



## **When should I use authentication, and when is encryption a better option?**

Encrypting data provides strong security to your data. When using the PKWARE® family of security products, encryption can be used with a public key infrastructure (PKI) deployment to encrypt data for an individual. Encryption offers the strongest security available, but can result in adding time to your existing processes. Encryption should be used whenever data privacy is required.

Digitally signing files is much like applying an electronic pen and ink signature; it ensures that the files have not been altered. A valid signature indicates the file has not been tampered with since it was signed, and that the sender holds a trusted certificate. Digitally signing files can verify the sender without adding additional processing time to your operations. Digital signing should be used when data integrity and sender authentication is needed.

In some cases, digital signing and encryption may be needed, and can work together to guarantee information protection.

## **What is the SecureZIP® Administrative Module?**

Corporate security policies can be easily implemented and controlled with the PKWARE Administrative Module. By enabling you to set policies for who can encrypt data and how it is encrypted, the Administrative Module aids enforcement of data security practices, helps ensure regulatory compliance, and improves email efficiencies — all from one central location. The Administrative Module even allows you to easily manage different policies for different business groups.

## **Where can I get a digital certificate?**

Digital certificates come in two basic forms — individual and organizational. Individual certificates are tied to the identity of an individual user and are used with desktop security products. Organizational or SSL certificates are typically associated with a particular server, and are used for business-to-business data transfer applications or secure storage.

There are three basic options for obtaining digital certificates. Organizations that require multiple certificates can choose to distribute and manage certificates from an internal IT or IS group, or decide to outsource the process to a trusted certificate authority. Single certificates may simply be purchased from one of the providers mentioned below.



## Issuing Certificates In-House

Companies such as RSA® Security, Inc. and Entrust®, Inc. provide software applications that enable organizations to establish their own certificate authorities for issuing, managing, and revoking certificates and generating corresponding public/private key pairs.

More information is available at the following websites:

**RSA Security:** <http://www.rsasecurity.com/>

**Entrust:** <http://www.entrust.com/>

If you currently own Microsoft® Windows Server™ 2003, you already have the ability to generate digital certificates via the Microsoft® Certificate Server. To learn more about using the Microsoft® certificate generation functionality with SecureZIP, please read our guide, "[How to Configure a PKI Using Microsoft® Windows Server™ 2003](#)" or [visit the Microsoft Windows Server 2003 TechCenter website.](#)

## Outsourcing Certificate Issuance

VeriSign® offers an alternative to in-house certificate issuance, providing outsourced certificate management (mPKI) and functioning as a service provider for issuing, managing, and revoking digital certificates on behalf of your organization.

More information is available at: <http://www.verisign.com/>

## Certificates for Individuals

Individuals may purchase single certificates from VeriSign on an à la carte basis. Please see <http://www.verisign.com> for more details.

## Organizational Certificates

Organizational certificates can be purchased individually or in bundles from the following vendors:

**VeriSign:** [www.verisign.com](http://www.verisign.com)

**GeoTrust:** [www.geotrust.com](http://www.geotrust.com)



Note: SecureZIP is compatible with any X.509 v3 digital certificates. PKWARE does not promote the products or services of any specific vendor of certificate authority software or services.

### **Why choose SecureZIP over WinZip®?**

PKWARE created the original .ZIP file format for storing and transporting compressed data files, PKZIP®. The company remains the technology leader in this market, and continues to add features and functionality to this popular file format.

Not only is PKWARE the technology leader, but it is also the **ONLY** provider of cross-platform interoperable zip applications. In addition, PKWARE products offer the following capabilities, unmatched by any other data-centric security product.

**Centralized Policy Management** – Control when, how, and by whom encryption is being used in the organization through policy that is non-restrictive and integrated into everyday workflow.

**Contingency Key** – Ensure corporate readiness for disaster recovery or regulatory audits with contingency key capabilities that provide administrative access to every file encrypted within the organization.

**Single Solution** – Reduce the cost and time of managing multiple solutions. The PKWARE solutions are available on every major computing platform, eliminating the need for disparate point solutions.