLocker przed pierwszym restartem

```
# polecenie pomocnicze
Get-BitLockerVolume -MountPoint 'C:' | Select-Object MountPoint, VolumeStatus,
ProtectionStatus
(Get-BitLockerVolume -MountPoint 'C:').KeyProtector |
    Where-Object KeyProtectorType -eq 'RecoveryPassword' |
    Select-Object KeyProtectorId, KeyProtectorType
```

Po pierwszym rozruchu z nowym boot managerem BitLocker potrafi jednorazowo zażądać klucza odzyskiwania. Samego hasła odzyskiwania nie wypisujemy na ekran ani do pliku — do porównania z kopią w katalogu wystarcza `KeyProtectorId`. Zanim cokolwiek zmienimy, sprawdzamy, że klucz dla każdej maszyny pilotażowej jest w AD albo w Entra ID i że potrafimy go stamtąd wyciągnąć — skrypt pobierający klucz z AD jest na stronie Skrypty audytowe Active Directory.

AD = Active Directory: katalog kont, komputerów i zasad w domenie Windows

Co wygasa i co z tego wynika

Wygasający certyfikat	Data wygaśnięcia	Gdzie leży i co podpisuje	Następca (2023)
Microsoft Corporation **KEK CA 2011**	**24 VI 2026**	KEK — autoryzuje zmiany w bazach DB i DBX	Microsoft Corporation KEK 2K CA 2023
Microsoft **UEFI CA 2011** („third-party”)	**27 VI 2026**	DB — programy ładujące firm trzecich, w tym shim Linuksa, aplikacje EFI, Option ROM-y	Microsoft UEFI CA 2023 oraz Microsoft Option ROM UEFI CA 2023
Microsoft **Windows Production PCA 2011**	**19 X 2026**	DB — Windows Boot Manager	Windows UEFI CA 2023

Maszyna, która dojdzie do daty wygaśnięcia bez nowych certyfikatów, **nadal się uruchomi i będzie działać normalnie**, a zwykłe aktualizacje Windows nadal się zainstalują — tak pisze Microsoft. Przestaje działać coś innego: nie da się zastosować nowych zabezpieczeń Secure Boot i boot managera, poprawek luk wczesnego rozruchu, mitygacji obejść BitLockera ani aktualizacji listy odwołań DBX. Rozruch zostaje zamrożony w stanie bezpieczeństwa z 2026 roku. Ryzyko „nie wstaje” tkwi w samej wymianie — w wadliwym firmware, w BitLockerze i w starych nośnikach po odwołaniu PCA 2011 — i dlatego wymianę robimy procedurą, a nie jednym kliknięciem na całą flotę.

> **Pojęcie: mitygacja BlackLotus (KB5025885).** BlackLotus (CVE-2023-24932) to bootkit UEFI obchodzący Secure Boot. Mitygacja Microsoftu ma trzy kroki: dodać Windows UEFI CA 2023 do DB, zainstalować boot manager podpisany nowym urzędem, wpisać Windows Production PCA 2011 do DBX — czyli odwołać zaufanie do wszystkich starych boot managerów; opcjonalnie podbić SVN w firmware. Fazy: 9 V 2023 (początkowa, ręczna), 11 VII 2023 (druga), 9 IV 2024 (ewaluacja), 9 VII 2024 (wdrożenie), faza egzekwowania — „nie wcześniej niż w styczniu 2026, z co najmniej sześciomiesięcznym wyprzedzeniem”. Wymiana certyfikatów z lat 2025–2026 i domknięcie BlackLotusa to ta sama operacja: wygaśnięcie tylko wyznaczyło twardy termin.

