PKWARE®

End-to-End Enterprise Encryption:

A Look at SecureZIP® Technology

TECHNICAL WHITE PAPER

Table of Contents

End-to-End Enterprise Encryption:
A Look at SecureZIP Technology

Every day sensitive data is exchanged within your organization, both internally and with external partners. Personal health & insurance data of your employees is shared between your HR department and outside insurance carriers. Customer PII (Personally Identifiable Information) is transferred from your corporate headquarters to various offices around the world. Payment transaction data flows between your store locations and your payments processor. All of these instances involve sensitive data and regulated information that must be exchanged between systems, locations, and partners; a breach of any of them could lead to irreparable damage to your reputation and revenue.

Organizations today must adopt a means for mitigating the internal and external risks of data breach and compromise. The required solution must support the exchange of data across operating systems to account for both the diversity of your own infrastructure and the unknown infrastructures of your customers, partners, and vendors. Moreover, that solution must integrate naturally into your existing workflows to keep operational cost and impact to minimum while still protecting data end-to-end. SecureZIP, from PKWARE, is that solution.

SecureZIP: The Next Generation of ZIP

PKWARE®, Inc., is the creator and continuing innovator of the ZIP standard. For over 20 years, PKWARE has continued to build on the ubiquitous .ZIP format. Today, PKWARE addresses the critical need to provide strong data security for its customers by adding encryption and signing using NIST[1]-approved algorithms. The result is SecureZIP—The Next Generation of ZIP.

SecureZIP provides all of the features and capabilities of its predecessor, PKZIP, including efficient data compression, sophisticated file management, and cross-platform capability. SecureZIP allows organizations to address both the continuing need for efficient data file management, while adding strong data security. Building on the foundation of ZIP, SecureZIP adds enterprise-class security in a single interoperable solution, across all the major enterprise operating systems: IBM® z/OS® and IBM i®; open systems servers including AIX®, HP-UX®, Solaris®, and Linux®; plus Windows® server and client.

SecureZIP ensures that information is protected throughout your organization, in motion as it is exchanged, or at rest in electronic or physical storage—it applies protection directly to the data, not to the network transport or application. Whether you choose to encrypt with passphrases, use a certificate for signing and authentication, or both, this data-centric solution provides the flexibility to secure your data using the world-renowned .ZIP format. SecureZIP also provides an efficient, easy-to-use method to implement data security and file management, whether you are using it on a single desktop or in the world's largest data centers. And since it works on every major enterprise computing platform, it minimizes the cost of managing multiple security products and vendors.

Traditional ZIP: The Foundation for SecureZIP

Phil Katz, the "PK" of PKZIP, created the .ZIP format in the late 1980s as a means to archive files; he included compression to make the process more efficient. Katz's .ZIP format became the foundation of all traditional .ZIP applications. He specifically developed the format to be extensible in order to maintain inclusion of new compression algorithms, carry metadata necessary to efficiently and effectively extract data, and generally improve upon other technologies.

Katz specification states that files are compressed individually, ordered into the archive format with local header information including elements such as a file comment, file name, size, date, etc. Each file is also marked with a four byte signature. Complementarily, the metadata for each file is listed in a central directory record holding the file sequence and other metadata, along with a corresponding four byte signature. PKWARE also included encryption support early in the evolution of the product, though the "traditional" PKZIP 96-bit encryption would not be considered sufficient by contemporary standards.

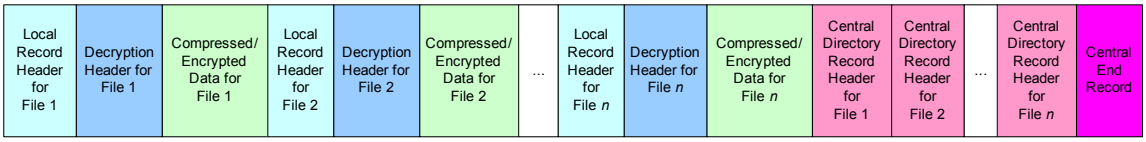


Figure 1: Conceptual View of the ZIP Format

Seeing the value of a standardized format for file exchange, Katz made the ZIP technology available to others, publishing the format via the APPNOTE[2]. Consequently, the use of ZIP is ubiquitous and has become one of the most familiar technologies in use today. PKWARE continues to support and publish

[1] National Institute of Science & Technology

the APPNOTE ZIP format specification, collaborating with other vendors to promote and evolve the standard to meet evolving market needs.

