Web Services Addressing defines two interoperable constructs that convey information that is typically provided by transport protocols and messaging systems. It is a standardized way of including routing data with SOAP headers. An endpoint references is an XML structure encapsulating information for addressing a message to a web service. It contains destination address of the message, additional parameters and optional metadata. The two constructs are endpoint references and message information headers. A web service endpoint is a entity where web service messages can be targeted. Endpoint references is used for convey the information to access a web service endpoint, but are also used to provide addresses for individual messages sent to and from web services. The message information headers convey end-to end message characteristics including addressing for source, destination endpoints and message identity. The net work -level transport is responsible for delivering the message to a dispatcher and the job of network-level transport is done as long as the message arrives at the dispatcher. There are several properties of message addressing including message destination, source endpoint, reply endpoint, fault endpoint, action, unique message ID and relationship to previous messages. Source endpoint is the end point of the service that dispatched the message. Reply end point is the endpoint to which reply messages should be dispatched. Fault endpoint is the endpoint to which fault messages should be dispatched. Action is the value indicating the semantics of the message, mechanisms for key exchange.

WS-trust emerged in the SOAP world to allow web services to share user identities by incorporating standard security tokens into SOAP headers. It is short for Web Services Trust Language and it is and specification which provides extensions to WS-security. It defines a number of new elements and concepts including Security Token Service, the formats of the messages used to request security tokens and the responses to those messages. Security Token Service is a web service that issues security tokens as defined in the WS-Security specification. It converts locally issued tokens into a format shared with web services providers and also for converting tokens into a format that can be used by local applications. WS-Trust standard specifies that Security Token Service can be used by web service clients and providers. The WS-Trust specification was authored by representatives of a number of companies. It can engage in secure communication designed work within the web services framework. WS-Trust deals with managing software security tokens include SAML tokens and UsernameTokens. It defines protocols to issue, cancel, renew WS-Security tokens and enable secure message through Web Services. STS converts whatever security token being used locally into a standard SAML security token containing the user’s identity on the web service client side. STS validates incoming security tokens and generate new local token for consumption by other applications on the web service provider side.

WS-Policy provides flexible grammar for expressing the capabilities, requirements and general characteristics of entities in an XML Web services-based system. It allows web services to use XML to advertise their polities and for web service consumers to specify policy requirements. It defines a policy to be a collection of policy alternatives. Some policy assertions specify traditional requirement. Other policy assertions have no wire manifestation yet to proper service selection and usage. It does not specify how policies are discovered or attached to a web service. The goal of WS-policy is to provide the mechanisms to enable Web services applications to specify policy information such as an XML infoset called policy expression that contains domain-specific, Web Service policy information and a core set of constructs to indicate how choices of domain-specific policy assertions apply in a Web series environment. An effective policy will be computed containing intersection of both policies if both provider and consumer specify a policy. The assertions in the new policy must not contradict each other except synonymous assertions, which is considered not compatible by a policy intersection. WS-policy defeins a flexible and powerful structure for expressing constrains of any form but the implementations of WS-policy processing used by web series stacks don’t implement much of the flexibility. Many useful features of WS-policy cannot be sued for web services to interoperate with a full range of web service stacks because of the lack of implementation support.