

Alliance AES Encryption Data Sheet



Alliance AES Encryption for Windows, Linux, UNIX

Alliance AES Encryption is a library of encryption functions that implement the Advanced Encryption Standard (AES) for the Windows, Linux, UNIX, and IBM System z platforms. The library implements the three main key sizes and five main encryption modes of AES and follows the National Institute of Standards and Technologies' recommendations for AES. This library is compatible with the Alliance AES Encryption support for UNIX, Windows, IBM System i (AS/400, iSeries), and IBM System z (mainframe, OS/390, z/OS) platforms.

Common Encryption APIs Speed Compliance

Alliance AES encryption implements a common interface to encryption across all Enterprise server platforms. This reduces project time, increases programmer efficiency, and minimizes points of failure.



Patagonia practices a special care in relation to the planet and environment. Their mission is "Build the best product, cause no unnecessary harm, use business to inspire and implement solutions to the environmental crisis." To achieve PCI compliance and protect their customers, Patagonia needed an AES encryption solution that was compatible with their JAVA applications running on Red Hat Linux and their RPG applications running on IBM i servers. Patagonia chose the Townsend Security AES encryption solutions to bridge these environments.

www.townsendsecurity.com

Encryption

- Advanced Encryption Standard (AES)

Key Sizes

- 128, 192, and 256-bit key support

Modes of Operation

- Electronic codebook (ECB)
- Cipher-block chaining (CBC)
- Output feedback (OFB)
- Counter (CTR)
- Cipher feedback (CFB)

Platforms

- Linux (Red Hat, SUSE)
- Linux PPC 64 (Red Hat, SUSE)
- IBM System i (AS/400, iSeries)
- IBM System i Linux (Red Hat, SUSE)
- IBM System z (mainframe)
- IBM System z Linux (Red Hat, SUSE)
- AIX
- Solaris
- Solaris 64
- Windows XP/2000/2003/2008

Implementation

- Shared library (Linux, AIX, Solaris)
- Dynamic Link Library DLL (Windows)
- Service program (IBM i)
- Shared library (IBM z)

Installation

- RPM for Linux, Solaris, AIX Windows MSI
- Installp for AIX
- Save file or LODRUN for IBM System i
- Binary FTP for IBM z

Language Compatibility

- C/C++
- Microsoft .NET
- Microsoft VB .NET
- Java (JNI)
- Microfocus Cobol
- OPM, ILE Cobol (IBM i)
- OPM, ILE RPG (IBM i)

Database & File Compatibility

- IBM DB2
- Oracle
- Microsoft SQL Server
- ISAM / VSAM
- Binary stream file

Compliance Logging

- Selective decryption logging
- Selective encryption logging
- Compliance reports

Monitor & Alert

- System audit journal (QAUDJRN)
- SNMP trap messages
- SMTP email notification
- QSYSOPR message queue
- PowerTech integration

Whole File Encryption

- DB2 file encryption
- Flat file encryption
- IFS / QNTC / NFS file encryption
- Save file (SAVF) encryption

Data Masking

- Mask all but last 4 digits
- Mask credit card number
- Mask name
- Mask address, city, state, zip code
- Mask driver's license
- Mask date

Cross-Platform Support

- Alliance AES Encryption for Windows
- Alliance AES Encryption for Linux (SUSE, Red Hat)
- Alliance AES Encryption for UNIX (AIX, Solaris)
- Alliance AES encryption for zSeries
- Self-decrypting archives for Windows

Discovery & Assessment

- User library discovery
- User file discovery
- Database analysis for sensitive data
- Program analysis and cross-reference
- User-defined search criteria
- Assessment reports

System Requirements

- IBM iSeries OS/400 or i5/OS V5R1 or later

Support

- Software maintenance
- Technical support
- 24/7/365 support available
- On site installation available
- Contract services available

Contact Us

Townsend Security
www.townsendsecurity.com
800.357.1019
360.359.4400