*presented by*

Microsoft

# Evolving the Secure Boot Ecosystem

UEFI Fall 2023 Developers Conference & Plugfest
October 9-12, 2023
Presented by
Jeffrey Sutherland (Microsoft)
Douglas Flick (Microsoft)

# Agenda

- Secure Boot
- Secure Boot Certificate Rolling
- UEFI CA Signing Requirements
- Secure Boot V.Next
- Tooling
- Testing
- Questions

# Secure Boot

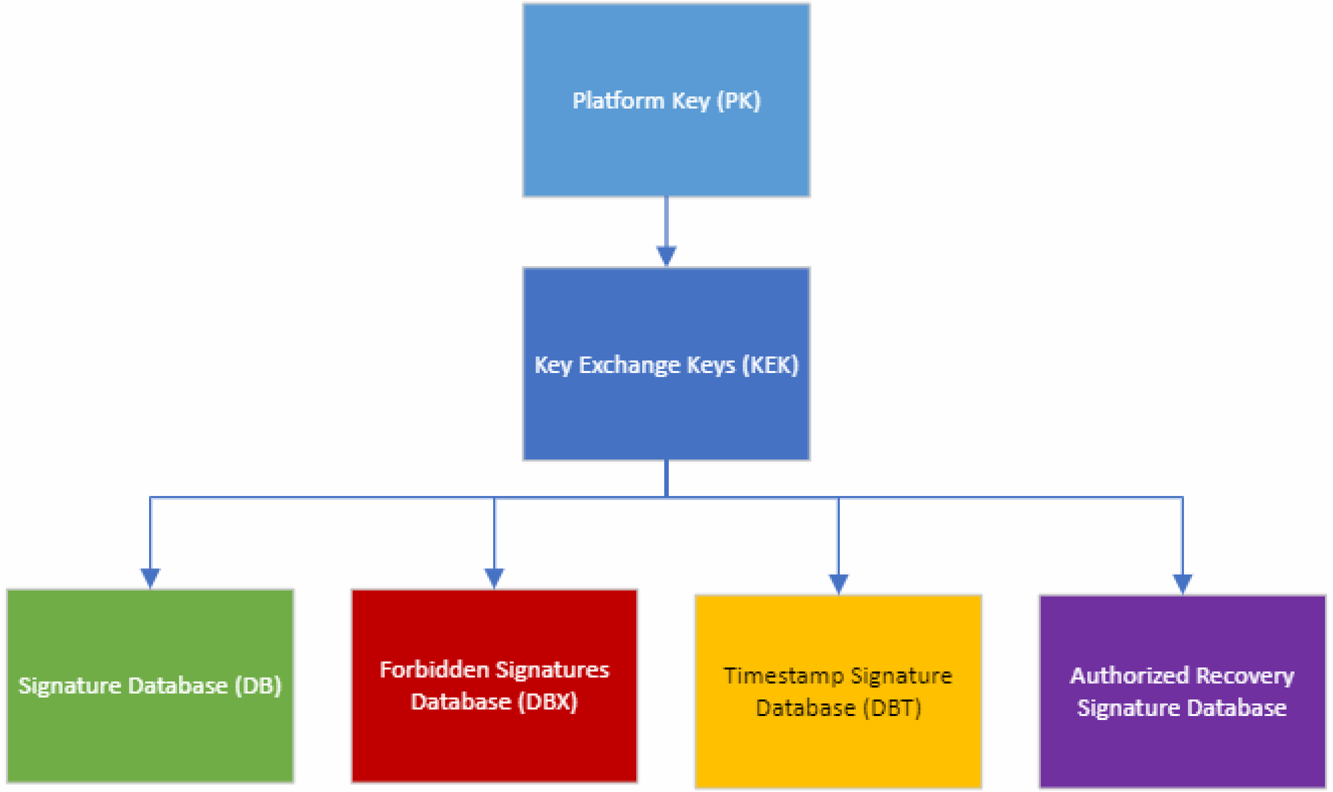
*A secure boot brought to you by DALLE 2*

# What Is It?

- UEFI Secure Boot is a technology that allows verified 3rd party firmware code to run in the OEM firmware environment.
- UEFI Secure Boot is just one of many security boundaries in the boot environment
  - Among consumer devices it a key participant in the chain of trust involved to load an OS
- Secure boot simply verifies the authenticity of the non-embedded drivers and applications
  - I.E. Boot loaders / drivers / option ROMS must be signed ahead of time and have their signatures verified during start up if they want to run in the UEFI environment
  - These non-embedded drivers and applications must be signed by an authority's certificate that exists in the DB (such as Microsoft 3rd Party CA)

