



Whitepaper
Guide to PCI DSS 1.2 Compliance
with Voltage SecureData

Contents

Introduction.....	3
Why PCI Compliance Is Complex.....	4
Voltage SecureData Summary.....	4
The Twelve PCI Requirements and Voltage SecureData.....	5
Conclusion	8

Introduction

With the introduction of PCI DSS 1.2, organizations processing and storing credit card data must define a program for strict compliance to a set of well-defined audit requirements in twelve areas of cardholder data management and privacy. Compliance with the regulation can be painful and disruptive, even without careful planning and consideration for pending requirements¹ such as end-to-end encryption. Compliance costs can increase substantially if adhoc technical approaches are adopted. A Particularly challenging requirement is PCI DSS Section 3: Encryption and Key Management. Any non-compliance can result in substantial fines and re-work, as well as additional audit scrutiny—all of which are invasive and costly. Thus it is imperative that organizations requiring PCI DSS compliance review technologies such as Voltage SecureData to:

- Reduce the risk of failure.
- Fast track compliance at minimal cost.
- Eliminate substantial IT change and business disruption.
- Avoid fines and increased PCI audit scope.
- Quickly enable best practices in encryption today, avoiding future change.

Voltage SecureData has already taken major Tier 1 merchants, some with over 3,500 retail stores and 20 million customers, to PCI compliance in less than 4 weeks, including integration with legacy card data warehouse operations, messaging systems, retail processing systems, card processing POS environments, reporting, and mission critical business platforms.

This document provides an overview of how Voltage SecureData can quickly address the PCI DSS requirements and, at the same time, provide convenient, transparent, and pain-free encryption services to the enterprise, allowing PCI compliance to become a best practice for data protection and data leakage prevention for any regulated or sensitive data.

“Becoming PCI-compliant is painful because it disrupts your company’s operations and security agenda. If you want to take credit cards, however, you have to be compliant, no matter how much disruption it causes or how costly the effort is.”

“Don’t be afraid of encryption. In the worst-case scenario of a breach, encryption is a lifesaver (or job saver). Make certain that if attackers do get to your cardholder data that it’s encrypted and unusable.”

John Kindervag, Forrester Research Whitepaper “Confessions Of A QSA: The Inside Story Of PCI Compliance”, September 2008

¹ The PCI Security Standards Council that manages the PCI DSS standards is in discussions with member organizations regarding the need for end-to-end encryption of cardholder data for the 2009 and beyond versions of the standard. Voltage Security is a member of the PCI Association (<https://www.pcisecuritystandards.org/>)

Why PCI Compliance Is Complex

At first glance, PCI compliance may seem simple; after all, the focus and intent is to either eliminate credit card data from systems or to encrypt the data if it is stored, and to form a policy framework protecting card processing systems and their data. However, PCI DSS is a comprehensive risk management strategy that covers people, systems, and process.

PCI DSS Compliance is not a one-time task. It is a continuous process with continuous assessment. Thus, any solution for compliance must handle the complexity of managing data privacy and system integrity over time, and across multiple business domains and boundaries.

Encryption has traditionally been very complex. Requirements such as support for aging legacy systems, managing encryption keys, encryption key rollover, dual controls, and the need to have separate views of card data on a “need to know” basis between customer service representatives, fraud investigators and administrators can make the task for compliance daunting. Consequently (and this is especially true for legacy systems), many organizations resort to costly and complex compensating controls, which increase costs and inhibit business, through the need for dedicated human resources and changes to business processes.

Fortunately, and for the first time, with innovations such as AES Format-Preserving Encryption and Voltage’s transparent and automated key management, Voltage SecureData takes away such inhibitors to comprehensive compliance, allowing PCI compliance to be achieved easily and quickly with minimal disruption.

Readers are encouraged to request the Voltage Security whitepapers on the Voltage SecureData solution for further details on how the technology works, and how it has successfully solved complex PCI and enterprise encryption problems.

Voltage SecureData Summary

Voltage offers unique encryption technology that protects information and prevents data leakage, targeting data protection requirements such as PCI DSS, GLBA, Identity Red Flag, SB1386, and so on. The Voltage SecureData product takes advantage of the U.S. government standard AES encryption algorithm in an advanced mode known as “Format-Preserving Encryption”² (FPE). FPE allows organizations to encrypt data fields like credit card numbers, government tax ID numbers, and names and addresses such that the encrypted versions match the format of the originals, thus avoiding the need to change database schema, screens, and processing systems dependent on a given data format — such as POS processing systems.

