



## ZixMail Technology

This document describes the encryption technology used to send and receive a ZixMail message.

The ZixMail process ensures user **privacy**, message **integrity**, sender and recipient **authentication** and **non-repudiation**. This is accomplished by using public key cryptography. In ZixMail public key cryptography, each ZixMail user has a complementary pair of keys, a Public Key and a Private Key. The Public Key is used for message encryption and for digital signature verification. The Private Key is used for message decryption and for digitally signing a message.

The Public Key is stored at the ZixIt Worldwide Signature Server (WSS). This central storage site removes the burden and complexity of key exchange and maintenance. The Private Key resides exclusively on the user's computer and is encrypted with a user defined Signature Phrase. The Signature Phrase prevents unauthorized access to the Private Key.

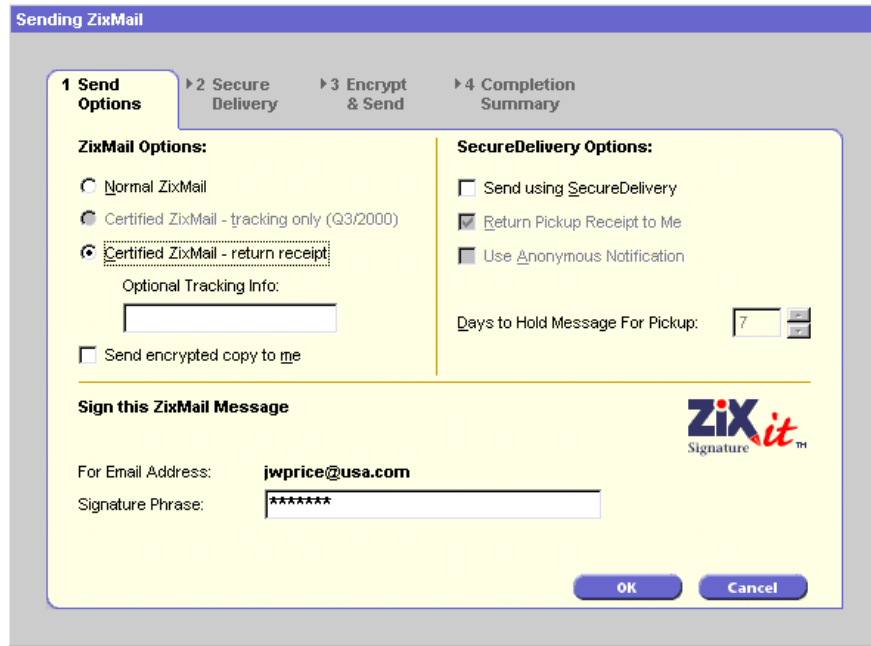
## Sending a ZixMail Message

1. A message to be sent is first composed in the ZixMail application as depicted below.



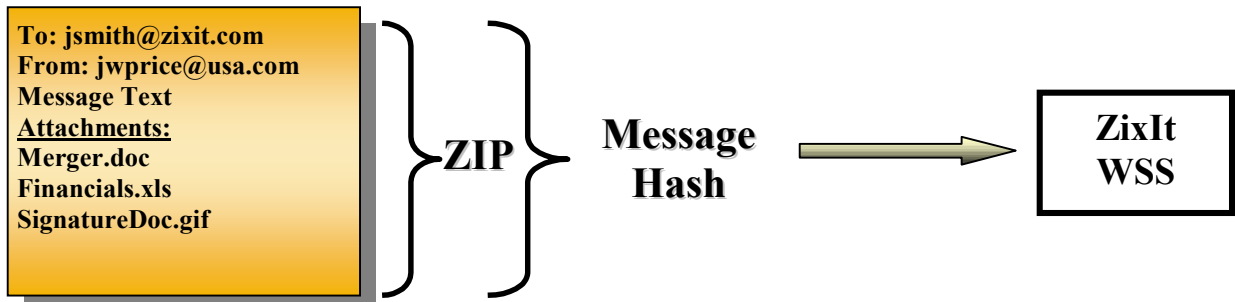


- To send a ZixMail message, the sender clicks the “send” button, selects sending options, such as “Certified ZixMail - return receipt,” and enters their Signature Phrase. An example of the Sending ZixMail dialog box follows:



- After the ZixMail message is composed, sending options selected, and the Signature Phrase is entered, the entire email message including **to**, **cc**, **subject** and **from** fields, the **message text** and **attached files**, is automatically compressed and a hash of the entire message is derived. The message hash (128-bit) is a unique, short-length numerical representation of the entire message that is sent to the ZixIt Worldwide Signature Server for processing.

