



SOLUTION BRIEF

# Complying with PCI Data Security Policies

## PCI 1.1 Compliance Matrix

**EXECUTIVE SUMMARY:** Retailers, financial institutions, data processors, and any other vendors that manage credit card holder data today must adhere to strict policies for ensuring that data is secure at all times. Whether they're working with American Express, Discover, MasterCard, Visa, or any other credit card issuer, these organizations face steep penalties, including fines and lost business, if this data is stolen. Ingrian can help address many of the critical security challenges of adhering to credit card issuer policies pertaining to data privacy within the enterprise.

### Regulation Overview

Last updated in September 2006, the Payment Card Industry (PCI) Data Security Standard is backed by all major credit card issuers, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International. While this standard features mandates on everything from changing employee passwords regularly to deploying firewalls, many rules focus on the security of data while it is stored within the enterprise.

Ingrian can help address many of the critical challenges of ensuring the security of sensitive data within the enterprise and adhering to credit card issuer policies.

In the pages that follow, we provide some specific requirements from the PCI standard, and illustrate how Ingrian can help address these specific mandates.

### PCI Data Security Standard

#### Regulation Specifics\* and How Ingrian Can Help

Regulations	How Ingrian Addresses
<p><b>Requirement 3: Protect stored cardholder data</b></p> <p>Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.</p>	<p>Ingrian delivers encryption capabilities that ensure the security of sensitive data, supporting standard, robust encryption algorithms.</p>

<b>Regulations</b>	<b>How Ingrian Addresses</b>
<p><b>Requirement 3.4</b></p> <p>Render PAN [Primary Account Number], 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:</p> <ul style="list-style-type: none"> <li>o Strong one-way hash functions (hashed indexes)</li> <li>o Truncation</li> <li>o Index tokens and pads (pads must be securely stored)</li> <li>o Strong cryptography with associated key management processes and procedures.</li> </ul>	<p>Ingrian supports strong cryptography encryption algorithms, including 3DES and AES 256-bit. Ingrian also supports DES, AES 128-bit and 192-bit, RC4 (40-bit and 128-bit) and RSA. (DES and RC4 are not generally recommended for protecting data at rest in production environments.) Ingrian also supports HmacSHA-1 hashes.</p> <p>Furthermore, Ingrian features secure key generation, secure key storage, and secure key management via a hardened hardware platform. Ingrian’s key management and security architecture includes both hardware and software based components that ensure secure key management and compliance with PCI.</p>
<p><b>Requirement 3.5.1</b></p> <p>Restrict access to keys to the fewest number of custodians necessary.</p>	<p>Ingrian centralizes the storage and management of keys on a single, dedicated security appliance—where all keys are stored encrypted and integrity checked within the platform, and are never available in plaintext to anyone.</p> <p>Access to keys may be restricted to designated key owners or groups of Ingrian users. More granular levels of permissions may also be granted based on key operations (Encrypt/Decrypt, Sign/Sign Verify, and MAC/MAC Verify) and key access (Time-based and rate-based) via Ingrian’s centralized policy management capabilities.</p>
<p><b>Requirement 3.5.2</b></p> <p>Store keys securely in the fewest possible locations and forms.</p>	<p>Ingrian centralizes the storage and management of encryption keys on a single appliance (or more typically an integrated cluster of dedicated security appliances)—where all keys are stored encrypted and integrity checked within the platform, and are never available in plaintext to anyone. Keys are encrypted using a multi-layered hierarchy of key encryption keys. Additionally, Ingrian offers a FIPS 140-2 Level 3 option that supports the U.S. government requirements to ensure that key management is tamper resistant.</p> <p>Encryption keys are also handled securely from an operations perspective. For example, when keys are replicated across clustered Ingrian devices or with remote Ingrian devices configured for disaster recovery, the keys are always encrypted. When keys are backed up, the keys (and any other Ingrian configuration information) are additionally encrypted in the backup configuration file.</p>
<p><b>Requirement 3.6</b></p> <p>Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:</p> <p>3.6.1 Generation of strong keys</p>	<p>With Ingrian’s solution, cryptographic keys never leave the DataSecure platform. The only way to access the DataSecure platform is at the administrator level, via a secure Web-management console, a command line interface over SSH, or a direct console connection. The platform can be configured so that individual administrators are granted access only to areas for which they are responsible.</p>

