thalesgroup.com

THALES

Using AMI CLEFs™ with SafeNet Data Protection on Demand or SafeNet Luna HSMs to Secure your BIOS and Firmware

The Challenge: Enabling Easy to Use, Secure Code Signing

Code signing is critical to digital security, because it guarantees where the code comes from and that it has not been modified or corrupted since release. Code signing helps prevent firmware from being manipulated in an unauthorized manner, and it enables safe firmware updates, because they can be digitally signed by an authorized party.

The burden to sign code often falls to software developers, which may pose unique challenges as they do not specialize in security. Consequently, code signing keys can wind up in vulnerable network locations, such as workstations or build servers.

The Solution

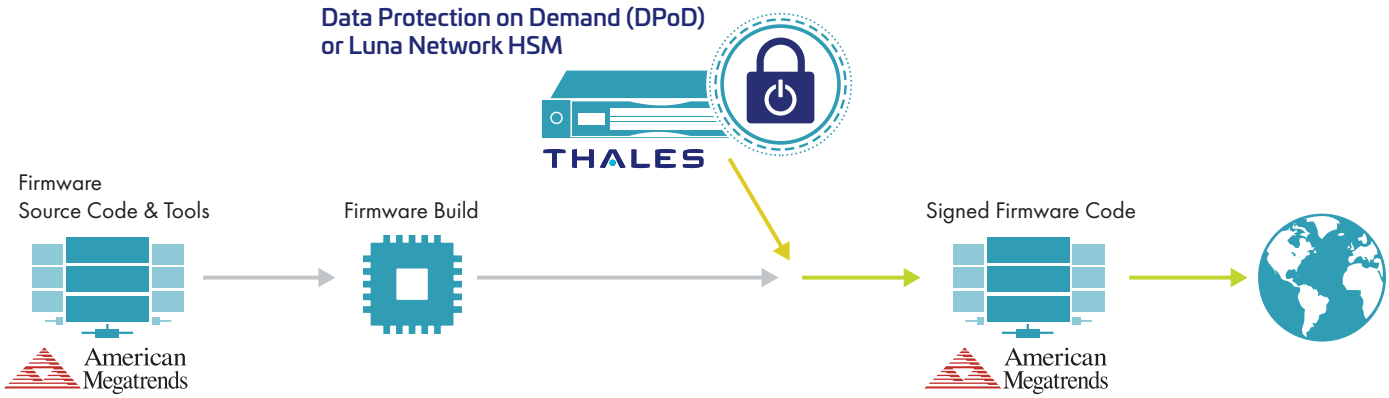
American Megatrends International (AMI) has partnered with Thales CPL to combine AMI's Cloud Environment for Firmware Signing (CLEFS™) and Thales' SafeNet Data Protection on Demand (DPoD) Hardware Security Module (HSM) services to offer an on-demand, subscription-based code-signing service available to customers of both UEFI and BMC firmware from AMI.

The CLEFS solution is a cloud-based HSM platform, which enhances code signing security by isolating keys and signing operations from certificate authorities, host platforms, and operating systems. It provides a wide range of scalable signing and key management services through a simple online portal, secured by DPoD.

With Thales DPoD and AMI CLEFS, code 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 reports. 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.

As part of this solution, Thales offers two FIPS 140-2 Level 3 HSM products that can generate and store the server keys, providing flexibility for cloud-based, hybrid/multi-cloud or on-premises private key generation, storage and protection.

- Data Protection on Demand (DPoD) HSM on Demand service is a cloud-based hardware security module (HSM) that can be deployed within minutes with no need for specialized hardware or associated skills. This subscription based HSM solution securely stores the keys in the cloud and keeps them hidden from AMI and Thales; only the customer has access to their keys.
- For customers that prefer or are required for compliance to keep their private keys local, Thales offers Luna HSMs to store, protect, and manage sensitive cryptographic keys on-premises. These tamper resistant HSMs provide high-assurance key protection within an organization's own IT infrastructure.



Key Benefits

- Delivers proven compliance, reliability and ease of use
- Customers maintain control of their signing keys at all times (separate from AMI or Thales)
- Isolates keys and signing operations from firmware source code
- Reduces cost through automating manual key lifecycle control and processes
- Is highly scalable to meet performance demands
- Subscription-based pricing requires no up-front capital investment

About American Megatrends International (AMI)

American Megatrends International (AMI) is an American hardware and software company, specializing in PC hardware and firmware. AMI is the world's largest BIOS firmware vendor, with AMIBIOS® and Aptio® deployed in a high proportion of all computers worldwide. AMI's extensive product line includes Aptio and AMIBIOS system software and firmware, MegaRAC® remote management software and firmware, Embedded Controller (EC) firmware, as well as a wealth of design, testing, validation and engineering services for system manufacturers. AMI maintains a 90% share of the firmware and bios market, and counts among its customers the leading technology companies in the world.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroupl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com