White Paper

Critical Steps to Encryption & Key Management in the Microsoft Azure Cloud

Understanding Options and Responsibilities for Managing Encryption in the Microsoft Azure Cloud

By Stephen Wynkoop,
SQL Server MVP, Founder & Editor at SSWUG.ORG

www.townsendsecurity.com

Data at Rest is Data at Risk

As soon as you have data stored for later reference, you are faced with the challenge of protecting that data. This essentially includes every piece of information - certainly those that are personally identifiable or relate to activities that require compliance and protection of information. That's quite a wide array of information, and it's important to make sure you're doing the important work of protecting information in a way that works both with your applications and with the regulations, agencies and compliance requirements that impact you.

Encryption addresses many facets of this challenge by protecting information at rest: the information that is stored and referenced, but needs to be unable to be used by unauthorized individuals or entities. Encryption works by having two elements to the process.

If you imagine a house, it typically has doors with locks and, of course, keys to those doors. Those keys are the same thing as your encryption keys. You first have to encrypt the data (lock it up), and then have a set of keys that provides for legitimate access, while working to prevent unauthorized access.

With technology-based solutions, the platforms used largely drive the process of locking and securing data. From the applications development tools and environment to the data storage tools, you'll find that there are a number of steps and options you have as a consideration for the job. Cloud providers both provide a level of security, and add complexity to the security picture, all at the same time. There are important questions to be understood and considerations in your deployment. We'll cover some of these here.

In this paper, we'll take a quick look at some of the considerations in these areas and see how they can help narrow down your options to those that best fit your requirements. We'll be looking specifically at the Microsoft Azure offering as the platform of choice.

Architecture Decisions Drive Technology Approach

When you set up your environment, you typically end up considering a couple of different approaches while selecting your data storage choice. The options range from fully-managed data storage and access (Windows Azure SQL Database, WASD) to setting up a SQL Server with a Virtual Machine instance.

Each certainly has its place, but there are big differences in options they support.

To get started, I'd recommend that you take a quick look at our appendix of terms. If you already know what we're talking about, you can go ahead and read on; however, we do want to provide some background for the best understanding.

Here are some essentials of encrypting data both in general and with SQL Server.

- **Transparent Data Encryption (TDE) –** There are tools within SQL Server to let you "point and shoot" to enable and activate encryption. This will let you indicate the database and log files you want to encrypt, set up the certificate and keys and "set it and forget it." This is more of an all-or-nothing approach to encryption.
- **Columnar Encryption –** SQL Server supports columnar (also referred to as column-level or cell-level) encryption. This lets you encrypt specific elements of your tables within a database, but can require development work when compared with TDE since it's not an all-or-nothing approach.
- **Master key –** Like a master key to the office or house, this key essentially opens the cabinet of certificates – it provides global access to the other encryption certificates and keys. You create the key and then must back it up, keeping it away from the server.
- **Certificate –** This is part of the encryption process and is used in encrypting your data. You use the certificate to securely retrieve an encryption key used to protect your data.
- **Extensible Key Management (EKM) –** An interface to SQL Server that allows for managing the keys in use in the system.
- **Hardware Security Modules (HSM) –** Typically third-party modules, physical or logical systems that manage and protect keys, rotation of keys and controlling access to the various encryption keys in use on the system.

> ***Important Note:***
> *Encrypting data is not the only encryption and data protection area you'll want to address.*
>
> *Specifically, data in transit to and from the database must also be protected. This includes front-end applications that use that information.*
>
> *Key information needs to be protected from*

"cradle to grave" – from the time it's input for the first time or received to the time it's ultimately destroyed, perhaps years down the road.

Virtual Machines

This option is a full implementation of SQL Server. You select the version, the edition of SQL Server, the hardware profile it will run against. This gives you the ultimate control and you have access to all of the tools of SQL Server for the edition you select. This means things like encryption and other functionality are available.

This also means, however, that you are responsible for the system. In this type of system, this means you will be managing backups, disaster recovery planning, systems growth, any kind of system updates and so-on. In traditional hosting terms, this is very similar to a co-located system.

You will also have access to key management opportunities, including integrating in an HSM to help manage your keys.

Key Decision Points, VMs

A key area of concern is the selection of a solid key management system. By selecting the right tools to manage your keys, and therefore the protection of your information, you can make sure that your security is implemented correctly. You must choose an encryption management system that is highly secure, certified and is able to work directly in the Windows Azure cloud environment.

You will need to select a hosting solution for your key management system – like the selection of the VM for hosting your SQL Server, you'll be choosing from very similar options to implement your key manager. You can host the solution on a VM managed by you – alternatively, you can use cloud services to provide for your key management.

Windows Azure SQL Database

When you move to WASD, you will be using a more managed approach to your systems; that is, you'll be working with Microsoft® to manage your systems. The cost of this management can change with some of the features offered. One of these features is the implementation of encryption for your databases.

In short, you'll need to encrypt the data as it is placed in the database, rather than having the database engine do the work for you. This means you'll need an encryption system that will let you step into the saving and updating process and encrypt and decrypt information as needed.

Important Note:
Key management options in WASD are limited and may not meet compliance regulations.

SQL Server and Data Encryption Choices

You have several areas to consider when setting up encryption for SQL Server. These include the application of TDE (as outlined earlier), where you encrypt the entire database and associated log files. This is a great option for protecting your systems on a very broad basis.

The second option you have is encrypting only specific bits of information. This allows for more control, but it can also have an impact on the development requirements for deployment of the solution. In other words, programming and development may be required, since the columns will be encrypted and decrypted selectively.

