thalescpl.com

THALES

SafeNet Data Protection On Demand

White Paper

Contents

Executive Summary

SafeNet Data Protection On Demand is a cloud-based platform that provides a wide range of on-demand encryption and key management services through a simple online marketplace. With SafeNet Data Protection On Demand, security is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain. Just click and deploy the services you need, provision users, and get usage reporting in minutes.

This document discusses the measures Thales has taken to ensure the security, robustness, and availability of the SafeNet Data Protection On Demand (DPoD) Service.

Major Takeaways

- SafeNet Data Protection On Demand uses a multi-tenant, and multi-tier architecture
- The architecture leverages Hardware Security Module (HSM) technology to ensure that only authenticated administrators have access to a tenant's key materials
- The scalable nature of SafeNet Data Protection On Demand ensures high-availability and disaster recovery
- All network traffic in and out of the solution is encrypted
- Thales regularly runs vulnerability and penetration tests to ensure robustness
- All data centers are certified to industry security and privacy standards

Introduction

In the past, enterprises have preferred to manage every aspect of their data protection strategy in-house due to the sensitive nature of the data they have access to, but the trend of outsourcing this function to organizations that specialize in the subject matter expertise necessary to manage an end-to-end data protection solution is gaining momentum and acceptance. Outsourcing this critical business component is allowing enterprises to focus more on their core competencies, and less on developing and maintaining sufficient data protection strategies. Many enterprises are enjoying the benefits of trusting a Managed Security Service Provider (MSSP) with their security needs.

Today's security strategy includes coverage areas such as breach prevention, meta-data protection, compliance requirements, security audits, and understanding when and how to integrate industry best practices for end-to-end data protection, just to name a few. This list of focus areas is ever growing, and is on the verge of out-pacing most enterprises' abilities to staff enough individuals that have the necessary experience to create and sustain an effective end-to-end data protection strategy. Fortunately, these are the subject matter areas where MSSPs thrive; they are equipped with the expertise to work closely with an enterprise to develop an ideal data protection solution that will address an overwhelming majority of their business use cases. Among the numerous benefits to the enterprise are the ability to reduce data protection capital expenditures, minimize data protection strategy implementation times and eliminate the routine tasks associated with maintenance, and refocus security and IT teams to working on value-add projects that align with the enterprise's core competencies. For any enterprise to invest in outsourcing their data protection strategy to an MSSP, it is imperative that they be confident in the fact they will be receiving comprehensive security paired with privacy solutions that can sufficiently protect their data—whether at rest, in motion, or in use—without the capital investment needed to manage critical security requirements.

This white paper details the general architecture of the SafeNet Data Protection On Demand service powered by Thales, and the functional and operational security measures put in place by Thales to ensure the high availability, privacy, and protection of customer data.