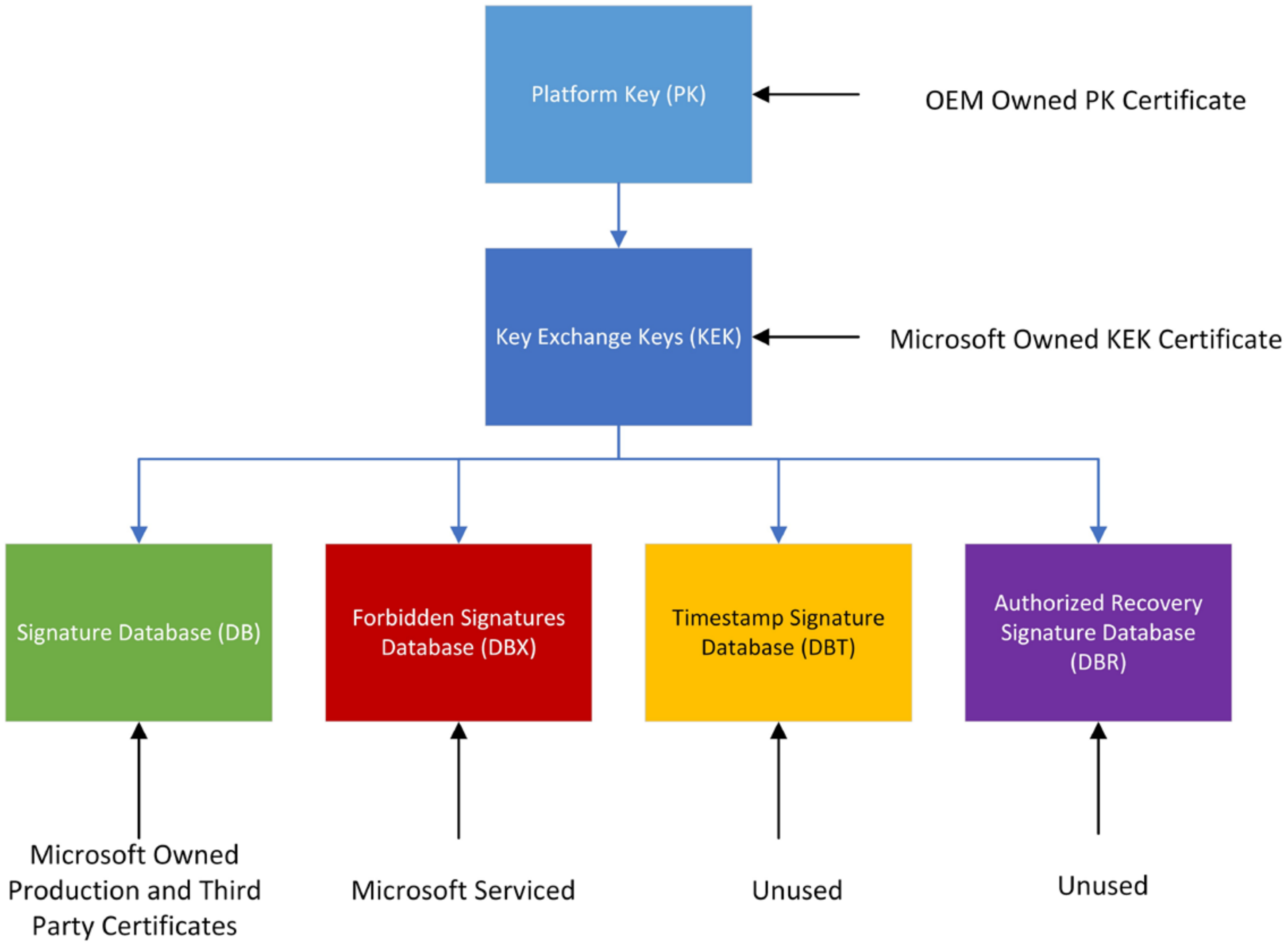
# Background

- Secure boot uses a hierarchy of variables to establish trust and then uses that trust to verify the authenticity of media.
- These variables are:
  - PK
  - KEK
  - DB
  - DBX
  - DBT
  - DBR
- The variables may contain a list of certificates, hashes or both
- For each of these variables there exists a default that is used to restore them if Secure Boot is disabled and reenabled


Platform Key (PK)
Key Exchange Keys (KEK)
Signature Database (DB)
Forbidden Signatures Database (DBX)
Timestamp Signature Database (DBT)
Authorized Recovery Signature Database

# Microsoft Configuration

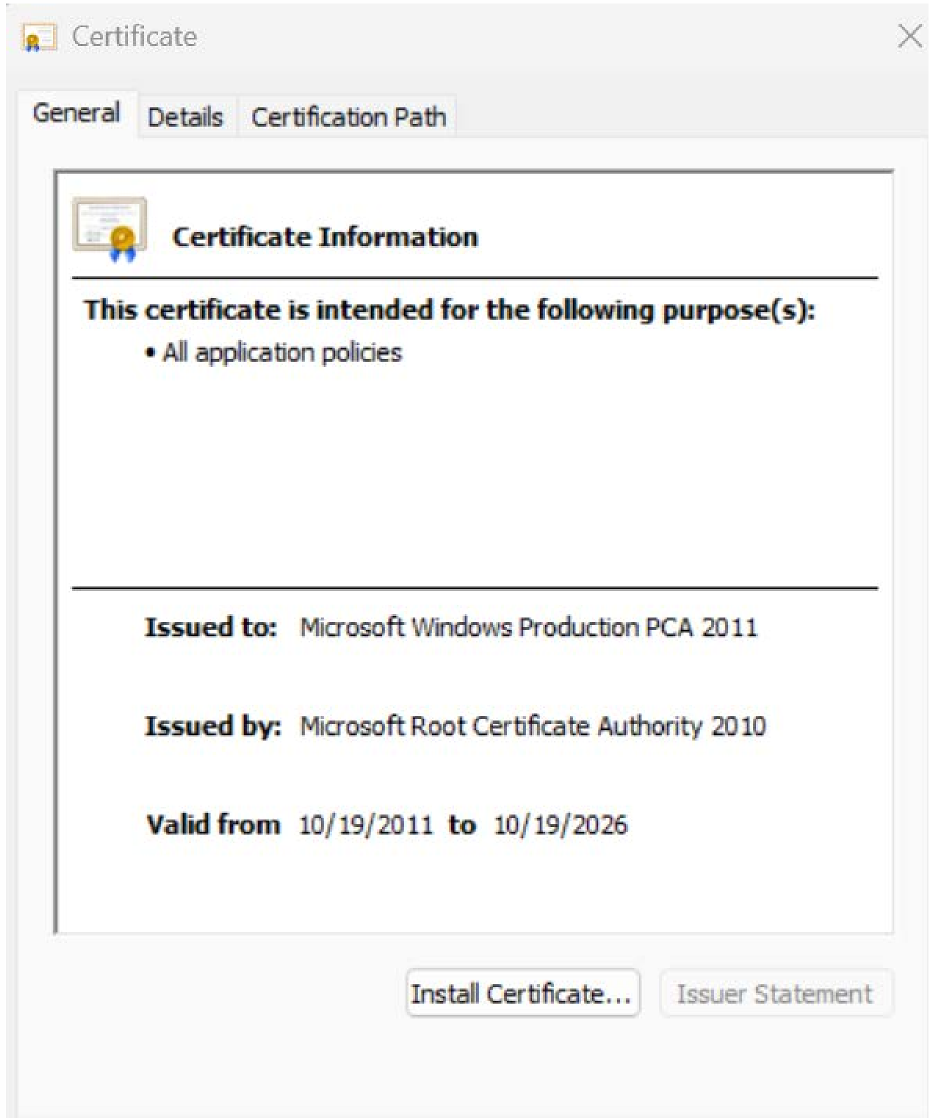
- Today, Microsoft asks OEMs to place Microsoft certificates in the KEK, DB and Microsoft services the DB and DBX.


