[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 V38.0 – 2021/04/07.

Errata Published*	Description
2021/05/03	In Section 3.5.4.5.1 NetrLogonSamLogonEx (Opnum 39), added behavior note about message fragmentation. Changed from: On receiving this call, the server MUST perform the following validation steps: Changed to: On receiving this call, the server MUST perform the following validation steps:<195> <195> Section 3.5.4.5.1: Windows will fragment a response that exceeds the maximum fragment size even if minor version is 0. If the RPC message is fragmented, operations are done on each message fragment. In Section 3.5.4.5.3 NetrLogonSamLogon (Opnum 2), added behavior note about message fragmentation. Changed from: Message processing is identical to NetrLogonSamLogonEx, as specified in section 3.5.4.5.1, except for the following: Changed to: Message processing<205> is identical to NetrLogonSamLogonEx, as specified in section 3.5.4.5.1, except for the following: <205> Section 3.5.4.5.1: Windows will fragment a response that exceeds the maximum fragment size even if minor version is 0. If the RPC message is fragmented, operations are done on each message fragment. In Section 4.1 NetrLogonSamLogon with Secure Channel, added text to include message fragmentation with reference to the RPC standard. Changed from: 3. The client signs and encrypts the RPC message. The data is first passed to RPC, where it is formatted according to the RPC standard. . . 9. Encrypt the caller's message using the encryption key. . .

Errata Published*	Description
	5. The server verifies the signature and decrypts the RPC message. The decryption of the RPC message includes the following steps: . . . 7. Decrypt the caller's message using the encryption key. . . Changed to: 3. The client signs and encrypts the RPC message or each message fragment. If the RPC message is fragmented, operations are done on each message fragment. The data is first passed to RPC, where it is formatted according to the RPC standard ([C706], see section 12.6.2). . . 9. Encrypt the caller's message or message fragment using the encryption key. . . 5. The server verifies the signature and decrypts the RPC message or each message fragment. If the RPC message is fragmented, operations are done on each message fragment. The decryption of the RPC message includes the following steps: . . . 7. Decrypt the caller's message or message fragment using the encryption key. . .

*Date format: YYYY/MM/DD