Using the Insyde Win Flash Package

12/20/2011
Insyde Software Corp.

insyde

Disclaimer

Insyde Software Corp. provides this document and the programs "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose.

This document could contain technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in future revisions of this document. Insyde Software Corp. is under no obligation to notify any person of the changes.

The following trademarks are used in this document:

Insyde is a registered trademark of Insyde Software Corp.

All other trademarks or trade names are property of their respective holders.

Using the Insyde Win Flash Package

The Insyde Win flash package can update your BIOS in a secure update mode. The package is only available for specific BIOS and hardware. The BIOS must support capabilities that include ROM part lock down and certificate check. The below will describe:

- The package version format
- The process of generating a BIOS image with digital signature
- How to enter secure update mode

Insyde Win Flash Package:

The Insyde Win flash package contains two sub-packages. One is the Windows flash utility package and the other is the security flash package.

a. **Windows flash utility package**: this package is the same as the non-secure Windows flash utility package, and there are no extra or removed components in this package. This same Windows flash utility can support un-secure flash mode and secure flash mode. This Windows flash utility will auto-detect whether or not the BIOS contains a secure BIOS signature. If the secure BIOS file exists, the Windows flash utility will invoke secure update mode. Otherwise, the Windows flash utility runs in an un-secure update mode. Please refer to the Windows flash user guide to know what functions are supported and the release notes in the Windows flash utility package for release information.

b. **Security flash package**: The package folder is used in secure flash mode. The folder contains a signature packager, QA certificates, and related usage guide. Complete instructions on generating a secure BIOS image are included in the Security flash package usage guide. The secure BIOS image consists of a BIOS image, a configuration file (platform.ini), UEFI flash utility and a digital signature. To understand how to enable the secure update mode please see the procedure “How to generate secure BIOS image” below.

Flash package name and version:

This section describes how to identify the secure flash package version. The whole package includes both the Windows flash utility and security flash.

a. The package version contains a major version, a minor version, a serial number and a build number.
   The version format is mm.nn.ss.bb
   Example: InsydeWinFlashPackage v1.00.01.00
   mm: Major version- If there is a major change, the version will be increased and the minor, serial and build number will be reset. The range is 00~99
   nn: Minor version- If there is a minor change, the version will be increased and serial number and build number will be reset. The range is 00~99
   ss: Serial number- If there is any change, the version will be increased and the build number will be reset. The range is 00~99
   bb: Build number- The version is for internal reference. The range is 00~99.

b. The Windows flash utility version contains a major version, a minor version and a build number.
   The version format is mm.nn.bb
   Example: InsydeFlashWin5.08.00
   mm: Major version- If there is a major change, the version will be increased and the minor and build number will be reset. The range is 00~99

nn: Minor version- If there is a minor change, the version will be increased and the build number will be reset. The range is 00~99.

bb: Build number- The version is for internal reference. The range is 00~99

c. Security flash version: contains a major version, a minor version, a serial number and a build number.
The version format is mm.nn.ss.bb
Example: SecurityFlash1.00.01.00
mm: Major version- If there is a major change, the version will be increased and the minor, serial and build number will be reset. The range is 00~99
nn: Minor version-If there is a minor change, the version will be increased and serial number and build number will be reset. The range is 00~99
ss: Serial number- If there is a change, the version will be increased and the build number will be reset. The range is 00~99
bb: Build number- The version is for internal reference. The range is 00~99

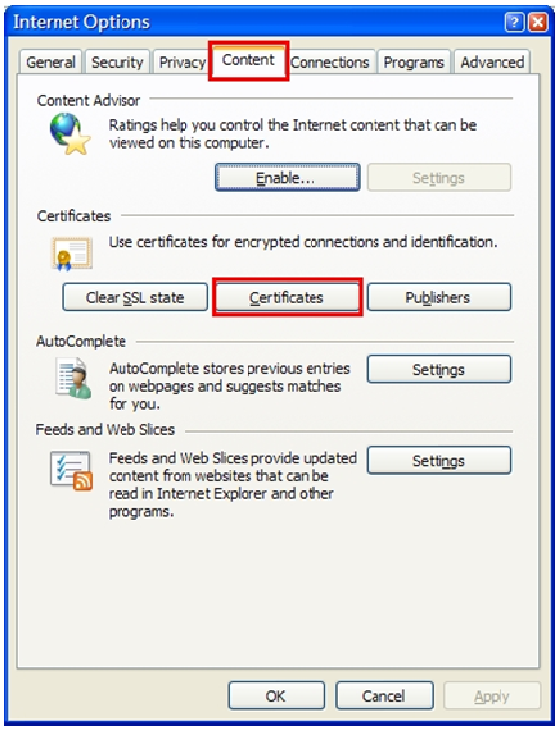
How to generate a secure BIOS image:

