White Paper

Tokenization

A Cost-Effective and Easy Path to Compliance and Data Protection

As companies work to meet regulatory requirements to protect Personally Identifiable Information (PII) such as credit card numbers and social security numbers, one option to minimize the risk of loss is to replace sensitive data with a non-sensitive replacement value, or "token." This white paper discusses the ways in which tokenization is implemented, the effectiveness of tokenization in meeting regulatory requirements, and the impact on your IT systems and business processes.

Townsend® SECURITY

www.townsendsecurity.com

724 Columbia Street NW, Suite 400 • Olympia, WA 98501 • 360.359.4400 • 800.357.1019 • fax 360.357.9047 • www.townsendsecurity.com

Introduction to Tokenization

Tokenization is the process of replacing sensitive information, such as a credit card or social security number, with a non-sensitive replacement value. The original value may be stored locally in a protected data warehouse, stored at a remote service provider, or not stored at all. The goal of tokenization is to reduce or eliminate the risk of loss of sensitive data, and to avoid the expensive process of notification, loss reimbursement, and legal action.

Implementing tokenization generally requires modifications to IT systems and databases. Usually there are applications that must be changed to substitute tokens for sensitive data, and some applications may need to be modified if an end user must be able to recover the sensitive information. Implementing tokenization will usually have an impact on current IT systems and business procedures.

Approaches to Tokenization

There are three primary approaches to tokenization:

- Tokens are recoverable and stored by external service providers
- Tokens are recoverable and stored locally
- Tokens are not recoverable

The first method of tokenization uses external storage of recoverable tokens and is implemented by a small number of credit card authorization networks. When a credit or debit card is authorized, the authorization response includes the token value for the card number. The merchant can store the token value locally and use it for any subsequent transaction such as payment settlement or recurring payments. The payment network stores the recoverable version of the card number and the merchant never stores the original card number.

The second approach to tokenization involves the creation and storage of the token on local IT servers. The token is protected by encryption and can be recovered by decryption when it is needed. The token value is then used in the applications and databases to help reduce the chance of loss of the sensitive data. This method can be used to protect any sensitive data such as social security numbers, drivers license numbers, and so forth.

The third type of tokenization involves the creation of a token on local IT servers, but does not allow for the recovery of the original value. The original value is not retained and there is no risk of loss of sensitive information from the token data store. This type of tokenization is rarely used in production IT systems, but can be useful in test and QA environments.

Tokenization and Recovering Protected Data

If your approach to tokenization provides for the recovery of the original value of the sensitive data, the sensitive data should be protected by strong encryption and appropriate encryption key management. Protecting the information in the tokenization database has the same requirements as protecting the data in the original database. If your tokens are stored by an external service provider, such as a payment network, they should encrypt the original data. If you store the sensitive data in a local tokenization database, you are fully responsible for protecting the sensitive data with strong encryption.

Tokenization and Regulatory Compliance

Tokenization is one of the methods of protecting data defined in Payment Card Industry data security standards (PCI DSS), state privacy notification laws, and other regulations. The use of tokenization does not satisfy a company's regulatory requirements, but may substantially reduce the impact of regulatory audits or notification requirements. Merchants who use payment system tokenization must still comply with PCI regulations, but will most likely have fewer compliance problems related to storing information.

The most effective security is provided by tokens which are stored at external service providers such as payment networks. Locally created and stored tokens which are recoverable provide very little additional security and almost no regulatory relief.

IMPORTANT: In regards to the PCI regulatory framework, tokenization provides no exemption from the PCI data security standards, or from any requirement for a PCI audit.

Local Tokenization

When tokens are created and stored locally on internal IT servers, you are responsible for the implementation, storage, maintenance, and security of the tokens. Normally the tokens are stored in a standard database so that they can be retrieved and managed easily. If the token is recoverable, the original value should be protected by strong encryption which uses appropriate encryption key management.

The challenge for most companies when implementing local tokenization is providing the proper applications to create and manage the tokens, implementing good encryption and key management, and modifying applications and databases to use tokens.

Types of Tokens

When a token is created to replace sensitive data it usually matches the original data in format and content rules. For example, when creating a token for a credit card number you may want the token to appear as an actual credit card number. For example, if you start with a credit card number of 4111222233334444 you might want to replace this value with bogus card number in the same format: 4777888899990001. Both the original card number and the substitute number appear to be Visa card numbers which always start with the number 4. A good tokenization strategy would give you the option of creating replacement tokens in this fashion. This strategy is called “Format Preserving” tokenization.

In addition to credit card numbers, you may wish to create token social security numbers, driver’s license numbers (each state has a different format), zip codes, and other data. Being able to create tokens that match the characteristics of the original data is important to maintaining the integrity of business applications and database systems. Tokens with invalid formats can cause unpleasant exceptions and errors in these systems.

Local Tokenization with Segmented Encryption Key Management

When tokens are recoverable, the original values must be protected with strong encryption and key management solutions. Best practices for implementing key management requires the separation of encryption keys from the data they are protecting. This means encryption keys should be stored on an external server and secure TLS must be used for key retrieval.

