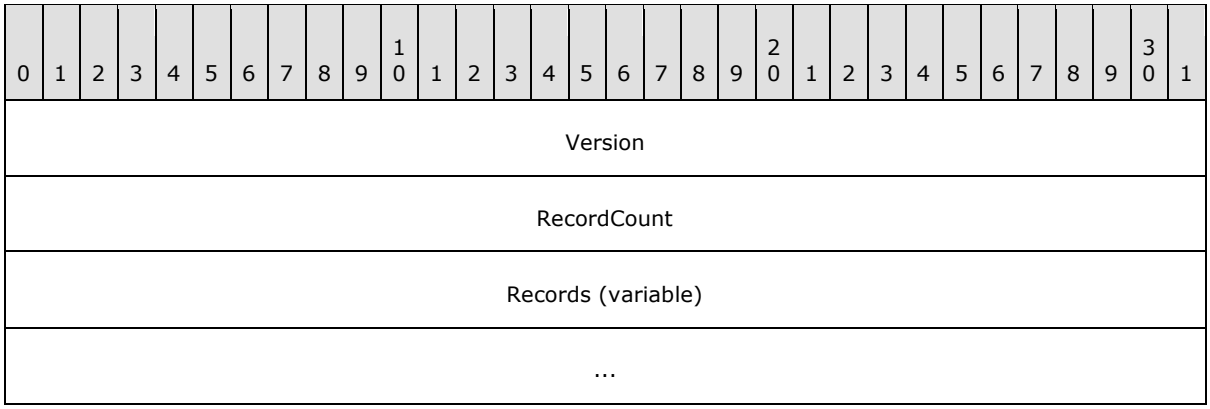
7.1.6.9.3 msDS-TrustForestTrustInfo Attribute

Information about trust relationships with other forests is stored in objects of class trustedDomain in the **domain** NC replica of the forest root **domain**. Specifically, the msDS-TrustForestTrustInfo attribute on such objects contains information about the trusted forest or realm. The structure of the information contained in this attribute is represented in the following manner.



Version (4 bytes): Version of the data structure. The only supported version of the data structure is 1.

RecordCount (4 bytes): Number of records present in the data structure.

Records (variable): Variable-length records each containing a specific type of data about the forest trust relationship.

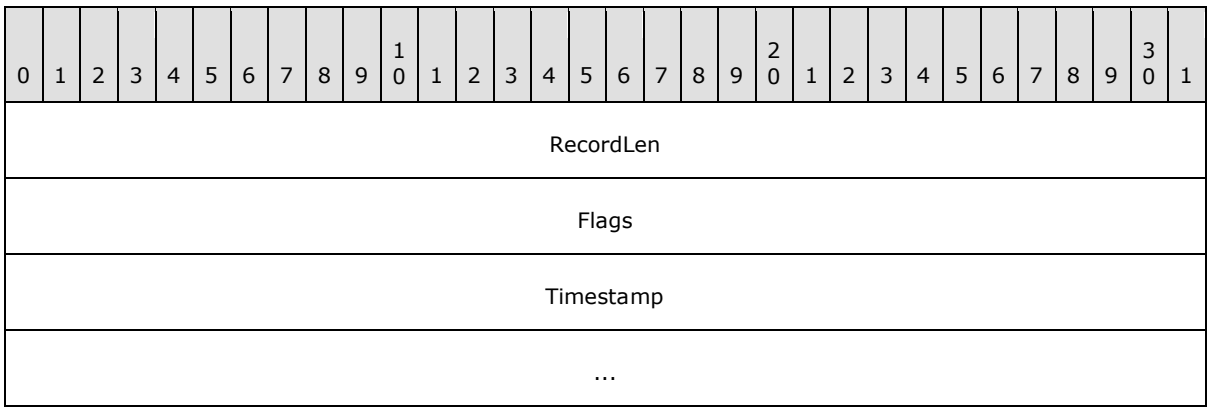
IMPORTANT NOTE: Records are not aligned to 32-bit boundaries. Each record starts at the next byte after the previous record ends.

Each record is represented as described in section 7.1.6.9.3.1 .

Note All fields have little-endian byte ordering.

7.1.6.9.3.1 Record

Each Record is represented in the following manner.



RecordType	ForestTrustData (variable)
…	

RecordLen (4 bytes): Length, in bytes, of the entire record.

