Message Integrity

This is for data at rest. Integrity of data in transit can easily be provided by TLS.
When using public key cryptography, encryption does guarantee confidentiality but it does not guarantee integrity since the receiver's public key is public. For the same reason, encryption does not ensure the identity of the sender.
Rule: For XML data, use XML digital signatures to provide message integrity using the sender's private key. This signature can be validated by the recipient using the sender's digital certificate (public key).

Server Authentication

Rule: TLS must be used to authenticate the service provider to the service consumer. The service consumer should verify the server certificate is issued by a trusted provider, is not expired, is not revoked, matches the domain name of the service, and that the server has proven that it has the private key associated with the public key certificate (by properly signing something or successfully decrypting something encrypted with the associated public key).

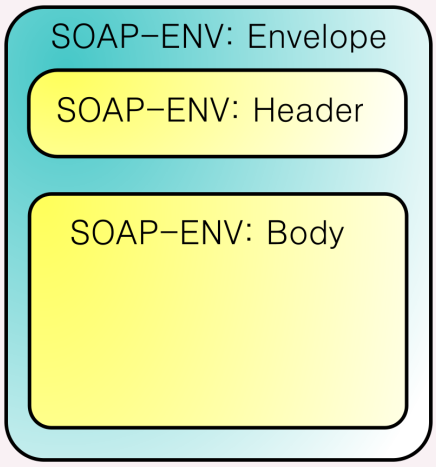
Transport Confidentiality

Transport confidentiality protects against eavesdropping and man-in-the-middle attacks against web service communications to/from the server.
Rule: All communication with and between web services containing sensitive features, an authenticated session, or transfer of sensitive data must be encrypted using well configured TLS. This is recommended even if the messages themselves are encrypted because TLS provides numerous benefits beyond traffic confidentiality including integrity protection, replay defenses, and server authentication. For more information on how to do this properly see the Transport Layer Protection Cheat Sheet..

Message Integrity

This is for data at rest. Integrity of data in transit can easily be provided by TLS.
When using public key cryptography, encryption does guarantee confidentiality but it does not guarantee integrity since the receiver's public key is public. For the same reason, encryption does not ensure the identity of the sender.
Rule: For XML data, use XML digital signatures to provide message integrity using the sender's private key. This signature can be validated by the recipient using the sender's digital certificate (public key).

SOAP structure



User Authentication

User authentication verifies the identity of the user or the system trying to connect to the service. Such authentication is usually a function of the container of the web service.
Rule: If used, Basic Authentication must be conducted over TLS, but Basic Authentication is not recommended.
Rule: Client Certificate Authentication using TLS is a strong form of authentication that is recommended.

Transport Encoding

SOAP encoding styles are meant to move data between software objects into XML format and back again.
Rule: Enforce the same encoding style between the client and the server.

Source

https://owasp.org/www-project-cheat-sheets/cheatsheets/Web_Service_Security_Cheat_Sheet.html

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com