



IN-DEPTH SOLUTION BRIEF

PCI DSS: CREDANT Endpoint Data | Security for Compliance



WWW.CREDANT.COM



PCI DSS:

CREDANT Endpoint Data | Security for Compliance

Credit cards have revolutionized the way we do business, effectively extending trillions of dollars in credit to over one billion people around the world.² In the United States alone, over 600 million cards are now in use.³

However, the value of the information associated with these payment cards — commonly referred to as “cardholder data” — has also prompted a growing number of attacks on this data.

Attacks can include hacking by outsiders, the physical theft of storage media and illegal activities by company employees. Even if the data is stored behind firewalls, the growing number of remote users – often with laptops, handhelds, smartphones, USB drives and CD-DVDs— increases the possibility that credit card numbers can be stolen. Literally millions of credit card numbers can be stored on a memory device and carried out the door in an employee’s pocket.

PCI DSS OVERVIEW

To address the security threats against cardholder data, the PCI Security Standards Council was founded in 2007 by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. Working with a wide range of industry and technology advisors, the Council developed the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS is a global security program created to reduce risks to PCI members, merchants, service providers and consumers. The PCI DSS program is based on 12 data-centric requirements that are designed to ensure cardholder data security. These requirements involve the use of data encryption and end-user access control with activity monitoring and logging. (A complete description of the standard and other materials are available from the PCI Security Standards Council at www.pcisecuritystandards.org.)

PCI DATA SECURITY STANDARD	
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across public networks open
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

PCI DSS:

CREDANT Endpoint Data | Security for Compliance



PCI DSS is an industry standard, not a law or government regulation such as the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill (SB) 1386 or the Gramm-Leach-Bliley Act (GLBA), which all have provisions for data security. However, PCI DSS non-compliance can result in severe fines and penalties for businesses supporting credit card transactions. Failure to comply with the security standard, promptly rectify a security issue or report a compromise can result in:

- › Possible restrictions on the merchant by the card associations, including the cancellation of the account with the credit card association.
- › Permanent prohibition of the merchant's participation in card association programs.
- › Compensation for fraud losses perpetrated by using the account numbers associated with compromised data.

CREDANT AND PCI DSS REQUIREMENTS

PCI DSS compliance is based on satisfying all 12 requirements. Organizations that develop a PCI DSS compliance initiative usually have a number of technology products, policies and procedures in place to address some of these requirements. However, few organizations can immediately demonstrate full compliance since today's IT environments are often highly complex, integrated with other environments across the Internet and constantly evolving. This is especially true for endpoints, including desktops and mobile devices.

CREDANT data protection solutions can help demonstrate compliance efforts for all of PCI DSS Requirements 2, 3 and 8. Relevant sections are cited below, along with a summary of CREDANT support.

REQUIREMENT 2:

Requirement 2.3: Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

CREDANT supports SSL for all non-console administrative access.

"Merchants are beginning to understand that the potential damage to their brand if they are involved in a security breach could far outweigh the cost of a fine."¹

Bob Russo, General Manager, PCI Security Standards Council

REQUIREMENT 3:

Requirement 3.4: Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- › Strong one-way hash functions (hashed indexes)
- › Truncation
- › Index tokens and pads (pads must be securely stored)
- › Strong cryptography with associated key management processes and procedures

The minimum account information that must be rendered unreadable is the PAN.

If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: 'Compensating Controls for Encryption of Stored Data.'

3.4.1: If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

CREDANT uses strong cryptography with associated key management processes and procedures on every device on which our solutions are installed.

REQUIREMENT 3.5:

Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.

PCI DSS:

CREDANT Endpoint Data | Security for Compliance



3.5.1: Restrict access to keys to the fewest number of custodians necessary.

3.5.2: Store keys securely in the fewest possible locations and forms.

CREDANT support: CREDANT provides all the implementation/configuration features necessary to allow customers to meet these requirements. In addition, all CREDANT storage of encryption material is secured and only authorized users and system resources are allowed access.

REQUIREMENT 3.6:

Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

3.6.1: Generation of strong keys

3.6.2: Secure key distribution

3.6.3: Secure key storage

3.6.4: Periodic changing of keys

- › As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically
- › At least annually

3.6.5: Destruction of old keys

3.6.6: Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)

3.6.7: Prevention of unauthorized substitution of keys

3.6.8: Replacement of known or suspected compromised keys

3.6.9: Revocation of old or invalid keys

3.6.10: Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities

CREDANT support: Provides all the implementation/configuration features necessary (including documentation where appropriate) to allow customers to meet these requirements.

REQUIREMENT 8:

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users

8.1: Identify all users with a unique user name before allowing them to access system components or cardholder data.

8.2: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- › Password
- › Token devices (e.g., SecureID, certificates, or public key)
- › Biometrics

8.3: Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

8.4: Encrypt all passwords during transmission and storage on all system components

8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

8.5.1: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects

8.5.2: Verify user identity before performing password resets

8.5.3: Set first-time passwords to a unique value for each user and change immediately after the first use

8.5.4: Immediately revoke access for any terminated users

8.5.5: Remove inactive user accounts at least every 90 days

8.5.6: Enable accounts used by vendors for remote maintenance only during the time period needed

8.5.7: Communicate password procedures and policies to all users who have access to cardholder data

8.5.8: Do not use group, shared, or generic accounts and passwords

PCI DSS:

CREDANT Endpoint Data | Security for Compliance



- 8.5.9:** Change user passwords at least every 90 days
- 8.5.10:** Require a minimum password length of at least seven characters
- 8.5.11:** Use passwords containing both numeric and alphabetic characters
- 8.5.12:** Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- 8.5.13:** Limit repeated access attempts by locking out the user ID after not more than six attempts
- 8.5.14:** Set the lockout duration to thirty minutes or until administrator enables the user ID
- 8.5.15:** If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal
- 8.5.16:** Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

CREDANT provides all the implementation/configuration features necessary (including documentation where appropriate) to allow customers to meet these requirements. CREDANT supports the necessary third-party components required (in order to meet sections 8.2, 8.3).

SUMMARY

CREDANT offers a range of data protection solutions to help you meet the requirements of PCI DSS. Centrally managed encryption that is simple to deploy and cost-effective to manage is essential to help ensure the security of card holder data and to meet the reporting requirements for PCI DSS.

-
1. PCI Security Standards Council.
 2. Wall Street Journal, November 20, 2008.
 3. ITPro, December 12, 2008.