



Payment Card Industry Data Security Standard (PCI DSS) Solution Map

nuBridges Protect™ and nuBridges Exchange™ software solutions address specific requirements defined in the Payment Card Industry Data Security Standard as follows:

Section	Requirement	nuBridges Solution
1.3	<p>Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:</p> <p>1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ (ingress filters)</p> <p>1.3.2 Restricting inbound and outbound Internet traffic to ports 80 and 443</p> <p>1.3.3 Not allowing internal addresses to pass from the Internet into the DMZ (egress filters)</p> <p>1.3.5 Placing the database in an internal network zone, segregated from the DMZ</p> <p>1.3.6 Restricting outbound traffic to that which is necessary for the payment card environment</p> <p>1.3.7 Securing and synchronizing router configuration files (e.g., running configuration files – used for normal running of the routers, and start-up configuration files - used when machines are re-booted, should have the same, secure configuration).</p> <p>1.3.8 Denying all other inbound and outbound traffic not specifically allowed</p>	<p>nuBridges Exchange ensures that all inbound traffic is restricted by only allowing validated and verified information to be brought into the enterprise through only a single outbound opening in the firewall.</p>
1.4	<p>Prohibit direct public access between external networks and any system component that stores cardholder information (e.g., databases)</p> <p>1.4.1 Implement a DMZ to filter and screen all traffic, to prohibit direct routes for inbound and outbound Internet traffic</p> <p>1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.</p>	<p>nuBridges Exchange provides the ability for all inbound traffic to be screened within the DMZ and then allowed into the enterprise using a single, outbound firewall opening. This restricts inbound traffic from having access to production systems and limits the required openings in the firewall.</p>
1.5	<p>Implement Internet Protocol (IP) masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).</p>	<p>nuBridges Exchange allows you to securely transmit information via FTP. The requirement requires you to use a NAT on a machine to conduct business. If you securely send or receive files using FTP, nuBridges Exchange with FTP provides a smart FTP client that supports NAT navigation.</p>
3.3	<p>Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p>	<p>nuBridges Protect allows you to automatically mask account numbers based on your configuration. You choose how many leading and trailing characters to display. Only authorized users can view entire account numbers.</p>
3.4	<p>Render sensitive cardholder data unreadable anywhere it is stored, (including data on portable media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:</p> <ul style="list-style-type: none"> – One-way hashes (hashed indexes) such as SHA-1 – Truncation – Index tokens and PADs, with the PADs being securely stored – Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures. <p>The MINIMUM account information that needs to be rendered unreadable is the payment card account number.</p>	<p>nuBridges Protect supports one-way hashing and recommends the use of SHA-1 specifically. Additionally, nuBridges Protect supports a number of strong cryptographic algorithms such as AES 256-bit and Triple-DES 128-bit.</p> <p>All backup media and audit logs must be encrypted and the keys secured, not incorporated, from them.</p>

<p>3.5</p>	<p>Protect encryption keys against both disclosure and misuse;</p> <p>3.5.1 Restrict access to keys to the fewest number of custodians necessary.</p> <p>3.5.2 Store keys securely in the fewest possible locations and forms.</p>	<p>nuBridges Protect restricts access to all keys and eliminates the need for users to know where keys are stored. Also, programmers are restricted to using APIs for keys access and are not given access to the keys themselves.</p>
<p>3.6</p>	<p>Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including:</p> <p>3.6.1 Generation of strong keys</p> <p>3.6.2 Secure key distribution</p> <p>3.6.3 Secure key storage</p> <p>3.6.4 Periodic key changes</p> <ul style="list-style-type: none"> • As deemed necessary re-keying; preferably • At least annually. <p>3.6.5 Destruction of old keys</p> <p>3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key)</p> <p>3.6.7 Prevention of unauthorized substitution of keys</p> <p>3.6.8 Replacement of known or suspected compromised keys</p> <p>3.6.9 Revocation of old or invalid keys</p> <p>3.6.10 Requirement for key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.</p>	<p>nuBridges Protect Key Manager enables the complete life cycle management of keys. The solution addresses: key generation, distribution, storage, rotation, archiving, revocation and deletion and limits access on an as-needed basis.</p> <p>Users do not have access to any part of the values of the keys.</p>
<p>4.1</p>	<p>Use strong cryptography and encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks.</p>	<p>nuBridges Protect and nuBridges Exchange provides strong cryptography through multiple algorithms including the Federally-approved AES and 3DES algorithms.</p>
<p>8.4</p>	<p>Encrypt all passwords during transmission and storage, on all system components.</p>	<p>nuBridges Protect encrypts all passwords and pass phrases when used to transmit documents and information as well as when storing them.</p>
<p>9.6</p>	<p>Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.</p>	<p>nuBridges Protect allows you to encrypt information at the field or file level before storing it on permanent media. This allows you to secure electronic media, encrypting data for backup that is not normally encrypted.</p>
<p>10.1</p>	<p>Establish a process for linking all access to system components (especially those with administrative privileges such as root) to an individual user.</p>	<p>nuBridges Protect and nuBridges Exchange record all activities related to encryption of credit card information, whether at-rest or in-transit and are logged for audit purposes. User access to encrypt or decrypt is recorded and available for viewing or for reporting by centralized logging facilities.</p>
<p>10.2</p>	<p>Implement automated audit trails to reconstruct the following events, for all system components:</p> <p>10.2.1 All individual accesses to cardholder data.</p> <p>10.2.2 All actions taken by any individual with root or administrative privileges.</p> <p>10.2.3 Access to all audit trails.</p> <p>10.2.4 Invalid logical access attempts.</p> <p>10.2.5 Use of identification and authentication mechanisms.</p> <p>10.2.6 Initialization of the audit logs.</p> <p>10.2.7 Creation and deletion of system-level objects.</p>	<p>nuBridges Protect and nuBridges Exchange record all activities related to encryption and decryption of credit card information, whether at-rest or in-transit and are logged for audit purposes. User access to encrypt or decrypt is recorded and available for viewing or for reporting by centralized logging facilities. Additionally, the logging files may be encrypted, if required, using a pass phrase.</p>

<p>10.3</p>	<p>Record at least the following audit trail entries for each event, for all system components:</p> <ul style="list-style-type: none"> 10.3.1 User identification 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.5 Origination of event 10.3.6 Identity or name of affected data, system component, or resource. 	<p>nuBridges Protect records each time a field or file is accessed for encryption or decryption. nuBridges Exchange records all transmission of data when being transported. nuBridges' logs contain all of the information required for compliance.</p>
<p>10.5</p>	<p>Secure audit trails so they cannot be altered, including the following:</p> <ul style="list-style-type: none"> 10.5.1 Limit viewing of audit trails to those with a job-related need 10.5.2 Protect audit trail files from unauthorized modifications 10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter 10.5.4 Copy logs for wireless networks onto a log server on the internal LAN. 10.5.5 Use file integrity monitoring/change detection software (such a Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). 	<p>nuBridges Protect is role-based and therefore audit information is only available to the administrator and users with access to the audit information. Audit logs are encrypted and signed so it can be determined if the information has been tampered with. Also audit logs can be replicated in an "Audit Vault" so that if the original files are removed, the information is still preserved for audit.</p>