[MS-SAMR]: Transport

By v-pachauhan

Archived: 2026-04-05 18:34:49 UTC

This protocol configures the RPC runtime to perform a strict Network Data Representation (NDR) data consistency check at target level 5.0, as specified in [MS-RPCE] section 3.

This protocol uses UUID 12345778-1234-ABCD-EF00-0123456789AC to identify the RPC interface.

This protocol enables the ms_union extension that is specified in [MS-RPCE] section 2.2.4.

This protocol asks the RPC runtime, via the **strict_context_handle** attribute, to reject the use of context handles that are created by a method of a different RPC interface than this one, as specified in [MS-RPCE] section 3.

This protocol uses the following RPC protocol sequences:<7>

- RPC over SMB, as specified in [MS-RPCE] section 2.1.1.2.<8>

  This protocol uses the pipe name "\PIPE\samr" for the endpoint name.<9>

- RPC over TCP.<10>

  This protocol uses RPC dynamic endpoints, as specified in [C706] section 6.

This protocol MUST indicate to the RPC runtime that it is to support both the Network Data Representation (NDR) and 64-bit Network Data Representation (NDR64) transfer syntaxes and provide a negotiation mechanism for determining which RPC transfer syntax will be used, as specified in [MS-RPCE] section 3.

This protocol MUST use the UUID as specified previously. The RPC version number is 1.0.

The protocol uses the underlying RPC protocol to retrieve the identity of the client that made the method call, as specified in [MS-RPCE] section 3.3.3.4.3. The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11>

RPC clients for this protocol MUST use the authentication level RPC_C_AUTHN_LEVEL_NONE when invoking RPC over SMB methods.

The server SHOULD<12> reject calls that do not use an authentication level of either RPC_C_AUTHN_LEVEL_NONE or RPC_C_AUTHN_LEVEL_PKT_PRIVACY (see [MS-RPCE] section 2.2.1.1.8).

RPC clients for this protocol MUST use RPC over TCP/IP for the SamrValidatePassword method and MUST use RPC over SMB for the SamrSetDSRMPassword method.

RPC clients MUST use only RPC over SMB for the SamrSetInformationUser and SamrSetInformationUser2 methods when UserInformationClass is UserAllInformation, UserInternal1Information, UserInternal4Information, UserInternal4InformationNew, UserInternal5Information, UserInternal5InformationNew, UserInternal7Information, or UserInternal8Information.

For the SamrValidatePassword method, the client SHOULD use transport security to encrypt the message because the message contents contain cleartext password data. That is, the client SHOULD use an SPNEGO security provider, as specified in [MS-RPCE] section 2.2.1.1.7, and SHOULD use the packet authentication level, as specified in [MS-RPCE] section 3.3.1.5.2.<13>
