PCI DSS Secure Implementation Guide For Huawei Cloud Engine product

Version : 0.2

Status : Release

Last Update : 2015-06-15

Classification: atsec & Huawei confidential

Huawei Technologies Co.,Ltd

Bantian, Longgang district, Shenzhen, 518129, P.R.China

http://www.huawei.com

Version History

Version	Date	Author	Changes
0.1	2015-04-09	Xiangdong Gao	Initial Release
0.2	2015-06-15	Li Zhang	Technical Review
0.3		Xiangdong Gao	Revised according to customer onsite result.

Classification

This document is classified as “Confidential”.

This classification level is for highly sensitive information. Access to "atsec confidential" information is limited to employees with a need to know. Information classified "atsec confidential" may be given to external persons with a need to know if they have signed an appropriate Non-Disclosure Agreement (NDA). Access to "atsec confidential" information stored on central IT systems must be controlled. Anyone obtaining information classified “atsec confidential” must apply the protection mechanisms necessary to ensure that the information cannot be obtained by anyone who does not have explicit authorization.

Information with this classification shall be clearly marked “atsec confidential” when it is in human-readable form. Electronic or other media storing information with this classification in unencrypted form shall be protected from any unauthorized access and shall be subject to specific handling procedures when they are reused or destroyed.

Copies of information classified “atsec confidential” shall only be made when necessary and must be strictly controlled.

Table of contents

List of tables

List of figures

Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

This PCI DSS Secure Implementation Guide provides a guideline for Huawei's Cloud Engine products (including 5800, 6800, 7800,12800 and 12800S series) Version V100R005C00 being implemented in a PCI DSS-compliant manner.

The PCI DSS Secure Implementation Guide is provided to instruct customers and resellers/integrators on secure product implementation, to document the secure configuration specifics mentioned throughout this document, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements.-

1.1 Basic Information

Item	Description
Product Manuafacturer	Huawei Technologies Co.,Ltd
Business Location	Bantian, Longgang District,Shenzhen 518129, P.R.China
URL	http://www.huawei.com/
Product Version	V100R005C00
Product Identification	Cloud Engine CE7800 series, including CE7850-32Q-E1.
	Cloud Engine CE6800 series, including CE6810-48S4Q-E1,CE6850-48S4Q-E1, CE6850-48T4Q-EI.
	Cloud Engine CE5800 series, including CE5810-24T4S-EI, CE5810-48T4S-EI, CE5850-48T4S2Q-EI, CE5850-48T4S2Q-HI, CE7850-32Q-EI,CE6851-48S6Q-HI, CE6850U-48S6Q-HI, CE6850U-24S2Q-HI, CE6850-48T6Q-HI, CE6850-48T4Q-EI, CE6850-48S6Q-HI, CE6850-48S4Q-EI, CE6810-48S-LI, CE6810-48S4Q-LI, CE6810-48S4Q-EI, CE6810-32T16S4Q-LI, CE6810-24S2Q-LI, CE5855-48T4S2Q-EI, CE5855-24T4S2Q-EI, CE5850-48T4S2Q-HI, CE5850-48T4S2Q-EI, CE5810-48T4S-EI, CE5810-24T4S-EI
	Cloud Engine CE12800 series, including CE12804, CE12808, CE12812,CE12816, CE12804S, CE12808S

Table 1 Basic Product Information

1.2 Target readers

The Secure Implementation Guide is provided to instruct customers and resellers/integrators on secure product implementation, to document the secure configuration specifics mentioned throughout this document, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements.

The target readers of this document are customers and resellers/integrators of Huawei Cloud Engine products. Customers & Resellers/Integrators could use this document for the configuration and implementation, so that Huawei Cloud Engine products facilitate and not prevent PCI DSS compliance of cardholder data environment.

This solution is targeted toward the following audiences:

- Technical or compliance-focused individuals seeking guidance on how to holistically design and configure for PCI compliance

- Organizations that require a qualified security assessor to provide a Report of Compliance
- Organizations interested in preparing for growth that will someday require a Report of Compliance.

Although all organizations that take credit cards are required to be PCI compliant, this solution is designed to help the larger companies simplify the complexity of compliance. Smaller companies can benefit from the design and guidance as well, but should consult their acquiring banks for specifics if they do not currently require an onsite audit. Specific card programs are available at the following locations to determine their specific categorization process;

- American Express—http://www.americanexpress.com/datasecurity
- Discover Financial Services—http://www.discovernetwork.com/fraudsecurity/disc.html
- JCB International—http://www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide—http://www.mastercard.com/sdp
- Visa, Inc.—http://www.visa.com/Cisp

1.3 Version of the PCI DSS

PCI SSC. 2015, Data Security Standard: Requirements and Security Assessment Procedures November 2015 Version 3.1
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

1.4 PCI DSS Requirements Overview

The PCI DSS requirements apply to all system components within the cardholder data environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The following high level 12 Requirements comprise the core of the PCI DSS:

- Build and Maintain a Secure Network
  - 1. Install and maintain a firewall configuration to protect data
  - 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - 3. Protect Stored Data
  - 4. Encrypt transmission of cardholder data and sensitive information across public networks
- Maintain a Vulnerability Management Program
  - 5. Use and regularly update anti-virus software
  - 6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - 7. Restrict access to data by business need-to-know
  - 8. Assign a unique ID to each person with computer access
  - 9. Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - 10. Track and monitor all access to network resources and cardholder data
  - 11. Regularly test security systems and processes
- Maintain an Information Security Policy
  - 12. Maintain a policy that addresses information security

The remainder of this document describes the essential guidance for implementing Huawei's Cloud Engine appliance in a PCI compliant environment.

----------Blank below in this page----------

2 Security features descpription

2.1 Network-level Access Control

IP-based advanced/user ACL is provided for this situation to identify traffic flow by matching all or part of IP source address, IP destination address, IP protocol number, TCP/UDP source port number, TCP/UDP destination port number etc, then to proceed with certain actions like rate limit, prioritization or discard.

2.2 Security Administration feature

The Huawei Cloud Engine product provides communication security by implementing SSH/SFTP protocols.

To protect the Cloud Engine product from eavesdrop and to ensure data transmission security and confidentiality, SSH/SFTP provides:

- Authentication by local AAA password and/or external RADIUS/HWTACACS password;
- AES encryption algorithms for password storage;
- RSA/DSA encryption algorithms for password transmission.

Besides default TCP port 22/21, manually specifying a listening port is also implemented since it can effectively reduce attack.

2.3 User account management feature

User privilege is managed by access level. There are total 16 access levels ranging from 0 ~ 15. The bigger number, the higher privilege. Correspondingly, 16 levels are assigned to all commands provided. A user can access those commands if the commands access level is less or equal to the user's access level.

By default, commands are registered with level 0 ~ 3.

- Level 0: visit level, network diagnostic commands like ping, tracert, can be executed.
- Level 1: monitor level, mainly used for system maintenance, including display commands.
- Level 2: configure level, to add, modify, or delete service configuration.
- Level 3: manage level, to support servicing, including operations on file system, changing configuration files, command level management, debugging commands for system diagnosis.

If a more subtle classification on commands are preferred, corresponding access level of these commands are to be modified, ranging from 0 ~ 15. The user access level must also be modified, respectively.

2.4 Secure Authentication feature

The authentication functionality provides validation by user's account name and password. Detailed functionalities, for example max idle time, max log-in attempts, UI lock, user kick out, can be applies by administrator according to networking environment, customized security considerations, differential user role on the Cloud Engine product, and/or other operational concerns.

2.5 NTP feature

NTP (Network Time Protocol) is an application layer protocol used on the internet to synchronize clock among a set of distributed time servers and clients. In this manner, the clock of the host is synchronized with certain time standards.

NTP synchronizes all the clocks of devices (switches, PCs, and routers) on the network so that these devices can provide multiple applications based on the uniform time.

2.6 Secure Audit feature

The log feature of the Huawei Cloud Engine products records all administrative accesses and operations on the product and events that occur to the product. The recorded events are log messages. Log messages provide evidence for diagnosing and maintaining a system. Log messages reflect the administrative status of the product and are used to analyze the conditions of a network and to find out the causes of network failure or faults.

