[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.

RSS
Atom

Errata below are for Protocol Document Version V17.0 – 2018/09/12.

Errata Published*	Description
2019/12/09	In Section 3.2.5.2, KDC Receives S4U2proxy KRB_TGS_REQ, moved content to subsequent sections to reorder processing steps. Changed from: When a KDC processes a TGS-REQ ([RFC4120] section 3.3.2) and it is a S4U2proxy KRB_TGS_REQ message, the KDC will perform the following steps. If the service ticket in the additional-tickets field is not set to forwardable<19> and the PA-PAC-OPTIONS [167] ([MS-KILE] section 2.2.10) padata type has the resource-based constrained delegation bit: • Not set, then the KDC MUST return KRB-ERR-BADOPTION with STATUS_NO_MATCH. • 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). Service 1's KDC verifies both server ([MS-PAC] section 2.8.1) and KDC ([MS-PAC] section 2.8.2) signatures of the PAC. If Service 2 is in another domain, then its KDC verifies only the KDC signature of the PAC. If verification fails, the KDC MUST return KRB-AP-ERR-MODIFIED. When a KDC determines that a referral TGT is required ([RFC6806] section 8), then if Service 2 is not in the KDC's realm, the KDC SHOULD<20> reply with referral TGT (section 3.2.5.3.1). Changed to: When a KDC processes a TGS-REQ ([RFC4120] section 3.3.2) and it is a S4U2proxy KRB_TGS_REQ message, the KDC will perform the steps in the following sections. Deleted Section 3.2.5.2.1, KDC Confirms Delegation is Allowed and moved Section 3.2.5.2.1.2, Using ServicesAllowedToSendForwardedTicketsTo. Changed from: 3.2.5.2.1 KDC Confirms Delegation is Allowed If the KDC is for the realm of: • Service 2 only: The KDC uses the ServicesAllowedToReceiveForwardedTicketsFrom parameter to check if Service 1 is allowed to receive a service ticket for the principal.<21>

Errata Published*	Description
	• Service 1 and Service 2: First the KDC uses the ServicesAllowedToReceiveForwardedTicketsFrom parameter to check if Service 1 is allowed to receive a service ticket for the principal. If it fails or the ServicesAllowedToReceiveForwardedTicketsFrom parameter is empty, then the KDC uses the ServicesAllowedToSendForwardedTicketsTo parameter to check if Service 2 is listed on Service 1 as allowed to receive a service ticket for the principal. <22> Changed to: 3.2.5.2.1 Using ServicesAllowedToSendForwardedTicketsTo If the KDC is for the realm of both Service 1 and Service 2, then the KDC checks if the security principal name (SPN) for Service 2, identified in the sname and srealm fields of the KRB_TGS_REQ message, is in the Service 1 account's ServicesAllowedToSendForwardedTicketsTo parameter. If it is, then the delegation policy is satisfied. If not, and the PA-PAC-OPTIONS [167] ([MS-KILE] section 2.2.10) padata type does not have the resource-based constrained delegation bit, then the KDC MUST return KRB-ERR-BADOPTION. If Service 1's ServicesAllowedToSendForwardedTicketsTo parameter was empty, this is returned with STATUS_NOT_SUPPORTED, else STATUS_NO_MATCH. If the service ticket in the additional-tickets field is not set to forwardable<19> and the PA-PAC-OPTIONS [167] ([MS-KILE] section 2.2.10) padata type has the resource-based constrained delegation bit set, then the KDC MUST return KRB-ERR-BADOPTION with STATUS_NO_MATCH. Added Section 3.2.5.2.2, Verification of the PAC and moved content from Section 3.2.5.2, KDC Receives S4U2proxy KRB_TGS_REQ to this new section. Changed from: --- Changed to: Service 1's KDC verifies both server ([MS-PAC] section 2.8.1) and KDC ([MS-PAC] section 2.8.2) signatures of the PAC. If Service 2 is in another domain, then its KDC verifies only the KDC signature of the PAC. If verification fails, the KDC MUST return KRB-AP-ERR-MODIFIED. Moved Section 3.2.5.2.1.1, Using ServicesAllowedToReceiveForwardedTicketsFrom, to after Section 3.2.5.2.1.2, Using ServicesAllowedToSendForwardedTicketsTo. Changed from: 3.2.5.2.1.1 Using ServicesAllowedToReceiveForwardedTicketsFrom If the Service 2 account's ServicesAllowedToReceiveForwardedTicketsFrom is nonempty and cname in the encrypted part of both TGTs match, the KDC creates a Token/Authorization Context ([MS-DTYP] section 2.5.2) for Service 1 from the PAC data in Service 1's TGT, and performs an access check using the ServicesAllowedToReceiveForwardedTicketsFrom parameter. If the access check succeeds, then the KDC replies with a service ticket for Service 2 (section 5.2.5.4.1).<23> Changed to:

