[MS-NRPC]: Netlogon Remote Protocol

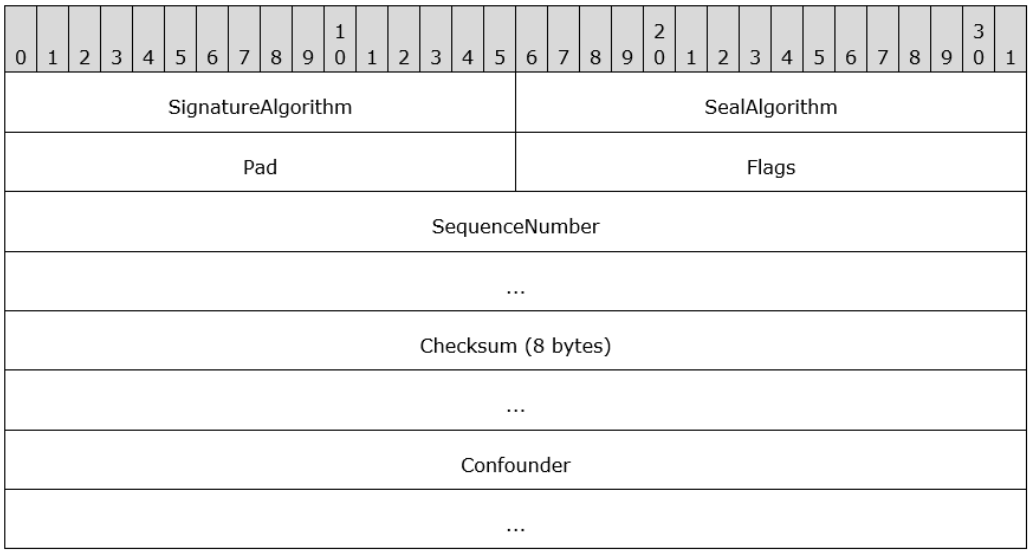
This topic lists the Errata found in [MS-NRPC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

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

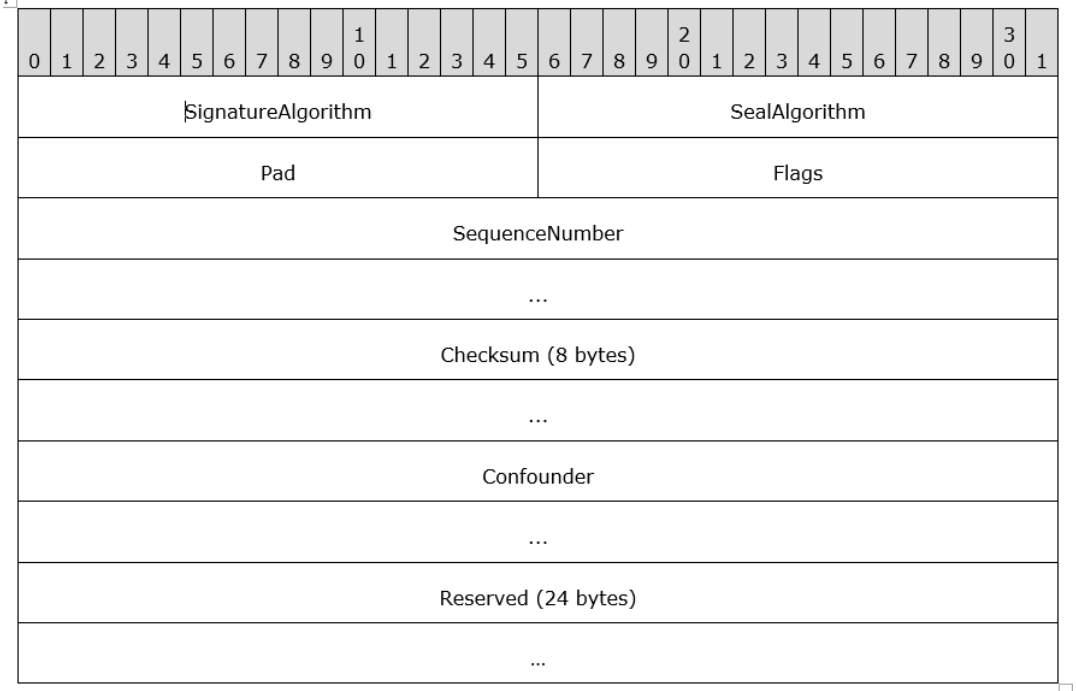
RSS
Atom

Errata below are for Protocol Document Version V35.0 – 2018/09/12.

