Vormetric Vaultless Tokenization with Dynamic Data Masking

Efficiently de-identifying sensitive data and reducing PCI DSS audit scope
## INTRODUCTION

### THE CHALLENGE

So Many Security Demands, So Little Time

### THE SOLUTION:

Efficiently De-Identify Sensitive Data

How Vaultless Tokenization Works

### DELIVER ROBUST DATA SECURITY

Strong Access Controls

Flexible Tokenization with Dynamic Data Masking

Tokenization Options

Deployment and Administrative Simplicity

Efficient Scalability and Agility

Key Benefits

Minimize Data Security Overhead and Training

Sample Implementations
Introduction

Today’s enterprise security teams have a lot on their plates and a lot on their minds. Attacks are becoming more sophisticated and persistent while insider threats continue to be an Achilles heel. According to the 2017 Thales Data Threat Report, 88% feel at least somewhat vulnerable to data threats. The report also proves those concerns are well founded: 42% of organizations experienced a data breach at some point.

Further, the financial ramifications of these breaches continue to grow. Consider just a few statistics from the most recent “Cost of Data Breach Study” by the Ponemon Institute:

- The average total cost of a data breach was $3.8 million, a figure that increased 23% since 2013.
- The average cost paid per compromised record grew more than six percent, and now stands at $154 per record.

Tokenization is a critical tool for enterprises to meet compliance standards, and reduce the risk of loss posed by this increasingly hostile environment. Most often, tokenization has been a great way for enterprises to reduce the cost of their Payment Card Industry Data Security Standard (PCI DSS) audits. Tokens are used to replace credit card numbers, removing the need for many servers to undergo expensive yearly audits. But use cases for tokenization are expanding today to safeguard more types of data and in more environments as the locations where this data is used proliferate.

Driven by data privacy and sovereignty regulations around the world, the data types that need to be protected are no longer just credit cards, but also include U.S. Social Security numbers, Drivers Licenses, U.K. National Insurance numbers, Passport numbers, and National Identity numbers in many countries around the world among other data. And the need to use this sensitive data in advanced technology environments like cloud and big data leads to further complications.


In this white paper we’ll first look at how Vormetric Tokenization works, key characteristics of the solution, and then examine sample implementations including PCI DSS compliance, customer contact centers, cloud, big data and more.

As noted earlier, tokenization is especially useful in PCI DSS compliance. In the past meeting requirements of the standard has been very complex and expensive, with extensive yearly audits of servers hosting credit card data required, or solutions that were limited in bandwidth and required extensive infrastructure to support.

Vormetric Tokenization now offers a better way to meet these requirements. The solution’s vaultless tokenization capabilities enable security teams to remove databases from PCI DSS scope, and so significantly reduce compliance cost and efforts. Implementations typically result in minimal disruption and administrative overhead and result in breakthroughs in operational efficiency.

Vormetric Vaultless Tokenization is also a solution deployed on the Vormetric Data Security Platform, which delivers a comprehensive range of data security and compliance controls that help IT teams efficiently address their requirements for encryption, privileged user access control, file access auditing, and more. With a single infrastructure, policy and encryption key management environment, the platform reduces the overall costs for organizations to implement and use data security tools while applying strong protections for data.
The Challenge

SO MANY SECURITY DEMANDS, SO LITTLE TIME

For today’s security teams, it seems virtually everything is proliferating:

➢ Threats. Risks posed by nation-states, cyber criminals, and malicious insiders continue to grow more sophisticated and more persistent.

➢ Data and repositories. The volume and diversity of assets and repositories that need to be protected continues to see explosive growth. Instead of just managing the traditional data center, which was challenging enough, there are now virtualized systems, big data environments, outsourced services, private clouds, public clouds, and hybrid models to contend with.

➢ Mandates and tools. As the number of repositories continues to grow, so do the number of systems that fall within the scope of PCI DSS and other regulations. Further, the scope and complexity of these regulatory mandates also continues to expand. As a result, security teams are compelled to deploy more safeguards and tools in order to establish the controls these mandates require. In particular, security teams face increased pressures to prepare for PCI DSS 3.0 audits, and adapt their security approaches as cardholder data moves into new environments—such as cloud and big data implementations—and is shared with outsourced service providers, such as analytics, development, and engineering firms.

All this proliferation continues to place increasing demands on security teams—but these teams don’t see their time, staffing, or budgets undergoing any commensurate expansion. To contend with these realities, many security professionals have explored the use of tokenization, which has the potential to provide a convenient way to protect sensitive assets. At a high level, tokenization is the process of replacing a sensitive record with a token, effectively a meaningless placeholder for the data that cannot be exploited or reverted back to its original form.

