KEY MANAGEMENT

# Alliance Key Manager for Microsoft Windows

Solution Brief

## Meet Regulatory Compliance with Key Management

Organizations of all sizes around the world are required to protect sensitive data such as credit card numbers, social security numbers, bank account numbers, driver's licenses, patient health information, and similar data. This information can be used for identity theft and other types of fraud, and protecting consumer and employee information is a high priority of governments and private regulators. The loss of sensitive data exposes organizations to civil and criminal penalties, and can lead to substantial financial losses.

One of the critical tools used by organizations to prevent data breaches is encryption combined with good encryption key management. Many compliance regulations such as the Payment Card Industry Data Security Standard (PCI DSS) require encryption to protect data. Other regulations strongly recommend encryption, or provide safe harbor exclusions from legal liability only if encryption is used (see HIPAA / HITECH Act of 2009). Encryption is now recognized as a best practice for protecting sensitive information, and is rapidly being deployed by organizations large and small.

Townsend® SECURITY

**NIST Compliant**
FIPS 140-2 Level 1

AES Encryption
(All key sizes, all modes of encryption)

SHA Validation

**Cost-Effective**
Affordable key management solutions for any size Enterprise.

**Compatible**
Alliance Key Manager works with all major business platforms, leading encryption applications, and even legacy devices connected via serial port.

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

## Data Security and Compliance

Encryption key management is a companion technology to encryption, and all data security regulations recognize that an encryption strategy is only as good as the method used to protect encryption keys. This is why PCI DSS and other regulations, and the security auditors who enforce these regulations, are reviewing encryption with a view to good key protection. Many organizations that use encryption to protect sensitive data are being required to address deficiencies in their key management strategy.

This solution brief describes how Alliance Key Manager from Townsend Security helps Windows customers achieve good key management practices to meet compliance regulations.

## Alliance Key Manager for Windows Data Security

The biggest challenge to Windows users deploying encryption is the proper implementation of key management. Microsoft provides encryption libraries in many of its development libraries, but key management is left to each Windows customer. Encryption key management is a specialized technology implemented in Hardware Security Modules (HSMs), Cloud HSMs, VMWare, or in the Cloud. Proper key management requires a separation of the encryption keys from the protected data, procedural controls to insure separation of duties, and access controls that insure dual control of key management.

Alliance Key Manager provides proper key management on Windows server platforms.

While not restricted to the Windows platform, Alliance Key Manager contains many features that are advantageous to Windows application developers, and which shorten the deployment time for key management. Additionally, Alliance Key Manager is an affordable solution for the many mid-size organizations that need to deploy key management.

## Key Retrieval Architecture

Alliance Key Manager implements a “wire” protocol for encryption key retrieval. This means that you do not need to install software libraries in order to communicate with the key server. Any application that can create a TLS connection to the server can initiate a key retrieval exchange. This exchange uses a mutually authenticated TLS connection to the key server over your existing TCP network. The X509 certificates used for the secure connection and for authentication are stored in the Windows certificate manager. Alliance Key Manager verifies that the certificate used is authorized to the encryption key you are retrieving.

Because Alliance Key Manager does not require the installation of software on the Windows platform, you do not have the challenge of updating that software with new versions, or due to security issues with the vendor software. Neither do you have to worry about client-side license fees and vendor license controls. This reduces the administrative effort and costs associated with key management.

While vendor software is not required from Townsend Security, we do provide you with pre-compiled binaries and sample source code to speed the deployment process. You can leverage this optional software to help get your data security projects completed quickly and at low cost.

## Key Management and Compliance

Encryption key management based on industry best practices and industry standards is now a de facto requirement by security auditors. The primary source of key management best practices is the National Institute of Standard and Technology (NIST) in the Special Publication 800-57 (Recommendation for Key Management). The primary standard for certification of key management solutions is the NIST Federal Information Processing Standard 140-2 (FIPS 140-2). This document and certification protocol are the basis for almost all compliance regulations where encryption is required. Organizations that want to insure they are deploying proper key management will look for the implementation of these standards.

Alliance Key Manager implements the best practices defined by NIST, and has achieved FIPS 140-2 validation (certificate number 1449). With Alliance Key Manager Windows customers can be sure that their key management solution meets current and future compliance regulations and best practices.

## Microsoft .NET Application Support

The most common .NET programming language used by Microsoft application developers is C# (C Sharp) and is supported in the Microsoft Visual Studio development platform. The .NET development environment is functionally rich and optimized for business and Web application development. This environment also provides support for AES encryption of sensitive data.

