

# **SecureZIP**<sup>™</sup>

## Trusted ZIP Solutions



### **SecureZIP Solutions**

Delivering Powerful and Easy-to-Use  
Security for Files

#### **Contributing Authors:**

Charles Kolodgy, Research Director,  
Security Products, IDC  
Jeffrey Schwartz

## Introduction

The explosion in the amount of information exchanged online has resulted in the need to efficiently secure sensitive data shared between individuals, corporations, and government agencies. Many organizations have attempted to address the need for data security by deploying specialized password protection, encryption, or digital signature products. Yet, while these attempts do provide some level of security within a controlled environment, they do not make secure data exchange simple or ubiquitous. Without easy-to-use solutions, end-users will default to not securing critical documents and ignoring the associated risks. In order to realize the true promise of electronic document interchange, organizations must have common mechanisms to not only efficiently store and exchange files, but also to secure them. The combination of advanced file compression software with advanced digital signature and encryption techniques—such as in SecureZIP™—provides an intuitive approach to solving this problem by delivering an easy-to-use, cost-effective, and easy-to-implement solution.

The combination of proven data compression technology with sophisticated data security capabilities provides a practical solution to a looming problem. ZIP compression technology is the de-facto standard for efficiently storing and sending files over networks. By extending the ZIP format to enable multiple levels of file security, the same technology that simplifies and improves the efficiency of the storage and transmission of files can also be used to secure them. This white paper explains why ZIP is the best-suited solution for providing an easy-to-use interface for adding security to files before they are stored or transmitted.

Individuals and platform administrators now use PKZIP and other forms of ZIP solutions in their simplest forms to password protect multiple files. For more fail-safe modes of communication, users can employ the newest release of PKWARE's SecureZIP to wrap contents in electronic containers or envelopes, which can be digitally signed and encrypted using strong encryption of up to 256-bits. Recipients can then apply their passwords or certificates to open these files. PKWARE, the creator of the ZIP file format, is leading the way by including advanced security in the latest version of the ZIP standard as well as offering these forms of security in the SecureZIP product line. SecureZIP-enabled solutions are available across all major computing platforms, including Windows, UNIX, Linux, iSeries, and zSeries.

## The Evolution of ZIP

Originally created to pack multiple files onto floppy disks when they were the media of choice for transporting data, ZIP is now widely used to compress files stored on servers and attachments sent via email or other transport methods. Sending multi-megabyte files without compression can be extremely slow, and most carriers, ISPs and corporate network operators routinely prohibit the transmission of large attachments. PKZIP, for example, compresses files by up to 95 percent, dramatically reducing storage and network costs.

ZIP has become the de-facto means of compressing data and putting multiple files into a single container for efficient storage and transmission. Moving forward, compressing files will be just

one reason to implement ZIP solutions—securing data at the file level will be equally important. Millions of users with ZIP file compression solutions will be able to use the same functionality and user interface to make these files secure.

## The Current Challenge

Companies mired in labor-intensive processes that require communicating sensitive data on paper are looking to use digital technology to increase efficiency, but must find practical, affordable solutions for protecting their data. At the same time, with federal initiatives such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), many organizations are required by law to implement some means of secure data transmission and storage. Regardless of what motivates organizations to secure files, when they do, processes that once took days or weeks to complete can be done in a fraction of the time.

These security challenges apply to two types of data—persistent data, which includes files stored on servers and desktops, and transient data, which refers to files sent to customers, suppliers, or partners via email or other electronic methods. Organizations of all types need to secure electronic files in order to prevent internal abuse or external intrusion. As companies look to share more information online, the risk of files getting into the wrong hands increases exponentially. This may lead to a stifling of new initiatives to improve efficiency for fear of compromising data integrity during transport. However, heightened competition, increasing customer demand for ever-faster responsiveness, as well as new business imperatives and mandates are making it harder and costlier for organizations to wait.

## Closing Security Gaps

Few organizations are currently placing barriers against unauthorized access at the file level. These companies have gone to great expense to secure the flow of data into and out of the organization, but have done very little to secure stored digital files or files taken outside of the corporate firewalls by remote users. Most security breaches happen from within an enterprise. For example, at one hospital, curious employees wanted to see the medical records of a celebrity, even though they were not authorized to do so. While the files were secure from outside access, the lack of file-level security made it easy for insiders not only to access the information, but also send it to others outside the hospital. Accidental breaches can also occur. Healthcare provider Kaiser Permanente inadvertently sent patient records to the wrong email addresses. Viruses can also forward messages to the wrong recipients. Regardless of the cause of a breach, once one occurs, the results can be disastrous and costly. Such security breaches can destroy customer trust, create costly liability issues, and can even lead to criminal penalties.

