[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 V35.0 – 2020/03/04.

Errata Published*	Description
2020/07/20	In Section 3.4.5.3, Processing Authorization Data, added processing for searching AD-IF-RELEVANT containers for authorization data. Changed from: The server MUST check if KERB-AD-RESTRICTION-ENTRY.Restriction.MachineID (section 2.2.6) is equal to Machine ID (section 3.1.1.4): Changed to: The server MUST search all AD-IF-RELEVANT containers for the KERB_AUTH_DATA_TOKEN_RESTRICTIONS and KERB_AUTH_DATA_LOOPBACK authorization data entries. The server MAY<76> search all AD-IF-RELEVANT containers for all other authorization data entries. The server MUST check if KERB-AD-RESTRICTION-ENTRY.Restriction.MachineID (section 2.2.6) is equal to machine ID (section 3.1.1.4): <76> Windows only searches the first AD-IF-RELEVANT container. In Section 3.2.5.8, AP Exchange, updated AD-AUTH-DATA-AP-OPTIONS is sent in the first AD-IF-RELEVANT element. Changed from: If ChannelBinding is set to TRUE, the client sends AD-AUTH-DATA-AP-OPTIONS data in an AD-IF-RELEVANT element ([RFC4120] section 5.2.6.1). Changed to: If ChannelBinding is set to TRUE, the client sends AD-AUTH-DATA-AP-OPTIONS data in the first AD-IF-RELEVANT element ([RFC4120] section 5.2.6.1).
2020/05/11	In Section 3.3.5.7.5, Cross-Domain Trust and Referrals, updated product support for the TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION flag. Changed from: <67> Section 3.3.5.7.5: The TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION flag is supported on Windows Server 2003 and later when [MSKB-4490425] is installed. Changed to:<67> Section 3.3.5.7.5: The TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION flag is supported on Windows Server 2008 and later when [MSKB-4490425] is installed.

Errata Published*	Description
2020/04/27	In Section 3.3.5.7.8, Key List Request, added reference to [RFC6806] to define EncKDCRepPart structure. Changed from: … the KDC SHOULD include the long-term secrets of the client for the requested encryption types in the KERB-KEY-LIST-REP [162] response message and insert it into the encrypted-pa-data of the EncKDCRepPart.<69> Changed to: … the KDC SHOULD include the long-term secrets of the client for the requested encryption types in the KERB-KEY-LIST-REP [162] response message and insert it into the encrypted-pa-data of the EncKDCRepPart structure, as defined in [RFC6806].<69>
2020/04/27	In Section 3.3.5.7.6, FORWARDED TGT etype, added PA data number to PA-SUPPORTED-ENCTYPES [165]. Changed from: … the client provides a PA-SUPPORTED-ENCTYPES structure (section 2.2.8) with encryption types (section 2.2.7) the KDC supports, then the KDC SHOULD<68> select the strongest encryption type that is both included in the PA-SUPPORTED-ENCTYPES structure (section 2.2.8) and supported by the KDC to generate the random session key. Changed to:… the client provides a PA-SUPPORTED-ENCTYPES [165] structure (section 2.2.8) with encryption types (section 2.2.7) the KDC supports, then the KDC SHOULD<68> select the strongest encryption type that is both included in the PA-SUPPORTED-ENCTYPES [165] structure (section 2.2.8) and supported by the KDC to generate the random session key
2020/04/27	In Section 3.3.5.3, PAC Generation, removed PA data number [128] as not part of KERB-PA-PAC-REQUEST Boolean structure. Changed from: The request to include a PAC is expressed through the use of a KERB-PA-PAC-REQUEST [128] (section 2.2.3) padata type that is set to TRUE: Changed to:The request to include a PAC is expressed through the use of a KERB-PA-PAC-REQUEST (section 2.2.3) padata type that is set to TRUE:
2020/04/27	In Section 1.3.2, Kerberos Network Authentication Service (V5) Synopsis, added product note for addition of PA-Data in the TGS-REQ and TGS-REP messages. Changed from: The Ticket-Granting Service (TGS) exchange ([RFC4120] section 3.3): Kerberos ticket-granting service (TGS) request message (KRB_TGS_REQ)… • Kerberos ticket-granting service (TGS) response message (KRB_TGS_REP)… Changed to: The Ticket-Granting Service (TGS) exchange ([RFC4120] section 3.3):<1> • Kerberos ticket-granting service (TGS) request message (KRB_TGS_REQ)… • Kerberos ticket-granting service (TGS) response message (KRB_TGS_REP)…

Errata Published*	Description
	<1>Added a PA-Data request in the TGS-REQ message and an encrypted PA-Data response in the TGS-REP message that includes the NTLM hash for the authenticated user in Windows 10 v1607 operating system client version and in Windows Server 2016 server version and later.
2020/04/13	In Section 3.1.5.4, Ticket Flag Details, the description of the transit policy enforcement has been clarified. Changed from: The TRANSITED-POLICY-CHECKED flag ([RFC4120] section 2.7): KILE does not check for transited domains on servers or a KDC. Application servers MUST ignore the TRANSITED-POLICY-CHECKED flag. Changed To: The TRANSITED-POLICY-CHECKED flag ([RFC4120] section 2.7): KILE does not check for transited domains on servers or a KDC. Application servers MUST ignore the TRANSITED-POLICY-CHECKED flag. For details on decoding a cross-realm TGTandcrealm filtering see [MS-PAC] section 4.1.2.3.

*Date format: YYYY/MM/DD