Huawei Technologies Co., Ltd.

Summary of Independent Assessment Report for Huawei CloudEngine Products

Supporting user compliance with Payment Card Industry Security Standards and Security Assessment Procedures version 3.1

Report Date: 2015-07-27

Report Number: C100-23

atsec (Beijing) Information Technology Co., Ltd.
3/F, Block C, Bld.1, Boya C-Center, Life Science Park, Changping District, Beijing, P.R. China, 102206
Tel: +86 10 5305 6679
Fax: +86 10 5305 6678
www.atsec.cn

Revision history

Version	Change date	Author(s)	Changes to previous version
0.1	2015-07-08	Xiangdong Gao	Initial draft
0.2	2015-07-10	Li Zhang	Improve the content.
0.3	2015-07-22	Gordon McIntosh	Quality Assurance
0.4	2015-07-24	Li Zhang	Modification according to Fiona's comments
1.0	2015-07-23	Li Zhang	Finalization and formal release.

Table of contents

1 Contact Information and Report Date

1.1 Contact information

Client	
▪ Company name:	Huawei Technologies Co., Ltd. (Branded as “Huawei”)
▪ Company address:	Administration Building, Headquarters of Huawei Technologies Co.,Ltd., Bantian, Longgang District, Shenzhen 518129, P.R.China. (Address in Chinese:中国广东省深圳市龙岗区坂田华为总部办公楼)
▪ Company URL:	www.huawei.com
▪ Company contact name:	Blue Li (Chinese name: 李文)
▪ Contact phone number:	+86 755 28976679
▪ Contact e-mail address:	blue.li@huawei.com
Assessor Company	
▪ Company name:	atsec (Beijing) Information Technology Co., Ltd
▪ Company address:	3/F, Block C, Bld.1, Boya C-Center, Life Science Park, Changping District, Beijing, P.R. China, 102206
▪ Company website:	www.atsec.com
Assessor	
▪ Assessor name:	Li Zhang, Xiangdong Gao
▪ Assessor phone number:	+86-10-5305 6679
▪ Assessor e-mail address:	li.zhang@atsec.com, xiangdong@atsec.com
Assessor Quality Assurance (QA) Primary Reviewer	
▪ QA reviewer name:	Yan Liu, Gordon McIntosh
▪ QA reviewer phone number:	+86-10-5305 6679 – 609
▪ QA reviewer e-mail address:	yan@atsec.com, Gordon@atsec.com

1.2 Date and timeframe of assessment

▪ Date of Report:	July 27, 2015
▪ Timeframe of assessment (start date to completion date):	April 2 ~ 3, 2015 June 25 ~ 26, 2015
▪ Identify date(s) spent onsite at the entity:	3 days.

1.3 PCI DSS version

▪ Version of the PCI Data Security Standard used for the assessment	PCI SSC. 2015, *Data Security Standard: Requirements and Security Assessment Procedures* April 2015, Version 3.1

1.4 Report Disclaimer

This Assessment Report is produced as a result of an assessment which is based on information provided by Huawei to atsec in regard to device functionality and Huawei processes.

This assessment is not a PCI-DSS assessment, but may be used in support of card holder data environments that are undergoing such an assessment.

The assessment does not imply that use of the devices cited provides compliance to the PCI DSS requirements in a cardholder data environment.

2 Executive Summary

2.1 General Description

Huawei Technologies Co., Ltd. (Branded as “Huawei”) (Chinese name: 华为技术有限公司), engaged atsec provide an independent security assessment for Huawei CloudEngine switches in regard to how the product supports PCI DSS compliance in a cardholder data environment. The assessment demonstrates how the products realize and/or support the relevant and applicable security requirements defined in PCI DSS (Payment Card Industry Data Security Standard) version 3.1, and facilitate Huawei customers’ PCI DSS compliance (i.e. that the products do not enforce implementation or configuration settings that violates a PCI DSS requirement).

Huawei provides secure network devices for its customers in the financial and payment segments, including banks, payment gateway companies, and e-business companies. When addressing this market, one goal for Huawei is to facilitate in the secure transfer and processing of sensitive data including sensitive authentication data and cardholder data in the cardholder data environment or between the internal network and the public/private network.

