[MS-NRPC]: Netlogon Remote Protocol

This topic lists the Errata found in [MS-NRPC] 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 V36.0 – 2019/09/23.

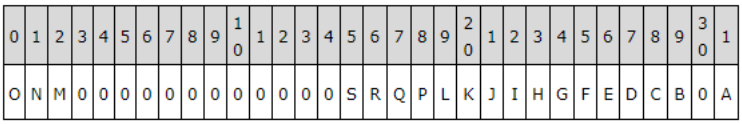
Errata Published*	Description
2020/08/17	In section 3.1.1 Abstract Data Model, added Netlogon server variable VulnerableChannelAllowList. Changed from: Implementations SHOULD<68> persistently store and retrieve the SealSecureChannel variable. Changed to: Implementations SHOULD<68> persistently store and retrieve the SealSecureChannel variable. The Netlogon server variable is as follows: VulnerableChannelAllowList: A setting expressed in Security Descriptor Description Language (SDDL) ([MS-DTYP] section 2.5.1) of Netlogon client allowed to not use secure bindings see Section 3.1.4.6.<69> <69> Section 3.1.1: VulnerableChannelAllowList is not supported by Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008. In section 3.1.4.1 Session-Key Negotiation, added session-key failure scenario in step 7. Changed from: 6. … If the comparison fails, the server MUST fail session-key negotiation without further processing of the following steps. 7. The server computes its server Netlogon credential by using the server challenge as input to the credential computation algorithm, as specified in section 3.1.4.4. … Changed to: 6. … If the comparison fails, the server MUST fail session-key negotiation without further processing of the following steps. 7. If none of the first 5 bytes of the client challenge is unique, the server MUST fail session-key negotiation without further processing of the following steps.<70> 8. The server computes its server Netlogon credential by using the server challenge as input to the credential computation algorithm, as specified in section 3.1.4.4. … <70> Section 3.1.4.1: Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008 allow the call to succeed.

Errata Published*	Description
	In section 3.1.4.2 Netlogon Negotiable Options, added in product note <73> option Y that Windows NT 4.0 SP4 does not support Secure RPC and secure bind. Changed from: Y is not supported in Windows NT prior to Windows NT 4.0 operating system Service Pack 2 (SP2). Changed to: Y is not supported in Windows NT prior to Windows NT 4.0 operating system Service Pack 2 (SP2). Windows NT 4.0 operating system Service Pack 4 (SP4) does not support Secure RPC and does not perform a secure bind. In section 3.1.4.6 Calling Methods Requiring Session-Key Establishment, Added product note for server security enforcement in earlier versions. Moved product note after MUST in step 1 to section 3.4.1.2 product note <73>. Added steps for server processing of secure bind and session-key. Changed from: The client follows this sequence of steps. The client SHOULD<72> bind to the RPC server using TCP/IP. The client and server SHOULD<73> utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([MS-RPCE] section 2.2.1.1.7) for privacy/integrity of the RPC messages. If the SealSecureChannel setting is TRUE, the client requests the Privacy authentication level from the RPC runtime. If the SealSecureChannel setting is FALSE, then the authentication level requested is Integrity. If the call to be made uses Netlogon authenticators, the client MUST compute the Netlogon authenticator to be passed as a parameter to the RPC method, as specified in section 3.1.4.5. The client calls the method on the server. If the RPC server denies access, the client attempts to re-establish the session key with the target server if the difference between the current time and value of ServerSessionInfo.LastAuthenticationTry (indexed by the name of the target server) is greater than 45 seconds. The server MUST verify the authenticator, if used, and compute the return authenticator, as specified in section 3.1.4.5. The client MUST validate the returned authenticator, if used. The client MAY unbind from the server, but it SHOULD<74> reuse the binding for multiple RPC calls. <72> Section 3.1.4.6: For Windows, the client binds to the RPC server using TCP (except for Windows NT, in which the client binds to the RPC server using the named pipe "\PIPE\NETLOGON",). If RPC returns an error indicating that the protocol sequence is not supported, the client binds to the RPC server using named pipes. <73> Section 3.1.4.6: Windows NT 4.0 operating system Service Pack 4 (SP4) does not support Secure RPC and does not perform a secure bind. Changed to: The client and server follow this sequence of steps.<74> The client SHOULD<75> bind to the RPC server using TCP/IP. The client and server MUST utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([MS-RPCE] section 2.2.1.1.7) for privacy/integrity of the RPC messages. If the SealSecureChannel setting is TRUE, the client requests the Privacy

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>authentication level from the RPC runtime. If the SealSecureChannel setting is FALSE, then the authentication level requested is Integrity.
If the call to be made uses Netlogon authenticators, the client MUST compute the Netlogon authenticator to be passed as a parameter to the RPC method, as specified in section 3.1.4.5.
The client calls the method on the server. If the RPC server denies access, the client attempts to re-establish the session key with the target server if the difference between the current time and value of ServerSessionInfo.LastAuthenticationTry (indexed by the name of the target server) is greater than 45 seconds.
If secure bind is not used, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.<76>
The server MUST verify the authenticator, if used, and compute the return authenticator, as specified in section 3.1.4.5.
If none of the first 5 bytes of the ClientStoredCredential computation result (step 1, section 3.1.4.5) is unique, the server MUST fail session-key negotiation without further processing of the following steps.<77>
The client MUST validate the returned authenticator, if used.
The client MAY unbind from the server, but it SHOULD<78> reuse the binding for multiple RPC calls.

<74> Section 3.1.4.6: Whenever a Windows 7 client or later creates a secure channel with a Windows Server 2008 server or later, the server will enforce that clients are using RPC Integrity and Confidentiality to secure the connection.
<75> Section 3.1.4.6: For Windows, the client binds to the RPC server using TCP (except for Windows NT, in which the client binds to the RPC server using the named pipe "\PIPE\NETLOGON"). If RPC returns an error indicating that the protocol sequence is not supported, the client binds to the RPC server using named pipes.
<76> Section 3.1.4.6: Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008 allow the call to succeed.
<77> Section 3.1.4.6: Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008 allow the call to succeed.</td></tr>
<tr><td>2020/05/11</td><td>In Section 2.2.1.2.1, DOMAIN_CONTROLLER_INFOW, added 'T' bit flag to indicate the DC supports Kerberos key list requests.

Changed from:

 
<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>20</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>30</td><td>1</td></tr>
<tr><td>O</td><td>N</td><td>M</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>S</td><td>R</td><td>Q</td><td>P</td><td>L</td><td>K</td><td>J</td><td>I</td><td>H</td><td>G</td><td>F</td><td>E</td><td>D</td><td>C</td><td>B</td><td>0</td><td>A</td></tr>
</table>
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>R</td><td>The DC has a functional level of DS_BEHAVIOR_WIN2012R2 or later.</td></tr>
<tr><td>S</td><td>The DC has a functional level of DS_BEHAVIOR_WIN2016 or later.</td></tr>
</table>

Changed to:</td></tr>
</table>

Errata Published*	Description

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
O	N	M	0	0	0	0	0	0	0	0	0	0	0	T	S	R	Q	P	L	K	J	I	H	G	F	E	D	C	B	0	A

Value	Description
...	...
R	The DC has a functional level of DS_BEHAVIOR_WIN2012R2 or later.
S	The DC has a functional level of DS_BEHAVIOR_WIN2016 or later.
T	The DC supports **key list requests**, as specified in [MS-KILE] section 2.2.11. If this bit is set, bit S and bit E must also be set.

*Date format: YYYY/MM/DD