Trusted Cyber Technologies

THALES
Building a future we can all trust

NIST 800-53 Mapping - Thales TCT CipherTrust Data Security Platform

White Paper

Contents

ABSTRACT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidance for the selection of security and privacy controls for federal information systems and organizations. Published by the National Institute of Standard and Technology, the publication details items from the Risk Management Framework that address security controls required to meet requirements in the Federal Information Processing Standard (FIPS) 200. Revision 4 is the most comprehensive update since the initial publication. Revision 4 was motivated principally by the expanding threat space and increasing sophistication of cyber- attacks. Major changes include new security controls and control enhancements to address advanced persistent threats (APTs), insider threats, and system assurance; as well as additions to address technology trends such as mobile and cloud computing.

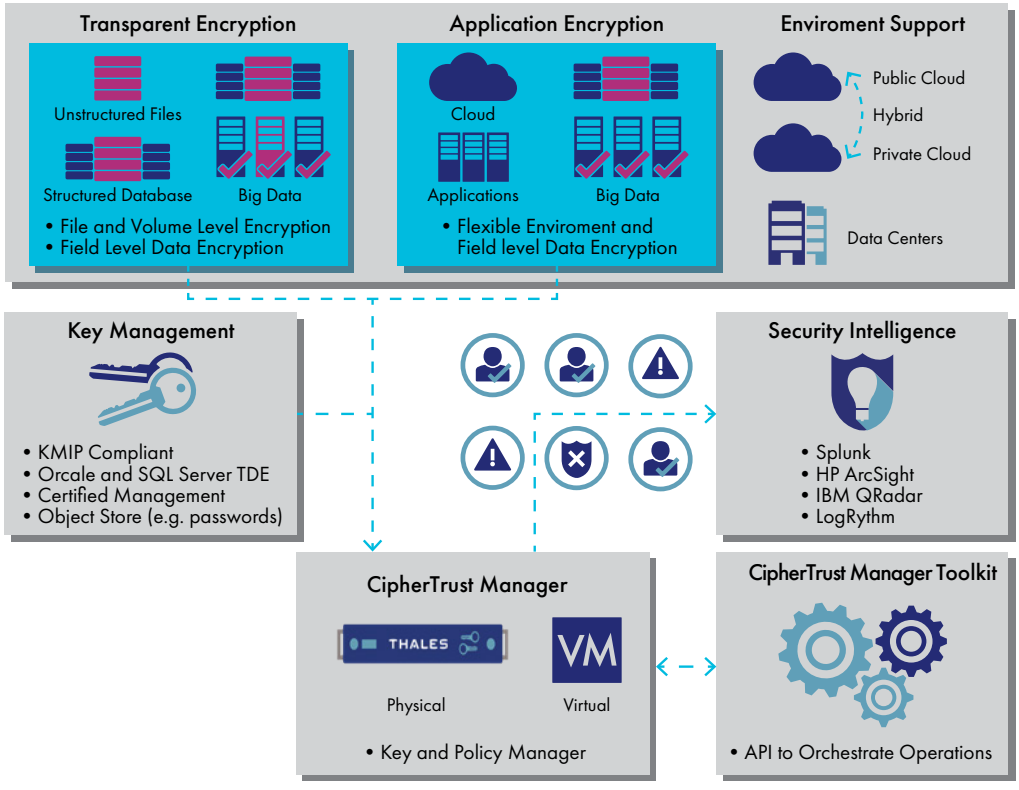
Critical to certification for meeting FIPS, is the implementation of security controls from NIST 800-53, Appendix F. Focusing on the capabilities needed to meet these requirements, this paper provides background about Thales Trusted Cyber Technologies's (TCT) CipherTrust Data Security Platform and the CipherTrust Transparent Encryption product that is delivered through that platform. It further details a mapping of the CipherTrust product line's capabilities against these NIST security controls, first with an initial summary for each Family Area (in the form of a table), and then with expanded details of how these controls are delivered.