An Inside Look at SafeNet Data Protection On Demand

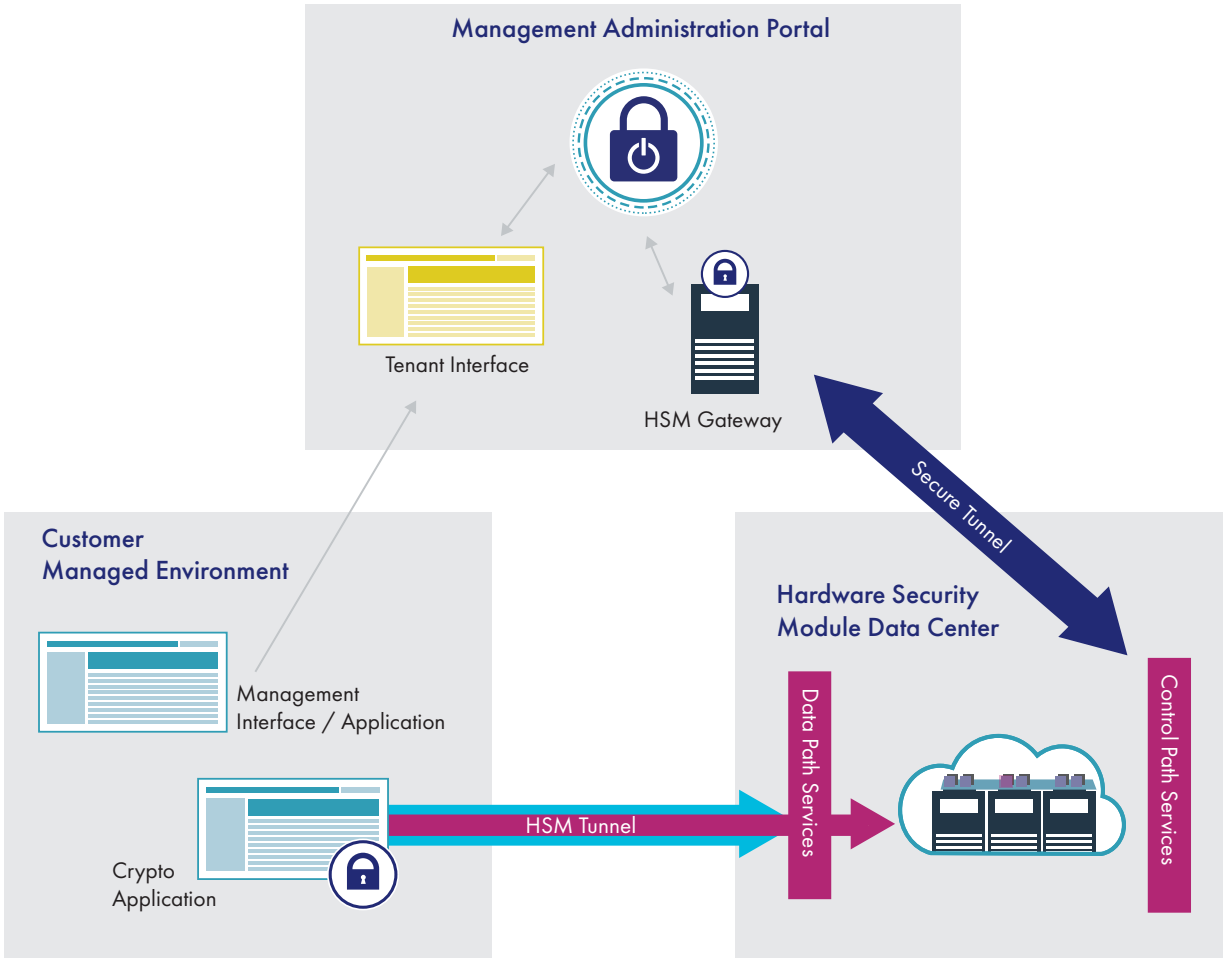
The SafeNet Data Protection On Demand service spans multiple environments. The SafeNet HSM and supporting software based services, are designed from the ground up with security in mind. They are stored in trusted, audited data centers which have been strategically positioned globally to maintain proximity with customer data. They also employ a micro-service architecture to enable a high degree of isolation and enable additional security controls such as rapid patching, credential rotation, and repaving of the environment.

The micro-service, cloud native architecture and Platform-as-a-Service (PaaS) layer gives Thales the flexibility to deploy on multiple Infrastructure-as-a-Service (IaaS) environments.

The data centers housing the physical HSMs are located in Europe and North America. Use of key material and Security Officer typical operations, such as management of the HSM, is performed by the service owner using externally created and managed credentials, to which Thales has no access.

A connection to an HSM On Demand instance goes from the client application to the HSM. There are two independent cryptographic tunnels protecting the information which flows between the client and the HSM, including an outer HTTPS tunnel which terminates at the service boundary, and another which is established between the HSMs and client.

When a client is given access to an HSM On Demand service, the service is completely empty and contains no secrets. The client must take control by initializing the service and creating the Security Officer and Crypto Officer for the HSM. The Security Officer is in sole possession of the secrets required to authenticate and manage the Crypto Officer role from this point. Without those credentials, no one (including Thales) has the ability to access the keys.



Multi-Tenant and Multi-Tier Structure

The HSM datacenter operates in a multi-tenant mode where HSMs can be loaded and scaled across the infrastructure. Access to the HSMs devices are credentials created by the customer (service owner) and they cannot be accessed by the rest of the environment. The supporting services in the datacenter operate as a scheduler and orchestrator ensuring that HSM services are always available.

At the platform level in the management portal, tenants are organized into sub-tenants in a multi-tier fashion.