Chronologia wdrożenia po stronie Microsoftu, przydatna przy czytaniu starszych poradników:

Data	Co udostępniono
11 XI 2025	klucze rejestru we wspieranych wersjach Windows
13 XI 2025	playbook wdrożenia
13 I 2026	styczniowe aktualizacje zbiorcze z „pierwszą porcją urządzeń High Confidence”
10 II 2026	kolejne urządzenia High Confidence
18 II 2026	wytyczne dla Intune i pulpit monitorowania

Data	Co udostępniono
23 II 2026	playbooki serwerowe
16 III 2026	przewodnik automatyzacji w PowerShell
19 III 2026	przewodnik rozwiązywania problemów
2 IV 2026	dokumentacja statusu w aplikacji Zabezpieczenia Windows
19 V 2026	raportowanie w Autopatch
8 IX 2026	KB5124008 — więcej danych kierowania o wysokiej pewności, więcej urządzeń kwalifikujących się do automatu

Zanim zaczniemy

Wybieramy ścieżkę. **„Microsoft-managed”** dotyczy urządzeń domowych i niezarządzanych: certyfikaty przychodzą przez Windows Update, stopniowo, według bazy High Confidence — od stycznia 2026 aktualizacje zbiorcze niosą kolejne porcje urządzeń, a wrześniowa KB5124008 zwiększyła ich liczbę. **„IT-managed”** to rejestr, GPO, Intune albo WinCS — i to jest ścieżka dla floty w domenie, bo to my decydujemy, która maszyna i kiedy.

Wydzielamy grupę pilotażową: **co najmniej 4 urządzenia na każdą unikalną kombinację producenta, modelu i wersji BIOS** — tyle zaleca Microsoft, zastrzegając, że większość firmware wyprodukowanego od 2012 roku powinna działać poprawnie, ale „konieczne jest staranne testowanie przed wdrożeniem”. Inwentaryzację modeli i wersji BIOS robimy z pierwszego kroku przebiegu.

Aktualizujemy BIOS/UEFI do bieżącej wersji od producenta — Microsoft utrzymuje listę stron producentów o Secure Boot. Jeśli instrukcja producenta każe na czas aktualizacji firmware wstrzymać BitLockera, robimy to zgodnie z nią (`Suspend-BitLocker -MountPoint 'C:' -RebootCount 1` — polecenie pomocnicze, nie z dokumentacji Secure Boot).

Mamy **klucze odzyskiwania BitLocker** każdej maszyny pilotażowej — w AD albo w Entra ID, sprawdzone, a nie założone. W kolejności rozruchu ustawiamy **dysk przed PXE** albo wyłączamy PXE: przy PXE przed dyskiem BitLocker mierzy w jednym cyklu dwa różne urzędy i prosi o klucz przy każdym rozruchu.

Hosty i goście Hyper-V muszą mieć aktualizacje co najmniej z **10 marca 2026** (Windows Server 2025 — z 14 kwietnia 2026), inaczej aktualizacja KEK w maszynach wirtualnych kończy się błędem „The media is write protected” i zdarzeniem 1795. Na hostach linuksowych z Secure Boot obowiązuje reguła Microsoftu: **najpierw zmienne UEFI Secure Boot, potem shim lub program ładujący**; wytyczne opublikowały m.in. AlmaLinux, Debian, Red Hat, SUSE, Ubuntu i Azure Linux.

Rezerwujemy czas: Microsoft każe przewidzieć **48 godzin i jeden lub więcej restartów** na zastosowanie certyfikatów. Samo zainicjowanie nie restartuje maszyny.

