

nuBridges Protect™ Token Manager

Solution Brief

Enterprises today face evolving global data privacy risks and challenges. Complicated compliance mandates. Explosive proliferation of business-critical and sensitive electronic data stored in multiple applications and databases. Mobile workforces and business partners scattered around the globe.

Perimeter security is no longer sufficient. It's time to change the way we think about data protection - the boundary isn't the network - it's the data itself.

Flexible Protection for Sensitive Data at Rest in the Enterprise

nuBridges Protect™ is an integrated encryption, tokenization, key management and audit logging software solution that protects sensitive, business-critical and regulated data in applications and databases. One of the industry's most adaptable data protection solutions, nuBridges Protect:

- Secures data on a wide range of enterprise platforms including IBM mainframe, IBM i, Windows, UNIX and Linux; and databases including Oracle, DB2 and Microsoft SQL Server; and
- Can be deployed in a variety of architectural models to support the industry's broadest set of enterprise use cases.

This Solution Brief describes the Token Manager module and associated implementation architecture. For information about the complete solution, please visit our Web site.

Format Preserving Tokenization - Introducing a New Model

nuBridges Protect Token Manager is a software module that intercepts the data you want to protect, generates format-preserving tokens and inserts them in place of the sensitive data. It then encrypts the original data and stores the cipher text in a central data vault. Tokens can be safely used by any application or database without risk of exposing sensitive data. When applications or databases require the clear-text value, they simply make a Web services call to the Token Manager and present the token. The Token Manager validates the request credentials and, if authorized, looks up the token in the data vault, identifies the appropriate cipher text, decrypts the value and presents it back to the database or application.

*The industry's first
data security software
that offers
strong encryption,
Format Preserving
Tokenization™ and
unified key management
in one solution.*

Token Manager encrypts sensitive data and stores the cipher text in a central data vault. It replaces the original values with Format Preserving Tokens. You get powerful, non-invasive protection, eliminating points of risk and simplifying compliance by reducing scope.

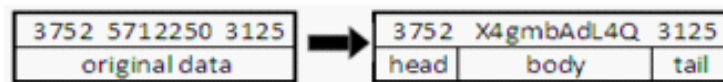
The relationship between data and token is preserved – even when encryption keys are rotated. The data vault contains a single encrypted version of each original plain text field. This is true even when encryption keys change over time -- there is only one instance of the encrypted value in the data vault. This means the returned tokens are always consistent whenever the same data value is encrypted throughout the enterprise.

Since a strict one-to-one relationship between the token and data value is maintained, referential integrity can be assured whenever the encrypted field is present across multiple data sets, and data and trend analysis can continue uninterrupted (this is a big difference between nuBridges Protect and outsourced solutions; along with the fact that nuBridges Protect can handle all types of sensitive data, not just credit cards) Because records are only created once for each given data value (and token) within the data vault, storage space requirements are minimized.

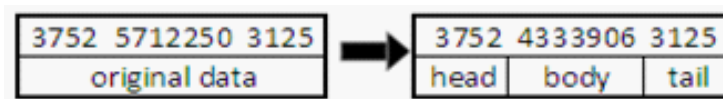
With nuBridges Protect Token Manager’s format-preserving model, tokens that maintain the length and format of the original data can be generated for all types of sensitive customer, employee and company confidential information.

Tokens can be formatted to:

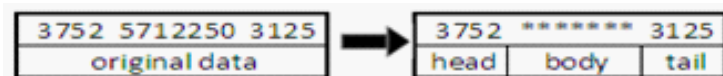
Preserve a number of leading and trailing characters



Preserve the format (length and data type)



Mask a portion of the token when a full value is not needed or desirable



nuBridges Protect Token Manager gives you the flexibility to support many different use cases – customer service applications that need the last four digits of the credit card; loyalty programs that need to match customer activity across a variety of applications; business intelligence analytics – seamlessly. It is engineered to minimize impact on existing systems and maximize data protection.

Narrow the Scope of Compliance and Risk

By centralizing the storage of encrypted data into a secure data vault, the Token Manager significantly minimizes the number of locations where encrypted values reside. Reducing the distributed footprint of encrypted data narrows the scope of systems, applications and processes that are subject to PCI DSS and other security audits; and simplifies security policy management.

A breach of encrypted or tokenized data is a non-event. Sure, you'll need to close that hole. But your brand, customers, shareholders and employees won't have to deal with the fallout of unintended disclosures.

It also solves the age-old problem of how to support systems development and testing – now enterprises can provide developers with tokens that look and act just like production data without exposing any sensitive information at all.

nuBridges Protect Token Manager Features

- Creates a central, protected data vault where sensitive data is encrypted and stored. This greatly reduces the footprint where encrypted data is located and eliminates points of risk.
- Generates tokens that act as surrogates for sensitive data wherever it resides. Tokens maintain the length and format of the original data so that applications don't require modification.
- Enforces a strict one-to-one relationship between tokens and data values so that 1) referential integrity can be assured whenever an encrypted field is present across multiple applications and data sets; and 2) data and trend analysis can continue uninterrupted.
- Provides complete control of the token-generation strategy. For example, the last four digits of the data can be preserved in the token, allowing the token to support many common use-cases.
- Supports multiple classifications of sensitive data, with each classification having its own policy.
- Integrates with nuBridges Protect Key Manager for full-lifecycle, PCI DSS-compliant key management, and the ability to rotate keys without having to re-encrypt old data (and therefore, no requirement to take systems down when rotating keys).
- Web Services interface enables diverse client platforms and languages to consume the services of the Token Manager.
- Browser-based interface for system administration and policy management.
- Generates Syslog-compliant security event logs that are easily integrated with Security Incident and Event Management (SIEM) and log management solutions.
- Scalable for high-volume, high-availability environments.

nuBridges, Inc.

U.S. HEADQUARTERS
1000 Abernathy Road
Suite 250
Atlanta, GA 30328
UNITED STATES
Tel. +1 770 730 3600

EMEA HEADQUARTERS

Lakeside House
1 Furzeground Way
Stockley Park
Uxbridge, Middlesex
UB11 1BD
UNITED KINGDOM
Tel. +1 44 (0) 20 8622 3841
www.nubridges.com

About nuBridges, Inc.

nuBridges is a leading provider of software and services to protect sensitive data at rest and in transit, and to transfer data internally or externally with end-to-end security, control and visibility. nuBridges data protection, managed file transfer and B2B integration solutions are used to comply with security mandates and to digitally integrate business processes among enterprises, systems, applications and people. Over 3,000 customers depend on nuBridges secure eBusiness solutions to encrypt millions of credit cards, exchange billions of dollars in B2B transactions and enable countless business-critical file transfers, including Walmart, Amazon.com, Timberland, American Eagle Outfitters, Belk, Bon Ton, John Deere, Wachovia, Sun Trust, AIG, Check-Free, Bank of America and Verizon. nuBridges is headquartered in Atlanta, Georgia, USA.