

Key Management Interoperability Protocol Specification 1.0

Committee Draft 04

21 October 2009

Deleted: 3

Deleted: 1

Deleted: 4

Specification URIs:

This Version:

<http://docs.oasis-open.org/kmip/spec/v1.0/cd04/kmip-spec-1.0-draft-04.html>

<http://docs.oasis-open.org/kmip/spec/v1.0/cd04/kmip-spec-1.0-draft-04.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/spec/v1.0/cd04/kmip-spec-1.0-draft-04.pdf>

Deleted: 3

Deleted: 3

Deleted: 3

Previous Version:

<http://docs.oasis-open.org/kmip/spec/v1.0/cd03/kmip-spec-1.0-draft-03.html>

<http://docs.oasis-open.org/kmip/spec/v1.0/cd03/kmip-spec-1.0-draft-03.doc> (Authoritative)

<http://docs.oasis-open.org/kmip/spec/v1.0/cd03/kmip-spec-1.0-draft-03.pdf>

Deleted: 2

Deleted: 2

Deleted: 2

Latest Version:

<http://docs.oasis-open.org/kmip/spec/v1.0/kmip-spec-1.0.html>

<http://docs.oasis-open.org/kmip/spec/v1.0/kmip-spec-1.0.doc>

<http://docs.oasis-open.org/kmip/spec/v1.0/kmip-spec-1.0.pdf>

Deleted: -draft-04

Deleted: 3

Deleted: -draft-04

Deleted: 3

Deleted: -draft-043

Technical Committee:

OASIS Key Management Interoperability Protocol (KMIP) TC

Chair(s):

Robert Griffin

Subhash Sankuratirpati

Editor(s):

Robert Haas

Indra Fitzgerald

Related work:

This specification replaces or supersedes:

- None

This specification is related to:

- [Key Management Interoperability Protocol Profiles v1.0](http://docs.oasis-open.org/kmip/profiles/v1.0/), <http://docs.oasis-open.org/kmip/profiles/v1.0/>
- [Key Management Interoperability Protocol Use Cases v1.0](http://docs.oasis-open.org/kmip/usecases/v1.0/), <http://docs.oasis-open.org/kmip/usecases/v1.0/>
- [Key Management Interoperability Protocol Usage Guide v1.0](http://docs.oasis-open.org/kmip/ug/v1.0/), <http://docs.oasis-open.org/kmip/ug/v1.0/>

Deleted: TBD

Declared XML Namespace(s):

None

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 document was last revised or approved by the Key Management Interoperability Protocol TC on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved Version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at <http://www.oasis-open.org/committees/kmip/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/kmip/ipr.php>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/kmip/>.

Notices

Copyright © OASIS® 2009. 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.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names and abbreviations here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

Table of Contents

1 Introduction	8
1.1 Terminology	8
1.2 Normative References	11
1.3 Non-normative References	13
2 Objects	14
2.1 Base Objects	14
2.1.1 Attribute	14
2.1.2 Credential	15
2.1.3 Key Block	15
2.1.4 Key Value	16
2.1.5 Key Wrapping Data	17
2.1.6 Key Wrapping Specification	18
2.1.7 Transparent Key Structures	19
2.1.8 Template-Attribute Structures	23
2.2 Managed Objects	23
2.2.1 Certificate	24
2.2.2 Symmetric Key	24
2.2.3 Public Key	24
2.2.4 Private Key	24
2.2.5 Split Key	24
2.2.6 Template	26
2.2.7 Secret Data	27
2.2.8 Opaque Object	27
3 Attributes	28
3.1 Unique Identifier	28
3.2 Name	29
3.3 Object Type	30
3.4 Cryptographic Algorithm	30
3.5 Cryptographic Length	30
3.6 Cryptographic Parameters	31
3.7 Cryptographic Domain Parameters	32
3.8 Certificate Type	33
3.9 Certificate Identifier	33
3.10 Certificate Subject	34
3.11 Certificate Issuer	35
3.12 Digest	35
3.13 Operation Policy Name	36
3.13.1 Operations outside of operation policy control	37
3.13.2 Default Operation Policy	37
3.14 Cryptographic Usage Mask	39
3.15 Lease Time	41
3.16 Usage Limits	41
3.17 State	43

3.18 Initial Date	45
3.19 Activation Date	45
3.20 Process Start Date	46
3.21 Protect Stop Date	46
3.22 Deactivation Date	47
3.23 Destroy Date	48
3.24 Compromise Occurrence Date	48
3.25 Compromise Date	48
3.26 Revocation Reason	49
3.27 Archive Date	50
3.28 Object Group	50
3.29 Link	50
3.30 Application Specific Information	52
3.31 Contact Information	52
3.32 Last Change Date	53
3.33 Custom Attribute	53
4 Client-to-Server Operations	54
4.1 Create	55
4.2 Create Key Pair	56
4.3 Register	57
4.4 Re-key	59
4.5 Derive Key	61
4.6 Certify	63
4.7 Re-certify	64
4.8 Locate	66
4.9 Check	68
4.10 Get	70
4.11 Get Attributes	70
4.12 Get Attribute List	71
4.13 Add Attribute	71
4.14 Modify Attribute	72
4.15 Delete Attribute	72
4.16 Obtain Lease	73
4.17 Get Usage Allocation	74
4.18 Activate	75
4.19 Revoke	75
4.20 Destroy	76
4.21 Archive	76
4.22 Recover	76
4.23 Validate	77
4.24 Query	77
4.25 Cancel	79
4.26 Poll	80
5 Server-to-Client Operations	81
5.1 Notify	81

5.2 Put	81
6 Message Contents	83
6.1 Protocol Version	83
6.2 Operation	83
6.3 Maximum Response Size	83
6.4 Unique Batch Item ID	83
6.5 Time Stamp	84
6.6 Authentication	84
6.7 Asynchronous Indicator	84
6.8 Asynchronous Correlation Value	84
6.9 Result Status	85
6.10 Result Reason	85
6.11 Result Message	86
6.12 Batch Order Option	86
6.13 Batch Error Continuation Option	86
6.14 Batch Count	87
6.15 Batch Item	87
6.16 Message Extension	87
7 Message Format	88
7.1 Message Structure	88
7.2 Synchronous Operations	88
7.3 Asynchronous Operations	89
8 Authentication	92
9 Message Encoding	93
9.1 TTLV Encoding	93
9.1.1 TTLV Encoding Fields	93
9.1.2 Examples	95
9.1.3 Defined Values	96
9.2 XML Encoding	115
10 Transport	116
11 Error Handling	117
11.1 General	117
11.2 Create	117
11.3 Create Key Pair	118
11.4 Register	118
11.5 Re-key	119
11.6 Derive Key	120
11.7 Certify	120
11.8 Re-certify	121
11.9 Locate	121
11.10 Check	121
11.11 Get	122
11.12 Get Attributes	122
11.13 Get Attribute List	122
11.14 Add Attribute	123

11.15 Modify Attribute	123
11.16 Delete Attribute	124
11.17 Obtain Lease.....	124
11.18 Get Usage Allocation.....	124
11.19 Activate	125
11.20 Revoke.....	125
11.21 Destroy.....	125
11.22 Archive	126
11.23 Recover.....	126
11.24 Validate	126
11.25 Query	126
11.26 Cancel.....	126
11.27 Poll.....	126
11.28 Batch Items	126
12 Implementation Conformance.....	128
12.1 Conformance clauses for a KMIP Server	128
A. Attribute Cross-reference	130
B. Tag Cross-reference	132
C. Operation and Object Cross-reference	137
D. Acronyms.....	138
E. List of Figures and Tables.....	141
F. Acknowledgements	148
G. Revision History.....	150

1 Introduction

This document is intended as a specification of the protocol used for the communication between clients and servers to perform certain management operations on objects stored and maintained by a key management system. These objects are referred to as *Managed Objects* in this specification. They include symmetric and asymmetric cryptographic keys, digital certificates, and templates used to simplify the creation of objects and control their use. Managed Objects are managed with *operations* that include the ability to generate cryptographic keys, register objects with the key management system, obtain objects from the system, destroy objects from the system, and search for objects maintained by the system. Managed Objects also have associated *attributes*, which are named values stored by the key management system and are obtained from the system via operations. Certain attributes are added, modified, or deleted by operations.

The protocol specified in this document includes several certificate-related functions for which there are a number of existing protocols – namely Validate (e.g., SVP or XKMS), Certify (e.g. CMP, CMC, SCEP) and Re-certify (e.g. CMP, CMC, SCEP). The protocol does not attempt to define a comprehensive certificate management protocol such as would be needed for a certification authority. However, it does include functions that are needed to allow a key server to provide a proxy for certificate management functions.

In addition to the normative definitions for managed objects, operations and attributes, this specification also includes normative definitions for the following aspects of the protocol:

- The expected behavior of the server and client as a result of operations
- Message contents and formats
- Message encoding (including enumerations)
- Error handling

This specification is complemented by three other documents. The Usage Guide **[KMIP-UG]** provides illustrative information on using the protocol. The KMIP Profiles Specification **[KMIP-Prof]** provides a selected set of conformance profiles and authentication suites. The Test Specification **[KMIP-UC]** provides samples of protocol messages corresponding to a set of defined test cases.

This specification defines the KMIP protocol version major 1 and minor 0 (see 6.1).

1.1 Terminology

The key words "SHALL", "SHALL NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. The words 'must', 'can', and 'will' are forbidden.

For definitions not found in this [document](#), see **[SP800-57-1]**.

Deleted: standard

Archive	To place information not accessed frequently into long-term storage
Asymmetric key pair (key pair)	A public key and its corresponding private key; a key pair is used with a public key algorithm
Authentication	A process that establishes the origin of information, or determines an entity's identity.
Authentication code	A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code).
Authorization	Access privileges that are granted to an entity; conveying an "official" sanction to perform a security function or activity.

<u>Certification authority</u>	<u>The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates, and exacting compliance to a PKI policy.</u>
<u>Ciphertext</u>	<u>Data in its encrypted form.</u>
<u>Compromise</u>	<u>The unauthorized disclosure, modification, substitution or use of sensitive data (e.g., keying material and other security related information).</u>
<u>Confidentiality</u>	<u>The property that sensitive information is not disclosed to unauthorized entities.</u>
<u>Cryptographic algorithm</u>	<u>A well-defined computational procedure that takes variable inputs including a cryptographic key and produces an output.</u>
<u>Cryptographic key (key)</u>	<u>A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Examples include:</u> <ol style="list-style-type: none"> <u>1. The transformation of plaintext data into ciphertext data.</u> <u>2. The transformation of ciphertext data into plaintext data.</u> <u>3. The computation of a digital signature from data.</u> <u>4. The verification of a digital signature.</u> <u>5. The computation of an authentication code from data.</u> <u>6. The verification of an authentication code from data and a received authentication code.</u>
<u>Decryption</u>	<u>The process of changing ciphertext into plaintext using a cryptographic algorithm and key.</u>
<u>Digest (or hash)</u>	<u>The result of applying a hash function to information.</u>
<u>Digital signature (signature)</u>	<u>The result of a cryptographic transformation of data that, when properly implemented with supporting infrastructure and policy, provides the services of:</u> <ol style="list-style-type: none"> <u>1. origin authentication</u> <u>2. data integrity, and</u> <u>3. signer non-repudiation.</u>
<u>Encryption</u>	<u>The process of changing plaintext into ciphertext using a cryptographic algorithm and key.</u>
<u>Hash function</u>	<u>A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:</u> <ol style="list-style-type: none"> <u>1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and</u> <u>2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.</u>
<u>Integrity</u>	<u>The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.</u>
<u>Key derivation (derivation)</u>	<u>A function in the lifecycle of keying material; the process by which one or more keys are derived from a shared secret and other information.</u>

<u>Key management</u>	<u>The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.</u>
<u>Key wrapping (wrapping)</u>	<u>A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key.</u>
<u>Message authentication code (MAC)</u>	<u>A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data.</u>
<u>Private key</u>	<u>A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used to:</u> <u>1. Compute the corresponding public key.</u> <u>2. Compute a digital signature that may be verified by the corresponding public key.</u> <u>3. Decrypt data that was encrypted by the corresponding public key, or</u> <u>4. Compute a piece of common shared data, together with other information.</u>
<u>Profile</u>	<u>A specification of objects, attributes, operations, message elements and authentication methods to be used in specific contexts of key management server and client interactions (see [KMIP-Prof]).</u>
<u>Public key</u>	<u>A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used to:</u> <u>1. Verify a digital signature that is signed by the corresponding private key.</u> <u>2. Encrypt data that can be decrypted by the corresponding private key, or</u> <u>3. Compute a piece of shared data.</u>
<u>Public key certificate (certificate)</u>	<u>A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity.</u>
<u>Public key cryptographic algorithm</u>	<u>A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that determining the private key from the public key is computationally infeasible.</u>
<u>Public Key Infrastructure</u>	<u>A framework that is established to issue, maintain and revoke public key certificates.</u>
<u>Recover</u>	<u>To retrieve information that was archived to long-term storage.</u>
<u>Split knowledge</u>	<u>A process by which a cryptographic key is split into n multiple key components, individually providing no knowledge of the original key, which can be subsequently combined to recreate the original cryptographic key. If knowledge of k (where k is less than or equal to n) components is required to construct the original key, then knowledge of</u>

	<u>any $k-1$ key components provides no information about the original key other than, possibly, its length.</u>
<u>Symmetric key</u>	<u>A single cryptographic key that is used with a secret (symmetric) key algorithm.</u>
<u>Symmetric key algorithm</u>	<u>A cryptographic algorithm that uses the same secret (symmetric) key for an operation and its complement (e.g., encryption and decryption).</u>
<u>X.509 certificate</u>	<u>The ISO/ITU-T X.509 standard defined two types of certificates – the X.509 public key certificate, and the X.509 attribute certificate. Most commonly (including this document), an X.509 certificate refers to the X.509 public key certificate.</u>
<u>X.509 public key certificate</u>	<u>The public key for a user (or device) and a name for the user (or device), together with some other information, rendered un-forgable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.</u>

33

34 1.2 Normative References

35 **[FIPS186-3]** *Digital Signature Standard (DSS)*, FIPS PUB 186-3, June 2009,
36 http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

37 **[FIPS197]** *Advanced Encryption Standard*, FIPS PUB 197, Nov 2001,
38 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

39 **[FIPS198-1]** *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS PUB 198-1, July
40 2008, http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

41 **[IEEE1003-1]** IEEE Std 1003.1, *Standard for information technology - portable operating
42 system interface (POSIX). Shell and utilities*, 2004.

43 **[ISO16609]** ISO, *Banking -- Requirements for message authentication using symmetric
44 techniques*, ISO 16609, 1991

45 **[ISO9797-1]** ISO/IEC, *Information technology -- Security techniques -- Message
46 Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher*,
47 ISO/IEC 9797-1, 1999.

48 **[KMIP-Prof]** OASIS Draft, *Key Management Interoperability Protocol Profiles v1.0*, Committee
49 Draft, October 2009.

50 **[PKCS#1]** RSA Laboratories, *PKCS #1 v2.1: RSA Cryptography Standard*, June 14, 2002.
51 <http://www.rsa.com/rsalabs/node.asp?id=2125>

52 **[PKCS#5]** RSA Laboratories, *PKCS #5 v2.1: Password-Based Cryptography Standard*,
53 October 5, 2006. <http://www.rsa.com/rsalabs/node.asp?id=2127>

54 **[PKCS#7]** RSA Laboratories, *PKCS#7 v1.5: Cryptographic Message Syntax Standard*.
55 November 1, 1993. <http://www.rsa.com/rsalabs/node.asp?id=2129>

56 **[PKCS#8]** RSA Laboratories, *PKCS#8 v1.2: Private-Key Information Syntax Standard*,
57 November 1, 1993. <http://www.rsa.com/rsalabs/node.asp?id=2130>

58 **[PKCS#10]** RSA Laboratories, *PKCS #10 v1.7: Certification Request Syntax Standard*, May
59 26, 2000. <http://www.rsa.com/rsalabs/node.asp?id=2132>

60 **[RFC1319]** B. Kaliski, *The MD2 Message-Digest Algorithm*, IETF RFC 1319, Apr 1992,
61 <http://www.ietf.org/rfc/rfc1319.txt>

62 **[RFC1320]** R. Rivest, *The MD4 Message-Digest Algorithm*, IETF RFC 1320, Apr 1992,
63 <http://www.ietf.org/rfc/rfc1320.txt>

64 **[RFC1321]** R. Rivest, *The MD5 Message-Digest Algorithm*, IETF RFC 1321, Apr 1992,
65 <http://www.ietf.org/rfc/rfc1321.txt>

Deleted: Specification

Deleted: 01

Deleted: , URI (TBD)

- 66 [RFC1421] J. Linn, *Privacy Enhancement for Internet Electronic Mail: Part I: Message*
67 *Encryption and Authentication Procedures*, IETF RFC 1421, Feb 1993,
68 <http://www.ietf.org/rfc/rfc1421.txt>
- 69 [RFC1424] B. Kaliski, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key*
70 *Certification and Related Services*, IETF RFC 1424, February 1993.
71 <http://www.ietf.org/rfc/rfc1424.txt>
- 72 [RFC2104] H. Krawczyk, M. Bellare, R. Canetti, *HMAC: Keyed-Hashing for Message*
73 *Authentication*, IETF RFC 2104. Feb 1007, <http://www.ietf.org/rfc/rfc2104.txt>
- 74 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
75 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 76 [RFC2898] B. Kaliski, *PKCS #5: Password-Based Cryptography Specification Version 2.0*,
77 IETF RFC 2898, Sep 2000, <http://www.ietf.org/rfc/rfc2898.txt>
- 78 [RFC 3394] J. Schaad, R. Housley, *Advanced Encryption Standard (AES) Key Wrap*
79 *Algorithm*, IETF RFC 3394, Sep 2002, <http://www.ietf.org/rfc/rfc3394.txt>
- 80 [RFC3447] J. Jonsson, B. Kaliski, *Public-Key Cryptography Standards (PKCS) #1: RSA*
81 *Cryptography Specifications Version 2.1*, IETF RFC 3447 Feb 2003,
82 <http://www.ietf.org/rfc/rfc3447.txt>
- 83 [RFC3629] F. Yergeau, *UTF-8, a transformation format of ISO 10646*, IETF RFC 3629, Nov
84 2003, <http://www.ietf.org/rfc/rfc3629.txt>
- 85 [RFC3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, *Internet X.509 Public Key*
86 *Infrastructure Certificate Policy and Certification Practices Framework*, IETF RFC
87 3647, November 2003. <http://www.ietf.org/rfc/rfc3647.txt>
- 88 [RFC4210] C. Adams, S. Farrell, T. Kause and T. Mononen, *Internet X.509 Public Key*
89 *Infrastructure Certificate Management Protocol (CMP)*, IETF RFC 2510,
90 September 2005. <http://www.ietf.org/rfc/rfc4210.txt>
- 91 [RFC4211] J. Schaad, *Internet X.509 Public Key Infrastructure Certificate Request Message*
92 *Format (CRMF)*, IETF RFC 4211, Sep 2005, <http://www.ietf.org/rfc/rfc4211.txt>
- 93 [RFC4868] S. Kelly, S. Frankel, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-*
94 *512 with IPsec*, IETF RFC 4868, May 2007, <http://www.ietf.org/rfc/rfc4868.txt>
- 95 [RFC4949] R. Shirey, *Internet Security Glossary, Version 2*, IETF RFC 4949, August 2007.
96 <http://www.ietf.org/rfc/rfc4949.txt>
- 97 [RFC5272] J. Schaad and M. Meyers, *Certificate Management over CMS (CMC)*, IETF RFC
98 5272, June 2008. <http://www.ietf.org/rfc/rfc5272.txt>
- 99 [RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, *Internet*
100 *X.509 Public Key Infrastructure Certificate*, IETF RFC 5280, May 2008,
101 <http://www.ietf.org/rfc/rfc5280.txt>
- 102 [RFC5649] R. Housley, *Advanced Encryption Standard (AES) Key Wrap with Padding*
103 *Algorithm*, IETF RFC 5649, Aug 2009, <http://www.ietf.org/rfc/rfc5649.txt>
- 104 [SP800-38A] M. Dworkin, *Recommendation for Block Cipher Modes of Operation – Methods*
105 *and Techniques*, NIST Special Publication 800-38A, Dec 2001,
106 <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>
- 107 [SP800-38B] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: The CMAC*
108 *Mode for Authentication*, NIST Special Publication 800-38B, May 2005,
109 http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
- 110 [SP800-38C] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: the CCM*
111 *Mode for Authentication and Confidentiality*, NIST Special Publication 800-38C,
112 May 2004, [http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-](http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf)
113 [38C_updated-July20_2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf)
- 114 [SP800-38D] M. Dworkin, *Recommendation for Block Cipher Modes of Operation:*
115 *Galois/Counter Mode (GCM) and GMAC*, NIST Special Publication 800-38D, Nov
116 2007, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>
- 117 [SP800-38E] M. Dworkin, *Recommendation for Block Cipher Modes of Operation: The XTS-*
118 *AES Mode for Confidentiality on Block-Oriented Storage Devices*, NIST Special

119 Publication 800-38E, Aug 2009 (draft), <http://csrc.nist.gov/publications/drafts/800-38E/draft-sp800-38E.pdf>

120

121 **[SP800-57-1]** E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, *Recommendations for Key Management - Part 1: General (Revised)*, NIST Special Publication 800-57 part 1, March 2007, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

122

123

124

125 **[SP800-67]** W. Barker, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67, Version 1.1, Revised 19 May 2008, <http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf>

126

127

128 **[SP800-108]** L. Chen, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, NIST Special Publication 800-108, October 2009, <http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf>

129

130

131 **[X.509]** International Telecommunication Union (ITU)-T, X.509: *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*, August 2005. <http://www.itu.int/rec/T-REC-X.509-200508-1/en>

132

133

134

135 **[X9.24-1]** ANSI, X9.24 - *Retail Financial Services Symmetric Key Management - Part 1: Using Symmetric Techniques*, 2004.

