



Security Header

Encrypted Key

Encrypted Key

Encrypted Data

Timestamp

Binary Security Token

Signature

The first encrypted key is used to encrypt the response content, in the message body.

The second encrypted key is used to encrypt the first attachment. The encrypted part is referenced indirectly through an Encrypted Data element.

This encrypted data element is a *reference* to an encrypted part.

The timestamp includes creation and expiry times.

The binary security token element is the X.509 certificate used to sign the message, Base64 encoded.

The signature element, in addition to the computed digital signature, includes references to the elements covered by the signature, as well as a reference to the certificate that can verify it (the preceding BST). Encrypted Key

Encryption Method

Key Info

Cipher Data

Reference List

The encryption method element is an attribute-only element that names the algorithm used to encrypt this key

Key Info contains a Security Token Reference used to locate the key that was used to encrypt this key

The Cipher Data element holds the Base 64-encoded bytes of the encrypted key

The Reference List element contains a list of Data Reference elements, one for each element that was encrypted using this key

Key Info

Security Token Reference

Key Identifier

The security token reference identifies the key that can decrypt this encrypted key

The Key Identifier is the Base 64-encoded SKI of the certificate whose key was used to encrypt this key

Reference List

Data Reference

Data Reference holds a URI identifying an element or part that was encrypted by the enclosing Encrypted Key element.

(Optional)
Data Reference