Errata Published *	Description
2019/09/02	In Sections 2, 3, and 7 of this document, the following has been changed: 1. "NETLOGON_LOGOFF_UAS_INFORMATION" changed to "NETLOGON_LOGOFF_UAS_INFO" .(2 places) 2. "DOMAIN_NAME buffer" changed to "DOMAIN_NAME_BUFFER". 3. "ERROR_ACCESS DENIED" changed to "ERROR_ACCESS_DENIED" (3 places) 4. "ServerSession" changed to "ServerSessionInfo". 5. "DsrGetDCName" changed to "DsrGetDcName" (2 places) 6. "STATUS_NOT SUPPORTED" changed to "STATUS_NOT_SUPPORTED". 7. "NETLOGON_WORKSTATION_INFOFORMATION" in reference to WkstaBuffer changed to "NETLOGON_WORKSTATION_INFO". 8. "TrustedDomainInformation" changed to "TrustedDomainInformationEx". 9. "AllowableControlBits" changed to "AllowableAccountControlBits".
2019/04/01	In Section 2.2.1.4.5, NETLOGON_NETWORK_INFO, the definition of the Identity field has been changed from: Identity: NETLOGON_LOGON_IDENTITY_INFO structure, as specified in section 2.2.1.4.15, that contains information about the logon identity. Changed to: Identity: NETLOGON_LOGON_IDENTITY_INFO structure, as specified in section 2.2.1.4.15, that contains information about the logon identity. The Identity.LogonDomainName field MUST match the DomainName field of the authenticate message received by the client. The authenticate message is defined in [MS-NLMP] section 2.2.1.3.

Errata Published *	Description
	In Section 2.2.1.4.15, NETLOGON_LOGON_IDENTITY_INFO, the definition of the LogonDomainName field has been changed from: LogonDomainName: Contains the NetBIOS name of the domain of the account. Changed to: LogonDomainName: Contains the NetBIOS name of the domain of the account. The case of the domain name MUST be preserved across all messages.
2018/10/15	In Section 2.2.1.3.3, NL_AUTH_SHA2_SIGNATURE, a 24-byte Reserved field has been added after the Confounder field. Changed from:  … Confounder (8 bytes): A buffer that is employed when the structure is used for encryption, in addition to signing. The bytes are filled with random data that is used by the encryption algorithm. If the structure is used only for signing, the Confounder is not included. For details about the Confounder and encrypting the data, see section 3.3.4.2.1. Changed to:

Errata Published *	Description



…

Confounder (8 bytes): A buffer that is employed when the structure is used for encryption, in addition to signing. The bytes are filled with random data that is used by the encryption algorithm. If the structure is used only for signing, the Confounder is not included. For details about the Confounder and encrypting the data, see section 3.3.4.2.1.

Reserved (24 bytes): The sender SHOULD<19> set these bytes to zero, and the receiver MUST ignore them.

In Section 3.3.4.2.1, Generating a Client Netlogon Signature Token, step 7 has been updated to specify that after the signature is computed, only the first 8 bytes are copied into the Checksum field of either NL_AUTH_SHA2_SIGNATURE (if AES is negotiated) or NL_AUTH_SIGNATURE.

Changed from:

…

7. If AES is negotiated, then a signature MUST be computed using the following algorithm:

CALL SHA256Reset(&HashContext, Sk, sizeof(Sk));

…

Note: In the second call to MD5Update, only the first 8-bytes of the NL_AUTH_SIGNATURE structure are used.

After the signature is computed, the signature MUST be truncated, with only the first 8 bytes being copied into the Checksum field of NL_AUTH_SIGNATURE.

Changed to:

…

7. If AES is negotiated, then a signature MUST be computed using the following algorithm:

CALL SHA256Reset(&HashContext, Sk, sizeof(Sk));

Errata Published *	Description
	… Note: In the second call to MD5Update, only the first 8-bytes of the NL_AUTH_SIGNATURE structure are used. After the signature is computed, the signature MUST be truncated, with only the first 8 bytes being copied into the Checksum field of NL_AUTH_SHA2_SIGNATURE (section 2.2.1.3.3) if AES is negotiated, otherwise, into the Checksum field of NL_AUTH_SIGNATURE (section 2.2.1.3.2).

*Date format: YYYY/MM/DD