



The PCI Data Security Standard

September, 2007

370 North Westlake Blvd, Suite 200
Westlake Village, CA 91362

805.497.0955
805.462.3980 fax
www.xirrus.com

Introduction

The Payment Card Industry (PCI) Data Security Standard was developed by major credit card companies to help those that process credit card transactions (or cardholder information) in order to secure cardholder information and protect it from unauthorized access, fraud and other security issues. The major contributors to the standard are VISA, MasterCard, American Express, JCB, and Discover. The standard also helps consolidate various individual standards that were developed by each of the listed card companies. Merchants or others who process credit card transactions are required to comply with the standard and are required to prove their compliance by way of an audit from a Qualified Security Assessor

Payment Card Industry (PCI) Data Security Standard (DSS) Requirements Overview

As of the current version of the standard (ver1.1, September 2006), the PCI Data Security Standard (PCI DSS) has 12 main requirements that are grouped into six “control objectives” the following section lists each control objective and the specific requirements for each objective.

Objective: Build and Maintain a Secure Network
<u>Requirement 1:</u> Install and maintain a firewall configuration to protect cardholder data
<u>Requirement 2:</u> Do not use vendor-supplied defaults for system passwords and other security parameters
Objective: Protect Cardholder Data
<u>Requirement 3:</u> Protect stored cardholder data
<u>Requirement 4:</u> Encrypt transmission of cardholder data across open, public networks
Objective: Maintain a Vulnerability Management Program
<u>Requirement 5:</u> Use and regularly update anti-virus software

<u>Requirement 6:</u> Develop and maintain secure systems and applications
Objective: Implement Strong Access Control Measures
<u>Requirement 7:</u> Restrict access to cardholder data by business need-to-know
<u>Requirement 8:</u> Assign a unique ID to each person with computer access
<u>Requirement 9:</u> Restrict physical access to cardholder data
Objective: Regularly Monitor and Test Networks
<u>Requirement 10:</u> Track and monitor all access to network resources and cardholder data
<u>Requirement 11:</u> Regularly test security systems and processes
Objective: Maintain an Information Security Policy
<u>Requirement 12:</u> Maintain a policy that addresses information security

PCI DSS and Wireless Networking Specific Requirements

The previous section indicated the overall requirements a network must adhere to in order to be compliant with the PCI Data Security Standard. This below information highlights the detailed PCI DSS requirements as they apply specifically to wireless networking.

Objective: Build and Maintain a Secure Network
<u>Requirement 1:</u> Install and maintain a firewall configuration to protect cardholder data <i>1.3.8: Install firewall between any wireless network and the cardholder data store</i>
<u>Requirement 2:</u> Do not use vendor-supplied defaults for system passwords and other security parameters <ul style="list-style-type: none">• <i>Default passwords must be changed,</i>• <i>Remove any unnecessary admin or user accounts</i>

- *Change SNMP community strings changed from default*
- *Change default WEP/WPA keys (note: WEP may soon be removed as an allowable form of PCI DSS compliant encryption)*
- *Use WPA2 and 802.1x authentication whenever possible*
- *Change default SSIDs from the manufacturer's default*
- *Secure console access to https/ssh*

Objective: Protect Cardholder Data

Requirement 3: Protect stored cardholder data

- *Do not use PSK(Pre-shared keys), use strong keys (Note: 802.1x does this automatically when used with a RADIUS server)*

Requirement 4: Encrypt transmission of cardholder data across open, public networks

4.1.1: *Use WPA/WPA2 , IPSEC or VPN or SSL/TLS. Never rely exclusively on WEP.*

If WEP must be used:

- *128bit WEP must be used (104+24bit IV).*
- *WEP should be used in conjunction with WPA/WPA2/ VPN, SSL/TLS.*
- *Rotate Shared WEP keys automatically or at least quarterly*
- *Change WEP keys when there are changes to personnel with access to the WEP keys*
- *Note: WEP may soon be removed as an allowable form of PCI DSS compliant encryption..*

Objective: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

- *Use Unix/Linux operating systems whenever possible to help reduce the threat of viruses.*