This report focuses on Huawei CloudEngine switches, which are high-speed network appliances intended to be used by IDC customers these include the CE6800,CE7800,CE5800 and CE12800 series which integrate multiple services including routing, switching, QOS and security functions in one device.

Use of a Huawei CloudEngine switch product by itself cannot make an entity PCI DSS compliant, since that product must be implemented into a PCI DSS conformant card holder data environment (CHDE) according to the entities own security policies. However to support implementations of the Huawei devices in such a CHDE, Huawei have produced the document “Huawei CloudEngine Switch PCI DSS Implementation Guide.

This independent assessment was led by atsec consultants who are Qualified Security Assessors (QSA), accredited and in good standing with the PCI SSC, and who have extensive experience in assessing cardholder data environments.

It is important to note that there are no specific PCI SSC standards related to network device validation or certification. Hence this independent report by PCI experts, uses the PCI DSS as a framework, aims to provide an assessment that informs the reader in a manner that supports PCI DSS compliance by the end users.

The assessors performed the security assessment using the PCI DSS requirements as a framework for assessing how Huawei devices can support those requirements. This report provides the assessment methodology and the results from the assessment.

atsec assessors provided the following recommendations to Huawei in this assessment:

- The assessors recommend that FIPS 140-2 compliance be considered by Huawei in order to increase the assurance offered to PCI users, follow the PCI SSC recommended best practices and to ensure that this is not a market differentiator that Huawei competitors take advantage of. NOTE: Security standards such as ISO, NIST and FIPS may be also recommended by a QSA or ASV, although the PCI DSS does not require them, for example, FIPS-140-2, Common Criteria and/or other certification for devices.
- The assessors recommend using multiple outside sources (e.g. SANS, CERT, Security Focus, vendor websites, etc.) to identify new vulnerability issues related to the products and further protect the customers’ cardholder data environment.
- The assessors recommend updating and implementing security functions and features according to the assessment (see more details in section 2.4 and section 4 of the assessment report) as well as industry developments.
- The assessors recommend performing the security assessment (including penetration testing / vulnerability assessment) for the products periodically (e.g. annually), and introducing the security assessment into and effectively combine with risks management process.

- It is suggested for Huawei to continually work on the compliance solution for PCI DSS in order to further help and support its customers on the protection of cardholder data environment. Some of references can be found in the following links:
  - HP: http://h30507.www3.hp.com/t5/Eye-on-Blades-Blog-Trends-in/Why-PCI-Compliance-is-something-that-should-not-keep-you-up-at/ba-p/109155#.UpYCfuLQbGY
  - IBM: http://www.atsec.com/us/news-pci-compliance-for-mainframe-large-computing-systems-190.html
  - Cisco: http://www.cisco.com/en/US/netsol/ns625/
- Currently, all ACLs are "permit-all" by default; it is suggested Huawei implement a rule that explicitly denies all other traffic. This rule should be specified at the bottom of each ACL and should not be modifiable. See Section 1.2.1.
- Currently, the Huawei documentation suggests the default password be changed; it is recommended that Huawei implement a one-time password mechanism and force password change on first boot. Additionally, password metrics should be enforced on this change. See Section 2.1.

2.2 PCI DSS Requirements Overview

In the cardholder data environment the PCI DSS requirements apply to all system components within the cardholder data environment these components include 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

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

3 Description of Scope of Work and Approach Taken

The Huawei CloudEngine series products (including CE7850-32Q-E1, CE6810-48S4Q-E1, CE6850-48S4Q-E1, CE6850-48T4Q-EI, CE5810-24T4S-EI, CE5810-48T4S-EI, CE5850-48T4S2Q-EI, CE5850-48T4S2Q-HI, CE12804, CE12808, CE12812 and CE12816.) were assessed in terms of how their design, development, maintenance, configuration and documentation support end users wishing to become or maintain PCI DSS compliance when using the devices in their CHDE.

