
PCI DSS Compliance

EncryptRIGHT

COPYRIGHT© 1988–2009 Prime Factors, Inc. All rights reserved.

This publication contains confidential and proprietary information which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval system, or translated into any language or computer language, or transmitted in any form whatsoever, without prior written consent of Prime Factors. For information, contact:

Prime Factors, Inc.
4725 Village Plaza Loop, Suite 100
Eugene, OR 97401
ATTN: Technical Publications
Phone: (541) 345-4334 Fax: (541) 345-6818

Disclaimer of Warranties and Limitation of Liabilities

The staff of Prime Factors has taken due care in preparing this manual. However, nothing contained herein modifies or alters in any way the standard terms and conditions of the Prime Factors purchase, lease, or license agreement by which the product was acquired, nor increases in any way Prime Factors' liability to the customer. In no event shall Prime Factors or its subsidiaries be liable for incidental or consequential damages in connection with or arising from the use of the product, the accompanying manual, or any related materials.

All Prime Factors publications and computer programs contain proprietary confidential information of Prime Factors, and its possession and use are subject to restrictions set forth in the License Agreement entered into between Prime Factors and its Licensees. No title or ownership of Prime Factors software is transferred and any use of the product and its related materials beyond the terms of this license, without the written authorization of Prime Factors, is prohibited.

Prime Factors reserves the right to revise this publication from time to time and to make changes in the content hereof without obligation to notify any person of such revisions or changes.

Restricted and Limited Rights Notice

Use, duplication or disclosure by any agency of the U.S. Government licensed with respect to this documentation is subject to restrictions, as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Prime Factors, Inc., 4725 Village Plaza Loop, Suite 100, Eugene, OR 97401.

EncryptRIGHT Version PCI DSS Compliance
Document Number crpz-PCI-04.07.09

Contents

About PCI DSS Compliance	4
How EncryptRIGHT Complies	4
PCI Requirement #2	4
PCI Requirement #3	4
PCI Requirement #4	6
PCI Requirement #7	7
PCI Requirement #8	7
PCI Requirement #10	8

About PCI DSS Compliance

The Payment Card Industry Data Security Standard was designed for bank card information security, however the recommendations apply to any general data security needs.

The PCI DSS document recommends 12 broad requirements which range from firewalls and physical access to software and data security systems, and documented procedures. EncryptRIGHT can help provide the software-related aspects of the PCI DSS compliance required for cryptography and key management.

How EncryptRIGHT Complies

The following is a breakdown of PCI DSS requirements and a description of how EncryptRIGHT addresses each.

PCI Requirement #2

Do not use vendor-supplied defaults for system passwords and other security parameters.

EncryptRIGHT does not have a default User ID or password. On installation a UserID and password must be created and given administrative rights before installation can continue.

PCI Requirement #3

Protect stored cardholder data.

EncryptRIGHT complies with this requirement in each of the following specifics:

Requirement	EncryptRIGHT Compliance
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	EncryptRIGHT provides the capability to define a group of users that only have rights to view a masked portion of a data field. This includes applications that decrypt the data, the EncryptRIGHT audit log and EncryptRIGHT trace files.
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs).	EncryptRIGHT provides strong cryptography and key management to protect your data. This includes strong hashing (SHA 2 256/384/512) and encryption (Triple DES 2/3 key, and AES 128/192/256).
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	EncryptRIGHT requires a UserID and password for all users. Each user is assigned to one (or more) groups. Each group is assigned the types of access within the EncryptRIGHT administration application. This includes the ability to view or maintain keys and other information. In addition EncryptRIGHT allows you to require a quorum of logged on users for administration functions.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data. 3.6.1 Generation of strong cryptographic keys.	EncryptRIGHT supports Triple DES 2/3 keys. AES 128, 192 and 256. RSA public keys from 1024 to 4096 bits.
3.6.2 Secure cryptographic key distribution.	Secure key distribution is provided in EncryptRIGHT when the client/server option is licensed. This provides for a server where keys are maintained and one or more client computers connected through a TCP/IP network. Each client computer is registered to the server and the server automatically distributes key changes to the clients. All key distributions are encrypted.
3.6.3 Secure cryptographic key storage	EncryptRIGHT hashes and encrypts all records within the EncryptRIGHT security database using a randomly generated local master key. The master key is protected by the software license which is restricted to licensed computers only.
3.6.4 Periodic cryptographic key changes	EncryptRIGHT allows you to change key values manually or automatically. Automatic key changes can be set to occur weekly, monthly, quarterly or yearly.

