10 Security Considerations

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

This specification makes no assumptions about the security requirements of the applications that use WS-MetadataExchange. However, once those requirements have been satisfied within a given operational context, the addition of WS-MetadataExchange to this operational context can not undermine the fulfillment of those requirements; the use of WS-MetadataExchange 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.

10.1 Metadata and Security Bootstrapping

There are cases in which the metadata used to describe a service might be considered sensitive information. In these cases it is advisable for services to authenticate and authorize consumers as part of the processing of any requests for this metadata. However, because the security aspects of a service (e.g. supported protocols and token formats, cipher suites, etc.) are usually described using metadata (i.e. the constructs defined by WS-SecurityPolicy), there is an obvious dilemma when attempting to protect metadata in this way. Services wishing to protect access to their metadata are advised to use the mechanisms described in Section 12 to advertise the security requirements for clients wishing to access metadata via the mechanisms defined in this specification.