White Paper

Encryption Key Management for Microsoft SQL Server 2008/2012

ORGANIZATIONS CONTINUE TO EXPERIENCE DAMAGING LOSSES DUE to data breaches. These losses include legal costs, costs to reimburse customers and employees, lost stakeholder value, and reduction of goodwill. The estimate of these financial losses range into the billions of dollars every year. This paper discusses compliance regulations, standards for protecting data with encryption, and how Microsoft provides for the encryption of sensitive data in its flagship SQL Server database system. Townsend Security's Alliance Key Manager HSM provides a cost effective, easy-to-deploy, and compliant solution for Microsoft customers.

Townsend SECURITY

www.townsendsecurity.com

Data Losses Mount Along with Financial Losses

In mid-2011 the rate of data breaches had risen and was on track to exceed the losses of the previous year. The Ponemon Institute, which monitors the cost of data breaches, reports that the average cost of a data breach is $214 per record, and the average cost to a company is over $7 million per breach. Financial costs include the replacement of credit cards, the cost of credit monitoring services, and the legal costs required to defend the organization from consumer and shareholder lawsuits. Long term reputational costs can be even more severe.

The costs of data breaches are rising and the frequency is rising, too.

Mid-market companies face an additional existential risk. A survey conducted by the Ponemon Institute and sponsored by the law firm of Scott and Scott, shows that 74% of companies experienced a loss of customers after a breach, and 32% experienced a loss in share value. In a difficult economic environment a company may not survive the financial impacts of a data breach.

Compliance Regulations & Asset Protection Drive Encryption

Compliance regulations such as the Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Act (GLBA), and state privacy laws force organizations to implement strong data protection controls including data encryption. In some cases regulations require the encryption of sensitive data, and in other cases encryption is strongly recommended. The only safe harbor from breach notification across all regulations is the use of strong encryption to protect sensitive data. While strong encryption is not the only data security effort needed to protect data, it is an essential component of any effective strategy.

Encryption Key Management is Crucial to an Encryption Strategy

The most important part of a data encryption strategy is the protection of the encryption keys you use. Encryption keys are the real secret that protects your data. Just as the key to your house is unique and can't be used anywhere else, the data encryption keys you use are unique and only known to your organization. Protecting these keys is the central challenge for a data encryption strategy.

Protecting encryption keys from loss is the special province of security companies who create encryption key hardware security modules (HSMs) for this purpose. These systems are a combination of hardware and software specifically designed to create and manage encryption keys, and to restrict their use to authorized users and applications. Key management HSMs also incorporate a variety of security techniques to thwart unauthorized access, report on suspicious system activity, and mirror critical information to backup servers for high availability.

Alliance Key Manager from Townsend Security is a key management system that provides all of these services to organizations large and small.

Key Management Standards and Best Practices

Because encryption key management is crucial to data protection, the National Institute of Standards and Technology (NIST) provides guidelines on best practices for key management, and a cryptographic module certification program. The NIST Special Publication SP-800-57 provides recommendations for encryption key management. Additionally, NIST publishes standards for cryptographic systems in the Federal Information Processing Standards 140-2 (FIPS 140-2). Key Management vendors can have their solutions certified by NIST to the FIPS-140-2 standard, and this certification is required for Federal agencies. Townsend's Alliance Key Manager solution is FIPS-140-2 certified to this standard.

Security Architects and Compliance Auditors Look for NIST-Certified HSM Solutions

Security professionals and compliance officers in private companies and organizations recognize the importance of FIPS 140-2 certification as an indicator of the quality of a key management solution, and insist on this certification from their vendors. Auditors also understand that proper encryption key management is beyond the technical scope of most organizations, and look for NIST standards and certification.

Organizations that use non-standard or uncertified solutions are often subject to extra scrutiny around key management practices. Mid-market and smaller organizations are experiencing audit failures around their key management practices. Rectifying a key management audit failure can be an expensive and time consuming task. You can avoid this potential problem by deploying a key management solution that can withstand auditor scrutiny.

From the PCI DSS:

> *Strong Cryptography: Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 for more information.*

Microsoft SQL Server 2008/2012 Extensible Key Management (EKM)

Recognizing the importance of proper key management for data security, Microsoft implemented Extensible Key Management (EKM) in SQL Server 2008. EKM is both a new architecture for encryption key management services, and a new interface for third party key managers such as Alliance Key Manager from Townsend Security. While EKM provides for local, on-server management of encryption keys, Microsoft and third party security professionals recommend the use of external key management HSMs. Alliance Key Manager is designed for use with Microsoft SQL Server EKM as a hardware security module.

From Jefferson Wells on HIPAA compliance:
When enabled, EKM can provide a common interface to third-party key management and HSM to encrypt the keys used for data encryption and to directly encrypt the data itself. Once registered with EKM, these modules can be used by SQL Server to leverage the extended functionality provided by the HSM. These solutions work seamlessly with SQL Server 2008/2012 databases and support enterprisewide, dedicated key management. This allows the key management function to be performed by a dedicated key management system instead of SQL Server. When implementing EKM, remember to:

- *Store all keys separately from the data (SQL Server 2008/2012 supports the use of HSMs to provide the physical separation of keys from data)*

Transparent Data Encryption (TDE)

Transparent Data Encryption, or TDE, is a part of the Microsoft SQL Server Extensible Key Management system. When implemented, TDE encrypts the entire database table space providing security for the entire database. The key management HSM contains the master key that protects the entire table. Many Microsoft customers prefer the TDE approach to protecting data for several reasons:

- It is easy to implement and does not require modification of the application.
- The key that protects the database never leaves the HSM, providing better security.
- The impact on performance is smaller than other alternatives.

