



PKWARE eNewsletter

August/September 2008

Hot off the virtual presses and straight to your mailbox...we're pleased to deliver the August/September 2008 edition of the bi-monthly PKWARE® eNewsletter! In this issue, you'll find helpful product and company news, success stories from some of our customers, and a white paper on how to control and ensure the security of data that must be exchanged with outside partners.

At PKWARE, we help thousands of companies around the world do business more securely and efficiently with our industry-leading data security, file management, and data compression solutions, SecureZIP® and PKZIP®. We hope this eNewsletter, in a small way, provides you with information that does a bit of the same. We welcome your comments, suggestions, and questions at editor@pkware.com.

In This Issue:

Product News: PKWARE Commits to Day One Support of Upcoming IBM® Mainframe Operating System Release 3

Success Story: Leading Financial Institution Achieves PCI DSS Compliance, Meets Multiple Security Initiatives with SecureZIP 4

Product Update: PKWARE Releases SecureZIP for Windows® Desktop, version 12.2 5

White Paper: Overcoming the Obstacles..... 6

Success Story: SecureZIP Delivers Ubiquitous Encryption Solution to Protect Sensitive Employee Data 6

Company News: PKWARE UK/EMEA Office Moves to London..... 7

Product News: Current Level Sets for IBM i and z/OS PKWARE Products 8

Product News: Technical Note – Masking Passphrases in JCL When Working with SecureZIP for z/OS 9

Product News: PKWARE® Commits to Day One Support of Upcoming IBM® Mainframe Operating System Release

PKWARE has committed that both SecureZIP® and PKZIP® for z/OS® will completely support IBM's next mainframe operating system release, z/OS v1.10, on Day One of its release, which IBM announced as September 26, 2008. PKWARE has ensured that versions 9 and 10 of the products are compatible with the new OS version and is, in fact, [one of only a handful of vendors worldwide](#) who have publically committed to such support.

Some time ago, a number of PKWARE customers notified IBM that our products are critical to their migration to the new release. Based on that endorsement and our good standing as an IBM Advanced Development Partner, PKWARE was included in IBM's Early Availability Program, giving us access to the new operating system release for testing, well in advance of many other independent software vendors.

The new z/OS release includes expanded capabilities for managing large data volumes, labeled as Extend Address Volume (EAV). EAV is planned to initially support 223 GB per volume on z/OS v1.10 and IBM System Storage DS8000, when available. This new capability will also be supported Day One for versions 9 and 10 of PKWARE's PKZIP and SecureZIP mainframe products.

"PKWARE prides itself as an industry leader in supporting mainframe operating systems and hardware advances," said Joe Sturonas, Chief Technology Officer for PKWARE. "We understand the importance our products can have in our customers' businesses, and highly value their confidence in and reliance on our products. Just as we've done to ensure Day One support for z/OS v1.10, we'll always work to deliver solutions that meet our customers' needs."

[Back to main page >>](#)

Success Story: Leading Financial Institution Achieves PCI DSS Compliance, Meets Multiple Security Initiatives with SecureZIP®

Company Background

Our client is one of the world's largest financial institutions, providing individual consumers, small/mid-market businesses, and large corporations with a full range of banking, investing, asset management, and other financial and risk-management products and services.

Challenges and Requirements

The company needed to meet PCI DSS compliance requirements, which required them to protect credit card data as it is transmitted, processed, and/or stored, impacting several processes throughout their organization. The company set out to protect and store this data for the mandated minimum of seven years. This information, however, was taking up space on their UNIX® Server, so the company also wanted a solution that could both encrypt and compress the data.

Every night, hundreds of thousands of settlement transactions containing confidential credit card information are sent to companies of all sizes. Without secure, dedicated lines set up for data transfer with smaller merchants, this confidential credit card data was sent via fax.

In an effort to secure this process, the company established an initiative to move all fax transmissions to email, electronically transferring encrypted data to multiple endpoints that would then need to decompress and decrypt the data after it was received. The data for these transactions originates on the company's z/OS® mainframe and is then transferred to an internal server before it is sent externally to merchants. The company needed a solution that would be easy to use and cost effective, especially for their business partners.

The Solution – SecureZIP

As soon as the company purchased SecureZIP, they quickly realized the solution could work for additional security initiatives throughout the organization. They engaged PKWARE® for assistance in achieving strong enterprise security across all major computing platforms.