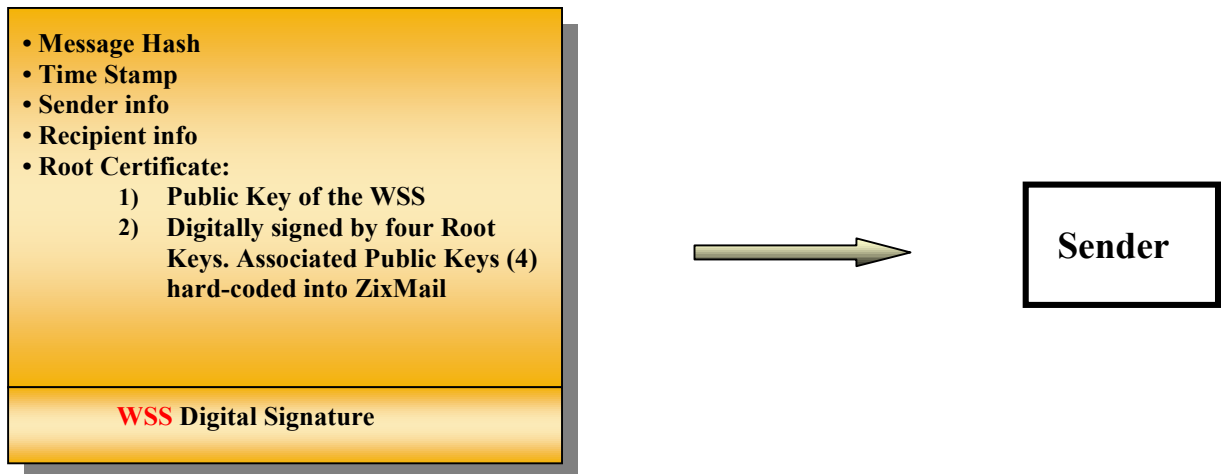
## Email Message



4. The WSS returns a Time Stamp Certificate (TSC) and the recipient's Public Key to the sender's ZixMail software. The TSC contains the message hash, a time stamp, sender and recipient key validity codes and a root certificate. The root certificate certifies the WSS Public Key and is signed by four root Private Keys. The four root Public Keys are hard-coded into each ZixMail program.

All ZixMail user's Public Keys are stored in the WSS, thus eliminating the need for direct Public Key exchange between users. Each Public Key status is validated in real-time during TSC processing.

### Time Stamp Certificate (TSC)



The TSC is a single-use digital certificate issued in real time that ties the following together:

- Sender's Public Key and identity (email address)
- Recipient's Public Key and identity (email address)
- The message hash
- The date and time

During the sending process, the TSC authenticates the recipient's Public Key before it is used to encrypt the message and verifies that the sender's Private Key has not been revoked.

Later, when the message is received and opened, the TSC will be used for authentication and verification purposes.

5. A digital signature is generated for the combination of the email message and the TSC. A digital signature uniquely identifies the sender and can be used to verify that the received message has not been altered since it was sent.

## Email Message

To: jsmith@zixit.com  
From: jwprice@usa.com  
Message Text  
Attachments:  
Merger.doc  
Financials.xls  
SignatureDoc.gif