1. Prepare applications package.
   Get the InsydeWinFlashPackage and Microsoft sign tools.

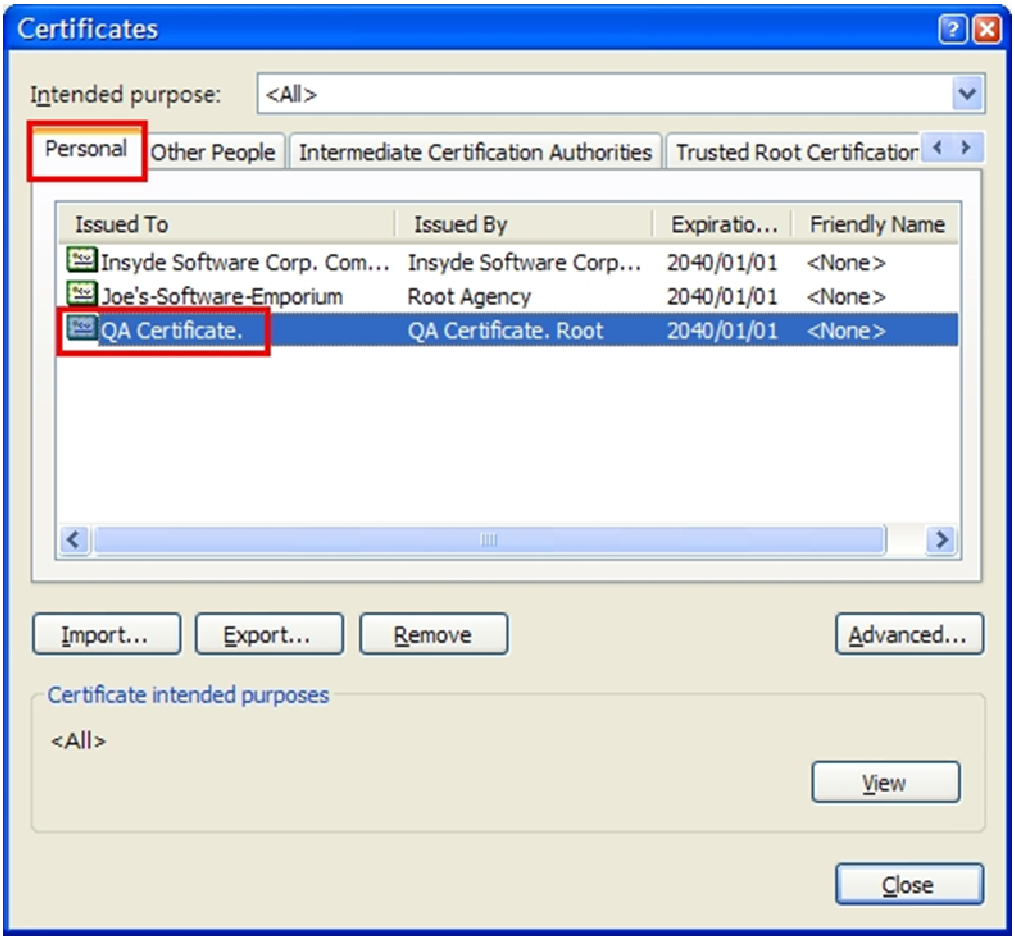
2. Unzip the packages to the folder, for example, C: \InsydeFlash and C:\SignTools. Then copy Microsoft sign tools to C:\SignTools folder.