Przebieg

1. Inwentaryzacja floty

🔒 TYLKO ODCZYT

Stan Secure Boot na wielu maszynach naraz: Invoke-Command

```
# polecenie pomocnicze; nazwy wartości i numery zdarzeń z dokumentacji Microsoftu
$komputery = Get-Content .\komputery.txt
Invoke-Command -ComputerName $komputery -ScriptBlock {
    $sb  = 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot'
    $srv = Get-ItemProperty "$sb\Servicing" -ErrorAction SilentlyContinue
    $zd  = Get-WinEvent -FilterHashtable @{ LogName = 'System'; ProviderName = '*TPM-WMI*'; Id = 1808,1801,1803,1802,1795,1796,1032 } `
               -MaxEvents 50 -ErrorAction SilentlyContinue
    $bios = Get-CimInstance Win32_BIOS
    $cs   = Get-CimInstance Win32_ComputerSystem
    [pscustomobject]@{
        Producent        = $cs.Manufacturer
        Model            = $cs.Model
        BIOS             = $bios.SMBIOSBIOSVersion
        SecureBoot       = try { Confirm-SecureBootUEFI } catch { $null }
        AvailableUpdates = '0x{0:X}' -f [int](Get-ItemProperty $sb -ErrorAction SilentlyContinue).AvailableUpdates
        Status           = $srv.UEFICA2023Status
        Blad             = $srv.UEFICA2023Error
        Zdarzenia        = ($zd | Select-Object -ExpandProperty Id -Unique) -join ','
    }
} -Credential (Get-Credential) |
    Select-Object PSComputerName, Producent, Model, BIOS, SecureBoot, AvailableUpdates, Status, Blad, Zdarzenia |
    Export-Csv .\secureboot-inwentaryzacja.csv -NoTypeInformation -Encoding UTF8
```

Wynik grupujemy po kolumnach `Producent`, `Model` i `BIOS` — z tych kombinacji wybieramy po cztery maszyny do pilotażu. Maszyny z `Status` = `Updated` i zdarzeniem 1808 pomijamy, bo dostały certyfikaty już przez Windows Update. Maszyny ze zdarzeniem 1803 odkładamy do

rozmowy z producentem, a z `SecureBoot` = `False` — do decyzji, czy Secure Boot ma zostać włączony w firmware. Wymaga działającego WinRM, patrz WinRM — zarządzanie zdalne. Microsoft opisał też gotowy skrypt monitorujący dla Intune Remediations — przy flocie w Intune warto go użyć zamiast własnego.

WinRM = Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting

2. Kopia zapasowa kluczy BitLocker

ZMIENIA SYSTEM

Zapis klucza odzyskiwania w AD albo w Entra ID

```
# polecenie pomocnicze
# -KeyProtectorId przyjmuje jeden identyfikator, więc przy kilku hasłach odzyskiwania
idziemy pętlą
$kp = (Get-BitLockerVolume -MountPoint 'C:').KeyProtector |
      Where-Object KeyProtectorType -eq 'RecoveryPassword'
# kopia do Active Directory (wymaga zasad pozwalających na zapis kluczy w AD)
foreach ($p in $kp) { Backup-BitLockerKeyProtector -MountPoint 'C:' -KeyProtectorId
$p.KeyProtectorId }
# albo kopia do Entra ID na urządzeniu przyłączonym do Entra
foreach ($p in $kp) { BackupToAAD-BitLockerKeyProtector -MountPoint 'C:' -KeyProtectorId
$p.KeyProtectorId }
```

Wykonujemy na każdej maszynie pilotażowej, na której w AD albo w Entra ID nie znaleźliśmy klucza. Polecenie niczego nie zmienia w samym szyfrowaniu, ale zapisuje dane w katalogu — dlatego pomarańczowa karta. Po zapisie sprawdzamy, że klucz da się odczytać z drugiej strony, zanim pójdziemy dalej.

AD = Active Directory: katalog kont, komputerów i zasad w domenie Windows

3. Pilotaż przez rejestr

OSTROŻNIE · NIEODWRACALNE

Zlecenie wymiany certyfikatów: AvailableUpdates = 0x5944

```
# 1. zlecenie: wdroż wszystkie potrzebne certyfikaty i przejdź na boot manager podpisany PCA2023
reg add HKLM\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x5944 /f

# 2. uruchomienie zadania od razu, zamiast czekać na jego cykl co 12 godzin
Start-ScheduledTask -TaskName "\Microsoft\Windows\PI\Secure-Boot-Update"

# 3. odczyt postępu (polecenie pomocnicze)
'0x{0:X}' -f (Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot).AvailableUpdates

# 4. gdy wynik to 0x4100: ręczny restart, a po nim ponownie krok 2
Restart-Computer

# 5. po ponownym kroku 2 oczekiwane 0x4000; zakończenie potwierdza UEFICA2023Status = Updated i zdarzenie 1808
```

