[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 V14.0 – 2021/06/25.

Errata Published*	Description
2021/09/07	In Section 3.1.5 Message Processing Events and Sequencing Rules, removed references to RC2 encryption mode and added reference to the security update. Changed from: In addition to the required ([RFC4556] section 3.1.1) and recommended ([RFC4556] section 3.1.2) algorithms, PKCA supports the rc2-cbc ([RFC4556] section 3.1.4) algorithm. An implementer SHOULD<12> specify des-ede3-cbc ([RFC4556] section 3.1.2) as the default algorithm. <12> Section 3.1.5: In Windows with PKCA, the KDC supports both des-ede3-cbc and rc2-cbc. If both des-ede3-cbc and rc2-cbc are present, the KDC uses des-ede3-cbc. Changed to: In addition to the required ([RFC4556] section 3.1.1) and recommended ([RFC4556] section 3.1.2) algorithms, an implementer MUST<12> specify des-ede3-cbc ([RFC4556] section 3.1.2) as the default algorithm. <12> Section 3.1.5: In Windows with PKCA, the KDC supports and uses des-ede3-cbc. The RC2 algorithm rc2-cbc is no longer supported for encryption mode based key delivery with Kerberos PKINIT ([RFC4556]). See Windows Key Distribution Center Information Disclosure Vulnerability July 13, 2021 [MSFT-CVE-2021-33764]. This update applies to Windows Servers with Domain Controllers, Windows Server 2008 and later.

*Date format: YYYY/MM/DD