SafeNet Authentication Service

SECURITY WHITE PAPER

SafeNet Authentication Service Security Considerations

Contents

Executive Summary 2
Introduction 3
General Service Architecture 4
Multi-Tenant and Multi-Tier Structure 5
User Store Synchronization 6
OTP Seed Protection 6
Token Manufacturing, Fulfillment and Seed Delivery 7
SafeNet Authentication Service Software 7
Privacy and Compliance 7
Point-of-Presence (PoP) Redundancy and Security 8
Service Penetration Testing 11
SafeNet Internal Controls and Procedures 12
SafeNet Organizational Structure and Functions 18

Executive Summary

Service robustness and high-availability are two of the main concerns when enterprises are considering a cloud-based offering; even more so when the offering is a fundamental data security solution, such as strong authentication and identity management. This document discusses the measures SafeNet has taken in ensuring the robustness of SafeNet Authentication Service (SAS).

Major Takeaways

- SafeNet Authentication Service supports a multi-tenant/multi-tier architecture, ensuring data separation between tenants of the service.
- The scalable architecture of SafeNet Authentication Service ensures high availability and disaster recovery.
- Customer user stores are synchronized with SafeNet Authentication Service using a lightweight synchronization agent. All communication between this agent and the SAS point of presence (POP) is encrypted with AES256 encryption running on a Secure Tunnel, which comprises an application layer tunnel on top of an SSL tunnel.
- Service Points of Presence run at military grade datacenters, ensuring physical protection, network protection and monitoring, as well as network and power resilience.
- SafeNet regularly runs tests at the application and network layers to ensure the robustness of the SAS.
- SafeNet Authentication Service has undergone SSAE 16 SOC 2 certification and was audited for high-availability and robustness. This document is based, in part, on the audit report. In addition SafeNet Authentication Service is undergoing ISO 27001 certification. This certification is expected to be finalized during 2013[1].

[1] SafeNet Authentication Service Point-of-Presence Datacenters are ISO 27001 certified. The current certification process applies to SafeNet and the service itself.

Introduction

For more than a decade, the software industry has been shifting towards service-based solution delivery. This is true for security solutions, including multi-factor authentication. Indeed, according to Gartner's User Authentication Magic Quadrant 2013, "By 2017, more than 50 percent of enterprises will choose cloud-based services as the delivery option for new or refreshed user authentication implementations, up from less than 10 percent today."

One of the main concerns when moving to a cloud-based service delivery model is the robustness and availability of the solution. These concerns increase when delivering info-security solutions from the cloud, and more so when offering a fundamental solution, such as user authentication, which is a critical layer in the organization's info-security architecture.

SafeNet, a leader in the user authentication and data protection markets, sees great importance in assuring its customers that information security services offered by SafeNet comply with the highest security standards.

The purpose of this document is to present the security and data protection methodologies and technologies SafeNet uses to ensure the robustness and continuous availability of SafeNet Authentication Service, as well as the procedures and controls that SafeNet has in place.

General Service Architecture

This chapter outlines the general architecture of SafeNet Authentication Service. SafeNet Authentication Service is hosted in two Points-of-Presence (PoP), each of which is a replica of the other (see Figure 1). The architecture is scalable in the sense that more PoPs and more service instances per PoPs can be added to support higher authentication traffic, as well as additional geographic regions.

User data is synchronized from the customer's user repository to the hosted environment using SafeNet Authentication Service's Directory Sync Agent, and a secure tunnel between the agent and the users' database in the PoP. Authentication requests are handled by RADIUS and SAML protocols that are considered to be secured and trusted.

Access to the service for customers and service providers is delivered via the Administrator's Portal. Connection to this portal is secured via HTTPS, ensuring that users have a secure connection from their browsers. Prior to being given access to the portal, each administrator must authenticate to the Service using their personally issued two-factor authentication token.

