

Six Tips for Complying with the PCI Data Security Standard



The Payment Card Industry Data Security Standard (PCI DSS) is a set of 12 requirements for enhancing payment account data security. Stricter wireless security requirements in new version 1.1 mean many wireless computers, printers and other peripherals retailers use every day do not comply. A single, non-compliant networked device can put the entire network at risk. Following are tips for complying with the PCI DSS v1.1 requirements relevant to wireless peripherals.

PCI DSS v1.1 Requirement	Comment	Solution
2—Do not use vendor-supplied defaults for system passwords and other security parameters.	At one time it was common to deploy wireless LANs secured with default passwords and security configurations, but this practice has largely been abandoned in favor of more secure methods.	Activate security settings during installation (some systems default to security turned off); create original passwords. Older systems should be reviewed to make sure they are compliant.
3—Protect stored cardholder data.	This requirement primarily applies to information held in data and enterprise applications.	Software is available for mobile devices that encrypts stored data to prevent unauthorized access if the device is lost or stolen.
4—Encrypt transmission of cardholder data across open, public networks.	PCI considers wireless LANs to be public networks. Internet and cellular transmissions are also covered by this requirement. Merchants who wirelessly process payments for delivery, service, home sales and other remote commerce are also covered by the public network requirement.	WPA, WPA2, 802.1x, 802.11i and other standard wireless LAN security protocols provide data encryption. Wide area networks provide encryption.
4.1—Use strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.	This requirement applies to wired and wireless, stationary and mobile, and local or Web communications over public networks.	Support for SSL, TLS and IPSEC is available for wireless peripherals. Pay careful attention to specifications because there are different varieties of these protocols, so compatibility with the network infrastructure is not assured.
4.1.1—Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.	WEP was the default security for many early 802.11-standard implementations. Most of these systems have probably been upgraded, but again, older systems should be checked.	The PCI standard defines WPA, WPA2 (referenced above) and VPNs as the acceptable alternatives to WEP.
4.1.1—If WEP is used, do the following: use with a minimum 104-bit encryption key and 24 bit-initialization value; rotate shared WEP keys quarterly (or automatically if the technology permits); rotate shared WEP keys whenever there are changes in personnel with access to keys; restrict access based on media access code (MAC) address.	WEP can be used if it is used together with WPA, WPA2, VPN or SSL/TLS.	Most of these requirements can effectively be addressed during system configuration. Mobile management systems can automatically rotate WEP keys and automate maintenance operations.



Find out how Zebra can help »

PCI Compatible Zebra® Printers



Did you know?

Zebra printers support WPA, WPA2, VPNs and many other leading wireless security protocols, and are in place at thousands of retail locations worldwide for mobile POS, shelf management, inventory control and other applications.

	Zebra QLPlus, RW and MZ mobile printers, Zebra PS4000 External Wireless PrintServer	Cameo 3, QL Plus, RW	QL, QL Plus, RW	XiIIIPlus™, 105SL™, PAX4™, S4M™, Z4Mplus™ with the External or Internal ZebraNet Wireless Plus Print server			
WLAN – Security	Zebra 802.11b/g	Zebra 802.11b	Motorola® Symbol 11b (LA-4137 CF)	Motorola Symbol 11b (LA-4121)	Motorola Symbol 11b (LA-1437 CF)	Cisco® 802.11b/g (CB21)	Cisco® 802.11b (CB350)
WEP (128-bit)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IEEE 802.1X Authentication schemes							
LEAP	Yes	Yes	Yes	No	Yes	Yes	Yes
EAP_FAST	Yes	Yes	Yes	No	No	Yes	Yes
PSK	Yes	No	No	No	No	Yes	Yes
PEAP	Yes	No	No	No	No	Yes	Yes
EAP-TLS	Yes	No	No	No	No	Yes	Yes
EAP-TTLS	Yes	No	No	No	No	Yes	Yes
(WPA) Wi-Fi Protected Access:802.1X + WPA TKIP							
with LEAP	Yes	Yes	Yes	No	No	Yes	Yes
with EAP-FAST	Yes	Yes	Yes	No	No	Yes	No
with PSK (Pre-shared Key)	Yes	Yes	Yes	No	No	Yes	No
with PEAP	Yes	No	No	No	No	Yes	No
with EAP-TLS	Yes	No	No	No	No	Yes	No
with EAP-TTLS	Yes	No	No	No	No	Yes	No
IEEE 802.11i = (WPA2):802.1X + AES encryption							
with PSK, EAP-TLS, EAP-TTLS, LEAP, PEAP, EAP-FAST	Yes	No	No	No	No	PSK Only	No
Airbeam Safe - VPN	Yes	Yes	No	No	No	No	No
Kerberos	Yes	Yes	Yes	No	Yes	No	No

©2007 ZIH Corp. All product names and numbers are Zebra trademarks, and Zebra, the Zebra head graphic, and ZebraNet are registered trademarks of ZIH Corp. All rights reserved. Motorola is a trademark of Motorola, Inc., registered in the U.S. Patent & Trademark Office. Cisco is a registered trademark of Cisco Systems, Inc.



GLOBAL/AMERICAS HEADQUARTERS

Zebra Technologies Corporation
333 Corporate Woods Parkway
Vernon Hills, IL 60061-3109 U.S.A.
T: +1 847 793 2600 or
+1 800 423 0442
F: +1 847 913 8766

EMEA HEADQUARTERS

Zebra Technologies Europe, Limited
Zebra House, Unit 14, The Valley Centre
Gordon Road, High Wycombe
Buckinghamshire HP13 6EQ, UK
T: +44 (0)1494 472872
F: +44 (0)1494 768251

ASIA-PACIFIC HEADQUARTERS

Zebra Technologies Asia Pacific, LLC
16 New Industrial Road
#05-03 Hudson TechnoCentre
Singapore 536204
T: +65 6858 0722
F: +65 6885 0838

www.zebra.com



An ISO 9001 registered company
GSA#: GS-35F-0268N
©2007 ZIH Corp. Printed in U.S.A.
#14307L (8/07) 5M

OTHER LOCATIONS » USA California, Rhode Island, Texas, Wisconsin EUROPE France, Germany, Italy, Netherlands, Poland, Spain, Sweden ASIA-PACIFIC Australia, China, Japan, South Korea LATIN AMERICA Florida (USA), Mexico AFRICA/MIDDLE EAST India, Russia, South Africa, United Arab Emirates