Key elements of log messages include event time, event origination, user identification, event type, result, severity, brief description, etc.

Information hierarchy is designed to help the user roughly differentiate between information about normal operation and information about faults. Since the information center needs to output information to the terminal, console, log buffer, SNMP agent, and log file, ten information channels are defined and the channels work independently from each other.

---------- Blank blow in this page ----------

3 Compliance Requirements

3.1 Compliance Environment Definition

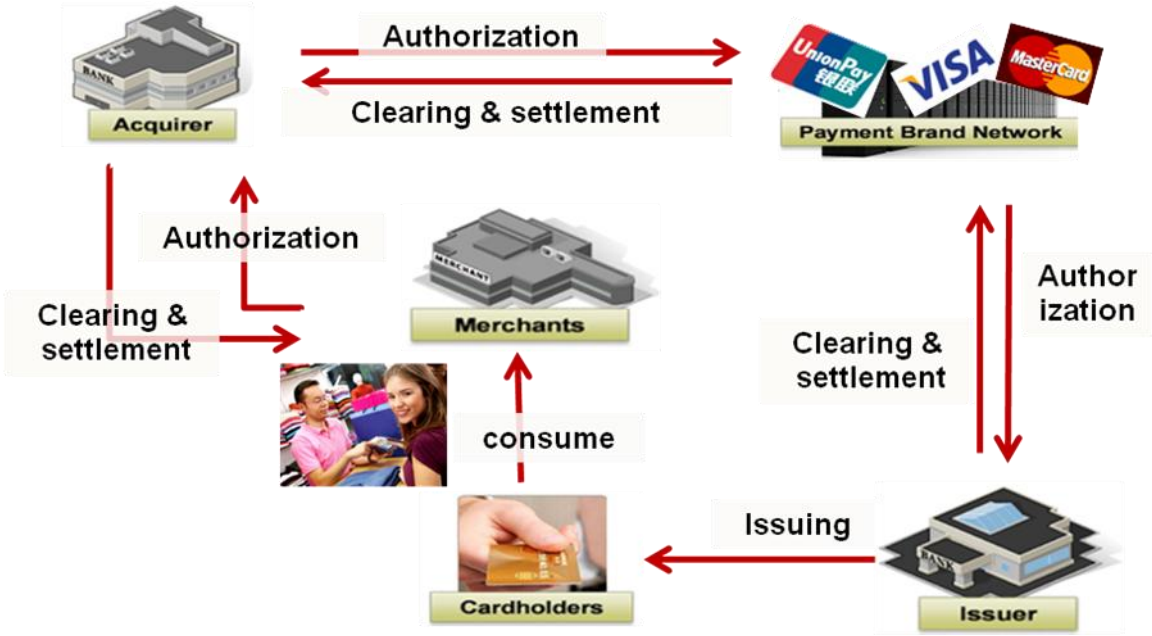

Figure 1 Involved Roles in PCI DSS Payment Process

As defined by PCI SSC (Payment Card Industry Security Standards Council), there are some roles shown above are generally involved in the processing, storage and transmission of card holder data, ie. Merchant, Acquirer, Service provider, issuer.

In a typical payment processing process, the payment business flows include the following business types:

- Payment Gateway/Switch

This type includes various businesses for merchants and cardholders, such as credit card repayment for cardholders, MAS (Merchant Acquiring Service), MPOS, etc.

- Clearing & settlement

Generally, clearing business deals with the financial balance between acquirer/card brands and issuer, settlement business handles the financial balance between acquirer and merchants.

Additionally, there are also administrative accesses generated by internal operational and maintenance employees (normally network administrators, system administrators, etc).

Huawei Cloud Engine products are hardware network appliances that work in the network environment of the customer.

Chapter	Compliance Requirement	Related ecurity features
1	1.2, 1.2.1, 1.2.2	Network-level access control
2	2.1,2.2, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3, 8.2.1	Secure administration
6	6.1, 6.2	Timely Development and Deployment of Security Patches
7-8	7.1, 7.1.1, 7.1.2, 7.2.2,7.2.3 8.2, 8.1.1, 8.1.2, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3, 8.5	User access control
10.4	10.4.1, 10.4.2, 10.4.3	Accurate time synchoronization

10	10.1, 10.2, 10.2.2, 10.2.3, 10.2.5, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5, 10.5.3	Audit trail monitoring

Table 2 Requirements and features mapping table

From the customer espect, PCI-related secure features should be properly implemented to ensure the compliance to PCI DSS. Here are the requirements and related implementation requirements.

3.2 Network-level Access Control

Related PCI DSS requirments
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
1.2.2 Secure and synchronize router configuration files.

Table 3 PCI DSS requirement of segmentation

Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. All other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement.

3.3 Secure Administration

Related PCI DSS requirments
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. **This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.**
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. **Sources of industry-accepted system hardening standards may include, but are not limited to:** *** Center for Internet Security (CIS)** *** International Organization for Standardization (ISO)** *** SysAdmin Audit Network Security (SANS) Institute** *** National Institute of Standards Technology (NIST)**
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. ***Note**: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.*

2.2.4 Configure system security parameters to prevent misuse.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access. ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.*
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

Table 4 PCI DSS requirements 2

Default accounts and passwords provides with attacks an easy way to get unauthorized accesses to appliances. Unnecessary services, protocols and daemons may introduce further threats, which have the risks of being compromised by hackers. A general process of security consolidation is shown below:

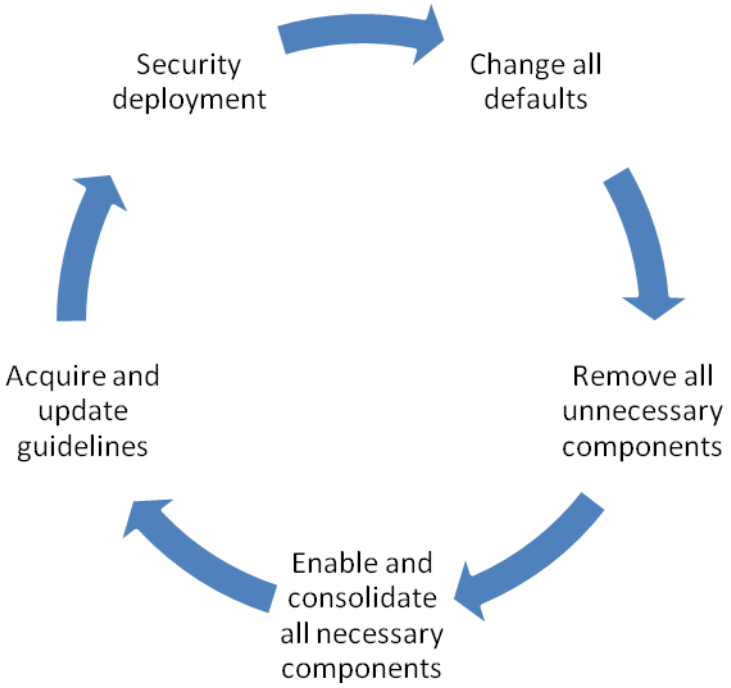

Figure 2 Security Consolidation Process

During the initial deployment and implementation, customer is suggested to acquire the guidelines and perform security consolidations, which includes following steps:

- change all vendor defaults, includes but not limited to administration password, SNMP community string and unnecessary accounts, especially during the initial deployment.
- disable unnecessary and unsecure services, protocols and daemons, especially FTP protocol, Telnet protocol, etc.
- enable these necessary services, protocols, then consolidate them to minimize security risks.
- Acquire and update vendor consolidation guidelines on a periodical basis, redo the consolidation tasks once new guidelines made available.

It is also suggested to introduce the items and benchmarks of security guidelines into the internal audit process, check and track the configuration changes at least annually.