When Katz developed ZIP, he also established PKWARE to develop applications for DOS and UNIX that used the specification. Shortly thereafter, PKWARE enhanced the ZIP format in a number of ways, including expanding its metadata management capabilities for better support of the data definition and space management controls required on those platforms.

In 2001, PKWARE began working with the ZIP community to expand the specification to include strong encryption for data privacy, as well as digital signing and authentication for data integrity validation. PKWARE developed products supporting these new structures under the brand SecureZIP, available for the IBM mainframe operating system z/OS, mid-range operating system i5/OS, UNIX in the AIX, Solaris, and HP-UX varieties, Linux (kernel 2.4 and forward, certified for the RedHat and SuSE distributions), and Microsoft Windows server and desktop.

The updated operating system range is significant, representing all major enterprise computing platforms. Both PKZIP and SecureZIP rigorously capture and store the significant metadata required to restore the data and its internal relationships. This facility is particularly useful for the large platform use cases, as PKWARE products automatically allocate appropriate disk space, provide the relevant data control block (DCB) information (e.g., record format [RECFM], logical record length [LRECL], block size [BLKSIZE]) needed to extract the data to large platform storage. Moreover, PKWARE ensures interoperability between all combinations of the supported operating systems, for all relevant archiving, compression, encryption, and signing/authentication functions. For example, organizations can use SecureZIP on the mainframe for data that will be distributed to and used on Windows clients. It automatically transforms from EBCDIC to ASCII character encoding when going from large to small platform (and vice versa), and places or removes line feed & carriage return characters when the data moves between UNIX and Windows.

Implementation of ZIP Encryption

Recognizing the value that a multi-file archive has for data protection, PKWARE developed SecureZIP, adding strong encryption support to the existing data compression and file management capabilities. SecureZIP complements the rigorous data-in-use physical and logical perimeter defenses that already exist in the enterprise. It also addresses data-at-rest and data-in-transit use cases with highly durable, yet still flexible data protection. SecureZIP applies data-centric encryption, protecting the data itself rather than protecting the transmission of the data (transport security) or access to the data through an application (access control), or the facilities that host the data (resource control). An organization's data loss risks are greatly reduced when SecureZIP is used to augment existing perimeter security and access control systems.

Encryption has emerged as a central way to secure data and protect privacy, but not all encryption is the same. Organizations must make decisions about where and how to apply encryption in order to maximize the benefits for their specific organization. The first choice is between using symmetric key encryption (i.e., passwords) or asymmetric encryption. Symmetric encryption relies solely on a single shared secret or key, typically a password. The symmetric approach tends to provide fast encryption, but sharing a single key is risky and secure key exchange is difficult. Unless such passwords are carefully managed, they can be compromised (e.g., an act as simple as finding the password hidden under a mouse pad). Likewise, unless passwords are very long and complex (therefore difficult to remember and use), they can be subject to compromise from simple brute force

[2]For the technical specification document, please see http://www.pkware.com/documents/casestudies/APPNOTE.TXT; for links to subscribe to the service publishing notifications when changes to the format are released, please see http://www.pkware.com/support/zip-application-note

attacks (automated repetitive attempts of all possible combinations) or dictionary attacks (similar to brute force attacks, using word combinations).

