Protegrity Vaultless Tokenization

To secure sensitive data, such as PCI, Privacy, PII or PHI information, businesses are increasingly turning to tokenization and masking to de-identify sensitive data with replacement values that hold no value to a potential thief. Vaultless Tokenization provides the benefits of both tokenization and masking in one high-performance, comprehensive data security solution.

ADOPTION OF TOKENIZATION

Tokenization's popularity has been increasing rapidly due to the greater convenience and flexibility over encryption for PCI data. However, tokenization can be used to de-identify any structured sensitive information, as defined by PCI DSS, HIPAA, and NIST, such as credit cards, names, SSN, addresses, and any other PCI, Personally Identifiable Information (PII), or Protected Health Information (PHI) data.

Enterprise-wide tokenization is far less intrusive than encryption, as key management is reduced or eliminated, the data type and length of the original data can be preserved, and tokens can be embedded with business intelligence, which can eliminate the need to de-tokenize sensitive data for many business processes. In PCI use cases, audit scope can be greatly reduced.

KEY FEATURES

- **Tokenize/mask any structured data**
- **High performance & proven scalability**
- **Tokenize in Big Data environments, such as Hadoop**
- **Compatible across heterogeneous environments**
- **Flexible deployment**
- **Many token type & format options**
- **Lowest TCO of any data security solution**
- **Tokens can be used in enterprise-wide business processes**

PERFORMANCE & SCALABILITY

Protegrity's high-performance token servers provide fast creation of new data tokens and re-identification of original data when needed. A recent performance study benchmarked Protegrity's token creation at over 200,000 tokens/second from a single commodity token server. Scaling the solution to very large token volumes is as simple as adding commodity or virtual token servers ensure the highest output of each server.

FLEXIBLE DEPLOYMENT

Vaultless Tokenization has no vault and no stored data, using static token tables with a very small footprint. Vaultless token servers can be deployed centrally, or easily deployed to geographically distributed environments to tokenize in close proximity to where the data resides. Recognizing that moving tokenization close to the data reduces the latency of token operations, Protegrity developed the unique form of token servers deployed directly on the node, nearly eliminating latency altogether. On node deployment also allows for tokenization and masking in Big Data environments, such as Hadoop®. Token servers can be purpose-built for specific functions, such as segregating payment transaction tokenization from PII or PHI masking.

TOKEN TYPES & FORMATS

Multiple token types and formats are supported, such as numeric and alphanumeric, in unlimited lengths and for any data types. Tokens can also be embedded with business intelligence, such as a merchant identifier, and can mask only part of the original data, useful when applications only need part of the sensitive data for business processing.

ECONOMICS OF TOKENIZATION

Vaultless Tokenization offers a number of operational benefits over data encryption. Tokens can be used enterprise-wide for business processes, have no cumbersome key management, and can dramatically reduce the scope of PCI compliance. Vaultless Tokenization provides the lowest total cost of ownership of any data security solution, and the benefits compound when considering future growth.

PLATFORM PROTECTION

As part of the Protegrity Data Security Platform, Vaultless Tokenization can be combined with file encryption, central policy-based access control, and advanced auditing and monitoring software for multi-layered protection. Deployed via Protegrity's Data Protectors (File Protector, Application Protector, Database Protector and Big Data Protector), the Protegrity Data Security Platform provides comprehensive enterprise data security in complex, heterogeneous environments.

> **"Protegrity's Vaultless Tokenization did exactly what we needed. It is easy to install, flexible, extremely proficient with regards to performance, and above all - secure."**
>
> **Leif Gyllsdorff**, *Preem*

Protegrity's award winning and innovative software is backed by over 30 pending or granted industry patents, all of which provide superior protection unique to the Protegrity Data Security Platform. The Platform is comprised of the Enterprise Security Administrator (ESA) and a suite of Database, File, and Application Protectors with advanced Vaultless Tokenization, format-preserving encryption, strong encryption, masking, hashing, and monitoring software.

