

## Review of the JANA encryption solution to Payment Card Industry Data Security Standard 1.2 requirements

Becoming compliant with the Payment Card Industry Data Security Standard (PCI DSS) has been a challenge for multiple businesses, especially in the field of data security. One of the most common issues found in companies trying to comply with the PCI DSS are encryption processes and procedures are not currently being used, and trying to retrofit technologies into the business is a daunting process.

Multiple vendors have created products to assist companies in meeting these strict requirements, the one being reviewed is the JANA hardware encryption device by Dark Matter Labs. The product was created with the PCI DSS specifically in mind; however as with most hardware devices of its type in the market it will assist companies in meeting compliance with other legislative or professional encryption requirements.

Shown below in table format are the PCI DSS v1.2 requirements that deal with encryption with observations and comments about the JANA device:

PCI DSS Requirements	Testing Procedures	Observations on compliance
<p><b>2.1</b> Always change vendor-supplied defaults <b>before</b> installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</p>	<p><b>2.1</b> 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.)</p>	<p>The JANA device requires that the initial key administrator account must enter a password at the time of installation.</p>
<p><b>2.3</b> Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</p>	<p><b>2.3</b> For a sample of system components, verify that non-console administrative access is encrypted by:</p> <ul style="list-style-type: none"> <li>▪ Observing an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested;</li> <li>▪ Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally; and</li> <li>▪ Verifying that administrator access to the web-based management interfaces is encrypted with strong cryptography.</li> </ul>	<p>All communication to the JANA device is over a secured SSL connection and no other non-console administrative access is available.</p>

PCI DSS Requirements	Testing Procedures	Observations on compliance
<p><b>3.4</b> Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:</p> <ul style="list-style-type: none"> <li>▪ One-way hashes based on strong cryptography</li> <li>▪ Truncation</li> <li>▪ Index tokens and pads (pads must be securely stored)</li> <li>▪ Strong cryptography with associated key-management processes and procedures</li> </ul> <p>The MINIMUM account information that must be rendered unreadable is the PAN.</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> <li>▪ <i>If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.</i></li> <li>▪ <i>“Strong cryptography” is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.</i></li> </ul>	<p><b>3.4.a</b> Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods:</p> <ul style="list-style-type: none"> <li>▪ One-way hashes based on strong cryptography</li> <li>▪ Truncation</li> <li>▪ Index tokens and pads, with the pads being securely stored</li> <li>▪ Strong cryptography, with associated key-management processes and procedures</li> </ul>	<p>The JANA device uses the strong cryptography with associated key-management processes and procedures to meet this requirement. The only cryptographic processes available for use are those documented as acceptable by the PCI DSS.</p>
	<p><b>3.4.b</b> Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).</p>	
	<p><b>3.4.c</b> Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable.</p>	<p>As the data is encrypted by the JANA device, the data is not able to be decrypted by backup solutions before being written to removable media.</p>
	<p><b>3.4.d</b> Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.</p>	<p>The logs of the JANA devices do not store the PAN in the logs and are compliant with this requirement.</p>
<p><b>3.6</b> Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:</p>	<p><b>3.6.a</b> Verify the existence of key-management procedures for keys used for encryption of cardholder data.</p> <p><i>Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>.</i></p>	<p>This requirement is a policy/procedural requirement and not something directly defined by the technology.</p>
	<p><b>3.6.b</b> For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer’s keys (used to transmit data between customer and service provider).</p>	<p>If a service provider was providing the service for the customer, the keys are controlled by the device and no customer interaction is required to store and/or change the keys. Keys are changed in the JANA device yearly by default to meet PCI requirements, however this duration can be set to a more frequent cycle if required.</p>
	<p><b>3.6.c</b> Examine the key-management procedures and perform the following:</p>	

