Reduce processing times, increase operational efficiencies, & leverage existing investments

Files that contain sensitive data, whether stored or being transmitted, need to be protected. SecureZIP® makes securing these files an effortless task. SecureZIP is the industry leading security and compression utility that greatly reduces transmission times and required storage space while securely protecting data, in transit and at rest. The combination of application, system, and ICSF integration make SecureZIP® for z/OS® an optimal solution for reducing processing times, increasing operational efficiencies, and leveraging existing investments within the mainframe environment.

CONSERVE STORAGE SPACE AND REDUCE FILE TRANSFER TIME

SecureZIP for z/OS includes advanced compression capabilities, which reduces file size by as much as 98%. Moreover, the solution improves network bandwidth and enables IT to store more files on the same storage devices. The resulting reduced costs ensures organizations get the most out of their existing investments without costly hardware acquisitions or upgrades.

ENCRYPT DATA USING PASSPHRASES, DIGITAL CERTIFICATES, OR BOTH

SecureZIP provides passphrase- and/or X.509 digital certificate-based encryption, allowing for flexibility and optimal support for an organization's data security infrastructure. SecureZIP also works with the leading commercial mainframe security servers, including CA ACF2, CA Top Secret, and RACF

ACCELERATE OPERATIONS WITH ENHANCED TAPE PROCESSING

SecureZIP can significantly reduce the time needed to write ZIP archives to, and extract files from, zip archives on tape media with Enhanced Tape Processing. Moreover, it integrates with IBM's Large Block Interface (LBI) so maximum use is made of today's robust tape drives. SecureZIP for z/OS also includes handlers for multiple file types to further accelerate critical business processes in the data center.

ACCESS ENCRYPTED FILES FOR AUDIT OR RECOVERY PURPOSES

Files that have been encrypted must remain accessible to the organization. When files have been encrypted with either digital certificates or passphrases, SecureZIP's Contingency Key capabilities ensure that encrypted data is accessible.

Contingency Key processing ensures SecureZIP customers can meet the need of auditors, compliance officers, or regulators to inspect or recover encrypted data, even if a password is forgotten or a decryption key lost - while still otherwise strongly protecting the data.

INCREASE DATA PROTECTION POLICY & ENFORCEMENT USING SAF MODULE ADD-ON

Improved encryption/decryption key protection and increased data protection policy & enforcement are available with the SAF Module add-on for SecureZIP Enterprise Edition and SecureZIP PartnerLink.

Enhanced Key Stores

- Protection of private keys used for signing & decryption, located in Security Server Key Rings
- Support for managing and using private keys in IBM's SAF-controlled ICSF CKDS (Cryptographic Key Data Set)
- Improved key management - shared keys across multiple enterprise applications from an industry standard key store

FEATURES AND BENEFITS

- Stream data directly into and out of applications without staging it to disk*
- Reduce number of steps required to create and extract archives
- Leverage previous investments in IBM z/OS hardware cryptography
- Encrypt data using passphrases, digital certificates, or both
- Reduce time needed to write files to, and extract files from, tape media
- Access encrypted files for audit or recovery purposes
- Exchange data between operating systems, including z/OS®, Linux on System z®, i5/OS®, UNIX®/Linux® server, and Windows® server and desktop
- Increase data protection policy & enforcement using SAF Module add-on*

*Feature available in SecureZIP for z/OS Enterprise Edition

> "...SecureZIP is an elegant solution for a z/OS environment because it encrypts, compresses, and manages many kinds of files — all in a single application and across many platforms... PGP® cannot compete with the overall value and ease of PKWARE's application."
>
> **Supply Chain Consultant**
> Leading National Retailer

SAF-Secured Passphrase Management

- Improved operational security with the elimination of exposed cryptographic passphrases
- SecureKey operations for algorithms supported by installed cryptographic coprocessors
- Passphrase management isolated from job execution

Hardened Policy Lockdown

- Establish security controls strictly enforced using SAF
- Separate resource control from product installation and job execution
- SAF enforcement of Contingency Key processing for encrypted data recovery and oversight
- Security audit trail with SMF (System Management Facility) records

LEVERAGE INVESTMENT IN IBM ICSF

SecureZIP leverages IBM System z® Integrated Cryptographic Services Facility (ICSF), enabling organizations to take advantage of significant cost savings as a result of reduced resource requirements.

SecureZIP maximizes the investment made by customers in hardware cryptography by utilizing the least expensive processor capabilities within a system, while maintaining the data security and portability that the standard .zip file format provides. Archives encrypted using IBM hardware can still be decrypted using the SecureZIP application for any other supported platform - interoperability remains intact. SecureZIP leverages the performance advantages of hardware-assisted cryptography on System z, utilizing the best cryptographic facility feature enabled in a specific installation.

PKWARE added support for Protected Key* in SecureZIP for z/OS v12. Protected Key is a blend of clear key and secure key, combining the performance attributes of clear key with the additional private key fortification of secure key. By adding support for IBM's Protected Key, SecureZIP for z/OS v12 uses a faster, CPU-friendly encryption processing method on IBM hardware.

REDUCE NUMBER OF STEPS REQUIRED TO CREATE AND EXTRACT ARCHIVES

Moving data between disparate computing systems often requires multiple steps and could require additional data transformation products and encoders. However, UNIX File System Support allows SecureZIP for z/OS to write directly to, and ready directly from, UNIX, Linux, and Windows file systems; this eliminates extra steps when moving files across systems.

System Integration also allows SecureZIP for z/OS to:

- Facilitate the exchange of data between different types of systems
- Automatically convert data to the appropriate format for the system
- Enhance PKWARE's extensive cross-platform capabilities. PKWARE is the only vendor to provide seamless, secure data exchange across z/OS for the mainframe, IBM i for the IBM Power midrange systems, UNIX/Linux/Windows servers, and Windows desktops.

MAINTAINING FIPS 140-2 COMPLIANCE

The NIST announced FIPS 140 algorithm changes that went into effect at the end of 2010. PKWARE will continue to support FIPS 140 compliance needs with our latest version releases. SecureZIP for z/OS v12 has been updated to meet your business requirements.

About PKWARE, Inc.

The PKWARE Solution is the only complete system for reducing, moving, storing and securing data across the extended enterprise, both internally and externally, from mainframes to servers to desktops and into the cloud. Used by more than 30,000 corporate entities and over 200 government agencies, PKWARE is the industry standard for portability, ensuring data security and cross-platform computing. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York and the United Kingdom.

For additional information and resources, please visit our website: www.pkware.com

To speak with a PKWARE Specialist in the U.S., call toll free: 1.866.583.1795

To speak with a PKWARE Specialist outside the U.S., visit www.pkware.com/contact for specific country offices and contact information

SYSTEM REQUIREMENTS

■ SECUREZIP FOR z/OS

- SecureZIP for z/OS runs on IBM supported levels of the z/OS operating system and hardware

  Please contact PKWARE support for the requirements for utilizing Protected Key