Security Standards Council™

Standard: Data Security Standard (DSS)
Version: 1.2
Date: July 2009
Author: Wireless Special Interest Group

Information Supplement: PCI DSS Wireless Guideline

Prepared by the PCI SSC Wireless Special Interest Group (SIG) Implementation Team

Table of Contents

1 Document Overview

1.1 Document purpose

This document provides guidance and installation suggestions for testing and/or deploying 802.11 Wireless Local Area Networks (WLAN) for organizations that require Payment Card Industry's Data Security Standard (PCI DSS) v1.2 compliance. The goal is to help organizations understand how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and practical methods and concepts for deployment of secure wireless in payment card transaction environments.

1.2 Document scope

This document will focus on suggestions about how 802.11 WLAN can be deployed in accordance with PCI DSS v1.2 within the Cardholder Data Environment (CDE). It will also briefly review possible installation suggestions and greater operational procedures required to make WLAN part of an overall PCI DSS compliant network.

This document will **not cover** any networks using Bluetooth or GPRS.

1.3 Audience

This document is intended for organizations that store, process or transmit cardholder data that may or may not have deployed wireless LAN (WLAN) technology as well as assessors that audit for PCI DSS compliance as it pertains to wireless.

2 Wireless Operational Guide for Complying with PCI DSS

PCI DSS wireless requirements can be broken down into the following two primary categories.

Generally applicable wireless requirements: These are requirements that all organizations should have in place to protect their networks from attacks via rogue or unknown wireless access points (APs) and clients. They apply to organizations regardless of their use of wireless technology and regardless of whether the wireless technology is a part of the CDE or not. As a result, they are generally applicable to organizations that wish to comply with PCI DSS.

Requirements applicable for in-scope wireless networks: These are requirements that all organizations that transmit payment card information over wireless technology should have in place to protect those systems. They are specific to the usage of wireless technology that is in scope for PCI DSS compliance, namely the Cardholder Data Environment (CDE). These requirements apply in addition to the universally applicable set of requirements.

2.1 Defining the Cardholder Data Environment (CDE)

Let's begin by defining, in very simple and generic terms, the CDE. The CDE is defined as the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment. In Figure 1 we see a CDE consisting of a **cabled network**.

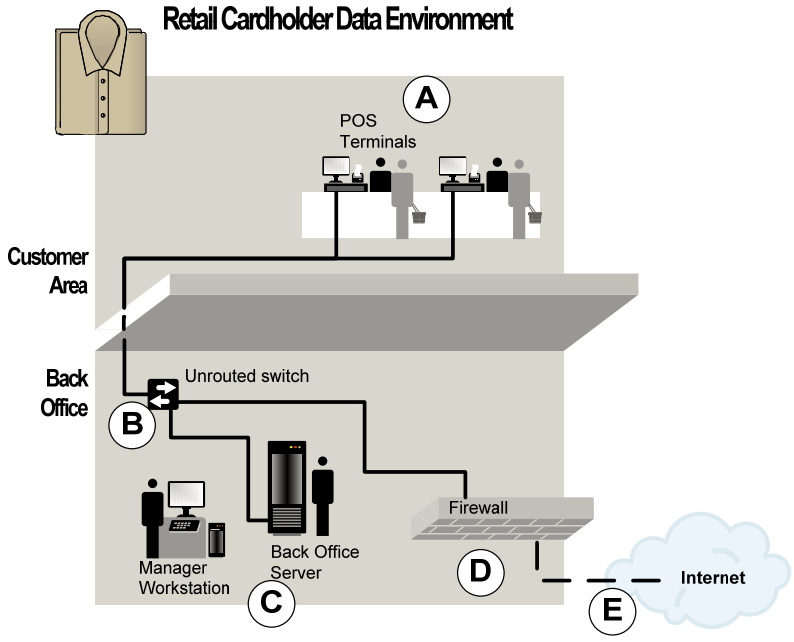

Figure 1: Cardholder Data Environment

A. These are the Point of Sale terminals wherein the cardholder data enters the network.

B. This could be a hub, switch or other network device that acts to connect all devices to the same data environment. In this case, it transmits cardholder data.

C. This is a back office server that is within the CDE by the fact that it is connected to the same cabled network, whether it stores cardholder data or not.

D. This is a firewall that demarcates the edge of the organization's CDE.

E. Traffic leaving the firewall and traversing an open or public network is encrypted to restrict the scope of the CDE to the end-points of the encryption and decryption process.

Wireless networking is a concern for all organizations that store, process or transmit cardholder data and therefore must adhere to the PCI DSS. Even if an organization that must comply with PCI DSS does not use wireless networking at all, the organization must verify that wireless networking has not been introduced into the CDE over time. Therefore, this CDE is in scope for PCI DSS *and* this guide, in that the organization must *verify* and continue to *ensure* that there are no WLANs attached to the network.

This is because there are validation requirements that extend beyond the known wireless devices and require monitoring of unknown and potentially dangerous rogue devices. A rogue wireless device is an unauthorized wireless device that can allow access to the CDE.

2.1.1 The "rogue" WLAN Access Point (AP)

A rogue Access Point (AP) is any device that adds an unauthorized (and therefore unmanaged and unsecured) WLAN to the organization's network. A rogue AP could be added by inserting a WLAN card into a back office server (C), attaching an unknown WLAN router to the network (F), or by various other means.

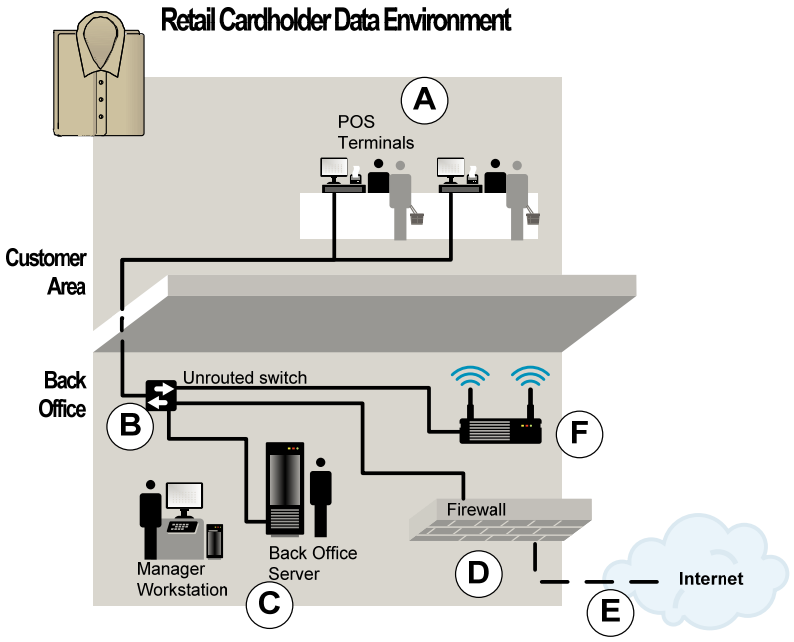

Figure 2: Rogue APs added to the CDE

2.1.2 Adding a known WLAN to the CDE

In the case where an organization has decided to deploy a WLAN for any purpose whatsoever, *and connect the WLAN to the CDE*, then that WLAN is now a part of the CDE and is therefore in scope within the PCI DSS and within the scope of this document.

