



OASIS Committee Note

Key Management Interoperability Protocol Test Cases Version 2.1

Committee Note 01

07 May 2020

This stage:

<https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/cn01/kmip-testcases-v2.1-cn01.docx> (Authoritative)
<https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/cn01/kmip-testcases-v2.1-cn01.html>
<https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/cn01/kmip-testcases-v2.1-cn01.pdf>

Previous stage:

N/A

Latest stage:

<https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/kmip-testcases-v2.1.docx> (Authoritative)
<https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/kmip-testcases-v2.1.html>
<https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/kmip-testcases-v2.1.pdf>

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chairs:

Tony Cox (tony.cox@cryptsoft.com), Cryptsoft Pty Ltd.
Judith Furlong (Judith.Furlong@dell.com), Dell EMC

Editors:

Tim Chevalier (Tim.Chevalier@netapp.com), NetApp
Tim Hudson (tjh@cryptsoft.com), Cryptsoft Pty Ltd.

Additional artifacts:

This document is one component of a Work Product that also includes:

- Test cases: <https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/cn01/test-cases/kmip-v2.1/>.

Related work:

This document replaces or supersedes:

- *Key Management Interoperability Protocol Test Cases Version 2.0*. Edited by Tim Hudson and Mark Joseph. Latest stage: <https://docs.oasis-open.org/kmip/kmip-testcases/v2.0/kmip-testcases-v2.0.html>.

This document is related to:

- *Key Management Interoperability Protocol Specification Version 2.1*. Edited by Tony Cox and Charles White. Latest stage: <https://docs.oasis-open.org/kmip/kmip-spec/v2.1/kmip-spec-v2.1.html>.
- *Key Management Interoperability Protocol Profiles Version 2.1*. Edited by Tim Chevalier and Tim Hudson. Latest stage: <https://docs.oasis-open.org/kmip/kmip-profiles/v2.1/kmip-profiles-v2.1.html>.
- *Key Management Interoperability Protocol Usage Guide Version 2.1*. Edited by Judith Furlong and Jeff Bartell. Latest stage: <https://docs.oasis-open.org/kmip/kmip-ug/v2.1/kmip-ug-v2.1.html>.

Abstract:

This document is intended for developers and architects who wish to design systems and applications that interoperate using the Key Management Interoperability Protocol specification.

Status:

This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

This document was last revised or approved by the OASIS Key Management Interoperability Protocol (KMIP) TC on the above date. The level of approval is also listed above. Check the “Latest stage” location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC’s public comment list, after subscribing to it by following the instructions at the “[Send A Comment](#)” button on the TC’s web page at <https://www.oasis-open.org/committees/kmip/>.

Citation format:

When referencing this document, the following citation format should be used:

[kmip-testcases-v2.1]

Key Management Interoperability Protocol Test Cases Version 2.1. Edited by Tim Chevalier and Tim Hudson. 07 May 2020. OASIS Committee Note 01. <https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/cn01/kmip-testcases-v2.1-cn01.html>. Latest stage: <https://docs.oasis-open.org/kmip/kmip-testcases/v2.1/kmip-testcases-v2.1.html>.

