2.2.1.4.13 NETLOGON_VALIDATION_SAM_INFO4

The **NETLOGON_VALIDATION_SAM_INFO4** structure extends **NETLOGON_VALIDATION_SAM_INFO2**, as specified in section 2.2.1.4.12, by storing the fully qualified domain name (FQDN) of the domain of the user account and the user principal.

All fields of this structure, except the following fields, have the same meaning as the identically named fields in the **KERB_VALIDATION_INFO** structure, as specified in [MS-PAC] section 2.5. The following is the list of fields that are not found in [MS-PAC].

```
typedef struct _NETLOGON_VALIDATION_SAM_INFO4 {
  OLD_LARGE_INTEGER LogonTime;
  OLD_LARGE_INTEGER LogoffTime;
  OLD_LARGE_INTEGER KickOffTime;
  OLD_LARGE_INTEGER PasswordLastSet;
  OLD_LARGE_INTEGER PasswordCanChange;
  OLD_LARGE_INTEGER PasswordMustChange;
  RPC_UNICODE_STRING EffectiveName;
  RPC_UNICODE_STRING FullName;
  RPC_UNICODE_STRING LogonScript;
  RPC_UNICODE_STRING ProfilePath;
  RPC_UNICODE_STRING HomeDirectory;
  RPC_UNICODE_STRING HomeDirectoryDrive;
  unsigned short LogonCount;
  unsigned short BadPasswordCount;
  unsigned long UserId;
  unsigned long PrimaryGroupId;
  unsigned long GroupCount;
  [size_is(GroupCount)] PGROUP_MEMBERSHIP GroupIds;
  unsigned long UserFlags;
  USER_SESSION_KEY UserSessionKey;
  RPC_UNICODE_STRING LogonServer;
  RPC_UNICODE_STRING LogonDomainName;
  PRPC_SID LogonDomainId;
  unsigned long ExpansionRoom[10];
  unsigned long SidCount;
  [size_is(SidCount)] PNETLOGON_SID_AND_ATTRIBUTES ExtraSids;
  RPC_UNICODE_STRING DnsLogonDomainName;
  RPC_UNICODE_STRING Upn;
  RPC_UNICODE_STRING ExpansionString1;
  RPC_UNICODE_STRING ExpansionString2;
  RPC_UNICODE_STRING ExpansionString3;
  RPC_UNICODE_STRING ExpansionString4;
  RPC_UNICODE_STRING ExpansionString5;
  RPC_UNICODE_STRING ExpansionString6;
  RPC_UNICODE_STRING ExpansionString7;
  RPC_UNICODE_STRING ExpansionString8;
  RPC_UNICODE_STRING ExpansionString9;
  RPC_UNICODE_STRING ExpansionString10;
} NETLOGON_VALIDATION_SAM_INFO4,
 *PNETLOGON_VALIDATION_SAM_INFO4;
```

ExpansionRoom: If NTLMV1 is used, the first 8 bytes represent the LMOWF as specified in [MS-NLMP] section 3.3.1. If NTLMV2, the first 8 bytes are set to the KXKEY ([MS-NLMP] section 3.4.5.1). This MAY be set to zero.<27>

DnsLogonDomainName: Contains the fully qualified domain name (FQDN) of the domain of the user account.

Upn: Contains the **user principal name (UPN)**.

ExpansionString1: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString2: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString3: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString4: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString5: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString6: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString7: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString8: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString9: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

ExpansionString10: MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section 1.3.8.1.3.

<27> Section 2.2.1.4.13: There is a security issue with ExpansionRoom. If the data in this field is known, the password can be generated. Because of this, it is recommended for implementers that this field be zero-filled.