

Protect data exchange and archiving processes

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 additional benefit of cross-platform compatibility makes it the ideal solution for exchanging data within the enterprise.

Access encrypted files for audit and recovery purposes with contingency key

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 for audit or data recovery purposes.

Exchange data securely across desktop, server, midrange, and mainframe systems

SecureZIP is available on all major platforms and supports secure data exchange between Windows[®] desktops, UNIX[®]/Linux[®] and Windows servers, i5/OS midrange, and z/OS mainframe operating systems. SecureZIP automatically converts data to the appropriate format based on the type of system it is being transferred to.

PKWARE is the only single-source vendor for data compression and security products across all major enterprise operating systems.

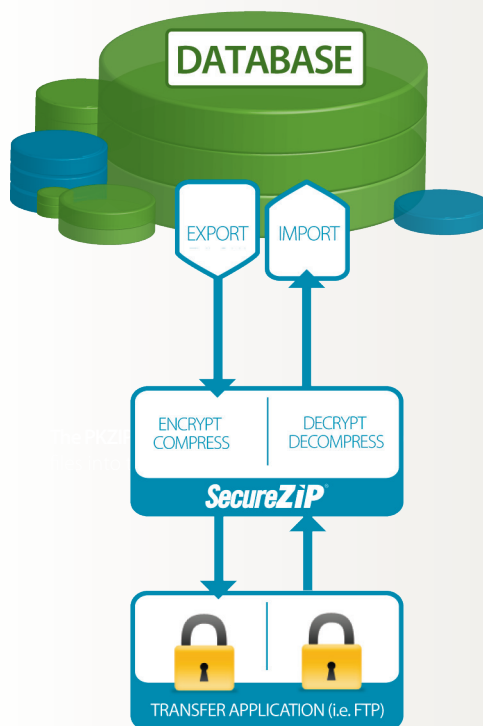
Automatically distribute files from server to desktop

By creating self-extracting files (PKSFX[®]), encrypted and compressed archives sent from servers are automatically decrypted and decompressed onto desktops. This process

is simple for desktop users, requiring just a few clicks, allowing for quick and easy transfer of files to desktop systems. Note: PKSFX is licensed for internal use only.

Process encrypted data without staging decrypted data to disk

SecureZIP with Application Integration decrypts data and streams it directly to the application without staging it to disk. After the application completes processing, it can then stream the data to SecureZIP for encryption – once again, unprotected data is never staged to disk.



Features and Benefits

Conserve storage space and reduce file transfer time

Process encrypted data without staging decrypted data to disk

Access encrypted files for audit and recovery purposes with contingency key*

Encrypt data using passphrases, X.509 digital certificates, or both

Apply added data protection by using smart cards and smart tokens (available on Windows server only)

Automatically distribute files from server to desktop

Verify documents have not been altered by using digital signatures

Operates on all major computing platforms, allowing seamless data transfer between operating systems, including z/OS[®], i5/OS[®], UNIX[®]/Linux[®] server, and Windows[®] server and desktop

*Feature included with SecureZIP for Server Enterprise Edition

"...SecureZIP was far and away the product that fit their need. It was going to deliver the security they needed, true enough, but as a solution, its advantages extended beyond security. SecureZIP's other features would vastly improve the client's processing efficiency at a lower cost."

Supply Chain Consultant
Leading National Retailer

Encrypt data using passphrases, X.509 digital certificates, or both

SecureZIP supports both passphrase- and digital certificate-based methods of encryption, offering flexible security that meets varying requirements within business environments. In comparison to passphrases, digital certificates offer higher levels of security, are easier to use, and allow secure communication with larger numbers of recipients. Passphrases provide an alternative when the intended recipient does not have a digital certificate.

Verify documents have not been altered by using digital signatures

SecureZIP enables users to sign files with their unique digital certificates. Recipients of signed files can validate the signature to ensure the sender is who they claim to be and verify that the document has not been altered or tampered with since signing. In addition, digital signatures offer non-repudiation - the signer cannot later claim that the signature is invalid.

Apply added data protection by using smart cards and smart tokens

SecureZIP's support for smart cards and smart tokens (available for Windows server) enables security professionals to apply an added layer of data protection by storing the user's private decryption key on a small portable device. Smart cards and smart tokens also enable two-factor authentication, requiring the user to present two credentials before they can access protected data, such as a password and a private key stored on a portable device.

About PKWARE

PKWARE, Inc., the creator and continuing innovator of the ZIP standard, is a global market and technology leader providing data-centric, cross-platform data security and compression software. The SecureZIP & PKZIP product families are used by over 30,000 corporate entities and over 200 government agencies to ensure data security, portability, and cross-platform computing exchange

- both internally and externally with partners. Organizations in financial services, banking, retail, healthcare, government, and manufacturing use PKWARE products daily for their unmatched scalability, ease of use, and rapid deployment. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York and the United Kingdom.

System Requirements

Windows®	Solaris®	IBM-AIX®	HP-UX®	Linux®
SecureZIP for Server				
<ul style="list-style-type: none">Windows 2000 SP4 and higher with IE 6.0 or above128 MB RAM (256 MB Recommended)13 MB available disk space	<ul style="list-style-type: none">Solaris 8 or greater64 MB RAM (128 MB recommended)15 MB available disk space	<ul style="list-style-type: none">IBM-AIX 5.2 or greater64 MB of RAM (128 MB recommended)15 MB available disk space	<ul style="list-style-type: none">HP-UX 11i v1 or greater64 MB of RAM (128 MB recommended)15 MB available disk space	<ul style="list-style-type: none">RedHat 4 and greater, SuSE 9 and greater64 MB of RAM (128 MB recommended)15 MB available disk space

United States
648 N. Plankinton Ave.
Suite 220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

UK/EMEA
Crown House
72 Hammersmith Road
London W14 8TH
United Kingdom
+44 (0) 207 470 2420

PKWARE®
DATA SECURITY & COMPRESSION