During the transmission of administrative access, hackers may capture the whole packets, analysis and cracking the password to gain unauthorized access, so it is necessary to enable secure encryption for enabled administrative protocols with strong cryptographic protection. For the common protocols and options in the CLOUD ENGINE appliance, the security suggestions are listed below:

Protocols	Suggestion	Descriptions
SNMP protocol	Enable only when necessary.	1. Enable SNMP V3 if applicable. 2. Use strong cryptographic algorithm for the authentication, such as 3DES-128 bits, AES-128 bits or above. 3. Change default SNMP community strings to a some characters that are difficult to guess.
TFTP	Enable only when necessary.	1. Default to be disabled, enable only during the appliance maintenance. 2. Restrict source IP address and destination IP address if applicable.
FTP	Disable	Introduce strong cryptographic algorithms and replace FTP protocols with secure protocols, such as SSH, SFTP, etc.
Telnet	Disable	Introduce strong cryptographic algorithms and replace Telnet protocol with secure protocols, such as SSH, etc.
SSH	Enabled with consolidation	1. Enable SSH V2, if applicable. 2. Restrict the source and destination IP addresses if necessary. 3. Use strong cryptographic algorithm for the password protection, such as 3DES-168 bits, AES-128 bits or above.
SFTP	Enabled with consolidation	1. Restrict the source and destination IP addresses if necessary. 2. Use strong cryptographic algorithm for the password protection, such as 3DES-168 bits, AES-128 bits, RSA-2048 bits or above. 3. For public-facing SFTP/FTPS services, use trusted 3-party certificates if necessary.

Table 5 Suggestions to administrative protocols

If there are difficulties to enable secure protocols, it is accept to disable all remote non-console management protocols and perform administrative tasks over serial console.

3.4 User Access Control

Related PCI DSS requirments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
7.1.1 Define access needs for each role, including: *** System components and data resources that each role needs to access for their job function.** *** Level of privilege required (for example, user, administrator, etc.) for accessing resources.**
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
7.2.2 Assignment of privileges to individuals based on job classification and function.
7.2.3 Default "deny-all" setting.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-

consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: *** Something you know, such as a password or passphrase.** *** Something you have, such as a token device or smart card.** *** Something you are, such as a biometric.**
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
8.1.4 Remove/disable inactive user accounts at least every 90 days.
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: *** Enabled only during the time period needed and disabled when not in use.** *** Monitored when in use.**
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: *** Something you know, such as a password or passphrase.** *** Something you have, such as a token device or smart card.** *** Something you are, such as a biometric.**
8.2.3 Passwords/phrases must meet the following: *** Require a minimum length of at least seven characters.** *** Contain both numeric and alphabetic characters.** **Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.**
8.2.4 Change user passwords/passphrases at least every 90 days.
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
8.3 Incorporate two-factor authentication for remote network access originating from outside the network, by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: *** Generic user IDs are disabled or removed.** *** Shared user IDs do not exist for system administration and other critical functions.** *** Shared and generic user IDs are not used to administer any system components.**

Table 6 PCI DSS requirement 7-8

The PCI DSS requires that access to all systems in the cardholder data environment be protected through use of unique users and complex passwords.

Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. Additionally any default accounts provided by switches should be removed/disabled/renamed, or at least should have PCI DSS compliant complex passwords and should not be used.

Examples of default administrator accounts include “admin”, “administrator”, “root”, etc.

The PCI standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords

PCI user account requirements beyond and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

The PCI standard requires that if employees (such as internal business operators), administrators (such as network administrators, system administrators, etc), or external entities (such as product vendor, product resellers or integrators, external merchants) are granted remote access to the cardholder data environment, access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of remote access accounts created for external entities, in addition to the standard access controls, these accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If the customer should decide to remotely access the card holder data environment, these accesses should involved with two factor authentication scenarios (such as user password+ digital certificates, password+ token, Pincode+passcode, etc) for access outsidee the payment application environment.

Additionally, it should be advised that customers and its‘ external entities use all available user access security features. Examples of user security features and practices suggested are as follows:

- All access priviledges must be approved and assigned based on job postion and responsibilities.
- Role-based access controls should be enforced for all system components within the cardholder data envrionment. These system components should configured with “deny-all“ by default.
- All users are assigned with a unique ID for access to system components based on business necessity. Two-factor authentication is implemented for remote network access
- Generic user IDs and accounts are disabled or removed
- Shared user IDs for system administration activities and other critical functions do not exist
- Shared and generic user IDs are not in use to administer any system components
- Vendor ID follow password policies/procedures that group and shared passwords are explicitly prohibited
- No group and shared passwords are not distributed by system administrators, even if requested
- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses.

- ☐ Use strong authentication and complex passwords for logins
- ☐ Enable account lockout after a certain number (6) of failed login attempts
- ☐ Enable the logging function
- ☐ Restrict access to customer passwords to authorized reseller/integrator personnel

3.5 Accurate time synchoronization

Related PCI DSS requirments
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
10.4.1 Critical systems have the correct and consistent time.
10.4.2 Time data is protected.
10.4.3 Time settings are received from industry-accepted time sources.

Table 7 PCI DSS requirements 10.4

To have accurate time in all the CDE system components is as important as having a solid network security strategy. It is one of the primary components of a system administration based on good practices, which leads to organization and security. Specially when administering all CDE applications, web-servers, database servers or even a centralized audit trail monitoring mechanisms, accurate time is a must. Below diagram is a sample structure for NTP synchronization:

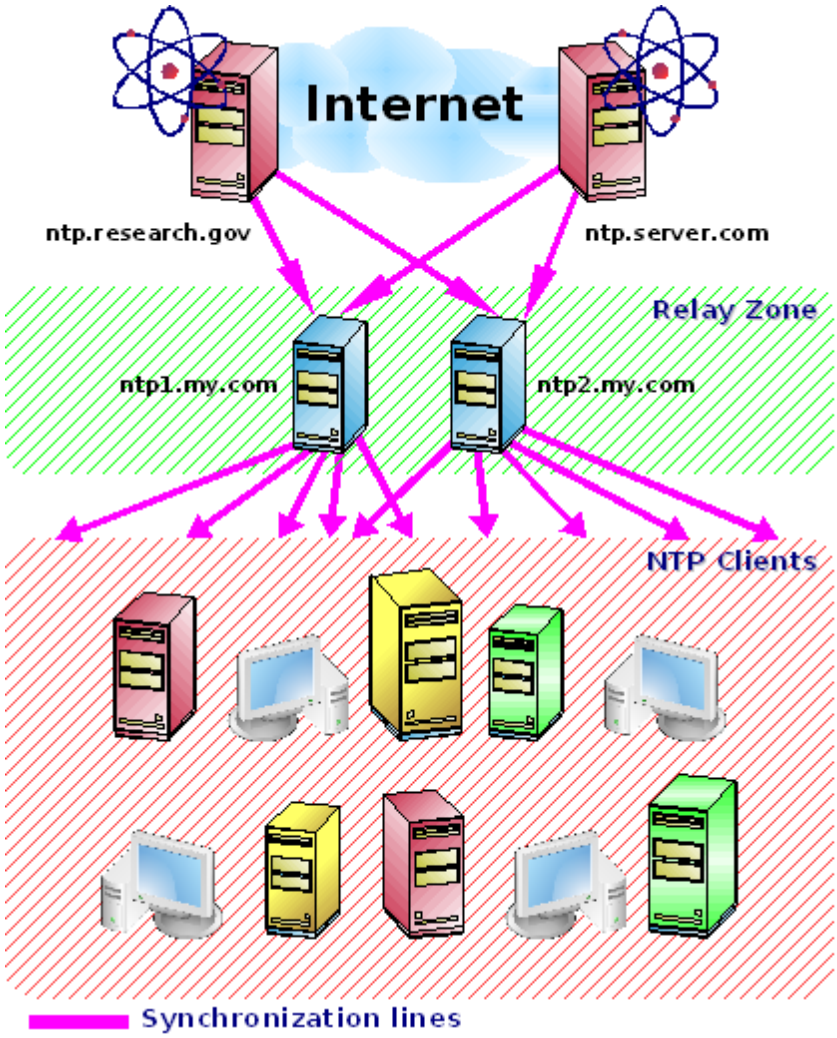

Figure 3 Sample NTP Sychronization Structure

Huawei Cloud Engine product can work both as NTP servers and as NTP client according to customer requirement. Based on typical PCI DSS compliances scenarios, it is recommended that customer administrators enable different NTP features as following:

Scenarios description	NTP role of Cloud Engine product	Recommended features for Cloud Engine product	Notes
There are dedicated NTP services in NTP servers or other appliances.	NTP client	Enable time synchronization setting, update time from dedicated NTP services.	
Enabled NTP services in a Huawei Cloud Engine product.	Stand-alone NTP server	Enable time server feature, update time signals from external trusted time sources. Other CDE system components update time signals from this stand-alone Huawei Cloud Engine product. Enable synchronization feature if applicable.	
Enabled NTP services in Huawei Cloud Engine products.	Primary NTP server	Enable time server feature, update time signals from external trusted time sources. Enable NTP synchronization feature with secure authentication, synchronize time signals to peered secondary NTP server. Other CDE system components update time signals from this primary NTP server or either from the secondary NTP server..	
	Secondary NTP server	Enabled NTP synchronization feature with secure authentication, synchronize time signals from peered Primary NTP server. Other CDE system components update time signals from the primary NTP server or either from this secondary NTP server.	