While tokenization offers the potential to address a wide range of security and compliance objectives, traditional tokenization tools and solutions have been far too costly and complex to procure and manage. These tools typically require security teams to invest in expensive appliances and contend with software agents that are difficult to deploy and manage. More than ever, security teams need to be able to leverage the benefits of tokenization—and they need to do so in a scalable, efficient, and cost-effective manner.
The Solution:

EFFICIENTLY DE-IDENTIFY SENSITIVE DATA

The Vormetric Data Security Platform offers tokenization capabilities that can dramatically reduce the costs and effort associated with complying with security policies and PCI DSS. With Vormetric Vaultless Tokenization with Dynamic Data Masking, organizations can efficiently address objectives for securing sensitive assets and cardholder records—whether they reside in the data center, big data environments, or the cloud.

HOW VAULTLESS TOKENIZATION WORKS

For illustration purposes, we’ll outline the process of tokenizing a credit card number.

1. The customer submits a credit card number into an application.
2. The application submits the credit card number to the Vormetric Token Server via the REST API.
3. The Token Server holds in memory a secure table created based on an AES-256 encryption key seed provided by the Vormetric Data Security Manager. This table holds with random matches for credit card numbers—the token matching that card is identified.
4. Through the REST API, the Vormetric Token Server returns the token to the application.
5. The application server then submits the tokenized value into the database.
Deliver Robust Data Security

STRONG ACCESS CONTROLS
Thales recommends creating at least two user accounts, or user groups from LDAP, be available on to the Tokenization Server:

- The first account or LDAP group with the permission to tokenize but not to detokenize, and the second account or LDAP group with the permission to detokenize.
- The user account with tokenization privileges can then be utilized by multiple servers, including a public-facing web server, for example. This allows data to be tokenized immediately as it is brought in through applications.
- Accounts or LDAP groups with permission to have detokenization privileges should be limited to a specific server that needs these permissions. For example, detokenization privileges could be restricted to a server that’s responsible for submitting credit card numbers to a remote card processing service.
- Any internal LDAP groups that have rights to detokenize data (Application administrators, for instance) should be strictly limited to the minimum number of members required.

Tokenized data can be used with databases or files needed for development, QA and Test, or deployed to Big Data environments without risk to sensitive information. For credit card data, servers using tokenized information are removed from expensive and time consuming yearly audits as well. Further, Thales offers a high availability, standards-based, FIPS 140-2 and Common Criteria validated policy management platform with the Vormetric Data Security Manager that can provide maximum security for cryptographic keys and policies used with tokenization.

FLEXIBLE TOKENIZATION WITH DYNAMIC DATA MASKING
Vormetric Vaultless Tokenization also offers the flexibility to establish varying levels of data redaction. Security administrators can establish settings to have an entire field tokenized or to dynamically mask only part of a field, keeping the remainder in the original clear-text. When combined with LDAP-based integration to Active Directory and other directory services solutions, this capability enables uses such as call centers. One example of call center usage is limiting credit card number visibility for customer service representatives to the last four digits of a customer’s credit card, while customer service supervisors can see the entire number.

The process of setting these policies is done using an intuitive administrative interface. Through the interface, administrators can choose exactly how they want data to be redacted, including specifying whether to replace a value with such characters as a pound sign, asterisk, or hyphen.
Dynamic Data Masking of Credit Cards for Customer Service

With Vormetric Vaultless Tokenization, policies could be implemented so that a customer service supervisor could see credit card numbers in the clear, while a customer service representative would only see the last four digits.

**Initial conditions:**
- Credit card data in a product database is tokenized
- A policy is set for the customer services representatives group in LDAP that allows them to see only the last four digits of a credit card number
- A second policy allows members of the customer services supervisor group to see the entire number

**Workflow**
1. Customer service representative request to see a credit card number
2. The application calls the token from the production databases
3. The application server then passes the token and User ID information to the Token Server using a RESTful API
4. The Token Server calls directory services requesting group information for the User ID
5. Based on the User ID, customer services group membership, and the policy that customer services representatives can only view the last four numbers of a credit card, the token is processed, and the credit card number retrieved. Data is then dynamically masked, with the card number set to XXXX-XXXX-XXXX-4321, where 4321 are the last four digits of the actual card. XXXX-XXXX-XXXX-4321 is then returned to the application server
6. The application server displays XXXX-XXXX-XXXX-4321 to the customer services representative
TOKENIZATION OPTIONS
As well as offering the capability to dynamically mask data for display, Vormetric Tokenization offers options for tokenizing a variety of fixed length data types – including Numeric, Text and Date formats. Options for data types to be tokenized include specific modes for:

- **Numbers** – Best for credit cards, U.S. Social Security numbers and other purely numeric data
- **Text** – All letters, all printable ASCII, All ASCII or AlphaNumeric for use with applications such as U.K. National Insurance numbers, drivers license numbers and others that include text only or mixed text and numbers
- **Partial tokenization** – Select only a portion of the fixed length field to be tokenized – keeping a portion of the data as the original information
- **One-time use tokens** – Used only when the data will never be de-tokenized
- **Dates** – including formats with various separators. Can also be modified with a start and end year
- **Prefix** – Prefixes can be appended to all tokens – for instance to designate a drivers license (DL)

DEPLOYMENT AND ADMINISTRATIVE SIMPLICITY
With Vormetric Vaultless Tokenization, you can capitalize on a range of features that streamline up-front implementation and ongoing operations. Vormetric Vaultless Tokenization enables efficient, enterprise-wide administration.

With the capabilities offered by the Vormetric Data Security Platform, you can choose from a range of technologies and employ the mix that’s optimally suited to an organization’s specific projects and use cases. At the same time, enterprises gain the cost savings and operational benefits of working with solutions that can be centrally and uniformly managed. With the Vormetric Data Security Platform from Thales, organizations can centrally manage keys for Vormetric Vaultless Tokenization, as well as for Vormetric Transparent Encryption, Vormetric Application Encryption, other Vormetric products, and third-party devices.

**Offers non-disruptive implementation**

With the solution’s capabilities, you can restrict access to sensitive assets, yet at the same time, format the protected data in a way that reduces the operational impact typically associated with encryption and other obfuscation techniques. For example, organizations can tokenize a credit card field in a database, yet keep the tokenized information in a format that is compatible with associated applications. Further, tokens can appear to be real credit card numbers and pass LUHN validation, so tokenization does not break existing validation processes.

**Eliminates manual efforts and complexity**

The Vormetric solution employs tokenization at the application layer, and it streamlines all the application development efforts associated with implementing tokenization in an enterprise. With the solution, developers don’t have to manually institute identity management or redaction policies. Vormetric Vaultless Tokenization offers an easy-to-use REST API for integration with the Vormetric Token Server, so that application developers can simply and quickly add tokenization and dynamic data masking to applications.

**Provides investment protection**

Customers that have already invested in the Vormetric Data Security Platform can get even more out of their investments. By leveraging existing Vormetric Data Security Manager implementations (required for all Vormetric Data Security Platform products), it is quick and cost effective to add Vormetric Vaultless Tokenization through an all software deployment.
EFFICIENT SCALABILITY AND AGILITY
Vormetric Vaultless Tokenization delivers the performance needed to address the operational demands of the most processing-intensive environments, enabling organizations to do millions of tokenization or detokenization operations per second. The Vormetric Token Server runs on virtual machines and can be quickly and efficiently scaled up and scaled down to accommodate changing workloads. For redundancy, Vormetric recommends deploying a cluster with at least two nodes. A three-node or four-node cluster multiplies the throughput, while providing added redundancy. Performance realized will vary depending on hardware platforms, cluster sizes, and client parallelism employed. It should be noted that Vormetric doesn’t charge for the Token Server or the number of processed transactions, so adding Token Servers to accommodate expanding workloads, or for high availability and scalability, does not add to procurement costs.

In addition, because this solution doesn’t require a traditional database running as a token vault, lookup latency is greatly reduced. This is because there is no need for the token server to make calls to the token database to identify original data. The entire process occurs within the Vormetric Token Server. This also simplifies operations, as there are no databases to back up, synchronize, and maintain.

KEY BENEFITS
Reduce PCI DSS compliance effort and scope
By leveraging Vormetric Vaultless Tokenization, you can minimize the repositories and processes that can gain access to payment data in the clear, organizations can significantly reduce PCI DSS compliance costs and efforts.

Fully leverage cloud, big data, and outsourced models
Vormetric Vaultless Tokenization enables organizations to more fully leverage cloud services, big data models, and outsourced environments, while retaining the security controls required. For example, tokenized data can be easily migrated tokenized data to a public cloud, without exposing sensitive data to unauthorized access, even access by administrators in the cloud provider’s environment.