Applying data security measures, such as encryption and authentication, at the file level greatly diminishes these risks. There are various ways to secure files, for example requiring a password to encrypting the file with a digital certificate, so that only an authorized user can open it.

SecureZIP achieves data security in two ways. First, files are encrypted using digital certificates or passwords. Second, authentication, in the form of a digital signature, is applied by using the originator's private key. The benefits of encryption and authentication are confidentiality, knowing the originator's identity, non-repudiation, and data integrity. By using SecureZIP to apply security at the file level, those creating documents can ensure that sensitive data won't get into the wrong hands.

## Authentication

Whether accessing a network or individual files, there are many ways to authenticate the identity of a user. Authentication is the process by which a user validates his or her identity, ownership or authorization before accessing a file or network or before encrypting or decrypting a file. The simplest form of authentication is a password. For stronger forms of authentication, a smart card or other token device may be used. Other forms of authentication, including biometrics (such as a fingerprint scanner) exist, but are not widely used today. Not only does authentication provide secure access to a file, but also the process can be critical in providing a recipient with validation that the sender of a file is who he or she claims to be.

Today, there is no universal method of invoking different forms of authentication at the file level. Over time, that promises to change as standards groups including the Internet Engineering Task Force (IETF) and the Trusted Computing Platform Alliance (TCPA) develop common protocols for stronger authentication. PKWARE understands that authentication is a natural extension of the file archival process. To this end, PKWARE has extended the ZIP format to support archive and file-level authentication using digital signatures, adding significant value to their product line while solving a key problem that has stifled the widespread adoption of electronic document exchange.

## Encryption

Sensitive information is typically encrypted, or encoded, so that the contents appear meaningless if accessed by an unauthorized user. The stronger the encryption, the harder it is for a hacker or unauthorized user to decrypt the file. There are various forms of file encryption, but symmetric keys of 128-bit or greater are typically used. The higher the number of bits, the longer the key and harder it is to hack.

Only a user who can authenticate his identity can decrypt a document. Unfortunately, until recently, there has been no common and simple means for encrypting a file. But, as a result of advances made by PKWARE, file compression software is now a viable tool for delivering sophisticated yet easy-to-apply encryption capabilities.

## Public/Private Key Encryption

Using public/private key encryption software effectively scrambles the bits of data so that they are meaningless until decoded. The recipient's public key is used to encrypt the file and is made available in the form of a digital certificate, which is issued by a certificate authority. Using this technology, only one private key, owned by the recipient, can decrypt the encrypted

files. Organizations that use this form of technology, known as Public Key Cryptography, provide users with digital certificates based on the X.509 standard. There are many providers of these certificates, including Entrust, RSA Security, and VeriSign.

Whether a user is archiving one or multiple documents, the user determines whether it should be password protected or digitally signed and/or encrypted using

a digital certificate. The user can apply any or all of these functions, regardless of the application used to create the file, using the familiar ZIP interface. Multiple users may also choose to digitally sign every file in a ZIP file archive by including a group workflow or file sign-off process. In essence, SecureZIP turns a traditional ZIP file into a secured ZIP file for the purpose of storage or transmission. Because SecureZIP provides certificate-based and traditional password-based encryption and authentication, as well as strong encryption algorithms (up to 256-bit symmetric key encryption), users can achieve multiple levels of security and choose the desired strength. The following options are available for encrypting a ZIP archive.

---

---

## Secure Data Features

*SecureZIP security functions include strong encryption tools using RSA BSAFE. SecureZIP provides the option for password or certificate-based access for encryption using DES, RC2, RC4, 3DES and AES. SecureZIP includes support for standard X.509 digital certificates with PKI to sign and encrypt compressed files. When sending to recipients that do not have digital certificates, the user can still encrypt the files using passwords.*