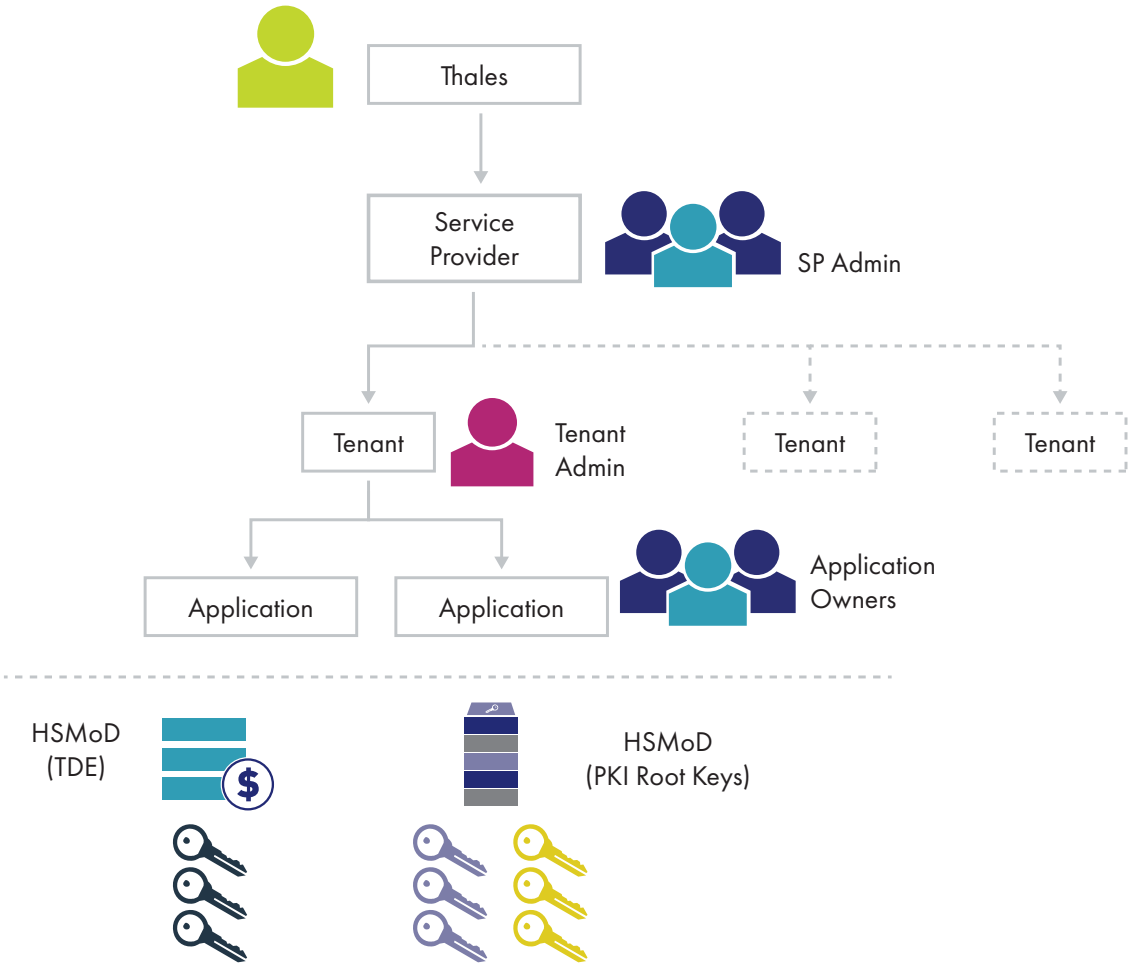
Data stored within the platform for tenant management is limited to the services which require it in a least privileged model.

SafeNet Data Protection On Demand is structured with multiple tiers in mind, allowing for parent-child relationships. This design allows Service Providers to make SafeNet Data Protection On Demand available to their customers and to white label it so it looks and operates as if it was a native service. At the top level, there is a Thales tier where the generic shared services execute.

Within a tier there are Tenant Administrator accounts which can view all the services and users within that tier. A level below the Tenant Administrator is the Application Owner. Application Owners are placed in logical groupings called subscriber groups and only have access to services within their subscriber group.

The parent of a tier can see data about the accounts and metadata useful for billing, but has no access to any confidential material such as secrets or keys.

The figure below illustrates the multi-tier and multi-tenant, environment.



Hardware Security Modules (HSM)

HSMs are secure cryptographic processing devices purpose-built for managing and protecting encryption keys. They are tamper-resistant, and protected from physical or logical attempts to break into the device and gain access to the encryption keys. The HSMs used for SafeNet Data Protection On Demand are FIPS 140-2 Level 3 certified. For the HSM On Demand instances, the service will generate initial private keys for tunnel establishment from clients to the boundary of the HSM On Demand layer. These keys are used to enable a connection to the HSM On Demand service boundary only. The key is one factor in allowing a connection to be opened to the environment.

Once the client application establishes the tunnel to the service boundary, it will perform attestations that it is talking to a valid SafeNet HSM and establish a shared session key. All of the secure communication between the client and HSM is protected by negotiated keys completely opaque to all other levels of the system.

HSM Supply Chain Security

The HSMs used for SafeNet Data Protection On Demand are manufactured in a secure facility, operated by a Thales contracted manufacturer. During manufacturing, the devices generate their own identity (RSA 4096-bit key), which is signed by the manufacturing key. The manufacturing key is in turn signed by a Thales root. This PKI is leveraged to identify genuine SafeNet HSMs.

Root Key Generation Ceremonies are performed for each Point of Presence under strict guidelines, in accordance with leading industry best practices. Segregation of Duties is maintained at all times under dual custody and strict oversight, ensuring that the chain of custody is maintained throughout the ceremony and for the life of the root key pair and its associated assets.

Communication between HSM cards establishes an ephemeral tunnel and is authenticated using key material chaining to the device identity (Hardware Origin) key/certificate. A device cannot be a member of multiple domains and; the device must be reset to factory conditions before it can join another domain. Service devices cannot perform administrative actions such as adding new members to the domain.

