[MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol

This topic lists the Errata found in [MS-NLMP] 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 V31.0 – 2019/09/23.

Errata Published*	Description

2020/08/17	In section 3.1.5.1.2 Client Receives a CHALLENGE_MESSAGE from the Server, added NTLMSSP_NEGOTIATE_SIGN and NTLMSSP_NEGOTIATE_SEAL Flags.
	
	Changed from:
	
	`If (NTLMSSP_NEGOTIATE_KEY_EXCH bit is set in CHALLENGE MESSAGE.NegotiateFlags )`
	`  Set ExportedSessionKey to NONCE(16)`
	`  Set AUTHENTICATE_MESSAGE.EncryptedRandomSessionKey to RC4K(KeyExchangeKey, ExportedSessionKey)`
	`Else`
	`  Set ExportedSessionKey to KeyExchangeKey`
	`  Set AUTHENTICATE MESSAGE.EncryptedRandomSessionKey to NIL`
	`Endif`
	
	Changed to:
	
	`If (NTLMSSP_NEGOTIATE_KEY_EXCH bit is set in CHALLENGE_MESSAGE.NegotiateFlags`
	`  AND (NTLMSSP_NEGOTIATE_SIGN OR NTLMSSP_NEGOTIATE_SEAL are set in CHALLENGE MESSAGE.NegotiateFlags))`
	`  Set ExportedSessionKey to NONCE(16)`
	`  Set AUTHENTICATE MESSAGE.EncryptedRandomSessionKey to RC4K(KeyExchangeKey, ExportedSessionKey)`
	`Else`
	`  Set ExportedSessionKey to KeyExchangeKey`
	`  Set AUTHENTICATE MESSAGE.EncryptedRandomSessionKey to NIL`
	`Endif`
	
	In section 3.2.5.1.2 Server Receives an AUTHENTICATE_MESSAGE from the Client, added server behavior when NTLMSSP_NEGOTIATE_KEY_EXCH is set.
	
	Changed from:
	
	If GuestSession is TRUE, a SessionBaseKey with all-zeroes, Z(16), is used.
	
	If NTLM v2 authentication is used and channel binding is provided by the application, then the server MUST verify the channel binding: <66>

Errata Published*	Description
	Changed to: If GuestSession is TRUE, a SessionBaseKey with all-zeroes, Z(16), is used. If NTLMSSP_NEGOTIATE_KEY_EXCH is set, the server MUST check if client supplied a valid EncryptedRandomSessionKey in the AUTHENTICATE_MESSAGE (section 2.2.1.3); otherwise, the server MUST return SEC_E_INVALID_TOKEN. If NTLM v2 authentication is used and channel binding is provided by the application, then the server MUST verify the channel binding:<66>
2020/08/17	In section 3.4.4.3 Without NTLMSSP_NEGOTIATE_SIGN, added section. Changed from: 3.4.4.2 With Extended Session Security . . . 3.4.5 KXKEY, SIGNKEY, and SEALKEY Changed to: 3.4.4.2 With Extended Session Security . . . 3.4.4.3 Without NTLMSSP_NEGOTIATE_SIGN When NTLMSSP_ALWAYS_NEGOTIATE_SIGN is set and message integrity (NTLMSSP_NEGOTIATE_SIGN) is not negotiated, the message signature for NTLM is a 16-byte value that contains the following components, as specified by the NTLMSSP_MESSAGE_SIGNATURE structure (section 2.2.2.9): • Version: A 4-byte number value that is set to 0x00000001. • All other bytes set to zero. 3.4.5 KXKEY, SIGNKEY, and SEALKEY
2019/12/16	In Section 3.4, Session Security Details, added ANONYMOUS user with Guest user and section reference. Changed from: For the case of Guest user login, there is no session security. Changed to: For the cases of ANONYMOUS user and Guest user login, there is no session security (see section 3.2.5.1.2). In Section 5.1, Security Considerations for Implementers, added ANONYMOUS user, Guest user, and Guest log in case 2 of 3. Changed from: The use of NullSession results in a SessionBaseKey with all zeroes, which does not provide security. Therefore, applications are generally advised not to use NullSession. The Guest user account is disabled by default in Windows for security reasons. If the Guest user account is enabled, it is strongly recommended to set a password so that logon failures do not result in Guest logins (section 3.2.5.1.2). Changed to:

Errata Published*	Description
	The use of ANONYMOUS user NullSession results in a SessionBaseKey with all zeroes, which does not provide security. Therefore, applications are generally advised not to use NullSession. The use of Guest user GuestSession results in a SessionBaseKey with all zeroes, which does not provide security. The Guest user account is disabled by default in Windows for security reasons. If the Guest user account is enabled, it is strongly recommended to set a password so that logon failures do not result in Guest logins (section 3.2.5.1.2). If a password is set on the Guest account, then there is a guest fallback where logons will be tried with unknown usernames against the Guest password.

*Date format: YYYY/MM/DD