---

---

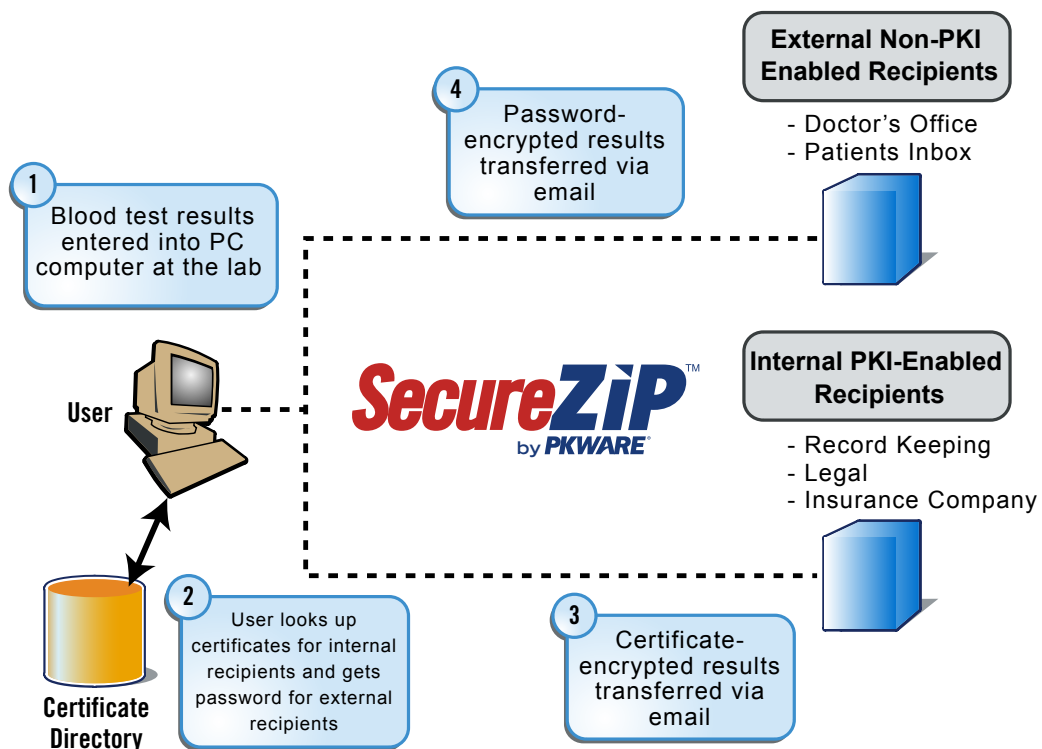
- **Strong password encryption:** At the simplest level, applying passwords may be the equivalent of putting an inexpensive lock on a door. While a determined hacker may be able to pick the lock, it will keep the average intruder from walking through an open door. Anyone can quickly apply a password to a ZIP archive and provide that password to the recipients via a separate message or some other form of communications. In many cases, that would widely satisfy the need for confidentiality in most corporate and government environments and would be a vast improvement over no security at all.
- **Certificate-based strong encryption:** This method requires an organization to set up a system that distributes digital certificates. Presuming an organization and the parties it exchanges files with have established a public key infrastructure (PKI) for encrypting files and opening them with digital certificates (typically those based on the X.509 standard), SecureZIP can be used to apply those certificates.
- **Digital signatures:** Just because a document has an X.509 certificate, how does a recipient know the sender is who he or she claims to be? Or how can the sender ensure that the recipient is legitimate? A digital signature effectively validates, through SecureZIP, the identity of the holder of the certificate and the Certificate Authority that issued the certificate.

## The PKWARE Architecture

When compressing one or more files into an archive, which may consist of any number of large documents, images, and spreadsheets, SecureZIP compacts them into an electronic container or envelope before storing them. The compression process also allows a user to apply a digital signature or encryption to that container at the file level.

By using the SecureZIP Explorer feature, the user selects the files to be compressed (or this can be selected using SecureZIP's integration with popular email clients such as Microsoft® Outlook® and Lotus Notes®). The user then specifies what level of authentication to implement—password, digital certificate and/or electronic signature. Then, depending on how the user has specified to apply SecureZIP security features, he enters a password or chooses specific digital certificates for the intended recipients. By using one or more public key certificates or passwords, a user can encrypt any number of files within the ZIP archive and limit access to only those recipients with the corresponding private key or password. A recipient can then open the encrypted ZIP envelope by applying the appropriate password or private key.

## How SecureZIP Bridges PKI and Non-PKI Environments to Protect Patient Health Information



## **Cross-Platform Support**

SecureZIP is suitable for all file types. Documents of any type, including graphics, may be compressed, authenticated and encrypted. A collection of files put in a ZIP container can be archived on Windows, UNIX, Linux, iSeries, zSeries, or other computing platforms. The documents within a container can consist of multiple file types such as Office files, PDF documents, HTML and image files. PKWARE also offers SDKs that enable vendors to embed SecureZIP technology directly into their applications and security products.

## **Meeting Current Challenges—Industry-Specific Mandates Financial Services Modernization Act**

The recently enacted Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, now permits the cross-ownership of banks, brokerage firms and insurance companies, which was previously banned. Prompted by the merger of Citicorp and Travelers Insurance, which also owned brokerage house Salomon Smith Barney, to form what is now known as Citigroup, the GLB Act was enacted in 1999 to enable financial services firms to provide a wide range of services to their customers.

To protect sensitive customer information, the GLB Act requires institutions to ensure the privacy and security of customer data. Compliance with these requirements is essential and organizations must have their infrastructures audited to ensure they are meeting federal guidelines.