136

137 **[X9.26]** ANSI, X9.26 - *Financial Institution Sign-On Authentication for Wholesale Financial Transaction*, 1996.

138

139 **[X9.31]** ANSI, X9.31-1992: *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Part 2: The MDC-2 Hash Algorithm*, June 1993.

140

141 **[X9.42]** ANSI, X9-42: *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*, 2003.

142

143 **[X9-57]** ANSI, X9-57: *Public Key Cryptography for the Financial Services Industry: Certificate Management*, 1997.

144

145 **[X9.62]** ANSI, X9-62: *Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 2005.

146

147 **[X9-63]** ANSI, X9-63: *Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography*, 2001.

148

149 **[X9-102]** ANSI, X9-102: *Symmetric Key Cryptography for the Financial Services Industry - Wrapping of Keys and Associated Data*, 2008.

150

151 **[X9 TR-31]** ANSI, X9 TR-31: *Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*, 2005.

152

153

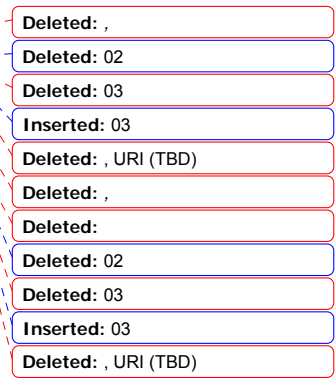
154 **1.3 Non-normative References**

155 **[KMIP-UG]** OASIS Draft, *Key Management Interoperability Protocol Usage Guide v1.0*,
 156 Committee Draft, October 2009.

157 **[KMIP-UC]** OASIS Draft, *Key Management Interoperability Protocol Use Cases v1.0*,
 158 Committee Draft, October 2009.

159 **[ISO/IEC 9945-2]** The Open Group, *Regular Expressions, The Single UNIX Specification version 2*,
 160 1997, ISO/IEC 9945-2:1993,
 161 <http://www.opengroup.org/onlinepubs/007908799/xbd/re.html>

162



163 2 Objects

164 The following subsections describe the objects that are passed between the clients and servers of the key
165 management system. Some of these object types, called *Base Objects*, are used only in the protocol
166 itself, and are not considered Managed Objects. Key management systems MAY choose to support a
167 subset of the Managed Objects. The object descriptions refer to the primitive data types of which they are
168 composed. These primitive data types are

- 169 • Integer
- 170 • Long Integer
- 171 • Big Integer
- 172 • Enumeration – choices from a predefined list of values
- 173 • Boolean
- 174 • Text String – string of characters representing human-readable text
- 175 • Byte String – sequence of unencoded byte values
- 176 • Date-Time – date and time, with a granularity of one second
- 177 • Interval – time interval expressed in seconds

178 Structures are composed of ordered lists of primitive data types or structures.

179 2.1 Base Objects

180 These objects are used within the messages of the protocol, but are not objects managed by the key
181 management system. They are components of Managed Objects.

182 2.1.1 Attribute

183 An Attribute object is a structure (see [Table 1](#)) used for sending and receiving Managed Object attributes.
184 The *Attribute Name* is a text-string that is used to identify the attribute. The *Attribute Index* is an index
185 number assigned by the key management server when a specified named attribute is allowed to have
186 multiple instances. The *Attribute Index* is used to identify the particular instance. Attribute Indices SHALL
187 start with 0. The *Attribute Index* of an attribute SHALL NOT change when other instances are added or
188 deleted. For example, if a particular attribute has 4 instances with Attribute Indices 0, 1, 2 and 3, and the
189 instance with Attribute Index 2 is deleted, then the *Attribute Index* of instance 3 is not changed. Attributes
190 that have a single instance have an *Attribute Index* of 0, which is assumed if the *Attribute Index* is not
191 specified. The *Attribute Value* is either a primitive data type or structured object, depending on the
192 attribute.

Deleted: Table 1

Object	Encoding	REQUIRED
Attribute	Structure	
Attribute Name	Text String	Yes
Attribute Index	Integer	No
Attribute Value	Varies, depending on attribute. See Section 3	Yes

193 **Table 1: Attribute Object Structure**

194 **2.1.2 Credential**

195 | A *Credential* is a structure (see [Table 2](#)) used for client identification purposes and is not managed by the
196 | key management system (e.g., user id/password pairs, Kerberos tokens, etc). It MAY be used for
197 | authentication purposes as indicated in **[KMIP-Prof]**.

Deleted: Table 2

Object	Encoding	REQUIRED
Credential	Structure	
Credential Type	Enumeration, see 9.1.3.2.1	Yes
Credential Value	Byte String	Yes

198 **Table 2: Credential Object Structure**

199 **2.1.3 Key Block**

200 | A *Key Block* object is a structure (see [Table 3](#)) used to encapsulate all of the information that is closely
201 | associated with a cryptographic key. It contains a Key Value of one of the following *Key Format Types*:

Deleted: Table 3

- 202 • *Raw* – This is a key that contains only cryptographic key material, encoded as a string of bytes.
- 203 • *Opaque* – This is an encoded key for which the encoding is unknown to the key management
204 | system. It is encoded as a string of bytes.
- 205 • *PKCS1* – This is an encoded private key, expressed as a DER-encoded ASN.1 PKCS#1 object.
- 206 • *PKCS8* – This is an encoded private key, expressed as a DER-encoded ASN.1 PKCS#8 object,
207 | supporting both RSAPrivateKey syntax and EncryptedPrivateKey.
- 208 • *X.509* – This is an encoded object, expressed as a DER-encoded ASN.1 X.509 object.
- 209 • *ECPrivateKey* – This is an ASN.1 encoded elliptic curve private key.
- 210 • *Several Transparent Key types* – These are algorithm-specific structures containing defined
211 | values for the various key types, as defined in Section 2.1.7
- 212 • *Extensions* – These are vendor-specific extensions to allow for proprietary or legacy key formats.

213 The Key Block MAY contain the Key Compression Type, which indicates the format of the elliptic curve
214 | public key. By default, the public key is uncompressed.

215 The Key Block also has the Cryptographic Algorithm and the Cryptographic Length of the key contained
216 | in the Key Value field. Some example values are:

- 217 • RSA keys are typically 1024, 2048 or 3072 bits in length
- 218 • 3DES keys are typically 168 bits in length
- 219 • AES keys are typically 128 or 256 bits in length

220 The Key Block SHALL contain a Key Wrapping Data structure if the key in the Key Value field is wrapped
221 | (i.e., encrypted, or MACed/signed, or both).

Object	Encoding	REQUIRED
Key Block	Structure	
Key Format Type	Enumeration, see 9.1.3.2.3	Yes
Key Compression Type	Enumeration, see 9.1.3.2.2	No
Key Value	Byte String: for wrapped Key Value; Structure: for plaintext Key Value, see 2.1.4	Yes
Cryptographic Algorithm	Enumeration, see 9.1.3.2.12	Yes, MAY be omitted only if this information is available from the Key Value. Does not apply to Secret Data or Opaque Objects. If present, Cryptographic Length SHALL also be present.
Cryptographic Length	Integer	Yes, MAY be omitted only if this information is available from the Key Value. Does not apply to Secret Data or Opaque Objects. If present, Cryptographic Algorithm SHALL also be present.
Key Wrapping Data	Structure, see 2.1.5	No, SHALL only be present if the key is wrapped.

222

Table 3: Key Block Object Structure

223 **2.1.4 Key Value**

224 The *Key Value* is used only inside a Key Block and is either a Byte String or a structure (see [Table 4](#)):

Deleted: Table 4

- 225 • The Key Value structure contains the key material, either as a byte string or as a Transparent Key
- 226 structure (see Section 2.1.7), and OPTIONAL attribute information that is associated and
- 227 encapsulated with the key material. This attribute information differs from the attributes
- 228 associated with Managed Objects, and which is obtained via the Get Attributes operation, only by
- 229 the fact that it is encapsulated with (and possibly wrapped with) the key material itself.
- 230 • The Key Value Byte String is the wrapped TTLV-encoded (see Section 9.1) Key Value structure.

Object	Encoding	REQUIRED
Key Value	Structure	
Key Material	Byte String; for Raw, Opaque, PKCS1, PKCS8, ECPrivateKey, or Extension Key Format types; Structure: for Transparent, or Extension Key Format Types	Yes
Attribute	Attribute Object, see Section 2.1.1	No. MAY be repeated

Table 4: Key Value Object Structure

231

232 2.1.5 Key Wrapping Data

233 The Key Block MAY also supply OPTIONAL information about a cryptographic key wrapping mechanism
 234 used to wrap the Key Value. This consists of a *Key Wrapping Data* structure (see [Table 5](#)). It is only used
 235 inside a Key Block.

Deleted: Table 5

236 This structure contains fields for:

- 237 • A *Wrapping Method*, which indicates the method used to wrap the Key Value.
- 238 • *Encryption Key Information*, which contains the Unique Identifier ([see 3.1](#)) value of the encryption
 239 key and associated cryptographic parameters.
- 240 • *MAC/Signature Key Information*, which contains the Unique Identifier value of the MAC/signature
 241 key and associated cryptographic parameters.
- 242 • A *MAC/Signature*, which contains a MAC or signature of the Key Value.
- 243 • An *IV/Counter/Nonce*, if REQUIRED by the wrapping method.

244 If wrapping is used, then the whole Key Value structure is wrapped unless otherwise specified by the
 245 Wrapping Method. The algorithms used for wrapping are given by the Cryptographic Algorithm attributes
 246 of the encryption key and/or MAC/signature key; the block-cipher mode, padding method, and hashing
 247 algorithm used for wrapping are given by the Cryptographic Parameters in the Encryption Key Information
 248 and/or MAC/Signature Key Information, or, if not present, from the Cryptographic Parameters attribute of
 249 the respective key(s). At least one of the Encryption Key Information and the MAC/Signature Key
 250 Information SHALL be specified.

251 The following wrapping methods are currently defined:

- 252 • *Encrypt* only (i.e., encryption using a symmetric key or public key, or authenticated encryption
 253 algorithms that use a single key)
- 254 • *MAC/sign* only (i.e., either MACing the Key Value with a symmetric key, or signing the Key Value
 255 with a private key)
- 256 • *Encrypt then MAC/sign*
- 257 • *MAC/sign then encrypt*
- 258 • *TR-31*
- 259 • *Extensions*

Object	Encoding	REQUIRED
Key Wrapping Data	Structure	
Wrapping Method	Enumeration, see 9.1.3.2.4	Yes
Encryption Key Information	Structure, see below	No. Corresponds to the key that was used to encrypt the Key Value.
MAC/Signature Key Information	Structure, see below	No. Corresponds to the symmetric key used to MAC the Key Value or the private key used to sign the Key Value
MAC/Signature	Byte String	No
IV/Counter/Nonce	Byte String	No

Table 5: Key Wrapping Data Object Structure

261 The structures of the Encryption Key Information (see [Table 6](#)) and the MAC/Signature Key Information
 262 (see [Table 7](#)) are as follows:

Deleted: Table 6

Deleted: Table 7

Object	Encoding	REQUIRED
Encryption Key Information	Structure	
Unique Identifier	Text string, see 3.1	Yes
Cryptographic Parameters	Structure, see 3.6	No

Table 6: Encryption Key Information Object Structure

263

Object	Encoding	REQUIRED
MAC/Signature Key Information	Structure	
Unique Identifier	Text string, see 3.1	Yes. It SHALL be either the Unique Identifier of the Symmetric Key used to MAC, or of the Private Key (or its corresponding Public Key) used to sign.
Cryptographic Parameters	Structure, see 3.6	No

Table 7: MAC/Signature Key Information Object Structure

264

265 2.1.6 Key Wrapping Specification

266 This is a separate structure (see [Table 8](#)) that is defined for operations that provide the option to return
 267 wrapped keys. The *Key Wrapping Specification* SHALL be included inside the operation request if clients
 268 request the server to return a wrapped key. If Cryptographic Parameters are specified in the Encryption
 269 Key Information and/or the MAC/Signature Key Information, then the server SHALL verify that they match
 270 one of the instances of the Cryptographic Parameters attribute of the corresponding key. If Cryptographic
 271 Parameters are omitted, then the server SHALL use the Cryptographic Parameters attribute with the
 272 lowest Attribute Index of the corresponding key. If the corresponding key does not have any
 273 Cryptographic Parameters attribute, or if no match is found, then an error is returned.

Deleted: Table 8

274 This structure contains:

- 275 • A Wrapping Method that indicates the method used to wrap the Key Value.
- 276 • An Encryption Key Information with the Unique Identifier value of the encryption key and
277 associated cryptographic parameters.
- 278 • A MAC/Signature Key Information with the Unique Identifier value of the MAC/signature key and
279 associated cryptographic parameters.
- 280 • Zero or more Attribute Names to indicate the attributes to be wrapped with the key material.

Object	Encoding	REQUIRED
Key Wrapping Specification	Structure	
Wrapping Method	Enumeration, see 9.1.3.2.4	Yes
Encryption Key Information	Structure, see 2.1.5	No, SHALL be present if MAC/Signature Key Information is omitted
MAC/Signature Key Information	Structure, see 2.1.5	No, SHALL be present if Encryption Key Information is omitted
Attribute Name	Text String	No, MAY be repeated

281 **Table 8: Key Wrapping Specification Object Structure**

282 2.1.7 Transparent Key Structures

283 *Transparent Key* structures describe key material in a form that is easily interpreted by all participants in
284 the protocol. They are used in the Key Value structure.

285 2.1.7.1 Transparent Symmetric Key

286 If the Key Format Type in the Key Block is *Transparent Symmetric Key*, then Key Material is a structure
287 as shown in [Table 9](#).

Deleted: Table 9

Object	Encoding	REQUIRED
Key Material	Structure	
Key	Byte String	Yes

288 **Table 9: Key Material Object Structure for Transparent Symmetric Keys**

289 2.1.7.2 Transparent DSA Private Key

290 If the Key Format Type in the Key Block is *Transparent DSA Private Key*, then Key Material is a structure
291 as shown in [Table 10](#).

Deleted: Table 10

Object	Encoding	REQUIRED
Key Material	Structure	
P	Big Integer	Yes
Q	Big Integer	Yes
G	Big Integer	Yes
X	Big Integer	Yes

292 **Table 10: Key Material Object Structure for Transparent DSA Private Keys**

293 P is the prime modulus. Q is the prime divisor of P-1. G is the generator. X is the private key (refer to
294 NIST FIPS PUB 186-3).

295 2.1.7.3 Transparent DSA Public Key

296 If the Key Format Type in the Key Block is *Transparent DSA Public Key*, then Key Material is a structure
297 as shown in [Table 11](#).

Deleted: Table 11

Object	Encoding	REQUIRED
Key Material	Structure	
P	Big Integer	Yes
Q	Big Integer	Yes
G	Big Integer	Yes
Y	Big Integer	Yes

298 **Table 11: Key Material Object Structure for Transparent DSA Public Keys**

299 P is the prime modulus. Q is the prime divisor of P-1. G is the generator. Y is the public key (refer to NIST
300 FIPS PUB 186-3).

301 2.1.7.4 Transparent RSA Private Key

302 If the Key Format Type in the Key Block is *Transparent RSA Private Key*, then Key Material is a structure
303 as shown in [Table 12](#).

Deleted: Table 12

Object	Encoding	REQUIRED
Key Material	Structure	
Modulus	Big Integer	Yes
Private Exponent	Big Integer	No
Public Exponent	Big Integer	No
P	Big Integer	No
Q	Big Integer	No
Prime Exponent P	Big Integer	No
Prime Exponent Q	Big Integer	No
CRT Coefficient	Big Integer	No

304 **Table 12: Key Material Object Structure for Transparent RSA Private Keys**

305 One of the following SHALL be present (refer to RSA PKCS#1):

- 306 • Private Exponent
- 307 • P and Q (the first two prime factors of Modulus)
- 308 • Prime Exponent P and Prime Exponent Q.

309 2.1.7.5 Transparent RSA Public Key

310 If the Key Format Type in the Key Block is *Transparent RSA Public Key*, then Key Material is a structure
311 as shown in [Table 13](#).

Deleted: Table 13

Object	Encoding	REQUIRED
Key Material	Structure	
Modulus	Big Integer	Yes
Public Exponent	Big Integer	Yes

312 **Table 13: Key Material Object Structure for Transparent RSA Public Keys**

313 2.1.7.6 Transparent DH Private Key

314 If the Key Format Type in the Key Block is *Transparent DH Private Key*, then Key Material is a structure
 315 as shown in [Table 14](#).

Deleted: Table 14

Object	Encoding	REQUIRED
Key Material	Structure	
P	Big Integer	Yes
G	Big Integer	Yes
Q	Big Integer	No
J	Big Integer	No
X	Big Integer	Yes

316 **Table 14: Key Material Object Structure for Transparent DH Private Keys**

317 P is the prime, $P = JQ + 1$. G is the generator $G^Q = 1 \text{ mod } P$. Q is the prime factor of $P-1$. J is the
 318 OPTIONAL cofactor. X is the private key (refer to ANSI X9.42).

319 2.1.7.7 Transparent DH Public Key

320 If the Key Format Type in the Key Block is *Transparent DH Public Key*, then Key Material is a structure as
 321 shown in [Table 15](#).

Deleted: Table 15

Object	Encoding	REQUIRED
Key Material	Structure	
P	Big Integer	Yes
G	Big Integer	Yes
Q	Big Integer	No
J	Big Integer	No
Y	Big Integer	Yes

322 **Table 15: Key Material Object Structure for Transparent DH Public Keys**

323 P is the prime, $P = JQ + 1$. G is the generator $G^Q = 1 \text{ mod } P$. Q is the prime factor of $P-1$. J is the
 324 OPTIONAL cofactor. Y is the public key (refer to ANSI X9.42).

325 2.1.7.8 Transparent ECDSA Private Key

326 If the Key Format Type in the Key Block is *Transparent ECDSA Private Key*, then Key Material is a
 327 structure as shown in [Table 16](#).

Deleted: Table 16

Object	Encoding	REQUIRED
Key Material	Structure	
Recommended Curve	Enumeration, see 9.1.3.2.5	Yes
D	Big Integer	Yes

328 **Table 16: Key Material Object Structure for Transparent ECDSA Private Keys**

329 D is the private key (refer to NIST FIPS PUB 186-3).

330 **2.1.7.9 Transparent ECDSA Public Key**

331 If the Key Format Type in the Key Block is *Transparent ECDSA Public Key*, then Key Material is a
332 structure as shown in [Table 17](#).

