ATIPXpress

Encryption of Data at Rest

v11.8.0

December 2024

OPEXUSTECH.COM

ATIPXpress v11.8.0 Encryption of Data at Rest

Notice of Rights

Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (AINS, LLC.) on an “As Is” basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

Notice of Trademarks

The publisher’s company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: AINS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

Non-Disclosure Statement

This document’s contents are confidential and proprietary to AINS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from AINS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of AINS, LLC.

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.

Contents

1 Introduction

Documents and Correspondence files in ATIPXpress can be secured through encryption when at rest, providing an additional layer of protection against unauthorized access. Encryption is turned on by default.

For Document and Correspondence encryption, the database is configured with one of the following values:

- No Encryption
- Use Encryption

When encryption is activated, one of the two following encryption types is selected:

Type	Description
New	The new encryption module, which is also compliant with FIPS 140-2, leverages the AES encryption algorithm with a 256-bit key length. Unlike the legacy encryption, it avoids storing any keys in the code. Instead, it generates the 256-bit length key, and the initialization vector values randomly during the data encryption process. It then encrypts the key using the public key from the certificate configured. The certificate's private key is used to decrypt the encryption key during the data decryption process. ATIPXpress offers a certificate maintenance tool to create and add self-signed certificate to the application server's machine certificate store (certificate name: AINS.Xpress.Encryption4). The certificate configured in the app server should be exported to all the VMs/containers where additional app servers or scheduler service instances run to ensure that they all use the same encryption and decryption keys.

Type	Description
Legacy	The legacy encryption module employs the AES encryption algorithm. This encryption module utilizes the AesCryptoServiceProvider and SHA256CryptoServiceProvider classes that are FIPS 140-2 complaint. It utilizes a 128-bit length key and stores key phrase, initialization vector, and other parameters in the library code. Protection of these parameters is enforced through obfuscation of the code and by permitting method calls only from authorized OPEXUS libraries.

If encryption is enabled, the same type of encryption is applied uniformly to both Documents and Correspondence throughout the application.

2 New Encryption

2.1 Introduction

FIPS 140-2 is a statement that is titled "Security Requirements for Cryptographic Modules." It specifies which encryption algorithms and which hashing algorithms can be used and how encryption keys are to be generated and managed.

ATIPXpress encrypts the data at rest using the FIPS 140-2 compliant encryption standards and methods. This document explains how ATIPXpress encrypts document data and database data at rest using the FIPS 140-2 validated Microsoft Cryptography API (CAPI) and Windows Cryptographic Service Providers (CSPs).

2.2 Document Encryption

2.2.1 About Document Encryption

ATIPXpress encrypts the documents and correspondence files in ATIPXpress document repository (document data at rest) using the AES (Advanced Encryption Standard) Symmetric Encryption algorithm and uses a 256 bit length key (AES-256). AES-256, which has a key length of 256 bits, supports the largest bit size and is practically unbreakable by brute force based on current computing power, making it the strongest encryption standard. The encryption is performed using a random generated key that's encrypted using a digital certificate configured by the system administrator. ATIPXpress installation and configuration guides provide more information on configuring the document encryption using the digital certificates.

2.2.2 AES Encryption using AESCryptoServiceProvider

ATIPXpress performs encryption and decryption of documents using its Ains.Xpress.CryptoLib library which is a Microsoft .NET library. This library uses Microsoft .NET's System.Security.Cryptography namespace and AESCryptoServiceProvider class which performs symmetric encryption and decryption using the Cryptographic Application Programming Interfaces (CAPI) implementation of the Advanced Encryption Standard (AES) algorithm.

2.3 User Password Encryption

ATIPXpress stores the one-way hash of the user passwords in the database when the authentication mode is Application Authentication (using Forms Authentication). The application uses SHA256 hashing algorithm to compute the hash value with salt bytes added and then stores the Base64 string value of the resultant bytes in the database. A salt is added to the hashing process to force their uniqueness, increase their complexity without increasing user requirements, and to mitigate password attacks like hash tables.

Note: This encryption is applicable only if the authentication mode is Application (Forms) Authentication. User passwords are not stored in the ATIPXpress database if the authentication mode is not Application/Forms.

2.3.1 SHA256 Hashing using SHA256CryptoServiceProvider

To compute the SHA256 hash value of the user passwords, ATIPXpress user management module uses the Microsoft.NET's System.Security.Cryptography namespace and **SHA256CryptoServiceProvider** class which provides the CAPI implementation of the SHA256 algorithm using the Cryptographic Application Programming Interfaces (CAPI) implementation of the SHA256 hashing algorithm. SHA256CryptoServiceProvider uses the FIPS 140-2 validated (FIPS = Federal Information Processing Standards) Crypto Service Provider (CSP).

2.3.2 Microsoft Windows Crypto API and FIPS Validation

Microsoft's Crypto API/CAPI uses RSAENH.DLL (Microsoft Enhanced RSA and AES Cryptographic Provider), which has been validated by NIST in the Cryptographic Module Validation Program. RSAENH.DLL is FIPS 140-2 complaint. Both AesCryptoServiceProvider and SHA256CryptoServiceProvider call the FIPS 140-2 version of this DLL on Windows servers supported by ATIPXpress application.

Please see below link for Microsoft's approach to FIPS 140-2 Validation and FIPS certification information by cryptographic modules.

https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation

2.4 Database Encryption

SQL Server database can be configured to be FIPS 140-2 compliant because it can be configured and run in such a way that it uses only the FIPS 140-2-certified algorithm

instances that are called by using CryptoAPI for encryption or by hashing in every instance in which FIPS 140-2 compliance is required. The SQL Server database files are encrypted using Microsoft's Transparent Data Encryption (TDE) technology with AES (Advanced Encryption Standard) 256 algorithm.

