RSA

The Security Division of EMC

RSA Solution Brief

Aligning Visa® Best Practices with RSA® Tokenization Server

Executive Summary

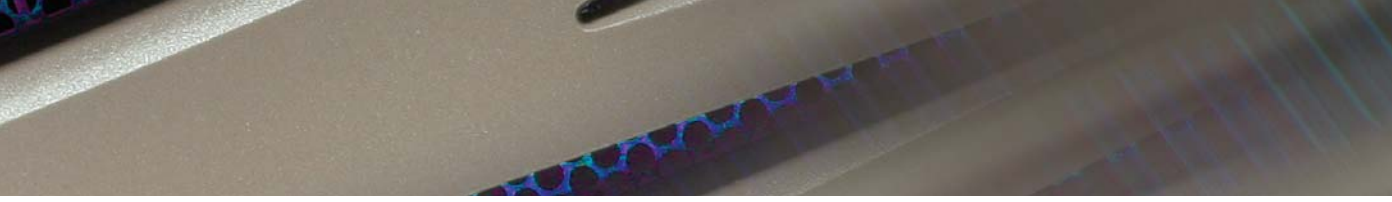
According to a Verizon Business study*, 99% of all breached records were compromised from servers or applications in 2008. Due to this, an organization interested in preventing data breaches or meeting compliance requirements must seek to protect sensitive data in the application layer, where the majority of threats reside. To date, encryption (along with strong key management) has been the preferred method of enforcing data protection in applications, but lately tokenization (also referred to as “aliasing” or “data masking”) has gained a lot of traction as an application control due to a variety of benefits.

Tokenization substitutes an arbitrary value of equivalent type and character for an element of sensitive information. In complying with PCI DSS, for example, eliminating the exposure of a credit card number both within and outside the enterprise is of paramount importance. Tokenization substitutes a different, randomly associated 16-digit number for the credit card number as soon as that credit card number is captured, such as at a point-of-sale device in the retail environment.

Tokenization has a number of unique advantages over encryption. First, tokenized values maintain their original format, reducing the amount of database schema or application changes that need to be made in order to implement. In addition, other applications can potentially make use of that data without ever having access to the real information. For example, when a social security number is tokenized, the last four digits of the original number can be preserved in the token. If another application like a call center application needed to verify the user’s identity using the last four digits of the social security number, they would never have to de-tokenize or get access to the original information.

That leads to the next business benefit of tokenization, which is reducing the scope of audits. In the same example as above, if the call center application needed to get the last four digits of the social security number using an encrypted value it would need to have access to the key management system and also decrypt the information. This puts the application in the scope of audits for compliance (i.e. state privacy laws related to PII). If a token is used, and the data is never de-tokenized, that application is out of audit scope. This can significantly reduce the amount of effort an organization devotes to compliance, and save a considerable amount of money over encryption solutions. Combine this with the same level of protection as application encryption, and you get a very compelling solution for data security.

*Verizon Business 2009 Data Breach Study, April 15th, 2009



RSA Tokenization Server in Retail Environments

RSA has implemented a comprehensive tokenization solution, which combines our industry-leading RSA Key Manager with Application Encryption with new tokenization functionality. RSA Key Manager with Application Encryption has been widely adopted by the largest retailers in the world and with the addition of tokenization capability, customers can get the benefit of the highest level of data protection with all of the cost saving benefits of tokenization.

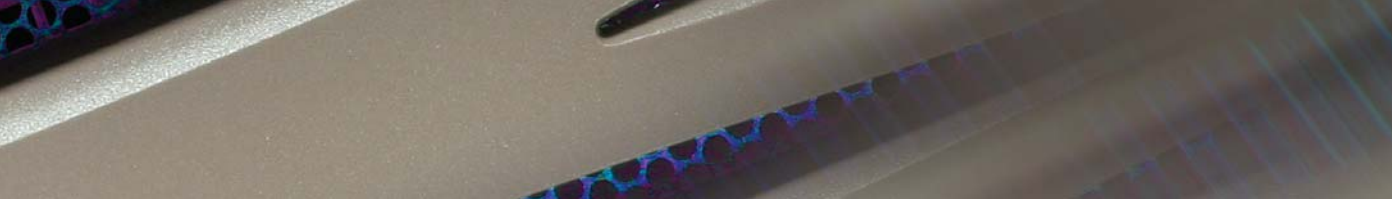
One of the most common uses for RSA Tokenization Server is within the retail environment for protecting credit card information. Tokenization fits well for payment card information because of its well-defined and consistent structure. In addition, credit card numbers can typically be tokenized at the moment of data capture and are typically needed, as a real value, in only a few applications in the enterprise. Furthermore, the tokenization of payment card information can vastly reduce the amount of data subject to PCI audit, assuming the tokenization environment aligns to industry best practices. This is because the tokens themselves have no mathematical relationships back to the original values; therefore do not have to be audited as they move into other applications or data stores.

Tokenization can be applied to many different types of data within an organization, but payment card information is by far the most regulated by industry. For this reason, RSA makes aligning with industry best practices a matter of critical importance. On July 14th, 2010, Visa announced global best practices for tokenization to provide guidance for merchants and vendors on how tokenization should properly be deployed. RSA Tokenization Server aligns with these best practices better than any other solution on the market. The table on the following pages maps each best practice authored by Visa with the corresponding RSA response.

Tokenization has unique advantages over encryption:

1. Tokenized values maintain their original format, reducing the amount of database schema or application changes that need to be made.
2. Other applications can potentially make use of that data without ever having access to the real information.
3. Reduce the scope of audits, i.e., if a token is used, and the data is never de-tokenized, that application is out of audit scope.

Domain	Best Practice	RSA Response
Tokenization System	**Network Segmentation:** The tokenization system must be adequately segmented from the rest of the network. The tokenization system must be deployed within a fully PCI DSS compliant environment and be subject to a full PCI DSS assessment.	Segmenting RSA Tokenization Server from the rest of the network is an implementation consideration and fully supported within the product. The token server is protected via RSA Key Manager to meet full PCI DSS compliance
	Authentication. Only authenticated entities shall be allowed access to the tokenization system	RSA Tokenization Server has built-in administrative roles on the server side, and makes use of RSA Access Manager to handle role based administration and access rights. Clients are authenticated via certificates to assure proper access to the server components.
	Monitoring. The tokenization system must implement monitoring to detect malfunctions or anomalies and suspicious activities in token-to-PAN mapping requests. Upon detection, the monitoring system should alert administrators and actively block token-to requests or implement a rate limiting function to limit PAN data disclosure.	RSA Tokenization Server logs failure events and those logs can be used within RSA envision® platform for correlation and monitoring. If action needs to be taken, administrators in the token server can actively send token commands to clients, such as marking a token as "compromised" or removing a client's ability to de-tokenize data.
	Token Distinguishability. The tokenization system must be able to identify and distinguish between tokenized and cleartext cardholder data and avoid the propagation of tokens to systems expecting cardholder data	The RSA Tokenization Server can always distinguish between a token value and a real value once a tokenize or de-tokenize call is made from the client. An attempt to de-tokenize a real value will result in an error, and the same holds true for an attempt to tokenize a token. We do not believe it is good practice for the client alone (with no request to the server) to be able to distinguish a token that was formatted similar to a payment card.
	Note: In accordance with the Visa Best Practices for Data Field Encryption, cardholder data must remain encrypted from the point where it enters and entity's system up to the point it is tokenized to achieve the full benefits of a tokenization solution.	This can be done with RSA's hybrid client environment, where data can be encrypted at the client immediately, even where a connection to the token server cannot be established.