Deleted: Table 17

Object	Encoding	REQUIRED
Key Material	Structure	
Recommended Curve	Enumeration, see 9.1.3.2.5	Yes
Q String	Byte String	Yes

333 **Table 17: Key Material Object Structure for Transparent ECDSA Public Keys**

334 Q String is the public key (refer to NIST FIPS PUB 186-3).

335 **2.1.7.10 Transparent ECDH Private Key**

336 If the Key Format Type in the Key Block is *Transparent ECDH Private Key*, then Key Material is a
337 structure as shown in [Table 18](#).

Deleted: Table 18

Object	Encoding	REQUIRED
Key Material	Structure	
Recommended Curve	Enumeration, see 9.1.3.2.5	Yes
D	Big Integer	Yes

338 **Table 18: Key Material Object Structure for Transparent ECDH Private Keys**

339 **2.1.7.11 Transparent ECDH Public Key**

340 If the Key Format Type in the Key Block is *Transparent ECDH Public Key*, then Key Material is a structure
341 as shown in [Table 19](#).

Deleted: Table 19

Object	Encoding	REQUIRED
Key Material	Structure	
Recommended Curve	Enumeration, see 9.1.3.2.5	Yes
Q String	Byte String	Yes

342 **Table 19: Key Material Object Structure for Transparent ECDH Public Keys**

343 Q String is the public key (refer to NIST FIPS PUB 186-3).

344 **2.1.7.12 Transparent ECMQV Private Key**

345 If the Key Format Type in the Key Block is *Transparent ECMQV Private Key*, then Key Material is a
346 structure as shown in [Table 20](#).

Deleted: Table 20

Object	Encoding	REQUIRED
Key Material	Structure	
Recommended Curve	Enumeration, see 9.1.3.2.5	Yes
D	Big Integer	Yes

347 **Table 20: Key Material Object Structure for Transparent ECMQV Private Keys**

348 **2.1.7.13 Transparent ECMQV Public Key**

349 If the Key Format Type in the Key Block is *Transparent ECMQV Public Key*, then Key Material is a
350 structure as shown in [Table 21](#).

Deleted: Table 21

Object	Encoding	REQUIRED
Key Material	Structure	
Recommended Curve	Enumeration, see 9.1.3.2.5	Yes
Q String	Byte String	Yes

351 **Table 21: Key Material Object Structure for Transparent ECMQV Public Keys**

352 **2.1.8 Template-Attribute Structures**

353 These structures are used in various operations to provide the desired attribute values and/or template
354 names in the request and to return the actual attribute values in the response.

355 The *Template-Attribute*, *Common Template-Attribute*, *Private Key Template-Attribute*, and *Public Key*
356 *Template-Attribute* structures are defined identically as follows:

Object	Encoding	REQUIRED
Template-Attribute, Common Template-Attribute, Private Key Template- Attribute, Public Key Template-Attribute	Structure	
Name	Structure, see 3.2	No, MAY be repeated.
Attribute	Attribute Object, see 2.1.1	No, MAY be repeated

357 **Table 22: Template-Attribute Object Structure**

358 Name is the Name attribute of the Template object defined in Section 2.2.6 .

359 **2.2 Managed Objects**

360 Managed Objects are objects that are the subjects of key management operations, which are described
361 in Sections 4 and 5 . *Managed Cryptographic Objects* are the subset of Managed Objects that contain
362 cryptographic material (e.g. certificates, keys, and secret data).

363 **2.2.1 Certificate**

364 A Managed Cryptographic Object that is a digital certificate (e.g., an encoded X.509 certificate).

Object	Encoding	REQUIRED
Certificate	Structure	
Certificate Type	Enumeration, see 9.1.3.2.6	Yes
Certificate Value	Byte String	Yes

365 **Table 23: Certificate Object Structure**

366 **2.2.2 Symmetric Key**

367 A Managed Cryptographic Object that is a symmetric key.

Object	Encoding	REQUIRED
Symmetric Key	Structure	
Key Block	Structure, see 2.1.3	Yes

368 **Table 24: Symmetric Key Object Structure**

369 **2.2.3 Public Key**

370 A Managed Cryptographic Object that is the public portion of an asymmetric key pair. This is only a public
371 key, not a certificate.

Object	Encoding	REQUIRED
Public Key	Structure	
Key Block	Structure, see 2.1.3	Yes

372 **Table 25: Public Key Object Structure**

373 **2.2.4 Private Key**

374 A Managed Cryptographic Object that is the private portion of an asymmetric key pair.

Object	Encoding	REQUIRED
Private Key	Structure	
Key Block	Structure, see 2.1.3	Yes

375 **Table 26: Private Key Object Structure**

376 **2.2.5 Split Key**

377 A Managed Cryptographic Object that is a *Split Key*. A split key is a secret, usually a symmetric key or a
378 private key that has been split into a number of parts, each of which MAY then be distributed to several
379 key holders, for additional security. The *Split Key Parts* field indicates the total number of parts, and the
380 *Split Key Threshold* field indicates the minimum number of parts needed to reconstruct the entire key.
381 The *Key Part Identifier* indicates which key part is contained in the cryptographic object, and SHALL be at
382 least 1 and SHALL be less than or equal to Split Key Parts.

Object	Encoding	REQUIRED
Split Key	Structure	
Split Key Parts	Integer	Yes
Key Part Identifier	Integer	Yes
Split Key Threshold	Integer	Yes
Split Key Method	Enumeration, see 9.1.3.2.7	Yes
Prime Field Size	Big Integer	No, REQUIRED only if Split Key Method is Polynomial Sharing Prime Field.
Key Block	Structure, see 2.1.3	Yes

Table 27: Split Key Object Structure

383
384 There are three *Split Key Methods* for secret sharing: the first one is based on XOR and the other two are
385 based on polynomial secret sharing, according to Adi Shamir, "How to share a secret", Communications
386 of the ACM, vol. 22, no. 11, pp. 612-613.

387 Let L be the minimum number of bits needed to represent all values of the secret.

- 388 • When the Split Key Method is XOR, then the Key Material in the Key Value of the Key Block is of
389 length L bits. The number of split keys is Split Key Parts (identical to Split Key Threshold), and
390 the secret is reconstructed by XORing all of the parts.
- 391 • When the Split Key Method is Polynomial Sharing Prime Field, then secret sharing is performed
392 in the field $GF(\text{Prime Field Size})$, represented as integers, where Prime Field Size is a prime
393 bigger than 2^L .
- 394 • When the Split Key Method is Polynomial Sharing $GF(2^{16})$, then secret sharing is performed in
395 the field $GF(2^{16})$. The Key Material in the Key Value of the Key Block is a bit string of length L ,
396 and when L is bigger than 2^{16} , then secret sharing is applied piecewise in pieces of 16 bits each.
397 The Key Material in the Key Value of the Key Block is the concatenation of the corresponding
398 shares of all pieces of the secret.

399 Secret sharing is performed in the field $GF(2^{16})$, which is represented as an algebraic extension of
400 $GF(2^8)$:

401 $GF(2^{16}) \approx GF(2^8)[y]/(y^2+y+m)$, where m is defined later.

402 An element of this field then consists of a linear combination $uy + v$, where u and v are elements
403 of the smaller field $GF(2^8)$.

404 The representation of field elements and the notation in this section rely on FIPS PUB 197,
405 Sections 3 and 4. The field $GF(2^8)$ is as described in FIPS PUB 197,

406 $GF(2^8) \approx GF(2)[x]/(x^8+x^4+x^3+x+1)$.

407 An element of $GF(2^8)$ is represented as a byte. Addition and subtraction in $GF(2^8)$ is performed as
408 a bit-wise XOR of the bytes. Multiplication and inversion are more complex (see FIPS PUB 197
409 Section 4.1 and 4.2 for details).

410 An element of $GF(2^{16})$ is represented as a pair of bytes (u, v) . The element m is given by

411 $m = x^5+x^4+x^3+x$,

412 which is represented by the byte 0x3A (or {3A} in notation according to FIPS PUB 197).

413 Addition and subtraction in $GF(2^{16})$ both correspond to simply XORing the bytes. The product of
414 two elements $ry + s$ and $uy + v$ is given by

415 $(ry + s)(uy + v) = ((r + s)(u + v) + sv)y + (ru + svu)$.

416 The inverse of an element $uy + v$ is given by
 417 $(uy + v)^{-1} = ud^{-1}y + (u + v)d^{-1}$, where $d = (u + v)v + mu^2$.

418 **2.2.6 Template**

419 A *Template* is a named Managed Object containing the client-settable attributes of a Managed
 420 Cryptographic Object (i.e., a stored, named list of attributes). A Template is used to specify the attributes
 421 of a new Managed Cryptographic Object in various operations. It is intended to be used to specify the
 422 cryptographic attributes of new objects in a standardized or convenient way. None of the client-settable
 423 attributes specified in a Template except the Name attribute apply to the template object itself, but instead
 424 apply to any object created using the Template.

425 The Template MAY be the subject of the Register, Locate, Get, Get Attributes, Get Attribute List, Add
 426 Attribute, Modify Attribute, Delete Attribute, and Destroy operations.

427 An attribute specified in a Template is applicable either to the Template itself or to objects created using
 428 the Template.

429 Attributes applicable to the Template itself are: Unique Identifier, Object Type, Name, Initial Date, Archive
 430 Date, and Last Change Date.

431 Attributes applicable to objects created using the Template are:

- 432 • Cryptographic Algorithm
- 433 • Cryptographic Length
- 434 • Cryptographic Domain Parameters
- 435 • Cryptographic Parameters
- 436 • Operation Policy Name
- 437 • Cryptographic Usage Mask
- 438 • Usage Limits
- 439 • Activation Date
- 440 • Process Start Date
- 441 • Protect Stop Date
- 442 • Deactivation Date
- 443 • Object Group
- 444 • Application Specific Information
- 445 • Contact Information
- 446 • Custom Attribute

Object	Encoding	REQUIRED
Template	Structure	
Attribute	Attribute Object, see 2.1.1	Yes. MAY be repeated.

447 **Table 28: Template Object Structure**

448 **2.2.7 Secret Data**

449 A Managed Cryptographic Object containing a shared secret value that is not a key or certificate (e.g., a
450 password). The Key Block of the *Secret Data* object contains a Key Value of the Opaque type. The Key
451 Value MAY be wrapped.

Object	Encoding	REQUIRED
Secret Data	Structure	
Secret Data Type	Enumeration, see 9.1.3.2.8	Yes
Key Block	Structure, see 2.1.3	Yes

452 **Table 29: Secret Data Object Structure**

453 **2.2.8 Opaque Object**

454 A Managed Object that the key management server is possibly not able to interpret. The context
455 information for this object MAY be stored and retrieved using Custom Attributes.

Object	Encoding	REQUIRED
Opaque Object	Structure	
Opaque Data Type	Enumeration, see 9.1.3.2.9	Yes
Opaque Data Value	Byte String	Yes

456 **Table 30: Opaque Object Structure**

457 3 Attributes

458 The following subsections describe the attributes that are associated with Managed Objects. These
459 attributes are able to be obtained by a client from the server using the Get Attribute operation. Some
460 attributes are able to be set by the Add Attribute operation or updated by the Modify Attribute operation,
461 and some are able to be deleted by the Delete Attribute operation if they no longer apply to the Managed
462 Object.

463 When attributes are returned by the server (e.g., via a Get Attributes operation), the returned attribute
464 value MAY differ depending on the client (e.g., the Cryptographic Usage Mask value MAY be different for
465 different clients, depending on the policy of the server).

466 The attribute name contained in the first row of the Object column of the first table in each subsection is
467 the canonical name used when managing attributes using the Get Attributes, Get Attribute List, Add
468 Attribute, Modify Attribute, and Delete Attribute operations.

469 A server SHALL NOT delete attributes without receiving a request from a client until the object is
470 destroyed.

471 The second table (see [Table 31](#)) in each subsection lists certain attribute characteristics (e.g., "SHALL
472 always have a value"). The "When implicitly set" characteristic indicates which operations (other than
473 operations that manage attributes) are able to implicitly add to or modify the attribute of the object, which
474 MAY be object(s) on which the operation is performed or object(s) created as a result of the operation.
475 Implicit attribute changes MAY occur even if the attribute is not specified in the operation request itself.

Deleted: Table 31

SHALL always have a value	All Managed Objects that are of the Object Types for which this attribute applies, SHALL always have this attribute set
Initially set by	Who is permitted to initially set the value of the attribute
Modifiable by server	Is the server allowed to modify the attribute without receiving a request from a client
Modifiable by client	Is the client able to modify the attribute value once it has been set
Deletable by client	Is the client able to delete an instance of the attribute
Multiple instances permitted	Are multiple instances of the attribute permitted
When implicitly set	Which operations cause this attribute to be set without an explicit request from a client
Applies to Object Types	Which Managed Objects MAY have this attribute set

476

Table 31: Attribute Rules

477 3.1 Unique Identifier

478 The *Unique Identifier* is generated by the key management system to uniquely identify a Managed Object.
479 It is only REQUIRED to be unique within the identifier space managed by a single key management
480 system, however it is RECOMMENDED that this identifier be globally unique, to allow for key

481 management domain export of such objects. This attribute SHALL be assigned by the key management
 482 system at creation or registration time, and then SHALL NOT be changed or deleted by any entity at any
 483 time.

Object	Encoding	
Unique Identifier	Text String	

484 **Table 32: Unique Identifier Attribute**

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

485 **Table 33: Unique Identifier Attribute Rules**

486 3.2 Name

487 The *Name* attribute is a structure (see [Table 34](#)) used to identify and locate the object, assigned by the
 488 client, and that humans are able to interpret. The key management system MAY specify rules by which
 489 the client creates valid names. Clients are informed of such rules by a mechanism that is not specified by
 490 this standard. Names SHALL be unique within a given key management domain, but are not REQUIRED
 491 to be globally unique.

Deleted: Table 34

Object	Encoding	REQUIRED
Name	Structure	
Name Value	Text String	Yes
Name Type	Enumeration, see 9.1.3.2.10	Yes

492 **Table 34: Name Attribute Structure**

SHALL always have a value	No
Initially set by	Client
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	Yes
Multiple instances permitted	Yes
When implicitly set	Re-key, Re-certify
Applies to Object Types	All Objects

493 **Table 35: Name Attribute Rules**

494 **3.3 Object Type**

495 The *Object Type* of a Managed Object (e.g., public key, private key, symmetric key, etc). This attribute
496 SHALL be set by the server when the object is created or registered and then SHALL NOT be changed.

Object	Encoding	
Object Type	Enumeration, see 9.1.3.2.11	

497 **Table 36: Object Type Attribute**

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

498 **Table 37: Object Type Attribute Rules**

499 **3.4 Cryptographic Algorithm**

500 The *Cryptographic Algorithm* used by the object (e.g., RSA, DSA, DES, 3DES, AES, etc). This attribute
501 SHALL be set by the server when the object is created or registered and then SHALL NOT be changed.

Object	Encoding	
Cryptographic Algorithm	Enumeration, see 9.1.3.2.12	

502 **Table 38: Cryptographic Algorithm Attribute**

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Re-key
Applies to Object Types	Keys, Certificates, Templates

503 **Table 39: Cryptographic Algorithm Attribute Rules**

504 **3.5 Cryptographic Length**

505 *Cryptographic Length* is the length in bits of the clear-text cryptographic key material of the Managed
506 Cryptographic Object. This attribute SHALL be set by the server when the object is created or registered,
507 and then SHALL NOT be changed.

Object	Encoding	
Cryptographic Length	Integer	

508

Table 40: Cryptographic Length Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Re-key
Applies to Object Types	Keys ,Certificates, Templates

509

Table 41: Cryptographic Length Attribute Rules

510 3.6 Cryptographic Parameters

511 | The *Cryptographic Parameters* attribute is a structure (see [Table 42](#)) that contains a set of OPTIONAL
512 fields that describe certain cryptographic parameters to be used when performing cryptographic
513 operations using the object. It is possible that specific fields only pertain to certain types of Managed
514 Cryptographic Objects.

Deleted: Table 42

Object	Encoding	REQUIRED
Cryptographic Parameters	Structure	
Block Cipher Mode	Enumeration, see 9.1.3.2.13	No
Padding Method	Enumeration, see 9.1.3.2.14	No
Hashing Algorithm	Enumeration, see 9.1.3.2.15	No
Role Type	Enumeration, see 9.1.3.2.16	No

515

Table 42: Cryptographic Parameters Attribute Structure

SHALL always have a value	No
Initially set by	Client
Modifiable by server	No
Modifiable by client	Yes
Deletable by client	Yes
Multiple instances permitted	Yes
When implicitly set	Re-key, Re-certify
Applies to Object Types	Keys ,Certificates, Templates

516

Table 43: Cryptographic Parameters Attribute Rules

517 | Role Type definitions match those defined in ANSI X9 TR-31 [X9 TR-31] and are defined in [Table 44](#);

Deleted: Table 44

BDK	Base Derivation Key (ANSI X9.24 DUKPT key derivation)
CVK	Card Verification Key (CVV/signature strip number validation)
DEK	Data Encryption Key (General Data Encryption)
MKAC	EMV/chip card Master Key: Application Cryptograms
MKSMC	EMV/chip card Master Key: Secure Messaging for Confidentiality
MKSMI	EMV/chip card Master Key: Secure Messaging for Integrity
MKDAC	EMV/chip card Master Key: Data Authentication Code
MKDN	EMV/chip card Master Key: Dynamic Numbers
MKCP	EMV/chip card Master Key: Card Personalization
MKOTH	EMV/chip card Master Key: Other
KEK	Key Encryption or Wrapping Key
MAC16609	ISO16609 MAC Algorithm 1
MAC97971	ISO9797-1 MAC Algorithm 1
MAC97972	ISO9797-1 MAC Algorithm 2
MAC97973	ISO9797-1 MAC Algorithm 3 (Note this is commonly known as X9.19 Retail MAC)
MAC97974	ISO9797-1 MAC Algorithm 4
MAC97975	ISO9797-1 MAC Algorithm 5
ZPK	PIN Block Encryption Key
PVKIBM	PIN Verification Key, IBM 3624 Algorithm
PVKPVV	PIN Verification Key, VISA PVV Algorithm
PVKOTH	PIN Verification Key, Other Algorithm

518

Table 44: Role Types

519 | Accredited Standards Committee X9, Inc. - Financial Industry Standards (www.x9.org) contributed to
520 | [Table 44](#). Key role names and descriptions are derived from material in the Accredited Standards
521 | Committee X9, Inc's Technical Report "TR-31 2005 Interoperable Secure Key Exchange Key Block
522 | Specification for Symmetric Algorithms" and used with the permission of Accredited Standards Committee
523 | X9, Inc. in an effort to improve interoperability between X9 standards and OASIS KMIP. The complete
524 | ANSI X9 TR-31 is available at www.x9.org.

Deleted: Table 44

525 | 3.7 Cryptographic Domain Parameters

526 | The *Cryptographic Domain Parameters* attribute is a structure (see [Table 45](#)) that contains a set of
527 | OPTIONAL fields that MAY need to be specified in the Create Key Pair Request Payload. Specific fields
528 | MAY only pertain to certain types of Managed Cryptographic Objects.

Deleted: Table 45

529 | For DSA, the domain parameter Qlength corresponds to the length of the parameter Q in bits. The length
530 | of P needs to be specified separately by setting the Cryptographic Length attribute.

Object	Encoding	Required
Cryptographic Domain Parameters	Structure	Yes
Qlength	Integer	No
Recommended Curve	Enumeration	No

531

Table 45: Cryptographic Domain Parameters Attribute Structure

Shall always have a value	No
Initially set by	Client
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Re-key
Applies to Object Types	Asymmetric Keys, Templates

532

Table 46: Cryptographic Domain Parameters Attribute Rules

533 3.8 Certificate Type

534 The type of a certificate (e.g., X.509, PGP, etc). The *Certificate Type* value SHALL be set by the server
535 when the certificate is created or registered and then SHALL NOT be changed.

Object	Encoding	
Certificate Type	Enumeration, see 9.1.3.2.6	

536

Table 47: Certificate Type Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Register, Certify, Re-certify
Applies to Object Types	Certificates

537

Table 48: Certificate Type Attribute Rules

538 3.9 Certificate Identifier

539 The *Certificate Identifier* attribute is a structure (see [Table 49](#)) used to provide the identification of a
540 certificate, containing the Issuer Distinguished Name (i.e., from the Issuer field of the certificate) and the
541 Certificate Serial Number (i.e., from the Serial Number field of the certificate). This value SHALL be set by
542 the server when the certificate is created or registered and then SHALL NOT be changed.

