SECURE COMMUNICATIONS

PGP® Encryption for IBM i
Solution Brief

A Complete PGP Solution for the IBM i

Pretty Good Privacy (PGP) is the de facto standard for encrypted file exchange among the world's largest financial, medical, industrial, and services companies. Based on open standards and tested by time, PGP has won the trust of governments and private enterprises to protect their sensitive data.

This solution brief explores some key topics related to PGP encryption technologies to help you make an informed decision when you choose PGP encryption technology for your IBM i.

About 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, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.

Townsend® SECURITY

Reduce your recurring software and support costs with an affordable PGP encryption solution

Meet PCI, HIPAA, Sarbanes-Oxley, and Privacy Notification requirements for data encryption

Reduce time to deployment by automating encryption and decryption tasks

Achieve compatibility with PGP solutions on Windows, Linux, UNIX, and IBM z mainframes

Protect your investment with standards-based OpenPGP support

www.townsendsecurity.com

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

PGP Encryption for IBM i

The Alliance PGP solution provides a full implementation of PGP encryption, decryption, signing, and key management functions for the IBM i platform. A native IBM i application, there is no need for a separate PC or UNIX server for encryption services. And Alliance PGP provides a full set of automation capabilities including IFS directory scan, library scan, (APIs), and other services.

Alliance PGP fully supports Additional Decryption Keys (ADK). ADK is a critical component to support data recovery and regulatory compliance rules such as those in the Sarbanes-Oxley Act (SOX). PGP implementations that support ADK provide a means of recovering data you send to your trading partners, and provide an auditable proof of the data content. PGP implementations that are based on Open PGP don't support ADK, and can't provide assurance.

The Alliance PGP Option gives you the ability to fully manage public and private keys on the IBM i. You can create your own keys, export your public key to distribute to your trading partners, import your partner's public keys for your encryption tasks, view lists of keys, and revoke keys as needed. The key support provides everything you need to work with your trading partners.

Alliance PGP is used with several financial and medical insurance organizations. These include Bank of America, ABN Amro, Citibank, Citicorp, Zirmed, NBP, VSP Enterprise, and others. New interfaces are certified on a frequent basis. Please contact Townsend Security if you have questions about PGP compatibility with your trading partner.

The Regulatory Environment

Many large Enterprises are struggling to meet the data security requirements of the Payment Card Industry (PCI), Sarbanes-Oxley Act (SOX), state Privacy Notification laws, Gramm-Leach-Bliley Act (GLBA), and federal standards defined by the National Institute of Standards and Technology (NIST). While new standards are being developed on both state and federal levels, there are some clear requirements that are common to all of the regulations. The choices you make for your data security solutions will affect how well you meet current and future regulations.

The Seven Things You Need to Know

Here they are, the seven key things to know about PGP encryption for your IBM i platform, and how to discuss them with your technology providers:

- PGP Additional Decryption Keys (ADK)
- Native IBM i PGP encryption
- Native IBM i PGP key management
- Automation and application integration
- PGP is one part of a comprehensive Data Security plan
- PCI, Sarbanes-Oxley, California Privacy Notification, and the regulatory environment
- Who is the leader in IBM i data security?

This paper discusses each of these important areas about PGP encryption.

Native IBM i PGP Encryption

IBM I customers are justifiably proud of the security controls built into the IBM i operating system. Over time the IBM i platform has proven to be one of the most secure systems for Enterprise applications. IBM has integrated strong security controls into every aspect of the IBM i system including database, user access, and application access.

Sometimes IBM i users ask us:

"Why shouldn't I use PGP on a PC? It is cheaper to purchase PGP on a PC and all I have to do is transfer the data with Client Access."

Consider this: When you transfer your sensitive data from the IBM i to a PC you move that data from one of the most secure systems to one of the most vulnerable systems. The Windows operating system on the PC is the most common target for hackers and identity thieves. The single largest loss of confidential information happened from a Windows system. Moving data to a PC for encryption and decryption tasks greatly increases the chances of loss and puts your most sensitive data at risk. In order not to defeat your data security goals it is important to encrypt and decrypt data directly on the IBM i.

BEST PRACTICE FOR DATA SECURITY:

Always encrypt and decrypt sensitive data on the platform where it is created. This is the only way to satisfy regulatory audit and privacy notification requirements.

Alliance PGP encryption is a native IBM i solution that helps you meet data security goals. When combined with Alliance FTP Manager you will have strong audit trails for regulatory compliance and a high level of automation.

Native IBM i PGP Key Management

Cryptographers and data security specialists tell us that the management of encryption keys is as important as the strength of the encryption itself. In fact, the proper management of PGP encryption keys may be more important - the loss of encryption keys may put all of the past encrypted files at risk. This may risk years of encrypted files sent to trading partners or backed up to tape.

BEFORE YOU BUY A PGP SOLUTION, ASK YOUR VENDOR:

How are PGP keys managed in your application? Does your solution support native IBM i key management? Are PGP keys ever created or accessed from a PC?

The best PGP encryption solutions manage PGP keys directly on the IBM i without the need for an external PC system, or key generation on a PC. Using a PC to generate or manage PGP keys exposes the keys on the most vulnerable system. The loss of PGP keys may trigger expensive and time-consuming privacy notification requirements and force the change of PGP keys with all of your trading partners.