Establish broad safeguards around sensitive assets
Unlike other dynamic data masking tools, the Vormetric solution tokenizes sensitive fields in the production database. As a result, enterprises can establish comprehensive safeguards around sensitive assets across the organization. Because the source and display data remain protected, this includes strong safeguards against cyberattacks from criminals and nation-states, as well as from insider abuse.

Minimize data security overhead and training
With the Vormetric Data Security Platform, enterprises can leverage a platform to centrally manage keys for Vormetric Vaultless Tokenization and as well for the full range of Vormetric Data Security encryption and access controls solutions. By leveraging a central platform that offers comprehensive capabilities, organizations can minimize the cost, effort, and training associated with managing point-products.

SAMPLE IMPLEMENTATIONS
PCI DSS 3.X Compliance
The more locations that hold primary account numbers (PANs), the more locations that fall under PCI DSS regulations. As the number of locations grow, so too do the cost and effort associated with establishing and sustaining compliance, preparing for audits, and so on. With Vormetric Tokenization, you can tokenized PANs, and significantly restrict the number of users, processes, and repositories that can get access to this data in the clear. As a result, organizations can dramatically reduce compliance efforts and costs. Further, through such capabilities as Luhn check support, Vormetric Vaultless Tokenization enables organizations to implement tokenization with minimal impact on applications and processes. In addition, the Vormetric Data Security Platform offers the controls you need to address many PCI DSS requirements, including least privileged access controls, encryption, key management, and file access audit logs.
Customer contact centers
Vormetric Vaultless Tokenization helps mitigate the threats that can be posed by support staff exploiting their access privileges to steal or leak sensitive data. Vormetric solutions from Thales can be effective both for securing sensitive data in internal contact centers and in outsourced or geographically distributed support environments. For example, enabling a support agent to see only the last 4 digits of a Social Security Number. As a result, agents can conduct any required customer verification processes, without being put in a position where they can maliciously or inadvertently leak sensitive and regulated PII.

Outsourced Development
For many organizations, application development is done by an increasingly dispersed set of teams, including geographically distributed employees as well as external contractors and service providers. While these distributed teams have helped improve the cost efficiency and agility of development efforts, they can pose significant challenges for those organizations that manage sensitive and regulated data. From initial development to testing and staging, developers need access to data repositories. If all data is left in the clear, it exposes a range of sensitive regulated data and intellectual property to any number of threats. With Vormetric Vaultless Tokenization, organizations can quickly and efficiently provide internal and external development teams with access to corporate data repositories, while tokenizing the specific assets that pose security or compliance risks.

A complementary product, Vormetric Batch Data Transformation, also helps organizations to quickly tokenize large data sets for this purpose when needed.

Big Data
To capitalize on the opportunities presented by big data, organizations need to aggregate information from a broad range of repositories—and in the process can create massive collections of highly sensitive and proprietary data. With Vormetric, enterprises can fully leverage big data, without introducing risk to the business. Sensitive records can be tokenized before they are incorporated into big data repositories, so big data scientists, developers, and business analysts don’t gain access to sensitive data that is not required for their work. At the same time, the solution’s flexible tokenization options ensure that tokenized records don’t disrupt big data migration, calculation, and analytics processes.

Cloud Services
When your organization moves to cloud computing models, whether infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS), or hybrid approaches, you may offload a number of responsibilities and efforts, but your organization ultimately still bears responsibility for the security of its sensitive and regulated data. With Vormetric Vaultless Tokenization, your organization can leverage the cloud models it needs, while managing tokenization policies locally. As a result, you can retain complete control and visibility over who can access sensitive assets in the clear, no matter where tokenized information ultimately resides.

Static Data Masking
Organizations can replace sensitive assets with tokens, so that outsourced application development and testing teams can run QA and analytics using realistic looking data, without having access to any sensitive assets. Once sensitive values in the database are tokenized, enterprises simply need to create a copy of the production database and give that copy to the outsourced development team. Since these teams don’t have access to both the Vormetric Tokenization Server and user credentials to detokenize, they won’t be able to access sensitive data in the clear. This protects the business, maintains compliance, and enables outsource development teams to access and test realistic production data.

Just as noted above under Outsourced Development, Vormetric Batch Data Transformation helps organizations to quickly tokenize large data sets for this purpose when needed.
About Thales e-Security

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn’t just reduce risk, it’s an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization’s digital transformation. Thales e-Security is part of Thales Group.