Deleted: Table 49

Object	Encoding	REQUIRED
Certificate Identifier	Structure	
Issuer	Text String	Yes
Serial Number	Text String	Yes (for X.509 certificates) / No (for PGP certificates since they do not contain a serial number)

543

Table 49: Certificate Identifier Attribute Structure

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Register, Certify, Re-certify
Applies to Object Types	Certificates

544

Table 50: Certificate Identifier Attribute Rules

545 3.10 Certificate Subject

546 | The *Certificate Subject* attribute is a structure (see [Table 51](#)) used to identify the subject of a certificate,
547 containing the Subject Distinguished Name (i.e., from the Subject field of the certificate). It MAY include
548 one or more alternative names (e.g., email address, IP address, DNS name) for the subject of the
549 certificate (i.e., from the Subject Alternative Name extension within the certificate). These values SHALL
550 be set by the server based on the information it extracts from the certificate that is created (as a result of
551 a Certify or a Re-certify operation) or registered (as part of a Register operation) and SHALL NOT be
552 changed during the lifespan of the certificate.

Deleted: Table 51

553 If the Subject Alternative Name extension is included in the certificate and is marked *CRITICAL*, then it is
554 possible to issue an X.509 certificate where the subject field is left blank. Therefore an empty string is an
555 acceptable value for the Certificate Subject Distinguished Name.

Object	Encoding	REQUIRED
Certificate Subject	Structure	
Certificate Subject Distinguished Name	Text String	Yes
Certificate Subject Alternative Name	Text String	No, MAY be repeated

556

Table 51: Certificate Subject Attribute Structure

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Register, Certify, Re-certify
Applies to Object Types	Certificates

557 **Table 52: Certificate Subject Attribute Rules**

558 **3.11 Certificate Issuer**

559 | The *Certificate Issuer* attribute is a structure (see [Table 54](#)) used to identify the issuer of a certificate,
560 containing the Issuer Distinguished Name (i.e., from the Issuer field of the certificate). It MAY include one
561 or more alternative names (e.g., email address, IP address, DNS name) for the issuer of the certificate
562 (i.e., from the Issuer Alternative Name extension within the certificate). The server SHALL set these
563 values based on the information it extracts from a certificate that is created as a result of a Certify or a
564 Re-certify operation or is sent as part of a Register operation. These values SHALL NOT be changed
565 during the lifespan of the certificate.

Deleted: Table 54

Object	Encoding	REQUIRED
Certificate Issuer	Structure	
Certificate Issuer Distinguished Name	Text String	Yes
Certificate Issuer Alternative Name	Text String	No, MAY be repeated

566 **Table 53: Certificate Issuer Attribute Structure**

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Register, Certify, Re-certify
Applies to Object Types	Certificates

567 **Table 54: Certificate Issuer Attribute Rules**

568 **3.12 Digest**

569 | The *Digest* attribute is a structure (see [Table 55](#)) that contains the digest value of the key or secret data
570 (i.e., digest of the Key Material), certificate (i.e., digest of the Certificate Value), or opaque object (i.e.,
571 digest of the Opaque Data Value). Multiple digests MAY be calculated using different algorithms. The
572 mandatory digest SHALL be computed with the SHA-256 hashing algorithm; the server MAY store
573 additional digests using the algorithms listed in Section 9.1.3.2.15 . The digest(s) are static and SHALL be
574 generated by the server when the object is created or registered.

Deleted: Table 55

Object	Encoding	REQUIRED
Digest	Structure	
Hashing Algorithm	Enumeration, see 9.1.3.2.15	Yes
Digest Value	Byte String	Yes

575

Table 55: Digest Attribute Structure

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	Yes
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects, Opaque Objects

576

Table 56: Digest Attribute Rules

577 3.13 Operation Policy Name

578 An operation policy controls what entities MAY perform which key management operations on the object.
579 The content of the *Operation Policy Name* attribute is the name of a policy object known to the key
580 management system and, therefore, is server dependent. The named policy objects are created and
581 managed using mechanisms outside the scope of the protocol. The policies determine what entities MAY
582 perform specified operations on the object, and which of the object's attributes MAY be modified or
583 deleted. The Operation Policy Name attribute SHOULD be set when operations that result in a new
584 Managed Object on the server are executed. It is set either explicitly or via some default set by the server,
585 which then applies to all subsequent operations on the object.

Object	Encoding	
Operation Policy Name	Text String	

586

Table 57: Operation Policy Name Attribute

SHALL always have a value	No
Initially set by	Server or Client
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

587

Table 58: Operation Policy Name Attribute Rules

588 **3.13.1 Operations outside of operation policy control**

589 Some of the operations SHOULD be allowed for any client at any time, without respect to operation
590 policy. These operations are:

- 591 • Create
- 592 • Create Key Pair
- 593 • Register
- 594 • Certify
- 595 • Validate
- 596 • Query
- 597 • Cancel
- 598 • Poll

599 **3.13.2 Default Operation Policy**

600 A key management system implementation SHALL implement at least one named operation policy, which
601 is used for objects when the *Operation Policy* attribute is not specified by the Client in a *Create* or
602 *Register* operation, or in a template specified in these operations. This policy is named *default*. It specifies
603 the following rules for operations on objects created or registered with this policy, depending on the object
604 type.

605 **3.13.2.1 Default Operation Policy for Secret Objects**

606 This policy applies to Symmetric Keys, Private Keys, Split Keys, Secret Data, and Opaque Objects.

Default Operation Policy for Secret Objects	
Operation	Policy
Re-Key	Allowed to creator only
Derive Key	Allowed to creator only
Locate	Allowed to creator only
Check	Allowed to creator only
Get	Allowed to creator only
Get Attributes	Allowed to creator only
Get Attribute List	Allowed to creator only
Add Attribute	Allowed to creator only
Modify Attribute	Allowed to creator only
Delete Attribute	Allowed to creator only
Obtain Lease	Allowed to creator only

Get Usage Allocation	Allowed to creator only
Activate	Allowed to creator only
Revoke	Allowed to creator only
Destroy	Allowed to creator only
Archive	Allowed to creator only
Recover	Allowed to creator only

Table 59: Default Operation Policy for Secret Objects

607

608 For mandatory profiles, the creator SHALL be the transport-layer identification (see [KMIP-Prof])
609 provided at the Create or Register operation time.

610 **3.13.2.2 Default Operation Policy for Certificates and Public Key Objects**

611 This policy applies to Certificates and Public Keys.

Default Operation Policy for Certificates and Public Key Objects	
Operation	Policy
Certify	Allowed to creator only
Re-certify	Allowed to creator only
Locate	Allowed to all
Check	Allowed to all
Get	Allowed to all
Get Attributes	Allowed to all
Get Attribute List	Allowed to all
Add Attribute	Allowed to creator only
Modify Attribute	Allowed to creator only
Delete Attribute	Allowed to creator only
Obtain Lease	Allowed to all
Activate	Allowed to creator only
Revoke	Allowed to creator only
Destroy	Allowed to creator only
Archive	Allowed to creator only
Recover	Allowed to creator only

Table 60: Default Operation Policy for Certificates and Public Key Objects

612

613 **3.13.2.3 Default Operation Policy for Template Objects**

614 The operation policy specified as an attribute in the *Create* operation for a template object is the operation
615 policy used for objects created using that template, and is not the policy used to control operations on the
616 template itself. There is no mechanism to specify a policy used to control operations on template objects,
617 so the default policy for template objects is always used for templates created by clients using the
618 *Register* operation to create template objects.

Default Operation Policy for Private Template Objects	
Operation	Policy
Locate	Allowed to creator only
Get	Allowed to creator only
Get Attributes	Allowed to creator only
Get Attribute List	Allowed to creator only
Add Attribute	Allowed to creator only
Modify Attribute	Allowed to creator only
Delete Attribute	Allowed to creator only
Destroy	Allowed to creator only

619 **Table 61: Default Operation Policy for Private Template Objects**

620 In addition to private template objects (which are controlled by the above policy, and which MAY be
621 created by clients or the server), publicly known and usable templates MAY be created and managed by
622 the server, with a default policy different from private template objects.

Default Operation Policy for Public Template Objects	
Operation	Policy
Locate	Allowed to all
Get	Allowed to all
Get Attributes	Allowed to all
Get Attribute List	Allowed to all
Add Attribute	Disallowed to all
Modify Attribute	Disallowed to all
Delete Attribute	Disallowed to all
Destroy	Disallowed to all

623 **Table 62: Default Operation Policy for Public Template Objects**

624 **3.14 Cryptographic Usage Mask**

625 The *Cryptographic Usage Mask* defines the cryptographic usage of a key. This is a bit mask that indicates
626 to the client which cryptographic functions MAY be performed using the key, and which ones SHALL NOT
627 be performed.

- 628 • Sign
- 629 • Verify
- 630 • Encrypt
- 631 • Decrypt
- 632 • Wrap Key
- 633 • Unwrap Key
- 634 • Export
- 635 • MAC Generate
- 636 • MAC Verify
- 637 • Derive Key
- 638 • Content Commitment
- 639 • Key Agreement
- 640 • Certificate Sign

- 641 • CRL Sign
- 642 • Generate Cryptogram
- 643 • Validate Cryptogram
- 644 • Translate Encrypt
- 645 • Translate Decrypt
- 646 • Translate Wrap
- 647 • Translate Unwrap

648 This list takes into consideration values that MAY appear in the Key Usage extension in an X.509
 649 certificate. However, the list does not consider the additional usages that MAY appear in the Extended
 650 Key Usage extension.

651 X.509 Key Usage values SHALL be mapped to Cryptographic Usage Mask values in the following
 652 manner:

X.509 Key Usage to Cryptographic Usage Mask Mapping	
X.509 Key Usage Value	Cryptographic Usage Mask Value
digitalSignature	Sign and Verify
contentCommitment	Content Commitment (Non Repudiation)
keyEncipherment	Wrap Key and Unwrap Key
dataEncipherment	Encrypt and Decrypt
keyAgreement	Key Agreement
keyCertSign	Certificate Sign
cRLSign	CRL Sign
encipherOnly	Encrypt
decipherOnly	Decrypt

653 **Table 63: X.509 Key Usage to Cryptographic Usage Mask Mapping**

654

Object	Encoding
Cryptographic Usage Mask	Integer

655 **Table 64: Cryptographic Usage Mask Attribute**

SHALL always have a value	Yes
Initially set by	Server or Client
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects, Templates

656 **Table 65: Cryptographic Usage Mask Attribute Rules**

657 **3.15 Lease Time**

658 The *Lease Time* attribute defines a time interval for a Managed Cryptographic Object beyond which the
659 client SHALL NOT use the object. This attribute always holds the initial value of a lease, and not the
660 actual remaining time. Once the lease expires, then the client is only able to renew the lease by calling
661 Obtain Lease. A server SHALL store in this attribute the maximum Lease Time it is able to serve and a
662 client obtains the lease time (with Obtain Lease) that is less than or equal to the maximum Lease Time.
663 This attribute is read-only for clients. It SHALL be modified by the server only.

Object	Encoding	
Lease Time	Interval	

664 **Table 66: Lease Time Attribute**

SHALL always have a value	No
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects

665 **Table 67: Lease Time Attribute Rules**

666 **3.16 Usage Limits**

667 The *Usage Limits* attribute is a mechanism for limiting the usage of a Managed Cryptographic Object. It
668 only applies to Managed Cryptographic Objects that are able to be used for applying cryptographic
669 protection and it SHALL only reflect their usage for applying that protection (e.g., encryption, signing,
670 etc.). This attribute does not necessarily exist for all Managed Cryptographic Objects, since some objects
671 are able to be used without limit, depending on client/server policies. Usage for processing
672 cryptographically-protected data (e.g., decryption, verification, etc.) is not limited. The attribute has four

673 fields for two different types of limits, bytes and objects. Exactly one of these two types SHALL be
674 present. These fields are:

- 675 • *Usage Limits Total Bytes* – the total number of bytes allowed to be protected. This is the total
676 value for the entire life of the object and SHALL NOT be changed once the object begins to be
677 used for applying cryptographic protection.
- 678 • *Usage Limits Byte Count* – the currently remaining number of bytes allowed to be protected by
679 the object.
- 680 • *Usage Limits Total Objects* – the total number of objects allowed to be protected. This is the total
681 value for the entire life of the object and SHALL NOT be changed once the object begins to be
682 used for applying cryptographic protection.
- 683 • *Usage Limits Object Count* – the currently remaining number of objects allowed to be protected
684 by the object.

685 When the attribute is initially set (usually during object creation or registration), the Count values are set
686 to the Total values allowed for the useful life of the object. The count values SHALL be ignored by the
687 server if the attribute is specified in an operation that creates a new object. Changes made via the Modify
688 Attribute operation reflect corrections to these Total values, but they SHALL NOT be changed once the
689 Count values have changed by a Get Usage Allocation operation. The Count values SHALL NOT be set
690 or modified by the client via the Add Attribute or Modify Attribute operations.

Object	Encoding	REQUIRED
Usage Limits	Structure	
Usage Limits Total Bytes	Big Integer	No. SHALL be present if Usage Limits Byte Count is present
Usage Limits Byte Count	Big Integer	No. SHALL be present if Usage Limits Object Count is not present
Usage Limits Total Objects	Big Integer	No. SHALL be present if Usage Limits Object Count is present
Usage Limits Object Count	Big Integer	No. SHALL be present if Usage Limits Byte Count is not present

691

Table 68: Usage Limits Attribute Structure

SHALL always have a value	No
Initially set by	Server (Total and/or Count) or Client (Total only)
Modifiable by server	Yes
Modifiable by client	Yes (Total only, as long as Get Usage Allocation has not been performed)
Deletable by client	Yes
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Re-key, Get Usage Allocation
Applies to Object Types	Keys, Templates

Table 69: Usage Limits Attribute Rules

692

693 3.17 State

694 This attribute is an indication of the *State* of an object as known to the key management server. The State
695 SHALL NOT be changed by using the Modify Attribute operation on this attribute. The state SHALL only
696 be changed by the server as a part of other operations or other server processes. An object SHALL be in
697 one of the following states at any given time. (Note: These states correspond to those described in NIST
698 Special Publication 800-57 [SP800-57-1]).

- 699 • *Pre-Active*: The object exists but is not yet usable for
700 any cryptographic purpose.
- 701 • *Active*: The object MAY be used for all cryptographic
702 purposes that are allowed by its Cryptographic Usage
703 Mask attribute and, if applicable, by its Process Start
704 Date (see 3.20) and Protect Stop Date (see 3.21)
705 attributes.
- 706 • *Deactivated*: The object SHALL NOT be used for
707 applying cryptographic protection (e.g., encryption or
708 signing), but, if permitted by the Cryptographic Usage
709 Mask attribute, then the object MAY be used to
710 process cryptographically-protected information (e.g.,
711 decryption or verification), but only under
712 extraordinary circumstances and when special
713 permission is granted.
- 714 • *Compromised*: It is possible that the object has been
715 compromised, and SHOULD only be used to process
716 cryptographically-protected information in a client that
717 is trusted to handle compromised cryptographic
718 objects.
- 719 • *Destroyed*: The object is no longer usable for any
720 purpose.
- 721 • *Destroyed Compromised*: The object is no longer

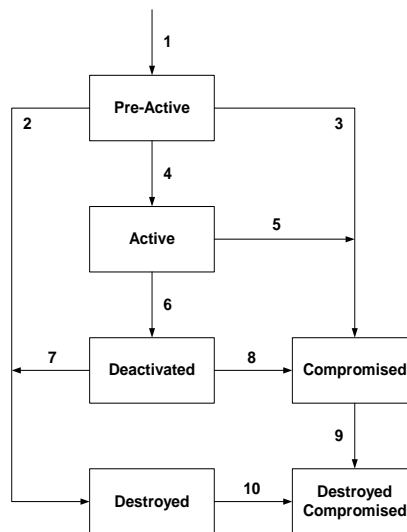


Figure 1: Cryptographic Object States and Transitions

722 usable for any purpose; however its compromised status MAY be retained for audit or security
723 purposes.

724 State transitions occur as follows:

- 725 1. The transition from a non-existent key to the Pre-Active state is caused by the creation of the
726 object. When an object is created or registered, it automatically goes from non-existent to Pre-
727 Active. If, however, the operation that creates or registers the object contains an Activation Date
728 that has already occurred, then the state immediately transitions to Active. In this case, the server
729 SHALL set the Activation Date attribute to the time when the operation is received, or fail the
730 request attempting to create or register the object, depending on server policy. If the operation
731 contains an Activation Date attribute in the future, or contains no Activation Date, then the
732 Cryptographic Object is initialized in the key management system in the Pre-Active state.
- 733 2. The transition from Pre-Active to Destroyed is caused by a client issuing a Destroy operation. The
734 server destroys the object when (and if) server policy dictates.
- 735 3. The transition from Pre-Active to Compromised is caused by a client issuing a Revoke operation
736 with a Revocation Reason of Compromised.
- 737 4. The transition from Pre-Active to Active SHALL occur in one of three ways:
 - 738 • The object has an Activation Date in the future. At the time that the Activation Date is
739 reached, the server changes the state to Active.
 - 740 • A client issues a Modify Attribute operation, modifying the Activation Date to a date in the
741 past, or the current date. In this case, the server SHALL either set the Activation Date
742 attribute to the date in the past or the current date, or fail the operation, depending on
743 server policy.
 - 744 • A client issues an Activate operation on the object. The server SHALL set the Activation
745 Date to the time the Activate operation is received.
- 746 5. The transition from Active to Compromised is caused by a client issuing a Revoke operation with
747 a Revocation Reason of Compromised.
- 748 6. The transition from Active to Deactivated SHALL occur in one of three ways:
 - 749 • The object's Deactivation Date is reached.
 - 750 • A client issues a Revoke operation, with a Revocation Reason other than Compromised.
 - 751 • The client issues a Modify Attribute operation, modifying the Deactivation Date to a date in
752 the past, or the current date. In this case, the server SHALL either set the Deactivation
753 Date attribute to the date in the past or the current date, or fail the operation, depending on
754 server policy.
- 755 7. The transition from Deactivated to Destroyed is caused by a client issuing a Destroy operation or
756 by a server in accordance with server policy. The server destroys the object when (and if) server
757 policy dictates.
- 758 8. The transition from Deactivated to Compromised is caused by a client issuing a Revoke operation
759 with a Revocation Reason of Compromised.
- 760 9. The transition from Compromised to Destroyed Compromised is caused by a client issuing a
761 Destroy operation or by a server in accordance with server policy. The server destroys the object
762 when (and if) server policy dictates.
- 763 10. The transition from Destroyed to Destroyed Compromised is caused by a client issuing a Revoke
764 operation with a Revocation Reason of Compromised.

765 Only the transitions described above are permitted.

Object	Encoding	
State	Enumeration, see 9.1.3.2.17	

Table 70: State Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Activate, Revoke, Destroy, Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects

Table 71: State Attribute Rules768 **3.18 Initial Date**

769 The *Initial Date* is the date and time when the Managed Object was first created or registered at the
 770 server. This time corresponds to state transition 1 (see Section 3.17). This attribute SHALL be set by the
 771 server when the object is created or registered, and then SHALL NOT be changed. This attribute is also
 772 set for non-cryptographic objects (e.g., templates) when they are first registered with the server.

Object	Encoding
Initial Date	Date-Time

Table 72: Initial Date Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

Table 73: Initial Date Attribute Rules775 **3.19 Activation Date**

776 This is the date and time when the Managed Cryptographic Object MAY begin to be used. This time
 777 corresponds to state transition 4 (see Section 3.17). The object SHALL NOT be used for any
 778 cryptographic purpose before the *Activation Date* has been reached. Once the state transition has
 779 occurred, then this attribute SHALL NOT be modified by the server or client.

Object	Encoding
Activation Date	Date-Time

Table 74: Activation Date Attribute

SHALL always have a value	No
Initially set by	Server or Client
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Activate Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects, Templates

Table 75: Activation Date Attribute Rules

782 3.20 Process Start Date

783 This is the date and time when a Managed Symmetric Key Object MAY begin to be used to process
 784 cryptographically-protected information (e.g., decryption or unwrapping), depending on the value of its
 785 Cryptographic Usage Mask attribute. The object SHALL NOT be used for these cryptographic purposes
 786 before the *Process Start Date* has been reached. This value MAY be equal to, but SHALL NOT precede,
 787 the Activation Date. Once the Process Start Date has occurred, then this attribute SHALL NOT be
 788 modified by the server or the client.

