IBE Myth #1: IBE is a One-Step-Process

As previously mentioned, the concept of IBE sounds simple; it requires only a recipient’s email address to send secure communication. However, there is more to the implementation of IBE, including setup requirements for both the sending and receiving sites. The recipient needs to get a [private] key from the sending organization in order to open encrypted files—an email address is used as a public key only. To decrypt a file, a recipient needs to get a private key associated with their public key (email address). Essentially, this is the same process that takes place using PKI.

While a recipient can retrieve their own key, they must authenticate to a server owned by the sending organization in order to do so. The process of authentication adds an extra setup step to the process of retrieving a key, requiring the sending organization to setup their server to grant the recipient access to the machine that provides the private key. Again, this is no different than the steps required to connect to a PKI Certificate Authority to obtain a PKI key-pair.

For organizations that may be considering implementing IBE, it is imperative to keep in mind that there can be multiple servers required before being able to manage and deliver keys to recipients. Soon the “simple” activity of encrypting using just an email address becomes much more complex.

IBE Myth #2: IBE Ensures the Privacy of its Users

IBE uses a public key generator (PKG) to supply private keys for its users. Private keys are generated on the IBE PKG server that is under the control of the IBE owner. Using IBE, private keys are not under the control of the person to whom the private key belongs (and represents). As a result, access to a private key is possible and it may be used to decrypt and/or sign any message without prior

SecureZIP by PKWARE can easily (and automatically) locate a recipient’s key by using their email address, eliminating one of the major concerns associated with traditional public-key cryptography. Each SecureZIP user can obtain their key by providing nothing more than an email address, providing a similar level of abstraction around keys as is provided by IBE. The sender does not need to explicitly go and get a public key; SecureZIP will automatically retrieve the public key using the recipient’s email address.

In addition, unlike traditional public-key cryptography approaches, SecureZIP eliminates the need to query a directory service to ask for a key. Using SecureZIP, user keys can be automatically placed into and retrieved from the SecureZIP Global Directory, eliminating the need for senders to query a directory before exchanging files. In addition, the limitation of querying an internal central directory is not an obstacle when using SecureZIP; the SecureZIP Global Directory is a publicly available directory that can be accessed from anywhere.

Some vendors recognize this misconception as common in the market and seek to take advantage of it. One proposed alternative for making public-key cryptography less cumbersome is identity-based cryptography, otherwise known as identity-based encryption (IBE). Supposedly, IBE offers all the strength for data protection offered by classical PKI, while reducing the burden on the organization and on users.

While IBE may seem simple on the surface, promoting that an email address is all that is required to securely exchange information is not entirely true. Implementing IBE poses challenges of its own, some of which may jeopardize the security of the data exchange. This paper focuses on correcting some of the common myths associated with IBE, as well as examining the inherent differences between IBE and PKI in terms of complexity and utility. The results show that, in fact, PKI is as easy to use as IBE, particularly when paired with SecureZIP® by PKWARE®, which uses the industry-standard X.509 digital certificates to ensure secure data exchange.
authorization from the key holder. Further, key escrow is one of the major short-falls of IBE, as someone will always have access to the back-up copies of the private keys used for encryption. While this provides a means to recover a private key should it be lost or damaged, it eliminates the complete privacy that other methods, such as digital certificates offer.

Accepted best-practices for private key integrity depend on private keys always existing in the hands of their attached identity, and only in the hands of the person for whom they were issued. Unlike private keys supplied by a PKG, SecureZIP uses X.509 digital certificates issued by a trusted third-party certificate authority (CA). This ensures that the private key is created on the owner's machine and is always held only by the owner. Rather than maintaining a back-up procedure to recover private keys, SecureZIP provides a contingency key feature which ensures the recoverability of data rather than keys.

**IBE Myth #3: IBE is Easily Accessible by Users**

As discussed previously, IBE involves creating private keys on the server of the IBE owner. Typically, an IBE owner's server is sufficiently sized to handle the limited number of users that may need to access a single site to obtain their keys. However, all users needing keys must access that server to obtain them. This means any IBE system, by its nature a centralist approach, can only handle a finite number of recipients, which limits its accessibility and scalability.

Using X.509 digital certificates, SecureZIP is not restricted by this limitation since private keys may be obtained from any source that provides X.509 V3 digital certificates. This also means SecureZIP is not limited to the capabilities of a single server and effectively scales to support the number of users that may need keys on the public Internet.

**IBE Myth #4: IBE does not Require a Key Exchange**

In addition, IBE purports that it does not require a public key exchange; however, in order for recipients to communicate, there must be an exchange. Instead of exchanging PKI public keys, which can be freely transferred using any commonly available method of exchange (e.g. unprotected email, posting on an unprotected website or bulletin board), IBE requires the exchange of a private key. While exchanging a private key is inherently a bad idea, if it is exchanged, it must be done only over a secure connection. This drastically limits the methods by which a private key can be delivered to its recipient.

SecureZIP's use of X.509 digital certificates avoids the risks and complexities of exchanging a private key by not requiring it in the first place. It further facilitates the exchange of public keys by providing the public SecureZIP Global Directory for sharing keys used by SecureZIP, as well as supporting any LDAP-compliant directory service for exchanging keys amongst a closed community.

**SecureZIP & X.509 Digital Certificates**

SecureZIP makes acquiring and using a digital certificate simple and easy, allowing you to exchange files and emails securely. Upon installation, SecureZIP will automatically request and install (if desired) a digital certificate1 from one of the industry’s leading certificate authorities.

Once your digital certificate is installed, people can send you secure files and emails, securing them with your public key. When you receive the secure, encrypted communication, SecureZIP uses your private key to decrypt. Digital certificates are also used for signing, which assures recipients that the communication has come from you and can be trusted.

The SecureZIP Global Directory is a depository of public keys for SecureZIP users, making it easy to send secure files with digital certificates. When you send a secure email using a digital certificate, SecureZIP automatically checks the Directory for the public key associated with the recipient's email address. If your recipient doesn't have a digital certificate, you can still secure your message with a passphrase.

---

1 SecureZIP makes acquiring and using a digital certificate simple and easy, allowing you to exchange files and emails securely. Upon installation, SecureZIP will automatically request and install (if desired) a digital certificate from one of the industry’s leading certificate authorities. Once your digital certificate is installed, people can send you secure files and emails, securing them with your public key. When you receive the secure, encrypted communication, SecureZIP uses your private key to decrypt. Digital certificates are also used for signing, which assures recipients that the communication has come from you and can be trusted. The SecureZIP Global Directory is a depository of public keys for SecureZIP users, making it easy to send secure files with digital certificates. When you send a secure email using a digital certificate, SecureZIP automatically checks the Directory for the public key associated with the recipient's email address. If your recipient doesn't have a digital certificate, you can still secure your message with a passphrase.