Milestone 1 Requirements 1.1.2 and 1.1.3
Network and Data Flow Diagrams

Network Diagrams

PCI-DSS Requirement 1.1.2: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.

The Network diagram documents information about the client’s environment. The Network diagram identifies all the segments and how each segment communicates with the others and how internal zones interact with the internet. Aided by the network diagram, the user or a Qualified Security Assessor can evaluate segmentation and determine which segment is to be considered in-scope or out-off scope. Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, technologies that restrict access to a particular segment of a network or physical isolation. If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the segmentation must be verified and assessed to be adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not.

Requirement 1.1.2 requires the assessor to validate that a current network diagram with all connections to cardholder data, including any wireless networks, be available and also ensure that a process is in place to keep the diagram current.

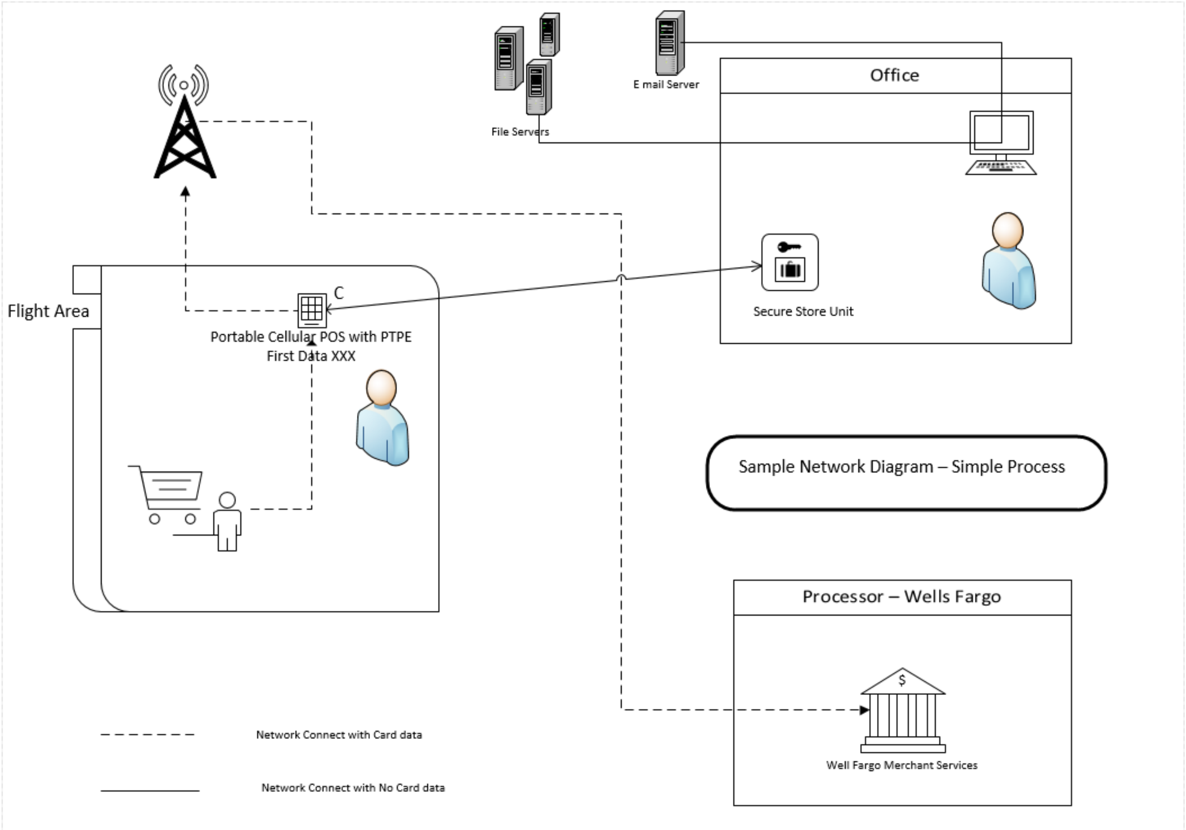
A network diagram should illustrate 3 key points about the network:

- What devices exist on your network
- How are those devices connected
- Where are those devices physically located

The goal in creating network diagrams should be to show everything that is contained in the cardholder data environment (CDE) and all of the network connections to the CDE. This level of detail is required to reconcile your configuration standards, running configurations and other relevant documentation to the network diagram as part of the process to ensure that the CDE is properly defined and securely configured.