Object	Encoding	
Process Start Date	Date-Time	

Table 76: Process Start Date Attribute

SHALL always have a value	No
Initially set by	Server or Client
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Derive Key, Re-key
Applies to Object Types	Symmetric Keys, Split Keys of symmetric keys, Templates

Table 77: Process Start Date Attribute Rules

791 3.21 Protect Stop Date

792 This is the date and time when a Managed Symmetric Key Object SHALL NOT be used for applying
 793 cryptographic protection (e.g., encryption or wrapping), depending on the value of its Cryptographic
 794 Usage Mask attribute. This value MAY be equal to, but SHALL NOT be later than the Deactivation Date.

795 Once the *Protect Stop Date* has occurred, then this attribute SHALL NOT be modified by the server or the
 796 client.

Object	Encoding
Protect Stop Date	Date-Time

797 **Table 78: Protect Stop Date Attribute**

SHALL always have a value	No
Initially set by	Server or Client
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Register, Derive Key, Re-key
Applies to Object Types	Symmetric Keys, Split Keys of symmetric keys, Templates

798 **Table 79: Protect Stop Date Attribute Rules**

799 3.22 Deactivation Date

800 The *Deactivation Date* is the date and time when the Managed Cryptographic Object SHALL NOT be
 801 used for any purpose, except for decryption, signature verification, or unwrapping, but only under
 802 extraordinary circumstances and only when special permission is granted. This time corresponds to state
 803 transition 6 (see Section 3.17). Once this transition has occurred, then this attribute SHALL NOT be
 804 modified by the server or client.

Object	Encoding
Deactivation Date	Date-Time

805 **Table 80: Deactivation Date Attribute**

SHALL always have a value	No
Initially set by	Server or Client
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Revoke Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects, Templates

806 **Table 81: Deactivation Date Attribute Rules**

807 3.23 Destroy Date

808 The *Destroy Date* is the date and time when the Managed Object was destroyed. This time corresponds
809 to state transitions 2, 7, or 9 (see Section 3.17). This value is set by the server when the object is
810 destroyed due to the reception of a Destroy operation, or due to server policy or out-of-band
811 administrative action.

Object	Encoding	
Destroy Date	Date-Time	

812 **Table 82: Destroy Date Attribute**

SHALL always have a value	No
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Destroy
Applies to Object Types	All Cryptographic Objects, Opaque Objects

813 **Table 83: Destroy Date Attribute Rules**

814 3.24 Compromise Occurrence Date

815 The *Compromise Occurrence Date* is the date and time when the Managed Cryptographic Object was
816 first believed to be compromised. If it is not possible to estimate when the compromise occurred, then this
817 value SHOULD be set to the Initial Date for the object.

Object	Encoding	
Compromise Occurrence Date	Date-Time	

818 **Table 84: Compromise Occurrence Date Attribute**

SHALL always have a value	No
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Revoke
Applies to Object Types	All Cryptographic Objects, Opaque Object

819 **Table 85: Compromise Occurrence Date Attribute Rules**

820 3.25 Compromise Date

821 The *Compromise Date* is the date and time when the Managed Cryptographic Object entered into the
822 compromised state. This time corresponds to state transitions 3, 5, 8, or 10 (see Section 3.17). This time

823 indicates when the key management system was made aware of the compromise, not necessarily when
 824 the compromise occurred. This attribute is set by the server when it receives a Revoke operation with a
 825 Revocation Reason of Compromised, or due to server policy or out-of-band administrative action.

Object	Encoding	
Compromise Date	Date-Time	

826 **Table 86: Compromise Date Attribute**

SHALL always have a value	No
Initially set by	Server
Modifiable by server	No
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Revoke
Applies to Object Types	All Cryptographic Objects, Opaque Object

827 **Table 87: Compromise Date Attribute Rules**

828 **3.26 Revocation Reason**

829 The *Revocation Reason* attribute is a structure (see [Table 88](#)) used to indicate why the Managed
 830 Cryptographic Object was revoked (e.g., “compromised”, “expired”, “no longer used”, etc). This attribute is
 831 only changed by the server as a part of the Revoke Operation.

Deleted: Table 88

832 The *Revocation Message* is an OPTIONAL field that is used exclusively for audit trail/logging purposes
 833 and MAY contain additional information about why the object was revoked (e.g., “Laptop stolen”, or
 834 “Machine decommissioned”).

Object	Encoding	REQUIRED
Revocation Reason	Structure	
Revocation Reason Code	Enumeration, see 9.1.3.2.18	Yes
Revocation Message	Text String	No

835 **Table 88: Revocation Reason Attribute Structure**

SHALL always have a value	No
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Revoke
Applies to Object Types	All Cryptographic Objects, Opaque Object

836 **Table 89: Revocation Reason Attribute Rules**

837 **3.27 Archive Date**

838 The *Archive Date* is the date and time when the Managed Object was placed in archival storage. This
 839 value is set by the server as a part of the Archive operation. This attribute is deleted whenever a Recover
 840 operation is performed.

Object	Encoding
Archive Date	Date-Time

841 **Table 90: Archive Date Attribute**

SHALL always have a value	No
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Archive
Applies to Object Types	All Objects

842 **Table 91: Archive Date Attribute Rules**

843 **3.28 Object Group**

844 An object MAY be part of a group of objects. An object MAY belong to more than one group of objects. To
 845 assign an object to a group of objects, the object group name SHOULD be set into this attribute.

Object	Encoding
Object Group	Text String

846 **Table 92: Object Group Attribute**

SHALL always have a value	No
Initially set by	Client or Server
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	Yes
Multiple instances permitted	Yes
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

847 **Table 93: Object Group Attribute Rules**

848 **3.29 Link**

849 The *Link* attribute is a structure (see [Table 94](#)) used to create a link from one Managed Cryptographic
 850 Object to another, closely related target Managed Cryptographic Object. The link has a type, and the
 851 allowed types differ, depending on the Object Type of the Managed Cryptographic Object, as listed
 852 below. The *Linked Object Identifier* identifies the target Managed Cryptographic Object by its Unique

Deleted: Table 94

853 Identifier. The link contains information about the association between the Managed Cryptographic
854 Objects (e.g., the private key corresponding to a public key; the parent certificate for a certificate in a
855 chain; or for a derived symmetric key, the base key from which it was derived).

856 Possible values of *Link Type* in accordance with the Object Type of the Managed Cryptographic Object
857 are:

- 858 • *Private Key Link*. For a Public Key object: the private key corresponding to the public key.
- 859 • *Public Key Link*. For a Private Key object: the public key corresponding to the private key. For a
860 Certificate object: the public key contained in the certificate.
- 861 • *Certificate Link*. For Certificate objects: the parent certificate for a certificate in a certificate chain.
862 For Public Key objects: the corresponding certificate(s), containing the same public key.
- 863 • *Derivation Base Object Link* for a derived Symmetric Key object: the object(s) from which the
864 current symmetric key was derived.
- 865 • *Derived Key Link*: the symmetric key(s) that were derived from the current object.
- 866 • *Replacement Object Link*. For a Symmetric Key object: the key that resulted from the re-key of
867 the current key. For a Certificate object: the certificate that resulted from the re-certify. Note that
868 there SHALL be only one such replacement object per Managed Object.
- 869 • *Replaced Object Link*. For a Symmetric Key object: the key that was re-keyed to obtain the
870 current key. For a Certificate object: the certificate that was re-certified to obtain the current
871 certificate.

872 The Link attribute SHOULD be present for private keys and public keys for which a certificate chain is
873 stored by the server, and for certificates in a certificate chain.

874 Note that it is possible for a Managed Object to have multiple instances of the Link attribute (e.g., a
875 Private Key has links to the associated certificate as well as the associated public key; a Certificate object
876 has links to both the public key and to the certificate of the certification authority (CA) that signed the
877 certificate).

878 It is also possible that a Managed Object does not have links to associated cryptographic objects. This
879 MAY occur in cases where the associated key material is not available to the server or client (e.g., the
880 registration of a CA Signer certificate with a server, where the corresponding private key is held in a
881 different manner).

Object	Encoding	REQUIRED
Link	Structure	
Link Type	Enumeration, see 9.1.3.2.19	Yes
Linked Object Identifier	Text String	Yes

882 **Table 94: Link Attribute Structure**

SHALL always have a value	No
Initially set by	Client or Server
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	Yes
Multiple instances permitted	Yes
When implicitly set	Create Key Pair, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Cryptographic Objects

883

Table 95: Link Attribute Structure Rules

884 **3.30 Application Specific Information**

885 | The *Application Specific Information* attribute is a structure (see [Table 96](#)) used to store data specific to
886 | the application(s) using the Managed Object. It consists of the following fields: an *Application Namespace*
887 | and *Application Data* specific to that application namespace. A list of standard application namespaces is
888 | provided in [\[KMIP-Prof\]](#).

Deleted: Table 96

Deleted: [TBD]

889 Clients MAY request to set (i.e., using any of the operations that results in generating new Managed
890 Object(s) or adding/modifying the attribute of an existing Managed Object) an instance of this attribute
891 with a particular Application Namespace while omitting Application Data. In that case, if the server
892 supports this namespace (as indicated by the Query operation in Section 4.24), then it SHALL return a
893 suitable Application Data value. If the server does not support this namespace, then an error SHALL be
894 returned.

895

Object	Encoding	REQUIRED
Application Specific Information	Structure	
Application Namespace	Text String	Yes
Application Data	Text String	Yes

896

Table 96: Application Specific Information Attribute

897

SHALL always have a value	No
Initially set by	Client or Server (only if the Application Data is omitted, in the client request)
Modifiable by server	Yes (only if the Application Data is omitted in the client request)
Modifiable by client	Yes
Deletable by client	Yes
Multiple instances permitted	Yes
When implicitly set	Re-key, Re-certify
Applies to Object Types	All Objects

898

Table 97: Application Specific Information Attribute Rules

899 **3.31 Contact Information**

900 The *Contact Information* attribute is OPTIONAL, and its content is used for contact purposes only. It is not
901 used for policy enforcement. The attribute is set by the client or the server.

Object	Encoding	
Contact Information	Text String	

902

Table 98: Contact Information Attribute

SHALL always have a value	No
Initially set by	Client or Server
Modifiable by server	Yes
Modifiable by client	Yes
Deletable by client	Yes
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

903

Table 99: Contact Information Attribute Rules

904 **3.32 Last Change Date**

905 The *Last Change Date* attribute is a meta attribute that contains the date and time of the last change to
 906 the contents or attributes of the specified object.

Object	Encoding	
Last Change Date	Date-Time	

907

Table 100: Last Change Date Attribute

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Activate, Revoke, Destroy, Archive, Recover, Certify, Re-certify, Re-key, Add Attribute, Modify Attribute, Delete Attribute, Get Usage Allocation
Applies to Object Types	All Objects

908

Table 101: Last Change Date Attribute Rules

909 **3.33 Custom Attribute**

910 A *Custom Attribute* is a client- or server-defined attribute intended for vendor-specific purposes. It is
 911 created by the client and not interpreted by the server, or is created by the server and MAY be interpreted
 912 by the client. All custom attributes created by the client SHALL adhere to a naming scheme, where the
 913 name of the attribute SHALL have a prefix of 'x-'. All custom attributes created by the key management
 914 server SHALL adhere to a naming scheme where the name of the attribute SHALL have a prefix of 'y-'.
 915 The server SHALL NOT accept a client-created or modified attribute, where the name of the attribute has

916 a prefix of 'y-'. The tag type Custom Attribute is not able to identify the particular attribute; hence such an
 917 attribute SHALL only appear in an Attribute Structure with its name as defined in Section 2.1.1 .

Object	Encoding	
Custom Attribute	Any data type or structure	The name of the attribute SHALL start with 'x-' or 'y-'.

918 **Table 102 Custom Attribute**

SHALL always have a value	No
Initially set by	Client or Server
Modifiable by server	Yes, for server-created attributes
Modifiable by client	Yes, for client-created attributes
Deletable by client	Yes, for client-created attributes
Multiple instances permitted	Yes
When implicitly set	Create, Create Key Pair, Register, Derive Key, Activate, Revoke, Destroy, Certify, Re-certify, Re-key
Applies to Object Types	All Objects

919 **Table 103: Custom Attribute Rules**

920 4 Client-to-Server Operations

921 The following subsections describe the operations that MAY be requested by a key management client.
 922 Not all clients have to be capable of issuing all operation requests; however any client that issues a
 923 specific request SHALL be capable of understanding the response to the request. All Object Management
 924 operations are issued in requests from clients to servers, and results obtained in responses from servers
 925 to clients. These operations MAY be combined into a batch, which allows multiple operations to be
 926 contained in a single request/response message pair.

927 A number of the operations whose descriptions follow are affected by a mechanism referred to as the *ID*
 928 *Placeholder*.

929 The key management server SHALL implement a temporary variable called the ID Placeholder. This
 930 value consists of a single Unique Identifier. It is a variable stored inside the server that is only valid and
 931 preserved during the execution of a batch of operations. Once the batch of operations has been
 932 completed, the ID Placeholder value is discarded and/or invalidated by the server, so that subsequent
 933 requests do not find this previous ID Placeholder available.

934 The ID Placeholder is obtained from the Unique Identifier returned in response to the Create, Create Pair,
 935 Register, Derive Key, Re-Key, Certify, Re-Certify, Locate, and Recover operations. If any of these
 936 operations successfully completes and returns a Unique Identifier, then the server SHALL copy this
 937 Unique Identifier into the ID Placeholder variable, where it is held until the completion of the operations
 938 remaining in the batched request or until a subsequent operation in the batch causes the ID Placeholder
 939 to be replaced. If the Batch Error Continuation Option is set to Stop and the Batch Order Option is set to
 940 true, then subsequent operations in the batched request MAY make use of the ID Placeholder by omitting
 941 the Unique Identifier field from the request payloads for these operations.

942 Requests MAY contain attribute values to be assigned to the object. This information is specified with a
 943 Template-Attribute (see Section 2.1.8) that contains zero or more template names and zero or more

944 individual attributes. If more than one template name is specified, and there is a conflict between the
 945 single-instance attributes in the templates, then the value in the subsequent template takes precedence.
 946 If there is a conflict between the single-instance attributes in the request and the single-instance attributes
 947 in a specified template, then the attribute values in the request take precedence. For multi-value
 948 attributes, the union of attribute values is used when the attributes are specified more than once.

949 Responses MAY contain attribute values that were not specified in the request, but have been implicitly
 950 set by the server. This information is specified with a Template-Attribute that contains one or more
 951 individual attributes.

952 For any operations that operate on Managed Objects already stored on the server, any archived object
 953 SHALL first be moved back on-line through a Recover operation (see Section 4.22) before they MAY be
 954 specified (i.e., as on-line objects).

955 4.1 Create

956 This operation requests the server to generate a new symmetric key as a Managed Cryptographic Object.
 957 This operation is not used to create a Template object (see Register operation, Section 4.3).

958 The request contains information about the type of object being created, and some of the attributes to be
 959 assigned to the object (e.g., Cryptographic Algorithm, Cryptographic Length, etc). This information MAY
 960 be specified by the names of Template objects that already exist.

961 The response contains the Unique Identifier of the created object. The server SHALL copy the Unique
 962 Identifier returned by this operation into the ID Placeholder variable.

Request Payload		
Object	REQUIRED	Description
Object Type, see 3.3	Yes	Determines the type of object to be created.
Template-Attribute, see 2.1.8	Yes	Specifies desired object attributes using templates and/or individual attributes.

963 **Table 104: Create Request Payload**

Response Payload		
Object	REQUIRED	Description
Object Type, see 3.3	Yes	Type of object created.
Unique Identifier, see 3.1	Yes	The Unique Identifier of the newly created object.
Template-Attribute, see 2.1.8	No	An OPTIONAL list of object attributes with values that were not specified in the request, but have been implicitly set by the key management server.

964 **Table 105: Create Response Payload**

965 | **Table 106** indicates which attributes SHALL be included in the Create request using the Template-
 966 Attribute object.

Deleted: Table 106

Attribute	REQUIRED
Cryptographic Algorithm, see 3.4	Yes
Cryptographic Usage Mask, see 3.14	Yes

Table 106: Create Attribute Requirements

967

968 4.2 Create Key Pair

969 This operation requests the server to generate a new public/private key pair and register the two
970 corresponding new Managed Cryptographic Objects.

971 The request contains attributes to be assigned to the objects (e.g., Cryptographic Algorithm,
972 Cryptographic Length, etc). Attributes and Template Names MAY be specified for both keys at the same
973 time by specifying a Common Template-Attribute object in the request. Attributes not common to both
974 keys (e.g., Name, Cryptographic Usage Mask) MAY be specified using the Private Key Template-Attribute
975 and Public Key Template-Attribute objects in the request, which take precedence over the Common
976 Template-Attribute object.

977 A Link Attribute is automatically created by the server for each object, pointing to the corresponding
978 object. The response contains the Unique Identifiers of both created objects. The ID Placeholder value
979 SHALL be set to the Unique Identifier of the Private Key.

Request Payload		
Object	REQUIRED	Description
Common Template-Attribute, see 2.1.8	No	Specifies desired attributes in templates and/or as individual attributes that apply to both the Private and Public Key Objects.
Private Key Template-Attribute, see 2.1.8	No	Specifies templates and/or attributes that apply to the Private Key Object. Order of precedence applies.
Public Key Template-Attribute, see 2.1.8	No	Specifies templates and/or attributes that apply to the Public Key Object. Order of precedence applies.

Table 107: Create Key Pair Request Payload

980

981 For multi-instance attributes, the union of the values found in the templates and attributes of the
982 Common, Private, and Public Key Template-Attribute is used. For single-instance attributes, the order of
983 precedence is as follows:

- 984 1. attributes specified explicitly in the Private and Public Key Template-Attribute, then
985 2. attributes specified via templates in the Private and Public Key Template-Attribute, then
986 3. attributes specified explicitly in the Common Template-Attribute, then
987 4. attributes specified via templates in the Common Template-Attribute

988 If there are multiple templates in the Common, Private, or Public Key Template-Attribute, then the
989 subsequent value of the single-instance attribute takes precedence.

Response Payload		
Object	REQUIRED	Description
Private Key Unique Identifier, see 3.1	Yes	The Unique Identifier of the newly created Private Key object.
Public Key Unique Identifier, see 3.1	Yes	The Unique Identifier of the newly created Public Key object.
Private Key Template-Attribute, see 2.1.8	No	An OPTIONAL list of attributes, for the Private Key Object, with values that were not specified in the request, but have been implicitly set by the key management server.
Public Key Template-Attribute, see 2.1.8	No	An OPTIONAL list of attributes, for the Public Key Object, with values that were not specified in the request, but have been implicitly set by the key management server.

Table 108: Create Key Pair Response Payload

990
 991 | [Table 109](#) indicates which attributes SHALL be included in the Create Key pair request using Template-
 992 Attribute objects, as well as which attributes SHALL have the same value for the Private and Public Key.

Deleted: Table 109

Attribute	REQUIRED	SHALL contain the same value for both Private and Public Key
Cryptographic Algorithm, see 3.4	Yes	Yes
Cryptographic Length, see 3.5	Yes	Yes
Cryptographic Usage Mask, see 3.14	Yes	No
Cryptographic Domain Parameters, see 3.7	No	Yes
Cryptographic Parameters, see 3.6	No	Yes

Table 109: Create Key Pair Attribute Requirements

993
 994 **4.3 Register**

995 This operation requests the server to register a Managed Object that was created by the client or
 996 obtained by the client through some other means, allowing the server to manage the object. The
 997 arguments in the request are similar to those in the Create operation, but also MAY contain the object
 998 itself, for storage by the server. Optionally, objects that are not to be stored by the key management
 999 system MAY be omitted from the request (e.g., private keys).

1000 The request contains information about the type of object being registered and some of the attributes to
 1001 be assigned to the object (e.g., Cryptographic Algorithm, Cryptographic Length, etc). This information
 1002 MAY be specified by the use of a Template-Attribute object.

1003 The response contains the Unique Identifier assigned by the server to the registered object. The server
 1004 SHALL copy the Unique Identifier returned by this operations into the ID Placeholder variable. The Initial
 1005 Date attribute of the object SHALL be set to the current time.