Regulations	How Ingrian Addresses
<p>3.6.2 Secure key distribution</p> <p>3.6.3 Secure key storage</p> <p>3.6.4 Periodic changing of keys</p> <ul style="list-style-type: none"> <li>o As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically</li> <li>o At least annually.</li> </ul> <p>3.6.5 Destruction of old keys</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>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 stating that they understand and accept their key-custodian responsibilities.</p>	<p>Ingrian offers a FIPS 140-2 Level 3-compliant hardware security module, which supports the U.S. government requirements to ensure that key management is tamper resistant. Following are some additional details around how Ingrian addresses specific requirements:</p> <p>3.6.1—Strong keys are generated in hardware using hardware based random number generation capability as provided by the cryptographic accelerators on the Ingrian device, using the Ingrian administration tools, either CLI or Admin GUI. The steps and procedures involved can easily be included in any security policy procedures.</p> <p>3.6.2—With Ingrian’s solution, cryptographic keys never leave the hardware appliance. Encryption keys are generated and always reside on the hardened appliance, and since cryptographic operations are performed on the appliance, keys need not be distributed or stored on Web, application or database servers. Ingrian also provides secure replication and secure backup mechanisms, such that keys do not leave the Ingrian platform in the clear for operational support purposes.</p> <p>3.6.3—Keys are always stored securely on the Ingrian platform. Encryption keys themselves are encrypted using a multi-layered hierarchy of key encryption keys. Additionally, Ingrian also offers a FIPS 140-2 Level 3 option where the encryption keys are stored in a tamper resistant hardware security module.</p> <p>3.6.4—Ingrian provides a key rotation mechanism that allows customers to efficiently rotate keys according to security policy.</p> <p>3.6.5—Keys are always stored on the Ingrian device in an encrypted form. The encrypted key is deleted from disk when the key is removed from the Ingrian device.</p> <p>3.6.6—Split knowledge for key creation and deletion/access is supported through our 20+ administrative ACLs. You can require that two people need to approve certain types of actions—i.e. key creation, etc.</p> <p>Additionally, split knowledge control of keys is often employed in situations in which raw key bits are stored, exposed, or accessed in the clear. Ingrian provides a more secure key storage mechanism in that the raw key bits may never be stored, exposed or accessed in the clear. With the Ingrian solution, authorized users of encryption keys have access to cryptographic operations, but not access to the raw key bits. Cryptographic operations are performed only with keys to which an authorized Ingrian user has access.</p> <p>Finally, there are ways to enforce that information shared across multiple Ingrian administrators is required before key-specific administrative operations are performed. There are also ways to enforce that multiple authentication levels are met before cryptographic operations are performed with specific encryption keys.</p>