Platform Key (PK)
OEM Owned PK Certificate
Key Exchange Keys (KEK)
Microsoft Owned KEK Certificate
Signature Database (DB)
Forbidden Signatures Database (DBX)
Timestamp Signature Database (DBT)
Authorized Recovery Signature Database (DBR)
Microsoft Owned Production and Third Party Certificates
Microsoft Serviced
Unused
Unused

# Secure Boot Certificate Rolling

# Overview

- The 2011 Windows Production CA, 2011 UEFI CA  and 2011 Microsoft KEK are expiring in 2026.
- In the history of Secure Boot, no one has never attempted to perform a firmware DB / KEK update at this scale.
- Microsoft depends on partners to help us find issues before in market devices have issues.



**Certificate Information**

**This certificate is intended for the following purpose(s):**

- All application policies

**Issued to:** Microsoft Windows Production PCA 2011

**Issued by:** Microsoft Root Certificate Authority 2010

**Valid from** 10/19/2011 **to** 10/19/2026

# Certificate Rolling Process for Devices Legacy vs New Devices

✓ New machines should begin shipping with new certificates

Existing in market machines will need servicing to ensure they continue to Boot

# New Devices

New certificates available at Keys Required for Secure Boot on all PCs | Learn Microsoft.

This serves as a transitional phase as we work towards Secure Boot V.Next, replacing all 2011 certificates with their corresponding 2023 certificate counterparts.

*2011 CAs -> 2023 CAs*

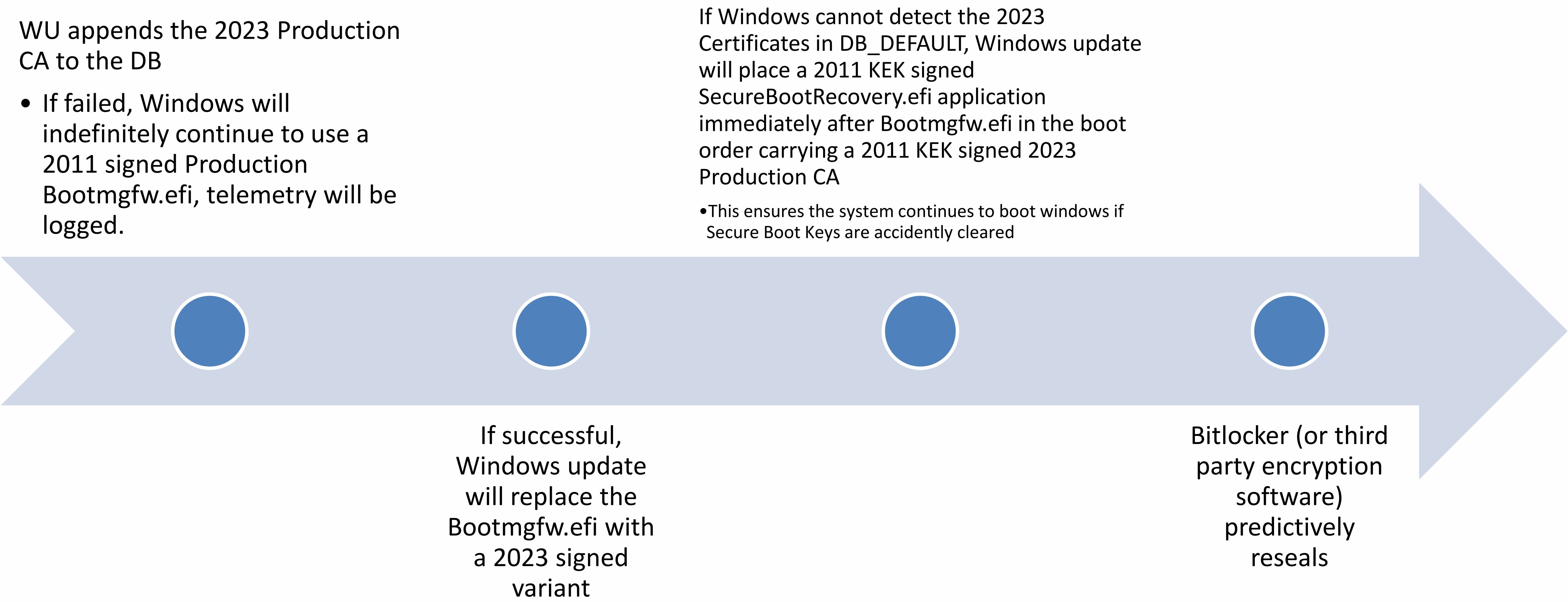
Microsoft highly encourages OEMs to promptly commence the distribution of firmware featuring these updated certificates. Furthermore, OEMs are advised to promptly disclose PK_DEFAULT, KEK_DEFAULT, DB_DEFAULT, and DBX_DEFAULT to inform Windows of the certificates they incorporate upon reset.