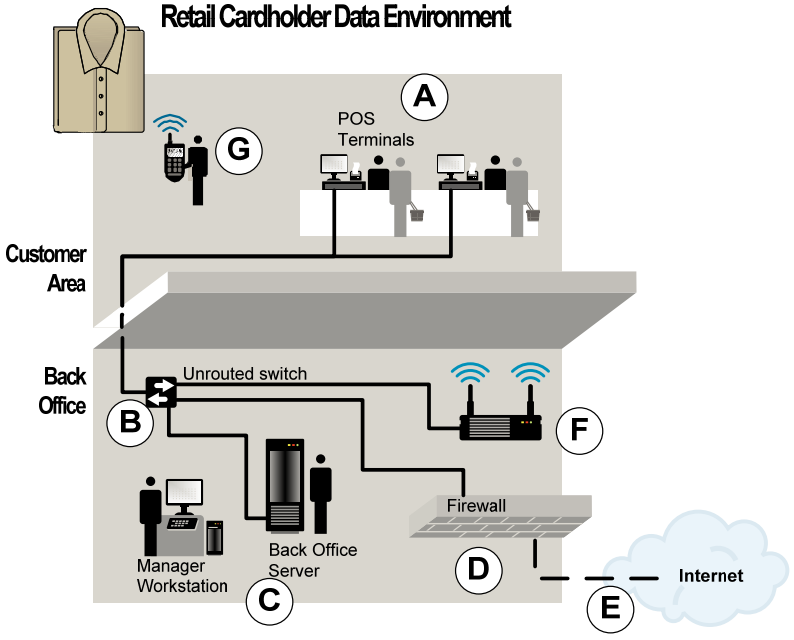

Figure 3: A CDE with an added WLAN

In this case, the WLAN Access Point (AP) is connected directly to the wired network within the CDE.

Even though the organization is only using WLAN technology for inventory control, and no cardholder data is being passed back and forth, the WLAN is nevertheless within the CDE by the fact that the network traffic is **not segmented** away.

2.1.3 Adding a known WLAN *outside* of the CDE

In the case where a WLAN is added *outside* of the CDE, so that *no traffic whatsoever* from the WLAN passes into the CDE, then that WLAN can be considered out of scope for the PCI DSS. However, if the WLAN is connected to the firewall on the CDE, or is connected to a network that is connected to the firewall on the CDE, then the **firewall's configuration** is in scope for both the PCI DSS and this document, even though the AP is outside of the scope of both PCI DSS and this document.

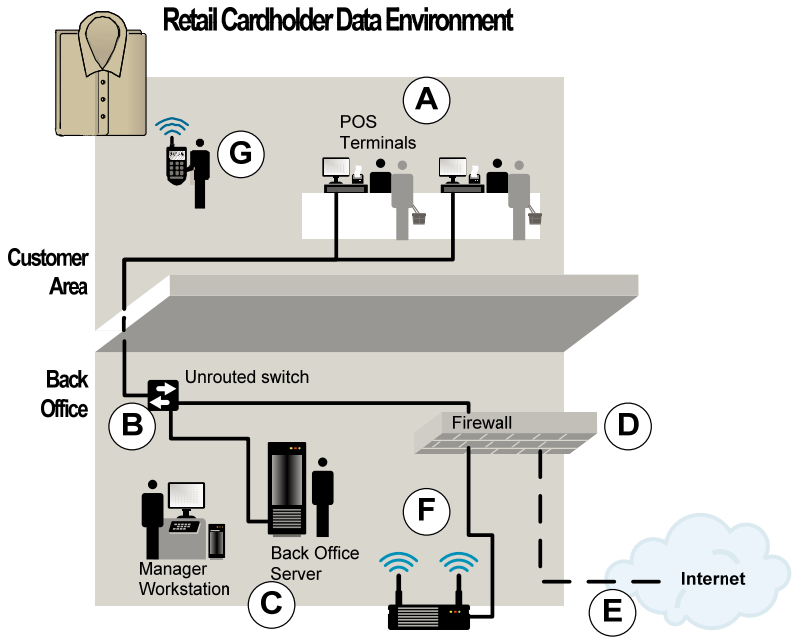

Figure 4: WLAN outside the CDE

2.2 How to use this guide

Figure 5 shows a step-by-step decision process for complying with PCI DSS wireless requirements. This guide will follow the path set forth in the flow chart, beginning with scanning the network for the potential existence of a WLAN and proceeding through the rest of the steps outlined in the chart.