Procedura testowa Microsoftu dla jednej maszyny. Karta jest czerwona, bo po przetworzeniu zlecenia nowe urzędy zostają zapisane w firmware, a z poziomu Windows nie ma wspieranej drogi wstecz (sekcja *Wycofanie zmian*) — dlatego wyłącznie na maszynach z grupy pilotażowej, z kluczem BitLockera sprawdzonym w katalogu. Zadanie `\Microsoft\Windows\PI\Secure-Boot-Update` obsługuje całą wymianę i samo uruchamia się co 12 godzin — ręczny start tylko przyspiesza. Samo zainicjowanie nie restartuje maszyny: restart robimy my, dopiero gdy `AvailableUpdates` pokaże `0x4100`, i po restarcie uruchamiamy zadanie jeszcze raz. Między krokami sprawdzamy dziennik zdarzeń z karty w Fiszce — zdarzenie 1800 znaczy „wymagany restart”, 1032 — że konfiguracja BitLockera spowodowałaby odzyskiwanie, więc zatrzymujemy się i wracamy do kroku 2.

Przykład (kolejne odczyty według procedury testowej Microsoftu):

```
0x5944   ← zaraz po reg add
0x4100   ← po zadaniu: czas na ręczny restart
0x4000   ← po restarcie i ponownym zadaniu: koniec procedury testowej
```

Pilotaż trwa, dopóki każda kombinacja producent/model/BIOS nie przejdzie co najmniej dwóch zwykłych restartów bez próśb BitLockera i z zdarzeniem 1808 w dzienniku. Dopiero wtedy przechodzimy na flotę.

4. Wdrożenie na flotę: GPO albo Intune

Na flotę nie wpisujemy rejestru ręcznie, tylko używamy polityk, które na niego się mapują:

Narzędzie	Ustawienie	Co robi
GPO (ADMX „Windows 11 2025 Update (25H2) v2.0” z 27 X 2025): Konfiguracja komputera → Szablony administracyjne → Składniki systemu Windows → Secure Boot	„Enable Secure Boot Certificate Deployment”	zleca wdrożenie certyfikatów na maszynach objętych GPO
jw.	ustawienie automatycznego wdrażania przez aktualizacje	jego **włączenie blokuje** automat Microsoftu — dla maszyn, które chcemy prowadzić wyłącznie sami
jw.	udział w Controlled Feature Rollout	zgoda na wdrożenie stopniowe przez Microsoft
Intune, Settings Catalog	„Enable Secureboot Certificate Updates”	mapowane na `AvailableUpdates`
Intune, Settings Catalog	„Configure High Confidence Opt-Out”	mapowane na `HighConfidenceOptOut`: 1 — rezygnacja z automatycznego wdrożenia dla urządzeń „wysokiej pewności”, domyślnie 0 (udział)
Intune, Settings Catalog	„Configure Microsoft Update Managed Opt In”	mapowane na `MicrosoftUpdateManagedOptIn`: 1 — zgoda na wdrożenie zarządzane przez Microsoft w ramach CFR, domyślnie 0

Wdrażamy falami, w kolejności wyznaczonej przez pilotaż: najpierw kombinacje sprzętowe, które przeszły bez uwag, potem reszta. Maszyny ze zdarzeniem 1803 albo 1802 wykluczamy z fali, a jeśli ma je objąć także automat Microsoftu — ustawiamy dla nich opt-out wysokiej pewności. Do monitorowania floty w Intune służy skrypt Microsoftu w Intune Remediations, a od 19 maja 2026 także raportowanie w Autopatch.

