



IBM Payment Card Industry Hardware Option

Achieve and assess PCI compliance

Highlights

- Helps meet payment card industry compliance requirements
 - Provides the ultimate security protection for sensitive cryptographic keys
 - Includes services to assess existing PCI compliance, which can lead to reduced audit costs
-

According to the 2012 Verizon Data Breach Investigations report, 96 percent of data breach victims subject to payment card industry (PCI) data security standards (DSS) had not achieved compliance.¹ Most of the breaches could have been avoided with PCI DSS adherence. Industries with payment card processors, such as banking, government and insurance need the ability to identify compliance issues. Merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits and brand damage should a breach event occur. IBM recognizes that these compliance requirements can create challenges for payment card processors and financial institutions, but they can also create opportunities.

Meeting PCI compliance can provide an opportunity to implement qualitative improvements to data protection within your organization. The IBM Payment Card Industry Hardware Option offering can help you protect sensitive customer cardholder information as it is stored, processed or transmitted. It combines hardware to aid in PCI compliance, along with services to help you determine your level of compliance with PCI. Trusted key entry workstation and smart card functions enable cryptographic key management through IBM® System z® hardware cryptography configuration in compliance with PCI requirements.



Helps meet payment card industry compliance requirements

Compliance with PCI DSS has become a global requirement for any business or entity that processes credit card transactions as payment for goods and services. In this evolving environment full of security concerns and security breaches, you need the ability to meet the latest payment card standards. This requires a robust hardware infrastructure like the Payment Card Industry Hardware Option offering. This hardware-based solution can help you meet PCI compliance requirements, such as:

- Building and maintaining a secure network.
- Protecting cardholder data.
- Maintaining a vulnerability management program.
- Implementing strong access control measures.
- Regularly monitoring and testing networks.
- Maintaining an information security policy.

Provides the ultimate security protection for sensitive cryptographic keys

IBM clients choose System z for the security and cryptographic capabilities it provides, as well as for the integrated environment which simplifies business continuity. By complementing

System z with a trusted key entry workstation and smart card reader, the Payment Card Industry Hardware Option offering provides the optimal environment for securing and managing System z hardware cryptography.

The offering helps reduce the complexity of managing System z hardware cryptographic coprocessors, simplifies processor migrations and improves the security of cryptographic keys. It can also provide the highest level of data protection while addressing the robust and comprehensive PCI Standards to which business need to adhere.

Includes services to assess existing PCI compliance

Credit card issuers are aggressively enforcing the PCI DSS to safeguard cardholder information and prevent losses, so you need an experienced partner with a proven process and track record of success. As a globally certified PCI Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), IBM is qualified to perform your PCI assessments.

As part of the Payment Card Industry Hardware Option offering, IBM provides an overall system assessment which can help you understand your present level of compliance with PCI, as well as validate your adherence to PCI requirements.

Leading the way with PCI compliance solutions

The Payment Card Industry Hardware Option offering forms the basis for establishing a highly secure management hardware cryptographic model. This solution works hand in hand with IBM cryptographic hardware to help ensure the security and privacy of highly sensitive key material.

IBM has helped many companies meet their compliance goals while also leveraging the compliance process. As a result, they can more effectively align their people, processes and technology, or introduce new capabilities to build a more integrated and effective security infrastructure. They recognize that compliance is an opportunity disguised as a challenge and that by taking a thoughtful approach to addressing this challenge they can better position their company for the long term.

It is important to choose a trusted, experienced, certified provider that not only fully understands the PCI DSS, but also comprehends its impacts to your business and associated business processes. When you are ready to take the next step, IBM can work with you to develop your roadmap.

Why IBM?

In addition to ASC and QSA certifications, IBM is one of only a handful of entities recognized by the Security Standards Council as a global PCI solutions provider. IBM maintains a staff of highly skilled, certified security professionals who have industry-specific expertise and use consulting methods based on information security best practices. These abilities go beyond simply assessing your PCI compliance status to providing detailed recommendations for creating a comprehensive security strategy.

For more information

To learn more about the IBM Payment Card Industry Hardware Option offering please contact your IBM representative or IBM Business Partner, or visit: ibm.com/systems/z/solutions/security

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: ibm.com/financing



© Copyright IBM Corporation 2013

IBM Corporation
Systems and Technology Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2013

IBM, the IBM logo, ibm.com, and System z are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

¹ Verizon 2012 Data Breach Investigations Report:
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf



Please Recycle
