



SOFTWARE SECURITY INSTITUTE

# Vendor Whitepapers

Copyright SANS Institute

Author Retains Full Rights

**Web Application Security 519**  
**Security Workshop**



# Best Practices in Data Protection: Encryption, Key Management and Tokenization

Protecting sensitive and business-critical data is essential to a company's reputation, profitability and business objectives. Companies know they can't afford a data breach – customer churn, loss of business, brand damage, fines and litigation. In today's global market, where business data and personal information know no boundaries, traditional point solutions that protect certain devices or applications against specific risks are insufficient to provide cross-enterprise data security.

As enterprises seek to protect data from cybercriminals, internal theft or even accidental loss, encryption and key management have become increasingly important and proven weapons in the security arsenal for data at rest in databases, files and applications and for data in transit. And now there is a new strategy that adds an extra layer of data protection – tokenization. Combined, these offer the most powerful enterprise-wide data protection available today.

This white paper describes best practices in encryption, key management and tokenization and how an integrated, multi-level solution can effectively meet these best practices.

## Introduction

Enterprises must recognize that enormous business risks are associated with the methods that they use to protect their sensitive and business-critical data. Think Coca-Cola and KFC and their secret recipes. Granted, a secret recipe probably isn't your company's greatest data asset. But you do have the equivalent competitive advantage in your customer lists, patents, financial statements and so on. Whatever business you are in, you need to ensure that your data is protected. By investing in an integrated data protection solution that offers encryption, key management and tokenization, you'll have the best available insurance against the potential loss of business, brand equity and customer loyalty.

---

*"In an economy that has companies doing everything they can to retain customers and brand reputation, and where federal, state and local governments are looking at ways to ensure sensitive citizen data is properly protected, encryption continues to be a best practice approach to an overall data protection strategy in 2009."*

---

## The Typical Enterprise Landscape

Today's enterprise faces a daunting security challenge. Not only must it build an impregnable fortress around its internal networks and applications, but it must also contend with the complications of sending and receiving encrypted data, and encrypting data at rest within application files and databases that were not designed for secure handling of data.

---

*"2009 Annual Study: U.S. Enterprise Encryption Trends" – Ponemon Institute, July 2009*

---

Many enterprises that handle private or confidential data such as credit card and debit card numbers, social security numbers and health care records have the data stored in plain text in multiple locations throughout the enterprise. Typically an enterprise will have a large number of applications that process private or sensitive data that must be adapted to handle encryption.

There will be applications that handle 'in-flight' data, sending and receiving data from external trading partners or other entities with a single company, and applications that handle 'static' data, or data at rest. The applications are on a variety of computers with a number of operating systems, languages and databases. The computers are on multiple networks or subnets.

The encryption and decryption of sensitive data distributed throughout the enterprise requires a large number of resources – keys and certificates – that must be managed across applications, computers and networks in a cost-effective and efficient way that does not compromise security. Additionally, user and application access to these resources must be controlled, managed and audited so that authorized access is quick and reliable, while malicious attacks are thwarted.

And, of course, a comprehensive approach to key management also must ask the question: "Who guards the guards?" The administration of encryption keys must itself have built-in protection against internal attack. And they must be rotated regularly and archived for future use.

## Best Practice: Encryption

Encryption is a perfect companion to strong perimeter and firewall protection. Enterprises have been using cryptography for computer security purposes for several decades. When networks were private, data was rarely encrypted. Its primary purpose was to protect certain secret fields such as passwords from someone accessing them in an unauthorized manner. And the associated encryption keys were rarely changed. Today, we rely on public networks to access and transmit information. Computing has burst out of the glass house and information travels on laptops, PDAs and thumb drives. Wireless connectivity is a Wild West of opportunity for eavesdroppers and thieves. The amount of information that must be encrypted and decrypted at rest and in transit is increasing exponentially, leading to a corresponding encryption key management challenge.

These processes must be performed in a manner that is secure, tamper-proof, available and auditable. They must allow for an infinite variety of lifecycle timelines – from seconds to years. And they must support regulation-specific key handling such as that mandated by the Payment Card Industry's Data Security Standard (PCI DSS).