Table 8 Time Sychronization scenarios

3.6 Audit trail monitoring

Related PCI DSS requirments
10.1 Implement audit trails to link all access to system components to each individual user.
10.2 Implement automated audit trails for all system components to reconstruct the following events:
10.2.2 All actions taken by any individual with root or administrative privileges.
10.2.3 Access to all audit trails.
10.2.4 Invalid logical access attempts.
10.2 5 Use of and changes to identification and authentication mechanisms (including but not limited to creation of new accounts and elevation of privileges) and all changes, additions, or deletions to accounts with root or administrative privileges.
10.2.6 Initialization, stopping, or pausing of the audit logs.
10.2.7 Creation and deletion of system-level objects.
10.3 Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource
10.5 Secure audit trails so they cannot be altered.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

Table 9 PCI DSS requirement 10

PCI DSS has had specific requirements for logging and review of those logs for some time now. The logging requirements (under Requirement 10) have a primary objective of supporting forensics in the event of a breach of cardholder data.

Administrative users must also be uniquely tracked. Often, when outside organizations assist companies in troubleshooting their IT systems, they may need the same level of administrative access as employees of the organization. In order to minimize the risk of outside users compromising the company's sensitive information, it's imperative to understand and track what actions have been performed on the system during that process. Administrators should be the only system users with access to view, modify or delete the logs, and even then you should be able to uniquely identify which administrator did so by ensuring that a shared administrator account is not used by multiple users.

As per PCI DSS requirement 10.1, to ensure all accesses to CDE system components are co-related to individuals, it is required to enable secure logging features for all audit trails in Huawei Cloud Engine product. The logging features should meet following requirements:

- All administrative accesses should be recorded as per PCI DSS requirement 10.2.1-10.2.7.
- Each record should contain necessary information as per PCI DSS requirement 10.3.1-10.3.6
- Audit trails should be exported to centralized locations, normally centralized log server as per PCI DSS requirement 10.5.1-10.5.4.

3.7 Timely Deployment of Security Patches

Related PCI DSS requirments
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.
Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Table 10 PCI DSS requirement 6.1 and 6.2

It is recommended to acquire the security vulnerability and patch information as soon as possible from

Huawei and industry resources, such as CVE, Bugtrap, OSVDB, etc, and then implement the critical patches within one month. A general process of patch management is shown below:

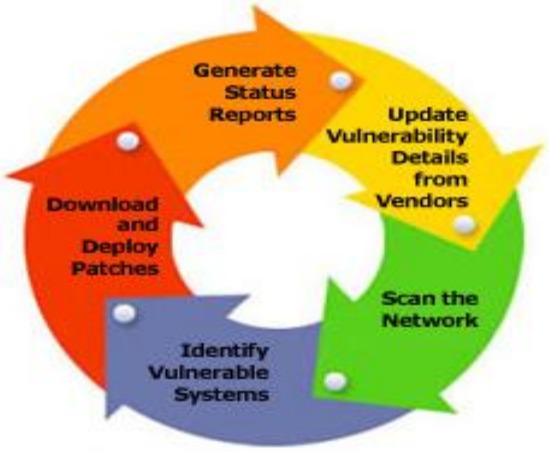

Figure 4 Security Patch Management Process

When a vulnerability is detected, Huawei develops and deploys a patch and/or update as following a development and fix management process . A technical notice will be sent out via email and the patch will be made available on Huawei service portal, and then these patches will be delivered to customer by using a known chain of trust.

If computer is connected via VPN or other high-speed connection, receive software updates via a firewall or a personal firewall per PCI DSS Requirement 1 or 12.3.9. Before the updates are applied, it is recommended to confirm that they are not modified by any unauthoritive third parties by either checking integration against the SHA-256 authentication code or verifying the embedded digital signatures.

Once the patch is received and verified, it is suggested to fix the vulnerability according to the security level. If the level is marked as “high” or above, these patches should be fixed within 30 days. It is also recommended to merge the patch management activities to customer’s internal patch cycle management process.

3.8 Information Security Policy/Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the cardholder data environment is necessary to protect the organization, sensitive authentication data and cardholder data.

The following is a very basic plan every merchant/service provider/issuer/acquirer should adopt in developing and implementing information security policies and procedures:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the remediation plan to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the system. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire, or perform annual assessment by PCI SSC accreditted QSA company.
- Call in outside experts as needed. PCI SSC has published a Qualified Security Assessor List of companies that can conduct on-site payment brands compliance assessment.

After completing all necessary installation and configuration requirements, the customer need state the specific goals of your data security policy, including all of the steps you expect to take, on an annual basis, to verify that the cardholder data environment is still secure. Specify the area of responsibility each type of employee has in your data security program, and implement a formal security awareness program to emphasize and enforce these responsibilities.

The customer must also implement an incident response plan, in the event of a system breach. Specify response procedures, business continuity processes, and data backup strategies and processes. Make specific lists of people and authorities to contact, both within the company and outside the company, to include law enforcement and transaction rocessors. The customers are also required to provide training to employees on the proper procedures to follow, in the event of a system breach.

---------- Blank blow in this page ----------

4 Secure Implementation Configuration

Here are implementation guides as per PCI DSS requirements.

4.1 Network-level Access Control

Related PCI DSS requirments	Implementation description
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	During the implementation, the network administrators should create different subnets for different areas according to the network segmentation requirements stated in page 11 in the PCI DSS standard V3.1. The suggested subnets include but not limit to DMZ area, application area, database area, management area, non-CDE area, etc. Once the network segmentations are properly implemented, it is required to restrict any CDE-related inbound and outbound traffic. It is recommended to use advanced ACL and user ACL to implement appropriate access controls and define default “deny-all” rule at the end. The configuration samples for advanced ACL are show as below: **1.Entering system view** *system-view* **2.Create Advanced ACL** *acl [number] acl-number [match-order { auto | config }]* **3.Define specific rules** Define related IP/TCP/UDP rules according to requirement *rule [rule-id] { deny | permit } ip [destination { destination-address destination-wildcard | any } | source { source-address source-wildcard | any } | time-range time-name | [dscp dscp | [tos tos | precedence precedence] *] | fragment] ** ▪ When the TCP protocol is used, run: *rule [rule-id] { deny | permit } { protocol-number | tcp } [destination { destination-address destination-wildcard | any } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { source-address source-wildcard | any } | source-port { eq port | gt port | lt port | range port-start port-end } | tcp-flag { ack | fin | psh | rst | syn | urg } * | time-range time-name | [dscp dscp | [tos tos | precedence precedence] *] | fragment] ** ▪ When the UDP protocol is used, run:

