**How to Comply to Requirement 4 of PCI DSS**

The requirement 4 of the Payment Card Industry Data Security Standard talks about the safe transmission of cardholder data from sender to receiver, across open networks. Public wireless networks are easy targets and hackers can extract sensitive data flowing across these networks with simple hacking techniques.

**PCI DSS Requirement 4: Encrypt transmission of cardholder data across open, public networks.**

Safe transmission of cardholder data across open networks requires that encryption be applied before transmitting data from one place to another. Encryption and authentication protocols should be strong enough and wireless networks should be correctly configured as malicious users can easily exploit their vulnerabilities and gain access to the Cardholder Data Environment (CDE).

The requirement 4 is further broken down into 3 sub-requirements and compliance to each is a must to achieve overall PCI DSS compliance.

**4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:**

* **Only trusted keys and certificates are accepted.**
* **The protocol in use only supports secure versions or configurations.**
* **The encryption strength is appropriate for the encryption methodology in use.**

For safe transmission of cardholder data from the sender to receiver over a public network, it is important to use reliable certificates or keys, strong encryption, and secure authentication protocol to transport data over the network. Any requests to join by systems that could result in an unsafe or unsecured connection to the network should be rejected. Some of the examples of open networks include the internet, wireless technologies such as Bluetooth, cellular technologies such as GSM and CDMA, satellite communications, General Packet Radio Service GPRS, etc. It is important to keep in mind that some of the authentication protocols such as TLS 1.0, SSL v2.0 and SSH v1.0 have vulnerabilities known to hackers and can easily be exploited by them for getting information access or even diverting the information flowing across a network. Hence, to prevent this exploitation, protocols should be configured with their secure versions only. The certificates should be obtained from a reliable certificate authority and should be verified for expiry.

To carry out a compliance check, all locations of cardholder data transmittal over public networks should be identified. The actual applied system configuration setting should then be checked against the documented procedures to ensure that they are actually being put into practice. The processes should be verified for recognition of trusted certificates and/or keys, use of secure version of protocol and a strong encryption methodology. Verification should be done by selecting a sample of data transmission and identifying whether strong cryptography is applied on the data during transit or not, protocol with secured version is being used and only trusted keys are accepted. For strong cryptography, verify that the wireless networks transmitting the cardholder data use industry best practices for encryption, such as IEEE 802.11.

Moreover, examine system configurations and check that the Transport Layer Security / Secure Sockets Layer (TLS/SSL) should be enabled before cardholder data is set to being transmitted across a network. TLS and SSL are internet security protocols used by internet browsers for implementing public-key encryption. These protocols are used by the web servers and browsers to send or receive confidential information. For example, when using an internet browser, a user puts his credit card information, it is important that he is doing so under the protection of a TLS/SSL protocol. Here, the simple “http” is replaced by “https” in the address line, ensuring that the information is passing along securely. TLS and its forerunner SSL also help make use of certificates. When the browser requests for a secure page by adding an “s” to “http”, it sends a public key along with a certificate and ensures that; the certificate is from a reliable trusted authority, it is still valid, and is related to the site from where it is being originated. Hence, it is important to verify that these security protocols are enabled whenever cardholder data flows across a network.

**4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).**

This requirement maintains that Personal Account Numbers should never be sent unencrypted or in plain text format over a messaging platform such as emails, instant messengers or chat, etc. These platforms are vulnerable to exposure through packet sniffers that can be used by malicious individuals to extract valuable confidential information such as PAN. A packet sniffer, also known as a network analyzer or network monitor, is actually intended for legitimate use by a network administrator who monitors and troubleshoots network traffic. But if a network administrator wants to use a packet sniffer for the wrong purpose, he can monitor the entire packets passing through the network and can view any information that is being transmitted in clear text format. Therefore, such messaging tools should only be used for sending such information if they have been configured to encrypt the data being sent or received.

Compliance to this requirement entails that a sample of outbound messages should be taken and examined. This would help to verify that Personal Account Numbers are encrypted via strong cryptography if end-user messaging technology is being used to send cardholder data. Moreover, there should be a written policy for this and it must be reviewed to check that it clearly forbids the transmittal of unprotected or unencrypted PAN’s across end-user messaging platforms.

**4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.**

To comply with the PCI DSS requirement, it is important to draft strong policies and procedures regarding the protection of cardholder data over a network. There should be policies for strong encryption, authenticated protocols and the use of reliable keys and certificates. Moreover, these policies and procedures should be communicated to every individual member of the staff and it should be ensured that every individual understands them. Only this way it will become possible to manage safe transmission of data on a regular basis.

To verify that this requirement is being met, the documentation needs to be examined and personnel should be interviewed to ensure their understanding.