◫◫ ZMIENIA SYSTEM

Edycja Pro i błąd 65000 w Intune: odświeżenie licencji

```
ClipDLS.exe removesubscription
ClipRenew.exe
```

Na Windows 11 Pro polityki Secure Boot z Intune były blokowane błędem **65000** — przez usługę licencyjną, nie przez Secure Boot. Poprawkę usługi wydano 27 stycznia 2026; licencje odnawiają się co miesiąc, więc usterka miała sama zniknąć do 27 lutego 2026. Jeśli na jakiejś maszynie Pro błąd wciąż się pojawia, ręcznie usuwamy subskrypcję i odświeżamy licencję powyższymi poleceniami, a potem wymuszamy synchronizację z Intune.

5. Hyper-V i maszyny wirtualne

TYLKO ODCZYT

Ostatnie aktualizacje na hoście i w gościu: Get-HotFix

```
# polecenie pomocnicze
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 5 HotFixID,
InstalledOn
```

Uruchamiamy na hoście Hyper-V i w każdym gościu z Secure Boot. Poprawka błędu zapisu KEK w wirtualnym firmware wymaga aktualizacji co najmniej z 10 marca 2026 (Windows Server 2025 — z 14 kwietnia 2026) **po obu stronach**; sama aktualizacja gościa nie wystarczy. Maszyny Trusted Launch w Azure, w tym Cloud PC i AVD, mają własny znany problem ze zdarzeniem 1795 — według Microsoftu bez potrzeby natychmiastowej akcji klienta; Cloud PC opisuje osobna strona Microsoftu o Windows 365.

AVD = Azure Virtual Desktop: pulpity i aplikacje Windows uruchamiane w chmurze Azure · **KEK** = Key Exchange Key: klucz UEFI autoryzujący zmiany baz DB i DBX · **PC** = Personal Computer: komputer osobisty

6. Nośniki serwisowe

Po przejściu maszyn na boot manager podpisany Windows UEFI CA 2023 odtwarzamy nośniki startowe: WinPE w SCCM albo MDT, pendrive'y instalacyjne i serwisowe, obrazy WDS i PXE. Nowy nośnik testujemy na maszynie, która ma już zdarzenie 1799, **zanim** ktokolwiek odwoła PCA 2011 w DBX — po odwołaniu stare nośniki odzyskiwania i instalacyjne przestają się uruchamiać.

7. Odwołanie PCA 2011 w DBX

OSTROŻNIE · NIEODWRACALNE

Warunki wstępne przed wpisaniem Windows Production PCA 2011 do DBX

```
# polecenie pomocnicze; numery zdarzeń z dokumentacji Microsoftu
$srv = Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing'
# ProviderName w zapytaniu, a nie w Where-Object: przy -MaxEvents 1 filtr po fakcie
```

```
mógłby zgubić zdarzenie 1033
$bm2023 = Get-WinEvent -FilterHashtable @{ LogName = 'System'; ProviderName = '*TPM-
WMI*'; Id = 1799 } -MaxEvents 1 -ErrorAction SilentlyContinue
$stary  = Get-WinEvent -FilterHashtable @{ LogName = 'System'; ProviderName = '*TPM-
WMI*'; Id = 1033 } -MaxEvents 1 -ErrorAction SilentlyContinue
[pscustomobject]@{
    CertyfikatyZaktualizowane = ($srv.UEFICA2023Status -eq 'Updated' -and
$srv.UEFICA2023Error -eq 0)
    BootManager2023           = [bool]$bm2023
    OdwolanyBootManagerNaEFI  = [bool]$stary
}
# Samo odwołanie celowo nie jest tu wpisane: wartość zlecenia dla wpisu PCA 2011 do DBX
# bierzemy z KB5025885 w dniu wdrożenia, nie z pamięci ani z tej strony.
```