Multiple levels of encryption enable role-based access to data: customer service representatives might see only the last four digits of an account or Social Security number,

² Refer to US Government NIST Website on AES Modes, FFSEM Mode AES

whereas fraud investigators or other applications (such as a payments gateway for credit card processing) might need the full field. With FPE, since the data format is unaltered, only "trusted" applications need changes — typically one or two lines of code — as most components can just use the encrypted value as is without change. And since SecureData is a multi-platform solution, data can reside encrypted in the database, traverse the network, and be decrypted by the application only when it reaches its final destination.

Combined with transparent simplified key management and full audit capabilities, Voltage SecureData adds controlled encryption technology to existing applications very easily for regulatory compliance — and without the key management headaches accompanying legacy solutions.

Voltage Security’s unified technology for data protection extends to protecting files and email, so content can also be protected to meet PCI needs across business boundaries and internally across domains. Please contact Voltage for additional information on our unified approach to enterprise data protection with our SecureFile and SecureMail solutions.

The Twelve PCI Requirements and Voltage SecureData

The fundamental principles of PCI DSS (1.1, 1.2) compliance are based on twelve tenets representing established best practices in handling sensitive data. Compliance programs and enterprise policies developed to address to PCI can also be extended to embrace wider enterprise encryption requirements as a framework for encryption best practices beyond PCI. Voltage SecureData applies to many of the twelve tenets. In addition, due to the unique technologies used, SecureData also provides compliance benefits to other areas of the twelve requirements beyond the section relating to encryption of cardholder data.

This section provides a high-level summary of Voltage SecureData’s capabilities with respect to PCI compliance scope.

PCI DSS Tenet	PCI DSS Requirement	Voltage SecureData
Build and Maintain a Secure Network	<i>Requirement 1:</i> Install and maintain a firewall configuration to protect cardholder data <i>Requirement 2:</i> Do not use vendor-supplied defaults for system passwords and other security parameters	These requirements focus on the management, maintenance, and configuration of traditional network perimeter and segmentation firewall systems. These sections are not strictly applicable to SecureData, although SecureData does not introduce any additional network complexity and uses standard ports and communications protocols for network communications (SSL), so network and firewall changes are minimized during SecureData implementation.

Protect Cardholder Data	<i>Requirement 3: Protect stored cardholder data</i>	<p>SecureData meets and exceeds all requirements of Section 3.</p> <ol style="list-style-type: none"> 1. Data is persistently encrypted from the point of capture (POS, Web Form, data warehouse load, etc.) to the point of consumption by applications (lookup, payment, reversal, investigation, discovery, etc.). This meets PCI DSS 1.2 and emerging PCI 2009 “end-to-end” application-to-database encryption requirements. 2. AES Format-Preserving Encryption encrypts data without changing field formats or schemas, minimizing change and thus implementation costs. Any intermediate system that transmits or processes credit card PAN data does not need to change — the encrypted data can retain the full format of a valid credit card field, strongly encrypted per PCI DSS requirements. 3. AES Format-Preserving Encryption (FPE/FFSEM Mode AES) is a published (NIST AES website) and proven method of using AES in a mode that retains field format without sacrificing strength or security. FPE was developed through ten years of cryptographic research and public scrutiny. 4. SecureData can also be used to create test data to eliminate live cardholder information from test and QA systems while still permitting full testing on valid format data. 5. Key Management is automated and transparent, including automation of key rollover tailored to any business and operational requirements. Full separation of duties (data, keys) and PCI compliance reporting are standard with Voltage SecureData. 6. Voltage SecureData’s service-oriented design also reduces PCI audit scope, ensuring minimum audit costs and automation of PCI compliance. 7. SecureData is agnostic of underlying databases and application infrastructure, with a choice of integration options based on performance, architecture, and distribution requirements of components. 8. Provides a robust, highly scalable, and easy to manage redundant infrastructure without complex networking.
	<i>Requirement 4: Encrypt transmission of cardholder data across open, public</i>	<p>SecureData meets and exceeds all requirements. Data remains encrypted at all times, removing the need for additional data-in-motion solutions, and reducing costs.</p>