The following link provides more information on TDE.

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15

The following link points to the article that introduces the FIPS 140-2 instructions and how to use SQL Server2016 in FIPS 140-2-compliant mode. This should be similar to the versions above 2016.

https://docs.microsoft.com/en-us/troubleshoot/sql/security/sql-2016-fips-140-2-compliant-mode

2.5 Field Encryption

ATIPXpress uses Microsoft SQL Server's Always Encrypted columns to encrypt selected fields in the database. Always Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine (SQL Database or SQL Server). As a result, Always Encrypted provides a separation between those who own the data and can view it, and those who manage the data but should have no access.

ATIPXpress Configuration Tool allows the administrator user to configure the field encryption settings.

Field encryption using Always Encrypted columns is supported for the following fields as of ATIPXpress version 10.8.

Module	Fields
ATIPXpress	▪ Email Id ▪ Address 1 ▪ Mobile ▪ Home Phone ▪ Work Phone 1 ▪ Work Phone 2 ▪ Request Custom Fields ▪ Requester Custom Fields
Public Access Link (PAL) Requester Fields	▪ Last Name ▪ Login ▪ Email Id ▪ Address 1 ▪ Mobile ▪ Home Phone ▪ Work Phone 1 ▪ Work Phone 2 ▪ Request Custom Fields ▪ Requester Custom Fields

3 Legacy Encryption

3.1 Legacy Encryption Introduction

3.1.1 About Legacy Encryption

ATIPXpress legacy encryption uses the Crypto API for Advanced Encryption Standard that is FIPS 140-2 complaint.

The ATIPXpress legacy encryption module uses the AesCryptoServiceProvider and SHA256CryptoServiceProvider classes that are FIPS complaint. These classes are available in the System.Core assembly of the Microsoft.NET framework. Both AesCryptoServiceProvider and SHA256CryptoServiceProvider classes call the Crypto API, which uses RSAENH.DLL (Microsoft Enhanced RSA and AES Cryptographic Provider), which has been validated by NIST in the Cryptographic Module Validation Program. RSAENH.DLL that is FIPS 140-2 complaint and AesCryptoServiceProvider and SHA256CryptoServiceProvider call the FIPS version of this DLL.

3.1.2 AesCryptoServiceProvider

Performs symmetric encryption and decryption using the Cryptographic Application Programming Interfaces (CAPI) implementation of the Advanced Encryption Standard (AES) algorithm.

AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES). The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable (see Advanced Encryption Standard process for more details). It became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages and is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.

The encryption module utilizes a 128-bit length key and stores key phrase, initialization vector, etc. parameters in the library code. The protection of these parameters is enforced through obfuscation of the code and by permitting method calls only from authorized OPEXUS libraries.

3.1.3 SHA256CryptoServiceProvider

The SHA256CryptoServiceProvider Defines a wrapper object to access the cryptographic service provider (CSP) implementation of the SHA256 algorithm.

The Secure Hash Algorithm is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS):

SHA-0	A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.
SHA-1	A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm.
SHA-2	A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. There are also truncated versions of each standardized, known as SHA-224 and SHA-384. These were also designed by the NSA.
SHA-3	A proposed hash function standard still in development. This is being chosen in a public review process from non-government designers. An ongoing NIST hash function competition is scheduled to end with the selection of a winning function, which will be given the name SHA-3 in 2012.

The corresponding standards have been FIPS PUB 180 (original SHA), FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA-1, SHA-256, SHA-384, and SHA-512), FIPS PUB 180-3 (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512).

3.2 FIPS Policy

Enabling FIPS policy from registry ensures that NON FIPS complaint algorithms will throw an exception saying “Error: This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms”. We don’t see this error with the ATIPXpress legacy encryption module because it uses all the FIPS 104-2 compliant cryptographic algorithms.

3.3 Compatibility and Support

AesCryptoServiceProvider and SHA256CryptoServiceProvider work on systems where AES was implemented in RSAENH.DLL which is Windows XP and higher OS’s. It will not run on Windows 2000.

The following link provides the document that specifies the security policy for Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) as described in FIPS PUB 140-
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1010.pdf

3.4 FIPS 140-2 Compliance Certification

The Microsoft Corporation’s Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) is a FIPS 140-2 Level 1 compliant, software-based, cryptographic service provider.

The following table shows the Microsoft’s certification details from the NIST site.

1010

Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA Dave Friant TEL: 425-704-7984 FAX: 425-936-7329
Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) (Software Versions: 6.0.6001.22202 and 6.0.6002.18005) (When operated in FIPS mode with Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1006 operating in FIPS mode) Validated to FIPS 140-2 Security Policy Certificate
Software
08/15/2008; 07/24/2009

Overall Level: 1

-Operational Environment: Tested as meeting Level 1 with Microsoft Windows Server 2008 (x86 Version); Microsoft Windows Server 2008 (x64 version); Microsoft Windows Server 2008 (IA64 version) (single-user mode)

-FIPS-approved algorithms: AES (Cert. #739); HMAC (Cert. #408); RNG (SP 800-90, vendor affirmed); RSA (Certs. #353 and #355); SHS (Cert. #753); Triple-DES (Cert. #656)

-Other algorithms: DES; MD2; MD4; MD5; RC2; RC4; RSA (key wrapping; key establishment methodology provides between 80 and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength)

Multi-chip standalone

“RSAENH encapsulates several different cryptographic algorithms in an easy-to-use cryptographic module accessible via the Microsoft CryptoAPI. Developers dynamically link the Microsoft RSAENH module into their applications to provide FIPS 140-2 compliant cryptographic support.”

The table above can be found at the following link: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm.