WHQL and Digital Signature considerations

Revision 1.6 – 15th Oct 2013
www.touch-base.com\documentation\technical

Signing procedure   Signing service - Internal   Signing service - External   Cost   Contact

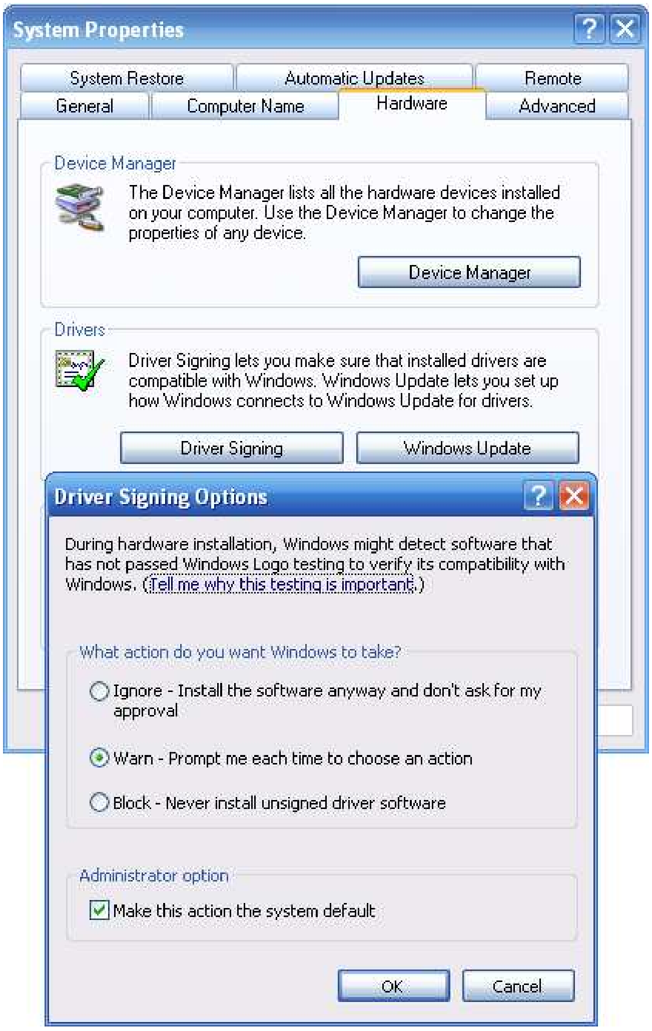
Our driver and utility programs carries an Authenticode Certificate. An Authenticode digital signature guarantees that the software was produced by the individual or company named in the certificate, which has been verified by the authority that issued the certificate.

However, not all builds of our driver will be WHQL (up to Win 7) / WHC (Win 8) digitally signed. Short for **W**indows **H**ardware **Q**uality **L**abs / **W**indows **H**ardware **C**ertification are a Microsoft facility that tests and certifies third-party hardware and driver products for compatibility with Windows operating systems. Products that meet the compatibility requirements are then allowed to display Windows logos on product packaging, advertising and collateral and other marketing materials, indicating that the product has met the standards of Microsoft and that the product has been designed to work with the Windows operating systems. Once a product has received the WHQL logo it is listed on the Microsoft Hardware Compatibility List. This subject is covered in full here. Wikipedia here.

The digital signature is associated with individual driver versions, and certifies to users that the driver provided with the device is identical to the driver that was tested.

Drivers cannot pass these tests in isolation; they have to be submitted with suitable hardware. It is our understanding that digital signatures are only available for PnP devices. USB devices by their very nature are PnP compatible. The other devices mainly supported by UPDD are serial and very few of these devices are PnP. Serial PnP device specification is described in the Serial PnP specification document. Once the submitted 'package' is approved with a suitable PnP device we have found a mechanism to subsequently embed non-pnp devices into the package so installing the driver for the non-pnp device will still install a signed driver. This allows us to offer digitally signed drivers for both USB and serial devices embedded in a single package.

A driver that passes the tests is allocated a 'digital signature' and as such is considered 'signed'. Drivers that have not been submitted for testing or have failed the tests are considered 'unsigned'. Depending on the Driver Signing setting in the Hardware Tab of the system applet in the Control Panel, unsigned drivers can be blocked, approved (most common setting) or ignored.



The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.

During hardware installation, Windows might detect software that has not passed Windows Logo testing to verify its compatibility with Windows. (Tell me why this testing is important.)

What action do you want Windows to take?