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	*rule [rule-id] { deny | permit }{ protocol-number | udp } [destination { destination-address destination-wildcard | any } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { source-address source-wildcard | any } | source-port { eq port | gt port | lt port | range port-start port-end } | time-range time-name | [dscp dscp | [tos tos | precedence precedence] *] | fragment] ** **4. To configure multiple rules, repeat this step.** **5. Add default deny policy at the end of rule set.** **6. Apply rule set to desired interface.** **Below are configuration samples for user ACL:** **1.Entering system view** *system-view* **2.Create Advanced ACL** *acl [number] acl-number [match-order { auto | config }]* **3.Define specific rules** Define related IP/TCP/UDP rules according to requirement *rule [rule-id] { deny | permit } ip [destination { { destination-address destination-wildcard | any } | user-group { name destination-group-name |any } } | source { { source-address source-wildcard | any } | user-group { name source-group-name |any } } | time-range time-name | [dscp dscp | [tos tos | precedence precedence] *] | fragment] ** ▪ When the TCP protocol is used, run: *rule [rule-id] { deny | permit } { protocol-number | tcp } [destination { { destination-address destination-wildcard | any } | user-group { name destination-group-name |any } } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { { source-address source-wildcard | any } | user-group { name source-group-name |any } } | source-port { eq port | gt port | lt port | range port-start port-end } | tcp-flag { ack | fin | psh | rst | syn | urg } * | time-range time-name | [dscp dscp | [tos tos | precedence precedence] *] | fragment] ** ▪ When the UDP protocol is used, run: *rule [rule-id] { deny | permit }{ protocol-number | udp } [destination { { destination-address destination-wildcard | any } | user-group { name destination-group-name |any } } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { { source-address source-wildcard | any } | user-group { name source-group-name |any } } | source-port { eq port | gt port | lt port | range port-start port-end } | time-range time-name | [dscp dscp | [tos tos | precedence precedence] *] | fragment] ** **4. To configure multiple rules, repeat this step.** **5. Add default deny policy at the end of rule set.** **6. Apply rule set to desired interface.**

1.2.2 Secure and synchronize router configuration files.	As for the synchronize of CLOUD ENGINE configuration files, it is suggested to synchronize the running configuration to the start-up configuration by either synchronizing configuration manually after the configuration change or using automatic configuration synchronization feature. The manual synchronization command is shown as following: *Save [configuration-file] ---for the manual synchronization.* The automatically configuration synchronization features can be enabled as following: *configuration file auto-save [interval interval | cpu-limit cpu-usage | delay delay-interval] * –for the automatic synchronization after specified period.* As for the exported configuration, it is suggested to implement necessary user access control and/or file encryption for any copies of configuration files.

Table 11 Implementation Table for Network Segmentation

4.2 Secure Administration

Related PCI DSS requirments	Implementation description
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. **This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.**	During the initial configuration, it is required to change all related defaults to complex and difficult-to-guess combinations. These defaults credentials and related password change suggestions include but not limited to the following: - **Default console login account “admin” and default password “admin@huawei.com”** It is suggested to change it in the console interface by using command: *"local-user user-name password [cipher password | irreversible-cipher irreversible-cipher-password]"* - **BootROM login account password “admin@huawei.com”** It is suggested to change it in the option “6. Change password” of the BootROM menu. Furthermore, it is also required to avoid use any publicized and easy-to-guess credentials. These credentials include but not limited to SNMP community strings, Local AAA authentication credentials, RADIUS authentication credentials, HWTACACS authentication credentials, IPSEC pre-shared key value, authentication value in wireless configuration template, etc. The commonly used and recommended configuration samples are shown as following: **1. SNMP community strings.** Default value “public” shouldn’t be used. The commands are shown as following: *snmp-agent community { read | write } { community-name | cipher community-name } [mib-view view-name | acl acl-number] ** **2. Local AAA authentication credentials.** Local administrative users should change password to complex and difficult-to-guess combinations.

	system-view *local-user user-name password [cipher password | irreversible-cipher irreversible-cipher-password]* **3. External RADIUS authentication credentials.** Configure a RADIUS authentication scheme. *<Commandline> system-view* *<Commandline> aaa* *<Commandline> authentication-scheme [authentication-scheme-name]* *<Commandline> authentication-mode radius* Configure RADIUS server group. *<Commandline> system-view* *<Commandline> radius enable* *<Commandline> radius server group [group-name]* *<Commandline> radius server authentication ipv4-address port [vpn-instance vpn-instance-name | source { interface-type interface-number | ip-address ip-address } | { shared-key key-string | shared-key-cipher cipher-string }]* *<Commandline> radius server accounting ipv4-address port [vpn-instance vpn-instance-name | source { interface-type interface-number | ip-address ip-address } | { shared-key key-string | shared-key-cipher cipher-string }]* *<Commandline>quit* Configuration Radius domain. *<Commandline> syste-view* *<Commandline> aaa* *<Commandline> domain [domain-name]* *<Commandline> authentication-scheme [authentication-scheme-name]* *<Commandline> radius server group [group-name]* *<Commandline> commit* **4. External HWTACACS authentication credentials.** Enable HWTACACS authentication and create a template. *system-view* *aaa* *authentication-scheme [authentication-scheme-name]* *authentication-mode hwtacacs* configure HWTACACS authentication server(s). *hwtacacs server ip-address [port] [{ vpn-instance vpn-instance-name | public-net } | shared-key { key-string | cipher cipher-string } | mux-mode]* *hwtacacs-server authentication ip-address [port] [{ vpn-instance vpn-instance-name | public-net } | shared-key { key-string | cipher cipher-string } | mux-mode]* *commit* Configure HWTACACS authentication domain. *System-view*

	Aaa *Domain [domain-name]* *Authentication-scheme [authentication-scheme-name]* *Hwtacacs server [template-name]* *Commit* Third-party AAA authentication schemas are supported by CloudEngine switches. If customer has these external AAA schemas, it is also recommended to use them for user authentication.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system. **2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.** **2.2.4 Configure system security parameters to prevent misuse.** **2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.** **2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.** **8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.**	Various services and protocols may be enabled for management purposes. The basic principals for services and protocols consolidation is to consolidate the required services with secure features while removing all unnecessary and insecure ones. Here are secure consolidation guides for common protocols. **1. SNMP protocol.** If this protocol is not a business necessity, it is suggested to disable it. Below are remindings for the protocol consolidation. **Change SNMP version to secure version, recommened to SNMP V3.** *snmp-agent sys-info { contact contact | location location | version { { v1 | v2c | v3 } * | all } [disable] }* **Specify authentication strings and encrypt it via SHA alogorithm.** *snmp-agent [remote-engineid engineid] usm-user v3 user-name authentication-mode { md5 | sha } [cipher password]* **Specify Privacy-mode to secure encryption algorithm, such as AES128.** *snmp-agent [remote-engineid engineid] usm-user v3 user-name privacy-mode { 3des168 | aes128 | aes192 | aes256 | des56 } [cipher password]* **2. RADIUS protocol.** It is suggested to enable Huawei Policycenter or third-party AAA servers and configure secure password attributes according to PCI DSS requirement 8.2.3-8.2.5. It is reminded to use keyword “cipher“ to encrypt the shared-key. *radius server { shared-key key-string | shared-key-cipher cipher-string }* **3. HWTACACS protocol.** It is suggested to enable Huawei Policycenter or third-party AAA servers and configure secure password attributes according to PCI DSS requirement 8.2.3-8.2.5. It is reminded to use keyword “cipher“ to encrypt the shared-key. *hwtacacs server shared-key { cipher cipher-string | key-string }* **3. FTP protocol.** This protocol is considered insecure protocol, so it is suggested to disable it and replace it with SFTP protocol if necessary. *Undo ftp server* **4. DHCP protocol.** If there is no explicit business necessary, it is suggested to disable it. By default, no DHCP server is configured in a DHCP server group. The commands to disable DHCP protocol are shown as following: *undo dhcp enable* **5. Telnet protocol.** This protocol is considered insecure protocol, so it is suggested to disable it

	and replace it with SSH protocol if necessary. The commands to disable Telnet protocol are shown as following: *telnet [ipv6] server disable* **6. SFTP protocol.** If there are file transmission requirement, it is suggested to enable SFTP protocol by using 2048 (recommended)or above bits key-size during RSA key-paire generation process. The configuration samples are shown as following: **Chossing 2048 bits key size during key generation.** *system-view* *Rsa local-key-pair create [choose 2048 bits strength].* *dsa local-key-pair create [choose 2048 bits strength]* **enabling SFTP protocol.** *sftp server enable* **7. SSH protocol.** As for the CLI management, it is suggested to enable SSH V2 by using 2048 (recommended) or above bits key-size during RSA/DSA key-pair generation process. The configuration samples are shown as following: **disabling SSH V1 support** *undo ssh server compatible-ssh1x enable* **Chossing 2048 bits key size during key generation.** *Rsa local-key-pair create [choose 2048 bits strength].* *dsa local-key-pair create [choose 2048 bits strength]* **8. Render credentials unreadable during storage.** As for these local user accounts, Cloud Engine product encrypted via strong cryptographic algorithms by defaults. It is reminded to enable strong cryptographic encryption by specifying keyword “cipher“ to render crendentials unreadable via AES-256 algorithms. Most Cloud Engine products are deployed in an internal network and in most cases there is no management protocols made accessible from the Internet, so it is not a mandatory requirement to import third-party trust certificates for the SSH/SFTP management. However, it is recommended to apply trustworthy PKI certificates both management and transmission purpose.