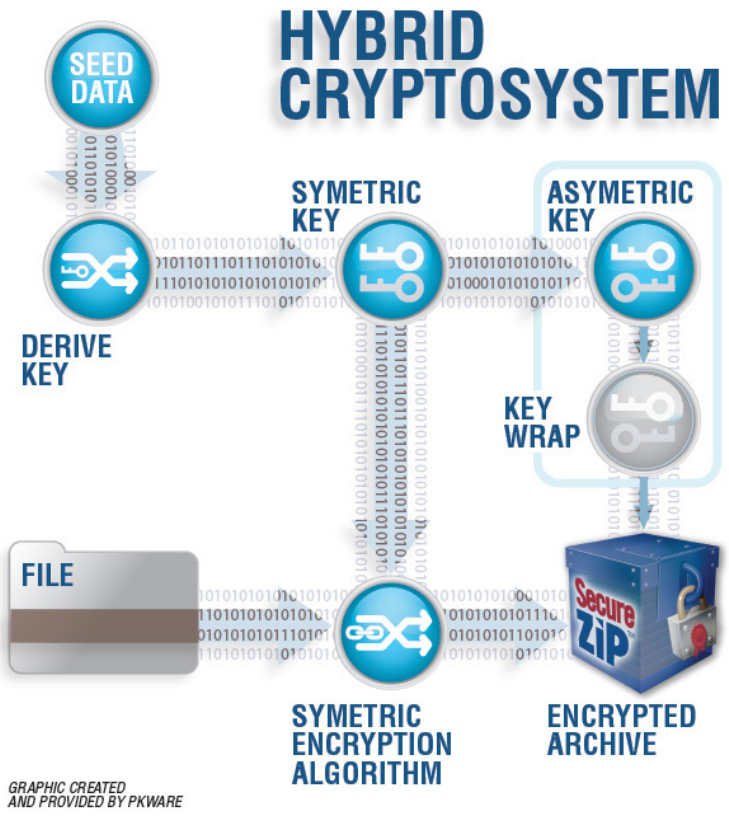
Asymmetric encryption uses a digital certificate with an associated key pair – a public and a private key that have a unique relationship based on factoring the product of two large prime numbers. Data that is encrypted with one can only be decrypted using the other, and the complexity of the mathematical relationship is such that the effort required to reverse-engineer one from the other makes it effectively impossible. The asymmetric approach is considered more secure but is more computationally-intensive, which presents performance issues when processing large amounts of data. Both symmetric and asymmetric encryption approaches have drawbacks.

Hybrid Cryptosystem

The hybrid crypto solution offers a blend of the two different encryption approaches, gaining the best attributes of each without the disadvantages. A hybrid cryptosystem automatically generates a random and complex symmetric session key to encrypt the target data, creating an encrypted payload. Hybrid systems then use the asymmetric public key of the X.509 key pair to encrypt the symmetric key (see Figure 1). It applies the computationally-intensive asymmetric encryption to only the small symmetric key which is used to encrypt the larger source data payload. As a consequence, it consumes fewer resources while providing fast, effective encryption. SecureZIP is implemented as a hybrid cryptosystem.

Cryptographic Calculation Sources

The value of an encryption application like SecureZIP is directly related to the quality of the



cryptographic algorithms it uses. Since SecureZIP is used in a variety of circumstances, it supports a variety of cryptographic algorithm sources to complement those needs. While the application continues to support a number of weak encryption algorithms (i.e., the original PKWARE "traditional" 96-bit encryption, DES, and RC4), most contemporary uses of the product focus on either the strong encryption available with 3DES and, particularly, the AES algorithm at various bit strengths. Regardless of the supported operating system, SecureZIP offers a FIPS[3] 197-compliant Advanced Encryption Standard (AES) algorithm implementation. Consistent implementation of the AES algorithm across the several supported operating systems was initially implemented by integrating the RSA BSAFE cryptographic libraries, Crypto-C and Cert-C.

PKWARE continues to reinvest in the SecureZIP product as market needs for additional levels of data protection to meet internal and external obligations increase. For example, on most supported operating systems, SecureZIP goes further to support FIPS 140-validated encryption sources. FIPS-140 is the best practice describing the security requirements for cryptographic modules, detailing the standard of care with which the implementation of the AES algorithm and the handling of keys must be performed. While the FIPS 140-validated cryptographic libraries used vary by operating system[4], PKWARE invests the resources to ensure that interoperability across the many supported operating systems is maintained. Equally important, the product offers the ability to lock-down or default configuration so that the FIPS 140-mode must be used – a distinct advantage compared to other offerings in this market.

SecureZIP also leverages IBM's Integrated Cryptographic Services Facility (ICSF), on the z/OS operating system, in part so customers can use the FIPS 140-validated hardware available on that platform. When encrypting on a mainframe equipped with a suitable add-on card for cryptography (PCIXCC or CEX2C), SecureZIP can be configured to automatically use that FIPS 140-validated encryption source and only that encryption source. Alternatively, the product can be configured to use IBM's Central Processor Assist for Cryptographic Function (CPACF) for cryptographic calculation, and significantly reduce the amount of resources required to AES encrypt data.