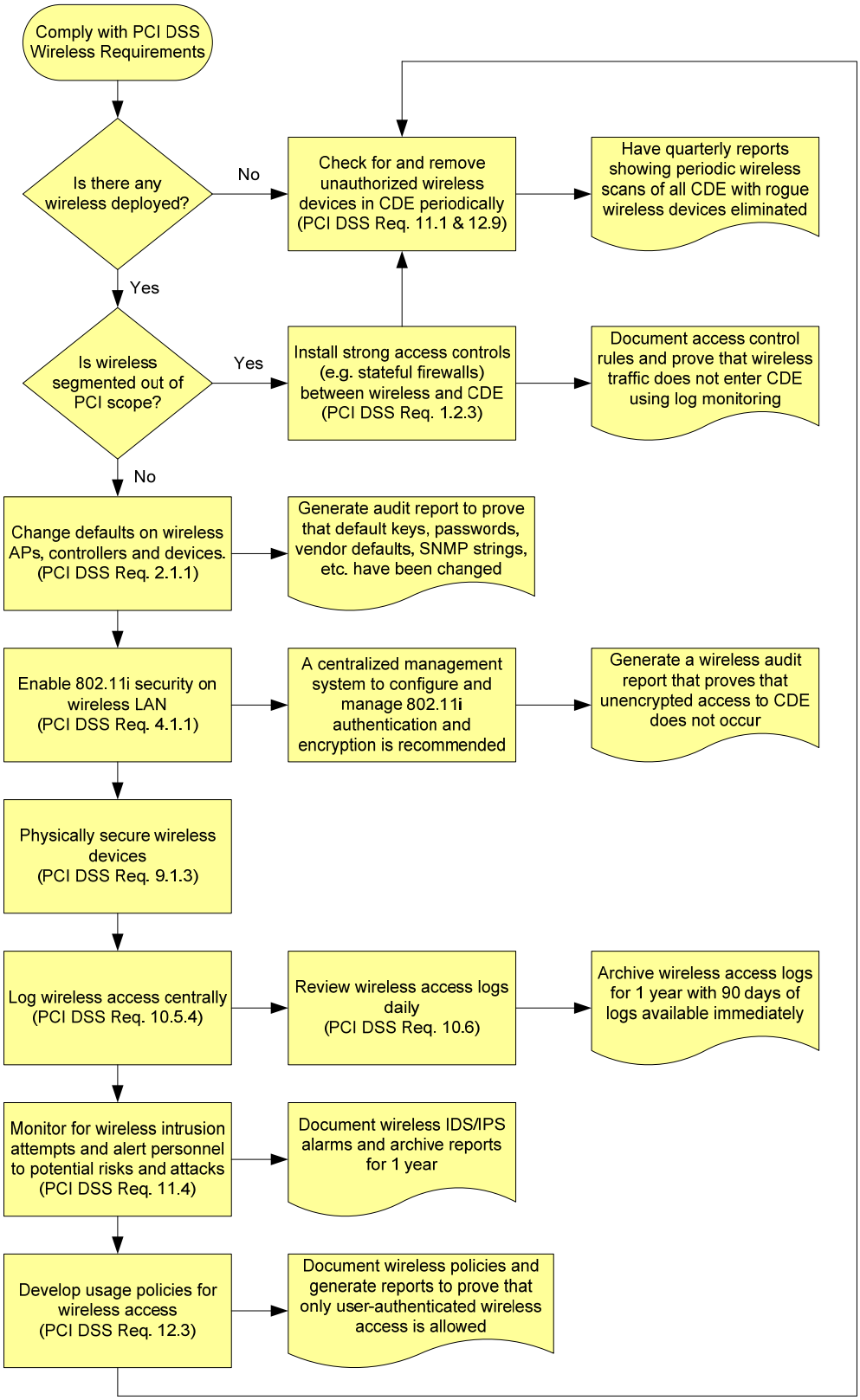

Figure 5: Complying with PCI DSS wireless requirements

3 Applicable Requirements Pertaining to Wireless for All Networks

Wireless networking is a concern for all organizations that store, process or transmit cardholder data and therefore must adhere to the PCI DSS. Even if an organization that must comply with PCI DSS does not use wireless networking as part of the Cardholder Data Environment (CDE), the organization must verify that its wireless networks have been segmented away from the CDE and that wireless networking has not been introduced into the CDE over time.

Although the PCI DSS outlines requirements for securing existing wireless technologies, there are validation requirements that extend beyond the known wireless devices and require monitoring of unknown and potentially dangerous rogue devices. A rogue wireless device is an unauthorized wireless device that can allow access to the CDE.

Wireless networks can be considered outside of PCI DSS scope if (i) no wireless is deployed or (ii) if wireless has been deployed and segmented away from the CDE. Regardless of whether wireless networks have been deployed, periodic monitoring is needed to keep unauthorized or rogue wireless devices from compromising the security of the CDE. Segmenting wireless networks out of PCI DSS scope requires a firewall between the wireless network and the CDE.

Note that risks in wireless networks are essentially equal to the sum of the risk of operating a wired network plus the new risks introduced by weaknesses in wireless protocols. Threats and vulnerabilities of wireless systems are discussed in multiple authority documents found in the list at the end of this document.

3.1 Maintain a hardware inventory

Answering the question “is a *known* WLAN deployed?” within the organization’s network depends upon the organization knowing the boundaries of the network and having an accurate networking inventory and hardware inventory. While there are no specific PCI DSS related authority documents that call for such an inventory, other authority documents that call for the management of a networking environment mandate such an inventory[i]. Others even go as far as to mandate a hardware inventory to ensure that rogue WLAN access cards are not added to existing computing devices[ii].

It is strongly recommended that the organization scan all CDE locations for known WLAN devices and maintain an up-to-date inventory. Without such an inventory, the organization would not know they existed and, therefore, any that were found would have to be initially treated as rogue devices. Therefore, while not specifically mandated by PCI DSS, related documents *imply* that such an inventory should exist while authority documents outside of the PCI DSS realm mandate it.

3.1.1 Summary of recommendations

Ensure that the organization maintains an up-to-date hardware inventory so that known APs can easily be distinguished from rogue APs.

3.2 Wireless scanning to look for rogue APs

The purpose of PCI DSS requirement 11.1 is to ensure that an unauthorized or rogue wireless device introduced into an organization's network does not allow unmanaged and unsecured WLAN access to the CDE. The intent is to prevent an attacker from using rogue wireless devices to negatively impact the security of cardholder data.

In order to combat rogue WLANs, it is acceptable to use a wireless analyzer or a preventative control such as a Wireless Intrusion Detection/Prevention System (IDS/IPS) as defined by the PCI DSS.

PCI DSS Requirement	Testing Procedure
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices. If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel. Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.

Table 1: PCI DSS § 11.1

Since a rogue device can potentially show up in any CDE location, it is important that *all locations* that store, process or transmit cardholder data are either scanned regularly or that wireless IDS/IPS is implemented in those locations.

An organization may not choose to select a sample of sites for compliance. Organizations must ensure that they scan **all** sites quarterly to comply with the standard. The organization's responsibility is to ensure that the CDE is compliant at all times.

With that said, during a PCI DSS assessment, the organization or its assessor may choose to validate compliance with requirement 11.1 by selecting a sample of all locations. The PCI Security Standards Council leaves sampling, for the purposes of validation, at the discretion of the assessor. As part of the validation, the assessor should check that the organization has the appropriate processes and technology in place to comply at all locations.

PCI DSS requirement 11.1 clearly specifies the use of a wireless analyzer or a wireless IDS/IPS system for scanning. Relying on wired side scanning tools (e.g. tools that scan suspicious hardware MAC addresses on switches) may identify some unauthorized wireless devices; however, they tend to have high false positive/negative detection rates. Wired network scanning tools that scan for wireless devices often miss cleverly hidden and disguised rogue wireless devices or devices that are connected to isolated network segments. Wired scanning also fails to detect many instances of rogue wireless clients. A rogue wireless client is any device that has a wireless interface that is not intended to be present in the environment.

Wireless analyzers can range from freely available PC tools to commercial scanners and analyzers. The goal of all of these devices is to "sniff" the airwaves and "listen" for wireless devices in the area and identify them. Using this method, a technician or auditor can walk around each site and detect wireless devices. The person would then manually investigate each device

to determine if it allows access to CDE and classify them as rogues or just friendly neighboring wireless devices. Although this method is technically possible for a small number of locations, it is often operationally tedious, error-prone, and costly for organizations that have several CDE locations. For large organizations, it is recommended that wireless scanning be automated with a wireless IDS/IPS system.

Although the PCI DSS standard does not directly state what the output of wireless analysis should be, it does imply that it should be created, reviewed, and used to mitigate the risk of unauthorized or rogue wireless devices. At a minimum, the list of wireless devices should clearly identify all rogue devices connected to the CDE. To comply with the intent of PCI DSS requirement 11.1, companies should immediately remediate the rogue threat in accordance with PCI DSS requirement 12.9 and rescan the environment at the earliest possible opportunity.

3.2.1 Summary of recommendations:

A. Use a wireless analyzer or a wireless IDS/IPS to detect unauthorized/rogue wireless devices that could be connected to the CDE at least quarterly at all locations. For large organizations having several CDE locations, a centrally managed wireless IDS/IPS to detect and contain unauthorized/rogue wireless devices is recommended.

B. Enable automatic alerts and containment mechanisms on the wireless IPS to eliminate rogues and unauthorized wireless connections into the CDE.

C. Create an “Incident Response Plan” to physically eliminate rogue devices immediately from the CDE in accordance with PCI DSS requirement 12.9.5.

3.3 Segmenting wireless networks

PCI DSS requires that wireless networks that do not store, process or transmit card holder data must be isolated from the CDE using a firewall as shown in Figure 6. The intent is to prevent unauthorized users from being able to access the CDE via a wireless network deployed for purposes other than credit card transactions.

