Trusted Cyber Technologies

THALES

Thales Trusted Cyber Technologies Solutions for Cybersecurity Maturity Model Certification (CMMC)

White Paper

Table of Contents

CMMC Summary

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense's (DoD) newest verification mechanism designed to ensure that cybersecurity controls and processes adequately protect Controlled Unclassified Information (CUI) that resides on Defense Industrial Base (DIB) systems and networks. It builds upon Defense Federal Acquisition Regulation Supplement (DFARS) and National Institute of Standards and Technology (NIST) frameworks by requiring every contractor to be audited and certified by a third party auditor.[1]

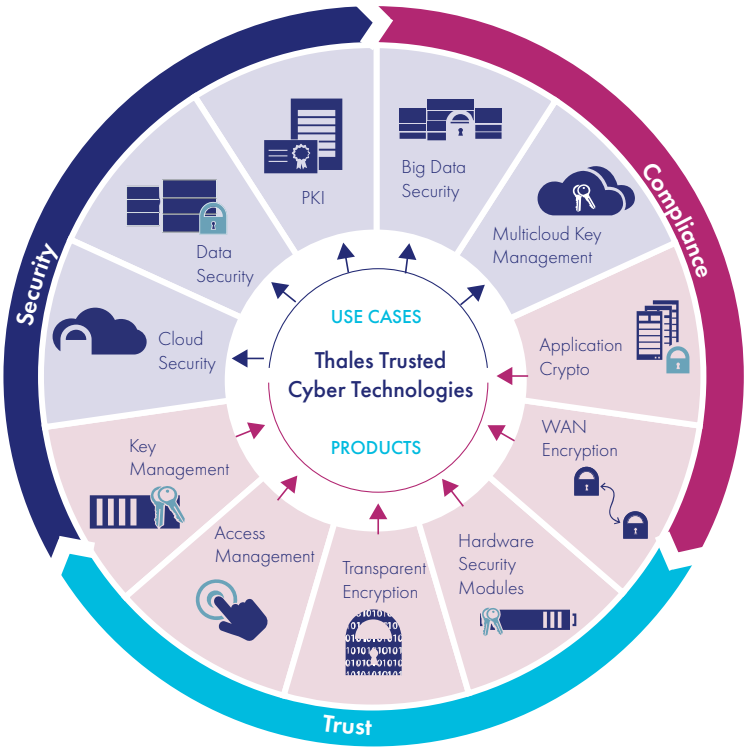
CMMC combines various cybersecurity control standards such as NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933 and others into one, unified standard for cybersecurity with maturity levels ranging from ranging from Basic Cybersecurity Hygiene to Advanced. CMMC also measures the maturity of a company's institutionalization of cybersecurity practices and processes.[2]

How Thales TCT Addresses CMMC Levels and Requirements

Thales TCT Trusted Cyber Technologies (TCT) is a U.S. based provider of government high-assurance data security solutions. The company's mission is to provide innovative solutions to protect the most vital data from the core to the cloud to the field for defense, intelligence, and civilian agencies across the U.S. Federal Government. With a concentration on Federal and other U.S. government agency requirements, Thales TCT is better able to serve its government customers while also investing in the development of future technologies to secure the Federal Government's most sensitive information.

With an extensive data security portfolio and compliance mapping methodology, Thales TCT is a key partner in helping organizations achieve CMMC requirements and cybersecurity maturity levels. Our solutions provide a platform for the implementation of cybersecurity controls and institutionalization of cybersecurity practices and processes.

Thales TCT's data security portfolio consists of data protection solutions that share a common, extensible implementation infrastructure for delivering data-at-rest encryption, enterprise key management, network encryption, authentication, access control, and security intelligence across an organization's infrastructure.



Thales TCT Data Security Portfolio Solutions

- **Data Security Platform** centrally manages policies and encryption keys for all Thales data security products.
- **Transparent Encryption** secures any database, file or volume across large agencies and implementations.
- **Application Encryption** provides a simple framework to deliver field level encryption.
- **Key Management** centralizes KMIP and TDE keys and certificate management.
- **Cloud Key Management** establishes strong controls over encryption keys and policies for data encrypted by cloud services.
- **Security Intelligence** accelerates the detection of APTs, Insider Threats and compliance report generation.
- **Network Encryption** provides end-to-end, authenticated encryption for data in transit using standards-based algorithms.
- **Hardware Security Modules** serve as "trust anchors" that protect an organization's cryptographic infrastructure.
- **Certificate-based, multi-factor authentication** controls access to sensitive data and protect user identities.

