

A Proven Data Security Methodology for Modern Regulatory Compliance

The modern enterprise architecture is often a complex environment, consisting of many disparate systems and network tiers. The workhorses of these architectures are often closed systems—mainframes, third-party databases, enterprise resource planning (ERP), or customer relationship management applications. Protecting these assets can be a daunting task.

For architects and security stakeholders looking to implement strong data security policy within their existing enterprise architecture, this brief presents a path toward data security that is not reliant upon retrofitting every closed system.

The Path to Encryption

Typically customers facing tough regulatory compliance mandates around data security, such as the Payment Card Industry Data Security Standard (PCI DSS), Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), or the increasing number of state notification laws, go through a standard evolution of questions:

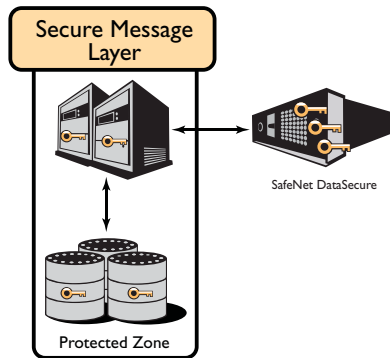
- **Can we delete the data?**
Why spend money protecting what you don't need? If you can eliminate the sensitive data, do it.
- **Can we mask the data?**
Is the sensitive data element ever used externally? Or is it used in such a way that only the original number will do? If not, hide it with an element of the same size and move on.
- **How can we encrypt the data?**
If sensitive data at rest cannot be deleted or masked, it must be encrypted for both regulatory compliance and as a best practice. But the process of encrypting data within a large enterprise can be daunting, and choosing a starting point even more so.

Common Encryption Hurdles

Encryption is not a new concept, but full scale mobilization of commercial off-the-shelf (COTS) products for data security is. These days, many vendors are “baking in” their own encryption or are being paid by their customers to do this on a by request basis. Data in these systems must be constantly encrypted and decrypted as it passes from one encrypted system to another.

Key management is an important consideration in a company's enterprise encryption strategy. And managing keys across various systems can be a difficult task. Even more troubling are those closed systems that have not implemented encryption. Many vendors either don't consider data security to be an issue their products need to address or are without the know-how to implement cryptography. In addition, many large enterprises actively use hardware and software that have reached end of life.

Can a large enterprise steer around these issues with a comprehensive encryption policy? The most common method is to select a logical starting point and use an enterprise-class appliance such as the SafeNet DataSecure platform, which will allow an enterprise to evolve their encryption policy as time goes on. Others have taken a different approach through the creation of a tokenization system.



Key Benefits

- Compliance with PCI DSS, HIPAA, and PII policies
- Full cryptographic strength through encryption
- Leverages SafeNet DataSecure as encryption policies evolve

Introduction to Tokenization

Tokenization is not a complicated concept. The system takes sensitive data values and replaces them with values (tokens) of the same size and type. Legacy systems that expect 16 byte credit card numbers or 9 byte Social Security numbers will receive 16 or 9 byte tokens. These tokens will reference sensitive data, but not actually be sensitive themselves. Sensitive data will be encrypted and stored in the tokenization system.

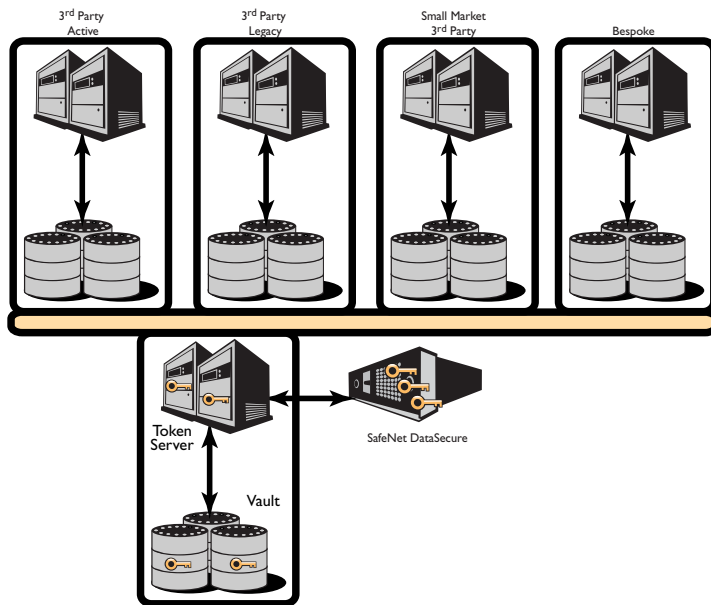
Tokenization is simple architecturally as well. A standard tokenization system consists of two pieces:

- The **Protected Zone**, a basic client-server middleware application and database
- The **Secure Message Layer**, for all necessary systems to input and retrieve sensitive information

A middleware application in the protected zone performs all security functions of authentication, as well as encryption/decryption, and can be involved in token assignment. All databases in the protected zone are responsible for simple storage of encrypted data and its token. Database in the protected zone can be easily locked down, as access should only come from one source, and communication will be highly predictable.

SafeNet Tokenization Solution

SafeNet Professional Services, in conjunction with SafeNet DataSecure, provides your enterprise with a full cryptographic tokenization solution that can evolve over time into a more comprehensive encryption solution that meets the most complex requirements.



With the SafeNet DataSecure tokenization deployment solution:

- Data comes in through a consumer system
- Data is passed through the Secure Message Layer into the Protected Zone
- Token Server calls DataSecure to encrypt the data, stores ciphertext in the Vault and returns a token
- Another consumer system passes tokens through the Secure Message Layer
- Token Server decrypts and returns clear text

SafeNet EDP

DataSecure is a key component of SafeNet's comprehensive Enterprise Data Protection (EDP) solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet EDP is the only solution that secures data across the connected enterprise, from core to edge, with protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit www.safenet-inc.com/edp.



www.safenet-inc.com

Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel.: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

©2009 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. SB-DataSecure Tokenization Solution-07.15.09