Keys proliferate exponentially as you manage the data encryption lifecycle. If not managed properly, a new problem emerges -- how to control and protect access to the keys to (1) assure that they don't get into the wrong hands and (2) assure they are available when needed to unlock data today and in the future. There is mounting demand for effective, practical, automated, risk-mitigating ways to manage keys throughout their lifecycle so that the good guys are facilitated and the bad guys are thwarted.

## Best Practice: Centralize Key Management

The more data you encrypt, the more difficult it becomes to effectively manage proliferating keys. The most effective solutions available are designed to balance two equally important, yet opposing objectives: Keep keys safe from unauthorized exposure and make sure they are available when you need them for authorized use.

These processes must be performed in a manner that is secure, tamper-proof, available and auditable. They must allow for an infinite variety of lifecycle timelines – from seconds to years. And they must support regulation-specific key handling such as that mandated by the PCI DSS, government privacy acts and other industry mandates.

Best practices calls for a centralized key manager that generates, distributes, rotates, revokes and deletes keys to enable encryption and to allow only authorized users to access sensitive data. A solution that rotates keys without requiring you to re-encrypt your data (unlike other solutions, which may require the overhead and risk of re-encryption, and also may require you to bring your applications and databases down during re-encryption).

What's more, the solution should also manage keys across disparate platforms and systems. This means that you can centrally manage the encryption keys across all of the different databases, operating systems and devices that you have throughout your organization.

This key manager, used to define and enforce policies that govern who can access keys, will track an infinite number of keys, and it will handle all backup media encryption without the need to pull tapes and re-encrypt

with new keys once old keys have expired. It provides intelligent backup media key management which eliminates the need to manually track keys, and allows you to utilize keys for tapes that have been stored for an extended period of time without having to store the key with the encrypted data (a requirement for PCI DSS compliance, and an important best practice in general).

### Best Practice: Centralize Key Management with Localized Encryption

Best practice calls for a hub-and-spoke architecture for centralized key management and localized encryption. Encryption and decryption nodes may exist at any point within the enterprise network. Spoke key management components are easily deployed to these nodes and integrate with the local encryption services.

Once the spoke components are active, all encryption and decryption of the formerly clear text data is performed locally, thus minimizing the risk of a network or single component failure having a large impact on the overall data security operation.

Data encryption is achieved through the use of symmetric keys which are used for both encryption and decryption (data encryption keys – DEKs). This technique is used for speed; however, it introduces the requirement to keep the keys secret. To address this requirement, the encryption keys are encrypted using asymmetric encryption keys (key encrypting keys - KEKs).

Asymmetric algorithms provide a high level of security. Rather than using a single secret key, asymmetric algorithms use a public key to encrypt data and a related private key to decrypt data. Once data is encrypted with the public key, only the private key can decrypt the data. This greatly reduces the key management requirements, since both parties no longer need to share the same, secret key. The drawback to asymmetric algorithms is they are very computationally expensive to implement. They are only suitable when encrypting a small amount of data – hence the design described above.

Combining a symmetric and an asymmetric algorithm provides the speed benefit of symmetric encryption and the simpler key management of asymmetric encryption. Other security features include:

- During export, secret keys are encrypted and can only be used and decrypted by the intended recipient.
- Keys are organized into groups (similar in concept to a key ring). The group is the unit of deployment. With this model, the spoke/endpoint only receives the keys it truly needs.

During export, the group of keys is packaged together in a key ring and digitally signed. Verification of the digital signature enables the spoke to detect any tampering with the keys and to establish that the keys came from a trusted source. Transport to the end-points is performed over SSL for confidentiality and integrity.

### Best Practice: Centralize Key Management with Tokenization

Key management solutions should enable tokenization models that intercept the data you want to protect and replace it with tokens. With tokenization, a token – or surrogate value – is returned and stored in place of the original data. The token is a reference to the actual cipher text, which is stored in a central data vault.