Requirement	EncryptRIGHT Compliance
<p>3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys</p>	<p>EncryptRIGHT allows you to designate when a key can be destroyed. The choices are never (for long term data storage), on expiration, expiration plus 1 week, expiration plus 1 month, expiration plus 1 quarter, expiration plus 1 year, expiration plus 2 years, expiration plus 3 years, expiration plus 4 years, expiration plus 5 years, expiration plus 6 years and expiration plus 7 years.</p> <p>Any key that becomes compromised or invalid can be marked as revoked. A new value can easily be created. Every production key value is assigned a unique key version number. When a specific key value is marked as revoked, or is otherwise superseded, a new version is created. Both keys still exist in the database, so if an application attempts to use a revoked key, they will receive an indication that the key is revoked.</p>
<p>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)</p>	<p>EncryptRIGHT provides the ability for up to 3 different people to enter key components. Additionally you can require that the components must be entered by different users. You also have the ability to require a quorum of users to be logged on. For example you can require two people with rights for key management be logged on at the same time to enter a key component, where one person enters the key and the other observes.</p>
<p>3.6.7 Prevention of unauthorized substitution of cryptographic keys</p>	<p>Key values cannot be substituted by unauthorized people. Every user should be assigned a unique UserID and password. Every key change is logged in the EncryptRIGHT secure audit log.</p>

PCI Requirement #4

Encrypt transmission of cardholder data across open, public networks.

Although this requirement talks about using SSL and TLS security over networks, it is always better to also encrypt sensitive data from application to application so the data is not only protected during transmission, but also between transmission and the application that will process the data. For example, when you send an un-encrypted file through a secure network, the file may temporarily reside on the receiving computer until some process uses the data. During this time someone could access or even change the data without your knowledge. Use EncryptRIGHT to protect this data until the receiving application can process the data.

PCI Requirement #7

Restrict access to cardholder data by business need-to-know.

EncryptRIGHT provides the ability to define the level of data access for each user. Access can be specified at the record and/or data field level. The type of access that can be defined is no access, masked access (specifying the mask character, the position and length of the clear data), read only or read/write. By default no access is allowed for anyone when creating record definitions. In order to use a definition you must provide access definitions.

PCI Requirement #8

Assign a unique ID to each person with computer access.

EncryptRIGHT complies with this requirement in each of the following specifics:

Requirement	EncryptRIGHT Compliance
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	EncryptRIGHT allows for all users to have a unique UserID and password. This is used not only for access to the EncryptRIGHT database, but also for access to cryptography for your defined user data records and fields.
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	Passwords are stored self encrypted. This means that they are encrypted using a key derived from the password itself. These passwords cannot be decrypted. The only way to verify a password is to enter the same password, which is encrypted and then compared to the original encrypted password.
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Only user administrators can add, delete and change users. In addition this can be further controlled by requiring a quorum of logged on users so no single person can maintain user information without supervision.
8.5.2 Verify user identity before performing password resets.	Passwords can only be changed by a user if the user also enters the current password.
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.	EncryptRIGHT defaults to forcing the user to change their password anytime an administrator sets or changes a user's password.

Requirement	EncryptRIGHT Compliance
<p>8.5.4 Immediately revoke access for any terminated users.</p> <p>8.5.5 Remove/disable inactive user accounts at least every 90 days.</p> <p>8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.</p>	<p>Users can be temporarily disabled or entirely deleted by user administrators at any time.</p>
<p>8.5.9 Change user passwords at least every 90 days.</p> <p>8.5.10 Require a minimum password length of at least seven characters.</p> <p>8.5.11 Use passwords containing both numeric and alphabetic characters.</p> <p>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.</p> <p>8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.</p> <p>8.5.14 Set the lockout duration to 30 minutes or until administrator enables the user ID.</p>	<p>EncryptRIGHT provides a password policy that can specify the following:</p> <ul style="list-style-type: none"> ■ Maximum and minimum password age. ■ Minimum password length ■ Password uniqueness. This includes how many passwords to remember, the maximum characters that can be repeated from the previous password, and a password dictionary. ■ Required special characters, upper/lower case and numerics. ■ Bad attempts lockout count, and the duration of the lockout.
<p>8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.</p>	<p>EncryptRIGHT can optionally require a UserID and password for API use. This means that in order for an application to use the EncryptRIGHT library to encrypt any data, a UserID and password has to be given to the library for verification. With this, EncryptRIGHT fetches the access rights the user has. When a data record definition in EncryptRIGHT is used to encrypt or decrypt data, the user's access rights are checked to determine if they can decrypt data, and if so, do they only see a masked version of the data, or can the view or update the data.</p>

PCI Requirement #10

Track and monitor all access to network resources and cardholder data.

EncryptRIGHT complies with this requirement in each of the following specifics:

Requirement	EncryptRIGHT Compliance
<p>10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</p>	<p>EncryptRIGHT allows for all users to have a unique UserID and password.</p>
<p>10.2 Implement automated audit trails for all system components to reconstruct the following events.</p>	<p>EncryptRIGHT provides the ability to create a secure audit log entry for access to data down to the field level. An audit log entry is made for Invalid access attempts also. Audit log entries are made for all changes made to definitions within EncryptRIGHT. An audit log entry is optionally created for all user logons and logoffs.</p>
<p>10.3 Record at least the following audit trail entries for all system components for each event.</p>	<p>The EncryptRIGHT audit log contains the UserID, the type of message, date and time, the EncryptRIGHT subsystem name and the success or failure message.</p>
<p>10.5 Secure audit trails so they cannot be altered.</p>	<p>The EncryptRIGHT audit log is secure. Each entry contains a sequence number and the entire entry is hashed and encrypted. When viewing the log, each entry hash and sequence number is verified. The ability to view the audit log can be assigned to groups of users.</p>