VAULTLESS TOKENIZATION

Protegrity's industry-first, patent-pending **Vaultless Tokenization** process that eliminates the challenges associated with standard, vault-based tokenization. Greatly reduced bottlenecks in performance and scalability caused by latency, no more fear of collisions, and no more sensitive data or tokens residing in your token server. In the event of a breach, tokens hold no value to a potential thief. Tokens can also be embedded with business intelligence, allowing for seamless analytics and business processes without the need to detokenize data.

DATA PROTECTION METHODS

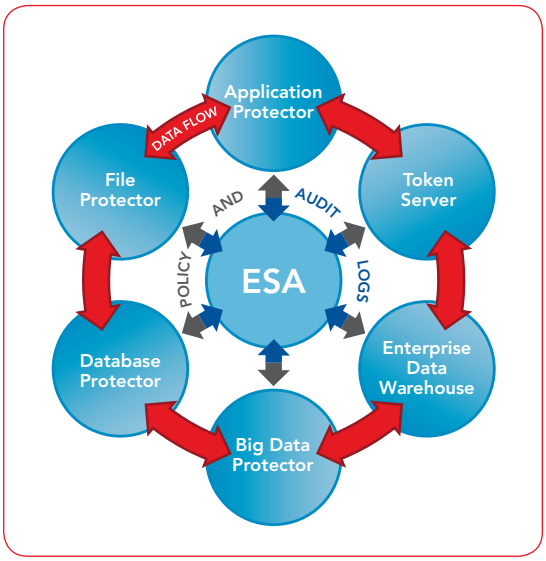
An effective data security strategy is defined by matching the risk associated with any particular type of data (e.g. credit card numbers, PII, etc.) with a specific data protection method. Protegrity supports a comprehensive range of **Data Protection Methods**, including Vaultless Tokenization, format-preserving encryption, strong encryption, masking, hashing, and monitoring.

ENTERPRISE COVERAGE

Protegrity has a proven record of successfully implementing data security solutions in complex, heterogeneous environments. The **Protegrity Data Security Platform** has extensive interoperability with the variety of databases, operating systems, applications, and platforms inherent in all large enterprises, including Oracle, DB2, SQL Server, IBM Mainframe, Hadoop, Teradata, and more.

DATA PROTECTORS

To help organizations implement a truly end-to-end data security strategy, Protegrity provides a collaborative set of Data Protectors, including the **Database Protector**, **File Protector**, and **Application Protector**. These Data Protectors can be combined as needed to provide flexible security for sensitive data in all forms across an entire enterprise.



BIG DATA

Protegrity is the first vendor to deliver a comprehensive data protection path to Apache™ Hadoop®, Teradata Aster, and other **Big Data** platforms. For the first time in Big Data platforms, data protection is no longer solely reliant on access controls. The actual data can be protected from external and internal threats while at rest in HDFS; in use during MapReduce, Hive, and Pig processing; and in transit to enterprise systems such as an Enterprise Data Warehouse.

CENTRAL POLICY & KEY MANAGEMENT

Protegrity's **Policy** level approach enables Security Officers to determine and specify *what, when, where* and *how* data will be protected, *who* is allowed access, and to record all attempts to access sensitive data. Protegrity also provides integrated, comprehensive **Key Management** capabilities, with an easy-to-use system.

SEPARATION OF DUTIES

The Protegrity Security Platform provides a **Separation of Duties**, isolating security administration to security officers. Database and application administrators and users are unable to access sensitive data in the clear, or grant security access to others. Since the data itself is protected, technologists – DBAs, programmers, or system engineers – can continue administering different aspects of the enterprise IT environments without disruption to business processes.

CENTRAL REPORTING

Protegrity's **Central Reporting** capability enables Security Officers to monitor the continuous enforcement of Policy throughout all protection points, while giving compliance assessors the information they need to certify compliance with applicable legal and regulatory requirements, such as PCI, HIPAA/HITECH, and PII.

protegrity

Corporate Headquarters
Protegrity USA, Inc.
5 High Ridge Park, 2nd Floor
Stamford, CT 06905
Phone: **203.326.7200**

United Kingdom
3 Regius Court
Church Road
Penn
Buckinghamshire
HP10 8RL
Phone: **+44 1494 857762**

www.protegrity.com