7 Security Considerations

This specification considers two sets of security requirements, those of the applications that use the WS-Transfer protocol and those of the protocol itself.

This specification makes no assumptions about the security requirements of the applications that use WS-Transfer. However, once those requirements have been satisfied within a given operational context, the addition of WS-Transfer to this operational context can not undermine the fulfillment of those requirements; the use of WS-Transfer SHOULD NOT create additional attack vectors within an otherwise secure system.

The material below is not a "check list". There are many other security concerns that need to be considered when implementing or using this protocol. Implementers and users of this protocol are urged to perform a security analysis to determine their particular threat profile and the appropriate responses to those threats.

7.1 Protecting Resources

Both resources and the information that makes up their representation might be sensitive. In these cases, it is advisable for resource managers to authenticate and authorize clients attempting Get, Put, or Delete operations. To protect representations sent over a network, the wst:Get, wst:GetResponse, wst:Put, and wst:PutResponse messages ought to have the appropriate authenticity, integrity, and confidentiality measures applied.

7.2 Protecting Resource Factories

In cases where resources and/or the information that makes up their representation are sensitive so, too, are the services that create these resources. In such cases it is advisable for resource factories to authenticate and authorize clients attempting Create operations. To protect representations sent over a network, wst:CreateResponse messages that include representations ought to have the appropriate authenticity, integrity, and confidentiality measures applied.