Notices

Copyright © OASIS Open 2020. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1	Introduction	7
1.1	References (non-normative)	7
2	KMIP Test Cases.....	8
2.1	TC-ASYNC-1-21.....	8
2.2	TC-ASYNC-2-21.....	8
2.3	TC-ASYNC-3-21.....	8
2.4	TC-ASYNC-4-21.....	8
2.5	TC-ASYNC-5-21.....	8
2.6	TC-ASYNC-6-21.....	9
2.7	TC-ASYNC-7-21.....	9
2.8	TC-ASYNC-8-21.....	9
2.9	TC-ASYNC-9-21.....	9
2.10	TC-ASYNC-10-21.....	9
2.11	TC-CERTATTR-1-21.....	9
2.12	TC-CREATE-SD-1-21	9
2.13	TC-CS-CORVAL-1-21.....	9
2.14	TC-DERIVEKEY-1-21	10
2.15	TC-DERIVEKEY-2-21	10
2.16	TC-DERIVEKEY-3-21	10
2.17	TC-DERIVEKEY-4-21	10
2.18	TC-DERIVEKEY-5-21	10
2.19	TC-DERIVEKEY-6-21	10
2.20	TC-DIGESTS-1-21	10
2.21	TC-DLOGIN-1-21	10
2.22	TC-DLOGIN-2-21	10
2.23	TC-DLOGIN-3-21	11
2.24	TC-DLOGIN-4-21	11
2.25	TC-DLOGIN-5-21	11
2.26	TC-DLOGIN-6-21	11
2.27	TC-DLOGIN-7-21	11
2.28	TC-DLOGIN-8-21	11
2.29	TC-DLOGIN-9-21	11
2.30	TC-DLOGIN-10-21	11
2.31	TC-DLOGIN-11-21	12
2.32	TC-DLOGIN-12-21	12
2.33	TC-DLOGIN-13-21	12
2.34	TC-ECC-1-21	12
2.35	TC-ECC-2-21	12
2.36	TC-ECC-3-21	12
2.37	TC-ECDSA-SIGN-1-21.....	12
2.38	TC-ECDSA-SIGN-DIGESTEDDATA 1-21	12

2.39 TC-EXTRACTABLE-1-21	13
2.40 TC-I18N-1-21	13
2.41 TC-I18N-2-21	13
2.42 TC-I18N-3-21	13
2.43 TC-IMPEXP-1-21	13
2.44 TC-IMPEXP-2-21	13
2.45 TC-IMPEXP-3-21	13
2.46 TC-IMPEXP-4-21	13
2.47 TC-IMPEXP-5-21	14
2.48 TC-LOGIN-1-21	14
2.49 TC-LOGIN-2-21	14
2.50 TC-LOGIN-3-21	14
2.51 TC-MD-1-21	14
2.52 TC-MD-2-21	14
2.53 TC-MD-3-21	14
2.54 TC-MD-4-21	14
2.55 TC-MD-5-21	15
2.56 TC-MD-6-21	15
2.57 TC-MD-21-21	15
2.58 TC-MD-22-21	15
2.59 TC-MD-23-21	15
2.60 TC-MD-24-21	15
2.61 TC-MDO-1-21	15
2.62 TC-MDO-2-21	15
2.63 TC-MDO-3-21	16
2.64 TC-OFFSET-1-21	16
2.65 TC-OFFSET-2-21	16
2.66 TC-PGP-1-21	16
2.67 TC-PING-1-21	16
2.68 TC-PKCS12-1-21	16
2.69 TC-PKCS12-2-21	16
2.70 TC-REENCRYPT-1-21	16
2.71 TC-REENCRYPT-2-21	17
2.72 TC-REENCRYPT-3-21	17
2.73 TC-REENCRYPT-4-21	17
2.74 TC-REENCRYPT-5-21	17
2.75 TC-REENCRYPT-6-21	17
2.76 TC-REKEY-1-21	17
2.77 TC-REKEY-2-21	17
2.78 TC-REKEY-3-21	17
2.79 TC-REKEY-4-21	17
2.80 TC-REKEY-5-21	18
2.81 TC-REKEY-6-21	18