[1] https://washingtonexec.com/2020/02/top-10-things-you-need-to-know-about-cmmc/#.XnjxSYhKiUk
[2] https://www.acq.osd.mil/cmmc/faq.htm

Data-at-Rest Protection
Thales TCT's data-at-rest protection solutions address critical CMMC data protection, training and awareness controls:

- **Encryption and Key Management** – strong, centrally managed, file encryption combined with simple, centralized key management that is transparent to processes, applications, and users. FIPS 140-2 and Common Criteria certified.
- **Access Policies and Privileged User Controls** – restrict access to encrypted data by permitting data to be decrypted only for authorized users and applications while allowing privileged users to perform IT operations without ability to see protected information. NIST Certified AES 256
- **Security Intelligence** – capture access attempts to protected data via logs, providing high value security intelligence information that can be used with a Security Information and Event Management (SIEM) solution and for compliance reporting.

Cryptographic Key Management
Thales TCT's industry leading Luna hardware security modules (HSMs) support CMMC standards with capabilities including:

- Address compliance requirements with FIPS 140-2 L3 and CNSS Approval*
- Automatically generate and store keys and certificates in hardware
- Ability to have multiple applications share the same hardware
- Cluster HSMs to avoid single point of failure
- CNSS approval for TCT HSMs on National Security Systems
- NCCoE reference architecture for TLS Server Certificate Management

Data-in-Motion Protection
Thales TCT's certified high speed network encryption solutions that support CMMC standards with capabilities including:

- Comprehensive data-in-motion security for Layer 2, 3, & 4 for IPv4 and IPv6 Networks.
- 95% bandwidth efficiency, which optimizes encrypted throughput from 10Mbps to 100Gbps.
- Integrated group key management system, which scales to support hundreds of encryptors with no-cost redundancy.
- Physical and logical separation of network administration and security responsibilities enforces policy and reduces opportunity for insider attacks.
- Capabilities not found natively in network switches and routers, such as tamper-resistant physical hardening, strong authentication for administrators, hardware-based key generation, and embedded and remote key management.

Authentication
Thales TCT's certificate-based authentication platforms support CMMC standards with capabilities including:

- Traditional high assurance authentication smart cards and usb tokens
- First-of-a-kind hardware security module-secured identity credentials

* Validation in Process

Data Protection Best Practices

Defend Data Where it Lives
By combining encryption at the file system level with integrated key and policy management, Transparent Encryption protects and controls access to sensitive data in cloud, big data, database, and file servers.

After protecting sensitive data, least privileged access policies are enforced, preventing privileged insiders and advanced persistent threats from accessing data. Because this is "transparent" encryption, there are no changes required to applications, infrastructure or business practices. Users will never even know that the sensitive data that they were accessing is now secure, unless they tried to access it in an unauthorized fashion!

Defend Data Where it Begins
Application Encryption enables organizations to design and embed encryption capabilities directly into their applications, when necessary. With this data security protection product, the data is protected from the application, through transmission, and into storage.

Application encryption helps organizations meet specific compliance requirements or take specific data out of compliance scope. The Thales TCT Security Platform removes the complexity and risk of building encryption into an application by providing libraries for NIST approved AES encryption and simplifying key management with the Data Security Platform.

Simplify and Centralize Key Management
A common data security challenge is how to manage and maintain all the different key and certificate management solutions. Thales TCT Key Management delivers centralized control of the most common encryption key management requirements in order to reduce the on-going management and maintenance burden of multiple solutions. Thales TCT is the choice for government agencies for generating, storing, protecting and managing cryptographic keys used to secure sensitive data and critical applications.

Thales TCT can not only manage the keys and policies for the Thales TCT line of data security protection products, but it is also a KMIP server, manages keys for Oracle and Microsoft SQL Server Transparent Data Encryption (TDE), handles certificate inventory and can securely store any object, such as passwords. The Thales TCT Key Management solutions offer an intuitive approach across all requirements. It is typically deployed in an architecture to meet the most demanding high-availability SLAs.

Detect Threats and Issue Alerts
Applying data protection controls is a good start to an effective cybersecurity strategy. However, organizations need awareness of who and what's accessing private and confidential data, including privileged users masquerading as other users.