Flags (4 bytes): Individual bit flags that control how the forest trust information in this record can be used.

If RecordType = 0 or 1, the Flags field, represented here in little-endian byte order, can have one or more of the following bits.

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
X	X	X	X	X	TDC	TDA	TDN	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

X: Unused. Must be zero and ignored.

TDN (LSA_TLN_DISABLED_NEW): Entry is not yet enabled.

TDA (LSA_TLN_DISABLED_ADMIN): Entry is disabled by administrator.

TDC (LSA_TLN_DISABLED_CONFLICT): Entry is disabled due to a conflict with another trusted domain.

If RecordType = 2, the Flags field, represented here in little-endian byte order, can have one or more of the following bits.

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
X	X	X	X	NDC	NDA	SDC	SDA	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

SDA (LSA_SID_DISABLED_ADMIN): Entry is disabled for SID, NetBIOS, and DNS name–based matches by the administrator.

SDC (LSA_SID_DISABLED_CONFLICT): Entry is disabled for SID, NetBIOS, and DNS name–based matches due to a SID or DNS name–based conflict with another trusted domain.

NDA (LSA_NB_DISABLED_ADMIN): Entry is disabled for NetBIOS name–based matches by the administrator.

NDC (LSA_NB_DISABLED_CONFLICT): Entry is disabled for NetBIOS name–based matches due to a NetBIOS domain name conflict with another trusted domain.

For RecordType = 2, NETBIOS_DISABLED_MASK is defined as a mask on the lower 4 bits of the Flags field.

For all record types, LSA_FTRECORD_DISABLED_REASONS is defined as a mask on the lower 16 bits of the Flags field. Unused bits covered by the mask are reserved for future use.

Timestamp (8 bytes): 64-bit timestamp value indicating when this entry was created, in system time (see the **FILETIME** structure in [MS-DTYP] section 2.3.1).

RecordType (1 byte): 8-bit value specifying the type of record contained in this specific entry. The structure of the content in the next field depends on this value. The allowed values for this field are specified by the following enumerated list.

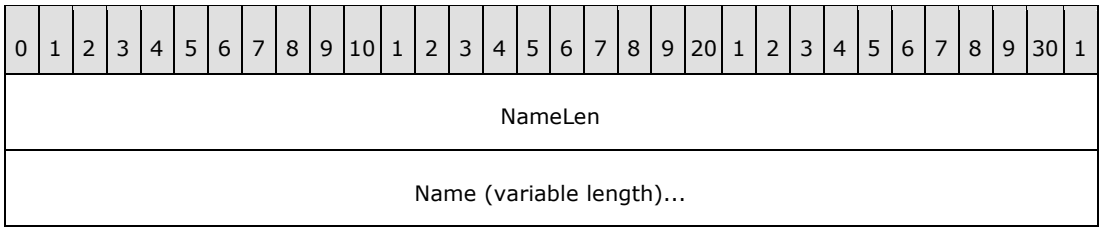
Name	Value
ForestTrustTopLevelName	0
ForestTrustTopLevelNameEx	1
ForestTrustDomainInfo	2

ForestTrustData (variable): Variable-length type-specific record, depending on the RecordType value, containing a specific type of data about the forest trust relationship.

IMPORTANT NOTE: The type-specific ForestTrustData record is not necessarily aligned to a 32-bit boundary. Each record starts at the byte following the RecordType field.

There are three different type-specific records. Depending on the value of the RecordType field, the structure of the type-specific record differs as follows:

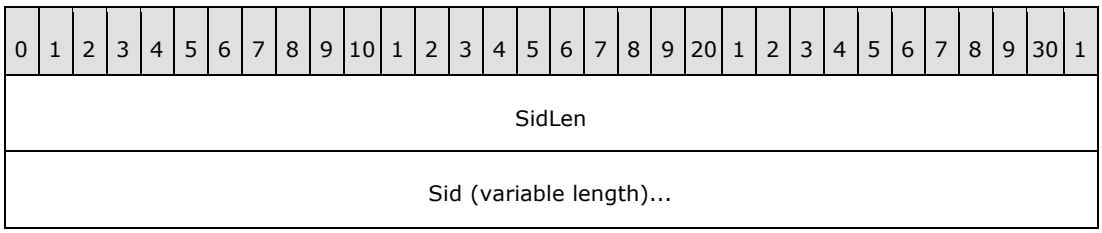
- If RecordType = 0 or RecordType = 1, then the type-specific record is represented in the following manner.



