EVERTRUST

Whitepaper

Ensuring PCI-DSS V4.0 Compliance

Beyond PCI-DSS: Comprehensive Regulatory Compliance

In March 2022, the Payment Card Industry (PCI) released version 4.0 of the Data Security Standard (DSS).

The new version introduces 64 additional requirements, with a focus on Public Key Infrastructure (PKI) and associated software architecture, posing significant challenges for organizations involved in payment card processing.

As the compliance deadline approaches, organizations involved in payment card processing must prepare to meet these rigorous standards in order to avoid the financial penalties and loss of credibility or reputation that can result from non-compliance.

Beyond PCI-DSS, EVERTRUST Horizon provides robust support for compliance with other critical regulations such as ISO 27001, HIPAA, GDPR, as well as various Central Bank regulations and country-specific laws.

EVERTRUST Stream (high-performance CA software) and OCSP solutions enhance your ability to meet various compliance and regulatory requirements.

As executives in charge of financial management, the introduction of PCI-DSS V4.0 represents a critical transition for compliance and risk mitigation. The transformation of the regulatory landscape, combined with the increasing complexity of cyber threats, underscores the importance of maintaining strong cryptographic practices and a strict certificate management system.

How EVERTRUST Horizon Meets These Challenges:

EVERTRUST Horizon offers a comprehensive, advanced CLM solution that aligns seamlessly with PCI-DSS V4.0 requirements. For financial institutions, this translates into a robust compliance framework that mitigates risks and supports secure, uninterrupted operations.

Strong cryptography is needed to protect Primary Account Numbers (PANs) and requires comprehensive support from people, procedures and technology.

CRYPTOGRAPHY STRENGTH

- Continually assesses the cryptographic strength of your systems, ensuring they meet the latest NIST standards.
- Provides you with detailed technical and management reports to assist you in developing audits and verifying compliance
- Protects sensitive financial data, helping to prevent data breaches that could result in significant financial penalties and loss of customer confidence.

EXHAUSTIVE INVENTORY OF CERTIFICATES AND KEYS

- Provides a real-time view of all certificates and keys, facilitating efficient management and decreasing the risk of unmanaged or expired certificates.
- Simplify effective certificate lifecycle management.
- Prevent unauthorized access to financial systems by ensuring that all cryptographic resources are accounted for and managed securely, protecting potential financial losses due to security errors.

How EVERTRUST Horizon Meets These Challenges:

TRUST IN THE CERTIFICATION AUTHORITY

- Ensures that only trusted CAs are recognized within your institution's policy framework, maintaining compliance with PCI and CPS requirements.
- Ensures organizational control over cryptographic keys minimizing the risk of unauthorized access and potential financial leakage.
- Ensures that financial data and transactions managed by institutions remain secure and reliable, reducing the risk of operational disruptions due to compromised certificates.

NO FALLBACK TO INSECURE PROTOCOLS

- Actively monitors and reports protocol configurations to prevent such rollbacks.
- Deployment flexibility ensures secure configurations in a variety of environments.
- Protects sensitive financial data, helping to prevent data breaches that could result in significant financial penalties and loss of customer confidence.
- Allows all financial transactions to be conducted securely, reducing the risk of cyber threats that could compromise the security of your institution's financial operations.

In conclusion

By leveraging the extensive capabilities of EVERTRUST Horizon and EVERTRUST Stream, organizations can ensure robust cryptographic practices and seamless certificate lifecycle management.

This dynamic approach not only greatly helps handling the compliance, but also improves the overall cybersecurity posture, protecting sensitive payment card data.

Whitepaper

Ensuring PCI-DSS V4.0 Compliance with EVERTRUST