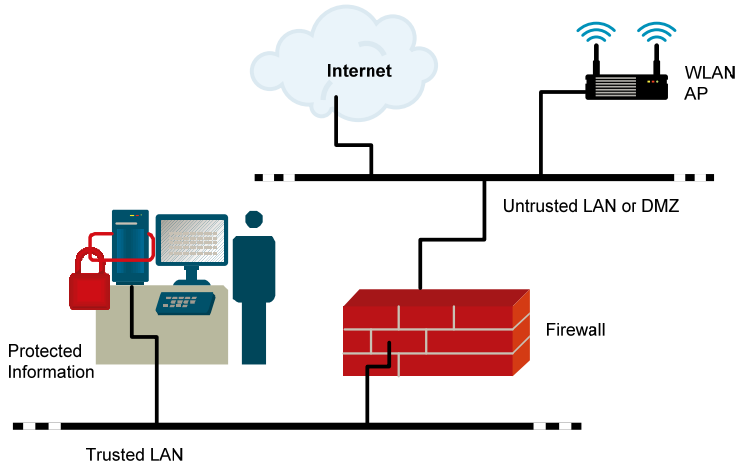

Figure 6: Illustration of AP outside of PCI DSS Scope

The wireless firewall should perform the following general functions:

A. Completely isolate wireless network traffic from entering the CDE by filtering wireless packets based on the 802.11 protocol.

B. Perform stateful inspection of connections.

C. Monitor and log traffic allowed and denied by the firewall in accordance with PCI DSS requirement 10.

PCI DSS Requirement	Testing Procedure
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Table 2: PCI DSS § 1.2.3

PCI DSS compliance requires that all firewall rules should be audited and reviewed at least every 6 months. If a firewall is being shared between wireless and other protocols/applications, the default policy for the firewall for handling inbound traffic should be to block all packets and connections into the CDE unless the traffic type and connections have been specifically permitted. This approach is more secure than another approach used often: permit all connections and traffic by default and then block specific traffic and connections. Wireless traffic should explicitly be blocked. Organizations should consider using outbound traffic filtering as a technique for further securing their networks and reducing the likelihood of internally based attacks.

Relying on Virtual LAN (VLAN) based segmentation alone is not sufficient. For example, having the CDE on one VLAN and the WLAN on a separate VLAN does not adequately segment the WLAN and take it out of PCI DSS scope. VLANs were designed for managing large LANs efficiently. As such, a hacker can hop across VLANs using several known techniques if adequate access controls between VLANs are not in place.

As a general rule, any protocol and traffic that is not necessary in the CDE, i.e., not used or needed for credit card transactions, should be blocked. This will result in reduced risk of attack and will create a CDE that has less traffic and is thus easier to monitor.

3.3.1 Summary of recommendations:

A. Use a stateful packet inspection firewall to block wireless traffic from entering the CDE. Augment the firewall with a wireless IDS/IPS.

B. Do not use VLAN based segmentation with MAC address filters for segmenting wireless networks.

C. Monitor firewall logs daily and verify firewall rules at least once every six months.

4 Applicable Requirements for In-Scope Wireless Networks

Wireless networks that are part of the CDE must comply with all PCI DSS requirements. This includes using a firewall (requirement 1.2.3) and making sure that additional rogue wireless devices have not been added to the CDE (requirement 11.1). In addition, PCI DSS compliance for systems that include WLANs as a part of the CDE requires extra attention to WLAN specific technologies and processes such as:

A. Physical security of wireless devices,

B. Changing default passwords and settings on wireless devices,

C. Logging of wireless access and intrusion prevention,

D. Strong wireless authentication and encryption,

E. Use of strong cryptography and security protocols, and

F. Development and enforcement of wireless usage policies.

This section will cover each of these requirements sequentially.

4.1 Physical security of wireless devices

PCI DSS promotes the need for physical security surrounding wireless devices. The focus of this requirement is on securing publicly accessible or risky devices. For example, one would not put a physical cage around every AP or chain down every handheld device, but one should secure those devices that are generally accessible to the public or at risk of being lost or compromised.

Obvious risks to physical security (other than theft) include the ability of an unauthorized person to reset the AP to factory defaults. The reset function poses a particular problem because it allows an individual to negate any security settings that administrators have configured in the AP. It does this by returning the AP to its default factory settings. The default settings generally do not require an administrative password, for example, and may disable encryption. An individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing. If a malicious user gains physical access to the device, that individual can exploit the reset feature and cancel out any security settings on the device. Additionally, reset can be invoked remotely over the management interface or by using a serial console interface on the AP. These require physical access and PCI DSS requires that adequate mechanisms need to be in place to prevent unauthorized physical access to wireless devices.

PCI DSS Requirement	Testing Procedure
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.	Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.

Table 3: PCI DSS § 9.1.3

Although the requirements do not state how to secure such devices, many ways exist to implement physical security.

Options for securing wireless devices may include physically restricting access (e.g. by mounting APs high up on the ceiling) and disabling the console interface and factory reset options by using a tamper-proof chassis. Instead of reverting to factory defaults, physically resetting an AP should result in centrally managed configurations being re-applied. Similarly, many enterprise APs are equipped with special mounting brackets that prevent ready access to the Ethernet cable.

Securing handheld wireless devices and laptops is more difficult since physical access to these devices is needed. Common sense precautions like not having Pre Shared Keys (PSKs) and passwords printed on the device or stored insecurely on the device are recommended. Inventory management of wireless devices and being able to track and report missing devices is recommended.

4.1.1 Summary of recommendations:

A. Mount APs on ceilings and walls that do not allow easy physical access.

B. Use APs with chassis and mounting options that prevent physical access to ports and reset features. APs housed in tamper-proof chassis are recommended.

C. Secure handheld devices with strong passwords and always encrypt PSKs if cached locally.

D. Use a wireless monitoring system that can track and locate all wireless devices and report if one or more devices are missing.

4.2 Changing the default settings of the APs

Changing default administrative passwords, encryption settings, reset function, automatic network connection functions, factory default shared keys and Simple Network Management Protocol (SNMP) access will help eliminate many of the vulnerabilities that can impact the security of the CDE through unauthorized wireless access.

PCI DSS Requirement	Testing Procedure
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES): Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions Default SNMP community strings on wireless devices were changed Default passwords/passphrases on access points were changed Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example WPA/WPA2) Other security-related wireless vendor defaults, if applicable

Table 4: PCI DSS § 2.1.1

Each WLAN AP device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example. For example, on some APs, the factory default configuration does not require a password (i.e., the password field is blank). Other APs might have simple and well-documented passwords (e.g. “password” or

"admin"). Unauthorized users can easily gain access to the device's management console if default settings are left unchanged. Similarly, many wireless APs have a factory default setting that allows unencrypted wireless access. Some APs might be pre-configured for WEP access with simple keys like "111111".

Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. The first two versions of SNMP, SNMPv1 and SMPv2, support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure. SNMPv3, which includes mechanisms to provide strong security, is highly recommended. If SNMP is not required on the network, the organization should simply disable SNMP altogether. It is common knowledge that the default SNMP community string that SNMP agents commonly use is the word "public" with assigned "read" or "read and write" privileges. Leaving this well-known default string unchanged leads to devices becoming vulnerable to attack. If an unauthorized user were to gain access and had read/write privileges, that user could write data to the AP, resulting in a data integrity breach. Organizations that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user/system requires.

All Wi-Fi APs have a Service Set ID (SSID). The SSID is an identifier that is sometimes referred to as the "network name" and is often a simple ASCII character string. The SSID is used to assign an identifier to the wireless network (service set). Clients that wish to join a network scan an area for available networks and join by providing the correct SSID. Disabling the broadcast SSID feature in the APs causes the AP to ignore the message from the client and forces it to perform active scanning (probing with a specific SSID). The default values of SSID used by many 802.11 wireless LAN vendors have been published and are well-known to would-be adversaries. The default values should be changed (always a good security practice) to prevent easy access. Suppressing the SSID is not necessarily a security mechanism as a hacker can sniff the SSID using fairly trivial techniques. However, broadcasting an SSID that advertises the organization's name or is easily identifiable with the organization is not recommended.