A variety of techniques were used during the assessment including

- Interviewing Huawei Development and Test engineers,
- Review and assessment of documentation,
- Implementing and configuring the devices in the laboratory, representing a typical network that might be specified in a CHDE
- Observing Huawei development, testing and production processes

3.1 *Typical Network diagram*

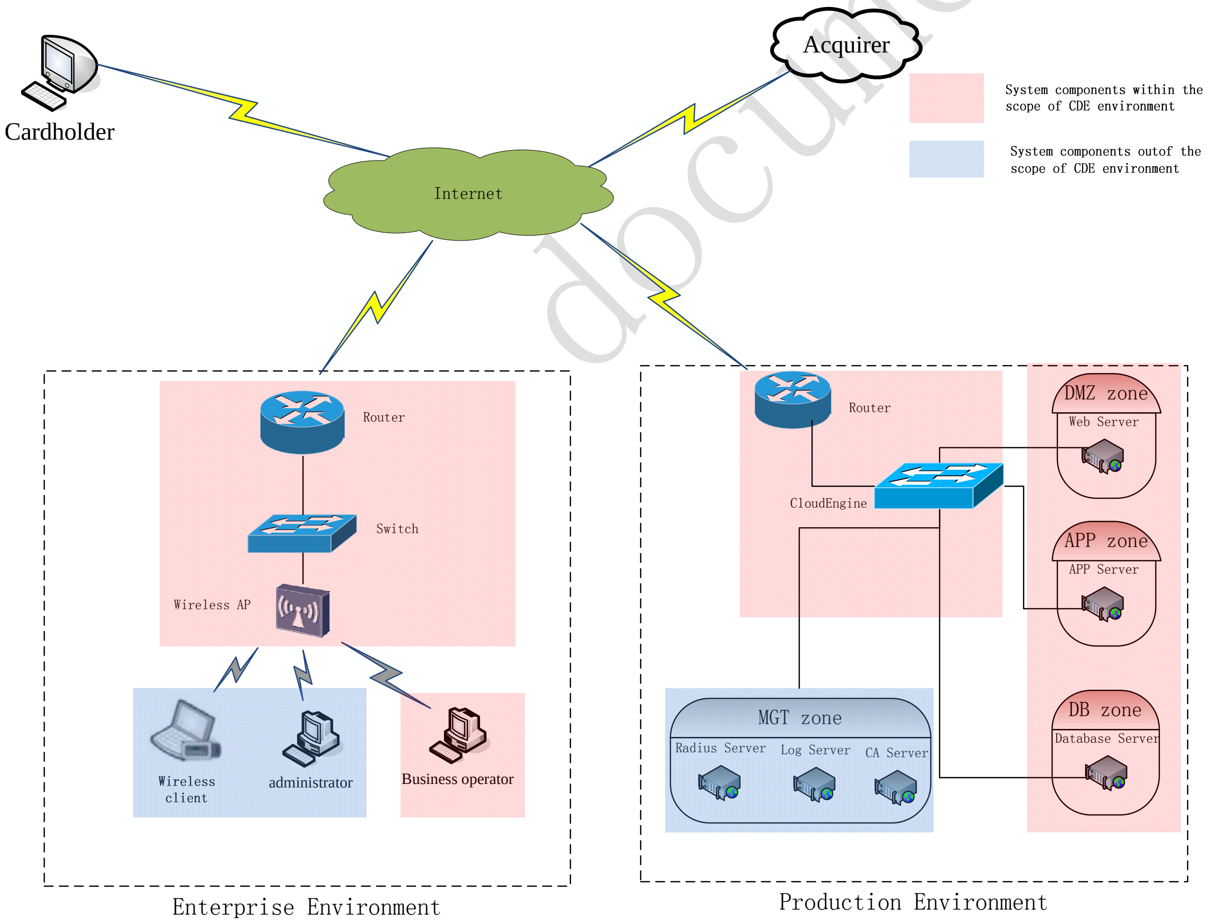

Figure 1: Typical network architecture and boundaries

The Figure 1 shows a typical network environment where the cardholder data environment resides. As shown in this figure, there are three major parts in the typical network environment:

- External entities

This part includes all external entities involved in the payment business process, such as Cardholder, merchants, acquirers, etc. Some of them are applicable for the PCI DSS compliance, nevertheless, normally they are required to conduct PCI DSS compliance themselves.

- Enterprise environment

  This part includes all internal system components in the enterprise, such as switches, routers, etc. If these system components involved in the processing, storage and transmission of cardholder data, they are involved in the scope of PCI DSS assessment.

- Production environment

  This part includes all system components in the production environment (normally resides in the server room of Data center), such as switches, routers, payment servers, database servers, etc. Based on the nature of these system components, those resides in the red box frame are involved in the processing, storage and transmission of cardholder data, thus are involved in the PCI DSS assessment.