SafeNet Data Protection On Demand Client Software

The SafeNet Data Protection On Demand HSM client software is available for Linux and Windows operating systems. The client software provides standard cryptographic APIs (PKCS#11, Java JCA/JCE, Microsoft CAPI/CNG, and OpenSSL) for applications to perform cryptographic operations in high-assurance hardware. The library establishes a TLS tunnel to the service endpoint, and an internal AES 256-bit tunnel which is established with the HSM service. The HSM On Demand service may be resident on multiple physical HSMs and may be migrated for load management, but only authenticated HSMs, which are part of the same service pool, may decrypt the data coming from the client. The transport key is derived independently for each HSM On Demand service. A successful connection/authentication with an HSM allows the HSM to deliver a transport key (AES 256-bit) and associated metadata (including a nonce) to the client.

Privacy and Compliance

Compliance

Thales uses data centers where all internal operations have been certified to the highest standards for data security, privacy controls, and operational reliability put in place by industry standards organizations. SafeNet Data Protection On Demand physical data centers in North America received an Independent Service Auditor's Report (SOC2) on Controls Relevant to Security and Availability. This is a Type 2 Report—a report on management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls. SafeNet Data Protection On Demand physical data centers in Europe have been awarded ISO 20771 certification.

SafeNet Data Protection On Demand operations, and operations-related IT is fully compliant with the ISO 27001:2013 standard, having achieved independent certification to ISO27001 for its Information Security Management System and processes.

In addition, SafeNet Data Protection On Demand has received SOC 2 certification, proving compliance with the defined five trust service principles, security, availability, processing integrity, confidentiality, and privacy.

Data Privacy

For many years, the European Union (EU) has had a formalized system of privacy legislation, which is regarded as more rigorous than that found in other areas in the world. Thales hosts the SafeNet Data Protection On Demand environment within data centers located in Europe and North America, in countries recognized by the EU Commission as offering adequate levels of protection.

Data which flows into the HSMs is completely opaque and only decrypted within the FIPS boundary of an HSM.

Point-of-Presence (PoP) Redundancy and Security

SafeNet Data Protection On Demand utilizes a distributed architecture consisting of a hosted web application and private data center based HSM hosting. The solution architecture addresses the availability concern, taking into account the specificities of the Cloud Provider. Best practices for availability are continually enforced from the early stages of the system design. The SafeNet Data Protection On Demand architecture has been designed and deployed with full redundancy, ensuring availability.

Safeguarding Data—Data Backup and Recovery

Within the cloud, Thales relies on snapshots to keep copies of storage volumes associated with the application instances. Snapshots are taken daily and deleted weekly. The retention period for snapshots is 1 week. Database backups are managed using relational database backups. Application logs are kept online for 3 months and securely stored for one year. Data is kept for a period of time that is related to the relative compliance specific to the region where the data is being stored.

In addition, a service wide restoration test is performed annually. For this test, a tape is recalled from off-site storage and the data is restored to a test environment.

Thales deploys a formal Disaster Recovery plan. The plan is maintained and tested on an annual basis. Any issues identified during the test are formally discussed and remediation plans are put in place. In addition, Thales has a formal Business Continuity plan, which is reviewed annually to determine if updates are required.

Procedures to address minor processing errors and outages are documented.

Data Center Physical Security

Physical security underpins any cloud-based service, so all data centers have 24-hour manned security, including foot patrols and perimeter inspections with access controls complying with industry best practices. This may vary based upon the data center but can include proximity, biometric, key, PIN or a combination of any of those controls listed. The data centers are fully equipped with video surveillance throughout each facility and their perimeters with tracking of asset removal, ensuring that equipment and security of data held within that equipment is assured. The data centers also utilize state of the art technologies ensuring redundancies in connectivity, power, safety and security.

The following is a list of physical security features of the SafeNet Data Protection On Demand Service:

- Video surveillance cameras are spread throughout each facility
- 24x7 manned protection—no unsecured access to the data center
- Multi-factor authentication is used at all times for entrance to the data center

Network Resilience

The private data center is provided with multi-vendor and neutral-network connections to major Internet Service Providers (ISPs), and is located near major Internet hubs so that Thales can retain the ability to select the most resilient network at any time. Network connections to the data centers are provided using secure links with high-capacity bandwidth over fiber connections to ensure minimum latency of authentication requests turn-around. All fiber-based connections enter the data center buildings via secure concrete vaults.

The internal network infrastructure of the PoP is built upon a high speed fiber based network to ensure high-capacity throughput. This infrastructure uses multiple connections through highly secured network firewalls and routers to deliver full redundancy, as well as optimal traffic delivery. The following is a list of network security features of SafeNet Data Protection On Demand Service PoPs:

- Data centers are network carrier neutral
- Multiple fiber channels at each data center
- Use of multiple Internet Service Providers to ensure continuous and high-bandwidth Internet access

Power Supply Redundancy

Power is delivered to the data centers using an underground utility power feed, which is then supplemented and backed up by on-site redundant (N+1) diesel generators with local diesel fuel storage. Power is delivered into the rooms via redundant (N+1) CPS/UPS systems to ensure ongoing supply, with power delivered to the PoP equipment racks using redundant power distribution units (PDUs).

