2.5 KERB_VALIDATION_INFO

The **KERB_VALIDATION_INFO** structure defines the user's logon and authorization information provided by the DC. A pointer to the **KERB_VALIDATION_INFO** structure is serialized into an array of bytes and then placed after the **Buffers** array of the topmost **PACTYPE** structure (section 2.3), at the offset specified in the **Offset** field of the corresponding **PAC_INFO_BUFFER** structure (section 2.4) in the **Buffers** array. The **ulType** field of the corresponding **PAC_INFO_BUFFER** structure is set to 0x00000001.

The **KERB_VALIDATION_INFO** structure is a subset of the **NETLOGON_VALIDATION_SAM_INFO4** structure ([MS-NRPC] section 2.2.1.4.13). It is a subset due to historical reasons and to the use of the common Active Directory to generate this information. NTLM uses the **NETLOGON_VALIDATION_SAM_INFO4** structure in the context of the server to domain controller exchange, as described in [MS-APDS] section 3.1. Consequently, the **KERB_VALIDATION_INFO** structure includes NTLM-specific fields. Fields that are common to the **KERB_VALIDATION_INFO** and the **NETLOGON_VALIDATION_SAM_INFO4** structures, and which are specific to the NTLM authentication operation, are not used with [MS-KILE] authentication.

The **KERB_VALIDATION_INFO** structure is marshaled by RPC [MS-RPCE].

The **KERB_VALIDATION_INFO** structure is defined as follows:

```
typedef struct {
  FILETIME LogonTime;
  FILETIME LogoffTime;
  FILETIME KickOffTime;
  FILETIME PasswordLastSet;
  FILETIME PasswordCanChange;
  FILETIME 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;
  USHORT LogonCount;
  USHORT BadPasswordCount;
  ULONG UserId;
  ULONG PrimaryGroupId;
  ULONG GroupCount;
  [size_is(GroupCount)] PGROUP_MEMBERSHIP GroupIds;
  ULONG UserFlags;
  UCHAR UserSessionKey[16];
  RPC_UNICODE_STRING LogonServer;
  RPC_UNICODE_STRING LogonDomainName;
  PSID LogonDomainId;
  ULONG Reserved1[2];
  ULONG UserAccountControl;
  ULONG Reserved3[7];
  ULONG SidCount;
  [size_is(SidCount)] PKERB_SID_AND_ATTRIBUTES ExtraSids;
  PSID ResourceGroupDomainSid;
  ULONG ResourceGroupCount;
  [size_is(ResourceGroupCount)] PGROUP_MEMBERSHIP ResourceGroupIds;
} KERB_VALIDATION_INFO;
```

LogonTime: A **FILETIME** structure that contains the user account's lastLogonTimestamp attribute ([MS-ADA1] section 2.352) value for interactive logon and SHOULD be zero for network logon.

LogoffTime: A **FILETIME** structure that contains the time the client's logon session should expire. If the session should not expire, this structure SHOULD have the **dwHighDateTime** member set to 0x7FFFFFFF and the **dwLowDateTime** member set to 0xFFFFFFFF. A recipient of the PAC SHOULD<3> use this value as an indicator of when to warn the user that the allowed time is due to expire.

KickOffTime: A **FILETIME** structure that contains **LogoffTime** minus the user account's forceLogoff attribute ([MS-ADA1] section 2.233) value. If the client should not be logged off, this structure SHOULD have the **dwHighDateTime** member set to 0x7FFFFFFF and the **dwLowDateTime** member set to 0xFFFFFFFF. The Kerberos service ticket end time is a replacement for **KickOffTime**. The service ticket lifetime SHOULD NOT be set longer than the **KickOffTime** of an account. A recipient of the PAC SHOULD<4> use this value as the indicator of when the client should be forcibly disconnected.

PasswordLastSet: A **FILETIME** structure that contains the user account's pwdLastSet attribute ([MS-ADA3] section 2.174) value for interactive logon and SHOULD be zero for network logon . If the password was never set, this structure MUST have the **dwHighDateTime** member set to 0x00000000 and the **dwLowDateTime** member set to 0x00000000.

PasswordCanChange: A **FILETIME** structure that contains the time at which the client's password is allowed to change for interactive logon and SHOULD be zero for network logon. If there is no restriction on when the client may change the password, this member MUST be set to zero.

PasswordMustChange: A **FILETIME** structure that contains the time at which the client's password expires for interactive logon and SHOULD be zero for network logon. If the password will not expire, this structure MUST have the **dwHighDateTime** member set to 0x7FFFFFFF and the **dwLowDateTime** member set to 0xFFFFFFFF.

EffectiveName: A **RPC_UNICODE_STRING** structure that contains the user account's samAccountName attribute ([MS-ADA3] section 2.221) value for interactive logon and SHOULD be zero for network logon.

FullName: A **RPC_UNICODE_STRING** structure that contains the user account's full name for interactive logon and SHOULD be zero for network logon. If **FullName** is omitted, this member MUST contain a **RPC_UNICODE_STRING** structure with the Length member set to zero.

LogonScript: A **RPC_UNICODE_STRING** structure that contains the user account's scriptPath attribute ([MS-ADA3] section 2.231) value for interactive logon and SHOULD be zero for network logon. If no **LogonScript** is configured for the user, this member MUST contain a **RPC_UNICODE_STRING** structure with the Length member set to zero.

ProfilePath: A **RPC_UNICODE_STRING** structure that contains the user account's

profilePath attribute ([MS-ADA3] section 2.166) value for interactive logon and SHOULD be zero for network logon. If no **ProfilePath** is configured for the user, this member MUST contain a **RPC_UNICODE_STRING** structure with the Length member set to zero.

