COMPLIANCE

Payment Card Industry Data Security Standard (PCI-DSS) Compliance with Rocket MultiValue

The Payment Card Industry requires all organizations that store or process credit card data and transactions to implement technical security requirements over all systems involved in data storage and transmission. The scope of these control requirements ranges from encryption methods to access rights management to vulnerability testing.

The Rocket® MultiValue Application Platform (Rocket MV), which includes Rocket UniData and Rocket UniVerse, enables robust technical security controls to help you implement many PCI-DSS requirements in your database environment. However, the scope of PCI-DSS extends to several organizational and procedural control areas that cannot be satisfied solely through technical means. PCI-DSS compliance will ultimately depend on effective implementation of the technical controls available through Rocket MV as well as appropriate technical and procedural controls over your entire Cardholder Data (CHD) environment. Relevant PCI-DSS requirements, and the capabilities Rocket MV offers to address them, are listed below.

PCI-DSS Requirements	Rocket MV Capabilities
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). No generic user accounts or default credentials are added or required by Rocket MV.
2.3 Encrypt all non-console administrative access using strong cryptography.	All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users. Rocket MV supports the latest implementations of the Secure Shell (SSH) and Transport Layer Security (TLS) encrypted protocols for maximum security.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Rocket Software offers technical security documentation surrounding its Rocket MV products that will assist in describing the technical security measures protecting your data.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures	OpenSSL-based Automatic Data Encryption protects data at rest. Access to database files or their storage media by an unauthorized party without encryption keys will not be intelligible to an unauthorized party. Key management policies can be defined and enforced for individual encryption keys.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Rocket MV supports robust password and encryption key management solutions for Automatic Data Encryption. Policies can be defined for individual keys.
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	OpenSSL-based Automatic Data Encryption protects data in transit. Parties can be certain they are talking to the intended party, and that data has not been accessed, corrupted, or maliciously altered during transmission. Rocket MV supports the latest implementation of the Transport Layer Security (TLS) encryption protocol, TLS 1.2, for data transfers. Data intercepted in transit will be unintelligible to any unauthorized party.

PCI-DSS Requirements	Rocket MV Capabilities
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Define access needs for each role, including system components and data resources that each role needs to access for their job function and level of privilege required (for example, user, administrator, etc.) for accessing resources. Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. Assign access based on individual personnel's job classification and function. Require documented approval by authorized parties specifying required privileges.	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users. User authentication is performed by the operating system and passed to the database. MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users. Audit logs can provide a secure record of any access or updates to user access rights, whether authorized or unauthorized.
8.1 Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows: • Assign all users a unique ID before allowing them to access system components or cardholder data. • Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. • Immediately revoke access for any terminated users. • Remove/disable inactive user accounts at least every 90 days. • Manage IDs used by vendors to access, support, or maintain system components via remote access • Limit repeated access attempts by locking out the user ID after not more than six attempts. • Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. • If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session	User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). Rocket MV inherits all user access security controls you have implemented within your operating system credentials, including account lockout for invalid login attempts, inactivity timeout, and disabling of dormant accounts. All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users. Rocket MV does not add or require any generic user accounts or default credentials.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	Enforced multi-factor authentication methods can be implemented at the operating system level, and the authentication login session passed to Rocket MV through LDAP, SAML, or token-based SSO.

PCI-DSS Requirements	Rocket MV Capabilities
8.5 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	Rocket MV does not add or require any generic user accounts or default credentials.
10.1 Implement audit trails to link all access to system components to each individual user.	Rocket MV records detailed audit logs of all activity occurring within the database, including the specific activity and the individual user performing the activity.
10.2 Implement automated audit trails for all system components to reconstruct the following events: • All individual accesses to cardholder data • All actions taken by any individual with root or administrative privileges • Access to all audit trails • Invalid logical access attempts • Use of identification and authentication mechanisms — including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges • Initialization, stopping, or pausing of the audit logs • Creation and deletion of system-level objects	Audit logs can provide a secure record of any access to cardholder data, whether authorized or unauthorized, as well as all required system-level events.
10.3 Record at least the following audit trail entries for all system components for each event: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource.	Audit logs include all relevant details of each recorded event.
10.5 Secure audit trails so they cannot be altered.	Audit logging configuration is stored in an encrypted file that can be password-protected and is only modifiable by authorized users. Rocket MV audit logging also protects log files in several ways: the log files can be put on a different machine than the one on which Rocket MV server is running; sequential log files are accessible only by privileged accounts; and log files can also be compressed and/or encrypted.

PCI-DSS Requirements	Rocket MV Capabilities
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Delayed Standby Replication lets you protect a subscriber from malicious damage caused by a compromise to the publisher. Real-time replication may introduce the same damage from the publisher to the subscriber, exposing you to potential data loss. Keeping the subscriber a defined interval behind the publisher (such as 6 hours) protects the business and helps address ‘Clear record’ events. Recoverable File System (RFS) helps maintain physical integrity of data at rest and ensure recovery from hardware failures. Audit logging can be configured to provide user-defined notifications when configured events occur in the system related to users’ critical activities, allowing immediate detection and response. Audit logging can also record pre- and after-images of changed data.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Detailed audit logging and reporting capabilities can assist in your incident response plans by letting you determine exactly which records were accessed, when, and by whom. This can aid in a forensic investigation into the extent of a data breach and the number of affected records.

Rocket®

rocketsoftware.com

info@rocketsoftware.com

US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405

twitter.com/rocket

www.linkedin.com/comp
rocket-software

www.facebook.com
RocketSoftwareInc

blog.rocketsoftware.com