In addition, when configuring the WLAN AP, ensure that the device's monitoring and logging capabilities are synchronized for proper traceability. This is done through synchronizing the AP's clock with the clocks of the other firewalls, routers, and servers. Without the clocks being synchronized, it is not possible to discern which logging events on the AP match logged events in other devices.

Disable all unnecessary hardware, services, and applications that the AP might have shipped with. Check for the following protocols to ensure that they aren't configured unless absolutely necessary:

A. Dynamic Host Configuration Protocol (for assigning IP addresses on the fly).

B. HTTP SSL (for protected web pages), and

C. Wireless zero configuration service (for those APs and devices connecting to them) that run on Windows OS.

4.2.1 Summary of recommendations:

A. Enable WPA or WPA2 and make sure that default PSKs are changed. Enterprise mode is recommended.

B. Disable SNMP access to remote APs if possible. If not, change default SNMP passwords and use SNMPv3 with authentication and privacy enabled.

C. Do not advertise organization names in the SSID broadcast.

D. Synchronize the APs' clocks to be the same as other networking equipment used by the organization.

E. Disable all unnecessary applications, ports, and protocols.

4.3 Wireless intrusion prevention and access logging

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. An Intrusion Detection System (IDS) is software that automates the intrusion detection process. An Intrusion Prevention System (IPS) is a system that has all the capabilities of an IDS and can also attempt to stop possible incidents.

PCI DSS Requirement	Testing Procedure
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	Verify the use of intrusion-detection systems and/or intrusion-prevention systems and ensure that all traffic in the cardholder data environment is monitored. Confirm IDS and/or IPS are configured to alert personnel of suspected compromises. Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

Table 5: PCI DSS § 11.4

Wireless IDS/IPS provides several types of security capabilities intended to detect misconfiguration, misuse, and malicious activity. These capabilities can be grouped into three categories: (i) rogue wireless device containment, (ii) detection of unsafe activity or configurations, (iii) detection of denial of service attacks, and wireless intrusion attempts.

Unauthorized wireless devices connected to the CDE must be detected and disabled. A wireless IPS should be able to find these rogue devices even when they are configured to not broadcast information about themselves or present in isolated network segments. In addition to rogue containment, organizations should evaluate the automatic device classification capabilities of the wireless IDS/IPS for situations when connectivity cannot be determined. A wireless IDS/IPS

should be able to observe all APs and clients, on all operational channels, and classify each device as authorized, unauthorized/rogue or neighboring. Many wireless IPS systems provide the ability to prevent clients from associating with an unauthorized AP or disable an ad hoc network; efficacy of these techniques vary widely and can provide adequate temporary mitigation of the risk. However, unauthorized devices should be physically and/or logically removed from the CDE as soon as possible.

A wireless IDS/IPS can detect misconfigurations and unsafe activity by monitoring and analyzing wireless communications. Most can identify APs and clients that are not using the proper security controls. This includes detecting misconfigurations and the use of weak WLAN protocols. This is accomplished by identifying deviations from organization-specific policies for configuration settings such as encryption, authentication, data rates, SSID names, and channels. For example, they could detect that a wireless device is using WEP instead of WPA2. Some wireless IDS/IPS use anomaly and/or behavior based detection methods to detect unusual WLAN usage patterns. For example, if there is a higher than usual amount of network traffic between a wireless client and an AP, one of the devices might have been compromised, or unauthorized parties might be using the WLAN. Some systems can also alert if any WLAN activity is detected during off-hours periods.

A wireless IDS/IPS can analyze wireless traffic to look for malicious activity such as Denial of Service (DoS) and individual attacks on devices. This task, as in wired IDS/IPS, requires the system to look for attempts to disrupt the wireless network, a device on the network, or to gain unauthorized access to the network. If these detections are signature-based, then organizations should ensure the signatures are updated when new threats are discovered.

Most wireless IDS/IPSs can identify the physical location of a detected threat by using signal strength triangulation. Triangulation is the process of estimating the threat's approximate distance from multiple sensors by the strength of the threat's signal received by each sensor, then calculating the physical location at which the threat would be located to satisfy the distance criteria from each sensor. This allows an organization to send physical security staff to the location to address the threat.

An IDS/IPS system can generate a lot of wireless threat information. In order for the organization to be able to use this information, the information has to be properly logged. This implies that the logs from the IDS/IPS have to be coordinated with other logging systems on the network (if there are any). In this case, the organization must ensure that at least the following logging items are coordinated correctly:

A. The log file prefix (used to identify the device conducting the logging).

B. The level of logging (the types of events to log).

C. The log auto-roll setting (whether a new log file is created when the device is restarted, or the maximum log size is reached).

D. The log maximum (log age in days).

After gathering the information within the IDS/IPS, the organization must **read and respond to the IDS/IPS reports**. If there are anomalies, they must be resolved. It is *not* enough to merely purchase and properly configure the IDS/IPS. This is a device doing the legwork of watching out for potential problems. However, what it *can't do* is stop a potential cardholder data breach without personnel interaction. The organization's policies and procedures must take into account the reading and taking action on the logs provided by this and other key monitoring devices.

4.3.1 Summary of recommendations:

A. Use a centrally controlled wireless IDS/IPS to monitor for unauthorized access and detect rogues and misconfigured wireless devices.

B. Enable historical logging of wireless access that can provide granular wireless device information and store event logs and statistics for at least 90 days.

C. Enable IPS features that automatically disable rogue wireless devices connecting to the CDE as well as accidental or malicious associations of wireless clients.

D. Ensure the IPS signature set is regularly updated as new threats are discovered.

E. Coordinate logging events with other networking devices within the organization.

F. Add processes and policies that will regularly read and act on the data provided by the IDS/IPS.

G. Maintain a current topology of all physical locations of access points.

4.4 Strong wireless authentication and encryption

By 2001, a series of independent studies from various academic and commercial institutions had identified weaknesses in Wired Equivalent Privacy (WEP), the original native security mechanism for wireless local area networks (WLANs), in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification. To learn more about this, you can refer to **Understanding WEP Weaknesses** [20]. These studies showed that, even with WEP enabled, an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to the wireless network via the WLAN.

In 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) as a strong, standards-based interoperable Wi-Fi security specification. WPA provides assurance that their data will remain protected and that only authorized users may access their networks. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption that changes keys used for encryption on a per packet basis.

In 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), the second generation of WPA security. Like WPA, WPA2 provides Wi-Fi users with a high level of assurance that their

data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance.

PCI DSS v1.2 requires discontinuing WEP as of June 30, 2010 and moving to robust encryption and authentication such as the IEEE 802.11i standard. The Wi-Fi Alliance certifies products as WPA or WPA2 compatible for interoperability based on the 802.11i standard.

PCI DSS Requirement	Testing Procedure
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. • For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. • For current wireless implementations, it is prohibited to use WEP after June 30, 2010.	4.1.1 For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.

Table 6: PCI DSS § 4.1.1

There are two modes in WPA and WPA2 - Enterprise and Personal. Both provide an authentication and encryption solution.