Every time someone attempts to access a resource under the protection of Thales TCT's platform, actionable intelligence logs of whom, when, where, which policies applied, and the resulting action can be generated. Because sifting through the rich granular data of Thales TCT's event logs can be time consuming, the Thales TCT platform integrates with leading SIEM (Security Information and Event Management) systems, including HP ArcSight, Splunk, IBM QRadar and LogRhythm, adding to their value with new inside-the- fence security intelligence and awareness. With pre-defined reports and visualizations, organizations will be better able to pinpoint which events are worth further investigation.

Compliance, Regulations and Contractual Mandates
Thales TCT addresses industry compliance mandates, global government regulations (such as NIST 800-171) and contractual mandates by securing data in traditional on-premise, virtual, cloud and Big Data infrastructures, through:

- Data-at-Rest encryption and centralized enterprise key management that allows agencies to lock down data using strong industry approved algorithms coupled with a virtual or physical FIPS 140-2 Level 3 certified appliance for key and policy management.
- Simplify the creation and consistent enforcement of data access and privileged user control policies. Fine-grained control to determine whom can access specific data in order to block privileged users, such as root, as well as preventing Advanced Persistent Threats (APTs) from gaining access to protected data.
- Thales TCT Security Intelligence delivers the fine-grained details of data access required to prove compliance to auditors. In addition, leveraging Thales TCT Security Intelligence connectors and reports for popular SIEM tools simplifies integration and analysis.

Thales TCT Solutions for CMMC Security Controls

Thales TCT offers solutions that can help organizations meet CMMC requirements. Our solutions can easily integrate with an existing infrastructure to strengthen overall security to address various CMMC security control components. Many of the CMMC controls will require a combination of people, process, and products to achieve. Thales TCT offers the broadest security platform to seamlessly transition requirements to stringent security postures. The following table outlines the specific CMMC security controls addressed by Thales TCT:

- Solutions that directly meet tool requirements (denoted in blue)
- Solutions mixed with process, procedures, and Thales TCT security solutions

Security Control Family	Compliance Baseline	Thales TCT Solution
Access Control (AC)	• Establish system access requirements (AC.1.001) • Control internal system access (AC.1.002) • Control remote system access (AC.3.014) • Limit data access to authorized users and processes (AC.2.016)	Data Security Platform Transparent Encryption with Access Control High Assurance Authentication Luna Credential System
Asset Management (AM)	• Identify and document assets (AM.4.226)	Transparent Encryption Data Security Platform
Audit and Accountability (AU)	• Define audit requirements (AU.2.041) • Perform auditing (AU.2.042) • Identify and protect audit information (AU.3.050) • Review and manage audit logs (AU.2.044)	Data Security Platform Transparent Encryption with Access Control SIEM Integration
Awareness and Training (AT)	• Conduct security awareness activities (AT.3.058) • Conduct training (AT.2.057)	Thales Advanced Services Group
Configuration Management (CM)	• Establish configuration baselines (CM.2.061) • Perform configuration and change management (CM.2.064)	Data Security Platform Transparent Encryption with Access Control SIEM Integration Luna Hardware Security Modules
Identification and Authentication (IA)	• Grant access to authenticated entities (IA.1.077)	Data Security Platform Transparent Encryption with Access Control SIEM Integration Luna Hardware Security Modules High Speed Encryption Authentication and Assurance Luna Credential System
Incident Response (IR)	• Plan incident response (IR.5.106) • Detect and report events (IR.2.093) • Develop and implement a response to a declared incident (IR.2.095) • Perform post incident reviews (IR.2.097) • Test incident response (IR.3.099)	Data Security Platform Transparent Encryption with Access Control SIEM Integration Luna Hardware Security Modules High Speed Encryption