At a minimum, the information needed on a network diagrams includes, all virtual local area network (VLAN) numbers (if applicable), IP address ranges/blocks for relevant network segments and key firewalls, routers, switches and servers along with their DNS names and IP addresses.

Milestone 1 Requirements 1.1.2 and 1.1.3
Network and Data Flow Diagrams


E mail Server
Office
File Servers
Flight Area
C
Portable Cellular POS with PTPE
First Data XXX
Secure Store Unit
Sample Network Diagram – Simple Process
Processor – Wells Fargo
$
Well Fargo Merchant Services
Network Connect with Card data
Network Connect with No Card data

Data Flow Diagrams

PCI-DSS Requirement 1.1.3: Current diagram that shows all cardholder data flows across systems and networks.

The purpose of a data flow diagram is to identify all CHD that is processed, stored or transmitted within the environment, it goes beyond what is on the network.

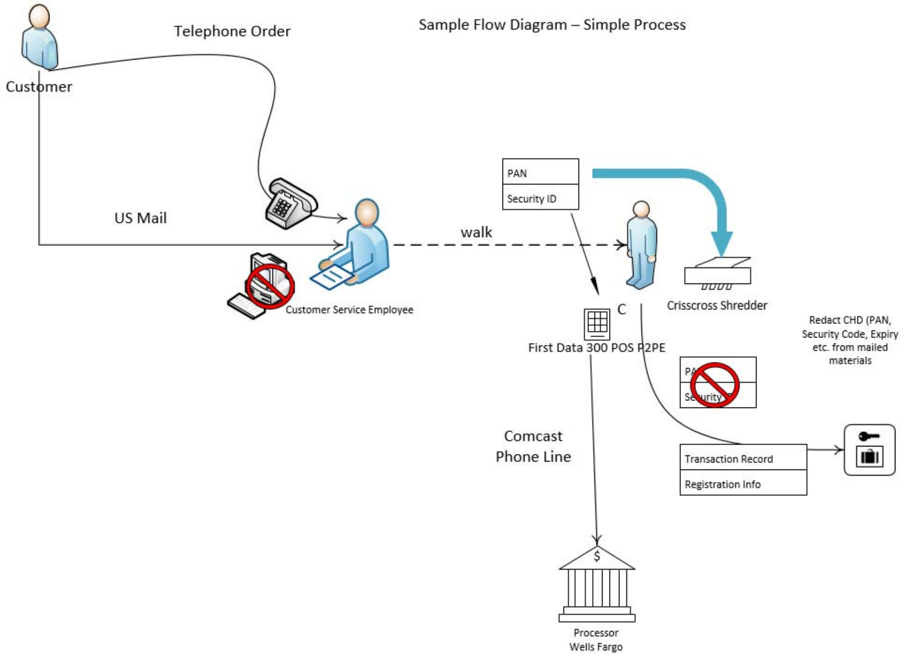
A Data Flow diagram illustrates and documents the following, if applicable:

- Where the data comes from and goes to ‘
  - Sources of received CHD
  - Destinations of transmitted CHD
- Where CHD is stored
- The process that destroys or purges CHD
- Where the hand-offs are between encrypted data and unencrypted data

Data Flow diagrams aid in the understanding data and data flow and are a tool to keep track of the CHD environment. Data Flow diagrams should identify the location of all CHD that is stored, processed or transmitted within the network. The diagram also depicts how CHD flows between individual systems, applications, processes and data stores. Finally it should aid the user in visualizing where the data comes from, goes to and the process that occurs between those two points.

Data flow diagrams need to provide the following.

- Identify all transmission and processing flows of cardholder data (CHD) including: authorization, capture, settlement, chargeback and any other CHD applicable data flows.
- For each transmission and processing flow: describe how cardholder data is transmitted and/or processed and identify the types of CHD involved (for example, full track, PAN, expiry date).



Data flow diagrams should contain enough detail for readers of the Report on Compliance (ROC), but not enough detail to aid an attacker if they get a hold of the ROC.

Data flow diagram let the assessor determine how the data is being transmitted in the system, how the inputs and outputs relate to each other and what encryption mechanism is being used to transmit the cardholder data.

Assuming a simple process one flow diagram may be enough, however for more complex flows you may need to create multiple diagrams to get your meaning across and avoid packing too much information into a single drawing.