[MS-KILE]: Kerberos Protocol Extensions

This topic lists the Errata found in [MS-KILE] 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 V31.0 – 2015/10/16.

Errata Published*	Description
2016/06/13	In two sections, updated text to indicate that KILE key version numbers are encoded and decoded as signed 32-bit integers. In Section 3.1.1, Abstract Data Model, removed the following line: KILE key version numbers (as defined in [RFC4120] section 5.2.9) are signed 32-bit integers. In Section 3.1.5.8, Key Version Numbers, changed from: KILE key version numbers (as defined in [RFC4120] section 5.2.9) are unsigned 32-bit integers. Changed to: KILE key version numbers (as defined in [RFC4120] section 5.2.9) are encoded and decoded as signed 32-bit integers.
2016/01/25	In Section 3.3.5.5, Determining Authentication Policy Setting, the Boolean value for the inspection of the BelongsToSilo field when the accound does not belong to a Silo was revised from TRUE to FALSE. Changed from: ▪ If the account does not belong to a Silo (BelongsToSilo == TRUE (section 3.3.5.4)) and AssignedPolicy (section 3.3.1.1) is NULL, the KDC SHOULD set PolicyName to NULL and Enforced to FALSE. ▪ If the account does not belong to a Silo (BelongsToSilo == TRUE (section 3.3.5.4)) and the AssignedPolicy is not NULL, the KDC SHOULD set PolicyName to AssignedPolicy.RDN, Enforced to AssignedPolicy.msDS-AuthNPolicyEnforced, and when the account is of type: Changed to: ▪ If the account does not belong to a Silo (BelongsToSilo == FALSE (section 3.3.5.4)) and AssignedPolicy (section 3.3.1.1) is NULL, the KDC SHOULD set PolicyName to NULL and Enforced to FALSE. ▪ If the account does not belong to a Silo (BelongsToSilo == FALSE (section 3.3.5.4)) and the AssignedPolicy is not NULL, the KDC SHOULD set PolicyName to AssignedPolicy.RDN, Enforced to AssignedPolicy.msDS-AuthNPolicyEnforced, and when the account is of type:
2016/01/25	In an existing section, added the sAMAccountName attribute to the user schema class and added two new sections for Server Principal Lookup and Client Principal Lookup.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
In Section 2.3, Directory Service Schema Elements, changed from:
<table>
<tr><th>Class</th><th>Attribute</th></tr>
<tr><td>trustedDomain</td><td>msDS-SupportedEncryptionTypes</td></tr>
<tr><td>user</td><td>logonHours
msDS-SupportedEncryptionTypes
servicePrincipalName
userAccountControl
userPrincipalName</td></tr>
</table>
Changed to:
<table>
<tr><th>Class</th><th>Attribute</th></tr>
<tr><td>trustedDomain</td><td>msDS-SupportedEncryptionTypes</td></tr>
<tr><td>user</td><td>logonHours
msDS-SupportedEncryptionTypes
servicePrincipalName
userAccountControl
userPrincipalName
sAMAccountName</td></tr>
</table>
Added new Section 3.3.5.1.1, Server Principal Lookup, and new Section 3.3.5.6.1, Client Principal Lookup.

3.3.5.1.1 Server Principal Lookup
This section is relevant only for KILE implementations that use Active Directory for the account database.
Note Some of the data types in the following procedures are defined in [RFC4120] section 5.2.
If the Name Type ([RFC4120] section 6.2) is NT-PRINCIPAL, NT-SRV-HST, or NT-SRV-INST, then the KDC SHOULD:

1. If the KerberosString[0] element of name-string of the PrincipalName is "krbtgt" and there are only two KerberosString elements in name-string, then call GetUserLogonInfoByAttribute ([MS-ADTS] section 3.1.1.13.6) where:
▪ SearchKey is set to KerberosString[1].
▪ Attribute is set to the sAMAccountName attribute ([MS-ADA3] section 2.222).