Security Control Family	Compliance Baseline	Thales TCT Solution
Maintenance (MA)	• Manage maintenance (MA.2.112)	Data Security Platform Transparent Encryption with Access Control Luna Hardware Security Modules High Speed Encryption
Media Protection (MP)	• Identify and mark media (MP.3.122) • Protect and control media (MP.2.119) • Sanitize media (MP.1.118) • Protect media during transport (MP.3.124)	Data Security Platform Transparent Encryption with Access Control Luna Hardware Security Modules
Personnel Security (PS)	• Screen personnel (PS.2.127) • Protect CUI during personnel actions (PS.2.128)	Data Security Platform Transparent Encryption with Access Control Luna Hardware Security Modules
Physical Protection (PE)	• Limit physical access (PE.1.131)	Data Security Platform Transparent Encryption with Access Control Luna Hardware Security Modules High Speed Encryption
Recovery (RE)	• Manage back-ups (RE.2.138)	Data Security Platform
Risk Management (RM)	• Identify and evaluate risk (RM.2.142) • Manage risk (RM.4.148)	Transparent Encryption with Access Control SIEM Integration
Security Assessment (CA)	• Develop and manage a system security plan (CA.2.157) • Define and manage controls (CA.2.159) • Perform code reviews (CA.3.162)	Data Security Platform Transparent Encryption with Access Control SIEM Integration Luna Hardware Security Modules High Speed Encryption Authentication and Assurance Luna Credential System
Situational Awareness (SA)	• Implement threat monitoring (SA.4.171)	Data Security Platform Transparent Encryption with Access Control SIEM Integration Luna Hardware Security Modules High Speed Encryption Authentication and Assurance Luna Credential System
Systems and Communications Protection (SC)	• Define security requirements for systems and communications (SC.3.187) • Control communications at system boundaries (SC.3.177)	Data Security Platform Transparent Encryption with Access Control Luna Hardware Security Modules High Speed Encryption Authentication and Assurance Luna Credential System
System and Information Integrity (SI)	• Identify and manage information system flaws (SI.1.210) • Identify malicious content (SI.1.212) • Perform network and system monitoring (SI.2.217)	Data Security Platform Transparent Encryption with Access Control SIEM Integration Luna Hardware Security Modules High Speed Encryption Authentication and Assurance

Security Control Detail

Access Control

Transparent Encryption

- Thales Transparent Encryption Agents installed on hosts intercept every attempt made to access protected data based upon a set of rules that will either permit or deny the access attempt. Each security rule evaluates who, what, when, and how protected data is accessed and, if these criteria match, the agent will permit or deny access. (AC.1.002, AC.2.007, AC.2.008, AC.2.016, AC.3.017, AC.3.018, AC.3.021)
- Thales Data Security Manager (DSM) is a hardened appliance for optimum security and comprises a policy engine and a central key and policy manager.
- The set of rules is defined in a policy is configured on the Thales DSM and downloaded to the agent through a secure SSL network connection. It provides separation of duties between data owners, administrators, key managers, and security managers. (AC.2.009, AC.3.017, AC.3.0191)

Data Security Manager

- Thales DSM Login – The Thales Data Security Manager has both a web-based and command-line GUI that can be configured for both administrator and role based separation. (AC.3.017)
- Separation of Domains and Roles – One of the functions of the Thales DSM is the notion of domain administration. A Domain is logical entry that is used to separate administrators and the data they access from other administrators, and can be applied internally to a program, a fixed number of programs, or externally to an entire enclave. The credentials of each of these domains can be integrated into Active Directory or LDAP groups, and monitors number of logins, login attempts, previous logons, and will lock each role out after 15 minutes of inactivity. The use of these domains and the protection of data through the use of Thales "guard points" enforces Least Privilege that is defined in an Information System's Security Plan, Concept of Operation, and proven through testing.

Luna Hardware Security Modules

- Luna HSMs can also be separated into cryptographically isolated partitions, with each partition acting as if it was an independent HSM This provides a tremendous amount of scalability and flexibility, as a single HSM can protect the cryptographic keys of several independent applications. Luna Network HSM partitions are designed with independent access controls and key storage, allowing use in multi-tenant environments.

High Speed Encryption

- Safeguards data in motion with high speed network encryption, proven to meet network performance demands for real time low latency and near-zero overhead, providing security without compromise for data traversing networks across data centers and the cloud.
- Preferred by the world's most secure organizations, the tamper resistant HSEs are certified to Common Criteria and FIPS 140-2 Level 3 requirements and supports standards based, end-to-end authenticated encryption and client-side key management. Advanced security features include traffic flow security, support for a wide range of elliptic curves (Safe Curves, Brainpool, NIST). VLAN based encryption provides unique key pairs in hub and spoke environments to protect against mis-configured traffic. For high-assurance environments, the encryptors also nested encryption. (AC.3.014, AC.4.023)