Thales TCT is a key partner in helping organizations to meet the standard. Focusing on protecting data-at-rest, Thales TCT delivers critical data protection controls, as well as training and awareness, to address each area. Core capabilities that support the standard include:

- **Encryption and Key Management** – strong, centrally managed, file and volume encryption combined with simple, centralized key management that is transparent to processes, applications and users.
- **Access Policies and Privileged User Controls** – that restrict access to encrypted data – 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.
- **Security Intelligence** – logs that capture access attempts to protected data, providing high value security intelligence information that can be used with a Security Information and Event Management (SIEM) solution and for compliance reporting.

THE CIPHERTRUST DATA SECURITY PLATFORM

The CipherTrust Data Security Platform consists of data protection product offerings that share a common, extensible implementation infrastructure for delivering data at rest encryption, enterprise key management, access control and security intelligence across an agency's infrastructure. CipherTrust Data Security Platform makes it simple to solve today's and future security and compliance concerns by simultaneously defending data in databases, files and Big Data nodes across cloud, virtual or traditional data centers. CipherTrust Data Security Platform products are centrally managed, making it easy to extend data security protection and satisfy compliance requirements across the entire organization, without adding new hardware or increasing operational burdens.



CIPHERTRUST DATA SECURITY PLATFORM PRODUCTS

- CipherTrust Manager centrally manages policies and keys for all CipherTrust data security products
- CipherTrust Transparent Encryption secures any database, file or volume across large agencies and implementations

CipherTrust Transparent Encryption and the CipherTrust Manager are the primary focus of this paper.

Other CipherTrust Data Security Platform products include:

- CipherTrust Developer Suite (which includes CipherTrust Application Data Protection and Tokenization) provides a simple framework to deliver field level encryption
- CipherTrust Enterprise Key Management centralizes KMIP and TDE keys and certificate management
- CipherTrust Manager captures syslog details and can forward them to popular SIEM tools to help accelerate the detection of APTs, Insider Threats and compliance report generation.

DEFENDING DATA WHERE IT LIVES

By combining encryption at the file system level with integrated key and policy management, CipherTrust Transparent Encryption protects and controls access to sensitive data in your Cloud, Big Data, database, and file servers. After protecting your sensitive data, least privileged access policies are enforced, preventing privileged insiders and APTs from accessing your data. Because this is "transparent" encryption, there are no changes required to your applications, infrastructure or business practices. Your 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!

DEFENDING DATA WHERE IT BEGINS

CipherTrust Developer Suite (which includes Application Data Protection and Tokenization) 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. Most commonly, deploying this data security protection product is to meet specific compliance requirements or to take specific data out of compliance scope. The CipherTrust 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 CipherTrust Manager

SIMPLIFY AND CENTRALIZING ENTERPRISE KEY MANAGEMENT FOR AGENCIES

A common data security challenge is how to manage and maintain all the different key and certificate management solutions.

CipherTrust TDE 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. CipherTrust TDE Key Management not only manages the keys and policies for the CipherTrust 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 CipherTrust TDE Key Management solution offers an intuitive web based interface and APIs. It is typically deployed in an architecture to meet the most demanding high- availability SLAs.

DETECTING THREATS AND ISSUING ALERTS

Thales TCT understands that protecting your data is good, but not good enough; you need awareness of who and what is accessing your private and confidential data, including privileged users masquerading as other users. Every time someone attempts to access a resource under the protection of the CipherTrust platform, rich logs of whom, when, where, which policies applied, and the resulting action can be generated. Because sifting through the rich granular data of CipherTrust Manager's event logs can be time consuming, the CipherTrust platform generates Syslog log files that can be integrated 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 those tools pre-defined reports and visualizations, you'll 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 800-53) 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.
- CipherTrust syslog feature delivers the fine-grained details of data access required to prove compliance to auditors. In addition, leveraging CipherTrust syslog and integration with popular SIEM tools simplifies integration and analysis.