Threat Monitoring at Thales

Thales's company-wide mission statement extends to those individuals that work on and with SafeNet Data Protection On Demand. The SafeNet Data Protection On Demand's control environment reflects the company's philosophy concerning the importance of the robustness of such a fundamental information security service. As Thales's core business is data protection, the company has several teams that constantly monitor Thales's ecosystem to address new risks and vulnerabilities, as well as to identify ways of mitigating them. Monitoring logs exist to track activity in the key applications and firewalls, and they are reviewed on a weekly basis. Proper separation of duties is in place between individuals accessing the log and individuals reviewing the log

Intrusion detection is deployed throughout the internal network in order to capture and report events to a security event management system for logging, alerts, and reports—thus delivering a high degree of network traffic auditability. A reputable third-party service provider scans the network externally and alerts of changes in the baseline configuration to increase audit levels. Additional levels of network traffic monitoring are conducted on a 24x7 basis across key points within the infrastructure and automated reports are delivered on a daily basis to the network administrator.

Within each PoP, a sophisticated network of routers and firewalls ensures network separation, integrity, and confidentiality of the data and access to that data. Within the network itself, internal firewalls segregate traffic between the application and database tiers to ensure confidentiality and integrity, as well as deliver a high level of availability.

Service Penetration Testing

Thales applications undergo regular application and network penetration testing by third parties, and SafeNet Data Protection On Demand adheres to this practice. The assessment methodology will include structured review processes based on recognized "best-in-class" practices as defined by such methodologies as the ISECOM's Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP), Web Application Security Consortium (WASC), and ISO 27001:2013 Information Security Standard.

A grey-box approach of the application security audit is adopted for the purpose of the audit. The following figure shows some of the security attack vectors that are being tested. Any issues found are resolved as part of the regular development cycle.

- Application Spidering
- Authentication Testing
- Session Management Testing
- Data Validation Testing
- Ajax Testing
- Business Logic Testing
- Risk Assessment
- Reporting

Thales Internal Controls and Procedures

This section describes the different procedures and controls that are taken by Thales to ensure the security and robustness of the service. The processes and procedures described below refer to measures implemented internally by Thales in its offices and development centers.

Security of Internal Networks and Information Technology

Thales utilizes Antivirus software within the SafeNet Data Protection On Demand cloud environment and Antivirus software is utilized on workstations. Virus definitions are updated in real time as they are released and monitoring is performed in real-time.

A third-party service provider scans the network externally and alerts the Thales Security Team regarding changes in the baseline configuration to increase audit levels. Additional levels of network traffic monitoring are conducted on a 24x7 basis across key points within the infrastructure and automated reports are delivered on a daily basis to the network administrator.

Monitoring logs exist to track activity in the key applications and firewalls. These logs are retained and reviewed as per audit policy. Proper separation of duties is in place between individuals accessing the log and individuals reviewing the log.

Logical Access

The following sections describe Thales's logical access policy with regard to SafeNet Data Protection On Demand.

Criteria for Logical Access

Only Thales employees and contractors whose job responsibilities require logical access to the environment are provided access. For the production environment, this is limited to the following personnel:

- Personnel with administrative responsibilities for the SafeNet Data Protection On Demand service
- Personnel with responsibilities to maintain the network and systems
- Personnel with responsibilities to deploy code

Requests for Logical Access

Requests for access are submitted as a ticket in the Thales ticketing system. Requests are reviewed by the SafeNet Data Protection On Demand Infrastructure Manager and approved by the Sr. Director of Infrastructure and Operations before access is granted.

Once a request is approved, access is provisioned by a member of the Technical Support team.

Note that this process is strictly governing internal access to the system for administrative or operational reasons. This process is not intended to cover external users.

Requests include the following information:

- Specific list of devices where access is required
- Level of access required, and
- Business justification for access

Revocation of Logical Access

Access grants are removed if one of the following events occur:

An employee terminates their employment, which is managed through the Separations process. When employment is terminated, HR creates a formal notice that is provided to the employee's manager. The employee's manager creates a ticket within Thales's internal ticketing system requesting that the employee's access be revoked. Additionally, if the employee has access to a shared or administrator level account, a request is made to have the password changed on that account. The ticket is sent to and completed by a member of the Technical Support team.

The job function of the employee changes and their new role no longer requires access. Changes in employee status are noted in a weekly report and reviewed to see if changes in logical access are warranted.

Review of Personnel with Logical Access to the SafeNet Data Protection On Demand Environment

The SafeNet Data Protection On Demand Infrastructure Manager maintains a listing of all personnel with access to the operational environment. The authorized access list is reviewed and signed-off monthly by the Sr. Director of Infrastructure. If this manager determines that an individual no longer needs access, he/she requests that access be revoked by the Technical Support team.