Authentication

- Thales TCT's Smart Card 650 (SC650) is the most secure, certificate-based smart card available today. It supports numerous algorithms, X.509 digital certificates, the SC650 enables strong two-factor authentication and proof-positive user identification in all Public Key Infrastructure (PKI) environments.
- The SC650 securely stores the user's credentials, such as digitally-signed certificates, private keys, and network login credentials and seamlessly supports secure key generation, secure key storage, encryption/decryption, and digital signature processing (sign and verify). (AC.3.012, AC.3.014)

Awareness Training

Thales TCT Training Program

Thales TCT's training courses provide the educational foundation that enables success when deploying, managing, and growing your investment. Each course is carefully constructed to cover capabilities, features and functionality based on roles. Additionally, the courses provide important best practices, and troubleshooting designed to empower students to effectively manage your production environments. (AT.2.056, AT.3.058, AT.4.059)

Audit and Accountability

Transparent Encryption

- Transparent encryption activity is closely monitored and logged. All auditable events, including backups, restores, and security operations can be logged at the Thales DSM or at the hosts. The Thales DSM is capable of storing up to 110,000 audit messages. The following audit event content is provided (AU.2.041, AU.2.044, AU.3.052):
    - Date and Time Event type Severity
    - User Identity
    - Process from which the attempt is being made Status: success or failure
    - Name of related policy (key, policy, host, etc)
    - Description
- Audit data can also be protected from unauthorized access or modification through encryption using Thales Transparent Encryption. The audit directory can be configured as a guard point and placed under access control. This is also a non-repudiation technique, as it will preserve the content path of any individual accessing an unauthorized component of an Information System. (AU.3.049, AU.3.050)
- Audit data is collected in an open Syslog format and can be integrated with several SIEM and log correlation tools. (AU.2.042, AU.3.048, AU.3.051, AU.4.053)
- When the agent component of Thales Transparent Encryption cannot contact the central manager (Thales Data Security Manager) for logging (network outage), logs from the agent are stored locally until network connectivity resume, at which point those logs are uploaded to the Thales DSM. By sending agent Host OS logs to an audit reduction or network monitoring tool, correlations can be created with the appropriate alerting. (AU.3.045, AU.3.046, AU.5.055)

Luna Hardware Security Modules (HSMs)

- Luna HSMs can be configured to selectively log HSM events for security auditing purposes. This allows for separation of duties between an Audit Officer/Team and the people they are auditing preventing both the administrative and user personnel from tampering with the log files and the auditors from doing anything administrative or accessing keys.
- These secure audit capabilities also monitor how keys are being used, as well as identifies failures in the cryptographic device. Built in log integrity verifies the authenticity of the logs origin. Reporting capabilities securely track and store audit trails to be signed for non-repudiation. Automated reports and email alerts may be set-up based on a number of cryptographic management criteria. (AU.2.042, AU.3.048, AU.4.053)

Security Assessment and Authorization

Transparent Encryption

- Thales Transparent Encryption can be tested as a part of an Information System. The agents are installed on operating systems that undergo security hardening and STIG configurations. (CA.2.158, CA.3.16)

Configuration Management

Key Management

- The configuration of the Thales DSM can be changed to match operational requirements for access control and encryption at rest, and can be saved/ backed up in order to track changes over time. (CM.2.062, CM.2.064, CM.3.067, CM.3.068, CM.3.069, CM.4.073, CM.5.074)
- Luna Hardware Security Modules verify the integrity of security applications via Root of Trust (CM.5.074)

Contingency Planning

- Thales Security appliances can operate in a clustered environment and can be added to a program's COOP/DR strategy.

Identification and Authentication

Encryption Agents

- Thales agent policies work in conjunction with a program's authentication and identification policies and procedures and are used to protect system files, data files and folders, and applications. (IA.1.077)
- Policy configuration can be fine-tuned to select (IA.1.077):
  - A desired database
  - A program's Operating System Host records
  - Key Type
  - User sets (Organizational Users) Group Identification
  - Specific processes and applications that are allowed to access a Thales guard point
- Each Thales agent is cryptographically signed by a certificate authority generated by the Thales DSM in order to identify and authorize access and encryption/decryption operations on the host system. The Thales DSM is available as a FIPS 140-2 Level 2 or 3 hardware appliance. (IA.1.077)
- The Thales DSM supports integration with existing technologies for identification and authentication(Active Directory and LDAP) and augments that process by specifying (through the use of policy) which user, application, or process is allowed to access a file, directory, or application on an information system component. (IA.1.076, IA.1.077)
- On the Thales Web Console, credentials of each of these domains can be integrated into Active Directory or LDAP groups, and monitors number of logins, login attempts, previous logons, and will lock each role out after 15 minutes of inactivity, requiring re-authentication. (IA.1.077, IA.2.078, IA.2.079, IA.2.080, IA.3.083, IA.3.084)
- Communication between Thales DSM and agents are cryptographically signed by the Thales DSM's certificate authority and passed in an encrypted format (AES256). (IA.1.077)

