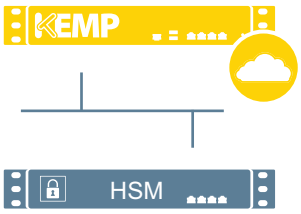
# Hardware Security Module

Solution Brief




## Overview

KEMP's LoadMaster supports the use of network attached Hardware Security Modules (HSM) for enhanced protection of private key material. The operational scenarios where HSMs may be deployed include Government (FIPS 140-2), security sensitive sectors (such as financial institutions), regulated environments (PCI-DSS) and secure key storage in public clouds. A HSM provides a physically secure environment for the storage of cryptographic keys and also executes cryptographic functions such as encryption (signing) and decryption. Kemp LoadMasters use attached HSMs to perform the private key cryptographic operations required to support a TLS (SSL) handshake.

## Private Key Protection

For Government agencies and their suppliers, the FIPS 140-2 standard from the National Institute of Standards and Technology (NIST), defines the level of physical security and cryptographic algorithm strength to be implemented in security products. The FIPS 140-2 standard defines four increasing, qualitative levels of security (level 1 to level 4) based on an assessment of eleven design and implementation areas. At levels 3 and 4, a HSM goes beyond just tamper evidence and provide mechanisms for tamper protection. At these levels of protection, the HSM can detect unauthorized access or excessive environmental changes and react by zeroing any key material stored.

## FIPS 140-2 on Virtual and Cloud

KEMP LoadMasters support the use of HSM appliances to deliver FIPS 140-2 compliance for load balancing deployments on virtual, physical, bare-metal and cloud platforms. As virtualization becomes the de-facto model for solution delivery, FIPS 140-2 compliance may become more challenge. However with LoadMaster you can continue to employ proven HSM platforms for key management and operations while using virtualized LoadMasters on your virtualization platform. As networked HSM appliances are supported on all our platforms you can also deploy physical LoadMaster appliances or leverage your preferential hardware platform with bare-metal LoadMaster.

Public or shared infrastructure cloud offers many benefits for Government agencies but deployments in such environments may also pose challenges regarding key management and protection. With LoadMaster's network HSM support, the HSM can be deployed in a secure environment such as an on-premise data center while the application and load balancers can be deployed in the cloud.