

Comparison of X.509/PKI and IBE based Secure Email Technologies

Overview

Identity-Based Encryption (IBE) is a form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages.

Using an email address as a public key may sound like a more convenient approach to encryption, as it will eliminate the need to know the recipient's public key beforehand, but in fact it has more security vulnerabilities than you would think.

In comparison, X.509/PKI users communicate securely through a public and a private key pair that has been securely generated and published through a trusted authority.

The overarching benefit of PKI is that it has well-established standards and is commonly supported by a large variety of interoperable vendors.

IBE is vendor specific and is not interoperable.

IBE essentially tries to solve a number of difficulties that comes with full RSA Public Key Installation:

1. The recipient needs a key-pair generated before anyone can send them an encrypted message
2. The sender should be able to find the public certificate of the recipient

Using the persons email address as the public key, addresses both of these issues, because it is possible to figure out the recipient's public certificate by knowing their email address.

An example of an IBE public key would be: name@gmail.com

An example of an RSA-PKI would be:

```
Public exponent=0x10001
Modulus=135066410865995223349603216278805969938881
560566702752448514385152651060485953383394028715
057190944179820728216447155137368041970396419174
304649658927425623934102086438320211037295872576
235850964311056407350150818751067659462920556368
552947521350085287941637732853390610975054433499
9811150056977236890927563
```

Definitions

A **PKI** (public key infrastructure) enables Internet users to securely and privately exchange confidential information through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key provides a digital certificate that identifies the individual or company. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message.

Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science and engineering. Applications of cryptography include ATM cards, computer passwords and e-commerce.

Identity-Based Encryption (IBE) is a form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages.

Cryptography **X.509** is the Telecommunications Standardization Sector (ITU-T) for a public key infrastructure. It specifies standard formats for public key certificates, certificate revocation lists, attribute certificates and a certificate path algorithm.

The IBE convenience comes with a number of serious security vulnerabilities and functionality deficiencies. In fact the convenience is only a perceived convenience because the IBE based solution doesn't address most of the usability issues:

- Although the email can be created without any knowledge of the recipient's public certificate, the recipient still needs to register to be able to read it, which is essentially how most PKI solutions handle unknown users today
- With IBE and RSA-PKI, the number of steps required to send or receive messages is identical
- Even though the lookup of public certificates for recipients is unnecessary, the private keys need to be created regularly. Therefore, the Private Key Generator (PKG) server needs to be highly trusted, and arguably can be vulnerable to a man-in-the-middle attack.

When choosing IBE over PKI consider the following:

- IBE is a relatively new technology with very few implementations
- IBE is not an internationally accepted standard
- PKI has well-established standards and is commonly supported by a large variety of interoperable vendors
- IBE implementations to date are vendor specific and not interoperable

Technical Comparison

Activity	X.509 PKI	IBE
Key revocation Once a key has been reported as being un-trustworthy PKI prevents it from being used	Yes	No
Identity Certificate A data file that strongly binds a key and an identity, usually including how and when the identity was verified, the certificate lifetime, revocation information, key usage and issuer information	Yes	No
Server does not have a private key The PKI server does not have a private key and cannot decrypt emails. With PKI emails can only be decrypted by the recipient. Unlike the IBE server which does have the ability to decrypt messages	Yes	No
Meets Digital Signature Requirement Legally, the signer must have total control of their private key. The PKI digital signatures meets this requirement	Yes	No
Authenticates Sender and Recipient PKI ensures that the sender and the recipient use valid credentials. Without this verification email messages can easily be spoofed and can be received by people other than the intended recipient	Yes	No
Verified Timestamp With PKI the sender cannot fake the time and date fields as each email is time stamped and verified	Yes	No
Verify Sender's Email Address PKI verifies the sender and logs who sent the email and when. IBE has no logs so the recipient cannot verify who the message came from before opening the message.	Yes	No
Prevents Phishing (Email Fraud) With PKI recipients can independently verify the authenticity of an email using digital signatures. By clicking on a link from an unverified source can lead to the inadvertent installation of malware and viruses.	Yes	No

Centralized Key Revocation A centralized location for key revocation notices eliminates a variety of notifications being posted for the same key at the same time	Yes	No
Secure Attachments IBE sends messages as secure attachments and they can remain in the recipients inbox indefinitely	No	Yes
Sender makes own certificate available The sender must make their own key certificate available to the recipient	No	Yes