Secure Boot behind the curtain

What is Secure Boot

- Secure Boot is a security standard developed by members of the PC industry to help make sure that your PC boots using only software that is trusted by the PC manufacturer
- May restrict user freedom by preventing the installation of alternative operating systems or unsigned drivers.
- Can be vulnerable to attacks that exploit vulnerabilities in the firmware itself.
- The basis of secure boot is to use a database in the PC to verify the integrity of the firmware and boot loader

Why Secure Boot

- During the boot process the system is most vulnerable.
- It can easily be compromised by rootkits and bootkits injecting malware into your system
- During booting there is no anti-virus software running
- The malware can even cloak itself so that when the anti-virus software runs it is hidden.

How does Secure Boot Work

- Secure boot uses digital signatures This is achieved by validating the digital signature of the software against a predefined set of trusted digital keys stored in the UEFI
- Trust and authenticity within Secure Boot rely on the Public-Key Infrastructure (PKI) model. This framework establishes a certificate management system that employs Certificate Authorities (CAs) to store digital certificates. These CAs, which include the Original Equipment Manufacturer (OEM) or their representatives and Microsoft, generate key pairs that serve as the foundation of trust for the system.

How does Secure Boot Work

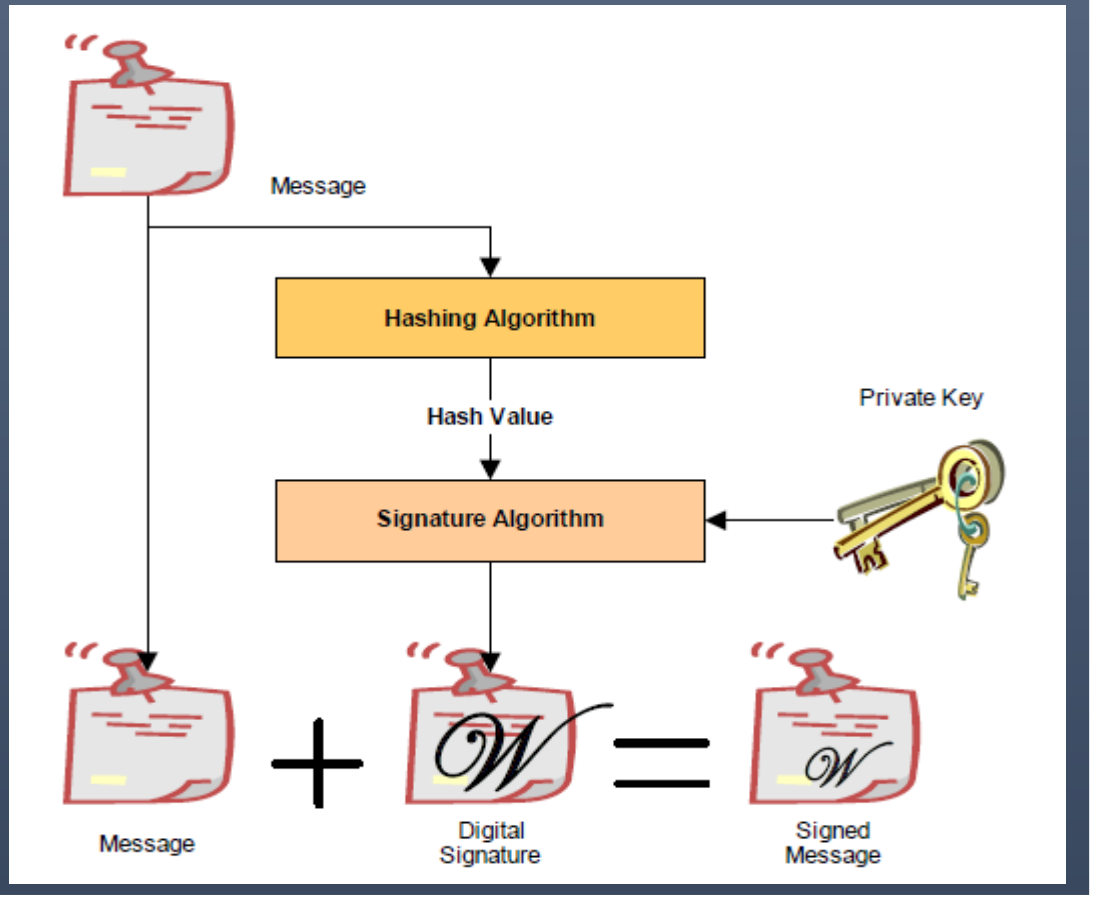
- When the PC starts it first verifies that the firmware is digitally signed and is valid
- Next the bootloader is checked that it is signed and has a trusted certificate
- The kernel is loaded and the digital signature is verified (Windows)
- The verification is done by checking that the keys stored in the NVRAM databases match the digital signature of the software.
- There verification is done using private and public keys in this process.