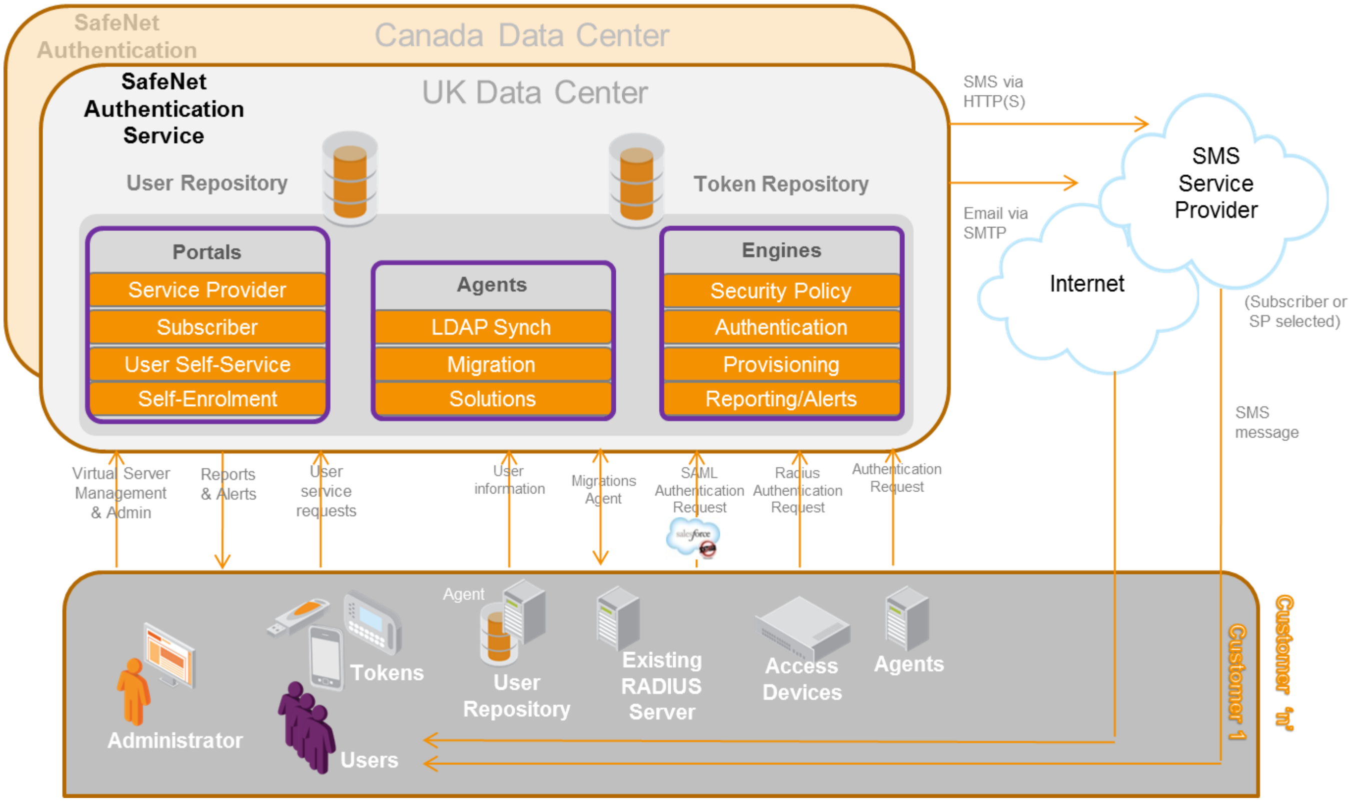

Figure 1: SafeNet Authentication Service High-Level Architecture

Multi-Tenant and Multi-Tier Structure

SafeNet Authentication Service is structure in a secure multi-tenant environment, where the information of each account is separated from the other. The Service uses a hierarchy of parent-child relationships for all accounts, whereby there is a central root account from which all sub-accounts are derived, up to an infinite level. That being said, privacy is protected in the chain, as an account can only be viewed and managed by its parent unless the account has explicitly delegated control to its grandparent or has explicitly invited an external operator to manage its operation. Figure 2 illustrates this multi-tier environment.

Administrators have access only to the users that belong to their account. The sensitive information related to each account is stored with an AES256 encryption key. Any attempt to access information in the Service database requires an encryption key. These encryption keys are needed not only for reading the data, but also for copying, moving, deleting, or restoring items (rows) in the database.