The detailed description of typical system components in each parts are shown below:

- External entities

Name of entities	Description of entities	Connection types
Cardholder	Individuals who generate purchase order and input cardholder data.	Cardholder data is transmitted over Internet, which is protected by a HTTPS tunnel .
Merchant	Process of payment information from cardholder and transfer cardholder data for payment authorization.	Cardholder data is transmitted over Internet, which is protected by a HTTPS tunnel .
Acquirer/Card Brands	Process of payment authorization for received authorization requests from service providers and merchants.	Cardholder data is transmitted over Internet, which is protected by an IPSEC VPN tunnel .

Table 1: Typical external entities

- Enterprise environment

Name of system components	Relevance to cardholder data environment.	Function description	notes
Router cluster	yes	1. firewall access control. 2. secure non-console management. 3. audit trail generation and delivery. 4. secure wireless connection for wireless business operations.	
Huawei CloudEngine Switch	yes	1. network segregation 2. secure non-console management. 3. audit trail generation and delivery.	
Administrative clients	no	administrative access to system components in the Production environment over SSL VPN tunnel.	These servers don't process CHD, nevertheless, their

			implementation and configuration are relevant to the security of CDE.

Table 2: Typical system components in Enterprise environment

- Production environment

Name of system components	**Relevance to cardholder data environment.**	**Function description**	**notes**
Router	yes	1. secure SSL VPN tunnel for administrative access from enterprise environment. 2. IPSEC VPN tunnel for the CHD transmission to Acquirer or Card Brands. 3. firewall access control. 4. secure non-console management. 5. audit trail generation and delivery. 6. embedded IDS (Intrusion Detection System) function.	
Huawei CloudEngine Switch	yes	1. network segregation 2. secure non-console management. 3. audit trail generation and delivery.	
DMZ web server farm	yes	1. public-facing services for Internet users. 2. secure HTTPS tunnel for cardholders and Merchants.	
Application server farm	yes	1. application service for DMZ web server farm. 2. storage cardholder data to database farm.	
Database server farm	yes	central storage of cardholder data.	
Non-CDE servers	no	servers that processing with non-CHD information.	These servers are out of the scope of PCI DSS assessment.
Management servers	no	1.centrailized AAA (authentication, authorization and accounting) service for CDE system components. 2. centralized monitoring service of audit trials and file integrity for CDE system components. 3. centralized Certification Authorization	These servers don't process CHD, nevertheless, their implementation and configuration are relevant to the security of CDE.

		infrastructure for CDE system components.	

Table 3: Typical system components in Production environment

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

3.2 Applicable PCI requirements

Huawei CloudEngine Switches are hardware network appliances that work in customer's network environment. Based on the network design, CloudEngine switch can work in stand-alone mode, or implemented in cluster mode.

The following table shows the map between the security features implemented in the products and related security requirements (sub-requirements) defined in PCI DSS.

See the implementation and assessment details in section 4 "Detailed PCI DSS Requirements and Security Assessment" of the assessment report.

Requirement	PCI Sub-Requirement assessment	Related security features
1	1.2, 1.2.1, 1.2.2	Network access control
2	2.1,2.2, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.3	Secure administration
6	6.1, 6.2, 6.3, 6.3.1, 6.3.2, 6.4.4, 6.4.5, 6.4.5.1, 6.4.5.2, 6.4.5.3, 6.4.5.4, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.7	Develop and maintain secure systems and application
7, 8	7.1, 7.1.1, 7.1.2, 7.2, 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, 8.2.1, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3	User access control and account/password complexity
10.4	10.4.1, 10.4.2, 10.4.3	Accurate time synchronization
10	10.1, 10.2, 10.2.2, 10.2.3, 10.2.4,10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.5, 10.3.6, 10.5.2, 10.5.4	Audit trail monitoring
11	11.3, 11.3.1, 11.3.2, 11.3,3, 11.3.4	Security testing

Table 4: Relevant PCI DSS requirements

In addition to the above-mentioned security requirements and their implementation, some of security features could be improved and/or updated in order to further facilitate the PCI DSS requirements, and they include but not limited to:

- PCI DSS requirement 2.3: It is suggested for Huawei to test and validate the cryptographic algorithms and modules according to the standard FIPS 140-2.