Payment networks that implement tokenization provide encryption key separation through the use of internal key management systems. When you implement local tokenization you should ensure that keys are separated from the token database. This can be accomplished by using a key management system, or using a tokenization server that implements encryption and token storage.

Tokenization and Certification

While several privacy regulations recognize the value of tokenization, there is no formal process for certifying tokenization solutions. This presents a challenge to security professionals when attempting to evaluate vendor solutions.

One area of tokenization is subject to validation through certification – encryption of recoverable tokens. A tokenization solution that encrypts the original sensitive data and allows for its recovery should use strong encryption and good key management solutions. The PCI Data Security Standards mandates the encryption of a credit card number stored in a token database. Fortunately, there is set of clear certification standards for encryption – the NIST AES Validation tests. These are rigorous tests defined by NIST and carried out by independent testing laboratories that have been charted by NIST. In addition to encryption, NIST also specifies a certification process for encryption key management solutions called FIPS-140. The combination of these two certifications apply to any tokenization solution.

Alliance AES encryption solutions have been certified to the NIST AES Validation tests, and the Alliance Key Manager solution is in the FIPS-140 certification process.

Performance Impacts of Tokenization

Deploying tokenization may have a significant performance impact on business applications. Like encryption and decryption, the use of tokens will impact performance when tokens are encrypted during token creation, and when decrypted during token retrieval. Other operations such as “query by token,” can also generate more demand on your business applications. A good practice is to evaluate a tokenization solution for performance in the project-feasibility stage before purchasing and deploying a tokenization solution.

Tokenization Audit Trails

When tokenization involves the ability to recover the original sensitive data, it is important to create audit trails when sensitive data is retrieved. In this case auditing access to sensitive information is the same as auditing access to the decryption operations. The tokenization solution you deploy should provide for the automatic creation of audit trails by security policy and not require applications developers to manually create audit entries.

Is Tokenization Right for You?

If you do not need to store sensitive data in your database systems, tokenization can greatly reduce your risk of data loss. The original sensitive data can still be used to query a database or locate information in a business application. But by not storing the sensitive data, you will not be at risk of losing it.

It is important to note that if you use recoverable tokens you will still have the risk of data loss and will not be protected from any liability for a loss. You will also still be subject to all of the regulations for protecting sensitive information.

Tokenization can be a powerful way to minimize risk in your development, QA, and UAT environments. When moving data to these environments you should always eliminate sensitive data to prevent its loss. Tokenization is an excellent way to do this.

Lastly, if you are a payment systems vendor you may wish to provide tokenization as a value added service to your merchant customers. Not only will you be helping them minimize their exposure to data loss, this can also be marketed as a competitive advantage for your business.

Tokenization for PCI Compliance

Tokenization provided by your payment system vendor can significantly reduce of your risk of a data loss. If you do not need to store a credit card number for settlement or recurring charges, your exposure is reduced to the initial authorization transaction. This is still a significant exposure, but through tokenization you can completely eliminate the exposure that stored information represents.

It is important to note that the use of localized tokens provides no reduction in your obligations to comply with PCI DSS. In this case the negative effects of performance degradation may far outweigh any benefits of tokenization.

Tokenization for Privacy Notification Compliance

Many state privacy notification laws provide a safe harbor if you encrypt or tokenize sensitive data. If you don’t need to store the sensitive data for later retrieval, tokenization provides an ideal way to reduce your level of risk. However, most Enterprise customers need to be able to recover the actual sensitive data. For example, an HR department will need to store the social security number of each employee. In this case deploying tokenization to separate the sensitive data from the production databases can significantly reduce the risk. If a production server is breached, but only contains tokenized data, you will have the safe harbor exclusion for notification. As long at the tokenized sensitive data resides on a separate secure server that has not been breached, you will have eliminated the requirement for notification.

Summary

Tokenization deserves a closer look by any Enterprise exploring their data security options. It substantially reduces data security risk and is a relatively easy path to regulatory compliance. As a method for minimizing the risk of data loss, tokenization is especially effective in IT test, QA, and UAT database environments. However, when considering implementing a tokenization solution, it’s important to carefully consider the impact on your systems performance, the commitment of vendors to encryption and NIST certification, and the ability to store data tokens separate from production data. Tokenization is gaining acceptance in the regulatory world, and will likely grow in popularity with credit card processors and any Enterprise that stores and transfers sensitive data.

Townsend Security

We know that data gets out, and that it can and routinely does fall into the wrong hands. When this happens, our solutions for encryption, key management, and system logging ensure that your Enterprise is compliant with regulations and that your sensitive data is protected.

Our data security solutions work on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. Many of these solutions are currently used by leaders in retail, health care, banking, and government.

You can contact Townsend Security for an initial consultation at the following locations:

Web:	www.townsendsecurity.com
Phone:	(800) 357-1019 or (360) 359-4400
International:	+1 360 359 4400
Email:	Info@townsendsecurity.com

A fully functional free trial is available for all Alliance products. You can evaluate Alliance capabilities on your own server systems.

Resources

PCI Data Security Standards

Visa Best Practices for Encryption and Tokenization

Townsend Security Compliance