SafeNet Authentication Service is planned to be integrated with a Hardware Security Module (HSM) ensuring that key management of each account's data encryption key, including creation, usage and storage, are performed using SafeNet's HSM.

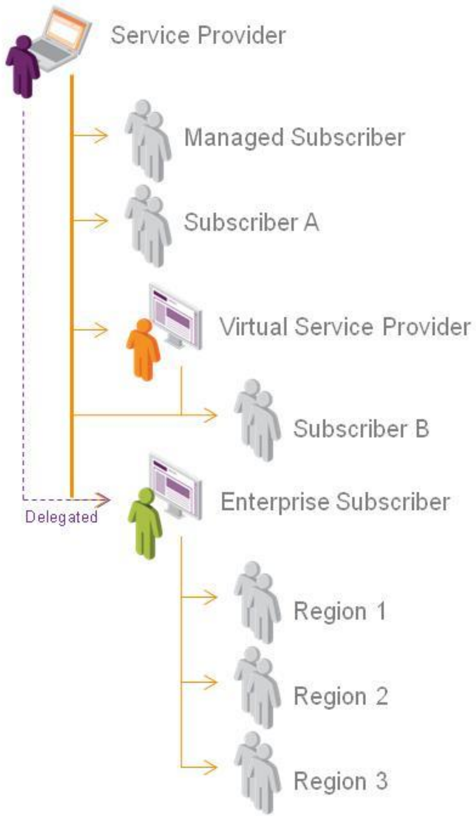

Figure 2: SAS in Multi-Tier Environment

User Store Synchronization

Synchronization between a customer's User-Store and the SafeNet Authentication Service User Repository is performed using an on-premises agent. The agent's key features are:

- LDAP Support: The agent can be used with almost any LDAP Directory Server. The agent supports custom LDAP schemas.
- Supports a large number of user stores and databases, besides LDAP, including Active Directory, and many more
- Non-Intrusive: The agent does not write to the user repository and does not require any scheme change.
- An administrator account is not required in order to connect to the Directory Server.
- Multiple Directory Servers can be synchronized.
- Secure Tunnel: All communication between the Synchronization Agent and SafeNet Authentication Service is encrypted with AES 256 encryption. In addition, an SSL secure tunnel is supported between the LDAP Synchronization Agent and the LDAP Directory Server. AES key exchange is done by AES key wrapping using RSA 1024-bit keys.

OTP Seed Protection

One Time Password solutions use a secret that is shared between the user's authenticator and the authentication server, which serves as a root of trust from which a publicly known mechanism creates the random One Time Password. These shared secrets are called OTP Seeds.

SafeNet Authentication Service encrypts the OTP Seed database using a FIPS 140-2 Level 3-designed Hardware Security Module (HSM)[2]. Hardware Security Modules (HSMs) are secure cryptographic processing appliances used for managing and protecting encryption keys, and accelerating cryptographic processes (in that sense, it acts as a cryptographic accelerator) for high-performance environments. The FIPS 140-2 Level 3 designed HSM is tamper-resistant, and is protected from physical or logical attempts to break into the device and gain access to the keys.

The use of HSMs will ensure that OTP Seed records and authentication secrets never exist in a decrypted form in the host memory and cannot be copied or stolen, and will provide a unique level of security, and will ensure robust and secure service delivery.

[2] HSM is planned to be supported in a future release of SafeNet Authentication Service version.

Token Manufacturing, Fulfillment and Seed Delivery

SafeNet hardware tokens are manufactured in a secure facility, operated by a SafeNet contracted manufacturer. While in transit between the token manufacturer and SafeNet fulfillment centers, and between the fulfillment centers and SafeNet's customers, OTP Seed records are encrypted using AES 256 encryption.

While at rest, Seed files are stored in a database and protected using a FIPS 140-2 certified hardware based database encryption tool (SafeNet's DataSecure).

SafeNet offers its customers a unique ability to re-program the Seed values of customers' hardware tokens in the field after tokens have been delivered. In such cases, the new Seed values need to be uploaded to SafeNet Authentication Service. This is done using the Service's Administrator Console. In such cases, the customer is responsible for the Seed protection of the Seed-data copies retained in the customer environment.