The final major area(s) of encryption consideration are SQL Server backups. Keep in mind – in a cloud environment you are, indeed, "sharing" a system (in all likelihood). This isn't so much a "scare tactic" point, but just to say that resources, backups, storage locations, etc. all are outside of your physical control.

You can protect your information and systems that you're backing up by using encryption on the backups. You have several options and each is available during the backup process and can be established using the maintenance plan tools or the manual backup job creation options.

Impact of Encryption

Encryption, and the impact of encryption on your systems, is a big area of concern for those deploying it. Three different areas are important to consider when impact on systems is considered.

Performance

Depending on the overall performance and utilization of your systems, you may see minor overhead (2-4%) processing encrypted information (or access to it). This is simply due to the processing required to encrypt/decrypt information. Typically the impact on applications performance is negligible. One area where performance impact can become more pronounced is in the case of larger databases. Be sure to test your specific application to determine how best to handle and deploy the encryption steps required for your own environment.

Backup and Restore Operations

Backup and restore operations that utilize encryption can take a bit longer as the information is processed and encrypted/decrypted as needed. This can add time to the

backup and restore process. With SQL Server it's possible to address this a number of ways, from segmenting backups to managing backup sizes, types and frequency. You may also see an increase in the backup file sizes (and therefore storage requirements) due to the poorer compression of encrypted data vs. its often text-based source data.

High Availability

Key management is fundamental in a high-availability environment. A strong key management solution brings load balancing, key mirroring, access policy mirroring and high-availability failover capabilities. These are key elements to making sure your systems are performing as required and they limit the risk to your applications in terms of availability and performance.

Key Management Fundamentals

There are core best practices to consider while you're deploying your selected solution. Some are procedural while others are software/hardware implementations. Keep in mind that the key is to protect your most important secret: the keys. You must provide for protection of the keys, while still providing for access, updates and rotation of those keys.

Segregation of Duties

Like compliance regulations surrounding database work in general, you want to make sure you segregate duties when it comes to managing keys. With proper software and solutions in place, you can control who has access to rotate keys, who can apply new keys and so-on, all while protecting access to master keys and elements you want and need to protect.

Dual Control & Split Knowledge

Much like a military missile launch, dual control and split knowledge requires that to work with keys and to execute certain critical tasks, it takes two people to do so. No one person has the ability to complete the task. This provides for the double-check that the operation needed is, indeed, needed.

This also applies to split-knowledge. No one person has all of the information needed to complete the operation. You need both people to be participating to complete the needed task.

Key Rotation

Key rotation refers to the practice of refreshing and replacing your keys. In essence, it's a re-encryption of the information in your systems. This means the creation and application of new keys for your information and the management of changing out those keys. Typical recommendations on key rotations vary based on the industry, types of regulation and compliance that are applied, etc. Some examples might include rotation of keys on an annual basis or even a monthly basis.

Protection of Keys

It may see obvious, but protecting your keys is essential. Your keys should never be kept on the same machine as they are used. Doing so is essentially providing access to your data, much like posting a file in the root of your server with a file name of "passwords.txt" and then including all access passwords for applications, your database systems and so-on.

Keys should be maintained in a secure location, preferably with a secure appliance built to provide that protection and access to authorized personnel only.

Access Controls and Audits, Logging

There are several different points of access control to consider as you set up your solutions. First is physical access. Like your servers, you want to limit physical (and logical) access to your servers and instances. Think of access as a "need to know" basis – you want to make sure those that have access have been fully vetted and understand the gravity of that access.

Next you must address access to the systems in terms of logins, access to the code, access to the keys and other applications. Access should be minimized, controlled and logged. It's also critical that those logs, and the logs of unauthorized attempted access, are reviewed and audited regularly.

How Townsend Security Answers These Challenges

Townsend Security's Alliance Key Manager provides key answers to these challenges of working with Azure, securing information and the need to manage the keys and security of that information.

Alliance Key Manager for Microsoft Azure provides a FIPS 140-2 compliant encryption key manager to Windows Azure users who need to meet data privacy compliance regulations and security best practices.

Alliance Key Manager for Microsoft Azure supports the following features:

- Deploys as a virtual machine in a cloud service
- Deployed in public or private clouds
- Protects data in Microsoft Azure Iaas and PaaS environments
- FIPS 140-2 compliant
- OASIS KMIP compliant
- Licensed as a subscription

These key features, and the industry proven Townsend Security solution's team will work with you to show you how to address compliance requirements and how to assure that your information is safe, protected and that you have the right systems in place to provide for that protection going forward.

Contact us today to find out more about getting started, activating a trial of the Alliance Key Manager or to further discuss exactly how compliance requirements, best practices and rock-solid security measures can come together to protect your systems and data.

Further Resources

For more information on Alliance Key Manager for Windows Azure, download our solution brief or get started with a free 30-day evaluation.

About Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST-validated and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, SOX, and other regulatory compliance requirements.

We invite you to learn more about us and view comments on the latest happenings in the security and encryption space by going to our blog.

About Stephen Wynkoop

Stephen Wynkoop is the founder and editor for SSWUG.ORG – the SQL Server Worldwide User's Group where he writes a column and maintains the site overall. SSWUG features a weekly video programs about the database and IT world, webcasts, articles, online virtual community events and virtual conferences several times a year. Stephen is a Microsoft SQL Server MVP and the author of more than 10 books, translated into at least 7 languages. Stephen has been working with SQL Server since the very first version, with a prior experience in database platforms that included dBase and Btrieve. Stephen can be contacted at swynk@sswug.org.