	<p>networks</p>	<p>In addition, for bulk unstructured data such as Card Data Warehouse load arrays arriving from partners, bulk retail store data, payroll information, etc., the same unified key management architecture for SecureData can manage keys for bulk unstructured data using Voltage SecureFile. This provides a complete solution, under a single enterprise encryption framework, including a single point for policy enforcement, auditing and reporting, management and monitoring.</p>
<p>Maintain a Vulnerability Management Program</p>	<p><i>Requirement 5:</i> Use and regularly update anti-virus software</p> <p><i>Requirement 6:</i> Develop and maintain secure systems and applications</p>	<p>This does not apply to Voltage SecureData, though meeting this requirement is not inhibited, and Voltage’s other solutions for Secure Email, protecting data exiting an organization over SMTP (in scope of PCI if email contains even a single credit card number), are unique in their ability to work with DLP, AV, and content inspection tools for electronic supervision.</p> <p>Voltage SecureData is based on the FIPS 140-2 certified Voltage Security Encryption toolkit³. The Voltage SecureData Web Services framework also allows secure applications to be built quickly and easily, by confining encryption and key management functions to a unified architecture, reducing PCI audit scope and compliance costs. Encryption, decryption, and management of sensitive data can be confined to an enterprise service, facilitating rapid design and integration in hours or days, and keeping compliance costs to a minimum.</p>
<p>Implement Strong Access Control Measures</p>	<p><i>Requirement 7:</i> Restrict access to cardholder data by business need-to-know</p> <p><i>Requirement 8:</i> Assign a unique ID to each person with computer access</p> <p><i>Requirement 9:</i> Restrict physical access to cardholder</p>	<p>SecureData meets and exceeds this requirement. Separation of duties is handled inherently by Voltage SecureData. Data remains persistently encrypted at all times — in the database; as it travels; in logs and files — until the data is needed by permitted applications or staff. SecureData can take advantage of existing identity and access management systems to provide role-based access to data while key management is fully separated from the data, enforcing separation of duties at all times.</p> <p>SecureData indirectly assists in meeting this requirement, since access to data can be driven optionally by existing identity and access management infrastructure, used to manage unique IDs. SecureData provides role-based access to the data itself, allowing existing investment in RBAC models and technology solutions to be re-used immediately.</p> <p>Not applicable to Voltage SecureData.</p>

³ <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt522.pdf>

	data	
Regularly Monitor and Test Networks	<i>Requirement 10:</i> Track and monitor all access to network resources and cardholder data	SecureData provides complete audit records in a PCI DSS-ready format for rapid audit and investigation compliance. When cardholder data is persistently encrypted, access to data is only permitted by policy-based access, which simplifies meeting this requirement.
	<i>Requirement 11:</i> Regularly test security systems and processes	Not specifically applicable to Voltage SecureData. However, the SecureData infrastructure can easily be tested at any time for correct operation, backup, restore, failover, and other business continuity functions, per this requirement.
Maintain an Information Security Policy	<i>Requirement 12:</i> Maintain a policy that addresses information security	Use of Voltage SecureData for comprehensive data protection of cardholder data allows written policies to be enforced at the data level. This data-centric approach to PCI compliance brings security policy-based control and, more, importantly, allows the organization to easily prove compliance to auditors through compliance attestation reports on a direct basis.

Conclusion

PCI DSS compliance can be a complex process, and introduce costly ongoing costs to the business, with invasive audits and continuous compliance assessments. Encryption can reduce the need for increasing costs, relating to compensating controls and their people and process impacts. However, in the past, encryption has been complex, invasive and difficult, especially in legacy environments.

Voltage SecureData addresses this complexity head on, resulting in an enterprise encryption platform that is not only easy to use and integrate into complex and high scale card processing infrastructure for PCI compliance, but also as an extensible platform for any private data privacy requirements such as protecting government tax IDs, Social Security numbers, name and address, and so on, for enterprise and business applications both internal and external.

For further information and to see how Voltage can quickly address your PCI compliance needs, please contact a specialist via <http://www.voltage.com/pci> or via info@voltage.com