The company wanted to use PKI to facilitate secure email communication, both internally and externally with business partners. SecureZIP was the only solution that could provide the level of functionality, customization, and ease of use required. The company also incorporated the RSA Keon Certificate Authority product, as well as the PKWARE ZIP reader, to round out the solution.

SecureZIP provided seamless integration with the centralized directories containing digital certificates issued by RSA. This supported the requirement for processing secure transactions, without slowing the delivery of reports to their partners. PKWARE's free ZIP reader extended the benefits of SecureZIP to the company's large network of partners, without requiring them to purchase additional software. As a result, our client is able to securely communicate with, and send information to, its partners, regardless of the computing environment or security infrastructure.

The company also needed to enable the secure exchange of confidential documents via email. Seamless integration with Outlook® was a necessity, in order for employees to easily use public key encryption through their email client. Once again, SecureZIP proved to be the best solution, providing the simple integration and user-friendliness the organization was looking for.

Our client deployed SecureZIP on their z/OS mainframes, UNIX Server, and on 1,700 desktops throughout the organization. They now have a consistent, corporate-wide, secure means of transferring sensitive information, both internally and externally with over 700,000 business partners daily.

[Read more customer success stories](#) on PKWARE's Website.

[Back to main page >>](#)

Product Update: PKWARE® Releases SecureZIP® for Windows® Desktop, version 12.2

Earlier this month, PKWARE released SecureZIP for Windows Desktop, version 12.2, which extends SecureZIP email integration to Microsoft® Outlook Express® and Windows Mail®. It also includes several customer-driven enhancements that further simplify the solution's usability.

With version 12.2, SecureZIP seamlessly integrates into Outlook Express and Windows Mail, making them secure email applications. Now, users of Microsoft Outlook, Outlook Express and Windows Mail can automatically secure emails and attachments or, with one click, can opt to do so on an individual basis. SecureZIP for Windows Desktop makes sending secure emails simple: write your email message, attach your files and, with the click of a button, you can quickly and efficiently send secure messages. In addition, SecureZIP's advanced compression eliminates the problems associated with sending large email attachments that exceed mail system size limits.

This new feature extends SecureZIP's integration with other Microsoft products, specifically Office®. With SecureZIP, users can easily save secure files directly to storage media from Word®, Excel®, or PowerPoint®. By simply selecting "Save as SecureZIP File," files are compressed and encrypted automatically.

Several customer-driven enhancements are also included in SecureZIP for Windows Desktop, version 12.2, such as:

- Extending the Policy Manager to support the deployment of enterprise defaults through policy files. Customers can now set both locked and unlocked options through policy, using an improved interface for setting, locking, and unlocking options. Customer defaults can quickly be restored using the "restore defaults" option.
- Support for the .Z format, allowing for the extraction of files compressed by other applications using the .Z (also known as "UNIX compress") format.
- Improvements that allow customers to streamline their workflow by suppressing notification prompts that are not required, according to their established workflow processes.

Also, with version 12.2, a certificate backup wizard is now available to assist users in backing up certificates issued through SecureZIP or any other Certificate Authority.

Version 12.2 of SecureZIP for Windows Desktop is currently available in the English language only. The Standard Edition is available for purchase starting at \$39.95 (quantity one) and the Enterprise Edition at \$59.95. A free 30-day trial version for commercial use is offered for download at www.pkware.com.

Originally released in 2005, SecureZIP is deployed in over 25,000 companies, including 60 percent of the Fortune 100. Learn more about SecureZIP for Windows Desktop, version 12.2, by [downloading the datasheet](#) or, for current SecureZIP for Windows Desktop customers, reviewing the [Technical Notes](#) that overview the new Enterprise Policy Manager capabilities.

[Back to main page >>](#)

White Paper: Overcoming the Obstacles: Creating cooperative partnerships in securing the exchange of data

Security-minded companies face a common challenge: how to control and ensure the security of data it must exchange with partners outside of the organization. After all, a company cannot force its affiliates to adopt its security policies, even though the protection of its data is paramount.

This white paper addresses the challenge and, more importantly, proposes a cost-effective and easily scalable data-centric security solution that allows an organization to secure its data, no matter what partner it is exchanged with.