Privileged Accounts Access

The credentials associated with privileged accounts (Administrator for Windows or root for Linux) are known by only two senior individuals:

- SafeNet Data Protection On Demand Infrastructure Manager, and
- Client Services Engineer

In addition, a copy of the privileged account credentials is maintained in a sealed envelope in the company safe.

Logical Access Monitoring

Logical access to the SafeNet Data Protection On Demand Infrastructure is monitored as follows:

- Use of Local Admin accounts, privileged accounts, as well as access to the SafeNet Data Protection On Demand databases. These logs are reviewed on a weekly basis by the Sr. Director of Infrastructure, who does not maintain the prior mentioned levels of access being reviewed.
- Access to and actions taken through the operator console are monitored via the monthly operator console report.

Physical Access & Environmental Controls

Scope

This procedure applies globally to all facilities that house Thales computing assets. This includes corporate data centers, third party data centers (including those used to host SafeNet Data Protection On Demand), server rooms, and server closets. Each of these facilities is secured in accordance with this policy.

Physical Access

Access to Thales data centers/computer rooms is strictly limited to personnel who have a job requirement that necessitates physical access to the data center. The following criteria is used in determining who can be allowed unescorted physical access:

- Thales employees responsible for the facility itself including the electrical and mechanical systems supporting the facility
- Thales employees directly responsible for the support and maintenance of computing and network equipment housed in the facility
- Thales employees designated to provide local hands and eyes in support of server and network maintenance/troubleshooting

A member of the local Corporate Information Services staff is designated by the Sr. Director of Global infrastructure to act as the local data center manager. This individual handles requests for data center access and ensures all personnel who are granted access meet the criteria above.

New Requests for Data Center Access

New requests for data center access are submitted as a help desk ticket and assigned to the appropriate data center manager. The ticket should include a justification indicating they meet the access criteria. Once the data center manager has verified that the requester meets the criteria, the data center manager emails a request to the Facilities Manager authorizing the Facilities Manager to grant access.

Termination of Data Center Access

Physical access to the data center is revoked from employees who leave the company, or whose job responsibilities change such that they no longer meet the access criteria. The data center manager is alerted of a termination through the Thales Separation process.

Physical Access Monitoring

Access logs are reviewed on a quarterly basis to ensure that only authorized individuals access the data center. Attempts to gain unauthorized access are investigated to see if they warrant escalation to Thales Security personnel. Emails and documentation associated with such investigations are maintained. The access list is reviewed bi-annually to ensure personnel on the list should continue to have access.

Problem Management

When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.

If customers and external users wish to inform Thales of possible security breaches and other incidents, they can do so by visiting http://www.Thales.com/csirt/index.

Change Management

Thales maintains two separate change management policies for changes required to SafeNet Data Protection On Demand. The first discusses changes to the IT environment while the second discusses changes in the software deployed as part of the service.

Engineering Group

The engineering group is responsible for design, development, testing and operation of the software deployed as part of the service in a devops model that includes in-service upgrades and incident response. A number of infosecurity and cryptography specialists are security specialists on the team. The security specialists are responsible for design issues related to the robustness of the system, for crypto-analysis based on specific engineering requirements, and for code-reviews where the robustness of the reviewed software is examined.

Thales engineering teams are working using a formal Application Development Lifecycle methodology. SafeNet Data Protection On Demand is developed using the agile development methodology that ensures quick, yet reliable turnaround between requirements gathered until service delivery. The agile methodology enables Thales to react quickly to new risks and changes in the global threat analysis.

IT and Service Operations Change Management

Thales maintains a formally documented Change Management policy and procedure that outlines how changes to Thales cloud computing environments are controlled. The policy is reviewed and updated on an annual basis. All changes are tested and signed-off by the tester and/or applicable business owner. Evidence of testing and the requisite approvals are attached to the change request ticket.

Emergency changes follow the standard change management process on an expedited timeline. However, unlike normal changes, approvals for emergency changes may be obtained after the fact within a reasonable time period.

Application Change Management

Thales's process was developed to ensure change to corporate applications and infrastructure are completely tested and approved prior to being implemented in the production environment. Based upon this commitment, the following change management process is being followed and practiced by all Corporate Information Services personnel.

All proposed changes to production environments/applications are subject to this policy. No changes may be made to production environments/applications without approval from the Change Management Approvers group.

All change requests are discussed and decisions are made during the weekly change management meeting. Ad-hoc requests can be made for changes that must be completed within 24 hours. The requester must attach:

- Change management requests
- Evidence of testing

Requests submitted without any of these documents, are not accepted. While all change management requests are managed by a Change Management Tracking application located on the corporate intranet, ad-hoc requests are communicated and approved using emails to the change management committee using a designated committee.

Ad-hoc requests are kept for archival purposes in the Change Management Tracking system as well.