Table 12 Implementation Table for Secure Administration

4.3 User Access Control

Related PCI DSS requirments	Implementation description
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. **7.1.1 Define access needs for each role, including:** *** System components and data resources that each**	There are no default user accounts available for appliance administration. To securely encrypt user account password, it is required to specify “cipher” password. The sample commands for create administrative user account are shown as following: **Enter into AAA configuration mode to create new user account.** *user-interface vty 0 4* *authentication-mode aaa* Create user account and specify the username.

role needs to access for their job function. *** Level of privilege required (for example, user, administrator, etc.) for accessing resources.** **7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.** **7.2.2 Assignment of privileges to individuals based on job classification and function.** **7.2.3 Default "deny-all" setting.**	**Encrypt password by using key word"cipher"in the command.** *local-user xxxx password cipher yyyyyyy* **Assign privilege level for the user account.** It is necessary to minimize user privilege by restricting user's previlege level and available command sets. *user privilege level 3* **Restricting command level** In case the command level is required to be adjusted, high privileged user can adjust the command level to restrict it to be executed only by users of specified or aboved levels. *command-privilege level level view view-name command-key*
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: *** Something you know, such as a password or passphrase.** *** Something you have, such as a token device or smart card.** *** Something you are, such as a biometric.**	It is required to specify user authentication method for each assigned user account. There are 3 types of configurable user credential databases, the configuration methods are shown as following: **1. Local AAA authentication.** Local administrative users should change password to complex and difficult-to-guess combinations. *system-view* *local-user user-name password [cipher password | irreversible-cipher irreversible-cipher-password]* **2. External RADIUS authentication.** Configure a RADIUS authentication scheme. <*Commandline*> *system-view* <*Commandline*> *aaa* <*Commandline*> *authentication-scheme [authentication-scheme-name]* <*Commandline*> *authentication-mode radius* Configure RADIUS server group. <*Commandline*> *system-view* <*Commandline*> *radius enable* <*Commandline*> *radius server group [group-name]* <*Commandline*> *radius server authentication ipv4-address port [vpn-instance vpn-instance-name | source { interface-type interface-number | ip-address ip-address } | { shared-key key-string | shared-key-cipher cipher-string }]* <*Commandline*> *radius server accounting ipv4-address port [vpn-instance vpn-instance-name | source { interface-type interface-number | ip-address ip-address } | { shared-key key-string | shared-key-cipher cipher-string }]* <*Commandline*>*quit* Configuration Radius domain. <*Commandline*> *syste-view* <*Commandline*> *aaa* <*Commandline*> *domain [domain-name]*

	<Commandline> authentication-scheme [authentication-scheme-name] *<Commandline> radius server group [group-name]* *<Commandline> commit* **3. External HWTACACS authentication credentials.** Enable HWTACACS authentication and create a template. *system-view* *aaa* *authentication-scheme [authentication-scheme-name]* *authentication-mode hwtacacs* configure HWTACACS authentication server(s). *hwtacacs server ip-address [port] [{ vpn-instance vpn-instance-name | public-net } | shared-key { key-string | cipher cipher-string } | mux-mode]* *hwtacacs-server authentication ip-address [port] [{ vpn-instance vpn-instance-name | public-net } | shared-key { key-string | cipher cipher-string } | mux-mode]* *commit* Configure HWTACACS authentication domain. *System-view* *Aaa* *Domain [domain-name]* *Authentication-scheme [authentication-scheme-name]* *Hwtacacs server [template-name]* *Commit* Third-party AAA authentication schemas are supported by CloudEngine switches. If customer has these external AAA schemas, it is also recommended to use them for user authentication.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	It is required to assign unique ID for each user, either administrative account or normal access user. If local AAA account database is used, make sure that each account is assigned to individual user with legimate business necessity. In case external Radius/HWTACACS authentication schema is applied for user account/password management, it is required to meet the requirement by following internal account/password management process. During the first-time or password reset, it is required user to change the password immediately once the password is received over secure means. The sample command is shown below: *local-user change-password .xxxxx. [input unique and strong password]* *local-user policy password change* No matter where the user account/password schema is, It is reminded not to use shared/generic user account/password.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: *** Generic user IDs are disabled or removed.** *** Shared user IDs do not exist for system administration and other critical functions.** *** Shared and generic user IDs are not used to administer any system components.**	
8.2.6 Set passwords/phrases for first-time use and upon	

reset to a unique value for each user, and change immediately after the first use.	
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: *** Enabled only during the time period needed and disabled when not in use.** *** Monitored when in use.**	**It is suggested to enable vendor accounts only when in use. The sample command to enable user accounts are shown as following:** *Local-user [user-name] state active* **Once the tasks have been completed, the sample command to disable user accounts are shown as following:** *Local-user [user-name] state block* **All actions taken by administrative accounts (including these accounts used by vendors) are recorded and monitored by default.**
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts. **8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.**	**1. External RADIUS/HWTACACS user accounts** It is required to enable external user authentication mechanisms and configure related password attribute in external AAA services. Third-party AAA authentication schemas are supported by CloudEngine switches. If customer has these external AAA schemas, it is also recommended to use them for user authentication. **2. Local AAA user accounts** The user password is required to be locked after specified times of failed attempts. The sample commands are shown as following: *local-user authentication lock times failed-times period*
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**1. External RADIUS/HWTACACS user accounts** It is required to enable external user authentication mechanisms and configure related password attribute in external AAA services. Third-party AAA authentication schemas are supported by Cloud Engine switches. If customer has these external AAA schemas, it is also recommended to use them for user authentication. **2. Local AAA user accounts** It is required to idle out remote sessions and require user to re-active the sessions.The sample commands are shown as following: *System-view* *User-interface vty 0 5* *Idle-timeout 15*
8.2.4 Change user passwords/passphrases at least every 90 days.	**1. External RADIUS/HWTACACS user accounts** There is no available password protection features for CloudEngine switch access user accounts, so it is strongly recommended that access user account use external RADIUS/HWTACACA authentication schema. As for CloudEngine product administrative user account, both Local AAA and external RADIUS/TACACS authentication are made available, thus authentication schema can be chosen according to management requirements. **2. Local AAA user accounts** It is required to specify the password expiration date as following sample command: *local-user user-name password expire [days]*

8.2.3 Passwords/phrases must meet the following: *** Require a minimum length of at least seven characters.** *** Contain both numeric and alphabetic characters.** **Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.**	**1. External RADIUS/HWTACACS user accounts** As for Cloud Engine product administrative user account, both Local AAA and external RADIUS/TACACS authentication are made available, thus authentication schema can be chosen according to management requirements. **2. Local AAA user accounts** If a new password is required, the typed passwords must meet the following requirements: ▪ The password is a string of 8 to 16 case-sensitive characters. ▪ The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. The commands for enable password minimum length and complexity check are shown as following: *local-user policy password min-len [min-length]* *local-user policy password complexity-enhance*
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	**1. External RADIUS/HWTACACS user accounts** There is no available password protection features for Cloud Engine access user accounts, so it is strongly recommended that access user account use external RADIUS/HWTACACA authentication schema. As for Cloud Engine product administrative user account, both Local AAA and external RADIUS/TACACS authentication are made available, thus authentication schema can be chosen according to management requirements. Third-party AAA authentication schemas are supported by Cloud Engine switches. If customer has these external AAA schemas, it is also recommended to use them for user authentication. **2. Local AAA user accounts** The command for enable password history check is shown as following: *local-user policy password complexity-enhance*

Table 13 Implementation Table for User Access Control

4.4 Accurate time synchoronization

Related PCI DSS requirments	Implementation description
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	There are many scenarios for configuring NTP modes and related settings, such as NTP client, NTP server, etc. The scenarios and configuring samples are shown as following: **1. Configuring NTP client.** It is required to update time signals from internal NTP resources. It is also suggested to enable authentication for time synchronization.The configuration samples are shown as following: *system-view* *ntp authentication enable* *ntp authentication-keyid xxxxx authentication-mode hmac-sha-256 yyyyy* *ntp unicast-server [internal NTP servers]*
10.4.1 Critical systems have the correct and consistent time.	
10.4.2 Time data is protected.	

