HACKMANIT

RUB

Secure web services check list

Goal	Feature	Fulfilled	Not fulfilled	Not relevant
Integrity + Authentication	Signature			
Confidentiality	Encryption			
Freshness	Timestamps and nonces			
Availability	DoS prevention			
Miscellaneous	Miscellaneous			

Configuration	Recommendation		Fulfilled	Not fulfilled	Achieved with
Signed parts	Body and other crucial parts (e.g. timestamps, nonces, encrypted parts, WS-A headers …)				
Signature algorithm	RSA (≥ 2048 bit keys) or ECDSA (≥ 250 bit keys)				
Digest algorithm	Algorithm from SHA2 or SHA3 family, e.g. SHA-256				
Prevent XSW attacks	Execute signed parts of the message only				
Certificate trust	Reference certificates by their ID and validate locally whether they are trustworthy				
Encrypted parts	Parts containing non-public information (e.g. Body)				
Encryption algorithms	Asymmetric key establishment	RSA-OEAP (≥ 2048 bit keys)			
	Symmetric data encryption	AES-128 or AES-256 in GCM-mode if available, CBC-mode in combination with a signature otherwise			
Combine encryption with a signature	Signed parts	All encrypted parts			
	Order to apply	Encrypt-then-Sign			
Timestamps	Enable for all messages				
Nonces	Enable for all messages				
Secure timestamps and nonces against tampering	Sign timestamps and nonces				
XML Schema Validation	Validate messages against SOAP, “WS-Security” and own schema				

http://ws-attacks.org/Security_Best_Practices:_Web_Services

DTDs/XML Entities	Disable support completely			
Data throttling	Enable a maximum message size and a maximum of messages accepted in a time period			
SOAPAction parameter	Disable or implement check if parameter and function call in Body match			
WS-Addressing	Disable or enforce strict whitelist			

http://ws-attacks.org/Security_Best_Practices:_Web_Services