Errata Published*	Description
	3.2.5.2.3 Using ServicesAllowedToReceiveForwardedTicketsFrom If the delegation policy was not satisfied via ServicesAllowedToSendForwardedTicketsTo, this is the KDC for Service 2, and the Service 2 account's ServicesAllowedToReceiveForwardedTicketsFrom is nonempty and cname in the encrypted part of both TGTs match, the KDC creates a Token/Authorization Context ([MS-DTYP] section 2.5.2) for Service 1 from the PAC data in Service 1's TGT. Then the KDC performs an access check using the ServicesAllowedToReceiveForwardedTicketsFrom parameter.<20> If the access check succeeds, then the KDC replies with a service ticket for Service 2. If the access check fails, the KDC MUST return KRB-ERR-BADOPTION with STATUS_NOT_FOUND. If this is the KDC for Service 1, and the service ticket in the additional-tickets field is not set to forwardable,<21> 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). When a KDC determines that a referral TGT is required ([RFC6806] section 8), then if Service 2 is not in the KDC's realm, the KDC SHOULD<22> reply with referral TGT (section 3.2.5.1.1). For details on the above changes, see the PDF doc here.
2019/10/16	In Section 3.2.5.2.2, KDC Replies with Service Ticket, the reference to the FORWARDABLE flag being set has been removed. Changed from: The KDC MUST reply with the service ticket where: ● The sname field contains the name of Service 2. ● The realm field contains the realm of Service 2. ● The cname field contains the cname from the service ticket in the additional-tickets field. ● The crealm field contains the crealm from the service ticket in the additional-tickets field. ● The S4U_DELEGATION_INFO structure is in the new PAC. ● If the TrustedToAuthenticationForDelegation parameter on the Service 1 principal is set to TRUE: ● The FORWARDABLE ticket flag is set. Changed to: The KDC MUST reply with the service ticket where: ● The sname field contains the name of Service 2. ● The realm field contains the realm of Service 2. ● The cname field contains the cname from the service ticket in the additional-tickets field. ● The crealm field contains the crealm from the service ticket in the additional-tickets field. ● The S4U_DELEGATION_INFO structure is in the new PAC
2019/09/02	In Section 3.2.5.2, KDC Receives S4U2proxy KRB_TGS_REQ, has been changed from: --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. Changed to:

Errata Published*	Description
	--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).

2019/07/22	In Section 2.2.1, PA-FOR-USER, corrected that PA-FOR-USER is not encrypted.
	
	Changed from:
	The following code defines the ASN.1 structure of the PA-FOR-USER padata type.
	
	`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`
	`}`
	
	Changed to:
	The following code defines the ASN.1 structure of the PA-FOR-USER padata type.
	
	`PA-FOR-USER ::= SEQUENCE {`
	`-- PA TYPE 129`
	`userName [0] PrincipalName,`
	`userRealm [1] Realm,`
	`cksum [2] Checksum,`
	`auth-package [3] KerberosString`
	`}`

2019/04/29	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. In Section 3.1.5.1.1, Service Sends S4U2self KRB_TGS_REQ, has been changed from: The user identification for these cases is carried in a PA-FOR-USER padata type or a PA-S4U-X509-USER padata type, respectively. Changed to: 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." A new section, Section 3.1.5.1.1.1, When to Use Each padata Type, has been added: 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.

Errata Published*	Description
	Service 1 SHOULD populate and send a PA-FOR-USER structure when one of the following is true: --No certificate was presented for the user. --No user name was explicitly provided, and instead a certificate was provided that contained the user name in the Subject Alternate Name (SAN) field. Service 1 SHOULD populate and send a PA-S4U-X509-USER structure when one of the following is true: --No PA-FOR-USER is being sent. --The session key of the TGT being used is not a DES or RC4 key type. 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". In Section 3.1.5.1.1.13.1.5.1.1.2, Sending the S4USelf KRB_TGT_REQ, has been changed from: 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. Changed to: If Service 1 sends a PA-FOR-USER (ID129) structure, it consists of four fields: userName, userRealm, cksum, and auth-package. In that same section, the following paragraph has been added: 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]." Section 3.1.5.1.1.2, Using the User's Certificate to Identify the User, has been removed. In Section 3.1.5.1.2, Service Receives S4U2self KRB_TGS_REP, the following paragraph has been added: 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. For details on the above changes, see the PDF doc here.

*Date format: YYYY/MM/DD