SafeNet Authentication Service Software

SafeNet Authentication Service was developed as a Microsoft Windows server application which is supported by a Microsoft SQL Server database, and is maintained by SafeNet's in-house software engineering group. The software engineering group develops and maintains SafeNet Authentication Service to provide multi-factor authentication services for the company's customers.

Privacy and Compliance

Compliance

SafeNet Authentication Service has undergone SSAE 16 SOC 2 assessment, and has been audited for high-availability and robustness. In addition, the Service is undergoing ISO 270001 certification. This process is expected to be completed in 2013.

Data Privacy within the European Union and Switzerland

The European Union (EU) has for many years 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. The Safe Harbor Privacy Principles allows US companies to register their certification if they meet the European Union requirements3.

[3] Source: International Safe Harbor Privacy Principles on Wikipedia.

SafeNet self-certifies annually to the Safe Harbor privacy principle and voluntarily agrees to meet the stringent privacy directives. Further to Safe Harbor certification, SafeNet hosts the SAS environment within data centers located in the United Kingdom and Canada. Further, data privacy protection can be afforded by limiting the amount of personal information need to utilize the service. SafeNet Authentication Service keeps this personal data to a minimum by using a username and email address.

Point-of-Presence (PoP) Redundancy and Security

SafeNet Authentication Service is based on a number of strategically located global Points-of-Presence (PoP). One PoP is in the UK and the other is in Canada.

The two PoPs operate under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), ensuring that sensitive information is protected under the Canadian privacy law and that the Canadian PoP complies with EU privacy regulations and vice versa

The datacenters are fully redundant at every point, be it Internet connectivity, network switching, or application and database access between the centers, as well as hot standby of all equipment within the datacenters. SafeNet Authentication Service Point-of-Presence Datacenters are ISO 27001 certified and ensure network separation between applications. They allow for multi-factor authentication for specific applications. All these are mandatory requirements for PCI-DSS compliance.

Data Backup and Recovery

Each PoP is essentially a mirror image of the other. Within each data-center, two instances of the database are maintained, which results in a total of four replicated instances of SafeNet Authentication Service data. To mitigate data corruption and loss risks, a daily back up of the data used by the service is written to tape from the Canadian Data-Center. An SQL log file is generated and written to tape each day. In addition, a backup of each server is taken from one instance in the Canadian Data-Center. Each server is backed up fully every week, with daily incremental updates. Once a week, a tape is sent off site for disaster recovery purposes.

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

SafeNet 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, SafeNet has a formal Business Continuity plan, which is reviewed annually to determine if updates are required.

Procedures to address minor processing errors, outages, and disposition of records are documented, including redundant servers, and daily backups of each server to disk.

Datacenter Physical Security

Physical security underpins any cloud-based service and so all datacenters have 24-hour manned security, including foot patrols and perimeter inspections with biometric scanning for access. SafeNet Authentication Service PoPs (i.e., the Service datacenters) 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.

SafeNet's equipment within the datacenter is housed within dedicated concrete-walled rooms, with all computing equipment located in access-controlled steel cages – again assuring a high level of protection over both equipment and data.

The following is a list of physical security features of SafeNet Authentication Service PoPs:

- Each PoP is surrounded by 3.5 meter/11.5 feet high perimeter fence.
- Army-trained guard dogs patrol the perimeter fence.
- The PoPs walls are 3 meter/10 feet thick.
- All doors within the datacenter are made of solid steel.
- Video surveillance cameras are spread throughout each facility.
- Protection against electromagnetic pulse attacks.
- 24x7 manned protection - no unsecured access to the datacenter.
- Three-factor authentication used for entrance to the datacenter.

Network Resilience

Each PoP is provided with multi-vendor and neutral-network connections to major Internet Service Providers (ISPs), and is located near major Internet hubs so that SafeNet can retain the ability to select the most resilient network at any time. Network connections to the datacenters 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 datacenter 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 Authentication Service PoPs:

- Datacenters are network carrier neutral
- Multiple fiber channels at each datacenter
- Use of multiple Internet service providers to ensure continuous and high-bandwidth Internet access

Power Supply Redundancy

Power is delivered to the datacenters 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).