*The best customer experience will be on devices with both set of certificates in the default variables.*

# Legacy and In Market Devices

1. Multiple stages are required to keep in market booting with the new certificates and serviceable
    1. Update DB with 2023 Windows Production CA
        1. **This keeps a machine booting windows!**
    2. Update DB with 2023 Microsoft UEFI CA
        1. **This allows Linux, option ROMs, etc, to continue booting!**
    3. Use the OEM PK to update KEK with 2023 Microsoft KEK CA
        1. **This allows Microsoft to continue servicing revocations to a machine (and any future need to roll the allow keys)**
    4. If required, OEM updates the PK with a new PK capable of authorizing KEK
        1. This is required to update the KEK.
2. OEMs are recommended to provide a firmware update that updates Secure Boot Defaults with new certificates and expose these variables at runtime to the OS
    1. If an OEM wants to provide the best customer experience in reference to BitLocker and Installation media
    2. It is imperative that the OS be the one to update KEK, DB, and DBX to avoid a BitLocker recovery

# DB Updates for Windows Production CA



WU appends the 2023 Production CA to the DB

- If failed, Windows will indefinitely continue to use a 2011 signed Production Bootmgfw.efi, telemetry will be logged.

If successful, Windows update will replace the Bootmgfw.efi with a 2023 signed variant

If Windows cannot detect the 2023 Certificates in DB_DEFAULT, Windows update will place a 2011 KEK signed SecureBootRecovery.efi application immediately after Bootmgfw.efi in the boot order carrying a 2011 KEK signed 2023 Production CA

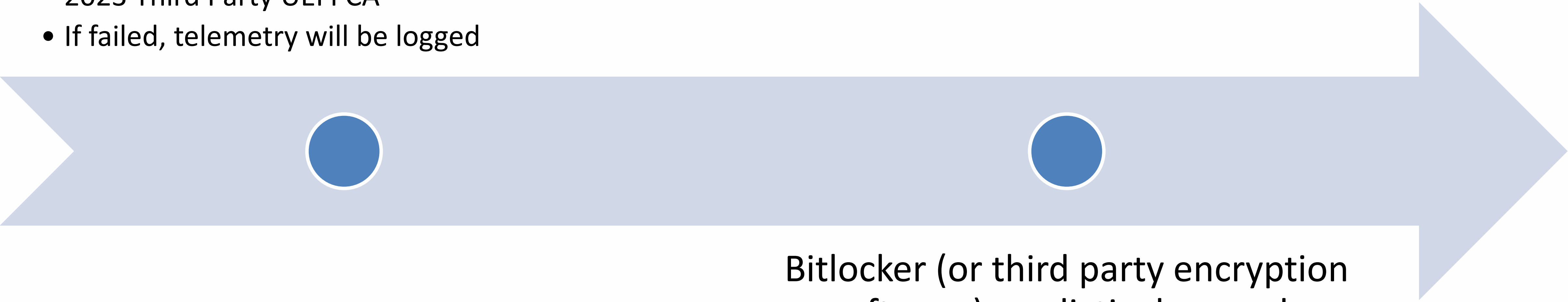
- This ensures the system continues to boot windows if Secure Boot Keys are accidently cleared

Bitlocker (or third party encryption software) predictively reseals

# DB Updates for Third Party CA

Microsoft has generated a 2023 Third Party UEFI CA

- Windows update will perform an APPEND operation on the DB with a 2011 KEK signed 2023 Third Party UEFI CA
- If failed, telemetry will be logged