## Time Stamp Certificate

- Message Hash
- Time Stamp
- Sender & Recipient Info
- Root Certificate

**WSS Digital Signature**



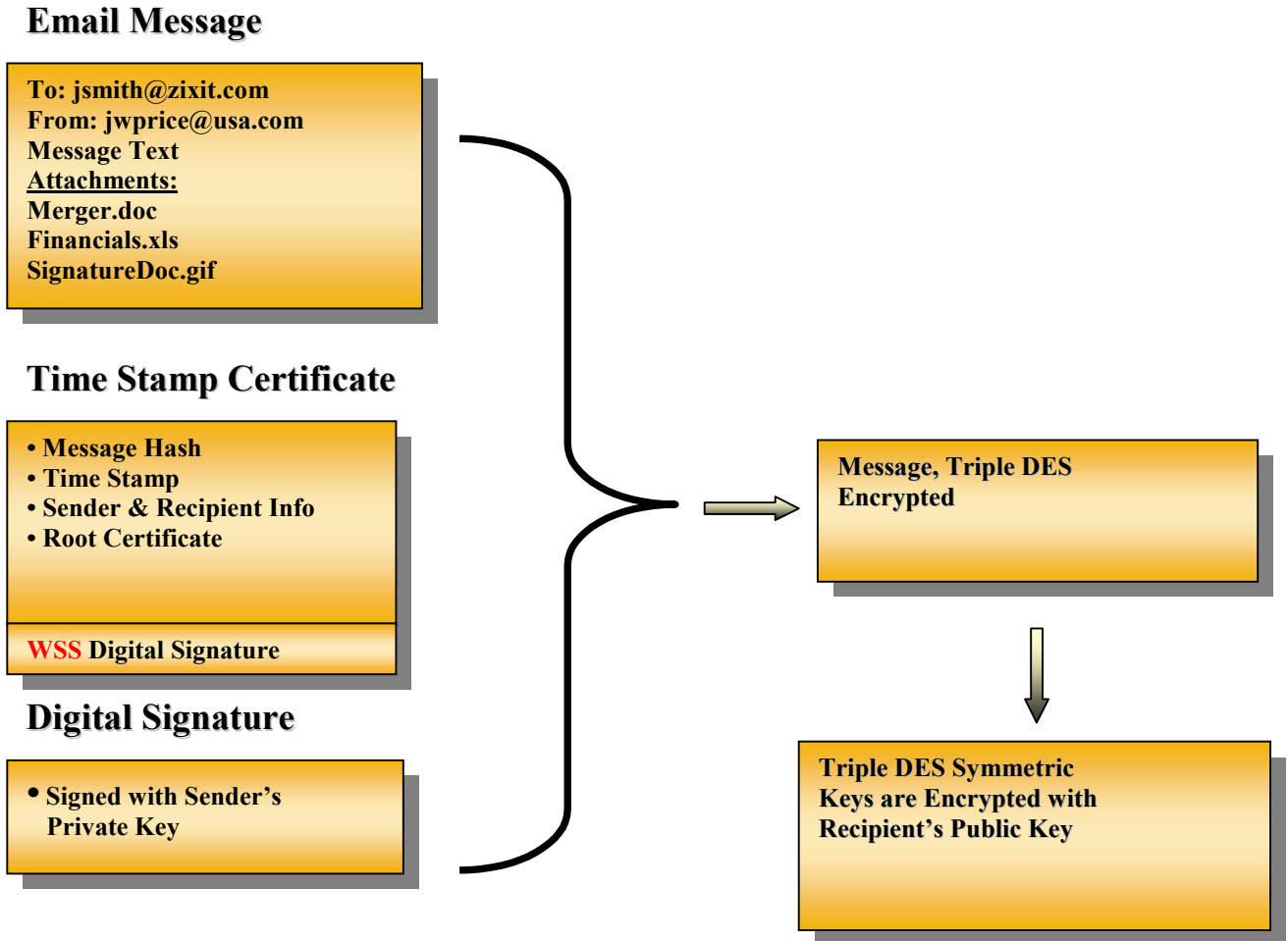
Signed with  
Sender's  
Private Key



## Digital Signature

- Signed with Sender's Private Key

- The three components; compressed email message, TSC and Digital Signature are Triple DES encrypted with randomly generated symmetric keys. The Triple DES symmetric keys are encrypted with the recipient's Public Key. The fully encrypted digitally signed ZixMail message is sent directly to the recipient's regular email inbox. The encrypted message does not travel through the ZixIt WSS.

