AMI CLEFS™
Cloud Environment for Firmware Signing

American Megatrends

A secure, on-demand cloud-based hardware security module (HSM) platform that provides a wide range of signing and key management services through a simple online portal

Private key management and firmware signing for UEFI and BMC firmware is seen as a growing potential vector of harm, both for manufacturers and their end users. The inappropriate storage of keys, when stored together with the source code they protect, is increasingly a key contributor to this threat - since an attack on the protected code can compromise its key as well.

Fortunately, use of a dedicated signing server, called a Hardware Signing Module or HSM, can isolate and protect keys from such an attack. Placing an HSM in the cloud adds an additional layer of security for vulnerable keys. But the deployment of HSM devices for key management is a complex and expensive undertaking, requiring significant investment in equipment, dedicated personnel and integration into the IT infrastructure in order to make them work.

THE SOLUTION

American Megatrends (AMI), the industry's trusted name in UEFI and BMC firmware, delivers secure, reliable and simple cloud-based signing services to its OEM and ODM firmware customers with its new AMI CLEFS™ Cloud Environment for Firmware Signing. This is an on-demand, subscription-based service available to customers of both UEFI and BMC firmware from AMI.

Who else but AMI - an industry leader that understands firmware security intrinsically - working together with Gemalto, a trusted, leading provider of data protection, can deliver a secure and trusted mechanism used to protect cryptographic keys and secrets that is both extremely economical and utterly reliable?

AMI CLEFS is a cloud based HSM platform that provides a wide range of signing and key management services through a simple online portal. With AMI CLEFS, key signing is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain. Simply click to deploy the necessary protection, provision keys and get usage reporting. AMI CLEFS offers a one-stop source code protection solution with a menu of security applications ranging from key security to digital signing and ensuring the root of trust.

KEY FEATURES

- **Integration of purpose-built tools from AMI add value and deepen functionality**
- **Isolate keys and signing operations from firmware source code**
- **Automate costly, manual key lifecycle control and processes**
- **Auto scale as private key management needs grow over time**
- **Proven reliability, delivered by an industry leader in firmware and security**