Keys

- All Secure Boot key use the Public Key Infrastructure (PKI).
- Keys are created using the SHA256 algorithm
- Each key includes two long numbers that are used for encryption and, in the case of Secure Boot, for data authentication.
- Secure Boot uses a private key and a public key.
- The private key is used to sign a file, which is an EFI program. That signature is then appended to the program.
- The public key in the case of Secure Boot is embedded in the firmware itself or is stored in NVRAM.

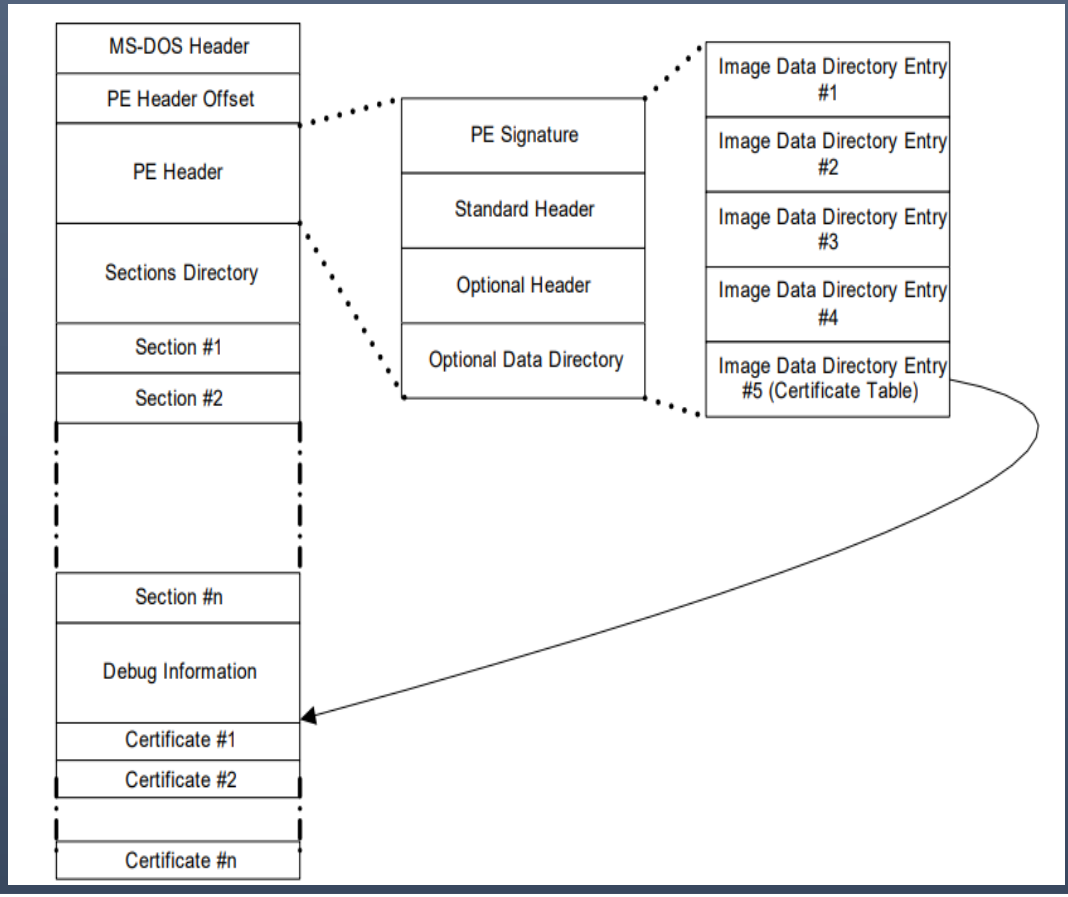
Digital Signatures

- In order to verify a signature, two pieces of data are required:
  - the original message
  - the public key.
- First, the hash is calculated.
- The digital signature is decoded using the public key and compared against the hash.