NameLen: Length, in bytes, of the following Name field.

Name: The **top level name** of the trusted forest, in UTF-8 format.

- If RecordType = 2, then the type-specific record is represented in the following manner. Note that the record contains the following structures one after another. It is important to note here that none of the data shown is necessarily aligned to 32-bit boundaries.



DnsNameLen
DnsName (variable length)...
NetbiosNameLen
NetbiosName (variable length)...

SidLen: Length, in bytes, of the following Sid field.

Sid: The SID of a domain in the trusted forest, specified as a SID structure, which is defined in [MS-DTYP] section 2.4.2.

DnsNameLen: Length, in bytes, of the following DnsName field.

DnsName: The DNS name of a domain in the trusted forest, in UTF-8 format.

NetbiosNameLen: Length, in bytes, of the following NetbiosName field.

NetbiosName: The NetBIOS name of a domain in the trusted forest, in UTF-8 format.

- If RecordType is not one of the preceding values, then the type-specific record is represented in the following manner.

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
BinaryDataLen																															
BinaryData (variable length)...																															

BinarydataLen: Length, in bytes, of the following BinaryData field.

BinaryData: Trusted forest data.

7.1.6.9.3.2 Building Well-Formed msDS-TrustForestTrustInfo Messages

The msDS-TrustForestTrustInfo attribute contains a String(Octet) with the data structures specified in the preceding sections. This attribute contains information about the namespaces that are served by a given trusted forest. For example, if forest a.com contains the domains a.com, b.a.com, and c.a.com, then the msDS-TrustForestTrustInfo for a.com would contain the FQDN and NetBIOS names for each domain, as well as the SID space served by each domain. This section details the rules that well-formed msDS-TrustForestTrustInfo messages must follow.

The msDS-TrustForestTrustInfo attribute is written on the PDC for the trusting and trusted domains. Both the trusted and trusting forest have forest functional level DS_BEHAVIOR_WIN2003 or greater.

Some concepts are necessary to understand the algorithm that is used when validating this attribute.

Namespaces

Namespaces are meant to represent those NetBIOS, FQDN, or SID values that a trusted forest or domain claims.

Top Level Names (TLNs)

TLNs are an important concept when detecting and resolving conflicts in namespaces between different TDOs, and for providing hints about which forest owns a given namespace. A TLN really corresponds to a forest namespace, and in order to be enabled, the TLN must be unique among all TDOs. For example, the TLN for the forest example.com is example.com. Note that it is possible that the forest example.com could have another domain corresponding to an entirely different TLN (for example, mailservers.com), in which case two TLNs would need to be registered for the example.com forest. TLNs for a TDO are stored in records identified by the ForestTrustTopLevelName Record Type.

TLNs that must be excluded from a namespace are identified by the ForestTrustTopLevelNameEx RecordType. Exclusion becomes necessary if the namespaces of two forests collide (for example, the forests corp.mycompany.com and the forest hr.corp.mycompany.com). These exclusions are set administratively to ensure proper functioning of the domain.

Superior/Subordinate Namespaces

When evaluating all forest trusts, TLNs are expressed as FQDNs. Parsing the FQDN allows the concept of superior and subordinate namespaces. For example, for the namespace sample.example.com, the superior namespace (and the TLN) is example.com. Similarly, the sample.example.com namespace is subordinate to the example.com namespace. This allows the routing mechanism to understand that the name sample.example.com is associated with the example.com namespace expressed in the TLN, as it is a subordinate.

Enabled Records vs. Disabled Records

During validation of the Records stored in the msDS-ForestTrustForestInfo, it is possible to have TLN or namespace conflicts. In these circumstances, the conflicting record is disabled. Namespace conflicts are determined using the Record Flags specified in the msDS-ForestTrustInfo data format definitions.

1. ForestTrustTopLevelName RecordType (0)

   If the TDN / TDA / TDC Flags are present, then the name that is present in the TLN and its subordinate namespaces (as well as all domains whose FQDNs are equal to or subordinate to the TLN) is not used for routing names or SIDs.