Mode	WPA	WPA2
Enterprise	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Table 7: The two modes in WPA

Personal mode is designed for home and Small Office Home Office (SOHO) users who do not have authentication servers available. It operates in an unmanaged mode that uses a Pre-Shared key (PSK) for authentication instead of IEEE 802.1X. This mode uses applied authentication in which a pass-phrase (the PSK) is manually entered on the access point to generate the encryption key. Consequently, it does not scale well in the enterprise. The PSK is typically shared among users. Weak passphrases are vulnerable to password cracking attacks. To protect against a brute force attack, a truly random passphrase of 13 or more characters (selected from the set of 95 permitted characters) is probably sufficient.

Enterprise mode operates in a managed mode to meet the rigorous requirements of enterprise security. It leverages the IEEE 802.1X authentication framework, which uses an Extensible Authentication Protocol (EAP) type, with an authentication server to provide strong mutual authentication between the client and authentication server. In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. TKIP employs an encryption cipher that issues encryption keys for each data packet communicated in each session of each user, making the encryption code

extremely difficult to break. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.

Recent attacks against the TKIP encryption algorithm have revealed some flaws in the protocol that can allow an attacker to decrypt small frames encrypted using TKIP such as Address Resolution Protocol (ARP) frames in about 15 minutes. Further, the attack revealed that it is possible to reuse the compromised encryption keystream to inject 7-15 arbitrary packets into the network using QoS mechanisms without triggering the replay protection countermeasures available in TKIP. While the attack does not lead to a compromise of the PSK, it is recommended that organizations use AES encryption, which is immune to the attack.

The Wi-Fi Alliance has announced the inclusion of additional EAP types to its certification programs for WPA and WPA2 Enterprise certification programs. This was to ensure that WPA-Enterprise certified products can interoperate with one another. Previously, only EAP-TLS (Transport Layer Security) was certified by the Wi-Fi alliance. The following table illustrates the popular EAP types certified by Wi-Fi along with a comparison of features.

WPA Enterprise Mode	PEAP	EAP-TLS	EAP-TTLS
User Authentication Database and Server	OTP, LDAP, NDS, NT Domains, Active Directory	LDAP, NT Domains, Active Directory	OTP, LDAP, NDS, NT Domains, Active Director
Native Operating System Support	Windows XP, 2000	Windows XP, 2000	Windows XP, 2000, ME, 98, WinCE, Pocket PC2000, Mobile 2003
User Authentication Method	Password or OTP	Digital Certificate	Password or OTP4
Authentication Transaction Overhead	Moderate	Substantial	Moderate
Management Deployment Complexity	Moderate Digital Certificate For Server	Substantial Digital Certificate Per Client and For Server	Moderate Digital Certificate For Server
Single Sign On	Yes	Yes	Yes

Table 8: WPA Enterprise mode security

ANS X9.112 [19] defines similar data confidentiality, entity authentication and data integrity requirements with an additional requirement for *security encapsulation*. Security encapsulation is the independent protection of specific data elements within another security protocol, such as separate PIN encryption at the point of entry within the WPA protocol.

4.4.1 Summary of recommendations:

A. WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is recommended for WLAN networks.

B. It is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.

C. Pre-Shared Keys should be changed on a regular basis.

D. Centralized management systems that can control and configure distributed wireless networks are recommended.

E. The use of WEP in the CDE is prohibited for all deployments after June 30, 2010.

4.5 Use of strong cryptography on transmission of cardholder data over wireless

In addition to encrypting and authenticating wireless LANs using WPA2, when using wireless as a transport medium in a CDE, it is a security best practice to treat the wireless network as part of a DMZ or a public network. This means all CDE data must be encrypted as suggested in PCI DSS Requirement 4.1. Section 4.4 described Layer 2 specific wireless encryption protocols such as AES that is used within WPA2 to provide confidentiality and integrity at the wireless link layer. Higher layer encryption methods such as SSL/TLS and IPSEC and could be used to provide end-to-end cryptographic protection of card-holder data.

PCI DSS Requirement	Testing Procedure
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* • *The Internet,* • *Wireless technologies,* • *Global System for Mobile communications (GSM), and* • *General Packet*	**4.1.a** Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks • Verify that strong encryption is used during data transmission • For SSL implementations: - Verify that the server supports the latest patched versions. - Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). - Verify that no cardholder data is required when HTTPS does not appear in the URL. • Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. • Verify that only trusted SSL/TLS keys/certificates are accepted. • Verify that the proper encryption strength is implemented for the encryption methodology in use.

Table 9: PCI DSS § 4.1

Figure 7 illustrates an example where wireless technology and "on line" credit card purchases intersect at a "wireless hot spot". Locations such as airports, cafés, etc., will provide an open wireless service which, when connected to, present users with a HTTPS/SSL web page that allows them to purchase access to the internet. This process is analogous to purchasing merchandise on the Internet.

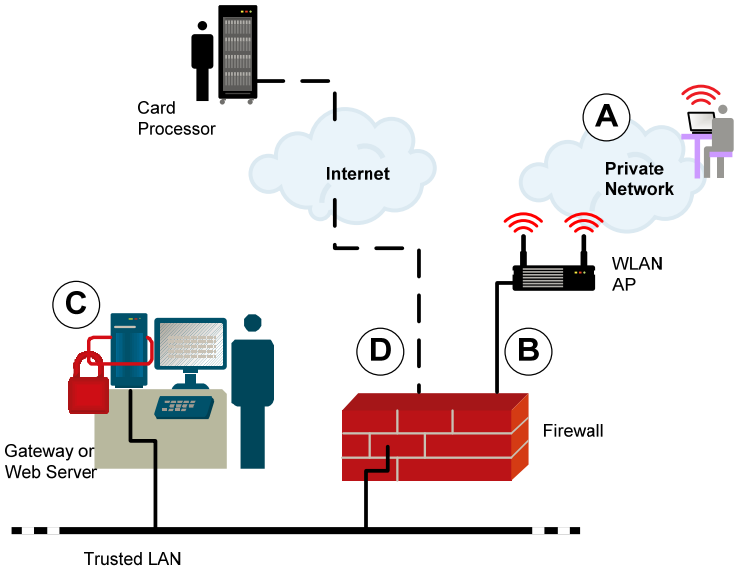

Figure 7: Wireless "Hotspot" example with SSLv3 HTTPS portal

A. The hot spot guest connects through the access point over a private WLAN connected to the firewall's external LAN port using SSLv3/TLS.

B. The firewall's LAN port must be configured for NAT as well as "Deny All", with only those exceptions that *must* be in place for the transaction to occur.

C. The gateway or web server that processes the transaction must do so using a secure connection using strong cryptography such as SSL or IPSEC.

D. The Internet port of the firewall must *also* be configured for NAT as well as "Deny All", with only those exceptions that *must* be in place for the transaction to occur. The dashed line signifies that the information flowing out through the Internet must be encrypted.

An example of a multi-service wireless network with both public and PoS services is shown in Figure 8. The "Guest Traffic" could be open or SSL as in the "Hot Spot" example. A recommended encryption for the Secure Application traffic would be IPSEC or WPA2-AES. In this example, the wireless network is treated as an "untrusted" network and is segmented using a firewall.