2.82 TC-REKEY-7-21	18
2.83 TC-REKEY-8-21	18
2.84 TC-REKEY-9-21	18
2.85 TC-REKEY-10-21	18
2.86 TC-REKEY-11-21	18
2.87 TC-REKEY-12-21	18
2.88 TC-RNG-ATTR-1-21	19
2.89 TC-RNG-ATTR-2-21	19
2.90 TC-RSA-SIGN-DIGESTEDDATA 1-21	19
2.91 TC-SENSITIVE-1-21	19
2.92 TC-SETTATTR-1-21	19
2.93 TC-SETTATTR-2-21	19
2.94 TC-SETTATTR-3-21	19
2.95 TC-SJ-1-21	19
2.96 TC-SJ-2-21	20
2.97 TC-SJ-3-21	20
2.98 TC-SJ-4-21	20
2.99 TC-STREAM-ENC-1-21	20
2.100 TC-STREAM-ENC-2-21	20
2.101 TC-STREAM-ENCDEC-1-21	20
2.102 TC-STREAM-HASH-1-21	20
2.103 TC-STREAM-HASH-2-21	20
2.104 TC-STREAM-HASH-3-21	21
2.105 TC-STREAM-MAC-1-21	21
2.106 TC-STREAM-SIGN-1-21	21
2.107 TC-STREAM-SIGNVFY-1-21	21
2.108 TC-WRAP-1-21	21
2.109 TC-WRAP-2-21	21
2.110 TC-WRAP-3-21	21
Appendix A. Acknowledgments	22
Appendix B. Revision History	23

1 Introduction

The purpose of this document is to describe test cases to demonstrate the Key Management Interoperability Protocol (KMIP) [KMIP-SPEC]. The test cases illustrate that the concepts within the protocol are sound and how the protocol may be used when implementing KMIP in applications. These test cases are not intended to fully test an implementation of KMIP.

1.1 References (non-normative)

- [KMIP-SPEC]** *Key Management Interoperability Protocol Specification Version 2.1*. Edited by Tony Cox and Charles White. Latest version: <https://docs.oasis-open.org/kmip/kmip-spec/v2.1/kmip-spec-v2.1.html>.
- [KMIP-PROFILES]** *Key Management Interoperability Protocol Profiles Version 2.1*. Edited by Tim Chevalier and Tim Hudson. Latest version: <https://docs.oasis-open.org/kmip/kmip-profiles/v2.1/kmip-profiles-v2.1.html>.
- [XML]** Extensible Markup Language (XML) 1.0 (Fifth Edition), T. Bray, J. Paoli, M. Sperberg-McQueen, E. Maler, F. Yergeau, Editors, W3C Recommendation, November 26, 2008, <http://www.w3.org/TR/2008/REC-xml-20081126/>. Latest version available at <http://www.w3.org/TR/xml/>.

2 KMIP Test Cases

The test cases define a number of request-response pairs for KMIP operations. Each test case is provided in the XML format specified in **[KMIP-PROFILES]** intended to be both human-readable and usable by automated tools.

Each test case has a unique label (the section name) with the protocol version as part of the identifier.

The test cases may depend on a specific configuration of a KMIP client and server being configured in a manner consistent with the test case assumptions.

Where possible, the flow of unique identifiers between tests, the date-time values, and other dynamic items are indicated using symbolic identifiers – in actual request and response messages these dynamic values will be filled in with valid values.

The test cases show one possible way to construct the messages, and the messages shown are not necessarily the only conformant constructions, as many items within KMIP are optional, and server behavior depends on the server's policy. Support for a test case is predicated on a server matching the test case assumptions and the behavior shown in the request-response pairs.

Symbolic identifiers are of the form \$UPPERCASE_NAME followed by an optional unique index value. Wherever a symbolic identifier occurs in a test cases, the implementation must replace it with a reasonable appearing datum of the expected type. Time values can be specified in terms of an offset from the current time in seconds of the form \$NOW or \$NOW-n or \$NOW+n.

2.1 TC-ASYNC-1-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-1-21.xml](#)

2.2 TC-ASYNC-2-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-2-21.xml](#)

2.3 TC-ASYNC-3-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-3-21.xml](#)

2.4 TC-ASYNC-4-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-4-21.xml](#)

2.5 TC-ASYNC-5-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-5-21.xml](#)

2.6 TC-ASYNC-6-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-6-21.xml](#)

2.7 TC-ASYNC-7-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-7-21.xml](#)

2.8 TC-ASYNC-8-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-8-21.xml](#)

2.9 TC-ASYNC-9-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-9-21.xml](#)

2.10 TC-ASYNC-10-21

Asynchronous test.