HomeDirectory: A **RPC_UNICODE_STRING** structure that contains the user account's HomeDirectory attribute ([MS-ADA1] section 2.295) value for interactive logon and SHOULD be zero for network logon. If no **HomeDirectory** is configured for the user, this member MUST contain a **RPC_UNICODE_STRING** structure with the Length member set to zero.

HomeDirectoryDrive: A **RPC_UNICODE_STRING** structure that contains the user account's HomeDrive attribute ([MS-ADA1] section 2.296) value for interactive logon and SHOULD be zero for network logon . This member MUST be populated if **HomeDirectory** contains a **UNC path**. If no **HomeDirectoryDrive** is configured for the user, this member MUST contain a **RPC_UNICODE_STRING** structure with the **Length** member set to zero.

LogonCount: A 16-bit unsigned integer that contains the user account's **LogonCount** attribute ([MS-ADA1] section 2.375) value.

BadPasswordCount: A 16-bit unsigned integer that contains the user account's badPwdCount attribute ([MS-ADA1] section 2.83) value for interactive logon and SHOULD be zero for network logon t.

UserId: A 32-bit unsigned integer that contains the RID of the account. If the UserId member equals 0x00000000, the first group SID in this member is the SID for this account

PrimaryGroupId: A 32-bit unsigned integer that contains the RID for the primary group to which this account belongs.

GroupCount: A 32-bit unsigned integer that contains the number of groups within the account domain to which the account belongs.

GroupIds: A pointer to a list of GROUP_MEMBERSHIP (section 2.2.2) structures that contains the groups to which the account belongs in the account domain. The number of groups in this list MUST be equal to **GroupCount**.

UserFlags: A 32-bit unsigned integer that contains a set of bit flags that describe the user’s logon information.

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
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	L	K	J	I	H	G	F	E	D	0	C	0	B	A

The following flags are set only when this structure is created as the result of an NTLM authentication, as specified in [MS-NLMP]. These flags MUST be zero for any other authentication protocol, such as MS-KILE authentication.

Value	Description
A	Authentication was done via the GUEST account; no password was used.
B	No encryption is available.
C	LAN Manager key was used for authentication.
E	Sub-authentication used; session key came from the sub-authentication package.
F	Indicates that the account is a machine account.
G	Indicates that the domain controller understands NTLMv2.
I	Profile path was returned.
J	The NTLMv2 response from the **NtChallengeResponseFields** ([MS-NLMP] Section 2.2.1.3) was used for authentication and session key generation.
K	The LMv2 response from the **LmChallengeResponseFields** ([MS-NLMP] Section 2.2.1.3)was used for authentication and session key generation.
L	The LMv2 response from the **LmChallengeResponseFields** ([MS-NLMP] Section 2.2.1.3)was used for authentication and the NTLMv2 response from the **NtChallengeResponseFields** ([MS-NLMP] Section 2.2.1.3) was used session key generation.

The following flags are valid for MS-KILE authentications; settings depend on the configuration of the user and groups referenced in the PAC.

Value	Description
D	Indicates that the **ExtraSids** field is populated and contains additional SIDs.
H	Indicates that the **ResourceGroupIds** field is populated.

All other bits MUST be set to zero and MUST be ignored on receipt.

UserSessionKey: A session key that is used for cryptographic operations on a session. This field is valid only when authentication is performed using NTLM. For any other protocol, this field MUST be zero.

LogonServer: A **RPC_UNICODE_STRING** structure that contains the NetBIOS name of the Kerberos KDC that performed the authentication server (AS) ticket request.

LogonDomainName: A **RPC_UNICODE_STRING** structure that contains the NetBIOS name of the domain to which this account belongs.

LogonDomainId: A SID structure that contains the SID for the domain specified in **LogonDomainName**. This member is used in conjunction with the **UserId**, **PrimaryGroupId**, and **GroupIds** members to create the user and group SIDs for the client.

Reserved1: A two-element array of unsigned 32-bit integers. This member is reserved, and each element of the array MUST be equal to 0x00000000 and MUST be ignored on receipt.

UserAccountControl: A 32-bit unsigned integer that contains a set of bit flags that represent information about this account. This field carries the **UserAccountControl** information from the corresponding **Security Account Manager** field, as specified in [MS-SAMR].

Reserved3: A seven-element array of unsigned 32-bit integers. This member is reserved, and each element of the array MUST be equal to 0x00000000 and MUST be ignored on receipt.

SidCount: A 32-bit unsigned integer that contains the total number of SIDs present in the **ExtraSids** member. If this member is not zero then the 0x20 bit MUST be set in the **UserFlags** member.

ExtraSids: A pointer to a list of KERB_SID_AND_ATTRIBUTES (section 2.2.1) structures that contain a list of SIDs corresponding to groups in domains other than the account domain to which the principal belongs. This member is not NULL only if the 0x20 bit has been set in the **UserFlags** member. If the **UserId** member equals 0x00000000, the first group SID in this member is the SID for this account.

ResourceGroupDomainSid: A SID structure that contains the SID of the domain for the server whose resources the client is authenticating to. This member is used in conjunction with the **ResourceGroupIds** member to create the group SIDs for the user. If this member is populated, then the 0x200 bit MUST be set in the **UserFlags** member.

When this field is not used; it MUST be set to NULL.

ResourceGroupCount: A 32-bit unsigned integer that contains the number of resource group identifiers stored in **ResourceGroupIds**. If this member is not zero, then the 0x200 bit MUST be set in the **UserFlags** member.

When this field is not used; it MUST be set to zero.

ResourceGroupIds: A pointer to a list of **GROUP_MEMBERSHIP** structures that contain the RIDs and attributes of the account's groups in the resource domain. If this member is not NULL, then the 0x200 bit MUST be set in the **UserFlags** member.

When this field is not used; it MUST be set to NULL.