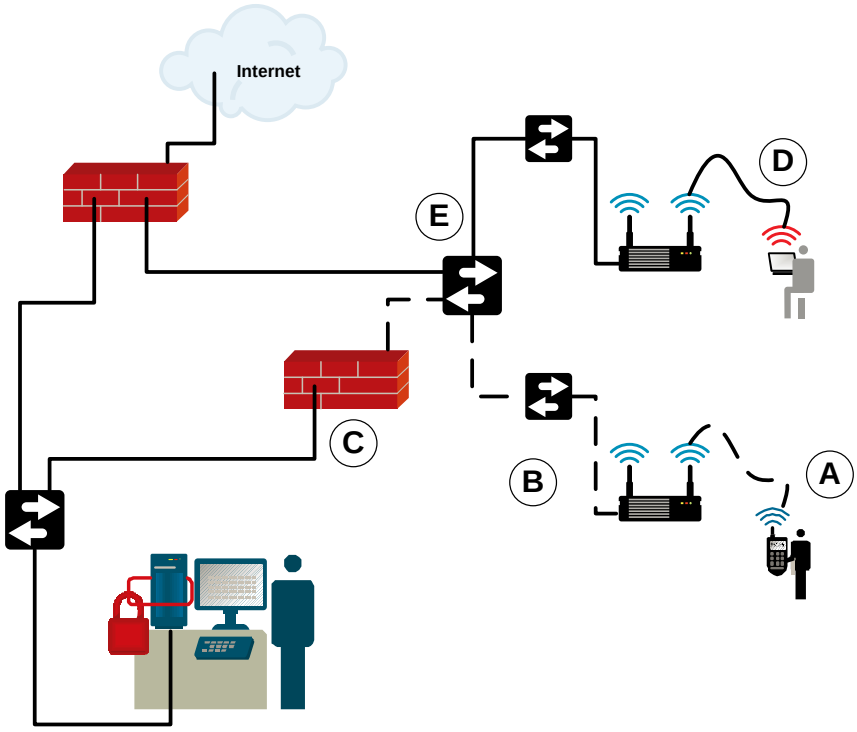

Figure 8: Secure Application Traffic using WPA2-AES/802.1X between client device and AP or Access Device

A. Secure wireless devices connect to the private WLAN through the APs. The dashed line signifies that the information flowing out through this segment must be encrypted.

B. Secure application traffic tunnels are created through the IDF switches to an internal firewall. The dashed line signifies that the information flowing out through this segment must be encrypted.

C. The firewall is the termination point for encrypted traffic. The firewall's connection rules also guarantee that traffic flowing between the secure application and the secure wireless device traverse no other path than this one.

D. Guest traffic attaches through private WLAN APs.

E. Guest traffic is separated from the secure application traffic tunnels through VLANs.

SSLv3 is recommended as it supports a range of Cipher Suites which define the key establishment algorithm, the encryption cipher, the hash function and their parameters. Historically, SSLv2 supported older encryption ciphers (e.g., RC2 and DES) and cryptographic key lengths (e.g., 512-bit RSA and 512-bit DH) that are inappropriate for today's networks. Refer to Table 9 for relative cryptographic strengths, which is based on NIST SP 800-57 [21].

IPSEC supports several Security Associations which define the cryptographic algorithms for the IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP). Historically IPSEC supports older algorithms (e.g., DES) with cryptographic strengths (e.g., 56-bit DES) that

are inappropriate for today's networks. Refer to Table 10 for relative cryptographic strengths, which is based on NIST SP 800-57 [21].

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	ECC Algorithms	RSA/DSA/DH Algorithms
56-bits	DES	-	-	-
80-bits	3DES-2K	SHA-1 (160)	160-bits	1024-bits
112-bits	3DES-3K	SHA-2 (224)	224-bits	2048-bits
128-bits	AES-128	SHA-2 (256)	256-bits	3072-bits
192-bits	AES-192	SHA-2 (384)	384-bits	7680-bits
256-bits	AES-256	SHA-2 (512)	512-bits	15360-bits

Table 10: Relative Cryptographic Strengths

4.5.1 Summary of recommendations:

A. SSLv3 is mandatory for traffic that carries cardholder data.

B. When possible, 256-bit encryption is preferred.

4.6 Development and enforcement of wireless usage policies

The PCI DSS mandates the need for acceptable usage policies and procedures, which include those for wireless devices. The importance here is that organizations understand how wireless is to be used within their environment, how it is to be secured and deployed and how the organization will address incidents as they occur. Another important aspect the policy should address is how employees can and should use their authorized wireless devices. For example, if employees receive laptops, they need to understand the acceptable usage and responsibilities of wireless networking. If an employee receives a wireless inventory device, he or she needs to understand how to properly protect, access, and store that device.

PCI DSS Requirement	Testing Procedure
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors.	12.3 Obtain and examine the policy for critical employee-facing technologies.

Table 11: PCI DSS § 12.3

4.6.1 Summary of recommendations:

A. Verify that the usage policies require explicit management approval to use wireless networks in the CDE. Any unsanctioned wireless must be removed from CDE.

B. Verify that the usage policies require that wireless access is authenticated with user ID and password or other authentication item (for example, token). WPA Enterprise supports this requirement. If PSKs are used, then they must be rotated whenever employees that have access to wireless devices leave the organization. In Enterprise mode, individual user access can be enabled/disabled centrally.

C. Verify that the usage policies require a list of all wireless devices and personnel authorized to use the devices.

D. Verify that the usage policies require labeling of wireless devices with owner, contact information and purpose.

E. Verify that the usage policies require acceptable uses for the wireless technology. For example, if wireless devices are being used to transmit card holder data, then the same networks should not be used for guest access.

F. Verify that the usage policies require a list of company-approved products. For example, if a wireless AP needs to be replaced, substituting it with a non-sanctioned AP is not acceptable.

G. Verify that the usage policies require automatic disconnect of sessions for wireless access after a specific period of inactivity. For example, a wireless POS terminal should automatically log out and disconnect from the CDE if left unattended.

H. Verify that the usage policies require activation of wireless-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.

I. Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via wireless-access technologies. For example, if a wireless POS is being used, card holder data should not be stored locally on the device; it should only be encrypted and transmitted.

5 Authority Documents and External References

The following table shows the documents upon which this document draws its source of authority.

Document	Location
PCI DSS v1.2	https://www.pcisecuritystandards.org/
PCI Security Scanning Procedures	http://selfservice.talisma.com/display/2/index.aspx?c=58&cpc=MSdA03B2IfY15uvLEKtr40R5a5pV2lnCUb4i1Qj2q2g&cid=81&cat=&catURL=&r=0.686736822128296
MasterCard International Wireless LANs – Security Risks and Guidelines	http://www.mastercard.com/us/sdp/assets/pdf/wl_entire_manual.pdf
Wireless Security Checklist Version 5, Release 2.2	http://iase.disa.mil/stigs/checklist/wireless-checklist_v5r2-2_final_20080326.pdf
MasterCard International Electronic Commerce Security Architecture Best Practices	http://www.powerpay.biz/docs/risk/MC_best_practices_online.pdf
The Center for Internet Security Wireless Networking Benchmark	http://www.cisecurity.org/tools2/wireless/CIS_Wireless_Benchmark_v1.0.pdf
NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth and Handheld Devices	http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std. 802.11S	http://standards.ieee.org/getieee802/download/802.11-2007.pdf
WPA Overview, WiFi Alliance	http://www.wifi.org/OpenSection/pdf/WiFi_Protected_Access_Overview.pdf
”Security risks and ways to decrease vulnerabilities in a 802.11b wireless environment”	http://www.attackprevention.com/ap/library/wirelessseccRJ.htm
“Ultimate wireless security guide: An introduction to LEAP authentication”	http://articles.techrepublic.com.com/5100-10878_11-6148551.html
“Battered, but not broken: understanding the WPA crack,” Glenn Fleishman, Nov, 2008	http://arstechnica.com/articles/paedia/wpa-cracked.ars
Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise	http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf
Church of Wifi WPA-PSK Rainbow Tables	http://www.renderlab.net/projects/WPA-tables/
Guidelines on Firewalls and Firewall Policy	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
Guide to Intrusion Detection and Prevention Systems (IDPS)	http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
ANS X9.112 Wireless Management and Security for the Financial Services Industry	http://www.x9.org

