OASIS

KMIP TC Comment resolution log

KMIP Specification v1.4 Committee Specification Draft

Item #	Date received	Submitted by	Location	Summary	Proposed resolution	Owner	TC Resolution
1	20-Mar-17	Conrado Gouvêa	https://lists.oasis-open.org/archives/k	Mismatch between Batch Continue Capability content and enumeration tag name	Apply change to 2.1.21 - Non-substantive change	Editor	Non-material change as proposed
2	22-Mar-17	TC Admin	https://lists.oasis-open.org/archives/k	Appendix E Acronyms Repeated	Remove repeated text - Non-substantive change	Editor	Non-material change as proposed
3	22-Mar-17	TC Admin	https://lists.oasis-open.org/archives/k	Sect 3.44 Template text not removed	Correct repeated text- Non -substantive change	Editor	Non-material change as proposed
4	22-Mar-17	TC Admin	https://lists.oasis-open.org/archives/k	Broken internal references - check section 6.2	Repair reference links - Non-substantive change	Editor	Non-material change as proposed
5	22-Mar-17	TC Admin	https://lists.oasis-open.org/archives/k	Some normative reference links are broken	Repair reference links - Non-substantive change	Editor	Non-material change as proposed
6	22-Mar-17	TC Admin	https://lists.oasis-open.org/archives/k	Some normative reference links are out of date	Update reference links - Non-substantive change	Editor	Non-material change as proposed
7	19-Apr-17	Annabelle Lee	https://lists.oasis-open.org/archives/k	Received after PR period - There are several references to NIST standards that are out of date: FIPS 180-4 was updated in 2015. FIPS 186-4 was updated in 2013. NIST SP 800-38A had an addendum in 2010. NIST SP 800-38B was updated in 2016. NIST SP 800-38c was updated in 7/2007. NIST SP 800-57-1 was updated in 2016	Update in next version for 1.x consistency - No Change	Editor	No Change
8	19-Apr-17	Annabelle Lee	https://lists.oasis-open.org/archives/k	Received after PR period - Several of the listed algorithms, such as MD2, MD4, and MD5 have not been approved by NIST, so why are they included?	The scope of this specification is not limited to NIST-approved algorithms. No Change	Editor	No Change
9	19-Apr-17	Annabelle Lee	https://lists.oasis-open.org/archives/k	Received after PR period - 9.1.3.2.7: RSA is listed as “RSA Encryption”. These are digital signature algorithms. RSA encryption is a different algorithm used for key transport.	No Change	Editor	No Change
10	19-Apr-17	Annabelle Lee	https://lists.oasis-open.org/archives/k	Received after PR period - The SHA3 algorithms are not listed.	Additional algorithms and associated items (Normative ref) inserted - Non-substantive change	Editor	Non-material change as proposed
11	19-Apr-17	Annabelle Lee	https://lists.oasis-open.org/archives/k	Received after PR period - Listed is a “NIST key wrap algorithm.” The algorithm referenced is AES key wrap.	No Change	Editor	No Change
12	19-Apr-17	Annabelle Lee	https://lists.oasis-open.org/archives/k	Received after PR period - Many of the algorithms have limitations specified by NIST, such as disallowed, acceptable, for legacy use. These use limitations would be useful to include.	No Change	Editor	No Change