<b>Regulations</b>	<b>How Ingrian Addresses</b>
<p><b>Requirement 4.1</b></p> <p>Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.</p>	<p>Ingrian supports SSL for transport encryption between database servers (or application servers) and the Ingrian appliance. The preference ordering of acceptable SSL ciphers and key sizes may be configured on the Ingrian appliance such that only 128-bit or higher key sizes are allowed. Ingrian generally recommends as part of our best practices to use SSL for transport encryption, however since the network connection between the Ingrian appliance and database server (or application server) is typically over the customer's private network, and not a public network, not all customers implement SSL.</p>
<p><b>Requirement 8.2</b></p> <p>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>o Password</li> <li>o Token devices (e.g., SecureID, certificates, or public key)</li> <li>o Biometrics.</li> </ul>	<p>The only way to access the Ingrian platform is at the administrator level, via a secure Web-management console, a command line interface over SSH, or a direct console connection. The platform can be configured so that individual administrators are granted access only to areas for which they are responsible. Administrative activities are logged and digitally signed in an audit log.</p> <p>Administrators may be granted permissions in 16 different categories based on their roles and responsibilities, thus enabling fine-grained administrative control. Two-factor authentication for administrative access may be enabled and enforced using digital certificates in conjunction with passwords. All administrator passwords are hashed and never exist on the Ingrian device in the clear.</p> <p>Because Ingrian administrators are distinct from users, i.e. applications or databases or end users that need to encrypt/decrypt, a built-in operational separation of responsibility is achieved between the people (administrators) who manage the device and set the cryptographic policies and the entities (users) that need to encrypt or decrypt data.</p> <p>Users have no administrative access to the Ingrian device. However, they are assigned a credential that enables them to request cryptographic operations with specific keys as allowed by Ingrian's customizable and centralized policies. Independent of two-factor authentication for administrative access, two-factor authentication for user access (to cryptographic operations) is also enforceable.</p>
<p><b>Requirement 8.4</b></p> <p>Encrypt all passwords during transmission and storage on all system components.</p>	<p>Passwords are encrypted via SSL when authentication to the DataSecure platform is performed. Within the platform, passwords are hashed so that they can never be exposed.</p>
<p><b>Requirement 8.5</b></p> <p>Ensure proper user authentication and password management for non-consumer users and administrators on all system components...</p>	<p>Ingrian provides best practices around credential management for authentication to the DataSecure platform. The platform also has an advanced set of password management options for expiry, password history, password length, and character set.</p>

Regulations	How Ingrian Addresses
<p><b>Requirement 10: Track and monitor all access to network resources and cardholder data</b></p> <p>Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.</p>	<p>Ingrian maintains an extensive set of centralized log files that provide the ability to track administrator and user activities. Log files are time-stamped and include specific administrator or user identification information. Log files are digitally signed to prevent tampering..</p>
<p><b>Requirement 10.2</b></p> <p>Implement automated audit trails for all system components to reconstruct the following events:</p> <p>10.2.1 All individual user 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>Log files include the following: System Log, Audit Log, NAE Log, Database Encryption Log, and SQL Logs. The log files may be individually configured for a desired rotation schedule, the number of log files archived on the Ingrian device and automatic off-device log transfer using secure copy (SCP) or FTP.</p> <p>Synchronization with other devices such as database or application servers may be achieved through the use of Network Time Protocol (NTP). The Ingrian device can be configured to point to an NTP source, such as a router or other network device.</p>
<p><b>Requirement 10.5</b></p> <p>Secure audit trails so they cannot be altered.</p> <p>10.5.1 Limit viewing of audit trails to those with a job-related need</p> <p>10.5.2 Protect audit trail files from unauthorized modifications</p> <p>10.5.3 Promptly back-up audit trail files to a centralized log server or media that is difficult to alter</p> <p>10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.</p> <p>10.5.5 Use file integrity monitoring and change detection software 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>	<p>As mentioned above, Ingrian's log files are digitally signed to prevent tampering. Plus, as part of the flexible set of log configuration options, Ingrian enables log files to be automatically rotated to a backup or archiving log server. As a result, an audit trail can be effectively maintained to meet audit history and legal regulations.</p>

\* Regulation specifics cited from "Payment Card Industry (PCI) Data Security Standard", version 1.1, September 2006

---

**ABOUT INGRIAN NETWORKS:** Ingrian Networks brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration, and centralized security management, DataSecure enables organizations to guard against a range of security threats, with unparalleled ease and cost effectiveness. Ingrian is a privately held company backed by such investors as Globespan Capital Partners (formerly JAFECO Ventures), Prism VentureWorks, HighBAR Ventures, and Partech International. For more information, visit [www.ingrian.com](http://www.ingrian.com).

---

Ingrian Networks Inc.  
350 Convention Way  
Redwood City, CA 94063  
650.261.2400  
866.INGRIAN  
[www.ingrian.com](http://www.ingrian.com)