2. ForestTrustTopLevelNameEx RecordType (1)

   If the TDN / TDA / TDC Flags are present, then the name that is present in the exclusion TLN is not used for exclusion purposes, and conflicts will be unresolved. All domains whose FQDNs are equal to or subordinate to the exclusion TLN are not used for routing names or SIDs.

3. ForestTrustDomainInfo RecordType (2)

   If the NDC or NDA Flags are set, then the NetBIOS name is excluded from routing for the NetBIOS name.

   If the SDA or SDC Flags are set, then the entire domain and all domains whose FQDN names are subordinate to the FQDN name of that domain are excluded from name routing by SID, FQDN, or NetBIOS names. The entire subtree of the forest that is rooted at the affected domain is effectively not computed in the trust domain name mappings.

msDS-TrustForestTrustInfo Validation

When the TDO information for a domain is added or changed, or if the DC possessing the PDC FSMO role in the root domain of the forest is freshly started, every TDO with msDS-ForestTrustInfo attributes is validated against all other TDOs. The results of that validation are then rewritten to the DS and replicated to the other DCs in the domain. DCs that do not own the PDC FSMO role treat the attribute as READONLY and internally consistent.

Validation of the matrix of trusted domains and trusted forest information stored in msDS-ForestTrustInfo includes a mechanism to prevent name collisions. Manipulations of this attribute ensure that each namespace is only assigned to a single TDO. If any of the following rules are violated, the colliding RecordFlag is marked as disabled.

The rules for determining whether namespaces collide for ForestTrustDomainInfo Records are as follows:

1. Each SID corresponding to a domain in a trusted forest is unique among all TDOs and among all of the SIDs listed within the ForestTrustData Records. If not, the Record MUST have the SDC bit in the Record Flags.

2. Each SID for each domain in a trusted forest does not equal any SIDs within the domains of the local forest. If not, the Record MUST have the SDC bit in the Record Flags.

3. Each FQDN corresponding to a domain in a trusted forest is unique among all TDOs and among all of the FQDNs and TLNs listed within the ForestTrustData Records. If not, the Record MUST have the SDC bit in the Record Flags.

4. Each FQDN for each domain in the trusted forest does not correspond to any FQDNs within the domains from the local forest. If not, the Record MUST have the SDC bit in the Record Flags.

5. Each NetBIOS domain name corresponding to a domain in a trusted forest is unique among all TDOs and among all of the NetBIOS domains listed within the Forest Trust Data records. If not, the Record MUST have the NDC bit in the Record Flags. For conflict resolution, the TDO with the alphabetically longest name is disabled.

6. Each NetBIOS name for each domain in the trusted forest does not equal any NetBIOS domain name within the domains of the local forest. If not, the Record MUST have the NDC bit in the Record Flags. Local forest NetBIOS names always take precedence over those of trusted forests.

The rules for determining whether namespaces collide for ForestTrustTopLevelName Records are as follows:

1. Each TLN corresponding to a domain in a trusted forest is unique among all TDOs, and among all of the FQDNs and TLNs listed within the Forest Trust Data records. If not, the conflicting Record has the TDC bit in the Record Flags. For the sake of consistency, since the two TLNs are equal, the first TLN Record that is read is authoritative, and subsequent conflicting Records are disabled.

2. Each TLN for each domain in the trusted forest does not correspond to any FQDNs within the domains from the local forest. If not, the Record has the TDC bit in the Record Flags.

ForestTrustTopLevelNameEx Records, by definition, cannot conflict.

Additionally, additions to msDS-TrustForestTrustInfo pass namespace consistency checks before the attribute is set. Any failures in the consistency checks cause the attempt to modify the msDS-TrustForestTrustInfo to fail. The following rules dictate the requirements that each trusted forest must match:

1. At least one ForestTrustTopLevelName TLN Record is specified for each msDS-TrustForestTrustInfo. It is possible for a forest to have more than one TLN if it contains additional TLNs.

2. All domains listed in the ForestTrustDomainInfo for a TDO are subordinate to the TLNs for that TDO.

3. All domains listed in the ForestTrustDomainInfo are not subordinate or superior to other TLNs unless an exclusion record for that TLN or domain is registered.

If all of the preceding tests pass, then the entry is written in binary format to the msDS-ForestTrustInfo, replicated, and honored by all DCs in the forest.