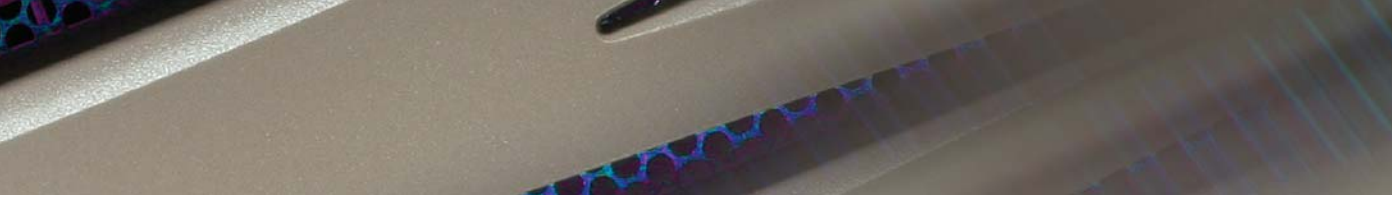


Domain	Best Practice	RSA Response
Tokenization Generation	**Token Generation.** Knowing only the token, the recovery of the original PAN must not be computationally feasible. Token generation can be conducted utilizing either: – A known strong cryptographic algorithm (with a secure mode of operation and padding mechanism) – A one-way irreversible function (e.g. as a sequence number, using a hash function with salt or as a randomly generated number)	RSA uses randomly generated numbers (or characters) for its token values. We use PRNG based on SHA-1 to generate those random values. PRNGs are relative to the Dual EC-DRBG using a P521 curve (ECDRBG256, ECDRBG192, ECDRBG128 (the default), HMACDRBG256)
	Single-user vs. Multi-use Tokens. Tokens can be generated as a single- or multi-use surrogate value, the choice of which depends largely on business processes: A single-use token should be used when there is no business need to track an individual PAN for multiple transactions. Acceptable methods for producing a single-use token include, but are not limited to, hashing of the PAN with a transaction-unique sale value, using a unique sequence number, or encrypting the PAN with an ISO- or ANSI-approved encryption algorithm using a transaction-unique key A multi-use token should be used when there is a business need to track an individual PAN for multiple transactions. A multi-use token will always map the same input PAN to the same token. An acceptable method for producing a multi-use token includes, but is not limited to, hashing of cardholder data using a fixed but unique salt value per merchant.	RSA Tokenization Server makes use of multi-use tokens within the system, so that the same value to map back to the same token.
Token Mapping	**PAN Processing.** In order to limit/eliminate storage of PAN data, the tokenization system should not provide PAN data to a token recipient (e.g. a merchant). If PAN data is returned, the receiving system will be in the scope of the PCI DSS. The token mapping should not perform the following: – Processes should not return the PAN as part of any response to the merchant – The tokenization platform should allow for charge-back and refund processing without the need for the merchant to retain or have access to full PAN	This applies mostly to the payment processor (token service provider) use case, where the token server is held off premise from the merchant themselves. RSA's partnership with First Data Corporation TransArmor® allows the merchant to completely remove the PAN from their system and only use tokens. For on-premise users of the RSA Tokenization Server, the server only returns the PAN to the client if a dedicated de-tokenize request is called. In addition, the RSA Tokenization Server can limit which clients can perform de-tokenize operations through server-side policy control. Therefore, in a highly regulated system RSA could allow only one application to de-tokenize while allowing numerous applications to tokenize input values.

Domain	Best Practice	RSA Response
Card Data Vault	PAN data must be encrypted in storage	RSA Tokenization Server is built upon RSA Key Manager, an industry leading key management system and provides built-in encryption of the token database.
	The card data vault must be managed and protected per PCI DSS requirements	RSA Tokenization Server is built upon RSA Key Manager, an industry leading key management system and fully meets PCI DSS requirements
Cryptographic Key	Encryption keys shall use a minimum bit strength of 112 bits. The following summarizes equivalent bit strengths for commonly used approved algorithms: TDES – 112 RSA – 2048 SHA – 224 AES – 128 ECC – 224	RSA Key Manager makes use of AES 256 bit keys when encrypting the token database
	Any cryptographic keys used by the tokenization system must be managed in accordance with PCI DSS	RSA Tokenization Server is built upon RSA Key Manager, an industry leading key management system and fully meets PCI DSS requirements
Management of Historical Data	Any retained historical or existing repositories of cardholder data must be protected (per PCI DSS requirements), tokenized or eliminated as part of the implementation	RSA can provide a complete solution to customers by making use of RSA Data Loss Prevention to find all copies of cardholder data and then using RSA Tokenization Server to tokenize that information.

Conclusion

Tokenization is a relatively new technology for protecting sensitive information, but it provides significant advantages to traditional encryption and other technologies such as format-preserving encryption, particularly in terms of reducing the operational costs and overhead associated with encryption. It can be applied across a broad range of industries and applications, such as sensitive financial services information, personally identifiable information for healthcare, and transformation of production data as it moves into development and test environments. The most widely adopted use case to date, however, has been to protect payment card information. By providing a solution that maps most effectively to industry best practices such as those recently published by Visa, RSA Tokenization Server is the most comprehensive and cost-effective form of application data protection available.



An organization interested in preventing data breaches or meeting compliance requirements must seek to protect sensitive data in the application layer, where the majority of threats reside.

RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control; governance, risk & compliance; encryption & key management; compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

VISABP SB 0710

RSA®
The Security Division of EMC

www.rsa.com