See [test-cases/kmip-v2.1/TC-ASYNC-10-21.xml](#)

2.11 TC-CERTATTR-1-21

A client registers a certificate and the server creates the certificate attributes based on the subject and issuer distinguished name values.

See [test-cases/kmip-v2.1/TC-CERTATTR-1-21.xml](#)

2.12 TC-CREATE-SD-1-21

A client requests a server to create a secret data managed object.

See [test-cases/kmip-v2.1/TC-CREATE-SD-1-21.xml](#)

2.13 TC-CS-CORVAL-1-21

A client sets a client correlation value and the server also responds with a server correlation value.

See [test-cases/kmip-v2.1/TC-CS-CORVAL-1-21.xml](#)

2.14 TC-DERIVEKEY-1-21

A client uses Derive Key with SHA_256.

See [test-cases/kmip-v2.1/TC-DERIVEKEY-1-21.xml](#)

2.15 TC-DERIVEKEY-2-21

A client uses Derive Key with HMAC-SHA_256.

See [test-cases/kmip-v2.1/TC-DERIVEKEY-2-21.xml](#)

2.16 TC-DERIVEKEY-3-21

A client uses Derive Key with PBKDF2.

See [test-cases/kmip-v2.1/TC-DERIVEKEY-3-21.xml](#)

2.17 TC-DERIVEKEY-4-21

A client uses Derive Key with PBKDF2.

See [test-cases/kmip-v2.1/TC-DERIVEKEY-4-21.xml](#)

2.18 TC-DERIVEKEY-5-21

A client uses Derive Key with PBKDF2 and SHA-256.

See [test-cases/kmip-v2.1/TC-DERIVEKEY-5-21.xml](#)

2.19 TC-DERIVEKEY-6-21

A client uses Derive Key with ASYMMETRIC_KEY and ECDH.

See [test-cases/kmip-v2.1/TC-DERIVEKEY-6-21.xml](#)

2.20 TC-DIGESTS-1-21

Multiple digests.

See [test-cases/kmip-v2.1/TC-DIGESTS-1-21.xml](#)

2.21 TC-DLOGIN-1-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-1-21.xml](#)

2.22 TC-DLOGIN-2-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-2-21.xml](#)

2.23 TC-DLOGIN-3-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-3-21.xml](#)

2.24 TC-DLOGIN-4-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-4-21.xml](#)

2.25 TC-DLOGIN-5-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-5-21.xml](#)

2.26 TC-DLOGIN-6-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-6-21.xml](#)

2.27 TC-DLOGIN-7-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-7-21.xml](#)

2.28 TC-DLOGIN-8-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-8-21.xml](#)

2.29 TC-DLOGIN-9-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-9-21.xml](#)

2.30 TC-DLOGIN-10-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-10-21.xml](#)

2.31 TC-DLOGIN-11-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-11-21.xml](#)

2.32 TC-DLOGIN-12-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-12-21.xml](#)

2.33 TC-DLOGIN-13-21

Delegated Login.

See [test-cases/kmip-v2.1/TC-DLOGIN-13-21.xml](#)

2.34 TC-ECC-1-21

A client registers an EC private key in ECPrivateKey format and an EC public key in X.509 format using the EC cryptographic algorithm.

See [test-cases/kmip-v2.1/TC-ECC-1-21.xml](#)

2.35 TC-ECC-2-21

A client registers an EC private key in PKCS8 format and an EC public key in X.509 format using the EC cryptographic algorithm.

See [test-cases/kmip-v2.1/TC-ECC-2-21.xml](#)

2.36 TC-ECC-3-21

A client registers an EC private key in ECPrivateKey format and an EC public key in X.509 format using the EC cryptographic algorithm.

See [test-cases/kmip-v2.1/TC-ECC-3-21.xml](#)

2.37 TC-ECDSA-SIGN-1-21

A client registers an EC private key in ECPrivateKey format and an EC public key in X.509 format using the EC cryptographic algorithm and performs a Sign operation followed by a Signature Verify operation.