<p><u>Requirement 6:</u> Develop and maintain secure systems and applications</p> <ul style="list-style-type: none">• <i>Install vendor-supplied security patches within one month after they are available.</i>
<p>Objective: Implement Strong Access Control Measures</p>
<p><u>Requirement 7:</u> Restrict access to cardholder data by business need-to-know</p> <ul style="list-style-type: none">• <i>Make use of user authentication</i>• <i>Make use of Access Control Lists</i>• <i>Use Syslog Messages</i>
<p><u>Requirement 8:</u> Assign a unique ID to each person with computer access</p> <p>8.3 Use RADIUS or other to authenticate users from remote networks</p> <ul style="list-style-type: none">• <i>Unique Un/pw for admin access</i>• <i>Encrypt all passwords during transmission and storage on all system components</i>• <i>Practice good password management policies for users and admin accounts</i>
<p><u>Requirement 9:</u> Restrict physical access to cardholder data</p> <p>9.1.2.1.2 Restrict access to wireless access points</p>
<p>Objective: Regularly Monitor and Test Networks</p>
<p><u>Requirement 10:</u> Track and monitor all access to network resources and cardholder data</p> <p>10.1 Ensure all accounts can be mapped to a single user</p> <p>10.2 Audit actions of all users with root or administrative privileges. Audit all re-initialization of logs or audit logs</p> <p>10.4 Synchronize all critical system clocks and times</p> <p>10.5 Secure audit trails so they cannot be altered</p>

10.5.4 copy logs from wireless networks to an internal log on the internal LAN

10.6 Review logs from IDS, RADIUS or other AAA servers

Requirement 11: Regularly test security systems and processes

11.1 Use a wireless analyzer at least quarterly to identify all wireless devices in use

11.2 Run network vulnerability scans by qualified vendor

11.3 Perform network penetration testing at least once per year

11.4 Use IDS/ IPS systems

11.5 Alert on critical file changes

Objective: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

12.3 Create a usage policy for all critical employee facing technologies such as modems and wireless access

Create incident response plans (including wireless)

The Xirrus Wi-Fi Array and PCI Security

The Xirrus Wi-Fi Array provides numerous security features that allow compliance with the PCI DSS standard. The current section indicates those specific features that allow the Xirrus Wi-Fi Array to comply with the PCI Data Security Standard

Objective: Build and Maintain a Secure Network

<u>Requirement 1: Install and maintain a firewall configuration to protect cardholder data</u>

- The Xirrus Array contains an embedded stateful firewall that can be used to ensure only legitimate sessions and protocols are bridged from the wireless network.

<u>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</u>

- The Xirrus Array allows the ability to enable only secure protocols are used for management of the Xirrus Array such as https and ssh (secure shell).
- The Xirrus Array has a PCI audit mode that will report and alert on default admin passwords, community strings, WEP keys or default SSIDs that are in use.

Objective: Protect Cardholder Data

<u>Requirement 3: Protect stored cardholder data</u>

- The Xirrus Array fully supports WPA and WPA2 along with 802.1x authentication for the strongest wireless encryption.

<u>Requirement 4: Encrypt transmission of cardholder data across open, public networks</u>

- The Xirrus Array fully supports WPA and WPA2 (AES encryption) along with

802.1x authentication for the strongest wireless encryption and authentication possible. Xirrus Also supports 128bit WEP for those instances where WEP must be used. (*note: WEP may soon be removed as an allowable form of PCI DSS compliant encryption*)

- Xirrus also allows multiple SSIDs to be used each with a separate encryption scheme allowing both WEP and WPA/WPA2 to be used when required per PCI requirements. Additionally SSID broadcast can be disabled so that they are not active publicized.

Objective: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

- The Xirrus Array is based on embedded Linux that helps protect the platform from viruses

Requirement 6: Develop and maintain secure systems and applications

- The Xirrus Array software can be easily updated to accept patches and updates.

Objective: Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

The Xirrus Array supports user authentication, Access Control Lists, MAC-based Access Control Lists, Dynamic user-based VLAN support, Syslog support, and firewall rules allowing fine grain control over access to network resources.

Requirement 8: Assign a unique ID to each person with computer access

- The Xirrus Array supports strong administrator passwords and encrypts any stored passwords or keys.

