

Study Case Remote Access for PCI DSS Compliance at Company in Jakarta

Rony Andry Anthony Sihotang

Faculty of Engineering and Information Technology, Swiss German University

Article Information

Received: 14 June 2016

Accepted: 22 August 2016

Published: 25 October 2016

DOI: 10.33555/ejaict.v3i2.95

Corresponding Author:

Rony Andry Anthony Sihotang

Email:

ISSN 2355-1771

ABSTRACT

The growth of electronic transactions in Indonesia has grown tremendously since the start of the government program of the Non-Cash National Movement (GNNT) by Bank Indonesia since 2014. It is expected that the use of cash will be replaced by electronic transactions (cashless) using ATM cards, debit cards, credit cards, electronic cards. Electronic transactions must be reliable and secure, this is what drives 5 international payment networks such as American Express, Discover, JCB, Mastercard and Visa create a data security standard to secure cardholder data PCI DSS (Payment Card Industry Data Security Standard). PCI DSS has always evolved to always keep cardholder data secure for transaction and now PCI DSS has released PCI DSS version 3.2 in April 2016.

Employees need to connect to internal private networks or corporation's network over the Internet from home or public areas such as hotels, airports, cafe mall etc. Security becomes a major consideration when access to internal networks or corporation's network from insecure network. In this case study, one company with head office located in Jakarta, Indonesia with team development located in Seoul, South Korea. Also see the connection between convenience and security when implementing remote access in accordance with PCI DSS requirements.

Keywords: Electronic transactions, Cardholder data, PCI DSS, Remote access

1. Introduction

Based on Indonesia's economic report of 2016 made by Bank Indonesia, the number of electronic money instruments increased significantly. Electronic money instruments increase 49,3% and volume and value of electronic money transaction increase 23,8 % and 34,3 % compare to 2015 (Bank Indonesia, 2016).

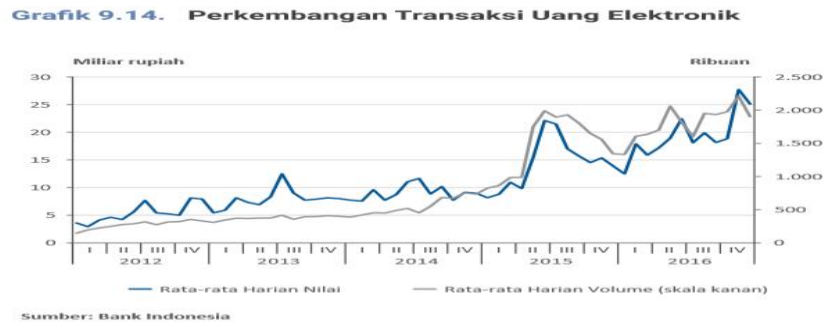


Figure 1. Electronic Transaction in Indonesia

1.1. PCI DSS (Payment Card Industry Data Security Standard)

With the growth of the above transactions, seen the numbers use of credit cards, debit, electronic money more and more done. This encourages the need for implementation security standard and procedure to secure information about credit card and debit card owners.

PCI DSS is a cardholder's data security standard whether credit cards, ATM cards, debit cards, or e-money cards issued by the Security Standard Council consisting of five major international payment networks, American Express, Discover, JCB, Mastercard and Visa. Previously international payment networks know how important it is to secure customer cardholder data so that each international payment network has its own security standards, Visa - Account Information Security (AIS), MasterCard - Site Data Protection (SDP), American Express - Data Security Standards (DSS), Discover Card - Discover Card Information Security (DISC) and JCB - Data Security Program.

Due to the similarities amongst standards, they collaborate to make security standard for payment industry PCI DSS on December 16, 2004. There are 6 principles, 12 requirements for PCI DSS.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 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 for all personnel

Figure 2. PCI DSS

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. All organization with access to cardholder data information must meet the data security standard.

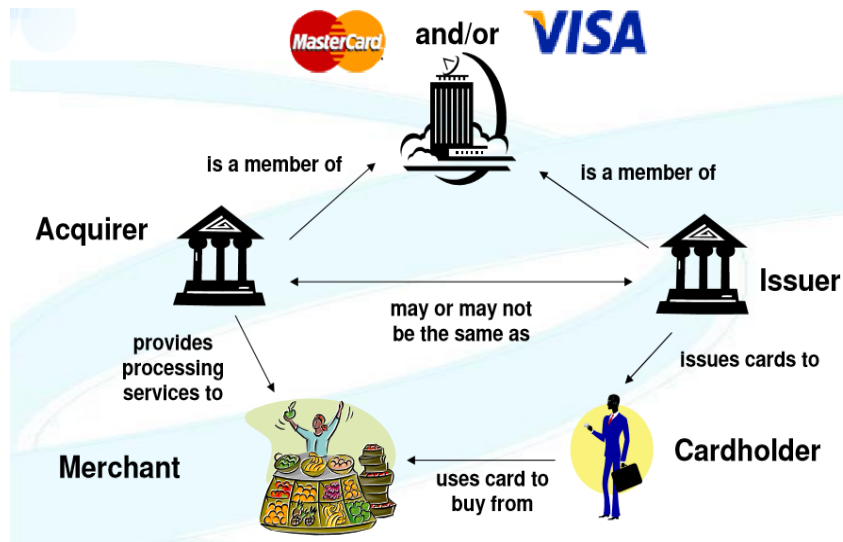


Figure 3. Flow Transaction Electronic Transaction Using Credit Card.