## **The Electronic Signature Act**

A digital signature is now just as valid as a handwritten one. The Electronic Signature Act went into effect in 2000, and states that a digital signature is legally binding. However, there has been no simple software tool that a business can give to an employee, or a customer for that matter, that allows individuals to easily apply a digital signature to a file.

By accepting digital signatures, companies can eliminate paper documents from processes that once required handwritten signatures—such as filing an application for a loan or opening a new brokerage account online. This streamlines an organization's ability to process transactions through further automation, and promises to improve customer satisfaction.

## **The Health Insurance Portability and Accountability Act**

HIPAA allows for the secure exchange of patient records between insurance companies and agencies, including clearing houses and the Medicare and Medicaid programs, with the aim of simplifying administration. HIPAA stipulates that industry participants should be able to exchange documentation electronically and that electronic signatures are binding. Those transmitting the data over networks are responsible for encrypting patient data to ensure patient privacy is not compromised.

Meeting critical HIPAA electronic security requirements using SecureZIP extends the trusted de-facto standard ZIP archive in an evolutionary way to provide persistent secure archives for

sensitive medical records for online transmission or transport. The United States Department of Health and Human Services has established rolling deadlines for supporting HIPAA, with some taking effect within months while others are yet to be determined. HHS recommends, however, that affected healthcare providers implement standards prior to any established deadlines. Meeting HIPAA security and electronic signature requirements now helps protect against fraud and abuse of patient information. Once the rules take effect, those entities that don't protect sensitive patient information as mandated by HIPAA could face criminal penalties and fines of \$25,000 per individual per year.

## Examples of How SecureZIP Enables Secure Document Exchange

There are numerous ways in which compressing and securing files can allow an enterprise to simplify the encryption and authenticity of documents, enabling secure exchange. Although these examples are hypothetical, they illustrate likely scenarios.

**Brokerage Firm:** A customer wants to transfer mutual funds from one brokerage house to another. Rather than going to a branch office, the client downloads the form, inputs the data and emails them for processing. In most instances, the customer has to mail in a signed copy. But the E-Sign Law allows a customer to digitally sign that form and supporting documentation and submit it electronically. SecureZIP lets the client compress the documents, encrypt them, and digitally sign them. Both parties are assured confidentiality, authenticity, and a legally binding transaction.

**Health Care:** A hospital wants to send patient records to an insurance carrier or another health care provider for processing. With SecureZIP, a user compress the files, which may include large files such as digital X-Rays and patient histories, encrypts them, and then sends—all in the same secure envelope. Patient privacy is assured and information can be transmitted in minutes or less.

**Insurance Company:** An individual changes jobs and now needs to change healthcare providers. There may be certain records the new carrier is entitled to see, but not others. Applying file level security using digital certificates and private keys ensures the data isn't misused.

**Government and Military:** Naturally, a great deal of classified information changes hands. An official can use SecureZIP to compress and encrypt files so that only those recipients who are authorized to see those documents can access them. Using the SecureZIP client, they can invoke the password or certificate needed to encrypt or decrypt the file.

## Summary

The need to secure sensitive data during transport and storage is increasingly evident. Combining proven data compression technology with sophisticated data security capabilities provides a logical mechanism for securely and efficiently storing and transferring sensitive information. Millions of users around the world already rely on and trust the ZIP format to store and exchange data. By offering support for digital signatures and multiple levels of encryption, PKWARE is now advancing the usability and accessibility of file security, enabling ZIP users to achieve more secure and efficient modes of data communication than were previously possible.

SecureZIP enables support for digital signatures and encryption and meets government established requirements for electronic authentication and encryption by applying strong encryption (DES, RC2, RC4, 3DES and AES) and digital signatures.

By implementing SecureZIP, users can apply any level of security they choose, from the simplest to the most complex, while overcoming this key barrier to electronic document exchange. As a result, organizations can quickly meet existing and emerging federal and industry regulations that require fail-safe data security. At the same time, organizations can measurably reduce the cost of processing documents and significantly improve customer service by streamlining the processing and fulfillment of orders or claims.

SecureZIP secure file compression provides an inert data container that enables security for single, multiple and large format files of almost unlimited size. SecureZIP provides data compression and multiple levels of security during transport and in storage—regardless of file type, operating system, or security infrastructure.

**PKWARE®**  
[www.pkware.com](http://www.pkware.com)

### United States

9025 North Deerwood Drive  
Brown Deer, WI 53223-2480  
1-888-4-PKWARE

### International

Hatch Farm, Mill Lane  
Sindlesham, Wokingham, RG41 5DF  
Phone: +44 (0) 118-979-9909  
Fax: +44 (0) 118-979-2998  
[internationalmarketing@pkware.com](mailto:internationalmarketing@pkware.com)