Change Management Meeting

The purpose of this meeting is to review current in progress Change Management requests as well as requests which were submitted since the last Change Management meeting. This meeting occurs weekly and is attended by representatives of each of the core Information Solutions and Services (ISS) teams:

- ISS—Infrastructure
- ISS—Applications
- ISS—Security
- ISS—Help Desk
- Technical Support

Engineering Change Management

Thales maintains a formally documented development life-cycle policy and process. SafeNet Data Protection On Demand is developed using the agile development methodology that ensures quick, yet reliable turnaround between requirements gathered until service delivery, and each release is accompanied by an approved Engineering Test Report (ETR).

All changes are developed and tested by the appropriate engineering teams in development sprints. All changes are tested and signed-off by the QA team leader and SafeNet Data Protection On Demand product manager. Evidence of testing and the requisite approvals are documented in the engineering project tracking system.

System Software Change Management

To ensure service security and robustness, Thales engineering teams are working using a formal Application Development Lifecycle method. SafeNet Data Protection On Demand is developed using the agile development method that ensures quick, yet reliable turnaround between requirements gathered until service delivery. The agile methodology enables Thales to react quickly to new risks and changes in the global threat analysis.

Requirements Definition

Product managers gather requirements as part of their day-to-day duties. In accordance with Thales's development methodology, these requirements are turned into user-stories. The input for these user-stories arrives from analysis of the market, requirements from Thales prospects and customers as well as innovative ideas coming from Thales's CTO Office or from the engineering teams.

As part of this step, threat modeling is carried out. The process considers the macro cyber-security environment and all known attacks. Changes to the current working assumptions are translated into user-stories and gain work priority during Sprint Planning.

Sprint Planning

Sprints are followed as the process of developing/coding to meet a specific requirement. Development sprints are scheduled on a periodic basis. the team in consultation with product management and engineering leaders evaluate the user-stories in the backlog and decide on the content of the specific sprint.

Sprint Testing

After all the different teams working on a specific sprint submit their developed code, sprint testing is shared responsibility within the engineer team and is carried out by on a continual basis by the team. Following successful testing, code undergoes source-code review, and walk-throughs are conducted regularly using a structured approach. Throughout the testing phases, an emphasis is put on security related aspects. In addition to the above testing, unit testing is performed by each developer.

Implementation

Upon approval, developed code is released into the production SafeNet Data Protection On Demand environment.

- Penetration testing: Penetration testing is done on a dedicated non-production system, but runs in the same environment as the operational service.
- At the last stage, all data is backed up from the operational service, which allows Thales to rollback immediately in case of any unexpected challenges.

Thales Organizational Structure and Functions

Thales's unwavering commitment to data security, privacy, and availability is a top-down approach that encapsulates everyone—from executives to individual contributors and contractors. The following is the organizational structure, functions and roles of the group that runs and manages SafeNet Data Protection On Demand:

- **Corporate.** Executives, senior operations staff, and company administrative support staff, such as legal, training, contracting, accounting, finance, and human resources.
- **Service Operation/Technical Support.** Staff that administer SafeNet Data Protection On Demand providers, and take care of the daily operations related to SafeNet Data Protection On Demand. SafeNet Cloud Operations administer the entire SafeNet service offering.
- **Engineering group.** The group develops and maintains the entire SafeNet Data Protection On Demand portfolio. Members of this group are located in Thales offices in Austin, Texas, Belcamp, Maryland, Tewksbury, Massachusetts, Ottawa, Canada and Noida, India. These groups are responsible for service design, development, and quality assurance aspects. In addition, these groups are responsible for information security and cryptography design aspects as well as business continuity design issues.

Information security and availability aspects are handled by three different groups:

- The engineering group is responsible for designing software elements that protect critical data and for the secure development of all software elements.
- The service operations group is responsible for the deployment aspects of information security and availability. In some cases they are helped by information security and networking specialists from Thales's IT group.
- Employees are subject to background checks as part of the initial hiring process, and undergo performance reviews during employment. In addition, Thales has a formalized whistleblower hotline and policy.

Frequently Asked Questions

Data protection and data separation

Q: How do you separate "my data" from other customers' data?

A: Tenant Administrators have access only to the data that belongs to their account. Tenant specific details and/or metadata are protected at rest using volume encryption.

Q: Does Thales, my Service Provider, or anyone else have access to my encryption keys stored in an HSMoD service?

A: When the HSM On Demand instance is initialized, the service owner creates passwords or phrases for both the Security Officer and Crypto Officer roles. Those secrets are used in a derivation scheme and are required to allow the HSM to unseal the cryptographic material. Only the Security Officer/Crypto Officer are in possession of those secrets. It is left to the discretion of those officers to share the credentials as needed.

Q: How strong is your encryption and data integrity?

A: Tenant specific details and/or metadata are protected at rest using volume encryption. Within each PoP, a sophisticated network of routers and firewalls ensures network separation, integrity, and confidentiality of the data and access to that data. Within the network itself, internal firewalls segregate traffic between the application and database tiers to ensure confidentiality and integrity, as well as deliver a high level of availability.

Vulnerability management

Q: Can you show evidence of your vulnerability management program?

