What is a Cardholder Data Environment?

Any part of an organisation or merchant where its people, processes, and technologies, store, process, or transmit payment card data, will be in scope for PCI DSS. This data will be classed as part of their Cardholder Data Environment (CDE).

As most data breaches involve a compromise of the CDE, PCI DSS requirements require a wide variety of security controls to be maintained to help protect this data.

In summary, the CDE consists of:

- All system components that store, process, or transmit Cardholder Data (CHD) or Sensitive Authentication Data (SAD).
- Any component that directly connects to CHD systems.
- Any component that supports CHD systems (such as update servers (WSUS, anti-virus, etc.) and authentication support (domain controllers, etc.) must be included.

The PCI DSS security requirements apply to all ‘system components’ included in, or connected to the CDE. Examples of system components include, but are not limited to the following:

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (e.g. domain controllers, name resolution, or web redirection servers) the CDE.
- Virtualisation components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Third party devices, systems, networks or people, such as remote access, VPNs, IT support.
- Any other component or device located within or connected to the CDE.

What is Payment Card Data?

Payment card data is comprised of Cardholder Data (CHD) and Sensitive Authentication Data (SAD) and must be protected as per the PCI SSC guidelines;
Why do I need a Cardholder Data Environment diagram?

The CDE diagram is one of the most important first steps for any organisation trying to determine CHD use across their people, departments, and systems. It should be used as one of the organisation’s central reference points when dealing with PCI compliance and protecting cardholder data.

For the PCI DSS SAQ B-IP & SAQ D questionnaires this diagram is mandatory. For the remaining questionnaires it is not mandatory but is good practice to create a diagram which will illustrate where cardholder data is potentially stored, how it flows through an organisation and how it is dealt with. Without a CDE diagram, CHD may be overlooked, unprotected, exposed to fraud, and stored in breach of PCI DSS.

By understanding where CHD is stored, processed, or transmitted, it can;

- Help an organisation understand and define it’s CDE.
- Define the relevant PCI DSS SAQ questionnaire/s.
- Help understand which PCI DSS requirements are applicable to the organisation.
- Highlight potential security weaknesses in systems/processes.
How to create a Cardholder Data Environment Diagram

To identify where CHD storage, processing, or transmission is within your organisation, it is necessary to understand all payment method/channels. This is a generally a collaborative effort between departments and can be broken down to three payment channels - Ecommerce, Face-to-face, and MOTO (Mail Order/Telephone Order).

To develop a CDE diagram you will need:

- **Up-to date IT network documentation**
  Without a current network diagram, devices could be overlooked, and unknowingly left out of the controls implemented for PCI DSS.

- **Knowledge of all payment processes within the organisation**
  How payment is taken, by who, and where? Is the data stored? Why? Who has access to the data? Sometimes this is the most difficult part to investigate due to the many different forms, and historic ways of taking cardholder data throughout an organisation.

The first step to creating a CDE diagram is to scope what is and isn’t included in the CDE (trusted), and the untrusted network.

Follow the movement of the data from its entry point(s), through the organisation until it permanently leaves the organisation or is destroyed. This will identify all the components that are involved in the processing, storage, and transmission of the cardholder data. A full definition of the components are listed in the ‘What is the Cardholder Data Environment’ section.

A list of Merchant ID’s (MIDs) used by an organisation/merchant will help highlight potential payment sources - this list will be available from the acquiring bank. If a MID is not owned by the merchant, the merchant does not need to comply with PCI DSS for that payment channel.

Steps to creating a Cardholder Data Environment Diagram

1. Create or use an existing network diagram showing all locations, networks, and connectivity (internal and external).

   A hand drawn diagram is the best place to start, and can be made professional using a design package. Due to requirement 1.1.2(b) requiring the CDE diagram to be updated when changes occur, a design package makes it easier to make revisions and create a document history.

   There are many different design packages that can be used to draw the diagram, some free, some expensive, all with different functionality.

   Here are a selection:

   - [Microsoft Visio](#)
   - [Gliffy](#)
   - [LucidChart](#)
   - [yEd](#)
An example of a basic network diagram;

2. Create a copy of the network diagram for each payment channel that is used - Ecommerce, Face-to-face, and MOTO. A single diagram can work for smaller configurations but may become confusing with multi-channel systems.

3. Add payment systems that store, process, or transmit CHD (listed in ‘What is a Cardholder Data Environment’) for each payment channel to the diagrams. Examples would be:
   - Websites hosted internally or via a 3rd party service provider
   - Applications/databases
   - Payment terminals (PSTN, network (IP), or mobile (GPRS)
   - Virtual terminals
   - POS systems (PC’s, servers, equipment)
   - Telephone call recording systems
   - VOIP telephone systems
   - Post/email
   - Merchant receipts/paper
   - Fax/e-fax
   - Backup systems/sites/devices/media
   - Archived cardholder data/systems
   - 3rd party devices/systems/support

4. Use arrows and numbers to show the cardholder data flow movement between people, devices, people, and entities as shown in the examples below. In addition, use colour coding and keys to assist in showing where CHD is;
5. All CDE diagrams should also include a date with the minimum being the last review data of the diagram which provides evidence that it has been reviewed and updated appropriately according to PCI requirements. The approver of the document and version should be maintained within the CDE diagram document.
A closer look at Requirement 1.1.2 – Cardholder Data Environment Diagram
December 2015 - Jason McWhirr, PCI QSA

References

- PCI DSS v3.1
- PCI SSC Cardholder Data Storage Whitepaper

Copyright © 2015 Sysnet Global Solutions. All rights reserved.
Public