Trusted Cyber Technology

THALES

DoD STIG Compliance

Virtualization-Based Security - External Key Management

Authority to Operate (ATO) on the DoD Information Network (DoDIN)

Thales Trusted Cyber Technologies (TCT) is a U.S. based provider of government high-assurance data security solutions. Our mission is to provide innovative solutions to protect the most vital data from the core to the cloud to the field. Thales TCT assists Department of Defense (DoD) customers in compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) in order to maintain Authority to Operate (ATO) on the DoDIN. Recent updates to the Windows Server 2019 Security Technical Implementation Guide will require customers in a VMware environment to implement an External Key Manager. These updates apply to Windows 2016 and Windows 2019 Server environments.

- Windows Server 2019 domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use
- Windows Server 2019 must be running Credential Guard on domain-joined member servers

These DISA STIG updates require enabling Credential Guard to meet DoD compliance. Credential Guard uses virtualization-based security within Windows to isolate and store secrets and user credentials so that only privileged system software can access them. TPM functionality in addition to UEFI with Secure Boot, allows Systems Adminstrators to enable Credential Guard on Windows 2016/2019 servers.

TPM is a hardware level crytpo processor to secure the generation of cryptographic keys. For virtualized server environments, this functionality is provided in software via a virtual TPM (vTPM). VMware's vSphere 6.7 adds support for TPM 2.0 hardware devices for ESXi hosts and also introduces virtual TPM (vTPM) 2.0 for Virtual Machines, ensuring integrity for both the hypervisor and the guest operating system (OS). VMware and the vSphere architecture provide this capability utilizing the following components:

- Implementation of Virtual Trusted Platform Modules (vTPMs) in a vSphere environment requires an external Key Management Server (KMS) utilizing KMIP
- Virtual Trusted Platform Modules (vTPMs) establish trust by enabling "Secure Boot" technology emulating a hardware based TPM
- vTPM data is securely stored in the virtual machine .nvram file, encrypted using VM encryption

NIST Special Publication 800-57 Part 2 Revision 1 recommends Moderate and High impact levels require a cryptographic module validated at FIPS 140 Level 3 or higher. Specifying Utilizing a FIPS 140 Level 1 cryptographic module could adversely affect the organization's ability to continue to engage in mission-critical processing and communications partnerships. FIPS requirement impact level of customer data (levels 1-3) and are deployed with high availability to support mission resiliency.

Thales TCT's Enterprise Key Manager is a VMware-certified KMS that protect vTMPs' cryptographic keys in an external hardware appliance. Thales TCT's Enterprise Key Manager The Data Security Platform also supports an embedded hardware root of trust utilizing a FIPS 140-2 Level 3 Luna for Government hardware security module. Developed for U.S. Government use, it is manufactured, sold, and supported in the U.S. exclusively by Thales TCT.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

For more information, visit www.thalestct.com