Request Payload		
Object	REQUIRED	Description
Object Type, see 3.3	Yes	Determines the type of object being registered.
Template-Attribute, see 2.1.8	Yes	Specifies desired object attributes using templates and/or individual attributes.
Certificate, Symmetric Key, Private Key, Public Key, Split Key, Secret Data or Opaque Object, see 2.2	No	The object being registered. The object and attributes MAY be wrapped. Some objects (e.g., Private Keys), MAY be omitted from the request.

1006

Table 110: Register Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the newly registered object.
Template-Attribute, see 2.1.8	No	An OPTIONAL list of object attributes with values that were not specified in the request, but have been implicitly set by the key management server.

1007

Table 111: Register Response Payload

1008 If a Managed Cryptographic Object is registered, then the following attributes SHALL be included in the
 1009 Register request, either explicitly, or via specification of a template that contains the attribute.

Attribute	REQUIRED
Cryptographic Algorithm, see 3.4	Yes, MAY be omitted only if this information is encapsulated in the Key Block. Does not apply to Secret Data. If present, then Cryptographic Length below SHALL also be present.
Cryptographic Length, see 3.5	Yes, MAY be omitted only if this information is encapsulated in the Key Block. Does not apply to Secret Data. If present, then Cryptographic Algorithm above SHALL also be present.
Cryptographic Usage Mask, see 3.14	Yes.

1010

Table 112: Register Attribute Requirements

1011 **4.4 Re-key**

1012 This request is used to generate a replacement key for an existing symmetric key. It is analogous to the
1013 Create operation, except that attributes of the replacement key are copied from the existing key, with the
1014 exception of the attributes listed in [Table 114](#).

Deleted: Table 114

1015 As the replacement key takes over the name attribute of the existing key, Re-key SHOULD only be
1016 performed once on a given key.

1017 The server SHALL copy the Unique Identifier of the replacement key returned by this operation into the ID
1018 Placeholder variable.

1019 As a result of Re-key, the Link attribute is set to point to the replacement key.

1020 An *Offset* MAY be used to indicate the difference between the Initialization Date and the Activation Date
1021 of the replacement key. If Offset is set and dates exist for the existing key, then the dates of the
1022 replacement key SHALL be set based on the dates of the existing key as follows:

Attribute in Existing Key	Attribute in Replacement Key
Initial Date (IT_1)	Initial Date (IT_2) $> IT_1$
Activation Date (AT_1)	Activation Date (AT_2) = $IT_2 + Offset$
Process Start Date (CT_1)	Process Start Date = $CT_1 + (AT_2 - AT_1)$
Protect Stop Date (TT_1)	Protect Stop Date = $TT_1 + (AT_2 - AT_1)$
Deactivation Date (DT_1)	Deactivation Date = $DT_1 + (AT_2 - AT_1)$

1023 **Table 113: Computing New Dates from Offset during Re-key**

1024 Attributes that are not copied from the existing key and are handled in a specific way are:

Attribute	Action
Initial Date, see 3.18	Set to the current time
Destroy Date, see 3.23	Not set
Compromise Occurrence Date, see 3.24	Not set
Compromise Date, see 3.25	Not set
Revocation Reason, see 3.26	Not set
Unique Identifier, see 3.1	New value generated
Usage Limits, see 3.16	The Total Bytes/Total Objects value is copied from the existing key, while the Byte Count/Object Count values are set to the Total Bytes/Total Objects.
Name, see 3.2	Set to the name(s) of the existing key; all name attributes of the existing key are removed.
State, see 3.17	Set based on attributes values, such as dates, as shown in Table 113 .
Digest, see 3.12	Recomputed from the new key value
Link, see 3.29	Set to point to the existing key as the replaced key
Last Change Date, see 3.32	Set to current time

Formatted: Font: 10 pt

Deleted: Table 113

Formatted: Font: 10 pt

Formatted: Font: 10 pt

1025

Table 114: Re-key Attribute Requirements

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the existing Symmetric Key being re-keyed. If omitted, then the ID Placeholder is substituted by the server.
Offset	No	An Interval object indicating the difference between the Initialization Date and the Activation Date of the replacement key to be created.
Template-Attribute, see 2.1.8	No	Specifies desired object attributes using templates and/or individual attributes.

1026

Table 115: Re-key Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the newly-created replacement Symmetric Key.
Template-Attribute, see 2.1.8	No	An OPTIONAL list of object attributes with values that were not specified in the request, but have been implicitly set by the key management server.

Table 116: Re-key Response Payload

1027

1028 4.5 Derive Key

1029 This request is used to derive a symmetric key using a key or secret data that is already known to the key
 1030 management system. It SHALL only apply to Managed Cryptographic Objects that have the Derive Key
 1031 bit set in the Cryptographic Usage Mask attribute of the specified Managed Object (i.e., are able to be
 1032 used for key derivation). If the operation is issued for an object that does not have this bit set, then the
 1033 server SHALL return an error. For all derivation methods, the client SHALL specify the desired length of
 1034 the derived key or secret using the Cryptographic Length attribute. If a key is created, then the client
 1035 SHALL specify both its Cryptographic Length and Cryptographic Algorithm. If the specified length
 1036 exceeds the output of the derivation method, then the server SHALL return an error. Clients MAY derive
 1037 multiple keys and IVs by requesting the creation of a Secret Data object and specifying a Cryptographic
 1038 Length that is the total length of the derived object. The length SHALL NOT exceed the length of the
 1039 output returned by the chosen derivation method.

1040 The fields in the request specify the Unique Identifiers of the keys or secrets to be used for derivation
 1041 (e.g., some derivation methods MAY require multiple keys or secrets to derive the result), the method to
 1042 be used to perform the derivation, and any parameters needed by the specified method. The method is
 1043 specified as an enumerated value. Currently defined derivation methods include:

- 1044 • *PBKDF2* – This method is used to derive a symmetric key from a password or pass phrase. The
 1045 *PBKDF2* method is published in [PKCS#5] and [RFC2898].
- 1046 • *HASH* – This method derives a key by computing a hash over the derivation key or the derivation
 1047 data.
- 1048 • *HMAC* – This method derives a key by computing an HMAC over the derivation data.
- 1049 • *ENCRYPT* – This method derives a key by encrypting the derivation data.
- 1050 • *NIST800-108-C* – This method derives a key by computing the KDF in Counter Mode as specified
 1051 in ~~[SP800-108]~~.
- 1052 • *NIST800-108-F* – This method derives a key by computing the KDF in Feedback Mode as
 1053 specified in ~~[SP800-108]~~.
- 1054 • *NIST800-108-DPI* – This method derives a key by computing the KDF in Double-Pipeline Iteration
 1055 Mode as specified in ~~[SP800-108]~~.
- 1056 • *Extensions*

Deleted: [SP800-108]

Deleted: [SP800-108]

Deleted: [SP800-108]

1057 The server SHALL perform the derivation function, and then register the derived object as a new
 1058 Managed Object, returning the new Unique Identifier for the new object in the response. The server
 1059 SHALL copy the Unique Identifier returned by this operation into the ID Placeholder variable.

1060 As a result of Derive Key, the Link attributes (i.e., Derived Key Link in the objects from which the key is
 1061 derived, and the Derivation Base Object Link in the derived key) of all objects involved SHALL be set to
 1062 point to the corresponding objects.

Request Payload		
Object	REQUIRED	Description
Object Type, see 3.3	Yes	Determines the type of object to be created.
Unique Identifier, see 3.1	Yes. MAY be repeated	Determines the object or objects to be used to derive a new key. At most, two identifiers MAY be specified: one for the derivation key and another for the secret data. Note that the ID Placeholder SHALL NOT be used here.
Derivation Method, see 9.1.3.2.20	Yes	An Enumeration object specifying the method to be used to derive the new key.
Derivation Parameters, see below	Yes	A Structure object containing the parameters needed by the specified derivation method.
Template-Attribute, see 2.1.8	Yes	Specifies desired object attributes using templates and/or individual attributes; the length and algorithm SHALL always be specified for the creation of a symmetric key.

1063

Table 117: Derive Key Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the newly derived key.
Template-Attribute, see 2.1.8	No	An OPTIONAL list of object attributes with values that were not specified in the request, but have been implicitly set by the key management server.

1064

Table 118: Derive Key Response Payload

1065 The *Derivation Parameters* for all derivation methods consist of the following parameters, except
 1066 PBKDF2, which requires two additional parameters.

Object	Encoding	REQUIRED
Derivation Parameters	Structure	Yes
Cryptographic Parameters, see 3.6	Structure	Yes, except for HMAC derivation keys.
Initialization Vector	Byte String	No, depends on PRF and mode of operation: empty IV is assumed if not provided.
Derivation Data	Byte String	Yes, unless the Unique Identifier of a Secret Data object is provided.

1067

Table 119: Derivation Parameters Structure (Except PBKDF2)

1068 Cryptographic Parameters identify the Pseudorandom Function (PRF) or the mode of operation of the
 1069 PRF (e.g., if a key is to be derived using the HASH derivation method, then clients are REQUIRED to
 1070 indicate the hash algorithm inside Cryptographic Parameters; similarly, if a key is to be derived using AES
 1071 in CBC mode, then clients are REQUIRED to indicate the Block Cipher Mode). The server SHALL verify
 1072 that the specified mode matches one of the instances of Cryptographic Parameters set for the
 1073 corresponding key. If Cryptographic Parameters are omitted, then the server SHALL select the
 1074 Cryptographic Parameters with the lowest Attribute Index for the specified key. If the corresponding key
 1075 does not have any Cryptographic Parameters attribute, or if no match is found, then an error is returned.

1076 If a key is derived using HMAC, then the attributes of the derivation key provide enough information about
 1077 the PRF and the Cryptographic Parameters are ignored.

1078 Derivation Data is either the data to be encrypted, hashed, or HMACed. For the NIST SP 800-108
 1079 methods **[SP800-108]**, Derivation Data is Label||{0x00}||Context, where the all-zero byte is OPTIONAL.

Deleted: [SP800-108]

1080 Most derivation methods (e.g., ENCRYPT) require a derivation key and the derivation data to be
 1081 encrypted. The HASH derivation method requires either a derivation key or derivation data. Derivation
 1082 data MAY either be explicitly provided by the client with the Derivation Data field or implicitly provided by
 1083 providing the Unique Identifier of a Secret Data object. If both are provided, then an error SHALL be
 1084 returned.

1085 The PBKDF2 derivation method requires two additional parameters:

Object	Encoding	REQUIRED
Derivation Parameters	Structure	Yes
Cryptographic Parameters, see 3.6	Structure	No, depends on the PRF.
Initialization Vector	Byte String	No, depends on the PRF and mode of operation: an empty IV is assumed if not provided.
Derivation Data	Byte String	Yes, unless the Unique Identifier of a Secret Data object is provided.
Salt	Byte String	Yes
Iteration Count	Integer	Yes

1086 **Table 120: PBKDF2 Derivation Parameters Structure**

1087 4.6 Certify

1088 This request is used to generate a Certificate object for a public key. This request supports certification of
 1089 a new public key as well as certification of a public key that has already been certified (i.e., certificate
 1090 update). Only a single certificate SHALL be requested at a time. Server support for this operation is
 1091 OPTIONAL, as it requires that the key management system have access to a certification authority (CA).
 1092 If the server does not support this operation, an error SHALL be returned.

1093 Requests are passed as Byte Strings, which allow multiple certificate request types for X.509 certificates
 1094 (e.g., PKCS#10, PEM, etc) or PGP certificates to be submitted to the server.

1095 The generated Certificate object whose Unique Identifier is returned MAY be obtained by the client via a
 1096 Get operation in the same batch, using the ID Placeholder mechanism.

1097 As a result of Certify, the Link attribute of the Public Key and of the generated certificate SHALL be set to
 1098 point at each other.

1099 The server SHALL copy the Unique Identifier of the generated certificate returned by this operation into
 1100 the ID Placeholder variable.

1101 If the information in the Certificate Request conflicts with the attributes specified in the Template-Attribute,
 1102 then the information in the Certificate Request takes precedence.

Object	Request Payload	
	REQUIRED	Description
Unique Identifier, see 3.1	No	The Unique Identifier of the Public Key being certified. If omitted, then the ID Placeholder is substituted by the server.
Certificate Request Type, see 9.1.3.2.21	Yes	An Enumeration object specifying the type of certificate request.
Certificate Request	Yes	A Byte String object with the certificate request.
Template-Attribute, see 2.1.8	No	Specifies desired object attributes using templates and/or individual attributes.

1103 **Table 121: Certify Request Payload**

Object	Response Payload	
	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the generated Certificate object.
Template-Attribute, see 2.1.8	No	An OPTIONAL list of object attributes with values that were not specified in the request, but have been implicitly set by the key management server.

1104 **Table 122: Certify Response Payload**

1105 **4.7 Re-certify**

1106 This request is used to renew an existing certificate with the same key pair. Only a single certificate
 1107 SHALL be renewed at a time. Server support for this operation is OPTIONAL, as it requires that the key
 1108 management system to have access to a certification authority (CA). If the server does not support this
 1109 operation, an error SHALL be returned.

1110 Requests are passed as Byte Strings, which allow multiple certificate request types for X.509 certificates
 1111 (e.g., PKCS#10, PEM, etc) or PGP certificates to be submitted to the server.

1112 The server SHALL copy the Unique Identifier of the new certificate returned by this operation into the ID
 1113 Placeholder variable.

1114 If the information in the Certificate Request field in the request conflicts with the attributes specified in the
 1115 Template-Attribute, then the information in the Certificate Request takes precedence.

1116 As the new certificate takes over the name attribute of the existing certificate, Re-certify SHOULD only be
 1117 performed once on a given certificate.

1118 The Link attribute of the existing certificate and of the new certificate are set to point at each other. The
 1119 Link attribute of the Public Key is changed to point to the new certificate.

1120 An *Offset* MAY be used to indicate the difference between the Initialization Date and the Activation Date
 1121 of the new certificate. If Offset is set, then the dates of the new certificate SHALL be set based on the
 1122 dates of the existing certificate (if such dates exist) as follows:

Attribute in Existing Certificate	Attribute in New Certificate
-----------------------------------	------------------------------

Initial Date (IT_1)	Initial Date (IT_2) > IT_1
Activation Date (AT_1)	Activation Date (AT_2) = IT_2 + Offset
Deactivation Date (DT_1)	Deactivation Date = DT_1 + (AT_2 - AT_1)

Table 123: Computing New Dates from Offset during Re-certify

1123
1124 Attributes that are not copied from the existing certificate and that are handled in a specific way are:

Attribute	Action
Initial Date, see 3.18	Set to current time
Destroy Date, see 3.23	Not set
Revocation Reason, see 3.26	Not set
Unique Identifier, see 3.2	New value generated
Name, see 3.2	Set to the name(s) of the existing certificate; all name attributes of the existing certificate are removed.
State, see 3.17	Set based on attributes values, such as dates, as shown in Table 123 .
Digest, see 3.12	Recomputed from the new certificate value.
Link, see 3.29	Set to point to the existing certificate as the replaced certificate.
Last Change Date, see 3.32	Set to current time

Formatted: Font: 10 pt

Deleted: Table 123

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Table 124: Re-certify Attribute Requirements

1125

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	The Unique Identifier of the Certificate being renewed. If omitted, then the <i>ID Placeholder</i> is substituted by the server.
Certificate Request Type, see 9.1.3.2.21	Yes	An Enumeration object specifying the type of certificate request.
Certificate Request	Yes	A Byte String object with the certificate request.
Offset	No	An Interval object indicating the difference between the Initialization Time of the new certificate and the Activation Date of the new certificate.
Template-Attribute, see 2.1.8	No	Specifies desired object attributes using templates and/or individual attributes.

1126

T able 125: Re-certify Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the new certificate.
Template-Attribute, see 2.1.8	No	An OPTIONAL list of object attributes with values that were not specified in the request, but have been implicitly set by the key management server.

1127

Table 126: Re-certify Response Payload

1128 4.8 Locate

1129 This operation requests that the server search for one or more Managed Objects, specified by one or
 1130 more attributes. All attributes are allowed to be used. However, no attributes specified in the request
 1131 SHOULD contain Attribute Index values. Attribute Index values SHALL be ignored by the Locate
 1132 operation. The request MAY also contain a *Maximum Items* field, which specifies the maximum number of
 1133 objects to be returned. If the Maximum Items field is omitted, then the server MAY return all objects
 1134 matched, or MAY impose an internal maximum limit due to resource limitations.

1135 If more than one object satisfies the identification criteria specified in the request, then the response MAY
 1136 contain Unique Identifiers for multiple Managed Objects. Returned objects SHALL match **all** of the
 1137 attributes in the request. If no objects match, then an empty response payload is returned.

1138 The server returns a list of Unique Identifiers of the found objects, which then MAY be retrieved using the
 1139 Get operation. If the objects are archived, then the Recover and Get operations are REQUIRED to be
 1140 used. If a single Unique Identifier is returned to the client, then the server SHALL copy the Unique
 1141 Identifier returned by this operation into the ID Placeholder variable. If the Locate operation matches
 1142 more than one object, and the Maximum Items value is omitted in the request, or is set to a value larger
 1143 than one, then the server SHALL NOT set the ID Placeholder value, causing any subsequent operations
 1144 that are batched with the Locate, and which do not specify a Unique Identifier explicitly, to fail. This
 1145 ensures that these batched operations SHALL proceed only if a single object is returned by Locate.

1146 When using the Name or Object Group attributes for identification, wild-cards or regular expressions

1147 (defined, e.g., in [ISO/IEC 9945-2]) MAY be supported by specific key management system
 1148 implementations.

1149 The Date attributes (e.g., Initial Date, Activation Date, etc) are used to specify a time or a time range. If a
 1150 single instance of a given Date attribute is used (e.g., the Activation Date), then objects with the same
 1151 Date attribute are considered to be matching candidate objects. If two instances of the same Date
 1152 attribute are used (i.e., with two different values specifying a range), then objects for which the Date
 1153 attribute is inside or at a limit of the range are considered to be matching candidate objects. If a Date
 1154 attribute is set to its largest possible value, then it is equivalent to an undefined attribute. The KMIP
 1155 Usage Guide [KMIP-UG] provides examples.

1156 When the Cryptographic Usage Mask attribute is specified in the request, candidate objects are
 1157 compared against this field via an operation that consists of a logical AND of the requested mask with the
 1158 mask in the candidate object, and then a comparison of the resulting value with the requested mask. For
 1159 example, if the request contains a mask value of 10001100010000, and a candidate object mask contains
 1160 10000100010000, then the logical AND of the two masks is 10000100010000, which is compared against
 1161 the mask value in the request (10001100010000) and fails the match. This means that a matching
 1162 candidate object has all of the bits set in its mask that are set in the requested mask, and MAY have
 1163 additional bits set.

1164 When the Usage Allocation attribute is specified in the request, matching candidate objects SHALL have
 1165 an Object or Byte Count and Total Objects or Bytes equal to or larger than the values specified in the
 1166 request.

1167 When an attribute that is defined as a structure is specified, all of the structure fields are not REQUIRED
 1168 to be specified. For instance, for the Link attribute, if the Linked Object Identifier value is specified without
 1169 the Link Type value, then matching candidate objects have the Linked Object Identifier as specified,
 1170 irrespective of their Link Type.

1171 The Storage Status Mask field (see Section 9.1.3.3.2) is used to indicate whether only on-line objects,
 1172 only archived objects, or both on-line and archived objects are to be searched. Note that the server MAY
 1173 store attributes of archived objects in order to expedite Locate operations that search through archived
 1174 objects.

Request Payload		
Object	REQUIRED	Description
Maximum Items	No	An Integer object that indicates the maximum number of object identifiers the server SHALL return.
Storage Status Mask, see 9.1.3.3.2	No	An Integer object (used as a bit mask) that indicates whether only on-line objects, only archived objects, or both on-line and archived objects are to be searched. If omitted, then on-line only is assumed.
Attribute, see 3	Yes, MAY be repeated	Specifies an attribute and its value that are REQUIRED to match the desired object.

1175 **Table 127: Locate Request Payload**

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No, MAY be repeated	The Unique Identifier of the located objects.

1176 **Table 128: Locate Response Payload**

1177 4.9 Check

1178 This operation requests that the server check for the use of a Managed Object according to values
1179 specified in the request. This operation SHOULD only be used when placed in a batched set of
1180 operations, usually following a Locate, Create, Create Pair, Derive Key, Certify, Re-Certify or Re-Key
1181 operation, and followed by a Get operation. The Unique Identifier field in the request MAY be omitted if
1182 the operation is in a batched set of operations and follows an operation that sets the ID Placeholder
1183 variable.