SECURITY CONTROL SUMMARY

As found in NIST 800-53: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Security Control Family	Compliance Baseline	Thales TCT Product Line Mapping
Access Controls (AC)	• Access Enforcement • Account Management • Separation of Duties • Least Privilege	Through the use of kernel level agents providing AES-256 Encryption, the CipherTrust Manager exceeds and augments current access control solutions at the file, directory, drive, or target level at the Operating System and provides Least Privilege.
Awareness and Training(AT)	• Training Policies • Security Awareness Training • Role Based Security Training	Deployment of CipherTrust Transparent Encryption is a part of program's Defense-In-Depth security architecture to protect sensitive data through fine-grained access controls and encryption at rest. On initial deployment, Thales (in-class, online) are used to train staff to use the solution. burden, and the training provided covers tasks and responsibilities for each desired/deployed role, with appropriate documentation provided.
Audit and Accountability(AU)	• Audit Events • Content • Response • Capacity • Non-Repudiation • Report Generation	CipherTrust Transparent Encryption provides full audit data at the CipherTrust Manager and host agents in an open format and can be integrated to a program or an agency's audit reduction tool or SIEM solution.
Security Assessment and Authorization(CA)	• System Interconnects • Plan of Action and Milestones • Continuous Monitoring	CipherTrust 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. The CipherTrust Manager is FIPS 140-2 Level 1 or Level 3 compliant depending upon configuration.
Configuration Management (CM)	• Baseline Configuration • Change Control • Security Impact Analysis • Least Functionality	The configuration of the CipherTrust Manager can be changed to match operational requirements for access control, encryption at rest, and can be saved, backed up, and added to a CMDB in to track changes over time.
Contingency Planning(CP)	• Contingency Plan • Contingency Testing	The CipherTrust Manager component can operate in a clustered environment in active or standby mode, and can be added to a program's COOP/DR strategy.
Identification and Authentication(IA)	• Organizational Users • Device Login • Authentication Management • Crytpographic Module • Incident Handling	Identification is provided through local web GUI login or Active Directory/ LDAP Integration at the CipherTrust Manager appliance. Authentication is provided through the use of kernel level system access to files, folders, and applications.
Incident Response(IR)	• Incident Response Testing • Training • Handling • Monitoring	The CipherTrust Data Security Platform processes incidents at the individual component level (host system, web GUI, CipherTrust Manager). These incidents and audit events are in an open syslog format that can be sent to an information system's monitoring/reporting tool, including 3rd party SIEM solutions. Log file formats can be tailored to match a program's security policy for user and application behavior.
Maintenance(MA)	• Controlled Maintenance • Tools	CipherTrust Manager is tamper resistant with zeroizing ciruitry. Additionally, maintenance and audit sessions is separable by domain and by administrator login.
Media Protection(MP)	• Media Access • Media Marking • Storage Transport	CipherTrust Manager has the ability to be zeroized at the appliance console.
Physical and Environmental Protection (PE)	• Access Authorizations • Control • Transmission	The CipherTrust Manager is a 19" 1ru hardware device and can be secured in a lockable data center rack enclosure
Planning(PL)	• Security Architecture • Concept of Operations	CipherTrust Data Secure Platform provides fine-grained access policies and AES256 encryption that can be used to limit privileged user access and implement least-privilege principles for users authorized for access to sensitive data.

Security Control Family	Compliance Baseline	Thales TCT Product Line Mapping
Personnel Security(PS)	• Personnel Termination and Transfer	Thales TCT Transparent Encryption should be operated by personnel at the appropriate level of clearance and information system access.
Risk Assessment(RA)	• Security Categorization • Vulnerability Scanning	CipherTrust Transparent Encryption can be used as part of a risk assessment process at both components in its architecture in an information system. The CipherTrust Manager is FIPS 140-2 Levels 1 or 3 compliant and the Host Agents can be installed on hardened servers to minimize risk.
System and Services Acquisition(SA)	• Allocation of Resources • System Development Life Cycle	System Components of the CipherTrust Manager are produced in USA by Thales TCT approved manufacturer. It is FIPS 140-2 Level 3 compliant.
Systems and Communications Protection(SC)	• Application Partitioning • Security Function Isolation • Confidentiality and Integrity • Cryptographic Key Management • Platform Agnosticism	As a part of the CipherTrust Transparent Encryption solution, AES 256 encryption keys are passed through an encrypted wrapper. The Administrator Web Interface is accessed through HTTPS. Agent-to-CipherTrust Manager communication is accomplished through the use of ephemeral ports. This provides and additional layer of encryption key protection and thus reduces risk.
Systems and Information Integrity (SI)	• Certified only for FIPS 140-2 Levels 1, 2 and 3 depending on model.	System Integrity on the CipherTrust Transparent Encryption product is satisfied through the CipherTrust Manager's FIPS 140-2 validation. Host agents installed on an Information System's server provide data encryption at rest capabilities to enhance system integrity.
Program Management(PM)	• Security Alerts and Advisories • Software and Information Integrity	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 the CipherTrust Transparent Encryption addresses.

