Zettaset

SOLUTION BRIEF

PCI / DSS Compliance & XCrypt™ Data Encryption Software Solutions

Data within distributed cloud and data center environments is fluid, as data is replicated in many places and moves as needed. Security must be consistently applied and enforced across a distributed computing environment. The Zettaset XCrypt(TM) Data Encryption Platform has been designed from the ground up to address the unique big data security challenges presented by these complex, distributed computing environments.

PCI / DSS (Payment Card Industry / Data Security Standards)

The term "PCI" refers to the Payment Card Industry Security Standards Council, a group originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International in 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standards.

The PCI Council formed a body of security standards known as the PCI Data Security Standards, consisting of 12 significant requirements including multiple sub-requirements which contain numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines.

By complying with qualified assessments of these standards, businesses can become accepted by the PCI Standards Council as compliant with the 12 requirements, and thus receive a compliance certification and a listing on the PCI Standards Council website. Compliance efforts and acceptance must be completed on a periodic basis.

The PCI Council compliance within any card handling business' security process can be considered part of inter-related disciplines of governance, risk, and compliance (GRCM), as well as part of information security.

Meeting PCI DSS v3.2 Security Compliance Requirement Standards with Zettaset

Payment Card Industry Data Security Standards (PCI DSS) compliance mandates that all organizations that accept, acquire, transmit, process, or store cardholder data must take appropriate steps to continuously safeguard all sensitive customer information.

The Zettaset XCrypt Data Encryption Platform provides PCI DSS security compliance solutions that secure and control enterprise data at rest, addressing critical portions of the PCI DSS v3.2 compliance control set for PCI DSS compliance requirements 3, 4, 7, 8 and 10 while also supporting additional components of the PCI DSS compliance requirements.

- **Requirement 3:** Protect secured cardholder data
- **Requirement 4:** Encrypt transmission of cardholder data
- **Requirement 7:** Restrict access to cardholder data by business need to know
- **Requirement 8:** Identify and authenticate access to systems components
- **Requirement 10:** Track and monitor access to network resource and cardholder data

PCI DSS security compliance solutions address encryption, access control, encryption key management and granular logging requirements across multiple use cases within the PCI DSS v3.2 compliance requirements — protecting unstructured files, structured databases as well as specific fields or columns within databases and files across traditional data centers, virtual environments, cloud implementations and big data environments.

This unified software-based solution to multiple PCI DSS security compliance requirements under the standard helps organizations meet PCI DSS v3.2 compliance requirements with an easy-to-deploy, centrally managed solution set.

Key features and benefits include:

- **Encryption and Access Controls:** Cardholder data can be encrypted for files and volumes, and file- and volume-level access is controlled and logged
- **High Performance:** Optimized for big data scalability in distributed computing architectures, resulting in minimal impact on SLAs and application latency
- **Auditing and Monitoring:** Log data is available for easy integration with auditing tools and Security Information and Event Management (SIEM) systems
- **Broad Database and Cloud Coverage:** Supports Relational, Object, NoSQL, and Hadoop, data environments; Deployable in the cloud or on-premises
- **Rapid deployment:** An all-software approach to encryption simplifies implementation and eases expansion in elastic cloud and extended enterprises, helps meet audit deadlines, and minimize deployment costs

Zettaset XCrypt Data Encryption Platform Support for PCI Data Security Standard Compliance

The following table outlines specific areas within the PCC/DSS where the Zettaset XCrypt Data Encryption Platform can assist financial organizations to achieve compliance.

Mandate	PCI DSS v3.2 Requirement	Zettaset XCrypt Platform Capabilities
Data should be rendered unreadable – anywhere that it is stored.	PCI DSS Compliance Requirement 3: Protect stored cardholder data. 3.2, 3.4, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6	Zettaset supports volume-level and file-level encryption with XCrypt Full Disk (volume) and XCrypt Hadoop (file).
Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals.	PCI DSS Compliance Requirement 4: Encrypt transmission of cardholder data across open, public networks. 4.1, 4.2	Zettaset supports volume-level and file-level encryption with XCrypt Full Disk(volume) and Zettaset XCrypt Hadoop (file).
Only users and resources that must access cardholder data in order to complete their job should have access to systems containing cardholder data.	PCI DSS Compliance Requirement 7: Restrict access to cardholder data according to business need to know. 7.1, 7.2	XCrypt adds access control on top of native operating system capabilities for both local system roles and directory services capabilities. It restricts privileged user role access, allowing them to perform their work, but decrypting data only for users and processes authorized by a centralized policy server.
Protect authentication credentials with strong cryptography; restrict access to databases containing cardholder data to DB administrators and the application.	PCI DSS Compliance Requirement 8: Identify and authenticate access to systems components. 8.1, 8.2.1	XCrypt integrates with existing directory services to authenticate user IDs, and uses access policies to encrypted data to limit direct access to database administrators and the database process.
Audit trails must be present for access to networks and cardholder data by system components, administrators and users.	PCI DSS Compliance Requirement 10: Track and monitor all access to network resources and cardholder data. 10.1, 10.2, 10.3	With XCrypt, audit logs of all access (and access attempts) to encrypted file system and volume level data, by all users and processes, are collected and made available for analysis.

For more information, please contact us at +1.650.314.7920 or sales@zettaset.com