There have been a numbers of version PCI DSS, currently now PCI DSS version 3.2 was released April 2016 and will be effective in 1 February 2018. The important things, PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements meanwhile PCI DSS mandatory as security framework in payment industry.

The PCI DSS represents a common set security standard for payment industry and measurements to help ensure the safe cardholder data and sensitive information.

Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
<ul style="list-style-type: none"> ▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code 	<ul style="list-style-type: none"> ▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

Figure 4. Cardholder Data and Sensitive Authentication Data.

1.2. Remote Access

Remote access is the ability get access for log on to a computer or network over network from remote distance. It's common used for employee to work offsite, home or public area such as restaurant, cafe, airport etc. Security becomes a major consideration when access to internal networks or corporation's network from insecure network.

Providing remote access to users means, making people to easy for access their data from anywhere in the world, and ensure that the data which is sent and received protected from compromise and unauthorized alteration. Most users use VPN technology (Virtual Private Network) with a more secure assumption because of the VPN concept that creates tunnels

between both sides as well as encrypted data packets. The National Institute of Standards and Technology (NIST) Special Publication, 800-77.

1.3. Multi-factor authentication (MFA)

To protect information customer need security standard policy and procedure. If not, a malicious person may steal customer's information and can access any information owned by the customer. That's why authentication is required. Authentication is one way to tell if a person accessing a system is a user of the right and appropriate or not. Currently most systems, authentication is limited to PIN and password only.

MFA is an authentication method that combines several factors such as something user know such as password, PIN, user has such as smartphone, token and user physical body such as fingerprint, retina, voice. One example of the use of MFA can be found when using internet banking to perform banking transactions, which in addition to using a username and password, must use a hard token or soft token before providing authorization when making transactions. This technology already popular since 2010 in Indonesia.

In this study case, one company in Jakarta have their developer team abroad, that needed access to develop, test and production for troubleshoot. To meet the needs of developers who are in South Korea for access into the internal/corporate network, VPN IPsec Site to site choose as solution.

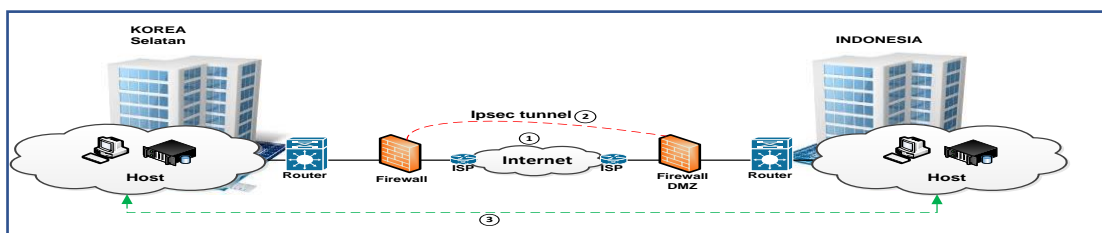


Figure 5. Existing Configuration Remote Access

Current configuration above is only limited to the remote access needs of office buildings located in South Korea, beyond the location of the office building the need for remote access cannot.

The question for the current configuration right now, *it's comply with PCI DSS?*

In the other case, new policy on remote access to PCI DSS version 3.2 - 8.3.1 *Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.* Where the use of multi-factor is requirement from 1 February 2018.

As a payment industry company where PCI DSS is an obligation and to meet new requirements in PCI DSS version 3.2, the company realizes that the current configuration *does not meet the standards of PCI DSS* especially in the current PCI DSS version 3.2 where the use of authentication multifactor is required. To meet the new requirements required on PCI DSS, the company makes configuration changes by combining multiple solutions simultaneously such as the use of access servers and the implementation of multi-factor authentication.