○ Ignore - Install the software anyway and don't ask for my approval

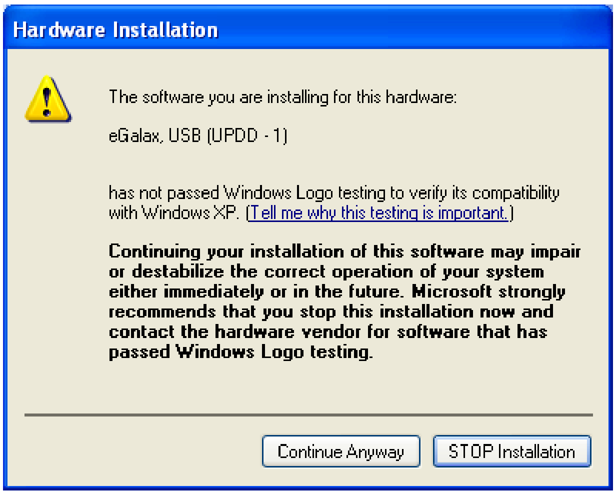
● Warn - Prompt me each time to choose an action

○ Block - Never install unsigned driver software

Administrator option

☑ Make this action the system default

This setting will result in the following dialog being shown when the hardware, handled by the unsigned driver, is used for the first time:



Hardware Installation

The software you are installing for this hardware:

eGalax, USB (UPDD - 1)

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

Given that the UPDD driver supports 100's of pointer devices, mostly unsigned, then most UPDD drivers run 'unsigned'. Signed drivers can only be utilised with hardware used in the signing process.

In most cases installing an unsigned driver is acceptable and many Windows drivers are unsigned. Given that UPDD has been signed it is proven to be a driver of good quality. However, in some cases it is required to supply signed drivers, especially for use on complete systems that need all components to be Microsoft approved so that the complete system can carry the 'Designed for Windows' logo.

Signing procedure

In very basic terms the WHQL/WHC compatibility tests are downloaded and installed and are run against a driver and controller combination. The tests have to be undertaken on a system that has passed WHQL/WHC system test and will not cause any conflicts during testing. A variety of specialised USB hubs, that conform to USB spec 1, 2 and 3, have to be utilised during the test. Tests are performed for both 32 and 64 bit drivers.

The tests generate logs which are processed and are submitted for review and approval. They can only be submitted by companies that have obtained a VeriSign Class 3 code-signing ID. Once approved a .cat file, containing the digital signature, is returned for distribution with the driver and controller combination.

Thereafter, the operating system performs signature detection whenever an INF file is referenced to install hardware from a device class that is subject to signature detection: that is, during any Plug and Play operation, when the user runs the Add New Hardware wizard in the Control Panel, and so on.

The system always installs the driver that is the closest match for the hardware, whether or not that driver is signed; however, given drivers of equal rank, the system installs the signed driver rather than the unsigned driver.

During driver installation, Windows compares the hashes contained in the driver's CAT file with the computed hash of the driver binaries to determine whether the binaries have changed since the CAT file was created. If a driver fails the signature check or there is no CAT file the driver is considered unsigned. Given this, once signed, no changes can be made to any binaries used in the signing process. For this reason most companies that offer signed drivers also offer the unsigned drivers with the latest development.

Given the level of knowledge required to undertake the signing procedure many companies use a third party WHQL services company to undertake this work.

Signing service

Starting with UPDD 4.1.6 we now offer an in-house facility to sign UPDD with a specific controller. Since March 2007, Microsoft requires that all WHQL logo and signature tests are performed with the Windows Logo Kit (WLK) and Driver Test Manager (DTM). Setting up DTM is no small task; the DTM system is a dedicated network of servers and client machines running in various operating systems. Our DTM laboratory is set up and ready to test pointer device class devices. Windows 8 WHC tests have introduced new hardware and software testing requirements.

As part of our production system we will maintain the digital signature files associated with each signed controller and UPDD build. This will allow us to offer signed drivers where available for specific controllers and yet continue further UPDD development.

- The new UPDD 4.1.x design has minimized the code used in kernel mode (the signed element of the driver) allowing us to add further functionality and maintain the UPDD utility programs outside of the signing process. We are hopeful that very few, if any, changes will be made to the kernel element thus maintaining the signed certification across new driver releases.

Costs

The cost of this service is GBP 2500.00 and covers signing the driver and testing – should issues arise there may be additional cost especially analysis of controller faults. The cost covers the initial 2 to 4 days needed to perform the tests against a supplied controller, monies paid to Microsoft as part of the acceptance process and digital signature generation. Controller specific tests are also run as part of the testing procedure and any failures with the pointer device hardware will prohibit the allocation of a digital signature.

Before requesting a UPDD digital signature the hardware must pass all Microsoft hardware compatibility tests. If a failure occurs due to a compatibility error then we will provide a report on the nature of the error and will perform further tests free of charge, so long as the retest is within one week of the original test.

We can perform a compatibility testing service for GBP 1500, in which we will run tests on a single platform (usually Windows 32 bit) and provide results as many times as required in a 2 week period. In this case, assuming the final test run is successful this can be used for a WHQL submission and submission cost will be GBP 1000.

It is important to note that the signature is for a specific kernel driver version and in the event that a later kernel driver version is required then a new digital signature will be required. The same charges will apply.

Contact

For further information or technical assistance please email the technical support team at technical@touch-base.com