Requirement 9: Restrict physical access to cardholder data

- The Xirrus Array can be locked at the mounting plate eliminating access to network ports
- The Xirrus Array can be housed in a lockable enclosure providing complete

physical security for the Array

Objective: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

- The Xirrus Array supports multiple syslog servers such that syslog messages can be sent to different servers at the same time allowing audit and logging to be copied from the wireless to the wired network per PCI requirements.
- The Xirrus Array can syslog all admin access
- The Xirrus Array supports NTP (Network Time Protocol) to ensure clock synchronization with other network devices.

Requirement 11: Regularly test security systems and processes

- The Xirrus Array contains a dedicated Wi-Fi Threat sensor to continuously scan the air and identify all wireless infrastructure and wireless client devices. The threat sensor will alert on any unauthorized “rogue AP”.
- Each Xirrus Array has a dedicated embedded Wi-Fi Spectrum analyzer to characterize interference issues and performance of the local environment. By having a distributed system of embedded spectrum analyzers, administrators are freed from having to walk the environment with hand-held devices
- Xirrus optionally offers a wireless Intrusion and Detection System that can actively shield unauthorized users and rogue access points from gaining access to the wireless network.

Objective: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

- An information security policy that addresses wireless incidents and responses should be created. Acceptable end-user wireless usage policies should be created and customized for your organization.

The Xirrus Array PCI Compliance Configuration Checklist

The below check list is designed to help customers ensure that Xirrus Wi-Fi Arrays are configured in a manner that is in compliance with PCI Data Security Standards. Detailed configuration steps to each section can be found in the Xirrus Array Users Manual.

Xirrus Array Configuration Checklist	Completed?
<ul style="list-style-type: none"> • <i>Enable the Xirrus Array Wi-Fi Firewall. Allow only necessary protocols and networks to be accessed</i> 	<input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Change the default Admin account password</i> • <i>Remove any unnecessary admin or user accounts</i> • <i>Change the SNMP community string from the default password</i> • <i>Use WPA2 and 802.1x authentication whenever possible</i> • <i>Change default SSID from Xirrus to a user-defined SSID</i> • <i>Disable SSID broadcast for all PCI compliant SSIDs</i> • <i>Enable ssh access</i> • <i>Disable telnet access</i> • <i>Confirm management over the wireless network is disabled</i> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Confirm WEP is being used only as a last resort</i> • <i>Confirm that 128bit WEP (versus 40bit) is being used for any SSID that requires WEP</i> • <i>Confirm that WPA or WPA2 is used on all SSIDs that do not require WEP</i> 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Confirm that the latest version of the Array OS is being used by checking the Xirrus website at www.xirrus.com</i> 	<input type="checkbox"/>

Xirrus Array Configuration Checklist	Completed?
<ul style="list-style-type: none"> • <i>Enable EAP for use with WPA and configuration. Make use of user authentication</i> • <i>Make use of MAC Access Control Lists for devices that cannot use 802.1x Authentication</i> 	<input type="checkbox"/> <input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Check that external RADIUS servers have been configured for use with WPA/WPA2</i> • <i>Confirm a unique username and password exists for each administrator of the Xirrus Array</i> 	<input type="checkbox"/> <input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Ensure that each Xirrus Array is physically inaccessible</i> 	<input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Enable syslog messaging and define a syslog server on the wired network to forward syslog messages to</i> • <i>Enable NTP and define an NTP server (optional)</i> 	<input type="checkbox"/> <input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Enable the RF Monitor radio in the Xirrus Array. Categorize known or approved devices as such . Respond to any alert of unknown or unapproved wireless devices discovered by the RF Monitor</i> • <i>Monitor Spectrum Analyzer results (optional)</i> 	<input type="checkbox"/> <input type="checkbox"/>
<ul style="list-style-type: none"> • <i>Create a usage policy for all wireless access</i> • <i>Create incident response plan that includes wireless</i> 	<input type="checkbox"/> <input type="checkbox"/>

Additional Resources

- PCI Security Standards Website: www.pcisecuritystandards.org
- List of Qualified PCI Security Assessors:
www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- For the latest version of this whitepaper and the latest versions of Xirrus software: please check: www.xirrus.com