See [test-cases/kmip-v2.1/TC-ECDSA-SIGN-1-21.xml](#)

2.38 TC-ECDSA-SIGN-DIGESTEDDATA 1-21

ECDSA Signing with the digested data provided by the client.

See [test-cases/kmip-v2.1/TC-ECDSA-SIGN-DIGESTEDDATA-1-21.xml](#)

2.39 TC-EXTRACTABLE-1-21

Show usage of Extractable and Never Extractable.

See [test-cases/kmip-v2.1/TC-EXTRACTABLE-1-21.xml](#)

2.40 TC-I18N-1-21

Client provides a key name containing a Greek capital Alpha.

Note: the encoding in XML has to be correctly converted into the valid UTF-8 format.

See [test-cases/kmip-v2.1/TC-I18N-1-21.xml](#)

2.41 TC-I18N-2-21

Client provides a key alternative name containing a Greek capital Alpha.

Note: the encoding in XML has to be correctly converted into the valid UTF-8 format.

See [test-cases/kmip-v2.1/TC-I18N-2-21.xml](#)

2.42 TC-I18N-3-21

Client provides a customer attribute containing a Greek capital Alpha with the attribute value containing a Greek capital Omega.

Note: the encoding in XML has to be correctly converted into the valid UTF-8 format.

See [test-cases/kmip-v2.1/TC-I18N-3-21.xml](#)

2.43 TC-IMPEXP-1-21

Import/Export.

See [test-cases/kmip-v2.1/TC-IMPEXP-1-21.xml](#)

2.44 TC-IMPEXP-2-21

Import/Export.

See [test-cases/kmip-v2.1/TC-IMPEXP-2-21.xml](#)

2.45 TC-IMPEXP-3-21

Import/Export.

See [test-cases/kmip-v2.1/TC-IMPEXP-3-21.xml](#)

2.46 TC-IMPEXP-4-21

Import/Export.

See [test-cases/kmip-v2.1/TC-IMPEXP-4-21.xml](#)

2.47 TC-IMPEXP-5-21

Import/Export.

See [test-cases/kmip-v2.1/TC-IMPEXP-5-21.xml](#)

2.48 TC-LOGIN-1-21

Login.

See [test-cases/kmip-v2.1/TC-LOGIN-1-21.xml](#)

2.49 TC-LOGIN-2-21

Login.

See [test-cases/kmip-v2.1/TC-LOGIN-2-21.xml](#)

2.50 TC-LOGIN-3-21

Login.

See [test-cases/kmip-v2.1/TC-LOGIN-3-21.xml](#)

2.51 TC-MD-1-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-1-21.xml](#)

2.52 TC-MD-2-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-2-21.xml](#)

2.53 TC-MD-3-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-3-21.xml](#)

2.54 TC-MD-4-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-4-21.xml](#)

2.55 TC-MD-5-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-5-21.xml](#)

2.56 TC-MD-6-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-6-21.xml](#)

2.57 TC-MD-21-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-21-21.xml](#)

2.58 TC-MD-22-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-22-21.xml](#)

2.59 TC-MD-23-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-23-21.xml](#)

2.60 TC-MD-24-21

Message digest testing.

See [test-cases/kmip-v2.1/TC-MD-24-21.xml](#)

2.61 TC-MDO-1-21

A client requests a meta-data-only object (no key material).

See [test-cases/kmip-v2.1/TC-MDO-1-21.xml](#)

2.62 TC-MDO-2-21

A client requests a meta-data-only object (no key material) and an object with key material and performs a Locate operation that only returns the meta-data-only object.

See [test-cases/kmip-v2.1/TC-MDO-2-21.xml](#)

2.63 TC-MDO-3-21

A client requests a meta-data-only object (no key material) using the URL format of the Key Value Location and performs Locate.

See <test-cases/kmip-v2.1/TC-MDO-3-21.xml>

2.64 TC-OFFSET-1-21

A client requests that the server create a number of symmetric keys and then uses the Offset parameter in Locate to return various items.

See <test-cases/kmip-v2.1/TC-OFFSET-1-21.xml>

2.65 TC-OFFSET-2-21

A client requests that the server create a number of symmetric keys and then uses the Offset parameter in Locate to return various items.