3. Install the certificate:
   Follow the “QA Certificate Installation Guide.doc” (in security flash package) to complete the installation.

4. Check the installed certificate:
   (1) Run IE, open [Tools] -> select [Internet options]
   (2) select [Content] Tab -> press [Certificates] button

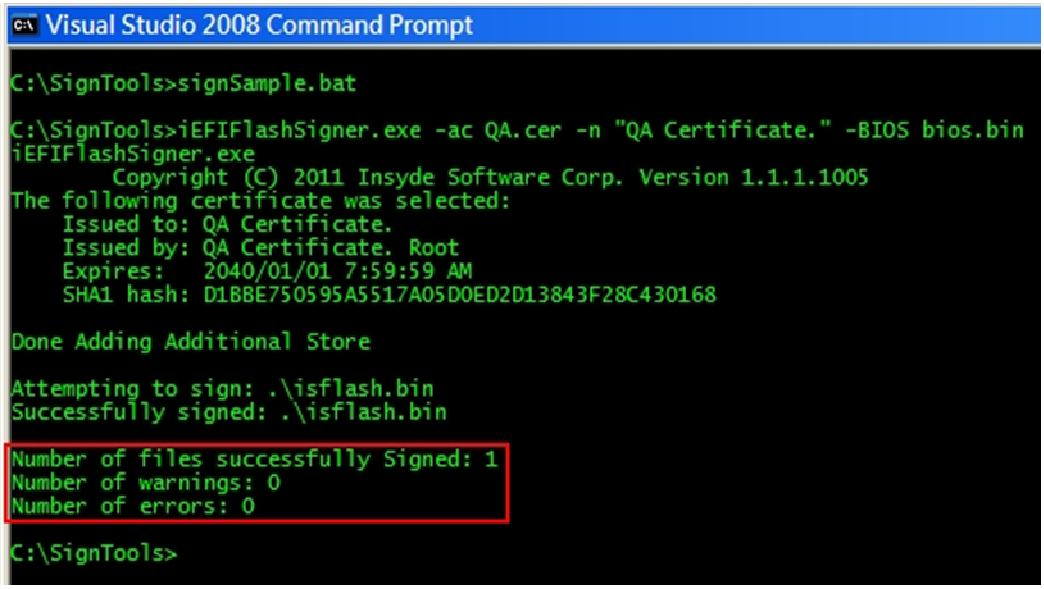


(3) click [Personal] tab, and check if QA certificate exists.



5. Sign package.
   (1) Copy the BIOS binary to the C:\SignTools folder.
   (2) Follow the “iEFIFlashSigner User Guide.txt” (in security flash package) to complete the sign package.

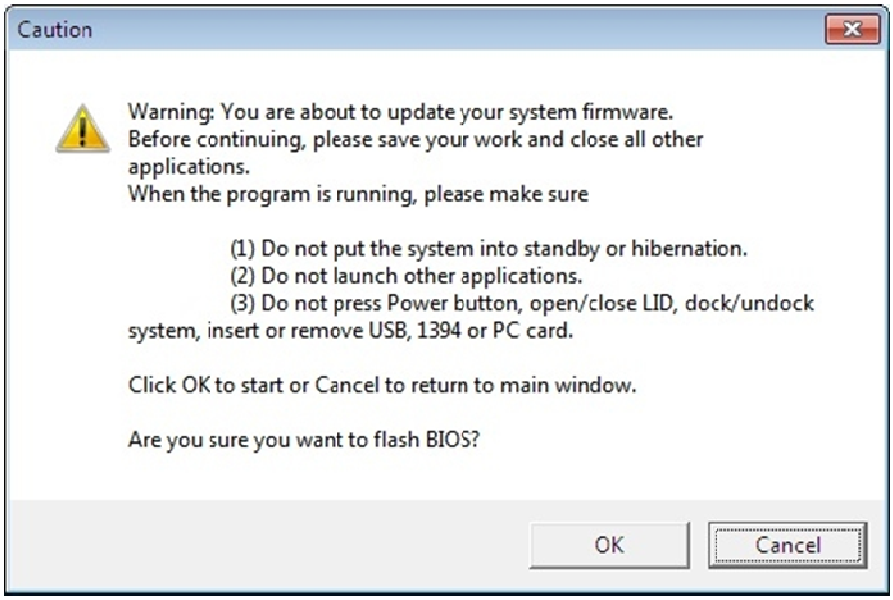
(3) If everything is ok, you will get a signed binary named “isFlash.bin” in C:\SignTools folder.



