**The Scope of PCI DSS**

The scope of PCI DSS pertains to everything that revolves around the cardholder data environment (CDE). This means that both the electronic as well as physical environment should be catered for against the PCI standard. This includes people, networks, applications, technologies, and everything that takes a direct or indirect role in storing, processing or transmitting cardholder information.

**How to Determine the Scope?**

In order to assess the scope of PCI DSS for your organization, the first and foremost step is to determine the cardholder data environment (CDE). Although it may seem easy to determine the CDE at first, it may prove to be a difficult task for even very small organizations. It is therefore important to understand exactly what should be considered when determining the CDE. The following steps must be taken to determine the PCI DSS scope:

* Identify and document the flow of cardholder data. This process should characterize all applications storing the cardholder data along with other involved applications.
* Build up a network diagram showing all the access points, firewalls, servers, switches and all other network devices.
* Scan the network to verify that the cardholder data does not lie anywhere outside the CDE defined by the organization. This can be done with the help of Data Loss Prevention (DLP) technology, or with the help of a number of free or open source utilities provided by various vendors. If your organization does not want to invest in a database scanning utility, the scan can also be performed manually. All you need to do is to take down the credit card account number field and comment fields preferably in a CSV file format and scan these files with the utility you are already using.
* Securely delete and migrate any data that is found out to be not included in the currently defined CDE after the scanning process and redefine the CDE.

**What falls under the scope of PCI DSS?**

To make it simpler to understand this, the following rules must be considered when determining the scope for PCI compliance

1. The PCI DSS requirements relate to every single component of the system that directly or indirectly forms a part of the cardholder data.
2. The CDE or Cardholder Data Environment consists of the processes, technology and people handling the data.
3. The standard is also applicable to any other system that is responsible for the security of the systems already in scope, such as log management, IDS management and authentication systems.

**Confusions Regarding the Scope Determination**

1. **Organizational Networks**

Organizational networks that are used for transmitting cardholder data are naturally in scope of PCI DSS. This is easily understandable and widely accepted. However, confusion arises when the talk of encrypted data comes under consideration. Many service providers argue that since the cardholder data is encrypted, it does not come under the scope of PCI DSS. What they fail to consider are the encryption endpoints. It is important to note here that the endpoints of encrypted information always come under the scope of PCI compliance. This is necessary for the QSA as they need to check for the compliance at the sender and receiver end, and not only the connecting medium between the two.

1. **Applications**

All applications that are involved in storing, processing or transmitting cardholder data come under the scope of PCI DSS. As easier as it may seem to be understood, confusions still exist as there are many entities related to applications and one needs to determine whether they fall under the scope or not. To minimize this confusion organizations are now more inclined towards taking help of application packages through vendors. This enables them to better understand cardholder data flow process. Although the PA-DSS has been a big help in getting these data flow diagrams, still, there are many credit card applications that do not supply any such diagrams.

Another confusion arises when two application packages are made to communicate and integrate with each other. It becomes difficult to determine whether the cardholder data during the integration process is in a legible format or whether it is encrypted. Yet again, the integration consoles are mostly based on browsers and anyone in the network can easily access the information. Therefore, these should also be considered when determining the scope of PCI DSS.

**How to Reduce the Scope of PCI DSS?**

To make things easier for the organization, and to effectively succeed in compliance to the PCI DSS, it is important to reduce the scope of compliance. Here are a number of ways that can be helpful in PCI scope reduction.

1. **Network Segmentation**

Network segmentation is one of the best methods for reducing PCI compliance scope. It is a process in which the cardholder data is isolated from the rest of the network. This relates to logical isolation through a firewall or with the help of router with restricted access, as well as physical separation of networks. If network segmentation is not implemented, the whole of the network comes under the PCI DSS assessment scope. The network segmentation should be done in such an accurate manner that even if an out-of-scope entity is compromised, it brings no harm to the information concerning the cardholder data. If network segmentation is used as a means to limit the scope of PCI DSS, the SQA must verify that it is correctly serving the very purpose.

1. **Tokenization**

Tokenization is a process in which a string of text is broken up into random words, symbols or numbers known as tokens. With the help of the tokenization process, the Permanent Account Number (PAN) of a card is replaced by a token that does not pose any security threat to the cardholder data even if it goes in the hands of a malicious user.

The difference between tokenization and conventional encryption method is that in the encryption process the sensitive information is encrypted and the cipher text returns to the original place. With tokenization however, a substitute value is returned instead of original data. This token serves as a reference to the actual cipher text. The process of tokenization and de-tokenization should take place in a well defined system consisting of approved applications.

**How Tokenization Works**

* The application is accessed by the user who also authenticates himself by providing the PIN.
* The application stores this information and passes along the PAN with the PIN to verify.
* The tokenization system checks for the authentication of the information provided.
* If the information provided is not authenticated, the tokenization process terminates.
* If the information is authenticated, a new token is generated with a PAN which is mapped with the vault PAN.
* The token generated is sent back.

**How De-tokenization Works**

* The application is accessed by the user who also authenticates himself by providing the PIN
* The application stores this information and passes along the PAN with the PIN to verify
* The tokenization system checks for the authentication of the information provided
* If the information provided is not authenticated, the tokenization process terminates.
* If the authentication proves successful, the card data vault is checked for any records related to the token and the PAN is retrieved.
* The tokenization system then returns PAN value that was retrieved in the earlier step.

## How does Tokenization help reduce PCI DSS Scope?

1. Tokens cannot provide the actual data value under any circumstances. The only relationship between the token and the data value is that of reference. If tokens are accessed by an outside individual, no threat is faced by the organization. The actual encrypted data is saved in a centralized data vault and a token is only a representation of that. Whenever an application needs to access that sensitive cardholder data, it has to generate a request through the tokenization process.
2. When tokenization is used, there is a lesser use of distribution of cryptographic keys. With lesser risk of a key being compromised, the scope of PCI DSS can be minimized. However, if the generation of a token is based upon cryptographic keys, then it is important to securely manage the keys as a breach of security of keys can result in the tokens being compromised.
3. In tokenization process, the original or encrypted form of the cardholder data is stored in a vault and is never exposed. The token that is used as their reference is then deployed for use in every database and/or application. This in turn greatly helps to reduce the PCI DSS compliance scope.