[MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol

This topic lists the Errata found in [MS-PKCA] 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 V15.0 – 2021/10/06.

Errata Published*	Description
2022/05/10	Section 3.1.5.2.1.5 Mapping Strength: added section. The KDC SHOULD<22> map a certificate to a user using one of the following mappings. These methods of mapping a certificate to a user are classified as strong or weak based on whether they depend on a name as a secure identifier. The following mappings are considered weak: • SAN UPNName • SAN DNSName • altSecurityIdentities Issuer Name and Subject Name • altSecurityIdentities Subject Name • altSecurityIdentities 822 field The following mappings are considered strong: • SID (section 3.1.5.2.1.6) • Key Trust (section 3.1.5.2.1.4) • altSecurityIdentities Issuer and Serial Number • altSecurityIdentities Subject Key Identifier • altSecurityIdentities SHA1 Hash of Public Key If a KDC maps a certificate to a user using one of the above weak mappings, it SHOULD<23> continue to search for more mappings until it encounters a strong mapping. If it does not find such a mapping, it MAY fail the authentication request with KDC_ERR_CERTIFICATE_MISMATCH. <22> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2012 and later.

Errata Published*	Description
	<23> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2012 and later. Section 3.1.5.2.1.6 SID: added section. If a KDC has exhausted all other mapping types for a certificate and found a weak mapping without finding a strong mapping, it SHOULD<24> check if the certificate contains a security identifier (SID). If it does and the SID matches the user the certificate weakly mapped to, the certificate is to be considered strongly mapped. If the SID does not match, the authentication MUST fail with KDC_ERR_CERTIFICATE_MISMATCH. If the certificate does not contain a SID, the KDC MAY fail the authentication request as no strong mapping is available. For more details on the objectSID in an issued certificate see [MS-WCCE] and section 2.2.2.7.7.4. <24> Section 3.1.5.2.1.6 Certificate SID mapping is applicable to Windows Server 2012 and later.

*Date format: YYYY/MM/DD