Using the Insyde Shell Flash Package

05/28/2013
Insyde Software Corp.

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 Shell Flash Package

The Insyde Shell 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 Shell Flash Package:

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

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

*** Attention:**

On secure boot supported system, the shell flash utility (isflashx64.efi) must be signed via iEFIFlashSigner.exe. Please refer "ReadMe.txt" in security flash package to know how to sign by iEFIFlashSigner.exe.

b. **Security flash package**: The package folder is used in secure flash mode. The folder contains a signature packager 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 Shell 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: InsydeShellFlashPackage 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 Shell flash utility version contains a major version, a minor version and a build number.
The version format is mm.nn.bb
Example: InsydeFlashShell1.2a.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 0a~9z.
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 get a key:

1. Purchases key from third-party, like VeriSign.
2. Use Microsoft makecert.exe (in Windows 8 SDK) to generate key pair.

a. Use command

```
makecert -r -cy authority -n "CN=Certificate_Test" -a sha256 -len 2048 -sv CerTest.pvk CerTest.cer
pvk2pfx -pvk CerTest.pvk -spc CerTest.cer -pfx CerTest.pfx
```

“Certificate_Test” is the subject name of the key, it can be changed as you want.

b. Use MakeKey.bat in security flash package

c. Related links
Windows 8 WDK (Windows Driver Kit)
http://msdn.microsoft.com/en-US/windows/hardware/hh852362
makecert.exe
http://msdn.microsoft.com/en-US/library/bfsktky3(v=vs.110).aspx
pvk2pfx.exe
http://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx

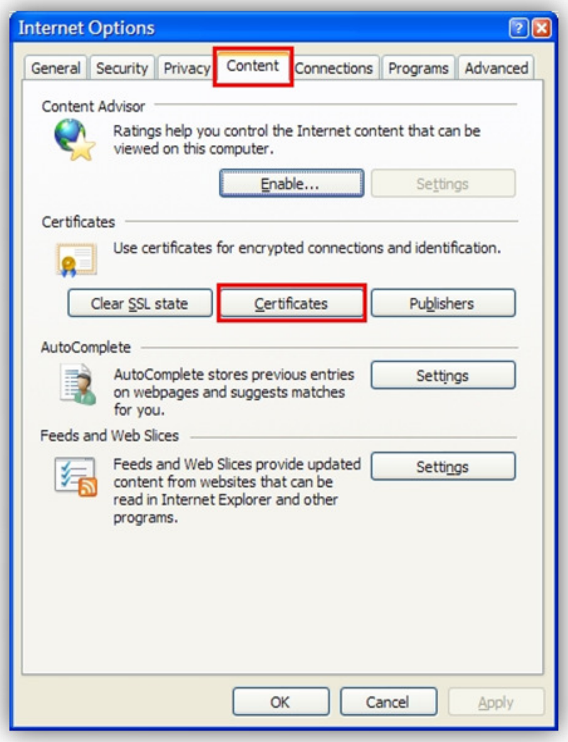
How to generate a secure BIOS image:

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

2. Unzip the Shell flash and security flash 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.pdf” (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