Trzeci krok mitygacji BlackLotus odwołuje zaufanie do wszystkich boot managerów podpisanych starym urzędem — **tego nie da się cofnąć z poziomu Windows**, a każdy stary nośnik, obraz PXE i pendrive serwisowy przestaje startować. Robimy go wyłącznie na maszynach, na których skrypt zwraca `True`, `True`, `False`, i wyłącznie po kroku 6. Po odwołaniu w dzienniku pojawia się zdarzenie **1037** (PCA 2011 dodany do DBX). Zdarzenia 1797 i 1798 znaczą, że DBX jest zablokowany, bo w DB brakuje urzędu z 2023 roku albo boot manager nie jest jeszcze podpisany nowym urzędem.

Faza egzekwowania, w której Microsoft sam wpisze PCA 2011 do DBX na wszystkich maszynach, ma nastąpić „nie wcześniej niż w styczniu 2026, z co najmniej sześciomiesięcznym wyprzedzeniem”. Czy jej data została już ogłoszona, nie ustaliłem — przed każdą falą sprawdzamy aktualną treść KB5025885.

DB = baza sygnatur dozwolonych w Secure Boot (zmienna UEFI db) · **DBX** = baza sygnatur zakazanych w Secure Boot, czyli lista odwołań (zmienna UEFI dbx) · **KB** = Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008) · **PCA** = Production Certificate Authority: urząd podpisujący produkcyjne pliki rozruchowe Windows · **PXE** = Preboot Execution Environment: rozruch komputera z sieci

Weryfikacja

Na każdej maszynie po wdrożeniu: `UEFICA2023Status` = `Updated`, `UEFICA2023Error` = 0, w dzienniku System zdarzenie **1808** ze źródła TPM-WMI i zdarzenie 1799 (boot manager podpisany Windows UEFI CA 2023). Dwa kolejne zwykłe restarty bez prośby BitLockera o klucz.

Aplikacja Zabezpieczenia Windows pokazuje status w Zabezpieczenia urządzenia → Secure Boot (zielony albo żółty znaczek) od 8 kwietnia 2026, a powiadomienia od 16 maja 2026 — na Windows

11 23H2–26H1. Na urządzeniach zarządzanych w przedsiębiorstwie i na Windows Server wskaźniki są **domyślnie wyłączone**; jeśli na jakiejś grupie maszyn ich nie chcemy, ukrywa je wartość `HideSecureBootStates` = 1 w `HKLM\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Device security`.

Na poziomie floty: ponowne uruchomienie skryptu z kroku 1 i porównanie CSV przed i po, albo raport z Intune Remediations i Autopatch.

Wycofanie zmian

Dopóki zadanie `Secure-Boot-Update` nie przetworzyło zlecenia, można przywrócić `AvailableUpdates` do `0` — wartości oznaczającej „nic nie zlecono”; **niepotwierdzone**: artykuł Microsoftu o kluczach rejestru nie opisuje tego jako sposobu anulowania, więc nie zakładamy, że zatrzyma to zadanie w połowie pracy. Po zapisaniu certyfikatów do firmware **nie ma wspieranej drogi wstecz z poziomu Windows**; nowe urzędy dopisane do DB i KEK zostają.

Maszyny, które nie powinny dostać wymiany automatycznie (znany problem firmware, czekamy na BIOS od producenta), wyłączamy z automatu ustawieniem „Configure High Confidence Opt-Out” albo odpowiednim ustawieniem GPO i nie obejmujemy ich falą.