Alliance Key Manager provides support for .NET application developers by providing sample C# source code to help developers quickly deploy good key management solutions. This source code can be added to existing .NET applications to replace poor key management solutions such as storing keys in database files, on shared folders, and so forth. In most cases Windows developers can quickly deploy key management with Alliance Key Manager very quickly using the provided sample code:

```
// Allocate the KeyService object
            KeyService keyService = new KeyService();

            // Set the address of the key server
            keyService.Server = “akm.example.com:6000”;

            // Set key name to retrieve
            String keyName = “Orders”;

            // Retrieve the key data from the server
            EncryptionKey encryptionKey = keyService.
RetrieveEncryptionKey(keyName, null);

            // Copy the key bytes into a pinned array
which is used in SymmetricAlgorithm’s key.
            byte[] key = new byte[encryptionKey.
ByteLength];
            GCHandle gch = GCHandle.Alloc(key,
GCHandleType.Pinned);
            try
            {
                encryptionKey.CopyKeyBytes(key);
                algorithm.Key = key;
            }
            finally
            {
                for (int i = 0; i < key.Length; i++)
                {
                    key[i] = 0;
                }
                gch.Free();
            }

            // The key can now be used for encryption
```

## Microsoft SQL Server Data Protection

Windows application developers need a functional and scalable database system to store business data. The most commonly used database is Microsoft SQL Server. This database can scale to handle many concurrent users and lots of data. Its functionality makes it a popular choice for Windows developers. It works well with .NET applications and enjoys wide support from Microsoft and the Windows developer community.

Windows users can easily protect sensitive data in SQL Server databases by encrypting column data before it is inserted into or updated in the database, and decrypting the column data when it is read from the database. C# makes this easy to do, and very minimal programming is required for key retrieval and encryption.

Because SQL Server uses the SQL language for data manipulation it is not necessary to modify any application that does not actually use the sensitive data.

## Microsoft Access and FoxPro Protection

In addition to the SQL Server database, Microsoft also supports the Access database (a part of the Microsoft Office suite) and FoxPro. These database systems are not a part of the .NET development platform, but they are popular alternatives for smaller applications. Developers have used these databases when they need to develop a solution quickly, and where multiple users and scalable database solutions are not required.

Alliance Key Manager supports key retrieval in these environments through the use of callable .NET applications that perform the key retrieval function. Your Visual Basic applications can make a call to a .NET module to perform key retrieval and encryption, and then update the Access database. In a similar way you can access key retrieval and encryption in your Visual FoxPro applications to read and write sensitive information to a FoxPro database. Microsoft provides documentation and samples on the MSDN web site for developers.

## Oracle, IBM, and MySQL Database on Windows

Some Windows customers use commercial database systems from IBM and Oracle, or the open source MySQL database. While it is feasible to use .NET development languages to interface with these databases, it is more common to use Java or other development languages. Alliance Key Manager provides example key retrieval source that can be used with these languages and databases, and you are not restricted to using one of the .NET languages.

## Java, Perl, PHP, Flex, and Other Languages

Many Windows customers use non-Microsoft application languages for business and web applications. These languages include Java, Perl, PHP, Adobe Flex, and many others. Because Alliance Key Manager uses a wire type of protocol based on TLS communications and authentication, you can easily retrieve encryption keys in these languages to perform encryption and decryption tasks. Alliance Key Manager provides sample code in Java, Perl and other languages to help you get started, and these samples can be used in the Windows environment.

## Sample Code and Pre-Compiled Libraries

To shorten the Windows development cycle Alliance Key Manager provides sample code and a pre-compiled .NET assembly that the developer can use for encryption key retrieval. The sample code and libraries implement the wire protocol for key management, and integrate with the Microsoft Windows certificate store to protect the certificates use in TLS connections and authentication. While the use of the Alliance Key Manager sample code and libraries is not required, they can be very helpful in speeding the development process.

## NIST Validation

Key management solutions are cryptographic systems that are validated by NIST to meet the highest standards for cryptographic modules. These standards are defined by NIST in the FIPS 140-2 standard. Alliance Key Manager has been validated by NIST to FIPS 140-2 Level 1 (certificate 1449). This standard incorporates the NIST standards for AES encryption, SHA secure hash, random number generation, and Hash-based Message Authentication Code. This is your assurance that Alliance Key Manager meets the strictest requirements for secure key management.

## Partner Programs for ISVs and OEMs

Townsend Security recognizes the need of Microsoft partners for an affordable key management solution and a partner who will help them integrate the solution with their applications. In addition, partners need a relationship that will help them meet their competitive requirements and business needs. This means flexibility in solution pricing, branding options, developer training, and a predictable business relationship. Townsend Security supports their partners by giving them the tools they need to meet compliance requirements in their applications.

## Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, and Linux. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.