<b>PCI DSS Requirements</b>	<b>Testing Procedures</b>	<b>Observations on compliance</b>
<b>3.6.1</b> Generation of strong cryptographic keys	<b>3.6.1</b> Verify that key-management procedures are implemented to require the generation of strong keys.	The JANA device only creates keys that have been stated by the PCI Council to be strong. All cryptographic keys are created with FIPS compliant encryption schemas.
<b>3.6.2</b> Secure cryptographic key distribution	<b>3.6.2</b> Verify that key-management procedures are implemented to require secure key distribution.	The JANA device controls the cryptographic keys and therefore removes the requirement that keys would have to be distributed to multiple systems.
<b>3.6.3</b> Secure cryptographic key storage	<b>3.6.3</b> Verify that key-management procedures are implemented to require secure key storage.	The JANA device only stores the keys in volatile memory and any loss of power will require the key be recreated.
<b>3.6.4</b> Periodic cryptographic key changes <ul style="list-style-type: none"> <li>▪ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically</li> <li>▪ At least annually</li> </ul>	<b>3.6.4</b> Verify that key-management procedures are implemented to require periodic key changes at least annually.	The default settings for the JANA devices for key rotation are set to automatically cycle after one year. This setting can be configured to change the encryption keys more frequently if desired.
<b>3.6.5</b> Retirement or replacement of old or suspected compromised cryptographic keys	<b>3.6.5.a</b> Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).	All keys that exceed the time duration set in the JANA device are retired at the time designated by the user (yearly by default).
	<b>3.6.5.b</b> Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.	If keys are suspected to have been compromised, key custodians can require the JANA device to expire the key and issue a new one at any time.
<b>3.6.6</b> Split knowledge and establishment of dual control of cryptographic keys	<b>3.6.6</b> Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key).	The JANA device has been architected to meet this requirement. The key custodian has the ability to set key creation to require multiple users to enter passphrases to create the encryption key.
<b>3.6.7</b> Prevention of unauthorized substitution of cryptographic keys	<b>3.6.7</b> Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.	The JANA will notify users in the event of the changing of encryption keys. The JANA device also supports the ability to offload the logs to a centralized server to have the device monitored by already deployed logging systems as required by the PCI DSS.
<b>3.6.8</b> Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	<b>3.6.8</b> Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.	This requirement is a policy/procedural requirement and not something directly defined by the technology.

PCI DSS Requirements	Testing Procedures	Observations on compliance
<p><b>4.1</b> Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS are:</i></p> <ul style="list-style-type: none"> <li>▪ <i>The Internet,</i></li> <li>▪ <i>Wireless technologies,</i></li> <li>▪ <i>Global System for Mobile communications (GSM), and</i></li> <li>▪ <i>General Packet Radio Service (GPRS).</i></li> </ul>	<p><b>4.1.a</b> Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks</p> <ul style="list-style-type: none"> <li>▪ Verify that strong encryption is used during data transmission</li> <li>▪ For SSL implementations: <ul style="list-style-type: none"> <li>– Verify that the server supports the latest patched versions.</li> <li>– Verify that HTTPS appears as a part of the browser Universal Record Locator (URL).</li> <li>– Verify that no cardholder data is required when HTTPS does not appear in the URL.</li> </ul> </li> <li>▪ Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.</li> <li>▪ Verify that only trusted SSL/TLS keys/certificates are accepted.</li> <li>▪ Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)</li> </ul>	<p>The JANA device uses only HTTPS (SSL) for all connections to the encryption device. The JANA device is typically not used over open, public networks but meets all the SSL requirements listed if used in such a manner.</p>
<p><b>8.1</b> Assign all users a unique ID before allowing them to access system components or cardholder data.</p>	<p><b>8.1</b> Verify that all users are assigned a unique ID for access to system components or cardholder data.</p>	<p>All users on the JANA device are required to have a unique ID for access to the system.</p>
<p><b>8.2</b> In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <li>▪ Password or passphrase</li> <li>▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)</li> </ul>	<p><b>8.2</b> To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following:</p> <ul style="list-style-type: none"> <li>▪ Obtain and examine documentation describing the authentication method(s) used.</li> <li>▪ For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).</li> </ul>	<p>The JANA device uses a User ID/Password authentication mechanism and is compliant with this requirement.</p>