AMI Signing Server

Managing UEFI Secure Flash and Secure Boot

AMI Signing Server provides a single point solution for verifying the authenticity and integrity of BIOS updates and protection from modification outside of the secure update process

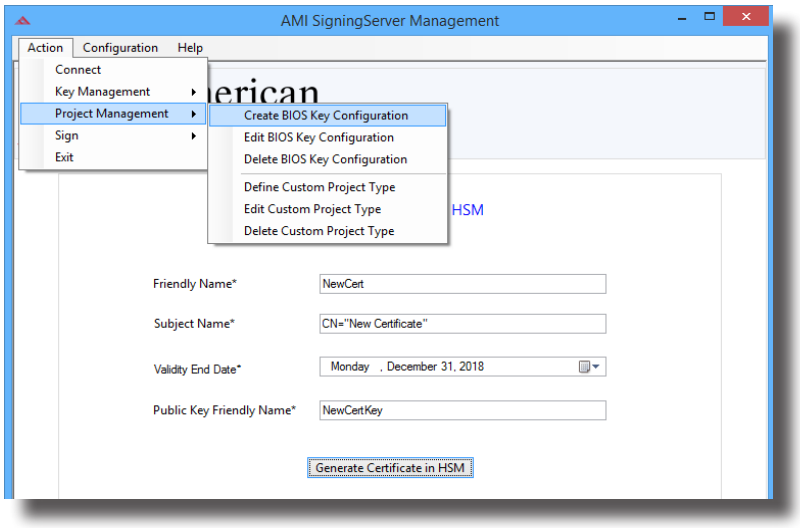
AMI Signing Server takes the complexity of key management and distribution, hardware setup and configuration, and the actual signing process to provide a manageable solution, shielding OEMs from the headaches caused by BIOS security concerns.

BIOS IMAGES AND SECURITY

With the AMI Signing Server solution, the signing process is separated from the BIOS build process, with the actual signing process occurring on a dedicated server. A signing client is available and handles the secure communication to the signing server using message security, making the signing process as simple as calling a command line tool. This allows for images to be signed outside of the build process. The private keys are maintained only on the dedicated signing server, so that there is no risk of them being compromised.

SECURE FLASH AND RECOVERY

Secure Flash Update and Recovery is designed to follow NIST publication 800-147 recommendations to protect BIOS firmware from being updated by unauthorized processes and have the new BIOS image verified for integrity and authenticity before update.



This solution offers a process of ensuring the authenticity and integrity of BIOS updates, and serves as a mechanism for ensuring the BIOS is protected from modifications outside of the secure update process.

Signing Server ensures a BIOS update image is generated by an authorized source and is unaltered in transit to a client machine. All updates to the BIOS shall either go through an authenticated BIOS update process or use a secure local update process.

The Aptio V ROM images are signed and distributed in the form of generic UEFI capsule package. The Aptio V capsule includes a header, digital signature block, ROM map information and the actual ROM image. The ROM map section is used to exclude ROM blocks from the signature.

HIGHLIGHTS:

- **Signing process is separated from the build process**
- **Private keys are not required to be distributed to all build systems**
- **Single point solution with remote access from any number of systems**
- **Easily deployable in manufacturing environments**
- **The keys used for signing need not be duplicated for each BIOS image.**
- **Key pairs and certificates are stored using Microsoft® key store**
  - **More secure than storing on disk**
- **Provides different clients that can be used based on differing requirements:**
  - **Web admin client**
  - **Script based client**
  - **GUI client**
- **Can be extended with additional clients as needed**
- **Secure authentication for users using the Microsoft Active Directory before granting access to signing process**
- **Supports different user roles.**
  - **Signing Administrator**
  - **Project Manager**
  - **Signing User**
- **Can be integrated with an HSM device, and the BIOS can be signed using the HSM**
- **Provides support to maintain different keys for signing different platforms**
- **Detects the required signature format from the input ROM, and hides the complex signing process from the user**

SIGNING WITH BIOS IMAGE FROM THE BUILD SYSTEM

Signing the ROM images locally on the build machine requires the following assets to be available on the build system:

- ROM image to be signed
- Cryptographic key required for signing
- The ROM map that defines the different regions in the ROM
- Signing tool, which signs the ROM image with the key

AMI SIGNING SERVER ROLES

- Signing Administrator: responsible for domain configuration
- Project Manager: responsible for all key management
- Signing User: perform sign operations only

The membership of each group is based on Active Directory groups for easy management of the user roles.

