[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 V18.0 – 2020/03/04.

Errata Published*	Description
2020/11/10	In Section 3.2.5.2.2 Verification of the PAC, added service ticket verification. Changed from: 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 (1), then its KDC verifies only the KDC signature of the PAC. If verification fails, the KDC MUST return KRB-AP-ERR-MODIFIED. 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. Because Service 1's KDC is ingesting a service ticket rather than a TGT, it SHOULD also ensure the integrity of the service ticket by verifying the ticket signature ([MS-PAC] section 2.8.3). If Service 2 is in another domain (1), then its KDC verifies only the KDC signature of the PAC. If verification fails, the KDC MUST return KRB-AP-ERR-MODIFIED.
2020/03/30	In Section 3.2.5.2.1, Using ServicesAllowedToSendForwardedTicketsTo, changed the secondary check to state that padata type does not have the resource-based constrained delegation bit set for the return values. Changed from: If the service ticket in the additional-tickets field is not set to forwardable and the PA-PACOPTIONS [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. Changed to: If the service ticket in the additional-tickets field is not set to forwardable and the PA-PACOPTIONS [167] ([MS-KILE] section 2.2.10) padata type does not have the resource-based constrained delegation bit set, then the KDC MUST return KRB-ERR-BADOPTION with STATUS_NO_MATCH. In Section 3.2.5.2.3, Using ServicesAllowedToReceiveForwardedTicketsFrom, removed the first check for the KDC for service 1. Changed from:

Errata Published*	Description
	If this is the KDC for Service 1, and the service ticket in the additional-tickets field is not set to forwardable, 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… Changed to: If the service ticket in the additional-tickets field is not set to forwardable, 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…
2020/03/30	In Section 3.2.5.2.4, KDC Replies with Service Ticket, the source of the cname and crealm has been added. Changed from: The KDC MUST also add the name of Service 1 to the S4UTransitedServices list in the structure. Changed to: The KDC MUST also add the name of Service 1 to the S4UTransitedServices list in the structure. Windows KDC constructs the impersonated client's principal name from the PAC. The cname and crealm in the KDC reply are set to the impersonated client's principal name, realm.

*Date format: YYYY/MM/DD