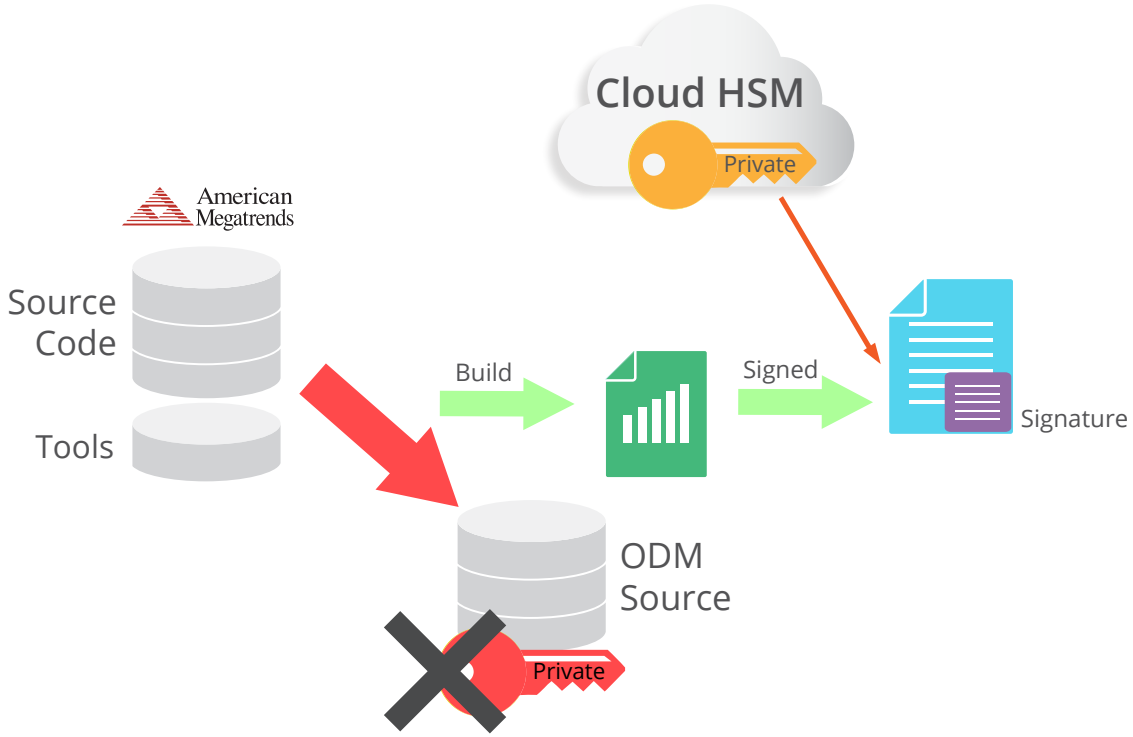
THE VALUE AND BENEFITS

Most importantly, the keys are kept secure and hidden from AMI, the service provider. The key ID generated by the HSM is stored securely in the cloud, with only the customer having access to this information. In this way, AMI CLEFS delivers truly secure and reliable firmware signing, along with integrated tools from AMI that make the service easy to use.

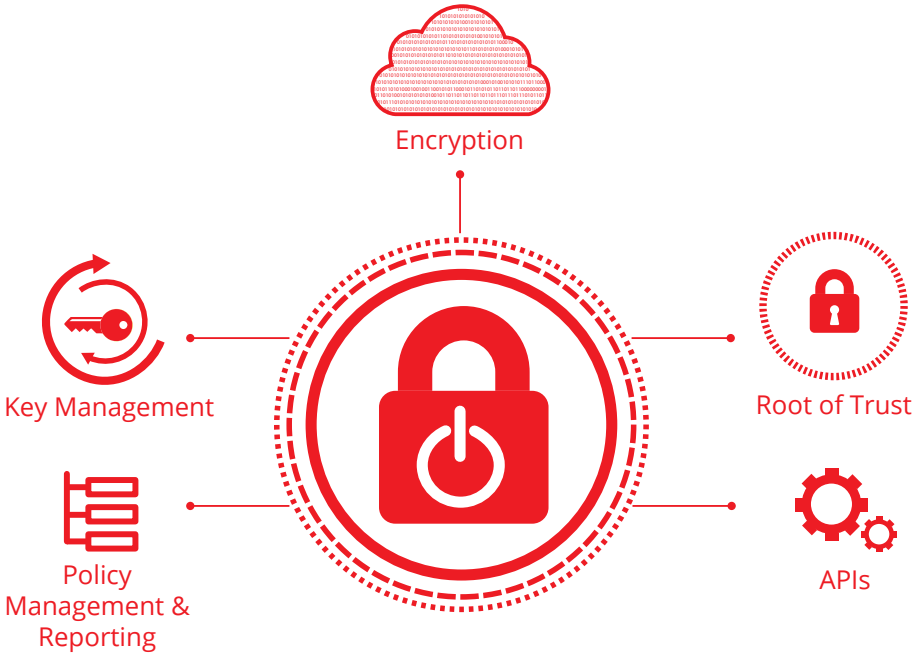
AMI CLEFS is also scalable, with keys being sold in tiles of a fixed number of keys per tile. Since old keys for old BIOS versions need to be kept while new keys are created for new devices, AMI CLEFS customers can simply add additional tiles as needed.

Moreover, AMI CLEFS delivers tremendous benefit to end users. OEM and ODM customers can take advantage of pay-as-you-go, subscription pricing with no upfront capital investment in hardware, software or dedicated personnel. Its flexible pricing model means that additional key management capacity is available at the click of a button to support the maintenance of legacy keys for previous versions of firmware.

This service is also easily integrated into the customer's existing key management workflow. AMI CLEFS includes preconfigured APIs and purpose-built tools to quickly deploy these secure key management services to protect vital firmware security keys.



Instead of storing source code together with the keys that protect them, AMI CLEFS separates source code and keys, removing the potential for the keys to be compromised. Private keys are used by the HSM to sign the firmware image produced by the build server, keeping the server that stores firmware source code free from sensitive information, in order to secure and protect images built from that source code.



Note that this is a separate contract/agreement for services aside from existing customers' BIOS or BMC source code agreements with American Megatrends. Interested parties should contact the AMI Software Sales Team at 1-800-828-9264 for more information.

American Megatrends

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