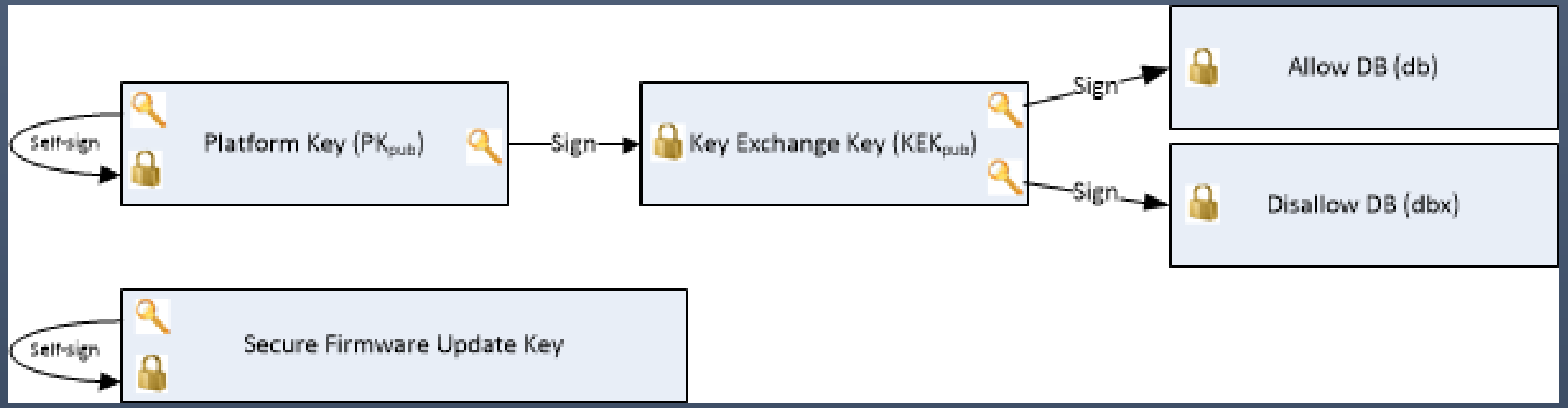
UEFI executables

- The signatures used for digital signing of are embedded in the executable itself.
- Within the header is an array of directory entries.
- The fifth data directory entry is a pointer to a list of certificates along with the length of the certificate areas.



Keys

- Hierarchy



Databases used

- There are three databases used in secure boot:

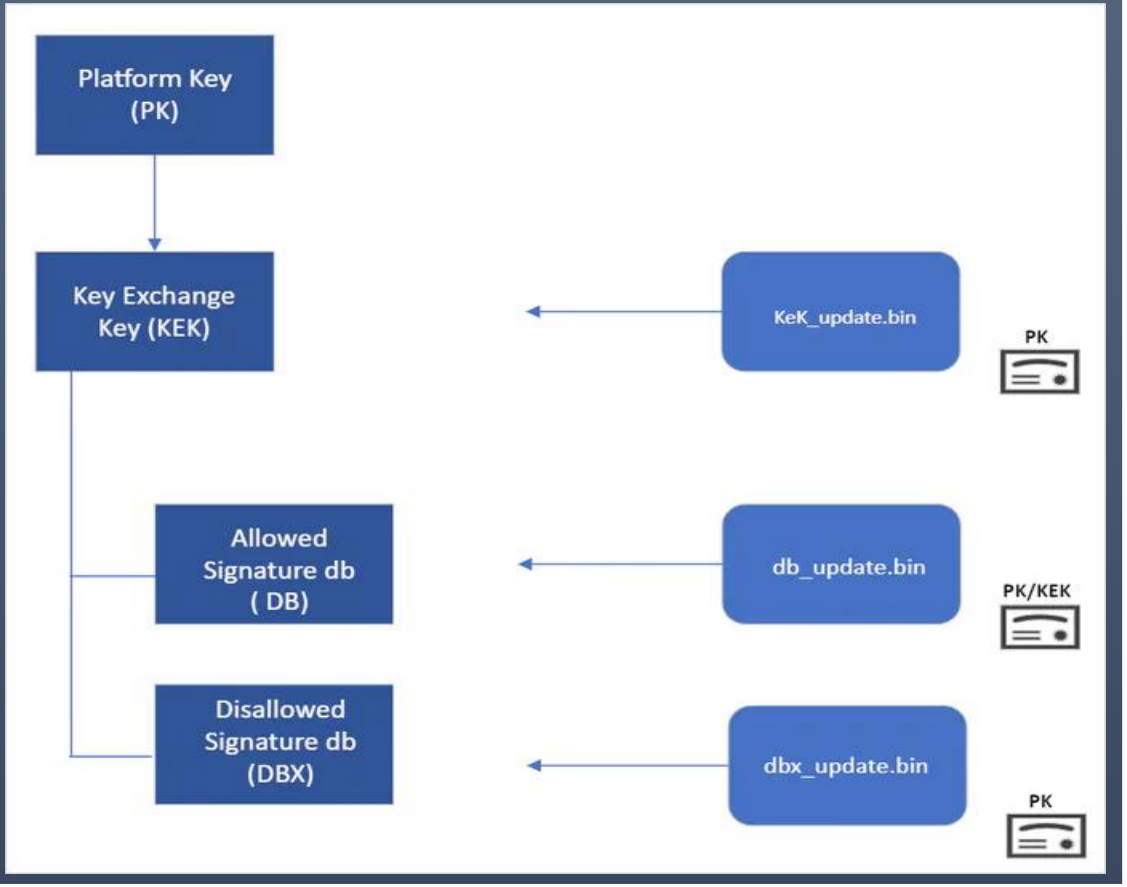
1. Allowed signature database (db),
2. Disallowed (revoked) signatures database (dbx),
3. Key Enrolment Key database (KEK).