1184 If the server determines that the client is allowed to use the object according to the specified attributes,
1185 then the server returns the Unique Identifier of the object.

1186 If the server determines that the client is not allowed to use the object according to the specified
1187 attributes, then the server invalidates the ID Placeholder value and does not return the Unique Identifier,
1188 and the operation returns the set of attributes specified in the request that caused the server policy denial.
1189 The only attributes returned are those that resulted in the server determining that the client is not allowed
1190 to use the object, thus allowing the client to determine how to proceed. The operation also returns a
1191 failure, and the server SHALL ignore any subsequent operations in the batch.

1192 The additional objects that MAY be specified in the request are limited to:

- 1193 • Usage Limits Byte Count or Usage Limits Object Count (see Section 3.16) – The request MAY
1194 contain the usage amount that the client deems necessary to complete its needed function. This
1195 does not require that any subsequent Get Usage Allocation operations request this amount. It
1196 only means that the client is ensuring that the amount specified is available.
- 1197 • Cryptographic Usage Mask – This is used to specify the cryptographic operations for which the
1198 client intends to use the object (see Section 3.14). This allows the server to determine if the
1199 policy allows this client to perform these operations with the object. Note that this MAY be a
1200 different value from the one specified in a Locate operation that precedes this operation. Locate,
1201 for example, MAY specify a Cryptographic Usage Mask requesting a key that MAY be used for
1202 both Encryption and Decryption, but the value in the Check operation MAY specify that the client
1203 is only using the key for Encryption at this time.
- 1204 • Lease Time – This specifies a desired lease time (see Section 3.15). The client MAY use this to
1205 determine if the server allows the client to use the object with the specified lease or longer.
1206 Including this attribute in the Check operation does not actually cause the server to grant a lease,
1207 but only indicates that the requested lease time value MAY be granted if requested by a
1208 subsequent, batched, Obtain Lease operation.

1209 Note that these objects are not encoded in an Attribute structure as shown in Section 2.1.1

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being checked. If omitted, then the ID Placeholder is substituted by the server.
Usage Limits Byte Count, see 3.16	No	Specifies the number of bytes to be protected to be checked against server policy. SHALL NOT be present if Usage Limits Object Count is present.
Usage Limits Object Count, see 3.16	No	Specifies the number of objects to be protected to be checked against server policy. SHALL NOT be present if Usage Limits Byte Count is present.
Cryptographic Usage Mask, see 3.14	No	Specifies the Cryptographic Usage for which the client intends to use the object.
Lease Time, see 3.15	No	Specifies a Lease Time value that the Client is asking the server to validate against server policy.

1210

Table 129: Check Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object.
Usage Limits Byte Count, see 3.16	No	Returned by the Server if the Usage Limits value specified in the Request Payload is larger than the value that the server policy allows. SHALL NOT be present if Usage Limits Object Count is present.
Usage Limits Object Count, see 3.16	No	Returned by the Server if the Usage Limits value specified in the Request Payload is larger than the value that the server policy allows. SHALL NOT be present if Usage Limits Byte Count is present.
Cryptographic Usage Mask, see 3.14	No	Returned by the Server if the Cryptographic Usage Mask specified in the Request Payload is rejected by the server for policy violation.
Lease Time, see 3.15	No	Returned by the Server if the Lease Time value in the Request Payload is larger than a valid Lease Time that the server MAY grant.

1211

Table 130: Check Response Payload

1212 The encodings of the Usage limits Byte and Object Counts is as shown in Section 3.16

1213 **4.10 Get**

1214 This operation requests that the server returns the Managed Object specified in the request by its Unique
 1215 Identifier. The Unique Identifier field in the request MAY be omitted if the *Get* operation is in a batched set
 1216 of operations and follows an operation that sets the ID Placeholder variable.

1217 Only a single object is returned. The response contains the Unique Identifier of the object, along with the
 1218 object itself, which MAY be wrapped using a wrapping key specified in the request.

1219 The following key format restrictions apply when requesting the server to return an object in a particular
 1220 format:

- 1221 • If a client registers a key in a given format, the server SHALL be able to return the key during the
 1222 Get operation in at least that same format as it was registered.
- 1223 • Any other format conversion MAY optionally be supported by the server.

1224

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being requested. If omitted, then the ID Placeholder is substituted by the server.
Key Format Type, see 9.1.3.2.3	No	Determines the key format type to be returned
Key Compression Type, see 9.1.3.2.2	No	Determines the compression method for elliptic curve public keys
Key Wrapping Specification, see 2.1.6	No	Specifies keys and other information for wrapping the returned object. This field SHALL NOT be specified if the requested object is a Template.

1225 **Table 131: Get Request Payload**

Response Payload		
Object	REQUIRED	Description
Object Type, see 3.3	Yes	Type of object
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object
Certificate, Symmetric Key, Private Key, Public Key, Split Key, Template, Secret Data, or Opaque Object, see 2.2	Yes	The cryptographic object being returned

1226 **Table 132: Get Response Payload**

1227 **4.11 Get Attributes**

1228 This operation returns one or more attributes of a Managed Object. The object is specified by its Unique
 1229 Identifier and the attributes are specified by their name in the request. If a specified attribute has multiple
 1230 instances, then all instances are returned. If a specified attribute does not exist (i.e., has no value), then it
 1231 SHALL NOT be present in the returned response. If no requested attributes exist, then the response
 1232 SHALL consist only of the Unique Identifier.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object whose attributes are being requested. If omitted, then the ID Placeholder is substituted by the server.
Attribute Name, see 2.1.1	Yes, MAY be repeated	Specifies a desired attribute of the object

1233

Table 133: Get Attributes Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object
Attribute, see 2.1.1	No, MAY be repeated	The requested attribute for the object

1234

Table 134: Get Attributes Response Payload

1235 4.12 Get Attribute List

1236 This operation returns a list of the attribute names associated with a Managed Object. The object is
1237 specified by its Unique Identifier.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object whose attribute names are being requested. If omitted, then the ID Placeholder is substituted by the server.

1238

Table 135: Get Attribute List Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object
Attribute Name, see 2.1.1	Yes, MAY be repeated	The requested attribute names for the object

1239

Table 136: Get Attribute List Response Payload

1240 4.13 Add Attribute

1241 This request adds a new attribute instance to a Managed Object and sets its value. The request contains
1242 the Unique Identifier of the Managed Object to which the attribute pertains, and the attribute name and
1243 value. For non multi-instance attributes, this is how they are created. For multi-instance attributes, this is
1244 how the first and subsequent values are created. Existing attribute values SHALL only be changed by the
1245 Modify Attribute operation. Read-Only attributes SHALL NOT be added using the Add Attribute operation.
1246 No Attribute Index SHALL be specified in the request. The response returns a new Attribute Index if the
1247 attribute being added is allowed to have multiple instances. Multiple Add Attribute requests MAY be
1248 included in a single batched request to add multiple attributes.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	The Unique Identifier of the object. If omitted, then the ID Placeholder is substituted by the server.
Attribute, see 2.1.1	Yes	Specifies the attribute of the object to be added.

Table 137: Add Attribute Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object
Attribute, see 2.1.1	Yes	The added attribute

Table 138: Add Attribute Response Payload

4.14 Modify Attribute

This request modifies the value of an existing attribute instance associated with a Managed Object. The request contains the Unique Identifier of the Managed Object whose attribute is to be modified, and the attribute name, OPTIONAL Attribute Index, and new value. Only existing attributes MAY be changed via this operation. New attributes SHALL only be added by the Add Attribute operation. Read-Only attributes SHALL NOT be changed using this operation. If an Attribute Index is specified, then only the specified instance is modified. If the attribute has multiple instances, and no Attribute Index is specified in the request, then the Attribute Index is assumed to be 0. If the attribute does not support multiple instances, then the Attribute Index SHALL NOT be specified. Specifying an Attribute Index for which there exists no Attribute Value SHALL result in an error.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	The Unique Identifier of the object. If omitted, then the ID Placeholder is substituted by the server.
Attribute, see 2.1.1	Yes	Specifies the attribute of the object to be modified.

Table 139: Modify Attribute Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object
Attribute, see 2.1.1	Yes	The modified attribute

Table 140: Modify Attribute Response Payload

4.15 Delete Attribute

This request deletes an attribute associated with a Managed Object. The request contains the Unique Identifier of the Managed Object whose attribute is to be deleted, the attribute name, and optionally the Attribute Index of the attribute. REQUIRED attributes and Read-Only attributes SHALL NOT be deleted by this operation. If no Attribute Index is specified, and the Attribute whose name is specified has multiple

1268 instances, then the operation is rejected. Note that only a single attribute SHALL be deleted at a time.
 1269 Multiple delete operations (e.g., possibly batched) are necessary to delete several attributes. Attempting
 1270 to delete a non-existent attribute or specifying an Attribute Index for which there exists no Attribute Value
 1271 SHALL result in an error.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object whose attributes are being deleted. If omitted, then the ID Placeholder is substituted by the server.
Attribute Name, see 2.1.1	Yes	Specifies the name of the attribute to be deleted.
Attribute Index, see 2.1.1	No	Specifies the Index of the Attribute.

1272 **Table 141: Delete Attribute Request Payload**

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object
Attribute, see 2.1.1	Yes	The deleted attribute

1273 **Table 142: Delete Attribute Response Payload**

1274 **4.16 Obtain Lease**

1275 This request is used to obtain a new *Lease Time* for a specified Managed Object. The Lease Time is an
 1276 interval value that determines when the client's internal cache of information about the object expires and
 1277 needs to be renewed. If the returned value of the lease time is zero, then the server is indicating that no
 1278 lease interval is effective, and the client MAY use the object without any lease time limit. If a client's lease
 1279 expires, then the client SHALL NOT use the associated cryptographic object until a new lease is
 1280 obtained. If the server determines that a new lease SHALL NOT be issued for the specified cryptographic
 1281 object, then the server SHALL respond to the Obtain Lease request with an error.

1282 The response payload for the operation also contains the current value of the Last Change Date attribute
 1283 for the object. This MAY be used by the client to determine if any of the attributes cached by the client
 1284 need to be refreshed, by comparing this time to the time when the attributes were previously obtained.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object for which the lease is being obtained. If omitted, then the <i>ID Placeholder</i> is substituted by the server.

1285 **Table 143: Obtain Lease Request Payload**

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object.
Lease Time, see 3.15	Yes	An interval (in seconds) that specifies the amount of time that the object MAY be used until a new lease needs to be obtained.
Last Change Date, see 3.32	Yes	The date and time indicating when the latest change was made to the contents or any attribute of the specified object.

1286

Table 144: Obtain Lease Response Payload

1287

4.17 Get Usage Allocation

1288 This request is used to obtain an allocation from the current Usage Limits values to allow the client to use
 1289 the Managed Cryptographic Object for applying cryptographic protection. The allocation only applies to
 1290 Managed Cryptographic Objects that are able to be used for applying protection (e.g., symmetric keys for
 1291 encryption, private keys for signing, etc.) and is only valid if the Managed Cryptographic Object has a
 1292 Usage Limits attribute. Usage for processing cryptographically-protected information (e.g., decryption,
 1293 verification, etc.) is not limited and is not able to be allocated. A Managed Cryptographic Object that has a
 1294 Usage Limits attribute SHALL NOT be used by a client for applying cryptographic protection unless an
 1295 allocation has been obtained using this operation. The operation SHALL only be requested during the
 1296 time that protection is enabled for these objects (i.e., after the Activation Date and before the Protect Stop
 1297 Date). If the operation is requested for an object that has no Usage Limits attribute, or is not an object that
 1298 MAY be used for applying cryptographic protection, then the server SHALL return an error.

1299 The fields in the request specify the number of bytes or number of objects that the client needs to protect.
 1300 Exactly one of the two count fields SHALL be specified in the request. If the requested amount is not
 1301 available or if the Managed Object is not able to be used for applying cryptographic protection at this time,
 1302 then the server SHALL return an error. The server SHALL assume that the entire allocated amount has
 1303 been consumed. Once the entire allocated amount has been consumed, the client SHALL NOT continue
 1304 to use the Managed Cryptographic Object for applying cryptographic protection until a new allocation is
 1305 obtained.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object whose usage allocation is being requested. If omitted, then the ID Placeholder is substituted by the server.
Usage Limits Byte Count, see 3.16	No	The number of bytes to be protected. SHALL be present if Usage Limits Object Count is not present.
Usage Limits Object Count, see 3.16	No	The number of objects to be protected. SHALL be present if Usage Limits Byte Count is not present.

1306

Table 145: Get Usage Allocation Request Payload

Response Payload		
Object	REQUIRED	Description

Unique Identifier, see 3.1	Yes	The Unique Identifier of the object.
----------------------------	-----	--------------------------------------

1307

Table 146: Get Usage Allocation Response Payload

1308 **4.18 Activate**

1309 This request is used to activate a Managed Cryptographic Object. The request SHALL NOT specify a
 1310 Template object. The request contains the Unique Identifier of the Managed Cryptographic Object. The
 1311 operation SHALL only be performed on an object in the Pre-Active state and has the effect of changing its
 1312 state to Active, and setting its Activation Date to the current date and time.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being activated. If omitted, then the ID Placeholder is substituted by the server.

1313

Table 147: Activate Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object

1314

Table 148: Activate Response Payload

1315 **4.19 Revoke**

1316 This request is used to revoke a Managed Cryptographic Object or an Opaque Object. The request
 1317 SHALL NOT specify a Template object. The request contains the unique identifier of the Managed
 1318 Cryptographic Object and a reason for the revocation (e.g., "compromised", "no longer used", etc).
 1319 Special authentication and authorization SHOULD be enforced to perform this request (see [KMIP-UG]).
 1320 Only the object creator or an authorized security officer SHOULD be allowed to issue this request. The
 1321 operation has one of two effects. If the revocation reason is "compromised", then the object is placed into
 1322 the "compromised" state, and the Compromise Date attribute is set to the current date and time.
 1323 Otherwise, the object is placed into the "deactivated" state, and the Deactivation Date attribute is set to
 1324 the current date and time.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being revoked. If omitted, then the ID Placeholder is substituted by the server.
Revocation Reason, see 3.26	Yes	Specifies the reason for revocation.
Compromise Occurrence Date, see 3.24	No	SHALL be specified if the Revocation Reason is 'compromised'.

1325

Table 149: Revoke Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object

1326

Table 150: Revoke Response Payload

1327 4.20 Destroy

1328 This request is used to indicate to the server that the key material for the specified Managed Object
1329 SHALL be destroyed. The meta-data for the key material MAY be retained by the server (e.g., used to
1330 ensure that an expired or revoked private signing key is no longer available). Special authentication and
1331 authorization SHOULD be enforced to perform this request (see [KMIP-UG]). Only the object creator or
1332 an authorized security officer SHOULD be allowed to issue this request. If the Unique Identifier specifies
1333 a Template object, then the object itself, including all meta-data, SHALL be destroyed.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being destroyed. If omitted, then the ID Placeholder is substituted by the server.

1334 Table 151: Destroy Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object

1335 Table 152: Destroy Response Payload

1336 4.21 Archive

1337 This request is used to specify that a Managed Object MAY be archived. The actual time when the object
1338 is archived, the location of the archive, or level of archive hierarchy is determined by the policies within
1339 the key management system and is not specified by the client. The request contains the unique identifier
1340 of the Managed Object. Special authentication and authorization SHOULD be enforced to perform this
1341 request (see [KMIP-UG]). Only the object creator or an authorized security officer SHOULD be allowed to
1342 issue this request. This request is only a "hint" to the key management system to possibly archive the
1343 object.

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being archived. If omitted, then the ID Placeholder is substituted by the server.

1344 Table 153: Archive Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object

1345 Table 154: Archive Response Payload

1346 4.22 Recover

1347 This request is used to obtain access to a Managed Object that has been archived. This request MAY
1348 require asynchronous polling to obtain the response due to delays caused by retrieving the object from
1349 the archive. Once the response is received, the object is now on-line, and MAY be obtained (e.g., via a
1350 Get operation). Special authentication and authorization SHOULD be enforced to perform this request
1351 (see [KMIP-UG]).

Request Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	No	Determines the object being recovered. If omitted, then the ID Placeholder is substituted by the server.

1352

Table 155: Recover Request Payload

Response Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object

1353

Table 156: Recover Response Payload

1354 4.23 Validate

1355 This requests that the server validate a certificate chain and return information on its validity. Only a
 1356 single certificate chain SHALL be included in each request. Support for this operation at the server is
 1357 OPTIONAL. If the server does not support this operation, an error SHALL be returned.

1358 The request may contain a list of certificate objects, and/or a list of Unique Identifiers that identify
 1359 Managed Certificate objects. Together, the two lists compose a certificate chain to be validated. The
 1360 request MAY also contain a date for which the certificate chain is REQUIRED to be valid.

1361 The method or policy by which validation is conducted is a decision of the server and is outside of the
 1362 scope of this protocol. Likewise, the order in which the supplied certificate chain is validated and the
 1363 specification of trust anchors used to terminate validation are also controlled by the server.

Request Payload		
Object	REQUIRED	Description
Certificate, see 2.2.1	No, MAY be repeated	One or more Certificates.
Unique Identifier, see 3.1	No, MAY be repeated	One or more Unique Identifiers of Certificate Objects.
Validity Date	No	A Date-Time object indicating when the certificate chain is valid.

1364

Table 157: Validate Request Payload

Response Payload		
Object	REQUIRED	Description
Validity Indicator, see 9.1.3.2.22	Yes	An Enumeration object indicating whether the certificate chain is valid, invalid, or unknown.

1365

Table 158: Validate Response Payload

1366 4.24 Query

1367 This request is used by the client to interrogate the server to determine its capabilities and/or protocol
 1368 mechanisms. The *Query* operation SHOULD be invocable by unauthenticated clients to interrogate server
 1369 features and functions. The *Query Function* field in the request SHALL contain one or more of the
 1370 following items:

- 1371 • Query Operations
- 1372 • Query Objects
- 1373 • Query Server Information
- 1374 • Query Application Namespaces

1375 The *Operation* fields in the response contain Operation enumerated values, which SHALL list the
 1376 OPTIONAL operations that the server supports. If the request contains a Query Operations value in the
 1377 Query Function field, then these fields SHALL be returned in the response. The OPTIONAL operations
 1378 are:

- 1379 • Validate
- 1380 • Certify
- 1381 • Re-Certify
- 1382 • Notify
- 1383 • Put

1384 The *Object Type* fields in the response contain Object Type enumerated values, which SHALL list the
 1385 object types that the server supports. If the request contains a *Query Objects* value in the Query Function
 1386 field, then these fields SHALL be returned in the response. The object types (any of which are
 1387 OPTIONAL) are:

- 1388 • Certificate
- 1389 • Symmetric Key
- 1390 • Public Key
- 1391 • Private Key
- 1392 • Split Key
- 1393 • Template
- 1394 • Secret Data
- 1395 • Opaque Object

1396 The *Server Information* field in the response is a structure containing vendor-specific fields and/or
 1397 substructures. If the request contains a *Query Server Information* value in the Query Function field, then
 1398 this field SHALL be returned in the response.

1399 The Application Namespace fields in the response contain the namespaces that the server SHALL
 1400 generate values for if requested by the client (see Section 3.30). These fields SHALL only be returned in
 1401 the response if the request contains a Query Application Namespaces value in the Query Function field.

1402 Note that the response payload is empty if there are no values to return.

Request Payload		
Object	REQUIRED	Description
Query Function, see 9.1.3.2.23	Yes, MAY be Repeated	Determines the information being queried

1403 **Table 159: Query Request Payload**

Response Payload		
Object	REQUIRED	Description
Operation, see 9.1.3.2.26	No, MAY be repeated	Specifies an Operation that is supported by the server. Only OPTIONAL operations SHALL be listed.
Object Type, see 3.3	No, MAY be repeated	Specifies a Managed Object Type that is supported by the server.
Vendor Identification	No	SHALL be returned if Query Server Information is requested. The Vendor Identification SHALL be a text string that uniquely identifies the vendor.
Server Information	No	Contains vendor-specific information possibly be of interest to the client.
Application Namespace, see 3.30	No, MAY be repeated	Specifies an Application Namespace supported by the server.

