3.1.1.2 Cryptographic Material

Kerberos V5 establishes a secret key that is shared by a principal and the KDC and a session key that forms the basis for privacy or integrity in the communication channel between client and server. When KILE creates an AES128 key, the password MUST be converted from a Unicode (UTF16) string to a UTF8 string ([UNICODE], chapter 3.9). KILE concatenates the following information to use as the key salt for principals:

- User accounts when provided UPN (A@B): <all upper case DNS name of the realm> | <A with "/" stripped off>
- User accounts when not provided UPN: <all upper case DNS of the realm> | <user name>
- Computer accounts: <all upper case DNS name of the realm> | "host" | <all lower case computer name with "$" stripped off> | "." | <all lower case DNS name of the realm >

Using KILE, application clients (for example, CIFS/SMB clients) MAY use the negotiated key directly. When an application client uses the session key, the application protocol MUST document the explicit use of the key in its protocol specification. The key MAY be exported as an attribute of the completed security context in the **SSPI** API.

The subkey in the **EncAPRepPart** of the KRB_AP_REP message SHOULD be used as the session key when mutual authentication is requested. (The KRB_AP_REP message and its fields are defined in section 5.5.2 of [RFC4120].) When DES and RC4 are used, the implementation is as described in [RFC1964]. With DES and RC4, the subkey in the KRB_AP_REQ message can be used as the session key, as it is the same as the subkey in KRB_AP_REP message; however when AES is used (see [RFC4121]), the subkeys are different and the subkey in the KRB_AP_REP SHOULD be used. (The KRB_AP_REQ message is defined in section 5.5.1 of [RFC4120]).

3.3.1.1 Account Database Extensions

The Kerberos V5 protocol specifies that KDCs MUST maintain a database of principals and their secret keys.

To support all functionality of KILE, the account database MUST be extended to support the following additional information for each principal:

- Group membership: The account database MUST be extended to support groups to support PAC generation. For more information, see section 3.3.5.3.2 and section 3.3.5.4.2.
- Realms or domains: The account database MUST have a larger database of accounts and their realms or domains to support referrals. For more information, see section 3.3.5.3.1.
- Services allowed to send forwarded tickets to: The account database MUST be extended to support the list of services to which a service can forward tickets to support constrained delegation. For more information, see section 3.3.5.4.4. KILE implementations which use an AD for the configuration database SHOULD use the **msDS-AllowedToDelegateTo** attribute ([MS-ADA2] section 2.182).

KILE implementations which use an AD for the account database SHOULD use the **userAccountControl** attribute ([MS-ADTS] section 2.2.15) for the following information:

- DK - Use DES only: When this flag is set on the principal, only the des-cbc-md5 and/or des-cbc-crc keys [RFC3961] SHOULD be used in the Kerberos exchanges for this account.

- DR - Pre-Authentication not required: When this flag is set on the principal, the KDC MUST issue a TGT without valid pre-authentication data ([RFC4120] section 7.5.2) provided.
- NA - Authorization data not required: When this flag is set on the Application Server's service account, the KDC MUST NOT include a PAC in the service ticket.
- ND - Delegation not allowed: When this flag is set on the principal, the KDC MUST NOT set the PROXIABLE or FORWARDABLE ticket flags ([RFC4120] sections 2.5 and 2.6).
- TA - Trusted to authentication for delegation: When this flag is set on the principal and the service obtains an S4USelf [MS-SFU] service ticket, the KDC MUST set the FORWARDABLE ticket flag ([RFC4120] section 2.6). When this flag is not set, the KDC MUST NOT set the FORWARDABLE ticket flag ([RFC4120] section 2.6) in the S4USelf service ticket.
- TD - Trusted for delegation: When this flag is set on the principal, the KDC MUST set the OK-AS-DELEGATE ticket flag ([RFC4120] section 2.8).

3.3.5 Message Processing Events and Sequencing Rules

KILE concatenates the following information to use as the key salt for realm trusts:

- Inbound trusts: <all upper case name of the remote realm> | "krbtgt" | <all upper case name of the local realm>
- Outbound trusts: <all upper case name of the local realm> | "krbtgt" | <all upper case name of the remote realm>