- Linux also uses MOK, (Machine Owner Keys) that you can create and sign those components that you trust. Requires SHIM as a go-between between EFI BIOS and GRUB).

How does Secure Boot Work

- As can be seen there is a platform key (the OEM typically managing the Platform Key)
- The PK is used to sign updates to the Key Exchange Key (KEK) database.
- The two main databases are:

  Allowed Signature Database(DB)
  Disallowed Signature Database (DBX)



Validation

- The validation of each item is done using public keys and checking the results in two databases:

  The Allowed Signature Database(DB)

  Forbidden Signature Database (DBX)

- First a check is done to see if the certificate is valid in the Allowed database, then if valid if it not present in the Forbidden database.

TPM

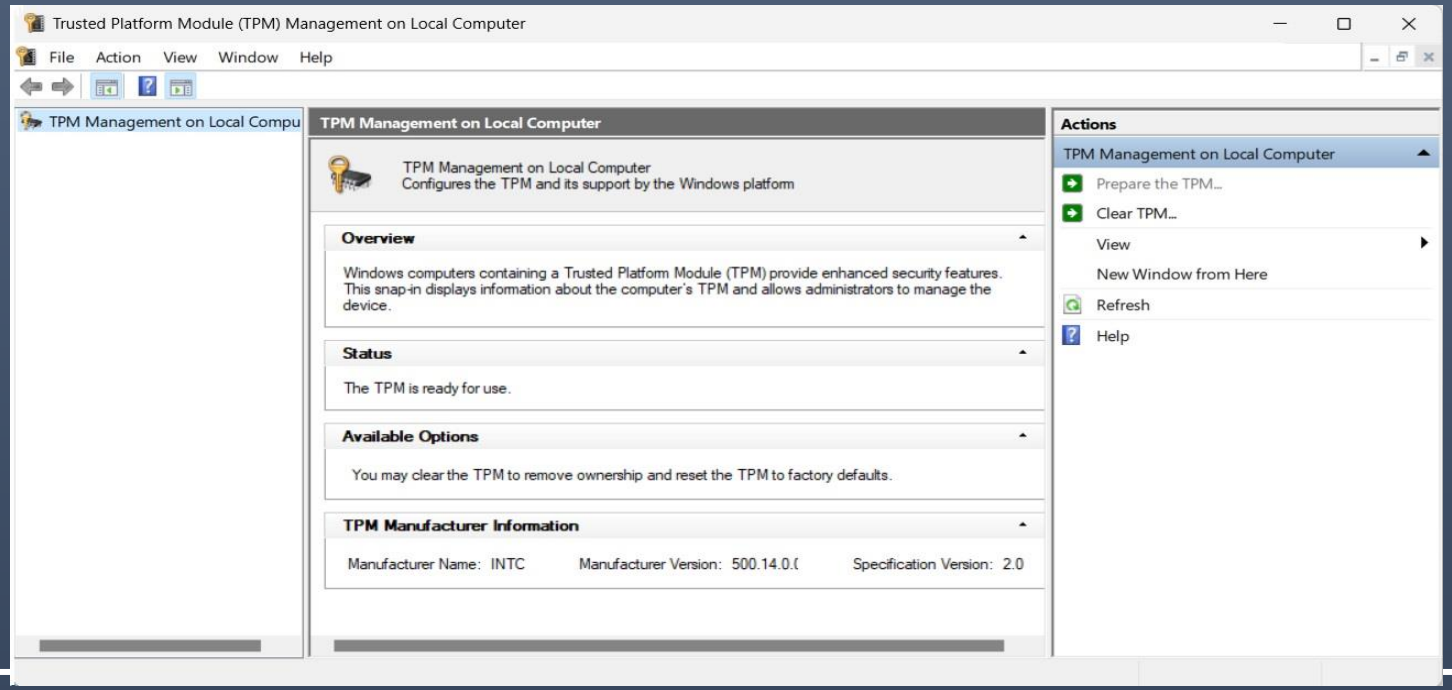
- Secure boot requires UEFI, not BIOS or a CSM
- It does not implicitly require a TPM (Trusted Platform Module)
- Officially W11 requires TPM
- A TPM is a physical or embedded (microcontroller) that resides on a computer's motherboard or in its processor!

TPM

- Some processors contain a TPM! For example 8th Gen or later Intel® Core™ Processor family and AMD: Ryzen processors from the first generation (Ryzen 1000 series) and newer
- The overwhelming majority of PCs built during the past 15 years include TPM technology, and most PCs designed in 2015 or later include the TPM

Do I have TPM?

- IN Linux read the value of /sys/class/tpm/tpm0/device/description
- In Windows from a command prompt type :tpm.msc



From Microsoft!

- All three Microsoft certificates are set to expire in 2026.
- The full DB update will follow a controlled rollout process to reach all Windows customers during the April 2024 servicing and preview updates, anticipating the certificate expiration in 2026.
- The Microsoft Corporation KEK CA 2011 is set to expire in 2026, and all OEMs must create, sign, and submit updates for the new Microsoft Corporation KEK CA 2023 to Microsoft. This will allow Microsoft to update in-market devices with the new Microsoft KEK CA, allowing systems to continue receiving DB and DBX updates after 2026.

Database update?

- The databases are not static but are updated when necessary
- In the case of Windows, this is done during the standard update cycle.
- A similar update is done in the Linux world.

Black Lotus - bootkit

- A stealthy Unified Extensible Firmware Interface (UEFI) bootkit called BlackLotus has become the first publicly known malware capable of bypassing Secure Boot defenses, making it a potent threat!
- It specifically attacks the Microsoft boot loaders!
- Nearly all bootloaders starting from Windows 8 are vulnerable!
- This includes the boot loaders for w11 up to May 9th 2023!
- To address this problem MS will update the Revoked database with all those bootloaders signatures.

Black Lotus - bootkit

- The question is how many certificates will there be updated?
- There is no default size specified for this db in the UEFI spec!
- To minimize the number, Microsoft will limit the certificates to the appropriate hardware (x86, ARM …) .
- As damage control Microsoft will implement the updated Code Integrity Boot Policy. This checks the drivers and system files on your device for signs of corruption or malicious software. Requires Secure Boot enabled.

What next?

- Secure boot was not well thought through (Database sizes not specified!)
- Next is PLUTON.
- Pluton is a separate chip on the same die as the CPU.
- Pluton is completely self-sufficient which implies that it is out of band. dTPM (discrete TPMs) are usually more susceptible than fTPMs (Firmware based TPMs) ????
- Security updates from the cloud.
- Pluton works with existing TPM specifications and APIs.

References

- BlackLotus

  https://thehackernews.com/2022/08/researchers-uncover-uefi-secure-boot.htmlcyber landscape
- UEFI specifications:

  https://uefi.org/sites/default/files/resources/UEFI_Spec_2_9_A_final_Aug29.pdf
- Pluton as TPM

  https://learn.microsoft.com/en-us/windows/security/hardware-security/pluton/pluton-as-tpm
- Secure Boot Keys

  https://blog.sonnes.cloud/secure-boot-what-it-is-and-how-to-update-secure-boot-keys/

Questions?

Thank You