



SOLUTIONS: XiSecure On-Demand

With XiSecure On-Demand, Paymetric's tokenization solution, merchants can render a security breach futile and reduce the cost and scope of PCI compliance.

THE PROBLEM

Merchants who store credit card data are fast becoming a target of choice for cyber criminals. As the number of data security breaches steadily rises, merchants face heightened pressure to secure their payment systems against data theft. The advent of the Payment Card Industry Data Security Standard (PCI DSS) and the demand to protect stored-cardholder data have driven merchants to invest in costly security solutions that may still leave their systems vulnerable to attack.

There were 50% more data breaches in 2008 than in 2007 with an estimated 35.7m individuals affected.¹

Merchants who store credit card numbers on-site are accountable for meeting PCI DSS requirements and invite unnecessary risk. Finding secure and cost-effective solutions to meet those requirements can be a daunting task. From large corporations to individual users, protecting sensitive information remains paramount – as failure to do so can result in irreparable brand damage and financial loss.

The total cost of a data breach grew to \$202 per record compromised, an increase of 2.5% since 2007.²

THE ANSWER

XiSecure On-Demand, Paymetric's tokenization solution, affords companies the opportunity to eliminate the transmission and storage of sensitive cardholder data, which radically improves data security while quickly reducing the scope and financial burden of PCI compliance. Merchants no longer transmit or store credit card numbers, yet can continue to conduct business as usual with "tokens" that span the entirety of the customer relationship. With no credit card numbers to be compromised, merchants are less exposed to a credit card security breach.

HERE'S HOW IT WORKS

XiSecure On-Demand is a technology that works by intercepting cardholder numbers entered into enterprise payment acceptance systems and replacing it with a surrogate value known as a "token." A "token" is a unique ID created to reference the actual data associated with the card number. The card number is stored off-site in Paymetric's secure, PCI-compliant data vault. This token can be passed throughout an enterprise to meet the demands of customer interactions and to support customer analytics. All of this is done without disruption of day-to-day business activities.

SOLUTIONS: XiSecure On-Demand

BENEFITS:

Reduced Scope and Cost of a PCI DSS Audit

When encountering a PCI DSS audit, all systems, applications and processes that have access to RAW or encrypted credit card numbers are considered “in scope” for a PCI DSS audit. However, substituting tokens for credit card numbers within the systems, applications and processes will render the data useless and will never require access to the token’s underlying value. The credit card numbers are not stored on-site and those merchant systems (where RAW card numbers are never entered or displayed) are considered “out of scope” for PCI Requirement 3 and do not need to be audited for compliance.

Accelerate Time to PCI Compliance

With Paymetric’s Software as a Service (SaaS) platform, organizations can quickly and easily deploy the **XiSecure On-Demand** solution, resulting in a decrease in time spent to achieve and maintain compliance with the PCI DSS.

Increase Security and Protect Your Brand

With Paymetric’s tokenization solution, **XiSecure On-Demand**, card numbers are never stored intact – anywhere, making it impossible for hackers to reassemble them through decryption or reverse engineering. This increased security allows companies to preserve their brand without the worry of unexpected fees, fines or legal costs associated with a data breach.

Works in any Enterprise Payment Acceptance System

With **XiSecure On-Demand**, cardholder data can be tokenized from anywhere payments originate within enterprise systems such as SAP,[®] legacy ERP and CRM systems, POS, order entry systems, web stores and call centers. With Paymetric’s **XiSecure On-Demand** solution, you can take comfort in the fact that all of your systems are safe.

STANDARD FEATURES:

- Removes stored credit card numbers from enterprise application databases
- Replaces credit card numbers in enterprise applications with tokens
- Stores tokens in an off-site, centralized and secure data vault
- Provides key management processes outside of enterprise applications, thus eliminating system and application down time
- Provides key rotation capabilities outside of enterprise applications
- Provides access logging for decryption requests
- Provides monitoring of decryption requests
- High availability –24x7 operation is supported via high availability mechanisms such as load balancing and database clustering
- Integrated back-up
- Disaster recovery - a disaster recovery site provides recovery from total-site outages

VALUE-ADDED SOLUTIONS:

Data Intercept Solutions: Tokens are generated outside of enterprise payment acceptance applications to ensure that sensitive cardholder data never enters the merchant environment. This solution integrates with any enterprise payment acceptance system.

ERP Integration Kits: A tokenization solution that is seamlessly integrated into sales order modules and ensures that sensitive data is never stored within your ERP systems. Instantly eliminate your system from the scope of PCI Requirement 3 and reap the financial and security benefits of integrated and secure electronic payment acceptance.

SECURE ENTERPRISE PAYMENT ACCEPTANCE SOLUTIONS



Paymetric, Inc. / 19500 SH 249, Suite 300 / Houston, Texas 77070 / tel 713-895-2000 / fax 713-895-2001 / www.paymetric.com

Copyright 2009 Paymetric, Inc. All rights reserved. Paymetric and Paymetric Solutions are either registered trademarks, service marks, or trademarks of Paymetric, Inc. in the United States and/or other countries. Other trademarks appearing on this document are the property of their respective owners. The names of third parties and their products referred to herein may be trademarks or registered trademarks of such third parties. All information provided herein is provided "AS-IS" without any warranty. *Washington Post, 1/6/2009. *2008 Annual Study: Cost of Data Breach, Ponemon Institute 2009. 07-2009/PM009