Authentication Solutions

- Thales TCT offers authentication solutions that address the evolution of identities. From traditional high assurance authentication tokens to first-of-a-kind hardware security module-secured identity credentials, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government. (IA.1.077, IA.2.081)
- Thales TCT's high assurance authenticators bring multi-factor authentication to applications and networks where security is critical. Available in USB and smart card form factors. Thales TCT's certificate-based authenticators support numerous algorithms and X.509 digital certificates enabling strong two-factor authentication and proof-positive user identification in all Public Key Infrastructure (PKI) environments. (IA.1.077)
- The Luna Credential System (LCS) introduces a new approach to multi-factor authentication by maintaining user credentials in a centralized hardware device that is securely accessible by endpoints in a distributed network. It unites the familiarity of certificate-based authentication with the security of a FIPS 140-2 certified HSM. LCS is a multi-purpose, secure credential system ideally suited for an environment in which the endpoints cannot use a traditional small form-factor token. Composed of the Luna Credential HSM and the Luna Credential Client, LCS supports a number of use cases including Windows Logon and authentication to PK-enabled applications and websites. (IA.1.077)

Incident Response

Transparent Encryption

- Thales Transparent Encryption processes incidents at the individual component level (host system, web GUI, DSM). (IR.2.093, IR.2.095)
- These incidents and audit events are in an open syslog format and can be sent to an information system's monitoring/reporting tool, including 3rd party SIEM solutions. (IR.5.106, IR.2.095)
- Log formats can be tailored to match a program's security policy for user and application behavior. (IR.2.093)

High Speed Encryption

- Protecting network transmitted data against cyber attacks and data breaches is imperative for federal agencies. Data network eavesdropping, innocent error or technical failure, data tampering and data theft have all become commonplace. The implications of a significant breach are often catastrophic. Only encryption may ensure that your agency's data remains protected while transmitted across data networks and links. However, not all encryption solutions are the same. (IR.2.095, IR.5.106)
- Robust encryption (also known as high-assurance encryption) features secure, dedicated encryption devices. In order to be truly high assurance, these devices must use embedded, zero-touch

encryption key management; provide end-to-end, authenticated encryption and use standards-based algorithms. (IR.2.095, IR.5.106)

- Only through high-assurance network data encryption can you be assured your data is rendered useless in unauthorized hands and that it will remain secure beyond the data's useful life. (IR 2.095, IR.5.106)

Maintenance

- Thales appliances available as a FIPS 140-2 Level 2 or 3 certified configuration (level 3 is tamper resistant) (MA.2.113)
- Additionally, maintenance and audit sessions can be separated by domain and by administrator login.

Media Protection

- As required by FIPS 140-2 level 3 certification, the Thales Data Security Manager, Luna HSMs, and High Speed Encryptors have the ability to be zeroized at the appliance console. (MP.1.118, MP.2.120, MP.3.125)

Physical and Environmental Protection

- The Thales DSM, Luna HSMs and High Speed Encryptors can be installed into a standard locking rack enclosure. (PE.1.131)
- Available as a FIPS 140-2 Level 2 or 3 certified configuration (level 3 is tamper resistant) (PE.1.131, PE.1.133, PE.3.136)
- High Assurance Authentication Certificate based Smart Cards limit physical access to information systems and controls access to devices. (PE.1.131, PE.1.134, PE.2.135, PE.3.136)

Personnel Security

- The Thales DSM supports integration into an organization's Active Directory tree or LDAP to support existing network and server based authentication methods including the ability to track a users' credentials as they enter and exit a program. (PS.2.128)

Risk Assessment

- Thales Transparent Encryption can be a part of a risk assessment process at both components in its architecture in an information system; The Thales DSM, and host agents. (RM.2.142)
- The Thales appliances are FIPS 140-2 Level 3 certified. (RM.2.142)
- The Thales Encryption Agents are installed on servers in an Information System that should meet security hardening and STIG guidance. (RM.2.142)

System and Services Acquisition

- The Thales DSM, KeySecure, HSM and HSE appliances are all FIPS 140-2 Level 3 compliant.