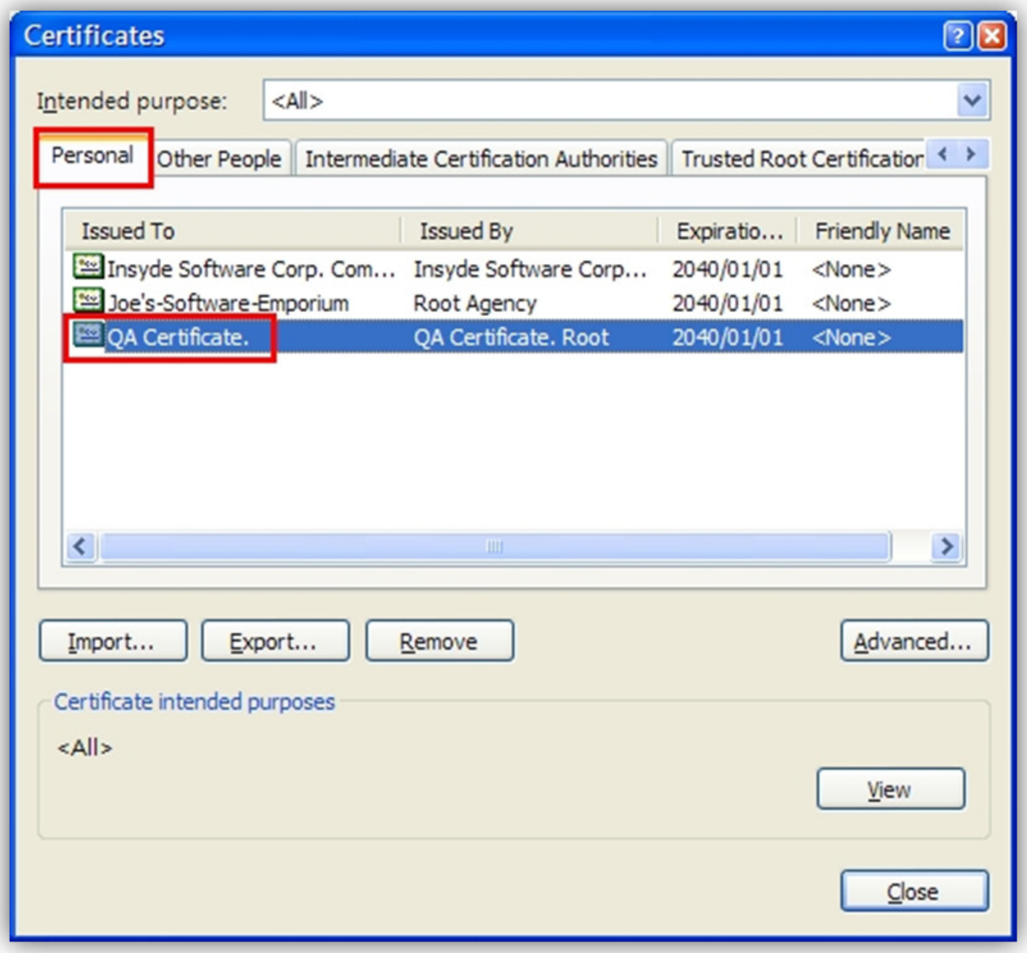
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

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

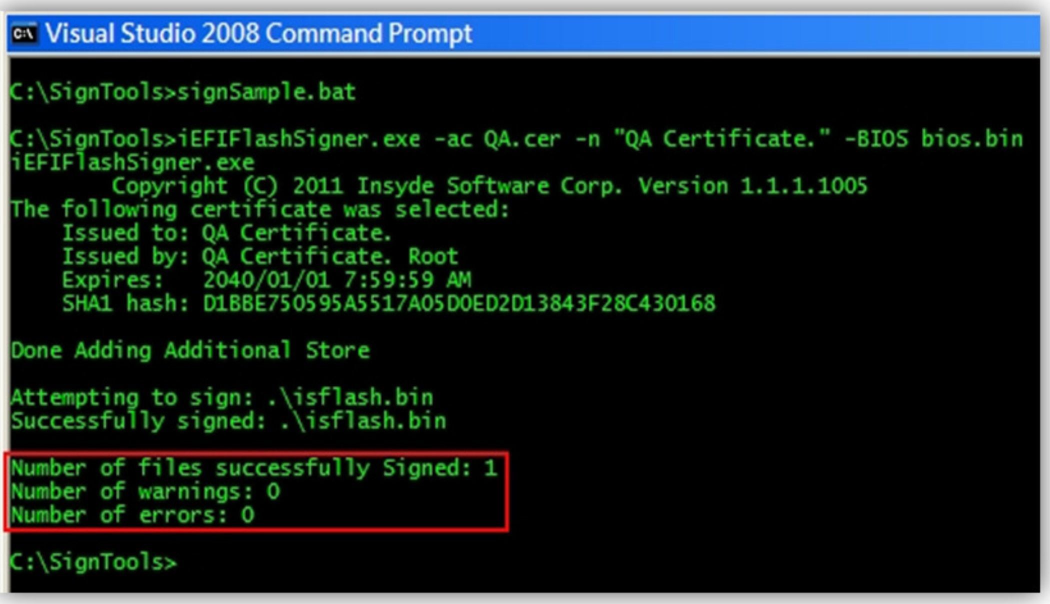

Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Insyde Software Corp. Com...	Insyde Software Corp...	2040/01/01	<None>
Joe's-Software-Emporium	Root Agency	2040/01/01	<None>
QA Certificate.	QA Certificate. Root	2040/01/01	<None>

<All>

5. Sign package.
   (1) Copy the BIOS binary to the C:\SignTools folder.
   (2) Follow the “ReadMe.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.