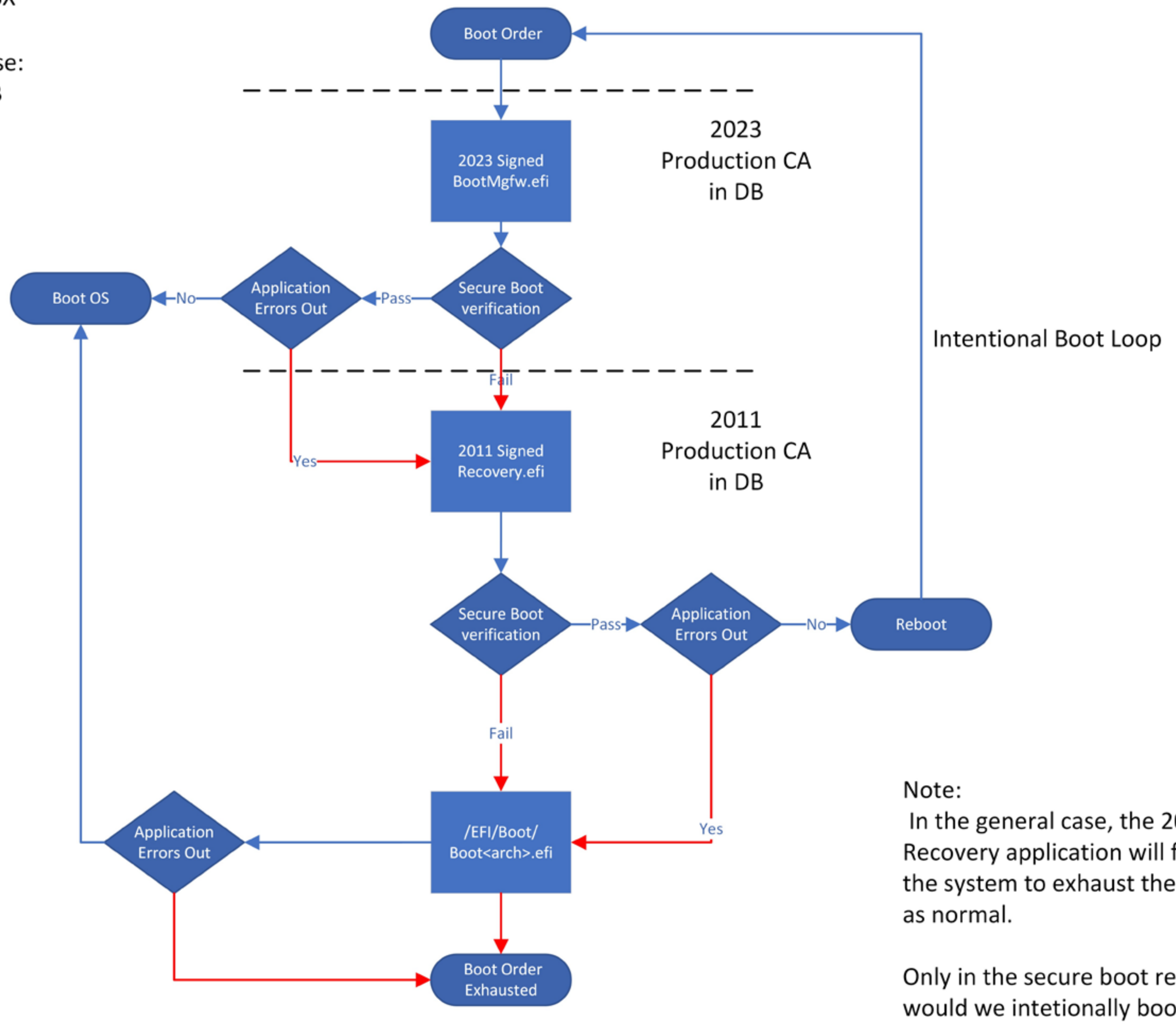


Bitlocker (or third party encryption software) predictively reseals

# SecureBootRecovery.efi

General Case:
2023 Production CA in DB
2011 Production CA in DBX

Secure Boot Recovery Case:
2011 Production CA in DB



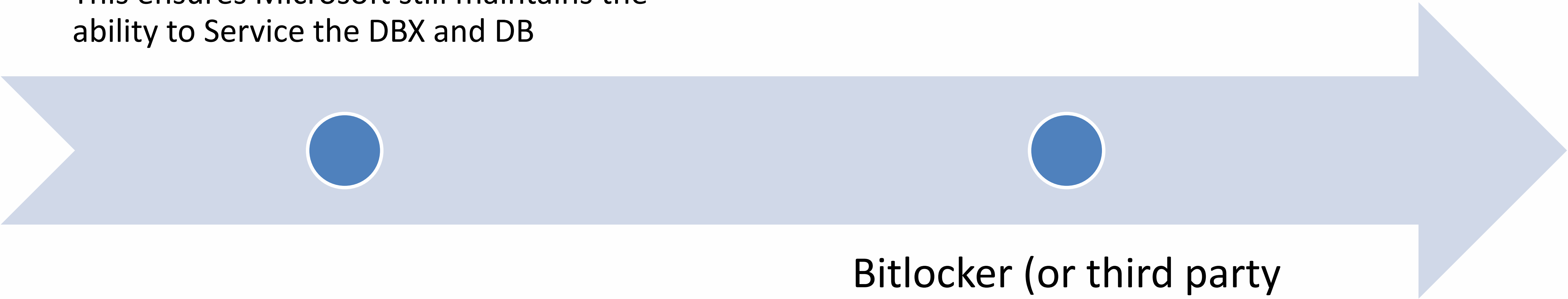
Note:
In the general case, the 2011 Signed Recovery application will fail allowing the system to exhaust the boot order as normal.

Only in the secure boot recovery case would we intetionally boot loop

# KEK Updates

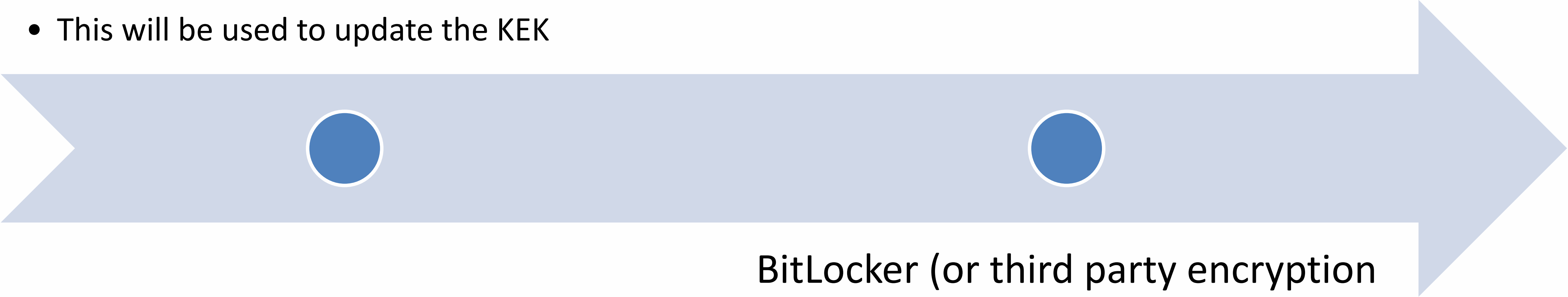
Windows Update will perform an APPEND operation on the KEK with an OEM PK signed KEK

- This ensures Microsoft still maintains the ability to Service the DBX and DB



Bitlocker (or third party encryption software) predictively reseals

# PK Update



Microsoft is working with OEMS who have lost access to a valid PK to ensure those devices can be remediated

- This will be used to update the KEK

BitLocker (or third party encryption software) predictively reseals

# Impact

- Edge Cases – **These are real cases we've seen in testing partner firmware**
  - For in market devices, the 2023 signed installation media needs to be used.
    - Microsoft will ship additional media that includes a recovery application to restore the 2023 certificate that may be required to boot.
  - OEM firmware menus and features for user modification of secure boot keys may undo some of the secure boot key servicing operations.
    - If Microsoft cannot detect the new certificates via DB_DEFAULT, Windows will begin placing SecureBootRecovery.efi behind bootmgfw.efi in the boot order.
  - Some OEM specific firmware implementations prevent updates to the Secure Boot variable store or **brick a system entirely**.
    - **These systems will need firmware updates!**
- Linux community shim will need to be signed by new certificates and need to test their systems will continue to boot.
  - Talks are underway with the Linux SHIM community to prepare them for this change.