Tokens can be safely used by any file, application, database, or backup media throughout the enterprise, minimizing the risk of exposing the data, and allowing business and analytical applications to work without modification. The combined solution that integrates encryption key management and tokenization delivers effective data protection in several ways:

- Minimizes the number of locations where sensitive and business-critical data is stored, virtually eliminating points of vulnerabilities
- Replaces data with tokens
- Stores cipher text in a secure, central data vault
- Minimizes the number of locations where keys exist

### Best Practice: Eliminate Decryption/Re-Encryption Cycle for Key Rotation or Expiration

To meet best practices, the encryption key management solution should not place constraints on the creation and changing of encryption keys. Keys can be changed annually, quarterly and/or monthly – this feature accommodates a variety of key lifecycle timelines. For PCI DSS compliance, keys must be rotated at least annually.

The actual process of using the correct key, when rotated, is automatic. To rotate a key, the administrator uses a key manager to generate and distribute a new key to the encryption endpoint. The encryption service will always use the most recent active key when encrypting. More importantly, the encryption service knows which key to use when decrypting. This is accomplished since the solution keeps track of which encryption keys are associated with individual data values. A key ID is associated with each cipher text value to provide the application with the knowledge of which key was used during encryption. Therefore, when keys are rotated and new keys are introduced to encrypt new values, the encryption service will continue to track which key to use when a decryption is required.

This would be important, for example, in the following situation:

*A new subscription is initiated and billed on December 20th and keys are then rotated on January 5th. New subscriptions and initial payments processed on January 5th would use a new key while the subscriptions billed on December 20th had credit card information encrypted with the prior key. If a customer requests a credit/refund on January 5th, when the subscription system accesses the credit card from December 20th, it must know to use the previous key. Alternatives to this would require you to decrypt and re-encrypt all historical data when rotating keys.*

Decrypting and re-encrypting data for the purposes of rotating keys is not required; therefore, there is no need to take applications or databases offline to rotate keys. The only time this is recommended is in the remote situation that keys are compromised and decryption and re-encryption are required as defined by the PCI DSS.

### Best Practice: Maintain Comprehensive Logs and Audit Trails

The encryption key management solution must record all encryption, decryption, tokenization and key management events - by user and time, so you always know when your sensitive data is accessed and by whom. It also records all unauthorized access attempts to encrypted data and keys. All logs are syslog-compliant, so you can easily integrate with your Security Incident and Event Manager (SIEM) package to proactively monitor the security of your data and prevent breaches. Allowing a centralized log management system to correlate this information with other network, database and application logging information provides an additional level of observation and another layer of defense.

### Best Practice: Use One Solution to Support Field, File, Database and Backup Storage

#### Field and File Encryption

Best practice calls for the capability to perform the field and file level encryption that is necessary when an application uses a file rather than a database to store sensitive data. This could be when storing data on the network, in an application, or when an entire file needs to be encrypted before it is put on to backup media. This level of encryption typically requires some small modifications to the original application, because new read and write commands need to be inserted that will invoke encryption and decryption components. In most cases, these modifications can be automated through scripts and filters that scan the applications and do 'find and replace' operations, thus minimizing the effort.

#### Database Encryption

Best practice provides the capability to encrypt and decrypt sensitive data at the database field level. Database field encryption is accomplished without any changes to the application accessing the database in most scenarios. All of the necessary modifications (if any) are implemented in the database itself.

### Summary

The good news for enterprises that need to protect any type of customer, employee or partner information – from credit card numbers to social security numbers to financial statements – is that there are extremely cost-effective, non-intrusive and iron-clad ways to secure data using an integrated encryption, key management and tokenization solution. These features and many more are built into nuBridges Protect™, a best-of-breed solution that fulfills the best practices explored in this white paper.

nuBridges, Inc.  
info@nubridges.com  
www.nubridges.com

**U.S. HEADQUARTERS**

1000 Abernathy Road, Suite 250  
Atlanta, GA 30328  
p: +1 770 730 3600

**EMEA HEADQUARTERS**

Lakeside House, 1 Furzeground Way  
Stockley Park, Uxbridge  
Middlesex, UB11 1BD  
United Kingdom  
p: +44 (0) 20 8622 3841  
f: +1 770 730 3784

## 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 encryption, key management and tokenization; 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, Wachovia, Sun Trust, AIG, Check-Free and Verizon. nuBridges is headquartered in Atlanta, Georgia, USA. More information is available at [www.nubridges.com](http://www.nubridges.com).