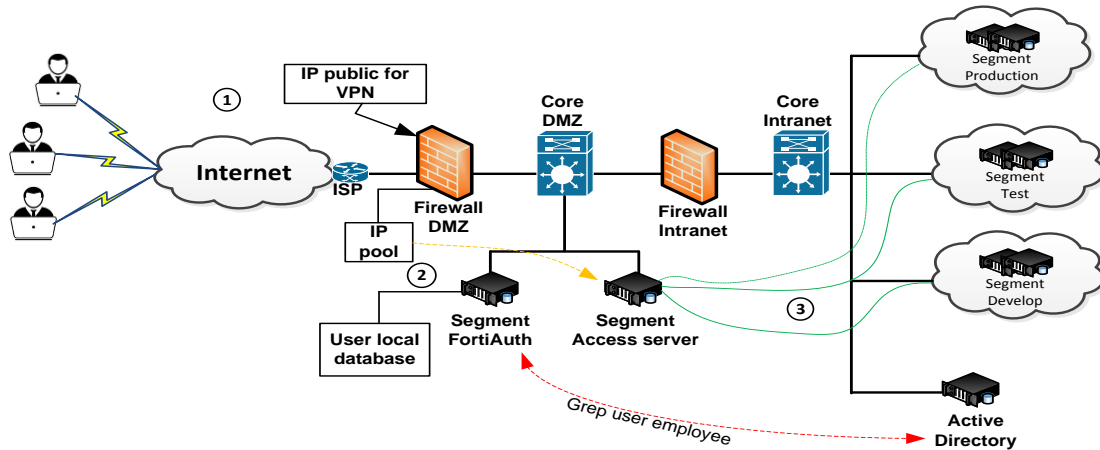


Figure 6. New Configuration

With new configuration changes there are some improvements and advantages gained in addition to the fulfillment of PCI DSS needs, among others, the need for remote access that can be implemented anywhere not limited to the location of the office only, the separation of authority in accordance with the job desk, the fulfillment of internal access needs that must also through multi factor to access cardholder data environments (CDE).

2. Methodology

A qualitative method using survey and interview involving 20 users of employee was conducted to explore impact of introducing remote access using multi factor authentication technology and to fulfill new requirement PCI DSS. (Dean, B., 2016). To obtain complete data is done, questioner filling stage for developers who are in Korea as well as for user and interview for developer, operation and planning in Indonesia. The execution time is held on mid Oct 2017.

The result of the interview and the questioner result is recorded to be analyzed so that the answer to the question with the following results can be obtained:

Participant Location		Job Description		Easy to use	
South Korea	40%	Developer	55%	Yes	85%
Indonesia	60%	Operations	30%	No	15%
Experience with MFA		User Experience		Secure	
Yes	85%	Good	85%	Yes	100%
No	15%	Average	10%	No	0%
Security awareness		Meet PCI DSS Requirement			
Good	90%	Yes	100%		
Not good	10%	No	0%		
Segregation of duty					
Yes	95%				
No	5%				

Figure 7. Result Interview and Questioner

3. Result

This section, the impact of implementation new configuration with using access server and MFA to improve the security and comply for PCI DSS new requirement is discussed. The results of interviews and questionnaires become the material to be analyzed in the discussion.

3.1. Remote Access

The survey and questionnaire results show that remote access is absolutely need as most developers are in South Korea. MFA as one of the authentication methods for remote access is absolutely and this is in accordance with the requirements of PCI DSS. From 8 of the questioner in South Korea, 3 of them very happy because with this new solution they can work offsite, not need come to office for support to handling problem.

3.2. Multi Factor Authentication

MFA is not new based on survey data and all users do not have problems with the use of MFA even for users who have never had experience with the use of MFA is not an obstacle in the work. One of the participants who had never had experience in using MFA during the interview stated that the current MFA usage is almost the same as the use of MFA in internet banking transactions.

3.3. Secure

All participants said the current configuration is very secure and confident it will meet PCI DSS requirement this is shown where the participant can only access in accordance with job description. Some of the participants showed a sense of objection because in the new configuration now they can only do remote access based on the authority they have in accordance with their job desk. This is different than the old solution where they can enter the network freely and can access the entire server. However, after obtaining an explanation that one of the concerns of PCI DSS regarding the granting of authority for access to CDE. Although 10% of the total participants lacked a degree of awareness about security but they realized the importance of PCI DSS as a necessary condition for companies that are in the payment industry.

4. Conclusion

The main purpose of this research is to investigate how remote access can comply with PCI DSS by assessing its impact on the key adoption factors. The findings show that the use of multi-factor authentication does not actually affect for user, still convenient to use, secure, meet the new requirement of PCI as perceived by the study participants.

References

Bank Indonesia. (2016). Online Available: <http://www.bi.go.id/id/publikasi/laporan-tahunan/perekonomian/Documents/LPI2016-web.pdf>.

Dean, B. (2016). Google's 200 Ranking Factors: The Complete List. <https://backlinko.com/google-ranking-factors>.

Lufei, H., Shi, W., Chaudhary, V. (2008). Adaptive Secure Access to Remote Services. IEEE: International Conference on Services Computing.

Neuman, W.L., (2006). Social Research Methods: Qualitative and Quantitative Approaches. USA: 6th Ed, Pearson.

PCI Security Standards Council. Online Available: https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

PCI Security Standards Council. Online Available: <https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf>.

Singhal, M., Tapaswi, S. (2012). Software Tokens Based Two Factor Authentication Scheme. International Journal of Information and Electronics Engineering, 2(3), May 2012.

The National Institute of Standards and Technology (NIST). Special Publication, 800-77.

The National Institute of Standards and Technology (NIST). Special Publication 800-113.

The SANS Institute. Online Available: www.sans.org.