Redundant air conditioning units guarantee stable temperature and humidity levels that are needed for proper operation of the datacenters.

Disaster Recovery

Each user's access device will typically be set up to connect to both a primary and a secondary PoP. As SafeNet Authentication Service performs real-time data replication between datacenters, should the primary connection fail, the customer's device will automatically authenticate users to the secondary PoP without any service interruption.

Data between PoPs is transmitted across encrypted links using AES256-based encryption to create a trusted and secure tunnel between the sites. Regular disaster recovery tests are conducted to verify projected recovery times, as well as prove the ongoing integrity of customer data within the PoPs, ensuring that the data was not changed in the backup and restore processes.

Network Security and Monitoring – Assuring Integrity

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.

Intrusion detection monitoring 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 third-party service provider continuously 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.

Service Penetration Testing

SafeNet undergoes regular application and network penetration testing by third parties. The assessment methodology includes 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 Information Security Standard.

A grey-box approach of application security audit is adopted for the purpose of the audit. Figure 3 shows the security attack vectors that are usually being tested during such tests. To date, no major security issues were found in these penetration tests, and all minor issues are being fixed as part of the regular development cycle.

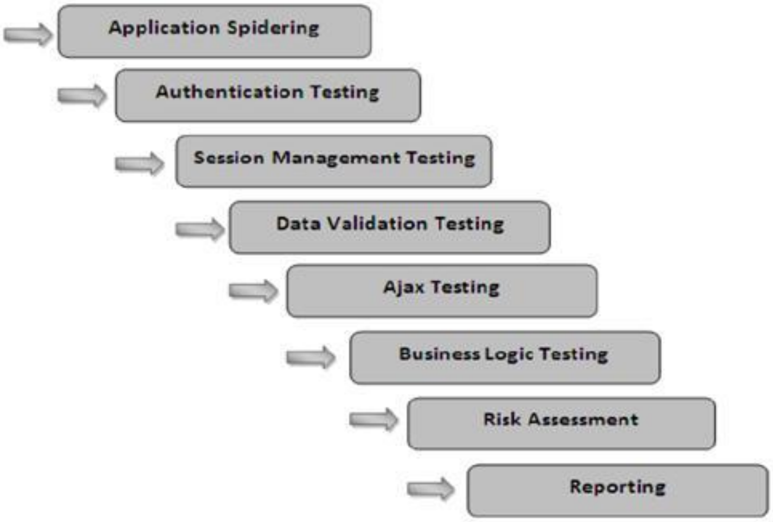

Figure 3: Application security attack vectors tested in Penetration Testing

SafeNet Internal Controls and Procedures

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

Security of Internal Networks and Information Technology

SafeNet utilizes Kaspersky Antivirus software within the SafeNet Authentication Service cloud environment and Trend Micro Antivirus software is utilized on workstations. Virus definitions are updated on a daily basis and monitoring is performed in real-time.

Intrusion detection monitoring 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 third-party service provider continuously scans the network externally and alerts the SafeNet 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 reviewed weekly by the Director of Infrastructure Technology. Proper segregation of duties is in place between individuals accessing the log and individuals reviewing the log.

Logical Access

The following sections describe SafeNet's logical access policy in regard to SafeNet Authentication Service.

Criteria for Logical Access

Only SafeNet 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 SAS service;
- Personnel with responsibilities to maintain the network and systems; and
- Personnel with responsibilities to deploy code.

Requests for Logical Access

Requests for access are submitted as a ticket in the SafeNet ticketing system. Requests are reviewed by the SafeNet Authentication Service 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.

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 occurs:

- 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 SafeNet's internal ticketing system requesting that the employees' 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 SAS environment

The SAS 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 Authentication Service Infrastructure Manager/Client Services Engineer; 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 Authentication Service Infrastructure is monitored as follows:

- LogRhythm is used to monitor use of Local Admin accounts, privileged accounts, as well as access to the SAS 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 SafeNet computing assets. This includes corporate data-centers, third party data centers (including those used to host SafeNet Authentication Service), server rooms, and server closets. Each of these facilities is secured in accordance with this policy.