A: Thales software applications undergo regular application and network penetration testing by third parties. The assessment methodology includes review processes based on recognized "best-in-class" practices as defined by such methodologies as the ISECOM's Open Source Security Testing Methodology Manual (OSSTMM), the Open Web Application Security Project (OWASP), Web Application Security Consortium (WASC), and ISO 27001:2013 Information Security Standard

Q: What is your vulnerability remediation process?

A: When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.

Prior to the actual service update the following tasks are performed:

Provisioning Testing: This is done on the updated service in a controlled environment and done by the Thales Service Operations team. With the conclusion of these tests the code has passed 3 rounds of testing successfully, each done by a different group: Unit testing done by the developer, Sprint Code Testing done by the QA group, and Service Update Provisioning Testing done by Service operations.

A Planned Release Notification (PRN) is sent to all existing customers notifying them on the scope of the update and planned date of actual service update

Penetration testing: Penetration testing is done on a dedicated non-production system, but runs in the same environment as the operational service.

At the last stage, all data is backed up from the operational service, which allows Thales to rollback immediately in case of any unexpected challenges.

Q: How often do you scan for vulnerabilities on your network and applications?

A: We conduct monthly reviews of all patches for servers and network equipment

Physical and personnel security

Q: Is there restricted and monitored access to critical assets 24x7?

A: Yes. Only Thales employees and contractors whose job responsibilities require logical access to the environment are provided access. For the production environment, this is limited to the following personnel:

- Personnel with administrative responsibilities for the SafeNet Data Protection On Demand service
- Personnel with responsibilities to maintain the network and systems
- Personnel with responsibilities to deploy code

Requests for access are submitted as a ticket in the Thales ticketing system. Requests are reviewed by the SafeNet Data Protection On Demand Infrastructure Manager and approved by the Sr. Director of Infrastructure and Operations before access is granted. Once a request is approved, access is provisioned by one of the Technical Support team. Note that this process is strictly governing internal access to the system for administrative or operational reasons. This process is not intended to cover external users.

Logical access to the SafeNet Data Protection On Demand Infrastructure is monitored as follows:

- LogRhythm is used to monitor use of Local Admin accounts, privileged accounts, as well as access to the SafeNet Data Protection On Demand Databases. These logs are reviewed on a weekly basis by the Sr. Director of Infrastructure, who does not maintain the prior mentioned levels of access being reviewed.
- Access to and actions taken through the operator console are monitored via the monthly operator console report.

Application security

Q: Do you follow OWASP guidelines for application development?

A: Yes, we follow OWASP guidelines.

Q: Do you have a rigorous testing and acceptance procedure for outsourced and packaged application code?

A: Thales maintains a formally documented development life-cycle policy and process. SafeNet Data Protection On Demand is developed using the agile development methodology that ensures quick, yet reliable turnaround between requirements gathered until service delivery. All changes are developed and tested by the appropriate engineering teams in development sprints. All changes are tested and signed-off by the QA team leader and SafeNet Data Protection On Demand product manager. Evidence of testing and the requisite approvals are documented in the engineering project tracking system.

Q: What application security measures do you use in your production environment (e.g., application-level firewall, database auditing)?

A: Thales utilizes Antivirus software within the SafeNet Data Protection On Demand cloud environment and Antivirus software is utilized on workstations. Virus definitions are updated in real-time as they are released and monitoring is performed in real-time. A third-party Service Provider scans the network externally and alerts the Thales Security Team regarding changes in the baseline configuration to increase audit levels.

Incident response

Q: What is your procedure for handling a data breach?

A: When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.

Compliance requirements

Q: Are your data centers under local compliance requirements?

A: SafeNet Data Protection On Demand is based on a number of strategically located global Points-of-Presence (PoPs). One PoP is in Europe and the other in North America, and conform to local compliance requirements.

For many years, the EU has had a formalized system of privacy legislation, which is regarded as more rigorous than that found in other areas of the world. Companies operating in the European Union are not allowed to send personal data to countries outside the EU unless there is a guarantee that it will receive adequate levels of protection. Thales hosts the DPoD environment within data centers located in Europe and North America. Data privacy protection can also be afforded by limiting the amount of personal information needed to utilize the service. The minimum SafeNet Data Protection On Demand personal data requirement is, email address, first and last name.

Q: Are you ISO-2700X compliant?

A: SafeNet Data Protection On Demand operations, and operations-related IT is fully compliant with the ISO 27001:2013 standard, having achieved independent certification to ISO27001 for its Information Security Management System and processes.

In addition, SafeNet Data Protection On Demand has received SOC 2 certification, proving compliance with the defined five trust service principles, security, availability, processing integrity, confidentiality, and privacy.

Reporting options

Q: Is it possible to monitor for service availability?

A: There is a SafeNet Data Protection On Demand service status dashboard available for all customers.

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.

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) Ltd
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

> thalescpl.com <

© Thales - October 2019 • ELC, v2