10.4.3 Time settings are received from industry-accepted time sources.	*commit* **2. Configuring NTP server.** It is required to configuring the NTP service to update time signals from external trusted time resources, such as time.nist.org. It is also suggested to enable authentication for time synchronization. The configuration samples are shown as following: *system-view* *ntp authentication enable* *ntp authentication-keyid xxxxx authentication-mode hmac-sha-256 yyyyy* *ntp refclock-master 2* *ntp unicast-server [external NTP servers]* *commit* **3. specifying trusted external time resources** It is suggested to using industry-acceptable time sources as the time source, such as time.nist.org, etc. The command to specify external time sources are shown below: *ntp unicast-server [external NTP servers]* **4. Protection of time settings.** Firstly, all the NTP configuration changes are logged in the log buffer and delivered to centralized syslog server (if it is configured properly). Secondly, it is helpful to adjust the NTP-related command level to be only executable by users of specified or aboved levels. *command-privilege level [level] view [view-name] [command-key]* At last, configuring ACLs is a necessary mechanisms to secure NTP protocols. In case ACLs are not configurable in other system components (such as firewalls), ACL features in Cloud Engine switches are avalable and configurable to restrict necessary access to NTP protocols only.

Table 14 Implementation Table for NTP

4.5 Audit trail monitoring

Related PCI DSS requirments	Implementation description
10.1 Implement audit trails to link all access to system components to each individual user.	Once log setting are enabled, Cloud Engine product export related audit trails to centralized log servers, such as Syslog host, etc. The sample settings are shown as following: *system-view* *sysname [hostname]* *info-center enable* *info-center loghost [IP address of log*
10.2 Implement automated audit trails for all system components to reconstruct the following events:	
10.2.2 All actions taken by any individual with root or administrative privileges	
10.2.3 Access to all audit trails	
10.2.4 Invalid logical access attempts	

10.2 5 Use of and changes to identification and authentication mechanisms (including but not limited to creation of new accounts and elevation of privileges) and all changes, additions, or deletions to accounts with root or administrative privileges.	*server]* It is required to implement related log server for centralized management of Cloud Engine event logs. Furthermore, it is also recommended to implement third-party security event management solutions and/or Huawei's own event management mechanisms, if these solutions have security events co-relation, analysis, reporting and alerting features.
10.2.6 Initialization of the audit logs	
10.2.7 Creation and deletion of system-level objects	
10.3 Record at least the following audit trail entries for all system components for each event:	
10.3.1 User identification	
10.3.2 Type of event	
10.3.3 Date and time	
10.3.4 Success or failure indication	
10.3.5 Origination of event	
10.3.6 Identity or name of affected data, system component, or resource	
10.5 Secure audit trails so they cannot be altered.	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	

Table 15 Implementation Table for Audit Trail Monitoring

4.6 Security Patches implementation

Related PCI DSS requirments	Implementation description
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. **6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.**	It is required to subscribe product patch information in Huawei website and fix all critical vulnerabilities as following customer's internal patch cycle. After the acquisition of patches, it is suggested to verify the source of patches, develop and deploy a patch and/or update within 30 days of discovery.

Table 16 Implementation Table for Security Patches

Note: all commands shown in tables above are configuration samples. For more configuration details, please refer to related documentations as following:

- CloudEngine 12800 product document.hdx (packed in 2015-01-20)

- CloudEngine 7800&6800&5800 product document.hdx (packed in 2015-01-20)
- Huawei CloudEngine 7800&6800&5800switch security consolidation guide(Chinese name: CloudEngine 7800&6800&5800 系列交换机安全加固指南)
- Huawei CloudEngine 12800 switch security consolidation guide(Chinese name: CloudEngine 12800 系列交换机安全加固指南)
- Huawei CloudEngine 7800&6800&5800switch security maintenance guide(Chinese name: CloudEngine 7800&6800&5800 系列交换机安全维护指南)
- Huawei CloudEngine 12800switch security maintenance guide(Chinese name: CloudEngine 12800 系列交换机安全维护指南)

Below is the link for Huawei CLOUD ENGINE documentations:

http://support.huawei.com/

---------- Blank blow in this page ----------

5 Bibliography

PCI Standards and Supporting Documents

PCI SSC standards and Supporting documents are available from the PCI SSC web site at https://www.pcisecuritystandards.org/

PCI PA-DSS standards and supporting documents:

PA-DSS Requirement and Security Assessment Procedures Version 3.1

https://www.pcisecuritystandards.org/documents/PA-DSS_v3-1.pdf

PA-DSS Requirement and Security Assessment Procedures Version 3.0

https://www.pcisecuritystandards.org/documents/PA-DSS_v3.pdf

Summary of Changes from PA-DSS Version 2.0 to 3.0

https://www.pcisecuritystandards.org/documents/PA-DSS_v3_Summary_of_Changes.pdf

Summary of Changes from PA-DSS Version 3.0 to 3.1

https://www.pcisecuritystandards.org/documents/PA-DSS_v3-1_Summary_of_Changes.pdf

PCI PA-QSA Feedback Forms:

PA-QSA Feedback Form – Brands and Others
https://www.pcisecuritystandards.org/docs/pa-qsa_brand_feedback_form.doc

PA-QSA Feedback Form- Clients
https://www.pcisecuritystandards.org/docs/pa-qsa_client_feedback_form.doc

Attestation of Validation
https://www.pcisecuritystandards.org/docs/aov_pa-dss_form.doc

PA-DSS Self Attestation Minor Updates
https://www.pcisecuritystandards.org/docs/pa-dss_self-attestation_minor_form.doc

PCI DSS standards and supporting documents:

PCI SSC. 2013, *Data Security Standard: Requirements and Security Assessment Procedures* Nov. 2013 Version 3.0

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_ZH-CN.pdf

PCI SSC. 2015, *Data Security Standard: Requirements and Security Assessment Procedures* Apr. 2015 Version 3.1

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

PCI SSC. 2014, *Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS): Glossary of Terms, Abbreviations, and Acronyms*.

https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf

PCI SSC. 2009, *Information Supplement: Requirement 11.3 Penetration Testing* August, 2009 Version 1.2
https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf

PCI SSC. 2009, *Information Supplement: Requirement 6.6 Application Reviews and Web Application Firewalls Clarified* August, 2009 Version 1.2
https://www.pcisecuritystandards.org/documents/information_supplement_6.6.pdf

PCI SSC. 2015, *PCI Data Security Standard: Penetration testing Guidance*

https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

PCI SSC. 2013, *PCI Data Security Standard: PCI DSS cloud Computing Guidances*

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

OWASP (Open Web Application Security Project)

NIST Publication 800-115: Technical Guide to Information Security Testing and Assessment, September 2008

Payment Card Brand Web Sites

Card Brand	URL
Mastercard	http://www.mastercard.com/us/sdp/index.html
VISA USA	http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html
American Express	https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&merch_van=datasecurity
Discover	http://www.discovernetwork.com/fraudsecurity/disc.html
JCB	http://www.jcb-global.com/english/pci/
VISA CEMEA	http://www.visacemea.com/ac/ais/data_security.jsp
VISA Europe	http://www.visaeurope.com/aboutvisa/security/ais/
VISA Southeast Asia	http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml

Table 17 Payment card brands websites

6 Glossary

Some of the terms in this document are formally defined by the PCI-SSC. Their list of terms is found in the Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS): Glossary of Terms, Abbreviations, and Acronyms.