For more details of each specific requirement, please refer to section 4 of this report.

Even Huawei CloudEngine switches use strong cryptographic algorithms for the password transmission and storage protection, it is also suggested for Huawei to test and validate the cryptographic algorithms and modules according to the standard FIPS 140-2.

3.3 Requirements Exclusions

Due to the nature of this assessment, several areas of a standard PCI assessment were excluded since they are not pertinent to this assessment of the devices. These are marked as "N/A" in the detailed assessment and include:

- Central cardholder data storage
- Audit log recording of all accesses to cardholder data
- Authorization/settlement processes

- Assessment of "in transit" cardholder data
- SDLC policies and procedures for general payment applications
- Live cardholder transactions (a POS environment, which includes authorization responses, was not available during the assessment)
- OS-layer system hardening (e.g. Windows servers) including anti-virus deployment
- Physical security for cardholder data environment
- PCI compliant management system including security policies and procedures

3.4 Conclusion

According to the independent assessment, it was concluded that the product(s) can be used in cardholder data environment to facilitate Huawei customers' PCI DSS compliance by configuring the product(s) correctly (refer to "Huawei CloudEngine Switch PCI DSS Implementation Guide" for how to configure and implement the product in PCI DSS manner).

For the applicable PCI DSS requirements and additional recommendation please refer to section 2.4.

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

4 Details about Reviewed Enviornment

4.1 Laboratory Testing Environment for this assessment

For each PCI-DSS requirement analyzed on the laboratory network, the QSA confirmed the status of the testing environment before conducting the security testing for the PCI DSS assessment.

The architecture and environment of the laboratory network shown in Figure 2 simulated the cardholder data environment for this PCI DSS assessment.

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

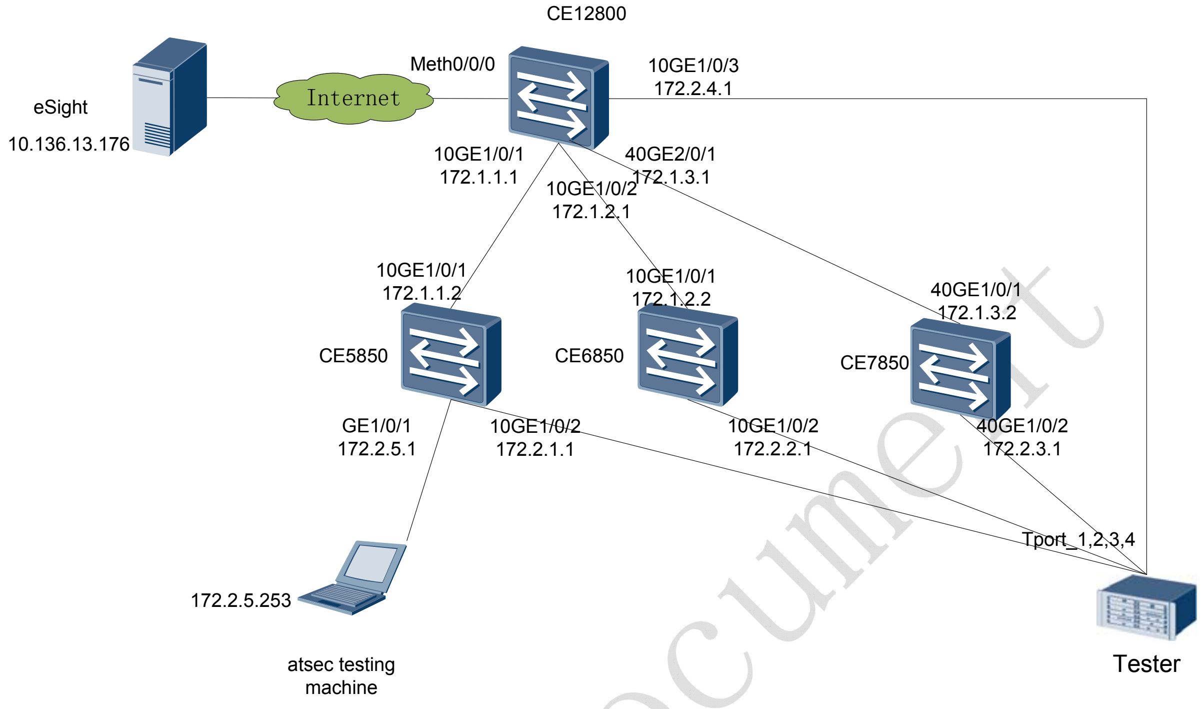

Figure 2: Laboratory testing diagram for this PCI-DSS on-site assessment

The hardware and applications that make up the laboratory testing environment are listed as following:

- Network Equipment

#	Name & version of device	Firmware Version	Number of devices in use	Connection type
1	Huawei CE 12800 switch	V100R005C10	1	Internet connection switch.
2	Huawei CE 5850 switch	V100R005C10	1	LAN switch.
3	Huawei CE 6850 switch	V100R005C10	1	LAN switch.
4	Huawei CE 7850 switch	V100R005C10	1	LAN switch.

Table 5: List of network equipment

- Related Servers and Systems

#	Name of system	OS & Version	Number of type	Connection type
1	Esight Server	V300R003C00	1	Centralized syslog collection and analysis server.
2	Testing machine	Debian 3.14.5-1kali1	1	Testing machine.

Table 6: List of servers and systems

- Utility and Software

#	Name & version of software	PCI Validated	Number in use	Systems installed on
1	Metasploit 4.10	N/A	1	atsec test machines
2	Nmap v6.45	N/A	1	atsec test machines
3	Wireshark v1.4.0	N/A	1	atsec test machines
4	Nessus 6.2.7	N/A	1	atsec test machine

Table 7: List of utilities and software

4.2 Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment.
- The cost of the PCI DSS assessment.
- The cost and difficulty of implementing and maintaining PCI DSS controls.
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations).

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, switches with strong access control lists or other technology that restricts access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

The network environment is used for the cardholder data environment. The scope for PCI DSS assessment is in the environment mentioned in section 3.2 and the network diagram in section 2.3.

4.3 Documentation reviewed

The details were stripped from the original version of the report due to the protection of confidential information.

4.4 Individuals interviewed

The details were stripped from the original version of the report due to the protection of confidential information.

5 Detailed PCI DSS Requirements and Security Assessment

For the purpose of the Security Assessment Procedures, the following definitions are used:

- PCI DSS Requirements – This column defines the Data Security Standard and lists requirements to achieve PCI DSS compliance; compliance will be validated against these requirements.
- Testing Procedures – This column shows the processes to be followed by the assessor to validate that PCI DSS requirements are “in place”
- In Place – This column must be used by the assessor to provide a brief description of controls which were validated as “in place” for each requirement, including descriptions of controls found to be in place as a result of compensating controls, or as a result of a requirement being “Not Applicable”. (Note: that this column must not be used for controls that are not yet in place or for open items to be completed at a future date.)

The details were stripped from the original version of the report due to the protection of confidential information.

6 Bibliography

6.1 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 SSC. 2013, *PCI DSS Summary of Changes V2.0 to V3.0*
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

PCI SSC. *PCI DSS* November, 2013 Version 3.0
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI SSC. 2014, *ROC Reporting Template for V3.0*.
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_ROC_Reporting_Template.pdf

PCI SSC. 2014, *Glossary of Terms, Abbreviations and Acronyms V3*
https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf

PCI SSC. 2013, *PCI DSS and PA-DSS 3.0 Version 3.0 Change Highlights*
https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

6.2 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

7 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.

Term	Definition	Explanation
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 Administrator	
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	

Term	Definition	Explanation
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	
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	Identification 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

Term	Definition	Explanation
		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
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	

Term	Definition	Explanation
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	
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

Term	Definition	Explanation
		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.
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-256 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	

Term	Definition	Explanation
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.
WEP	Wired Equivalent Privacy	
WLAN	Wireless local area network	
WPA	WiFi Protected Access	Security protocol created to secure wireless networks. WPA is the successor to WEP and is deemed to provide better security than WEP. WPA2 was also released as the next generation of WPA
WPA2	WiFi Protected Access	Security protocol created to secure wireless networks. WPA is the successor to WEP and is deemed to provide better security than WEP. WPA2 was also released as the next generation of WPA
XSS	Cross site scripting	

---------------------- The end of the report ----------------