The benefits of using Transparent Data Encryption with a key management HSM are clear. Customers protect all of their data and rest assured that they did not miss important information; it matches the best practice recommendations of security professionals and compliance auditors; the performance degradation is minimal; and it is the easiest and least expensive solution to implement.

In a white paper on SQL Server security Caturano and ParenteBeard recommend:

> *"... key management is best handled through an EKM provider. An EKM provider can handle split key management by requiring multiple users to authenticate when performing administrative functions on the keys, such as changing permissions. To ensure segregation of duties, however, please bear in mind that the database owner and/or sysadmin should be independent of the EKM administrator. As another added control feature, EKM also separates the keys from the SQL Server application using the keys, so that keys are not stored with the data."*

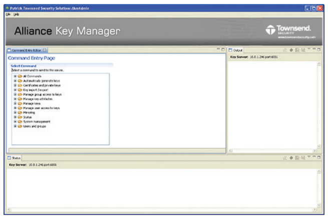
Cell Level Encryption

Cell Level Encryption, or column encryption, is also a part of the Microsoft SQL Server Extensible Key Management system. When implemented, cell level encryption encrypts a single column of a table. Unlike TDE, the Microsoft developer must implement cell level encryption in their application code using SQL calls. For Microsoft customers and ISVs who have legacy applications that perform encryption, this may be the best way to implement data protection in the SQL Server database.

The benefits of using encryption with a key management HSM are clear. Customers protect their sensitive data from loss; the costs of breach notifications are minimized or eliminated; it matches the best practice recommendations of security professionals and compliance auditors; legal liability is minimized; and it is easy to implement in the SQL Server database.

Alliance Key Manager for SQL Server

Alliance Key Manager is a general purpose HSM from Townsend Security that integrates naturally with Microsoft SQL Server. The key manager creates, stores, and protects encryption keys used by SQL Server and provides the Separation of Duties and Dual Control required by the PCI Data Security Standard and other compliance regulations. In addition to providing key management services to SQL Server, Alliance Key Manager provides encryption keys for applications throughout the organization.



Key Server: 10.0.1.246 port 6001

Key Server: 10.0.1.246 port 6001

The Key Connection software that accompanies Alliance Key Manager installs on the Windows Server running the SQL Server database to provide the connection between SQL Server and the key manager. Key Connection stores the configuration information, the list of available key servers, and information on the certificates used to protect the connection to the HSM. Key Connection is the EKM Provider registered to SQL Server by the database administrator to start encryption of the SQL Server database. A natural Windows install, licensing, and configuration interface makes it easy to deploy by system administrators.

EKM and Key Manager Secure Connections with TLS

Key management best practices require that encryption keys be protected at all times and not be exposed to loss as they move from the key server HSM to the SQL Server application. Alliance Key Manager uses authenticated and secure Transport Layer Security (TLS) version 1.2 communications to insure that critical information is protected as it moves to and from the key server. The Alliance Key Manager HSM uses standard PKI methods for TLS protection. Your organization can use existing PKI infrastructure to create the necessary X509 certificate and private keys used to protect TLS sessions, or you can use OpenSSL to generate the necessary certificates and keys. Regardless of the method you use to create the certificates and keys, Alliance Key Manager will always protect encryption keys and sensitive data as it moves between SQL Server and the HSM.

Key Management Resilience

Encryption key management systems are a part of an organization's critical infrastructure and must be able resilient to normal disruptions. Alliance Key Manager for SQL Server incorporates a number of features to increase resilience:

- Key server hardware uses dual, hot swappable, RAID protected disk drives to protect against disk failure (1U rackmount system)
- Alliance Key Manager mirrors all encryption keys in real time to a high availability key server
- Key Connection software on the Windows Server automatically fails over to one or more high availability key servers
- Key Connection software automatically restarts as a service in the event of an operating system interruption.

When combined with other system protections in the modern data center such as UPS power, the Alliance Key Manager HSM achieves a very high resiliency profile.

Key Management Scalability

Organizations often start small when implementing encryption and increase their use of encryption over time. The Alliance Key Manager HSM can scale with your growing need to protect encryption keys across a wide variety of applications and servers. You can start with the small footprint mini-server version of the Alliance Key Manager HSM and use it just with SQL Server, then graduate to multiple key servers or the 1U rackmount server. The larger key manager server has a larger key storage capacity ranging into millions of encryption keys, more memory to handle higher workloads, and faster processors. You can also mix small and large key servers in the same organization to support a distributed application environment or point solutions.

Barriers to Adoption (Money, Time, Complexity)

There are many barriers to the deployment of good data protection. Overpriced key management HSMs; complex solutions that require a lot of time to deploy or expensive developer resources; expensive consulting services required by vendors; hard to deploy and install software; and a variety of other challenges slow down the adoption of good data protection.

Townsend Security's Alliance Key Manager solution drives down these barriers with an HSM that scales in price to your actual needs, is easy to install and configure, is NIST certified to keep you compliant, and works automatically with the Microsoft SQL Server database. You can centrally manage multiple key server HSMs to reduce the cost of administration, and built-in key mirroring reduces the costs of backup and recovery procedures.

Townsend Security

Townsend Security provides NIST-certified encryption and logging solutions for the Enterprise. Our encryption, key management, tokenization, and logging solutions protect sensitive data from loss, whether it rests within, or is transmitted outside, of your organization.

Our certified database encryption and key management solutions are guaranteed to meet the encryption and key management meet or exceeds the standards in PCI, HIPAA/HITECH and more. Organizations worldwide rely on Townsend Security for their data privacy needs.

Web:	www.townsendsecurity.com
Phone:	(800) 357-1019 or (360) 359-4400