Document	Location
Understanding WEP Weaknesses: *Hacking Wireless Networks for Dummies*, by Kevin Beaver, Peter T. Davis, Devin K. Akin, ISBN: 978-0-7645-9730-5	http://www.dummies.com/WileyCDA/DummiesArticle/Understanding-WEP-Weaknesses.id-3262,subcat-NETWORKING.html
NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General	http://csrc.nist.gov/publications/PubsSPs.html

6 Glossary of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
CCMP	Counter Mode CBC MAC Protocol
CDE	Cardholder Data Environment
DSS	Data Security Standard
EAP	Extensible Authentication Protocol
GPRS	General packet radio service
GSM	Global System for Mobile
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IDF	Intermediary Distribution Frame
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control

Acronym	Definition
MIC	Message Integrity Code
NDS	Netware Directory Services
OTP	One Time Password
PCI	Payment Card Industry
PDA	Personal Data (Digital) Assistant
PoS	Point of Sale
PSK	Pre-Shared Key
QoS	Quality of Service
SIG	Special Interest Group
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SSID	Service Set Identifier
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
URL	Universal Record Locator
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected ACCESS

7 PCI DSS v1.2 Cross Reference

The following table provides a cross reference between PCI DSS v1.2 and the contents of this guideline. The PCI DSS requirements below overtly refer to wireless (underlined in blue). The third column in the table references the section within this guide that addresses the corresponding requirement.

PCI DSS Requirements	Testing Procedures	Doc Section
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.	-
	1.1.2.b Verify that the diagram is kept current.	-
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	§3.1
2.1 Always change vendor-supplied defaults **before** installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor supplied accounts/passwords.)	-
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	**2.1.1** Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES): ▪ Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions ▪ Default SNMP community strings on wireless devices were changed ▪ Default passwords/passphrases on access points were changed ▪ Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2) ▪ Other security-related wireless vendor defaults, if applicable	§4.3

PCI DSS Requirements	Testing Procedures	Doc Section
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* ▪ *The Internet,* ▪ *Wireless technologies,* ▪ *Global system for mobile communications (GSM), and* ▪ *General packet radio service (GPRS).*	**4.1.a** Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks ▪ Verify that strong encryption is used during data transmission ▪ For SSL implementations: - Verify that the server supports the latest patched versions. - Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). - Verify that no cardholder data is required when HTTPS does not appear in the URL. ▪ Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. ▪ Verify that only trusted SSL/TLS keys/certificates are accepted. ▪ Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)	§4.2
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (e.g., IEEE 802.11i) are used to implement strong encryption for authentication and transmission.	§4.1
9.1.3 Restrict physical access to wireless access points, gateways and handheld devices.	**9.1.3** Verify that physical access to wireless access points, gateways and handheld devices is appropriately restricted.	§4.4
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.	-

PCI DSS Requirements	Testing Procedures	Doc Section
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	**11.1.a** Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.	§3.2
	11.1.b If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.	§3.2
	11.1.c Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.	§3.2
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	**12.3** Obtain and examine the policy for critical employee-facing technologies and perform the following: 12.1 Explicit management approval 12.2 Authentication method 12.3 Inventory of devices and authorized users 12.4 Device labeling 12.5 Acceptable use policy (AUP) 12.6 Acceptable network locations 12.7 Approved products 12.8 Session management (inactivity limits) 12.9 Remote access for vendors 12.10 Protect cardholder data	§4.6
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify, through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	
12.9.5 Include alerts from intrusion detection, intrusion-prevention, and file-integrity monitoring systems.	**12.9.5** Verify, through observation and review of processes, that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.	

8 Acknowledgments

The PCI Security Standards Council recognizes the following individuals for their contributions to the Wireless Special Interest Group and thanks them for producing this valuable resource.

Group lead, and Board of Advisors representative:

Doug Manchester, VeriFone

Special Interest Group Members:

Amit Sinha, Air Defense
Chris Hinsz, Motorola
Daniela Christoffel, Deutsch Card Services
Dave Whitelegg, Capita
Deborah Offink, Sprint
Deven Bhatt, ARC
Dorian Cougias, Unified Compliance Framework
Ed Martin, Chico's
Gary Zempich, Hypercom
Jeff Stapleton, Information Assurance Consortium
Jeremy Bennett, Aruba Networks
Kris Strittmater, Apriva
Larry Hitchew, Citigroup
Marcelo Halpern, Latham & Watkins LLP
Marek Kosinski, Shell
Matt FitzGerald, Hewlett-Packard
Maurice Lee, Tesco
Pabo Lopez-Tello, PayPal
Paul Lazarr, CollegeBoard
Rich Shetina, McDonald's
Rick Moy, NSS Labs
Ryan Townsend, TimeInc.
Scott Hutchinson, Spacenet
Steve Bernard, CollegeBoard
Terri Quinn, Cisco
Tim Cormier, Ingenico
Vikram Phatak, NSS Labs

[i] Australian Government ICT Security Manual (ACSI 33) § 3.8.31, 3.8.33; Gramm-Leach-Bliley Act (GLB) 16 CFR § 314.4(b)(2); FFIEC IT Examination Handbook – Business Continuity Planning Pg E-3, Pg G-7; FFIEC IT Examination Handbook – Operations Pg 9, Exam Tier II Obj A.1; The Standard of Good Practice for Information Security CB4.2.2, CB4.3.2, CI2.5.1, NW1.4.1, NW1.4.2(b), NW2.3.3, SM6.5.5; ISO 17799:2000, Code of Practice for Information Security Management § 5.1.1; Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST SP 800-14 § 3.3.1; Recommended Security Controls for Federal Information Systems, NIST SP 800-53 CM-8; Guide for Assessing the Security Controls in Federal Information Systems, NIST 800-53A § CM-2, CM-2.10; IT Service Management Standard - Code of Practice, BS 15000-2 § 5.6.1a

[ii] Gramm-Leach-Bliley Act (GLB) 16 CFR § 314.4(b)(2); FFIEC IT Examination Handbook – Development and Acquisition Pg 32, Exam Obj 11.1; FFIEC IT Examination Handbook – Business Continuity Planning Pg G-7; FFIEC IT Examination Handbook – Operations Pg 7, Pg 8, Exam Tier II Obj A.1; FFIEC IT Examination Handbook – E-Banking Pg 28; The Standard of Good Practice for Information Security SM4.3.6, SM4.3.7, CB4.2.2, CI1.3.2, CI1.3.3, CI1.3.4, CI2.5.1, NW5.1.3; ISO 17799:2000, Code of Practice for Information Security Management § 5.1.1; Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST SP 800-14 § 3.3.1; Recommended Security Controls for Federal Information Systems, NIST SP 800-53 CM-8; Guide for Assessing the Security Controls in Federal Information Systems, NIST 800-53A § CM-2, CM-2.10; IT Service Management Standard - Code of Practice, BS 15000-2 § 5.6.1a

Check local laws as applicable.