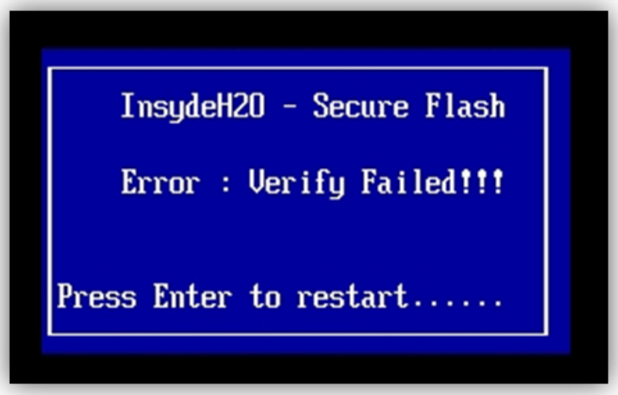
```
C:\SignTools>signSample.bat

C:\SignTools>iEFIFlashSigner.exe -ac QA.cer -n "QA Certificate." -BIOS bios.bin
iEFIFlashSigner.exe
        Copyright (C) 2011 Insyde Software Corp. Version 1.1.1.1005
The following certificate was selected:
    Issued to: QA Certificate.
    Issued by: QA Certificate. Root
    Expires:   2040/01/01 7:59:59 AM
    SHA1 hash: D1BBE750595A5517A05D0ED2D13843F28C430168

Done Adding Additional Store

Attempting to sign: .\isflash.bin
Successfully signed: .\isflash.bin

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0

C:\SignTools>
```

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 as you want.
3. Run isflashx64.efi isFlash.bin, and the application will check is the image a secure BIOS.
   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.
   3: update by doing nothing (return to OS).

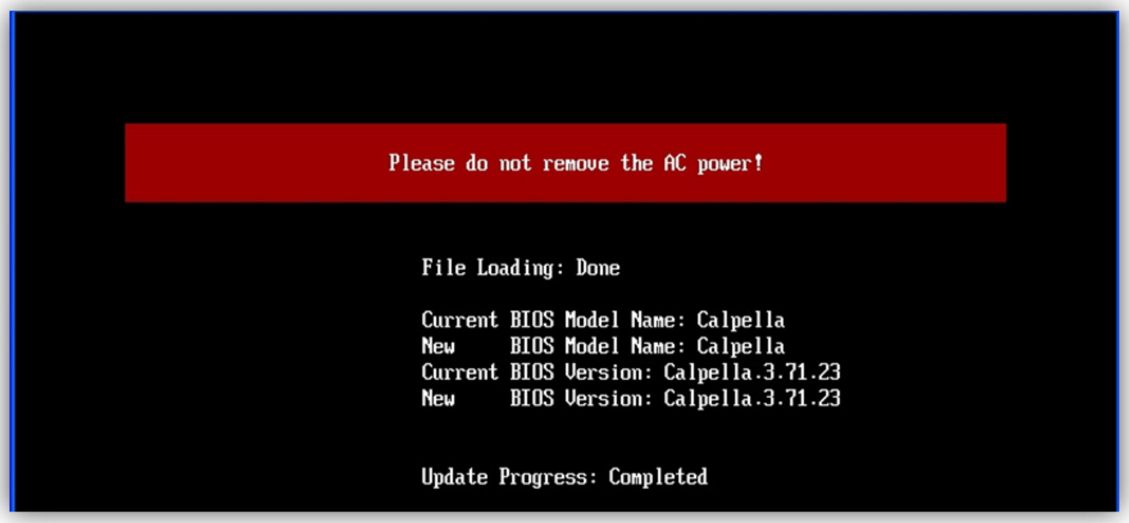
If everything is OK, it will reset and start to update the BIOS.

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.



```
    InsydeH2O - Secure Flash

    Error : Verify Failed!!!


Press Enter to restart......
```

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



```
                  Please do not remove the AC power!

File Loading: Done

Current BIOS Model Name: Calpella
New     BIOS Model Name: Calpella
Current BIOS Version: Calpella.3.71.23
New     BIOS Version: Calpella.3.71.23


Update Progress: Completed
```

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