[Download the white paper](#)

[Back to main page >>](#)

Success Story: SecureZIP® Delivers Ubiquitous Encryption Solution to Protect Sensitive Employee Data

Company Background

Our client is a consumer products company with one of the largest and strongest portfolios of trusted household brands. The company is as strong internationally as it is domestically, with employees located in 81 countries.

Challenges and Requirements

The employee services division of the company manages all of the internal HR, payroll, training, and travel expense systems globally for all employees. Historically, the company outsourced some or all of its HR functions.

As increasingly more employee data was being sent to third-party providers, it became clear that a standardized encryption solution was needed across the organization, in order to protect sensitive information and ensure the company remained in compliance with various government regulations.

However, many of the encryption solutions being used internally were not versatile enough to work across different computing platforms. These systems were also often incompatible with the wide variety of systems run by third-party vendors. The company needed a solution that was not proprietary to a single provider.

Competitive Landscape

The company's information services division looked at several encryption solutions, including WinZip® and PGP®. They also researched best practices with Gartner analysts before deciding on SecureZIP.

The Solution – SecureZIP

SecureZIP was the only solution that met all three of the company's primary requirements:

1. It provided industry-standard encryption
2. It was a public standards-based solution
3. It was capable of being deployed across all required platforms (Windows®, HP-UX, and IBM® zSeries®)

SecureZIP also supported the organization's future aspirations of implementing PKI, because it supports certificate-based encryption and digital signing.

SecureZIP has enabled the HR department to exchange encrypted email attachments with other departments, remote offices, and third-party providers quickly and easily. By adding SecureZIP to the server environment, PDF reports queried from the SAP database are now encrypted.

An added benefit for the company is that SecureZIP also compresses attachments by up to 95 percent, conserving bandwidth and storage space.

For special projects, such as mergers and acquisitions, when large volumes of employee data is exchanged, the company now sends encrypted files, rather than copying personal employee information onto a CD for hand-delivery. The new process is both more efficient and more secure.

[Read more customer success stories](#) on PKWARE's Website.

[Back to main page >>](#)

Company News: PKWARE® UK/EMEA Office Moves to London

To better serve our customers and business partners, PKWARE's UK/EMEA office has moved to London. The new address is:

PKWARE UK Ltd.
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom

Telephone: +44 (0) 207 470 2420
Fax: +44 (0) 207 470 2421
Email: uk_office@pkware.com

[Back to main page >>](#)

Product News: Current Level Sets for IBM® i and z/OS® PKWARE® Products

PKWARE works constantly to improve the quality and performance of our applications on all platforms. For PKWARE products running on IBM large platforms (z/OS and IBM i), new level sets are published monthly, containing the latest updates.

Not sure if you're working with the latest? Check out the below listing of current level sets for supported versions of PKWARE's IBM i and z/OS mainframe products.

z/OS

Product/Level Set	Date
SecureZIP® v10.0 non-SMP/E Levelset (Refresh 7)	08.07.2008
SecureZIP v10.0 SMP/E Levelset (Refresh 7)	08.07.2008
SecureZIP v9.0 non-SMP/E Levelset (Refresh 15)	08.07.2008
SecureZIP v9.0 SMP/E Levelset (Refresh 15)	08.07.2008
SecureZIP v8.2 non-SMP/E Levelset (Refresh 17)	10.18.2007
SecureZIP v8.2 SMP/E Levelset (Refresh 17)	10.18.2007
SecureZIP v8.1 non-SMP/E Levelset (Refresh 15)	10.18.2007
SecureZIP v8.1 SMP/E Levelset (Refresh 15)	10.18.2007
PKZIP® v9.0 non-SMP/E Levelset (Refresh 15)	08.07.2008
PKZIP v9.0 SMP/E Levelset (Refresh 15)	08.07.2008
PKZIP v8.2 non-SMP/E Levelset (Refresh 15)	10.18.2007
PKZIP v8.2 SMP/E Levelset (Refresh 15)	10.18.2007
PKZIP v5.6 non-SMP/E Levelset (Refresh 36)	10.18.2007
PKZIP v5.6 SMP/E Levelset (Refresh 36)	10.18.2007

i operating system

Product/Level Set	Date
SecureZIP v10.0.0C	03.25.2008
SecureZIP v9.0.1H	03.25.2008
SecureZIP v8.2.1C	01.10.2007
PKZIP v9.0.1H	03.25.2008
PKZIP v8.2.1C	01.10.2007
PKZIP v5.6.1H	03.15.2007

[Back to main page >>](#)

Technical Note: Masking Passphrases in JCL When Working with SecureZIP® for z/OS®

SecureZIP for z/OS customers need a means to prevent encryption passphrases from appearing in the clear, when running SecureZIP encryption and decryption jobs. On the mainframe, exposing the passphrase in cleartext in the JCL that's used for encryption or decryption is not a best practice and, in some cases, violates an organization's security policy.