# Risks / Issues

| Risk / Issue | Mitigations |
|---|---|
| DB and KEK default values | • There is no way to programmatically update the DB and KEK default values<br>• Toggling Secure Boot after our updates would result in our keys being omitted leading to machines that cannot boot if they have boot loaders signed by the new certificates |
| **BitLocker and TPM** interaction | • Windows will use a similar process for KEK updates that we use for DBX updates<br>• Designing these updates alongside the BL and TPM ENS teams<br>• Exhaustive validations and selfhost prior to retail updates |
| Lost/expired OEM **PK keys** | • OEM must push Firmware update for the PK |
| Secure Boot firmware code doesn’t work as required for these scenarios | • OEM must push Firmware update for Secure Boot |
| OEM specific security features prevent updating Secure Boot | • OEM must push Firmware update OEM specific security feature |
| UEFI variable space is at it limits – Secure Boot variable space is not reserved appropriately | • OEM must push a Firmware update addressing these limits |

# Certificate Rolling Process Takeaways

- The current implementation of Secure Boot is not effectively accommodating the growing diversity of the ecosystem.
  - The DBX cannot withstand the scale at which revocations occur
    - Utilizing certificate or hash-based revocation methods offers limited flexibility for articulating precise revocation policies and adhering to variable size constraints.
  - Microsoft cannot reduce the attack surface of a device when it must make decisions for every device in existence together.
- Inability to Update Secure Boot Defaults
- Reliance on PK makes it so that Microsoft must talk to every OEM to update the KEK.
  - This is a near impossible challenge and drastically increases the risk that a machine will become un-serviceable. In fact some number of devices will likely become un-serviceable due to this event.
- Multiple implementations of the Secure Boot and crypto code increases the uncertainty and ultimately creates hesitancy about how a machine will behave if serviced – which slows down the entire industry.

# UEFI CA Signing Requirements

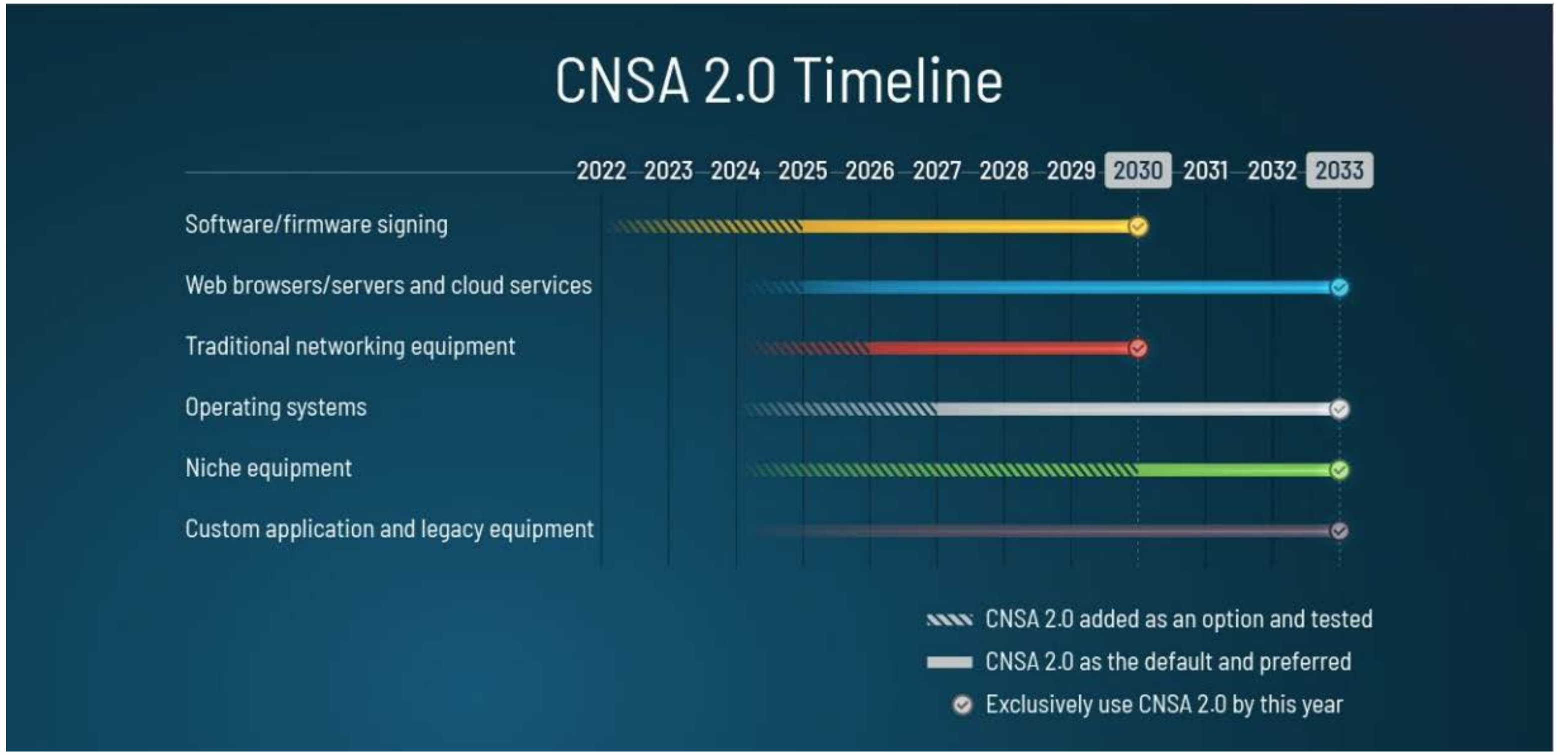
# New Requirements

1. (NEW for 2023 CA) All binaries submitted to be signed must include metadata (format under discussion; investigating SBM) that at a minimum includes information such as:
    1. Company Name
    2. Product Name
    3. Version
2. (NEW for 2023 CA) All binaries that use OpenSSL must use an updated version (3.0+)
3. (As of Nov 2022) All binaries must meet the Microsoft 3rd Party UEFI CA memory
    1. Must be aligned with page size.  This must be 4kb, or a larger power of 2 (ex 64kb)
    2. Must not combine IMAGE_SCN_MEM_WRITE and IMAGE_SCN_MEM_EXECUTE for any given section.
    3. If targeting NX compatible firmware, DLL Characteristics must include IMAGE_DLLCHARACTERISTICS_NX_COMPAT.
    4. See UEFI CA memory mitigation requirements for signing - Microsoft Community Hub for more information.