Term	Definition	Explanation
AAA	Authentication, authorization, and accounting	
ACL	Access Control List	
Acquirer		Entity that initiates and maintains relationships with merchants for the acceptance of payment cards
AES	Advanced Encryption Standard	Block cipher used in symmetric key cryptography adopted by NIST in November 2001 as U.S. FIPS PUB 197 (or “FIPS 197”). See Strong Cryptography
ANSI	American National Standards Institute	Private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system
AP	Access Point	
ARP	Address Resolution Protocol	
ASV	Approved Scanning Vendor	Company approved by the PCI SSC to conduct external vulnerability scanning services
ATM	Automated Teller Machine	
ATM	Asynchronous Transfer Mode	
Attack		attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (ISO/IEC 27000)
BSP	Best Security Practice	
Cardholder		The end user. Someone who carries a payment card.
Cardholder data environment		Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment. (from PCI-Glossary V1.1)
CAV	Card Authentication Value	This term is used by JCB payment cards
CAV2	Card Authentication Value 2 (JCB payment cards)	This term is used by JCB payment cards
CDA	Confidential Disclosure Agreement	
CDE	Cardholder data environment	See "Cardholder data environment"
CHD	Card Holder Data	
CID	Card Identification Number	This term is used by American Express and Discover payment cards
CIS	Center for Internet Security	Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls
CISM	Certified Information Security Manager	

Term	Definition	Explanation
Compensating Controls		Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement (from PCI-Glossary V1.1)
COTS	Commercial of the Shelf	
CSC	Card Security Code	This term is used by American Express
CVC	Card Validation Code	This term is used by MasterCard
CVC2	Card Validation Code 2	This term is used by MasterCard
CVE	Common Vulnerability and Exposure	
CVE ID	Common Vulnerability and Exposure Identifier	unique, common identifiers for publicly known information security vulnerabilities
CVE name	Common Vulnerability and Exposure	unique, common identifiers for publicly known information security vulnerabilities
CVE number		A unique number to identify a CVE database entry
CVV	Card Verification Value	This term is used by VISA and Discover
CVV2	Card Verification Value 2	This term is used by VISA
DAC	Discretionary Access Control	
DBA	Doing Business As	
DES	Data Encryption Standard	
DMZ	De-Militarized zone	Physical or logical sub-network or computer host that provides an additional layer of security to an organization’s internal private network. The DMZ adds an additional layer of network security between the Internet and an organization’s internal network so that external parties only have direct access to devices in the DMZ rather than all of the internal network
DNS	Domain Name System	
DSE	Data Storage Entity	This term is used by MasterCard
DSS	Data Security Standard	
Dynamic Packet Filtering	See Stateful Inspection	
EAR	Export Administration Regulations (U.S.)	Export Administration Regulations, 15 CFR 768-799
EC2	Elastic Computing Cloud	Amazon's virtualized hosting system
ESA	External Sales Agents	
FAQ	Frequently Asked Questions	
FIM	File Integrity Monitoring	
FSO	File System Objects	

Term	Definition	Explanation
FTP	File Transfer Protocol	
GPRS	General Packet Radio Service	
HSM	Hardware Security Module	
HTTP	Hypertext Transfer Protocol	
HTTPS	Hypertext Transfer Protocol over Secure Socket layer	
I&A	Indentification and Authentication	The process of identifying an individual, usually based on a username and password.
ID	Identity	
IDS	Intrusion Detection System	
IG	Implementation Guidance	Guidance produced by a program regarding the interpretation of a standard as it is implemented in practice
Interpretation		Rulings produced by a program regarding the interpretation of a standard as it is implemented in practice
IPC	Inter Process Communications	
IPS	Intrusion Prevention System	
IPSEC	Internet Protocol Security	
ISO	International Organization for Standardization	
ISO	Independent Sales Organization	
KEK	Key Encrypting Key	
LAN	Local Area Network	
LPAR	Logical Partition	
Malware		Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent. (from PCI-Glossary V1.1)
Merchant		any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
MoTo	Mail order / Telephone order	
MSP	Managed Service Provider	
NAT	Network Address Translation	
NCSC	The National Computer Security Center	a U.S. government organization within the National Security Agency (NSA) that evaluates computing equipment for high security applications to ensure that facilities processing classified or other sensitive material are using trusted computer systems and components

Term	Definition	Explanation
NDA	Non Disclosure Agreement	
NDC	Network Development Consultant	
NFS	Network File System	
NIS	Network Information Service	
NMAP		Security-scanning software that maps networks and identifies open ports in network resources.
NTP	Network Time Protocol	
NVD	National Vulnerability Database	
OS	Operating System	
OTP	One Time Pad	one-time pad is an encryption algorithm with text combined with a random key or "pad" that is as long as the plain-text and used only once. Additionally, if key is truly random, never reused, and, kept secret the one-time pad is unbreakable
OTS	Off-The-Shelf	
OWASP	Open Web Application Security Project	
PAN	Primary Account Number	also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
PA-QSA	Payment Application Qualified Security Assessor	
PAT	Port Address Translation	Feature of a network address translation (NAT) device that translates transmission control protocol (TCP) or user datagram protocol (UDP) connections made to a host and port on an outside network to a host and port on an inside network. From PCI-Glossary V1.1)
PCI	Payment Card Industry	
PCI DSS	Payment Card Industry Data Security Standard	
PCI SSC	Payment Card Industry Security Standards Council	
PDA	Personal Data Assistant	
PED	Pin Entry Device	PCI SSC prefer to use the term PTS now/ See PTS
Penetration Test		an attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.
PIN	Personal Identification Number	Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.
PKI	Public Key Infrastructure	

Term	Definition	Explanation
PO	Purchase Order	
POS	Point of Sale	
PSP	Payment Service Provider	Discover use this term
Public network		Network established and operated by a telecommunications provider or recognized private company, for specific purpose of providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify, and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS, and GSM. (From PCI-Glossary V1.1)
PVV	PIN verification Value	Discretionary value encoded in magnetic stripe of payment card
QMS	Quality Management System	
RADIUS	Remote Authentication and Dial-In User Service	
RBAC	Role Based Access Control	
RNG	Random Number Generator	
ROC	Report on Compliance	Report containing details documenting an entity's compliance status with the PCI DSS
ROV	Report on Validation	Report containing details documenting a payment application's compliance with the PCI PA-DSS
RSA	Rivest Shamir Addleman	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); The letters RSA are the initials of their surnames.
S3	Simple Storage Service	
SaaS	Software as a Service	
SAD	Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction (From PCI-Glossary V1.1)
SANS	SysAdmin, Audit, Networking and Security	An institute that provides computer security training and professional certification
SAP	Service Access Points	
SAQ	Self Assessment Questionnaire	
SAS	Software as a Service	See SaaS
SDLC	System Development Life Cycle	Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation
SEM	Security Enterprise Management	
Sensitive Authentication Data		Security-related information (card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

Term	Definition	Explanation
Service Code		Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
SHA	Secure Hash Algorithm	A family or set of related cryptographic hash functions including SHA-1 and SHA-2.
SHS	Secure Hash Standard	
SIG	Special Interest Group	
SOW	Statement of Work	
SP	Service Pack	
SPI	Stateful Packet Inspection	
SQL	Structured Query Language	
SQL Injection		Form of attack on database-driven web site
SSH	Secure Shell	
SSID	Service Set Identifier	
SSL	Secure Socket Layer	
Stateful Inspection	See "dynamic filtering"	A firewall capability that provides enhanced security by keeping track of communications packets. Only incoming packets with a proper response (“established connections”) are allowed through the firewall.
SV	Site Visit	
TACACS	Terminal Access Controller Access Control System	
TCP	Transmission Control Protocol	
TDES	Triple Data Encryption Standard	
TELNET	Telephone Network protocol	
Threat		a potential cause of an unwanted incident, which may result in harm to a system or organization. (ISO/IEC 27000)
TLS	Transport Layer Security	
TPP	Third Party Processor	This term is used by Mastercard, Discover, JCB and Amex.
TWG	Technical Working Group	
UI	User Interface	
URL	Uniform Resource Locator	
VLAN	Virtual LAN	
VNP	Visanet Processor	
VPN	Virtual Private Network	
VTL	Virtual Tape Library	
Vulnerability		Weakness of an asset or control that can be exploited by a threat.

Term	Definition	Explanation
XSS	Cross site scripting	

Table 18 Glossary table

---------- The end of the document----------