Physical Access

Access to SafeNet 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 are used in determining who can be allowed unescorted physical access.

- The local Facility Security Officer (FSO)
- Assistant FSO (if one is designated)
- SafeNet employees responsible for the facility itself including the electrical and mechanical systems supporting the facility
- SafeNet employees directly responsible for the support and maintenance of computing and network equipment housed in the facility
- SafeNet 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 SafeNet Separation process. Changes in job responsibilities are reviewed weekly through the Weekly Status Report of New Hires, Separations, and Status Changes.

Physical Access Monitoring

The Data-Center Manager reviews the access logs to ensure that only authorized individuals accessed the data-center on a monthly basis. Attempts to gain unauthorized access are investigated to see if they warrant escalation to SafeNet 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.

The process for customers and external users to inform SafeNet of possible security breaches and other incidents is posted on the SafeNet website and is provided as part of the User Welcome Kit.

Change Management

SafeNet maintains two separate change management policies for changes required to SafeNet Authentication Service. 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, and testing of the software deployed as part of the service. A number of info-security and cryptography specialists are working as the security specialists in 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.

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

IT and Service Operations Change Management

SafeNet maintains a formally documented Change Management policy and procedure that outlines how changes to SafeNet 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

SafeNet'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. 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 on every Wednesday and is attended by representatives of each of the core Corporate Information Services (CIS) teams:

- CIS - Infrastructure
- CIS -Applications
- CIS - Security
- CIS - Help Desk
- Technical Support

Engineering Change Management

SafeNet maintains a formally documented development life-cycle policy and process. SafeNet Authentication Service 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 Authentication Service 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, SafeNet engineering teams are working using a formal Application Development Lifecycle method. This SafeNet Authentication Service is developed using the agile development method that ensures quick, yet reliable turnaround between requirements gathered until service delivery. The agile methodology enables SafeNet 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 SafeNet's development methodology, these requirements are turned into user-stories. The input for these user-stories arrives from analysis of the market, requirements from SafeNet prospects and customers as well as innovative ideas coming from SafeNet's CTO Office or from the engineering teams.

As part of this step, threat modelling 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. For each sprint, product management, engineering leaders as well as representatives from the CTO office evaluate the user-stories that are still open 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 carried out by SafeNet Quality Assurance group who perform black-box testing on the entire Sprint code. 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 Authentication Service environment. Developers are restricted from migrating changes into the production environment.

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 SafeNet 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 that is not in use, 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 SafeNet to rollback immediately in case of any unexpected challenges.

SafeNet Organizational Structure and Functions

Following is the organizational structure, functions and roles of the group that runs and manages SafeNet Authentication Service:

- **Corporate***.* Executives, senior operations staff, and company administrative support staff, such as legal, training, contracting, accounting, finance, and human resources.
- **Service Operations/Technical Support**. Staff that administers SafeNet Authentication Service providers, and take care of the daily operations related to SafeNet Authentication Service. SafeNet Cloud Operations administers the entire SafeNet service offering.
- **IT**. Help desk, IT infrastructure, IT networking, IT system administration, IT information security, and IT operations personnel manage electronic interfaces and implementation support and telecom.
- **Engineering group*.*** The group develops and maintains the entire SafeNet authentication solutions portfolio. Members of this group are located in SafeNet offices in Belcamp, MD, USA; Petach Tikva, Israel; Ottawa, Canada; and Concord, CA, USA. 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 two 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 SafeNet's IT group.
- Employees are subject to background checks as part of the initial hiring process. During employment, employees undergo annual performance reviews. In addition, SafeNet has established a formalized whistleblower hotline and policy.

Management Philosophy

SafeNet, Inc.'s companywide mission statement extends to those individuals that work on and with SafeNet Authentication Service. SafeNet Authentication Service's control environment reflects the philosophy of senior management concerning the importance of the robustness of such a fundamental information security service as SafeNet Authentication. As SafeNet's core business is data-protection, the company has several teams that constantly monitor SafeNet's ecosystem to address new risks and vulnerabilities, as well as to identify ways of mitigating them.