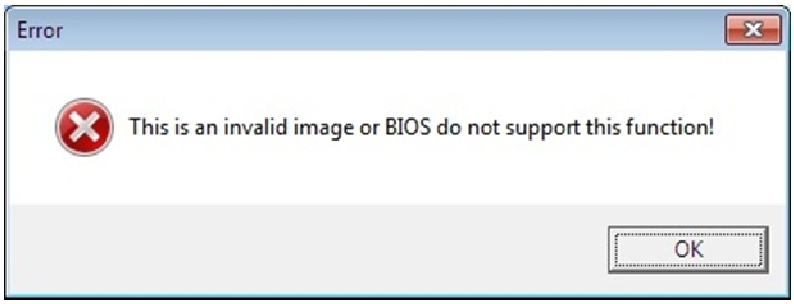
How to launch secure flash mode and then update BIOS:

1. Copy the signed binary “isFlash.bin” into the C:\InsydeFlash folder.
2. You can rename the secure BIOS filename and set the filename in platform.ini
   [FDFile] FileName=SecureBIOSFilename
3. Run InsydeFlash.exe, and the application will check if the secure BIOS image exists.
   Yes -> launch as secure flash mode.
   No -> launch as normal flash mode.
4. In secure flash mode, eventually the apps will call IHISI, and get BIOS support secure flash type:
   0: update by doing an S3.
   1: update by doing a re-boot.
   2: update by doing a shutdown.

If everything is OK, you will see the Caution dialog window shown below. Press the [OK] button to update the BIOS.

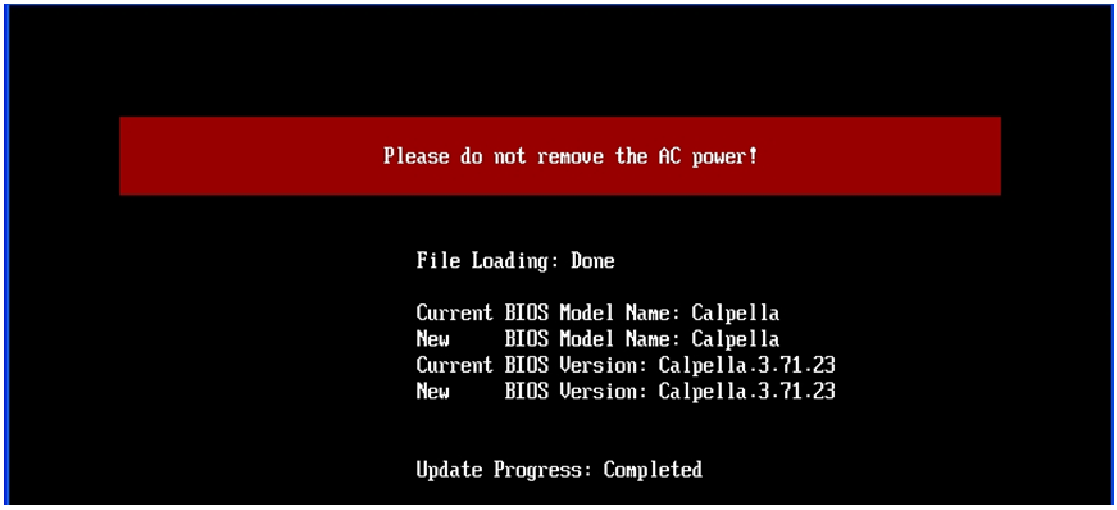


If anything is wrong, you will see the following error message. Press the [OK] button to go back to Windows.



5. After resume from (S3, re-boot or shutdown) the BIOS will do a security check. If the security check fails, the following error message will be shown and prompt the user to restart the system.

6. When the security check passes, the BIOS will launch isFlash to perform the update BIOS process.



7. If everything completes successfully, the system will restart.