[MS-WSMV]: Web Services Management Protocol Extensions for Windows Vista

This topic lists the Errata found in [MS-WSMV] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V29.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Sections 2.2.9.1.1.1, HTTP Headers, 2.2.9.1.2.1, HTTP Headers, 2.2.9.1.3.1.1, HTTP Headers, and 2.2.9.1.3.2.1, HTTP Headers, updated that the protocolvalue token contains the authentication mechanism that is used to establish the security encryption context. For example, in Section 2.2.9.1.1.1, HTTP Headers, changed from: protocolvalue: Contains the authentication mechanism that is used to establish the security token. It MUST be set to "application/HTTP-SPNEGO-session-encrypted", which indicates the security context that is obtained from authentication by using SPNEGO over HTTP, as specified in [RFC4559] section 6, and is used to encrypt the message. Changed to: protocolvalue: Contains the authentication mechanism that is used to establish the encryption context. It MUST be set to "application/HTTP-SPNEGO-session-encrypted", which indicates the security context that is obtained from authentication by using SPNEGO over HTTP, as specified in [RFC4559] section 6, and is used to encrypt the message. In Section 2.9.1.2.2.2, Encrypted Data, updated that the Length-Field token specifies the length of the per-message token portion of the Message field. Changed from: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the encryption header portion of the Message field. Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework specific to the authentication protocol selected by SPNEGO. SPNEGO can select Kerberos or NTLM as the underlying authentication protocol. For Kerberos, the framework is as specified in [RFC4121]. For NTLM, the encryption details are as described in [MS-NLMP]. The initial bytes of the Message vary based on the chosen authentication protocol: • For Kerberos, it MUST be the per-message token as specified in [RFC4121]. • For NTLM, it MUST be its Message Signature. The length of the initial bytes of the Message MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.1.2.1. Changed to:

Errata Published*	Description
	Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the encryption header portion of the Message field (see the discussion of the Message encryption header that follows). Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework specific to the authentication protocol selected by SPNEGO. SPNEGO can select Kerberos or NTLM as the underlying authentication protocol. For Kerberos, the framework is as specified in [RFC4121]. For NTLM, the encryption details are as described in [MS-NLMP]. The encryption header of the Message token varies based on the chosen authentication protocol: For Kerberos, it MUST be the per-message token as specified in [RFC4121]. • For NTLM, it MUST be its Message Signature. The length of the encryption header of Message MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.1.2.1. In Section 2.2.9.1.1.2.2, Encrypted Data, clarified that the Message token encryption header varies based on the chosen authentication protocol. Changed from: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the security token portion of the Message field. Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose original length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.2.2.1. Changed to: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the per-message token, as specified in [RFC4121], portion of the Message field. Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the per-message token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose original length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.2.2.1
2016/02/22	In several subsections, clarified the use of TLS encryption. In Section 2.2.9.1.3, CredSSPEncryptedMessage, updated that CredSSPEncryptedMessage message can be encrypted by the Transport Layer Security (TLS) security context established as part of the CredSSP protocol. Changed from:

Errata Published*	Description
	This message is used when CredSSP, as specified in [MS-CSSP], is used for setting up a security context between the client and server. The client and server can encrypt the message by using the GSS-API security context.<41> Changed to: This message is used when CredSSP, as specified in [MS-CSSP], is used for setting up a security context between the client and server. The client and server can encrypt the message by using the Transport Layer Security (TLS) security context established as part of the CredSSP protocol.<41> In Section 2.2.9.1.3.1.2.2, Encrypted Data, updated that EncryptedData message is an octet stream of TLS encrypted SOAP message. Changed from: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the security token portion of the Message field. Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose original length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.3.1.2.1. Changed to: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of any trailer portion of the Message field. Message: The encrypted message. This is an octet stream of TLS encrypted SOAP message. In Section 2.2.9.1.3.2.2.2, Encrypted Data, updated that EncryptedData message is an octet stream of TLS encrypted SOAP message. Changed from: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the security token portion of the Message field. Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose original length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.3.2.2.1. Changed to: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of any trailer portion of the Message field. Message: The encrypted message. This is an octet stream of TLS encrypted SOAP message.

*Date format: YYYY/MM/DD