# Secure Boot V.Next

# Post Quantum Crypto

- Firmware must move to Post-Quantum Crypto
  - This means that there will be a lot of churn impacting firmware for years to come
- Investigating a method by which the OS may be able to securely service crypto, secure boot, security essential code without requiring OEMs to provide firmware updates

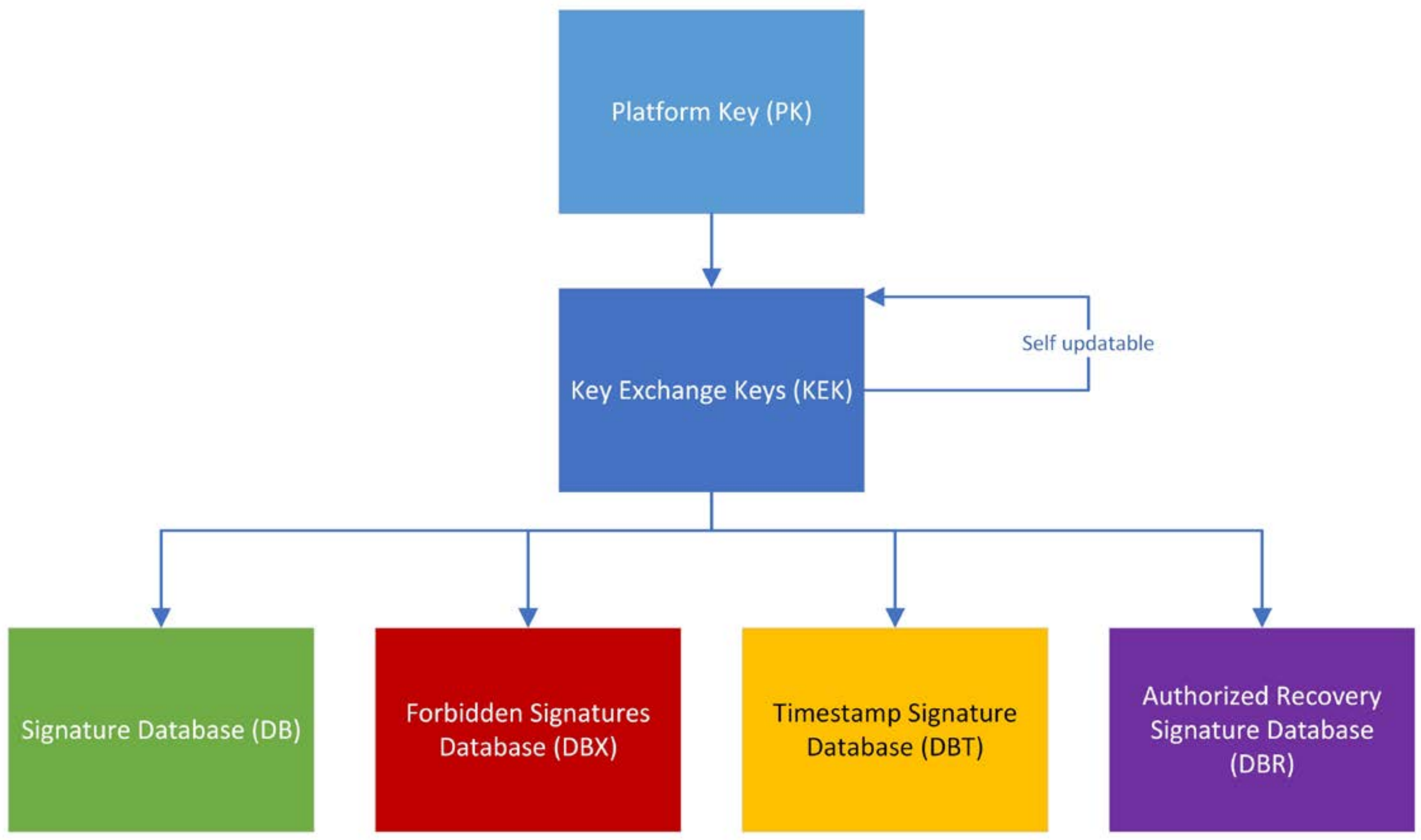


# Firmware Based SBAT

- Investigating adding an additional EFI Signature Type ‘SBAT’ that may be used to revoked by policy-based expressions
  - All binaries signed by the new certificates will be required to carry signed info that can be used to revoke them instead of by hash or certificate
  - Further the inclusion of this additional metadata may be used for SBOM purposes

# KEK Signed KEK Updates

- As mentioned, it’s a near impossible challenge to have the PK reauthorize a KEK at Scale
  - This change would allow an authority to rotate keys as needed
  - Optionally Microsoft will begin offering a Microsoft PK for any OEM who would want to exit the Certificate owning business

