

## [MS-SFU]: Kerberos Protocol Extensions Service for User and Constrained Delegation Protocol

This topic lists the Errata found in the MS-SFU document 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.

Errata below are for Protocol Document Version [V17.0 – 2018/09/12](#).

Errata Published*	Description
2019/10/16	<p>In Section 3.2.5.2.2, KDC Replies with Service Ticket, the reference to the FORWARDABLE flag being set has been removed.</p> <p>Changed from:</p> <p>The KDC MUST reply with the service ticket where:</p> <ul style="list-style-type: none"> <li>• The sname field contains the name of Service 2.</li> <li>• The realm field contains the realm of Service 2.</li> <li>• The cname field contains the cname from the service ticket in the additional-tickets field.</li> <li>• The crealm field contains the crealm from the service ticket in the additional-tickets field.</li> <li>• The S4U_DELEGATION_INFO structure is in the new PAC.</li> <li>• If the TrustedToAuthenticationForDelegation parameter on the Service 1 principal is set to TRUE: <ul style="list-style-type: none"> <li>• The FORWARDABLE ticket flag is set.</li> </ul> </li> </ul> <p>Changed to:</p> <p>The KDC MUST reply with the service ticket where:</p> <ul style="list-style-type: none"> <li>• The sname field contains the name of Service 2.</li> <li>• The realm field contains the realm of Service 2.</li> <li>• The cname field contains the cname from the service ticket in the additional-tickets field.</li> <li>• The crealm field contains the crealm from the service ticket in the additional-tickets field.</li> <li>• The S4U_DELEGATION_INFO structure is in the new PAC</li> </ul>
2019/09/02	<p>In Section 3.2.5.2, KDC Receives S4U2proxy KRB_TGS_REQ, has been changed from:</p> <p>--Set and the USER_NOT_DELEGATED bit is set in the UserAccountControl field in the KERB_VALIDATION_INFO structure ([MS-PAC] section 2.5), then the KDC MUST return KRB-ERR-BADOPTION with STATUS_NOT_FOUND.</p> <p>Changed to:</p> <p>--Set and the USER_NOT_DELEGATED bit is set in the UserAccountControl field in the KERB_VALIDATION_INFO structure ([MS-PAC] section 2.5), then the KDC MUST return KRB-ERR-BADOPTION with STATUS_ACCOUNT_RESTRICTION ([MS-ERREF] section 2.3.1).</p>
2019/07/22	<p>In Section 2.2.1, PA-FOR-USER, corrected that PA-FOR-USER is not encrypted.</p>

Errata Published*	Description
	<p>Changed from:</p> <p>The following code defines the ASN.1 structure of the PA-FOR-USER padata type.</p> <pre>         padata-type      ::= PA-FOR-USER         -- value 129         padata-value     ::= EncryptedData                            -- PA-FOR-USER-ENC          PA-FOR-USER-ENC ::= SEQUENCE {             userName      [0] PrincipalName,             userRealm     [1] Realm,             cksum         [2] Checksum,             auth-package  [3] KerberosString         } </pre> <p>Changed to:</p> <p>The following code defines the ASN.1 structure of the PA-FOR-USER padata type.</p> <pre>         PA-FOR-USER ::= SEQUENCE {             -- PA TYPE 129             userName      [0] PrincipalName,             userRealm     [1] Realm,             cksum         [2] Checksum,             auth-package  [3] KerberosString         } </pre>
2019/04/29	<p>In this document, changes have been made to clarify the behavior of S4u2Self with x509 certificate regarding use of PA_FOR_USER following a cross-realm referral.</p> <p>In Section 3.1.5.1.1, Service Sends S4U2self KRB_TGS_REQ, has been changed from:</p> <p>The user identification for these cases is carried in a PA-FOR-USER padata type or a PA-S4U-X509-USER padata type, respectively.</p> <p>Changed to:</p> <p>The PA-FOR-USER padata type can be used only in the former case, while a PA-S4U-X509-USER padata type can carry the user identity in both cases."</p> <p>A new section, Section 3.1.5.1.1.1, When to Use Each padata Type, has been added:</p> <p>What padata type Service 1 sends is determined by two factors. First, determine whether the TGT session key is of a newer type, defined here as ciphers that are not DES or RC4 based. Second, determine whether the client username was provided explicitly or was extracted from a certificate.</p> <p>Service 1 SHOULD populate and send a PA-FOR-USER structure when one of the following is true:</p> <ul style="list-style-type: none"> <li>--No certificate was presented for the user.</li> <li>--No user name was explicitly provided, and instead a certificate was provided that contained the user name in the Subject Alternate Name (SAN) field.</li> </ul>

Errata Published*	Description
	<p>Service 1 SHOULD populate and send a PA-S4U-X509-USER structure when one of the following is true:</p> <ul style="list-style-type: none"> <li>--No PA-FOR-USER is being sent.</li> <li>--The session key of the TGT being used is not a DES or RC4 key type.</li> </ul> <p>In Section 3.1.5.1.1.2, the title has been changed from "Using the User's Realm and User Name" to "Identify the User".</p> <p>In Section 3.1.5.1.1.13.1.5.1.1.2, Sending the S4Uself KRB_TGT_REQ, has been changed from:</p> <p>The S4U2self information in the KRB_TGS_REQ consists of: padata-type = PA-FOR-USER (ID129), which consists of four fields: userName, userRealm, cksum, and auth-package.</p> <p>Changed to:</p> <p>If Service 1 sends a PA-FOR-USER (ID129) structure, it consists of four fields: userName, userRealm, cksum, and auth-package.</p> <p>In that same section, the following paragraph has been added:</p> <p>If sending a PA-S4U-X509-USER (ID 130) structure, the cname and crealm should contain the same values as used for userName and userRealm in a PA-FOR-USER. If a client certificate was provided, the subject-certificate field MUST contain the client's X509 certificate encoded in ASN.1, as specified in [RFC3280]."</p> <p>Section 3.1.5.1.1.2, Using the User's Certificate to Identify the User, has been removed.</p> <p>In Section 3.1.5.1.2, Service Receives S4U2self KRB_TGS_REP, the following paragraph has been added:</p> <p>In service tickets from KDCs that support S4U, the cname contains the name of the user. Services can further detect if the KDC supports PA_S4U_X509_USER by checking the reply padata for a PA-S4U-X509-USER preauth data. Furthermore, the KDC uses this reply padata to return a normalized form of the user name. Service 1 MUST take the cname from the reply PA-S4U-X509-USER and use it to replace both the cname from PA-S4U-X509-USER and the userName from PA-FOR-USER in any subsequent KRB_TGS_REQ requests used to chase referrals back to Service 1's realm. Additionally, the certificate is removed from the PA-S4U-X509-USER padata.</p> <p>For details on the above changes, see the PDF doc <a href="#">here</a>.</p>

\*Date format: YYYY/MM/DD