Alliance PGP encryption solutions use best practices for PGP key management. All PGP keys are created and managed directly on the IBM i platform and are controlled by native IBM i security and authorization lists.

Automation and Application Integration

Most Enterprise customers find that the cost of the software for an encryption solution is small compared to the cost of integrating the solution into their business applications. Data must be extracted from business applications, encrypted using PGP, transmitted to a trading partner, archived for future access, and tracked for regulatory audit. When receiving an encrypted file from a trading partner the file must be decrypted, transferred to a IBM i library, and processed into the business application.

All of these operations have to be automated to avoid expensive and time-consuming manual intervention. And, if something goes wrong (your trading partner's key expired, for example), you want to be automatically notified of errors.

The best data security solutions will provide you with IBM i automation tools that help minimize additional programming and meet your integration requirements. Look for these features in your solution:

- Automated encryption and transmission of files in a library
- Automated decryption of files with flexible rules for copying to a library
- Built-in Integration with IBM i and third party schedulers such as Robot
- Easy integration with business applications
- Automatic error notification in the event of an encryption or decryption failure
- Automatic error notification when transfers fail
- Error notification with SNMP, Email, and operator messages
- Audit trails of all encryption and transfer activity
- Operator's menu for retransmission
- Application monitoring of vendor and user jobs

ASK YOUR VENDOR:

How will your solution help us minimize the costs of automation and end-to-end application integration?

Alliance PGP encryption incorporates easy-to-use automation and integration facilities. Many Alliance customers find that they can automate their data security tasks without the need for application programming. Alliance customers successfully automate the secure transfer of thousands of files every day.

PGP is Part of a Comprehensive Data Security Plan

PGP encryption is ideal for exchanging data with trading partners, banks, insurance companies, benefits providers, and many other external partners. It's ability to run on any computing platform makes it ideal for this type of secure data exchange. But your data security needs reach far beyond PGP file encryption and the capabilities of PGP. A comprehensive plan for IBM i data security will also include:

- Database field encryption
- Tape encryption for archival
- Database whole file encryption
- IFS file encryption
- Spool file encryption, archival, and secure retrieval
- Save file encryption
- Compatible Windows and Linux encryption
- Point-of-Sale encryption solutions
- Encryption as a web service

These data security components are critical to complete your data security plan. But not all vendors of PGP encryption software are fully committed to the data security needs of the IBM i Enterprise customer. You can recognize a fully committed data security software vendor by their ability to meet all of your data security needs.

ASK YOUR VENDOR:

How will your solution help us minimize the costs of automation and end-to-end application integration?

Alliance data security products include all of the critical components you need for a comprehensive data security plan. Alliance encryption products include Windows and Linux solutions that support Visual Basic, .NET, SQL Server, and Point-of-Sale applications.

PCI, SOX, Privacy Notification, and the Regulatory Environment

There is one clear direction of payment industry, federal, and state regulations: You must secure your sensitive data at every place it exists on all of your computer systems and when you transfer it to outside vendors, customers, or employees. You must use approved encryption and key management techniques that are based on recognized standards. Additionally you must have audit trails and recovery methods that provide historical information about data transfer.

Even if your company is not directly subject to Sarbanes-Oxley and similar regulations, you will soon find that your customers who are subject to these laws will require that you be in compliance, too. As the financial auditing profession matures, auditors realize that their customers cannot meet regulatory requirements unless their suppliers meet these requirements. And they are moving to insure that this is the case. Don't get caught short with inadequate data security, you could find your most valuable customer relationships in jeopardy.

DATA SECURITY BEST PRACTICE:

Assume that you will be responsible for meeting all current and future data security requirements of Payment Card Industry (PCI), Sarbanes-Oxley, California Privacy Notification, and other data security regulations. Develop an action plan that shows demonstrable and achievable data security goals.

Who is the Leader in IBM i Data Security?

We all know that in every field of endeavor there are individuals and companies who stand out as leaders. Their commitment to excellence shows in the quality and completeness of their solutions, in their ethical standards, and in their company history. They respond to developing market trends and help their customers stay ahead of those trends. When their customers talk, they listen and respond.

Who is the leader in data security solutions for the IBM i platform?

Consider this list of data security firsts from Townsend Security:

- First native Triple DES encryption solution for the IBM i.
- First native PGP file encryption solution for the IBM i.
- First native 256-bit AES data encryption software product for the IBM i.
- First AES data encryption with CTR mode for the best database field security.
- First software-only tape encryption solution for the IBMi.
- First automated spool file encryption for the IBM i.
- First Save File encryption software for the IBM i.
- First cross-platform AES encryption solutions.
- First AES self-decrypting archive created completely on the IBM i.
- First AES encryption as a TCP sockets service on the IBM IBM i.
- The only data security solution for every aspect of your IBM i

When it comes to choosing a vendor for your IBM i data security needs, there is an easy choice: Townsend Security is the only company with a complete solution and a history of leadership.

CONSIDER THIS:

When PGP Corporation selected a partner to bring PGP version 9 to the IBM i, POWER Linux, and System 3 platforms, they selected Townsend Security as their exclusive partner. PGP Corporation's knowledge of Townsend's history with PGP on the IBM i platform made us the natural choice.

Free Trial

You can request a 30-day trial of Alliance PGP for your IBM i, or get a complete information packet.

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, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.