**Signed files, verified v unverified publishers, criteria for verification**

* **Microsoft Specific verification**
* A digital signature is a stamp of authentication of digital information or programs
* Publisher verification gives app users and orgs information about the authenticity of the application.
  + Verified publisher means that the organization that published the app has been verified to be authentic by Microsoft.
    - Verifying an app with Microsoft includes using a Microsoft Cloud Partner Program account that’s been verified and associating the PartnerID with the app during registration
* **General verification and signing**
* A verified publisher is someone whose software products and code are trusted by Microsoft or other operating systems and browsers.
  + The publisher must undergo digital identity verification (code signing validation)
  + Software or code must be signed by using a publicly trusted certificate
    - DigiCert, Sectigo, etc.
    - Not all cert are equal
      * Individual or standard certs will require additional verification about personal or organizational information
      * Extended Validation allows for longer validation periods, but has more strict requirements and vetting.
  + Drivers must also be signed by a publicly trusted cert, but they must have it signed with an extended validation certificate, as the drivers are interacting at the kernel level
    - For windows you also have to achieve a “Windows compatibility certification”
* Unsigned programs will be programs that a user downloads from a non-windows trusted source or third-party vendor that hasn’t gone through proper vetting processes.
  + Side Tangent also explains why some Windows processes Via autoruns will flag as “unverified”
* Windows has a setting in their settings menu that you can change to only allow downloads from verified publishers on Microsoft Store
  + Settings > Apps > Apps & Features
* **Side Tangent (About verification and autoruns)**
  + Autoruns will classify “protected” folders and programs as Unverified when in reality they are, in order to further check that it is legit, you can use the *SigCheck* tool in order to read the signature given for the binaries.
  + <https://answers.microsoft.com/en-us/windows/forum/all/is-it-normal-for-some-microsoft-entries-to-appear/d3990e1e-ea59-434c-bd5c-77b7f17137d6>
* **Different types of services**
  + Win32, Win32\_own\_process, Win32\_share\_process, f0 error, e0 user\_share\_process instance,
    - Win32 – Generic Windows Service
    - Win32OwnProcess – A Win32 program that can be started by the Service Controller and obeys the service control protocol
      * Typically runs in a process all of its own
    - Win32ShareProcess – A Win32 service that can share a process with another win32 service
    - Adapter – A service for a hardware that needs its own driver
    - FileSystemDriver – A file system driver or Kernel device driver
    - Interactive Process – A service communicable with the desktop
    - KernelDriver – A Kernel device such as a hard disk or other low level hardware driver
    - RecognizerDriver – A file system in use during startup in order to determine the file systems present on the system.
* **What are Drivers**
  + A driver is a software component that lets the operating system and a device communicate.
  + The driver, usually developed by the device's manufacturer, knows how to communicate with the device hardware to get the data. Once the driver gets the data, it gives it back to the operating system, which then gives it back to the app.
  + Not all drivers communicate directly with a device. Often, several drivers layered in a driver stack take part in an I/O request.
  + Types of Hardware Drivers:
    - **Function driver**: The driver that communicates directly with the device is called the function driver*.*
    - **Filter driver**: Drivers that do auxiliary processing are called filter drivers*.*
  + Software Drivers
    - Software drivers always run in kernel mode. They're primarily written to access protected data only available in kernel mode. However, not all device drivers need access to kernel-mode data and resources, so some device drivers run in user mode.

**Sources**

[**https://codesigningstore.com/how-to-become-a-verified-publisher-with-microsoft#:~:text=A%20Microsoft%2Dverified%20publisher%20is%20someone%20whose%20software%20products%20and,process%20called%20code%20signing%20validation**](https://codesigningstore.com/how-to-become-a-verified-publisher-with-microsoft#:~:text=A%20Microsoft%2Dverified%20publisher%20is%20someone%20whose%20software%20products%20and,process%20called%20code%20signing%20validation)**.**

[**https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules**](https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules) **(Driver blocklist, known vuln drivers)**

[**https://learn.microsoft.com/en-us/dotnet/api/system.serviceprocess.servicetype?view=net-8.0**](https://learn.microsoft.com/en-us/dotnet/api/system.serviceprocess.servicetype?view=net-8.0)

[**https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/what-is-a-driver-**](https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/what-is-a-driver-)

[**https://www.hp.com/us-en/shop/tech-takes/what-are-computer-drivers#:~:text=A%20driver%2C%20or%20device%20driver,external%20peripherals%2C%20like%20a%20printer**](https://www.hp.com/us-en/shop/tech-takes/what-are-computer-drivers#:~:text=A%20driver%2C%20or%20device%20driver,external%20peripherals%2C%20like%20a%20printer)**.**

[**https://www.tenforums.com/tutorials/126607-export-list-running-stopped-services-windows.html**](https://www.tenforums.com/tutorials/126607-export-list-running-stopped-services-windows.html)