See <test-cases/kmip-v2.1/TC-OFFSET-2-21.xml>

2.66 TC-PGP-1-21

Register a PGP public key block and private key block and add appropriate links between the managed objects.

See <test-cases/kmip-v2.1/TC-PGP-1-21.xml>

2.67 TC-PING-1-21

Ping operation.

See <test-cases/kmip-v2.1/TC-PING-1-21.xml>

2.68 TC-PKCS12-1-21

Register objects and then perform a Get returning objects in PKCS#12 format.

See <test-cases/kmip-v2.1/TC-PKCS-12-1-21.xml>

2.69 TC-PKCS12-2-21

Register objects in PKCS#12 format and then perform a Get returning the individual objects.

See <test-cases/kmip-v2.1/TC-PKCS-12-2-21.xml>

2.70 TC-REENCRYPT-1-21

Re-encrypt.

See <test-cases/kmip-v2.1/TC-REENCRYPT-1-21.xml>

2.71 TC-REENCRYPT-2-21

Re-encrypt.

See [test-cases/kmip-v2.1/TC-REENCRYPT-2-21.xml](#)

2.72 TC-REENCRYPT-3-21

Re-encrypt.

See [test-cases/kmip-v2.1/TC-REENCRYPT-3-21.xml](#)

2.73 TC-REENCRYPT-4-21

Re-encrypt.

See [test-cases/kmip-v2.1/TC-REENCRYPT-4-21.xml](#)

2.74 TC-REENCRYPT-5-21

Re-encrypt.

See [test-cases/kmip-v2.1/TC-REENCRYPT-5-21.xml](#)

2.75 TC-REENCRYPT-6-21

Re-encrypt.

See [test-cases/kmip-v2.1/TC-REENCRYPT-6-21.xml](#)

2.76 TC-REKEY-1-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-1-21.xml](#)

2.77 TC-REKEY-2-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-2-21.xml](#)

2.78 TC-REKEY-3-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-3-21.xml](#)

2.79 TC-REKEY-4-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-4-21.xml](#)

2.80 TC-REKEY-5-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-5-21.xml](#)

2.81 TC-REKEY-6-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-6-21.xml](#)

2.82 TC-REKEY-7-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-7-21.xml](#)

2.83 TC-REKEY-8-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-8-21.xml](#)

2.84 TC-REKEY-9-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-9-21.xml](#)

2.85 TC-REKEY-10-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-10-21.xml](#)

2.86 TC-REKEY-11-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-11-21.xml](#)

2.87 TC-REKEY-12-21

Create a key and perform multiple rekey operations.

See [test-cases/kmip-v2.1/TC-REKEY-12-21.xml](#)

2.88 TC-RNG-ATTR-1-21

A client registers a symmetric key including details of the RNG that the client is claiming was used to generate the symmetric key.

See [test-cases/kmip-v2.1/TC-RNG-ATTR-1-21.xml](#)

2.89 TC-RNG-ATTR-2-21

A client requests that the server create a symmetric key. The server does and also includes the required details of the RNG that was used to generate the symmetric key.

See [test-cases/kmip-v2.1/TC-RNG-ATTR-2-21.xml](#)

2.90 TC-RSA-SIGN-DIGESTEDDATA 1-21

RSA Signing with the digested data provided by the client.

See [test-cases/kmip-v2.1/TC-RSA-SIGN-DIGESTEDDATA-1-21.xml](#)

2.91 TC-SENSITIVE-1-21

Show the usage of Sensitive and Always Sensitive.

See [test-cases/kmip-v2.1/TC-SENSITIVE-1-21.xml](#)

2.92 TC-SETTATTR-1-21

Show the usage of Set Attribute.

See [test-cases/kmip-v2.1/TC-SETATTR-1-21.xml](#)

2.93 TC-SETTATTR-2-21

Show the usage of Set Attribute.