Systems and Communications Protection

Transparent Encryption

- Thales Transparent Encryption provides a fine- grained set of access controls that can act as a secondary set of controls beyond those available from a system or identity management solution to ensure that general users cannot gain access to administrative or security capabilities. (SC.3.187)
- The solution is platform independent and security functions on the Thales DSM are isolated from normal operation and include domain creation, key creation, host creation, and audit-only. (SC.3.177)
- Once a system's data has been encrypted through data transformation, it remains encrypted at rest and is under fine-grained access controls. (SC.3.177)
- If more than one domain is deployed, domain administrators and users are separated by domain. Administrators have the option of using different encryption algorithms and key lengths to provide even more separation. Encryption algorithms for each domain include AES 128 and 256.
- Encrypted communications between Thales DSM and agent is selectable, options are NSA Suite B or RSA algorithms. (SC.3.177, SC.3.187)

High Speed Encryption & Hardware Security Modules

- Thales High Speed Encryptors (HSE) and Hardware Security Modules (HSM) utilize encrypted sessions for the management of network devices and employ FIPS-validated hardware to protect the confidentiality of CUI (SC.1.175, SC.2.179, SC.3.177, SC.3.189, SC.3.190, SC.5.230)
- Thales HSE and HSMs prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicate via some other connection to resources in external networks (e.g., split tunneling)(SC.3.183, SC.3.184, SC.3.185, SC.3.186)
- Establish and manage cryptographic keys for cryptography employed in organizational systems (SC.3.187, SC.4.197, SC.4.228)

Data Security Manager

- There is secure transmission control between the Thales DSM, the Thales daemon running on the host, and the SecFS portion that sits in the host's kernel space. The Thales DSM creates a public/private key pair, generates a Certificate Signing Request (CSR), which generates a certificate authority certificate that is stored in the Thales DSM database. (SC.3.177, SC.3.181)
- The user space portion of the Thales agent creates a public/private key pair. The public key is used to create a CSR for the host, and is sent back to the Thales DSM, where the request is signed, sent back to the host, and creates a "blueprint" of the host, along with the certificate. (SC.3.177)
- The kernel space portion also creates an asymmetric key pair and follows the same certificate creation process in order to send the kernel space public key to the Thales DSM. (SC.3.177)
- Keys are passed between the Thales DSM and the host by generating a one-time AES256 random key on the Thales DSM. The desired encryption keys are encrypted using the random key. The random key password is encrypted using the kernel space public key. The entire payload is sent to the host system, where the kernel space private key decrypt the random key and password. The random key then decrypts the desired encryption keys, and those keys are applied to the file/directory/executable that is to be encrypted. (SC.3.177, SC.3.182, SC.3.187, SC.3.191)
- The Thales Key Vault is a secure inventory of certificates, keys, and other materials. It provides alerting and upcoming event status regarding certificate and key expiration. Key strength and type are also available to check compliance on any weak keys applied to an information system. Import and export of 3rd party keys is also supported. The key vault is protected from tampering through the Thales DSM, which is a FIPS 140-2 hardened appliance. (SC.3.177, SC.3.186, SC.4.197, SC.4.228)

System and Information Integrity

Transparent Encryption

- Thales Transparent Encryption monitors an information system at these points, and creates audit data on (SI.2.214):
  - Thales Data Security Manager
  - Web-based GUI
  - Host Agents Host logon
- Thales Transparent Encryption enforces information handling through the use of guard points. A guard point is a protected device or directory that is encrypted, and provides decryption rules within policy. Each rule specifies a condition that will permit or deny access based on a particular combination of (SI.2.217, SI.4.22, SI.5.222, SI.5.223):
  - User (either local user/group or Active Directory user/group)
  - Process (the actual binary used; i.e. mssql.exe) Action (read, write, change attribute, delete, list directory, etc.)
  - Result (specific files or directories within the guard point)
  - Time (Time of Day, eg 9am-5pm M-F)

Luna Hardware Security Modules

- Thales HSMs provide protection from malicious code at appropriate locations within organization information systems (SI.4.221)

Program Management

- Program Management controls are typically implemented at an organization Level and not directed to Information Systems. As such, it is not a technical control that Thales TCT Transparent Encryption addresses

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.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com