2. Otherwise:
1. Call GetUserLogonInfoByAttribute where:
▪ SearchKey is set to KerberosString[0] + "/" + the concatenation of the remaining KerberosString elements in order.
▪ Attribute is set to the userPrincipalName attribute ([MS-ADA3] section 2.349).
</td></tr>
</table>

Errata Published*	Description
	2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([MS-ERREF] section 2.3.1) and there is only one KerberosString element in name-string, then: 1. Call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to KerberosString[0]. ▪ *Attribute* is set to **sAMAccountName**. 2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to KerberosString[0] + "$". ▪ *Attribute* is set to **sAMAccountName**. 3. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then the KDC MUST return KDC_ERR_S_PRINCIPAL_UNKNOWN ([RFC4120] section 7.5.9). If the Name Type ([RFC4120] section 6.2) is NT-ENTERPRISE, then the KDC SHOULD: 1. Set local variable *UPNServerName* to the contents of the **sname** field of the request before the @ character. 2. If there is only one KerberosString element in name-string, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to KerberosString[0]. ▪ *Attribute* is set to the **servicePrincipalName** element. 3. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNServerName*. ▪ *Attribute* is set to **sAMAccountName**. 4. If ERROR_SUCCESS is returned and the account has no SPNs registered, then the KDC MUST return KDC_ERR_S_PRINCIPAL_UNKNOWN. 5. Or if STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNServerName* + "$". ▪ *Attribute* is set to **sAMAccountName**. 6. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then the KDC MUST return KDC_ERR_S_PRINCIPAL_UNKNOWN. In all cases, if the call succeeds, the Active Directory account for the requested principal was found. **3.3.5.6.1 Client Principal Lookup** This section is relevant only for KILE implementations that use Active Directory for the account database. If the Name Type ([RFC4120] Section 6.2) is NT-PRINCIPAL, then the KDC SHOULD:

Errata Published*	Description
	1. If the **realm** field is not present in the request or is the DC's domain name, call GetUserLogonInfoByAttribute ([MS-ADTS] section 3.1.1.13.6) where: ▪ *SearchKey* is set to the **cname** field of the request. ▪ *Attribute* is set to the **sAMAccountName** attribute ([MS-ADA3] section 2.222). 2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([MS-ERREF] section 2.3.1), then if **realm** is not present or is the DC's domain name, call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to **cname** + "$". ▪ *Attribute* is set to **sAMAccountName**. 3. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByUPNOrAccountName ([MS-ADTS] section 3.1.1.13.7) where *UPNOrName* is set to: ▪ If **realm** is present, cname@realm. ▪ Otherwise, cname@DC's domain name. 4. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and: ▪ If no preauthentication data was provided, then call IDL_DRSCrackNames ([MS-DRSR] section 4.1.4) where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME_AND_ALTSECID. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to: ▪ If **realm** is present, cname@realm. ▪ Otherwise, cname@DC's domain name. ▪ If preauthentication data was provided, then call IDL_DRSCrackNames where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to: ▪ If **realm** is present, cname@realm. ▪ Otherwise, cname@DC's domain name.

Errata Published*	Description
	5. If DS_NAME_ERROR_NOT_FOUND is returned ([MS-DRSR] section 4.1.4.1.8), then the KDC MUST return KDC_ERR_C_PRINCIPAL_UNKNOWN ([RFC4120] section 7.5.9). If the Name Type is NT-ENTERPRISE, then the KDC SHOULD: 1. Set local variable *UPNClientName* to the contents of **cname** before the @ character. 2. Set local variable *UPNDomainName* to the contents of **cname** after the @ character. 3. Call GetUserLogonInfoByUPNOrAccountName where *UPNOrName* is set to **cname**. 4. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and *UPNDomainName* is the same as the DC's domain name, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNClientName*. ▪ *Attribute* is set to **sAMAccountName**. 5. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and *UPNDomainName* is the same as the DC's domain name, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNClientName* + "$". ▪ *Attribute* is set to **sAMAccountName**. 6. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and: ▪ If no preauthentication data was provided, then call IDL_DRSCrackNames where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME_AND_ALTSECID. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to **cname**. ▪ If preauthentication data was provided, then call IDL_DRSCrackNames where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to **cname**. 7. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then the KDC MUST return KDC_ERR_C_PRINCIPAL_UNKNOWN.

Errata Published*	Description
	In all cases, if the call succeeds, the Active Directory account for the requested principal was found.

* Date format: YYYY/MM/DD