Digital Signing

PKWARE's authentication implementation follows the traditional models for digital signing, wherein the full body of data is first passed through a hash function to derive a fixed length output. The output is then encrypted using the signer's private key and this encrypted hash then becomes the digital signature. The digital signature and a copy of the signer certificate are attached to the data. Authentication is performed by using the signer's public key to decrypt the signed hash and then comparing that hash to an independently derived hash using the same input data and hash function. SecureZIP can attach one or many signatures to each file in a ZIP archive and one signature to the archive as a whole. It supports contemporary hash functions including MD5, SHA-1, and SHA-2 in a variety of bit strengths. While no longer considered sufficiently strong, MD5 remains available within SecureZIP to ensure compatibility with older archives and other ZIP-compatible applications.

In Step with the Market's Data Protection Needs

End-to-end encryption requires stringent attention to implementation and workflow issues. Many regulations, such as Payment Card Industry Data Security Standard (PCI DSS) call for encryption as a means to protect sensitive data. However, as the Heartland Payment Systems data breach in 2009[5] illustrated, encryption needs to be applied to the data wherever it goes, however it get there, to ensure

[3]Federal Information Processing Standards are models of best practice published by NIST. Federal guidelines require agencies to follow many of the FIPS practices, and many non-governmental organizations also subscribe to them as recognized best practices.

[4]Please contact your PKWARE representative to obtain a copy PKWARE's letter of attestation describing the FIPS 140 implementations.

unanticipated exposure is not left unaddressed. Consequently, SecureZIP for z/OS and SecureZIP Server for UNIX/Linux/Windows have been engineered to support genuinely seamless end-to-end encryption. Data can be protected immediately as it is extracted from a data source.

Application Integration (see Figure 2) ensures that data is encrypted before it is staged to disk, record-by-record (mainframe) or as a stream (server), anticipating the emerging best practices anticipated to be part of the Payment Card Industry (PCI) Data Security Standard (DSS) v1.3, expected to be announced in the latter part of 2009 . End-to-end encryption for data privacy is seen as a natural extension for the need to protect data-in-motion and data-at-rest. By ensuring protection is applied the moment the target data shifts from being data-in-use to data-in-motion, an organization significantly reduces their attack surface and their associated risk. Gartner analyst, Avivah Litan, recently said, 'I think the payments industry needs to take some long-needed security steps including end-to-end encryption…so that even if data is stolen, it's useless…'[6]

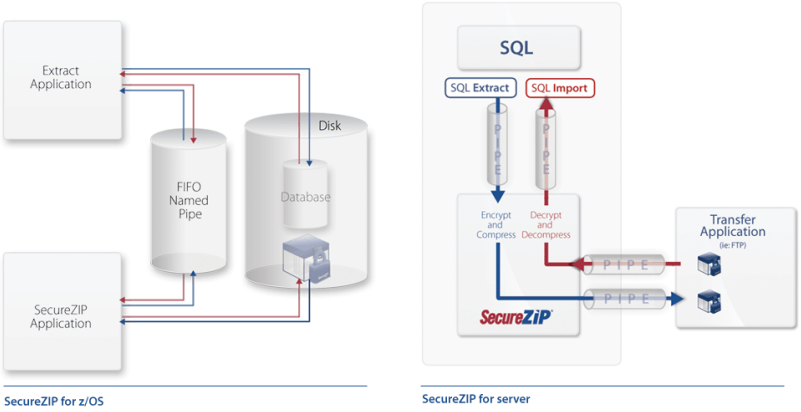


Figure 2: SecureZIP Application Integration

Conclusion

PKWARE continues today to build upon the ZIP technology first introduced over 20 years ago. PKZIP technology was applied first to efficient data management by combining the multi-file, cross-operating system archive format with data compression. Market needs have evolved and PKWARE continues to help its customers meet critical business requirements with SecureZIP, providing the same data compression and file management capabilities coupled with strong data protection and authentication.

[5]Credit-Card security standard issued after much debate' Computerworld IDG news online. 'The Payment Card Industry Security Standards Council…issued revised security rules, while also indicating next year it will focus on new guidelines for end-to-end encryption, payment machines and virtualization.'

[6]Downloaded March 9, 2009, from http://news.idg.no/cw/art.cfm?id=BA7B7F65-17A4-0F78-31E98FBD41716840.

United States
648 N. Plankinton Ave. Suite220
Milwaukee, WI 53203
1.888.4.PKWARE
www.pkware.com

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