Jedyny udokumentowany scenariusz, w którym maszyna po wymianie nie startuje, to firmware nadpisujący bazę DB zamiast do niej dopisywać — znikają certyfikaty z 2011 roku potrzebne obecnemu boot managerowi. Naprawa: reset kluczy Secure Boot do ustawień fabrycznych w firmware i poprawiony firmware od producenta. Odwołania PCA 2011 w DBX (krok 7) nie cofamy wcale — dlatego nośniki odtwarzamy przed nim.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
Zdarzenie **1803**	producent nie dostarczył KEK-a podpisanego kluczem platformy (PK) dla tego urządzenia	wspieranego obejścia nie ma — zgłoszenie do producenta; maszynę wykluczamy z fali
Zdarzenie 1802	znany błąd firmware blokuje aktualizację	strona producenta o Secure Boot, aktualizacja BIOS
Zdarzenia 1795 / 1796 na fizycznej maszynie	firmware zwrócił błąd przy zapisie zmiennej; 1796 — ponowienie przy restarcie	restart; jeśli błąd wraca — aktualizacja BIOS od producenta
1795 i „The media is write protected” w Hyper-V	wirtualny firmware nie przyjmował zapisu KEK	aktualizacje co najmniej z 10 III 2026 (Server 2025: 14 IV 2026) na hoście i w gościu

Objaw	Przyczyna	Naprawa
1795 na maszynie Trusted Launch (Azure, Cloud PC, AVD)	znany problem Microsoftu	według Microsoftu bez natychmiastowej akcji klienta
Długo utrzymuje się 1801, pojawia się 1800	certyfikaty zaktualizowane, ale jeszcze niezastosowane w firmware	ręczny restart i ponowne uruchomienie zadania
Zdarzenia 1797 / 1798	brak CA 2023 w DB albo boot manager niepodpisany nowym urzędem — DBX zablokowany	dokończyć krok 3 i sprawdzić zdarzenie 1799 przed krokiem 7
Zdarzenie 1032	konfiguracja BitLockera spowodowałaby odzyskiwanie	wstrzymać fale, sprawdzić klucze i kolejność rozruchu
BitLocker jednorazowo prosi o klucz po pierwszym rozruchu	firmware z opóźnieniem raportuje nowe wartości przy ponownym zapieczętowaniu	wpisać klucz; przy następnym rozruchu wraca do normy
BitLocker prosi o klucz przy każdym rozruchu	w kolejności rozruchu PXE jest przed dyskiem — mierzone są dwa różne urzędy	dysk przed PXE albo wyłączenie PXE
Brak wartości w rejestrze i brak zdarzeń	Secure Boot wyłączony w firmware	`Confirm-SecureBootUEFI`; decyzja o włączeniu Secure Boot
Po aktualizacji maszyna nie startuje	firmware nadpisał DB zamiast dopisać	reset Secure Boot w firmware, poprawiony firmware od OEM
Błąd 65000 przy polityce Secure Boot z Intune na Pro	usługa licencyjna blokowała polityki MDM	`ClipDLS.exe removesubscription`, potem `ClipRenew.exe`
Stary pendrive albo obraz PXE nie startuje	PCA 2011 jest już w DBX	nowy nośnik zbudowany po przejściu na boot manager z 2023 roku
Host linuksowy nie przyjmuje nowego shima	shim zaktualizowany przed zmiennymi UEFI	najpierw zmienne UEFI Secure Boot, potem shim — według wytycznych dystrybucji

Powiązane: Windows 11 w firmie 2026 — przegląd zmian · Skrypty audytowe Active Directory · WinRM — zarządzanie zdalne · Windows Update z wiersza poleceń · Quick Machine Recovery, Recall i Click to Do

Źródła: Windows Secure Boot certificate expiration and CA updates · When Secure Boot certificates expire · przewodnik dla IT · aktualizacje i ogłoszenia · klucze rejestru · metoda GPO · metoda Intune · monitorowanie przez Intune Remediations · zdarzenia DB i DBX · status w aplikacji Zabezpieczenia Windows · Get-SecureBootUEFI -Decoded · przewodnik rozwiązywania problemów · znane problemy · strony producentów · Windows 365 · Linux w Azure · KB5025885 — BlackLotus · KB5124008

Revision #3
Created 2026-09-27 17:44:15 UTC by Tomasz Konieczny
Updated 2026-10-18 23:00:54 UTC by Tomasz Konieczny