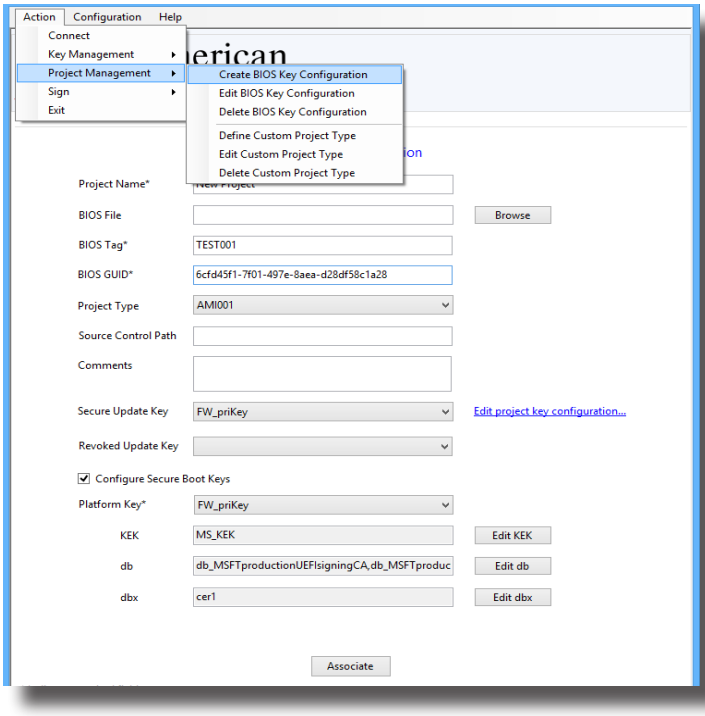
GENERATE OR IMPORT KEYS

The AMI Signing Server supports generating keys. But for greater security, it supports importing existing keys to the server, such as those keys generated by an HSM or purchased from a CA. The following key types can be imported:

- DER encoded RSA key
- PFX file (PKCS #12)
- HSM key

CREATE PROJECT TO ASSOCIATE BIOS WITH KEY

Signing Server offers project management functionality for keys that are generated/imported. All keys that have been generated or imported will be available for easy association with a platform project.



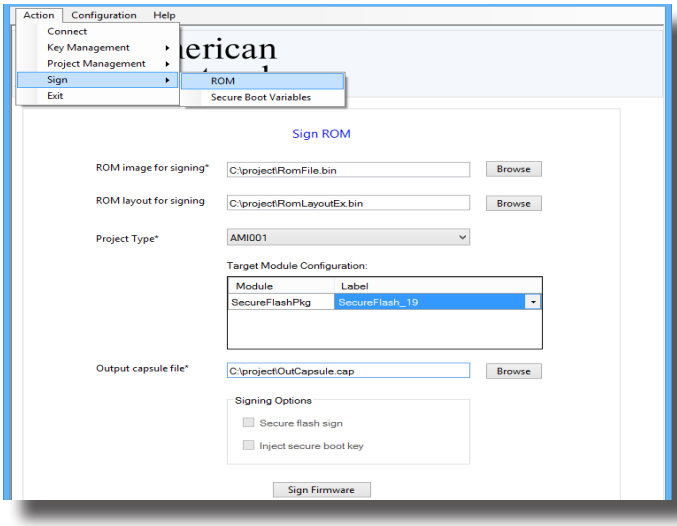
Signing Server Project Manager supports:

- Multiple sets of keys for signing multiple BIOS projects
- Secure Boot

ROM IMAGE SIGNING

The AMI Signing Server detects the required signature format from the input ROM and hides the complex signing process from the user.

The ROM signing process can be performed from a GUI client or scripted from a command line client. This makes it possible to integrate the signing step into the BIOS build process.



KEY MANAGEMENT

Key management features include generating new keys, importing existing keys to the server, and exporting the keys available in the server or deleting the keys from the server.

SUPPORTED OPERATING SYSTEMS

Server Machine

- Windows 7 SP1 Professional/Enterprise/Ultimate
- Windows 8.1/10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

Client Machine

- Windows Vista SP2
- Windows 7 SP1
- Windows 8.1/10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

American Megatrends

American Megatrends Inc. | ami.com
5555 Oakbrook Parkway, Bldg. 200
Norcross, GA 30093 | 770.246.8600

AptioV

For more information: https://ami.com/