SECURITY CONTROL DETAIL

1. ACCESS CONTROL

Access Control applies to the following places within the CipherTrust Transparent Encryption solution:

- **CipherTrust Data Security Platform Product Policy**
    1. The CipherTrust Manager is a hardened appliance for optimum security and comprises a policy engine and a central key and policy manager. Agents installed on hosts intercept every attempt made to access protected data and, based upon a set of rules, either permit or deny the access attempt.
    2. CipherTrust product line policy is comprised of sets of security rules that must be satisfied in order to allow or deny access to an information system under its control. 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.
    3. The set of rules is defined in a policy is configured on the CipherTrust Manager and downloaded to the agent through a secure TLS network connection. It provides separation of duties between data owners, administrators, key managers, and security managers.

- **CipherTrust Manager Login –** The CipherTrust Manager has both a web-based and command-line GUI that can be configured for both administrator and role based separation.

- **Separation of Domains and Roles** – One of he functions of the CipherTrust Manager 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 numberof 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 "guard points" enforces Least Privilege that is defined in an Information System's Security Plan, Concept of Operations, and proven through testing.

2. AWARENESS TRAINING

- Deployment of CipherTrust Transparent Encryption is a part of program's Defense-In-Depth security architecture to protect sensitive data through fine grained access controls and encryption for data at rest. On initial deployment, Thales TCT Professional Services Group and a host of learning options (in-class, online) are used to train staff to use the solution. CipherTrust Transparent Encryption has low administrative burden. Available training covers tasks and responsibilities for each desired/deployed role, with appropriate documentation provided.

3. AUDIT AND ACCOUNTABILITY

- Agent activity is closely monitored and logged. All auditable events, including backups, restores, and security operations can be logged at the CipherTrust Manager or at the hosts. The CipherTrust Manager is capable of storing up to 110,000 audit messages. The following audit event content is provided:
  - 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 CipherTrust 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. Audit data is collected in an open Syslog format and can be integrated with several SIEM and log correlation tools.
- When the agent component of CipherTrust Transparent Encryption cannot contact the central manager (CipherTrust 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 CipherTrust Manager. By sending agent Host OS logs to an audit reduction or network monitoring tool, correlations can be created with the appropriate alerting.

4. SECURITY ASSESSMENT AND AUTHORIZATION

- CipherTrust 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.
  - The following ports and protocols are required for operation:

Protocol	Port	Communication Direction	Purpose
TCP	22	Workstation -> CM	SSH Access for CLI Management
TCP	22	CM -> HSM	SSH Communication for Hardware Security Modules (if using Luna Network HSM, TCT Luna T-Series Network HSM, or AWS Cloud HSM)
TCP	80	Workstation -> CM	HTTP Access for UI Management
TCP	443	Workstation -> CM	HTTPS Access for UI Management
TCP	443	HSM -> CM	HTTPS for DPoD HSM on Demand Service
TCP	5432	CM <-> CM	PostgreSQL for Cluster Heartbeat/Information Exchange
TCP	9000	Agent -> CM	NAE-XML server/interface
TCP	5696	Agent -> CM	KMIP (Key Management Interoperability Protocol) Interface
TCP	1792	CM -> HSM	If using Luna Network HSM, TCT Luna T-Series Network HSM, or AWS CloudHSM
TCP	123	CM -> NTP Server	Network Time Protocol
TCP	514	CM -> Syslog	Syslog
ICMP	6514	CM -> Syslog	Syslog
ICMP	161	Agent -> CM	SNMP
UDP	162	CM -> Agent	SNMP

* Note: The CipherTrust Manager will automatically use Suite B communications unless ports 8446, 8447, 8448 are not available. If not available (or communicating with older versions of an agent that does not support Suite B), communications fall back to using Ports 8443, 8444, 8445 and TLS/RSA encrypted communications

5. CONFIGURATION MANAGEMENT

- The configuration of the CipherTrust Manager 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.