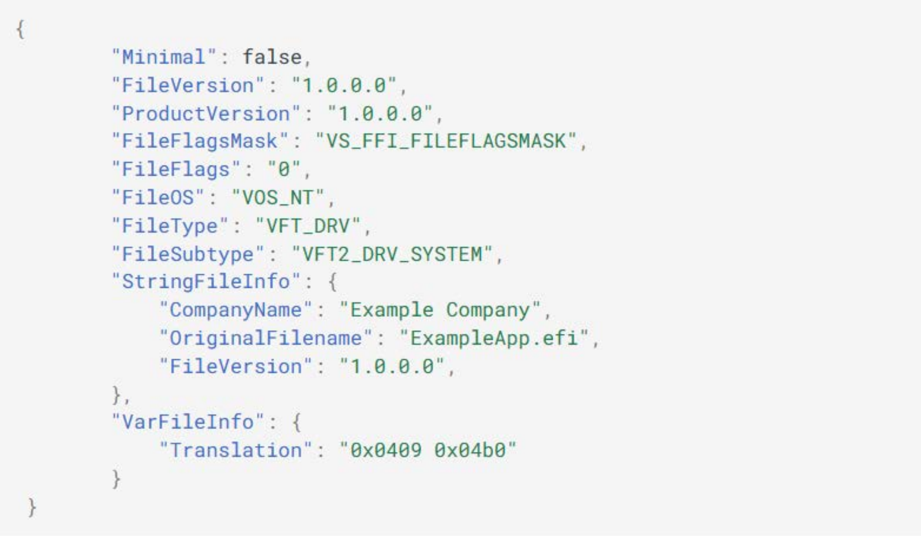

Platform Key (PK)
Key Exchange Keys (KEK)
Self updatable
Signature Database (DB)
Forbidden Signatures Database (DBX)
Timestamp Signature Database (DBT)
Authorized Recovery Signature Database (DBR)

# Updateable Secure Boot Defaults

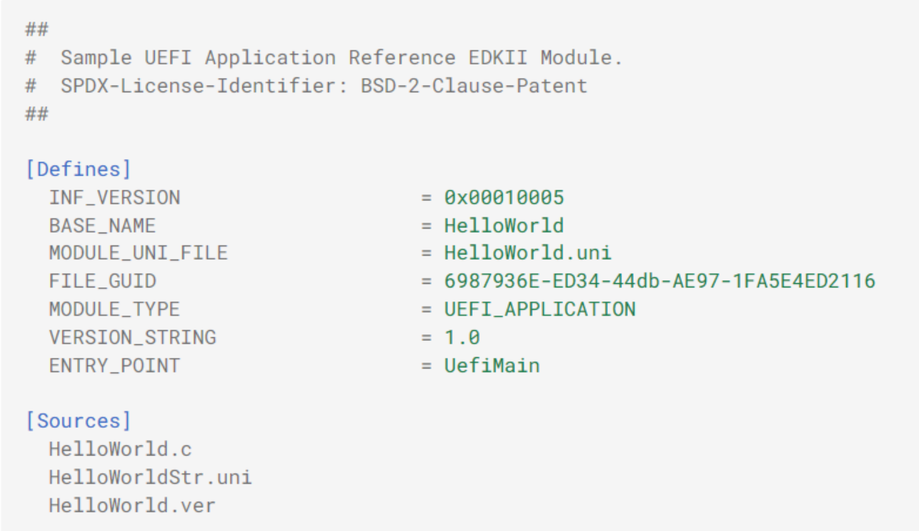
- Currently exploring methods to update Secure Boot defaults through a cryptographically secure channel.
  - This would remove the need for a recovery application in future certificate rolling events

# Tooling

# Version Info Tool



```
{
        "Minimal": false,
        "FileVersion": "1.0.0.0",
        "ProductVersion": "1.0.0.0",
        "FileFlagsMask": "VS_FFI_FILEFLAGSMASK",
        "FileFlags": "0",
        "FileOS": "VOS_NT",
        "FileType": "VFT_DRV",
        "FileSubtype": "VFT2_DRV_SYSTEM",
        "StringFileInfo": {
            "CompanyName": "Example Company",
            "OriginalFilename": "ExampleApp.efi",
            "FileVersion": "1.0.0.0",
        },
        "VarFileInfo": {
            "Translation": "0x0409 0x04b0"
        }
}
```



```
##
#  Sample UEFI Application Reference EDKII Module.
#  SPDX-License-Identifier: BSD-2-Clause-Patent
##

[Defines]
  INF_VERSION                    = 0x00010005
  BASE_NAME                      = HelloWorld
  MODULE_UNI_FILE                = HelloWorld.uni
  FILE_GUID                      = 6987936E-ED34-44db-AE97-1FA5E4ED2116
  MODULE_TYPE                    = UEFI_APPLICATION
  VERSION_STRING                 = 1.0
  ENTRY_POINT                    = UefiMain

[Sources]
  HelloWorld.c
  HelloWorldStr.uni
  HelloWorld.ver
```

- Version Info
  - Available in tianocore/edk2-pytool-extensions: Extensions to the edk2 build system allowing for a more robust and plugin based build system and tool execution environment (github.com)
- This tool may be used to meet the Version Info Requirement!
  - *Or use your own tooling..*

# Secure Boot Objects

- microsoft/secureboot_objects: Secure boot objects recommended by Microsoft. (github.com)
- This repo will contain the most up to date versions of the KEK, DB and DBX that should be included in firmware.
- Pipeline generates ESL formatted Secure Boot objects that can be traced back to what produced them.
  - Consumers may append additional certificates as they see fit
- Downstream consumers can subscribe to the repo to get notified when a new version is available to be included in their firmware

# Testing

# Secure Boot Tests

- Hello UEFI test application
  - This tests that the ‘APPEND’ operation in your firmware works and that your system will boot with the new 2023 Certificates.
- Recovery Flow Test
  - This tests that the ‘APPEND’ operation and entire recovery flow works.
- Authenticated Variable tests
  - This tests that authenticated variables work as they expected to work.

Thanks for attending the UEFI Fall 2023 Developers Conference & Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

*presented by*

Microsoft