See [test-cases/kmip-v2.1/TC-SETATTR-2-21.xml](#)

2.94 TC-SETTATTR-3-21

Show the usage of Set Attribute.

See [test-cases/kmip-v2.1/TC-SETATTR-3-21.xml](#)

2.95 TC-SJ-1-21

Create a symmetric key, performing split and join operations in various combinations.

See [test-cases/kmip-v2.1/TC-SJ-1-21.xml](#)

2.96 TC-SJ-2-21

Register a symmetric key, performing split and join operations in various combinations.

See [test-cases/kmip-v2.1/TC-SJ-2-21.xml](#)

2.97 TC-SJ-3-21

Register split keys and perform join operations in various combinations.

See [test-cases/kmip-v2.1/TC-SJ-2-21.xml](#)

2.98 TC-SJ-4-21

Create a symmetric key and perform split and join operations in various combinations using the XOR method.

See [test-cases/kmip-v2.1/TC-SJ-4-21.xml](#)

2.99 TC-STREAM-ENC-1-21

Create a symmetric key and perform encrypt with streaming.

See [test-cases/kmip-v2.1/TC-STREAM-ENC-1-21.xml](#)

2.100 TC-STREAM-ENC-2-21

Register a symmetric key and perform encrypt and decrypt with streaming.

See [test-cases/kmip-v2.1/TC-STREAM-ENC-2-21.xml](#)

2.101 TC-STREAM-ENCDEC-1-21

Register a symmetric key and perform encrypt with streaming.

See [test-cases/kmip-v2.1/TC-STREAM-ENCDEC-1-21.xml](#)

2.102 TC-STREAM-HASH-1-21

Hash operation for data 'abc' in a single request followed immediately by a streaming equivalent for which the result must be identical.

Note: - test vector data from http://csrc.nist.gov/groups/ST/toolkit/documents/Examples/SHA_All.pdf

See [test-cases/kmip-v2.1/TC-STREAM-HASH-1-21.xml](#)

2.103 TC-STREAM-HASH-2-21

Hash operation for data 'abc' in a single request followed immediately by a streaming equivalent for which the result must be identical.

Note: - test vector data from http://csrc.nist.gov/groups/ST/toolkit/documents/Examples/SHA_All.pdf

See [test-cases/kmip-v2.1/TC-STREAM-HASH-2-21.xml](#)

2.104 TC-STREAM-HASH-3-21

Hash operation for data 'abc' in a single request followed immediately by a streaming equivalent for which the result must be identical.

Note: - test vector data from http://csrc.nist.gov/groups/ST/toolkit/documents/Examples/SHA_All.pdf

See [test-cases/kmip-v2.1/TC-STREAM-HASH-3-21.xml](#)

2.105 TC-STREAM-MAC-1-21

MAC with streaming.

See [test-cases/kmip-v2.1/TC-STREAM-MAC-1-21.xml](#)

2.106 TC-STREAM-SIGN-1-21

Sign with a known asymmetric key with streaming.

See [test-cases/kmip-v2.1/TC-STREAM-SIGN-1-21.xml](#)

2.107 TC-STREAM-SIGNVFY-1-21

Sign and Signature Verify with a known asymmetric key with streaming.

See [test-cases/kmip-v2.1/TC-STREAM-SIGNVFY-1-21.xml](#)

2.108 TC-WRAP-1-21

Show usage of Key Wrap Type as Registered.

See [test-cases/kmip-v2.1/TC-WRAP-1-21.xml](#)

2.109 TC-WRAP-2-21

Show usage of Key Wrap Type as Not Wrapped.

See [test-cases/kmip-v2.1/TC-WRAP-2-21.xml](#)

2.110 TC-WRAP-3-21

Show usage of returning wrapped key wrapped with a different wrapping key.

See [test-cases/kmip-v2.1/TC-WRAP-3-21.xml](#)

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

Appendix B. Revision History

Revision	Date	Editor	Changes Made
wd02	30-Apr-2020	Tim Hudson	Updated test list from interop
wd01	28-Aug-2019	Tim Chevalier	Initial draft