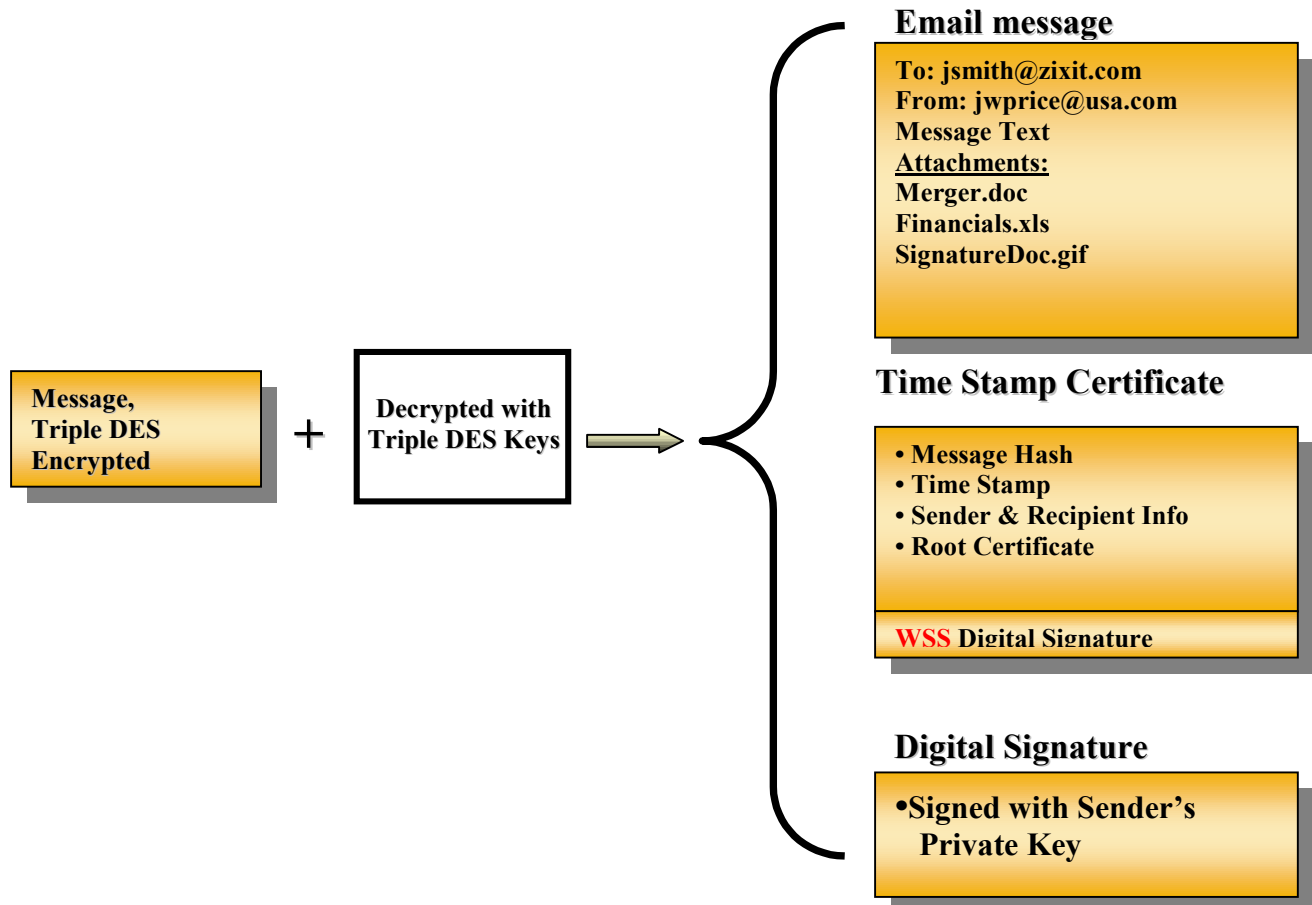


## Receiving a ZixMail Message

- ZixMail arrives in the recipient's regular email inbox. Clicking or double clicking the ZixMail attachment and entering the recipient's Signature Phrase opens the ZixMail message. The Signature Phrase enables the decryption of the Private Key file to obtain access to the Private Key. The recipient's Private Key decrypts the Triple DES Symmetric Keys that were created during the message sending encryption process.



- The message is then decrypted with the Triple DES Symmetric Keys and the message, after various authentications, is displayed to the recipient. This process keeps the communication confidential and private because only the recipient has the Private Key needed to decrypt the message.



9. ZixMail verifies the sender's digital signature using the sender's Public Key, verifies the TSC to ensure authenticity of the sender's Public Key, verifies the root certificate to ensure the authenticity of the WSS Public Key used to verify the digital signature on the TSC, verifies that the message hash inside the TSC matches the hash computed from the message, and verifies that the time in the TSC is within the validity period of all keys and certificates. If all the verifications succeed, it ensures the following:

- **Authenticity and Non-repudiation**, because only the sender has the Private Key that created the digital signature
- **Integrity**, because the newly generated hash matches the hash carried inside the sender's digital signature
- **Irrefutable Time Stamp**, because an external authority (WSS) has digitally signed the TSC that contains the time stamp.

### Email message

To: jsmith@zixit.com  
 From: jwprice@usa.com  
 Message Text  
Attachments:  
 Merger.doc  
 Financials.xls  
 SignatureDoc.gif

### Time Stamp Certificate

- Message Hash
- Time Stamp
- Sender & Recipient Info
- Root Certificate

WSS Digital Signature

### Digital Signature

- Signed with Sender's Private Key