Fortunately, there is an easy process to apply passphrases when encrypting or decrypting, yet avoid exposing such passphrases in the clear. Moreover, the recommended method follows standard IBM mainframe operational and data security best practices.

NOTE: Suppressing display of the passphrase used to encrypt or decrypt SecureZIP-protected data is optional, but a frequently desired best practice. SecureZIP can automatically suppress the display of the passphrase value in *output*. For *input*, customers must ensure the best practice described in this Technical Note is applied consistently.

Solution

The passphrase(s) used for encryption or decryption jobs are managed outside the JCL used to execute such jobs. The passphrases are, instead, placed in a partition data set (PDS) from which they are accessed at run-time.

The below JCL illustrates a simplified example of this approach. The job is configured to encrypt a sequential file, using a passphrase obtained from an external PDS:

```
//HIDEPASS JOB 'PKWARE',CLASS=A,REGION=8M,
// MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=&SYSUID
// *
//*****
//* SAMPLE JOB STREAM TO ZIP SEQ FILE "SECZIP.TEST.SEQ" TO AN *
//* ARCHIVE OF "SECZIP.HIDE.PASSWORD.ZIP" USING STRONG ENCRYPTION *
//* AND USING THE INCLUDE_CMD PARAMETER TO PULL THE SECURED PASSWORD *
//* INTO THE JOB STREAM *
//*****
// *
//ENCRYPT EXEC PGM=SECZIP,REGION=8M
//STEPLIB DD DISP=SHR,DSN=SECZIP.SZV10.LOAD
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
-ARCHIVE_DSN(SECZIP.HIDE.PASSWORD.ZIP)
-ACTION(ADD)
SECZIP.TEST.SEQ
-ECHO(N)
-INCLUDE_CMD(SECZIP.SECURED.LIBRARY(PASSWORD))
/*
```

The PDS MEMBER (SECZIP.SECURED.LIBRARY(PASSWORD)) contains the appropriate encryption method, password parameter, and desired passphrase (see sample below):

```
BROWSE RCE.SECURED.LIBRARY(PASSWORD) - 01.00 Line 00000000 Col 001 080
Command ==> Scroll ==> CSR
***** Top of Data *****
-ENCRYPTION_METHOD(AES128)
-PASSWORD(LOCKDOWN)
***** Bottom of Data *****
```

The run-time UserID must have READ access to the PDS member that contains the passphrase. By using the ECHO (N) parameter, an operator viewing the job output will *not* see which PDS member was specified to import the passphrase for the encryption process.

Resulting Output

Within the output below, the ENCRYPTION_METHOD and PASSWORD parameters were incorporated into the job stream and used to provide the desired encryption. Please note the passphrase used to secure the data has been masked in the output for security purposes.

```
-ARCHIVE_DSN(SECZIP.HIDE.PASSWORD.ZIP)
-ACTION(ADD)
SECZIP.TEST.SEQ
-ECHO(N)
ZPAM030I OUTPUT Archive opened: SECZIP.HIDE.PASSWORD.ZIP
ZPAM253I ADDED File SECZIP.TEST.SEQ
ZPAM254I as SECZIP/TEST/SEQ
ZPAM255I (DEFLATED 76%/75%) SecureZIP(R) AES128 ; DATA SIZE 800; ZIP SIZE 198
ZPAM140I FILES: ADDED EXCLUDED BYPASSED IN ERROR COPIED
ZPAM140I 1 0 0 0 0
ZPMT002I PKZIP processing complete. RC=00000000 0(Dec)
```

Another option to secure the PDS member containing the passphrase and encryption method would be to set access permissions for that PDS member to NONE, but provide READ access to the job under a different user account than that of the operator. This allows an operator, who does not have READ access to the secured PDS member, to submit the encryption (or decryption) job. The job will use the authorized user account credentials that do have READ access and effectively pull the PDS member into the job stream for encryption.

[Back to main page >>](#)