6. CONTINGENCY PLANNING

- The CipherTrust Manager can operate in a clustered environment and can be added to a program's COOP/DR strategy.

***7.* IDENTIFICATION AND AUTHENTICATION**

- CipherTrust 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
  - Applications
- Policy configuration can be fine-tuned to select:
  - 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 guard point
- Each CipherTrust agent is cryptographically signed by a certificate authority generated by the CipherTrust Manager in order to identify and authorize access and encryption/ decryption operations on the host system. The CipherTrust Manager is available as a FIPS 140-2 Level 3 hardware appliance.
- The CipherTrust Manager 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.
- On the CipherTrust Manager 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.
- Communication between CipherTrust Manager andagents are cryptographically signed by the CipherTrust Manager's certificate authority and passed in an encrypted format (AES256).

8. INCIDENT RESPONSE

- CipherTrust Transparent Encryption processes incidents at the individual component level (host system, web GUI, CipherTrust Manager).
- 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.
- Log formats can be tailored to match a program's security policy for user and application behavior.

9. MAINTENANCE

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

10. MEDIA PROTECTION

- As required by FIPS 140-2 level 3 certification, the CipherTrust Manager has the ability to be zeroized at the appliance console.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION

- The CipherTrust Manager dimensions are 19" x 1ru. The CipherTrust Manager:
  - Can be installed into a standard locking rack enclosure.
  - Is available as a FIPS 140-2 Level 2 or 3 certified configuration (level 3 is tamper resistant)

12. PLANNING

- CipherTrust Transparent Encryption provides fine-grained access policies that can be used to limit privileged user access and implement least-privileges principles for users authorized for access to sensitive data. Thales TCT's Technical Services team includes top subject matter experts who can help organizations to architect secure and efficient solutions for managing and controlling privileged access and access to their data.
- Key and policy management is centralized using CipherTrust Transparent Encryption.

13. PERSONNEL SECURITY

- The CipherTrust Manager 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

14. RISK ASSESSMENT

- CipherTrust Transparent Encryption can be a part of a risk assessment process at both components in its architecture in an information system; The CipherTrust Manager and host agents.
  - The CipherTrust Manager is FIPS 140-2 Levels 1 or 3 certified depending on model.
  - The CipherTrust encryption agents are installed on servers in an Information System that should meet security hardening and STIG guidance.

15. SYSTEM AND SERVICES ACQUISITION

- The CipherTrust Manager is a FIPS 140-2 Level 3 appliance.

16. SYSTEMS AND COMMUNICATIONS PROTECTION

- CipherTrust 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.
  - The solution is platform independent
  - Security functions on the CipherTrust Manager are isolated from normal operation and include domain creation, key creation, host creation, and audit-only.
  - Once a system's data has been encrypted through data transformation, it remains encrypted at rest and is under fine-grained access controls.
  - 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 CipherTrust Manager and agent is selectable.
  - CTE uses REST API for communicating over TLS 1.2 channel with CM.
- There is secure transmission control between the CipherTrust Manager, the daemon running on the host, and the SecFS portion that sits in the host's kernel space. The CipherTrust Manager creates a public/private key pair, generates a Certificate Signing Request (CSR), which generates a certificate authority certificate that is stored in the CipherTrust Manager database.
- The user space portion of the CipherTrust 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 CipherTrust Manager, where the request is signed, sent back to the host, and creates a "blueprint" of the host, along with the certificate.
- 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 CipherTrust Manager.
- Keys are passed between the CipherTrust Manager and the host by generating a one-time AES256 random key on the CipherTrust Manager. 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
- The CipherTrust Manager 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 CipherTrust Manager, which is a FIPS 140-2 hardened appliance.

17. SYSTEM AND INFORMATION INTEGRITY

- CipherTrust Transparent Encryption monitors an information system at these points, and creates audit data on::
  - CipherTrust Manager
  - CipherTrust Manager Web-based GUI
  - Host Agents Host logon
- CipherTrust 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:
  - 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, e.g. 9am-5pm M-F)

18. 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 CipherTrust Transparent Encryption addresses.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

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