1404 **Table 160: Query Response Payload**

1405 **4.25 Cancel**

1406 This request is used to cancel an outstanding asynchronous operation. The correlation value (see Section
1407 6.8) of the original operation SHALL be specified in the request. The server SHALL respond with a
1408 *Cancellation Result* that contains one of the following values:

- 1409 • *Canceled* – The cancel operation succeeded in canceling the pending operation.
- 1410 • *Unable To Cancel* – The cancel operation is unable to cancel the pending operation.
- 1411 • *Completed* – The pending operation completed successfully before the cancellation operation
1412 was able to cancel it.
- 1413 • *Failed* – The pending operation completed with a failure before the cancellation operation was
1414 able to cancel it.
- 1415 • *Unavailable* – The specified correlation value did not match any recently pending or completed
1416 asynchronous operations.

1417 The response to this operation is not able to be asynchronous.

Request Payload		
Object	REQUIRED	Description
Asynchronous Correlation Value, see 6.8	Yes	Specifies the request being canceled

1418 **Table 161: Cancel Request Payload**

Response Payload		
Object	REQUIRED	Description
Asynchronous Correlation Value, see 6.8	Yes	Specified in the request
Cancellation Result, see 9.1.3.2.24	Yes	Enumeration indicating result of cancellation

1419 **Table 162: Cancel Response Payload**

1420 **4.26 Poll**

1421 This request is used to poll the server in order to obtain the status of an outstanding asynchronous
1422 operation. The correlation value (see Section 6.8) of the original operation SHALL be specified in the
1423 request. The response to this operation SHALL NOT be asynchronous.

Object	Request Payload	
	REQUIRED	Description
Asynchronous Correlation Value, see 6.8	Yes	Specifies the request being polled

1424 **Table 163: Poll Request Payload**

1425 The server SHALL reply with one of two responses:

1426 If the operation has not completed, the response SHALL contain no payload and a Result Status of
1427 Pending.

1428 If the operation has completed, the response SHALL contain the appropriate payload for the operation.

1429 This response SHALL be identical to the response that would have been sent if the operation had
1430 completed synchronously.

1431 5 Server-to-Client Operations

1432 Server-to-client operations are used by servers to send information or Managed Cryptographic Objects to
1433 clients via means outside of the normal client-server request-response mechanism. These operations are
1434 used to send Managed Cryptographic Objects directly to clients without a specific request from the client.

1435 5.1 Notify

1436 This operation is used to notify a client of events that resulted in changes to attributes of an object. This
1437 operation is only ever sent by a server to a client via means outside of the normal client request/response
1438 protocol, using information known to the server via unspecified configuration or administrative
1439 mechanisms. It contains the Unique Identifier of the object to which the notification applies, and a list of
1440 the attributes whose changed values have triggered the notification. The message is sent as a normal
1441 Request message, except that the Maximum Response Size, Asynchronous Indicator, Batch Error
1442 Continuation Option, and Batch Order Option fields are not allowed. The client SHALL send a response in
1443 the form of a Response Message containing no payload, unless both the client and server have prior
1444 knowledge (obtained via out-of-band mechanisms) that the client is not able to respond. Server and Client
1445 support for this message is OPTIONAL.

Message Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object.
Attribute, see 3	Yes, MAY be repeated	The attributes that have changed. This includes at least the Last Change Date attribute.

1446 **Table 164: Notify Message Payload**

1447 5.2 Put

1448 This operation is used to “push” Managed Cryptographic Objects to clients. This operation is only ever
1449 sent by a server to a client via means outside of the normal client request/response protocol, using
1450 information known to the server via unspecified configuration or administrative mechanisms. It contains
1451 the Unique Identifier of the object that is being sent, and the object itself. The message is sent as a
1452 normal Request message, except that the Maximum Response Size, Asynchronous Indicator, Batch Error
1453 Continuation Option, and Batch Order Option fields are not allowed. The client SHALL send a response in
1454 the form of a Response Message containing no payload, unless both the client and server have prior
1455 knowledge (obtained via out-of-band mechanisms) that the client is not able to respond. Server and client
1456 support for this message is OPTIONAL.

1457 The *Put Function* field indicates whether the object being “pushed” is a new object, or is a replacement for
1458 an object already known to the client (e.g., when pushing a certificate to replace one that is about to
1459 expire, the Put Function field would be set to indicate replacement, and the Unique Identifier of the
1460 expiring certificate would be placed in the *Replaced Unique Identifier* field). The Put Function SHALL
1461 contain one of the following values:

- 1462 • *New* – which indicates that the object is not a replacement for another object.
- 1463 • *Replace* – which indicates that the object is a replacement for another object, and that the
1464 Replaced Unique Identifier field is present and contains the identification of the replaced object.

1465 The Attribute field contains one or more attributes that the server is sending along with the object. The
1466 server MAY include attributes with the object to specify how the object is to be used by the client. The
1467 server MAY include a Lease Time attribute that grants a lease to the client.

1468 If the Managed Object is a wrapped key, then the key wrapping specification SHALL be exchanged prior
1469 to the transfer via out-of-band mechanisms.

Message Payload		
Object	REQUIRED	Description
Unique Identifier, see 3.1	Yes	The Unique Identifier of the object.
Put Function, see 9.1.3.2.25	Yes	Indicates function for Put message.
Replaced Unique Identifier, see 3.1	No	Unique Identifier of the replaced object. SHALL be present if the <i>Put Function</i> is <i>Replace</i> .
Certificate, Symmetric Key, Private Key, Public Key, Split Key, Template, Secret Data, or Opaque Object, see 2.2	Yes	The object being sent to the client.
Attribute, see 3	No, MAY be repeated	The additional attributes that the server wishes to send with the object.

Table 165: Put Message Payload

1470

1471 6 Message Contents

1472 The messages in the protocol consist of a message header, one or more batch items (which contain
1473 OPTIONAL message payloads), and OPTIONAL message extensions. The message headers contain
1474 fields whose presence is determined by the protocol features used (e.g., asynchronous responses). The
1475 field contents are also determined by whether the message is a request or a response. The message
1476 payload is determined by the specific operation being requested or to which is being replied.

1477 The message headers are structures that contain some of the following objects.

1478 6.1 Protocol Version

1479 This field contains the version number of the protocol, ensuring that the protocol is fully understood by
1480 both communicating parties. The version number is specified in two parts, major and minor. Servers and
1481 clients SHALL support backward compatibility with versions of the protocol with the same major version.
1482 Support for backward compatibility with different major versions is OPTIONAL.

Object	Encoding	REQUIRED
Protocol Version	Structure	
Protocol Version Major	Integer	Yes
Protocol Version Minor	Integer	Yes

1483 **Table 166: Protocol Version Structure in Message Header**

1484 6.2 Operation

1485 This field indicates the operation being requested or the operation for which the response is being
1486 returned. The operations are defined in Sections 4 and 5

Object	Encoding	
Operation	Enumeration, see 9.1.3.2.26	

1487 **Table 167: Operation in Batch Item**

1488 6.3 Maximum Response Size

1489 This field is optionally contained in a request message, and is used to indicate the maximum size of a
1490 response that the requester SHALL handle. It SHOULD only be sent in requests that possibly return large
1491 replies.

Object	Encoding	
Maximum Response Size	Integer	

1492 **Table 168: Maximum Response Size in Message Request Header**

1493 6.4 Unique Batch Item ID

1494 This field is optionally contained in a request, and is used for correlation between requests and
1495 responses. If a request has a *Unique Batch Item ID*, then responses to that request SHALL have the
1496 same Unique Batch Item ID.

Object	Encoding	
Unique Batch Item ID	Byte String	

1497 **Table 169: Unique Batch Item ID in Batch Item**

1498 **6.5 Time Stamp**

1499 This field is optionally contained in a request, is REQUIRED in a response, is used for time stamping, and
1500 MAY be used to enforce reasonable time usage at a client (e.g., a server MAY choose to reject a request
1501 if a client's time stamp contains a value that is too far off the known correct time). Note that the time
1502 stamp MAY be used by a client that has no real-time clock, but has a countdown timer, to obtain useful
1503 "seconds from now" values from all of the Date attributes by performing a subtraction.

Object	Encoding	
Time Stamp	Date-Time	

1504 **Table 170: Time Stamp in Message Header**

1505 **6.6 Authentication**

1506 This is used to authenticate the requester. It is an OPTIONAL information item, depending on the type of
1507 request being issued and on server policies. Servers MAY require authentication on no requests, a
1508 subset of the requests, or all requests, depending on policy. Query operations used to interrogate server
1509 features and functions SHOULD NOT require authentication.

1510 The authentication mechanisms are described and discussed in Section 8 .

Object	Encoding	REQUIRED
Authentication	Structure	
Credential	Structure, see 2.1.2	Yes

1511 **Table 171: Authentication Structure in Message Header**

1512 **6.7 Asynchronous Indicator**

1513 This Boolean flag indicates whether the client is able to accept an asynchronous response. It SHALL
1514 have the Boolean value True if the client is able to handle asynchronous responses, and the value False
1515 otherwise. If not present in a request, then False is assumed. If a client indicates that it is not able to
1516 handle asynchronous responses (i.e., flag is set to False), and the server is not able to process the
1517 request synchronously, then the server SHALL respond to the request with a failure.

Object	Encoding	
Asynchronous Indicator	Boolean	

1518 **Table 172: Asynchronous Indicator in Message Request Header**

1519 **6.8 Asynchronous Correlation Value**

1520 This is returned in the immediate response to an operation that requires asynchronous polling. Note: the
1521 server decides which operations are performed synchronously or asynchronously. A server-generated
1522 correlation value SHALL be specified in any subsequent Poll or Cancel operations that pertain to the
1523 original operation.

Object	Encoding	
Asynchronous Correlation Value	Byte String	

1524 **Table 173: Asynchronous Correlation Value in Response Batch Item**

1525 **6.9 Result Status**

1526 This is sent in a response message and indicates the success or failure of a request. The following values
1527 MAY be set in this field:

- 1528 • *Success* – The requested operation completed successfully.
- 1529 • *Pending* – The requested operation is in progress, and it is necessary to obtain the actual result
1530 via asynchronous polling. The asynchronous correlation value SHALL be used for the subsequent
1531 polling of the result status.
- 1532 • *Undone* – The requested operation was performed, but had to be undone (i.e., due to a failure in
1533 a batch for which the Error Continuation Option was set to Undo).
- 1534 • *Failure* – The requested operation failed.

Object	Encoding	
Result Status	Enumeration, see 9.1.3.2.27	

1535 **Table 174: Result Status in Response Batch Item**

1536 **6.10 Result Reason**

1537 This field indicates a reason for failure or a modifier for a partially successful operation and SHALL be
1538 present in responses that return a Result Status of Failure. In such a case the Result Reason SHALL be
1539 set as specified in Section 11 . It is OPTIONAL in any response that returns a Result Status of Success.
1540 The following defined values are defined for this field:

- 1541 • *Item not found* – A requested object was not found or did not exist.
- 1542 • *Response too large* – The response to a request would exceed the *Maximum Response Size* in
1543 the request.
- 1544 • *Authentication not successful* – The authentication information in the request was not able to be
1545 validated, or there was no authentication information in the request when there SHOULD have
1546 been.
- 1547 • *Invalid message* – The request message was not understood by the server.
- 1548 • *Operation not supported* – The operation requested by the request message is not supported by
1549 the server.
- 1550 • *Missing data* – The operation requires additional OPTIONAL information in the request, which
1551 was not present.
- 1552 • *Invalid field* – Some data item in the request has an invalid value.
- 1553 • *Feature not supported* – An OPTIONAL feature specified in the request is not supported.
- 1554 • *Operation canceled by requester* – The operation was asynchronous, and the operation was
1555 canceled by the Cancel operation before it completed successfully.
- 1556 • *Cryptographic failure* – The operation failed due to a cryptographic error.
- 1557 • *Illegal operation* – The client requested an operation that was not able to be performed with the
1558 specified parameters.
- 1559 • *Permission denied* – The client does not have permission to perform the requested operation.
- 1560 • *Object archived* – The object SHALL be recovered from the archive before performing the
1561 operation.
- 1562 • *General failure* – The request failed for a reason other than the defined reasons above.

Object	Encoding	
Result Reason	Enumeration, see 9.1.3.2.28	

1563

Table 175: Result Reason in Response Batch Item

1564 6.11 Result Message

1565 This field MAY be returned in a response. It contains a more descriptive error message, which MAY be
1566 used by the client to display to an end user or for logging/auditing purposes.

Object	Encoding	
Result Message	Text String	

1567

Table 176: Result Message in Response Batch Item

1568 6.12 Batch Order Option

1569 A Boolean value used in requests where the Batch Count is greater than 1. If True, then batched
1570 operations SHALL be executed in the order in which they appear within the request. If False, then the
1571 server MAY choose to execute the batched operations in any order. If not specified, then False is
1572 assumed (i.e., no implied ordering). Server support for this feature is OPTIONAL, but if the server does
1573 not support the feature, and a request is received with the batch order option set to True, then the entire
1574 request SHALL be rejected.

Object	Encoding	
Batch Order Option	Boolean	

1575

Table 177: Batch Order Option in Message Request Header

1576 6.13 Batch Error Continuation Option

1577 This option SHALL only be present if the Batch Count is greater than 1. This option SHALL have one of
1578 three values:

- 1579 • *Undo* – If any operation in the request fails, then the server SHALL undo all the previous
1580 operations.
- 1581 • *Stop* – If an operation fails, then the server SHALL NOT continue processing subsequent
1582 operations in the request. Completed operations SHALL NOT be undone.
- 1583 • *Continue* – Return an error for the failed operation, and continue processing subsequent
1584 operations in the request.

1585 If not specified, then Stop is assumed.

1586 Server support for this feature is OPTIONAL, but if the server does not support the feature, and a request
1587 is received containing the *Batch Error Continuation* option with a value other than the default Stop, then
1588 the entire request SHALL be rejected.

Object	Encoding	
Batch Error Continuation Option	Enumeration, see 9.1.3.2.29	

1589

Table 178: Batch Error Continuation Option in Message Request Header

1590 **6.14 Batch Count**

1591 This field contains the number of Batch Items in a message and is REQUIRED. If only a single operation
 1592 is being requested, then the batch count SHALL be set to 1. The Message Payload, which follows the
 1593 Message Header, contains one or more batch items.

Object	Encoding	
Batch Count	Integer	

1594 **Table 179: Batch Count in Message Header**

1595 **6.15 Batch Item**

1596 This field consists of a structure that holds the individual requests or responses in a batch, and is
 1597 REQUIRED. The contents of the batch items are described in Sections 7.2 and 7.3 .

Object	Encoding	
Batch Item	Structure	

1598 **Table 180: Batch Item in Message**

1599 **6.16 Message Extension**

1600 The *Message Extension* is an OPTIONAL structure that MAY be appended to any Batch Item. It is used
 1601 to extend protocol messages for the purpose of adding vendor specified extensions. The Message
 1602 Extension is a structure containing a Vendor Identification, a Criticality Indicator, and vendor-specific
 1603 extensions. The *Vendor Identification* SHALL be a text string that uniquely identifies the vendor, allowing
 1604 a client to determine if it is able to parse and understand the extension. If a client or server receives a
 1605 protocol message containing a message extension that it does not understand, then its actions depend
 1606 on the *Criticality Indicator*. If the indicator is True (i.e., Critical), and the receiver does not understand the
 1607 extension, then the receiver SHALL reject the entire message. If the indicator is False (i.e., Non-Critical),
 1608 and the receiver does not understand the extension, then the receiver MAY process the rest of the
 1609 message as if the extension were not present.

Object	Encoding	REQUIRED
Message Extension	Structure	
Vendor Identification	Text String	Yes
Criticality Indicator	Boolean	Yes
Vendor Extension	Structure	Yes

1610 **Table 181: Message Extension Structure in Batch Item**

1611 **7 Message Format**

1612 Messages contain the following objects and fields. All fields SHALL appear in the order specified.

1613 **7.1 Message Structure**

Object	Encoding	REQUIRED
Request Message	Structure	
Request Header	Structure, see Table 184 and Table 188	Yes
Batch Item	Structure, see Table 185 and Table 189	Yes, MAY be repeated

1614 **Table 182: Request Message Structure**

Object	Encoding	REQUIRED
Response Message	Structure	
Response Header	Structure, see Table 186 and Table 190	Yes
Batch Item	Structure, see Table 187 and Table 191	Yes, MAY be repeated

1615 **Table 183: Response Message Structure**

1616 **7.2 Synchronous Operations**

Synchronous Request Header		
Object	REQUIRED in Message	Comment
Request Header	Yes	Structure
Protocol Version	Yes	See 6.1
Maximum Response Size	No	See 6.3
Authentication	No	See 6.6
Batch Error Continuation Option	No	If omitted, then Stop is assumed, see 6.13
Batch Order Option	No	If omitted, then False is assumed, see 6.12
Time Stamp	No	See 6.5
Batch Count	Yes	See 6.14

1617 **Table 184: Synchronous Request Header Structure**

Synchronous Request Batch Item

- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt, Check spelling and grammar
- Deleted: Table 184
- Deleted: Table 188
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt, Check spelling and grammar
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Deleted: Table 189
- Formatted: Font: 10 pt, Check spelling and grammar
- Deleted: Table 185
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt, Check spelling and grammar
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt, Check spelling and grammar
- Deleted: Table 186
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt, Check spelling and grammar
- Deleted: Table 190
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt, Check spelling and grammar
- Deleted: Table 187
- Formatted: Font: 10 pt, Check spelling and grammar
- Deleted: Table 191
- Formatted: Font: 10 pt
- Formatted: Font: 10 pt

Object	REQUIRED in Message	Comment
Batch Item	Yes	Structure, see 6.15
Operation	Yes	See 6.2
Unique Batch Item ID	No	REQUIRED if <i>Batch Count</i> > 1, see 6.4
Request Payload	Yes	Structure, contents depend on the Operation, see 4 and 5
Message Extension	No	See 6.16

1618

Table 185: Synchronous Request Batch Item Structure

Synchronous Response Header		
Object	REQUIRED in Message	Comment
Response Header	Yes	Structure
Protocol Version	Yes	See 6.1
Time Stamp	Yes	See 6.5
Batch Count	Yes	See 6.14

1619

Table 186: Synchronous Response Header Structure

Synchronous Response Batch Item		
Object	REQUIRED in Message	Comment
Batch Item	Yes	Structure, see 6.15
Operation	Yes, if not a failure	See 6.2
Unique Batch Item ID	No	REQUIRED if <i>Batch Count</i> > 1, see 6.4
Result Status	Yes	See 6.9
Result Reason	No	Only present if Result Status is not <i>Success</i> , see 6.10
Result Message	No	Only present if Result Status is not <i>Success</i> , see 6.11
Response Payload	Yes, if not a failure	Structure, contents depend on the Operation, see 4 and 5
Message Extension	No	See 6.16

1620

Table 187: Synchronous Response Batch Item Structure

1621 7.3 Asynchronous Operations

1622 If the client is capable of accepting asynchronous responses, then it MAY set the *Asynchronous Indicator*
 1623 in the header of a batched request. The batched responses MAY contain a mixture of synchronous and
 1624 asynchronous responses.

Asynchronous Request Header		
Object	REQUIRED in Message	Comment
Request Header	Yes	Structure
Protocol Version	Yes	See 6.1
Maximum Response Size	No	See 6.3
Asynchronous Indicator	Yes	SHALL be set to True, see 6.7
Authentication	No	See 6.6
Batch Error Continuation Option	No	If omitted, then Stop is assumed, see 6.13
Batch Order Option	No	If omitted, then False is assumed, see 6.12
Time Stamp	No	See 6.5
Batch Count	Yes	See 6.14

1625

Table 188: Asynchronous Request Header Structure

Asynchronous Request Batch Item		
Object	REQUIRED in Message	Comment
Batch Item	Yes	Structure, see 6.15
Operation	Yes	See 6.2
Unique Batch Item ID	No	REQUIRED if <i>Batch Count</i> > 1, see 6.4
Request Payload	Yes	Structure, contents depend on the Operation, see 4 and 5
Message Extension	No	See 6.16

1626

Table 189: Asynchronous Request Batch Item Structure

Asynchronous Response Header		
Object	REQUIRED in Message	Comment
Response Header	Yes	Structure
Protocol Version	Yes	See 6.1
Time Stamp	Yes	See 6.5
Batch Count	Yes	See 6.14

1627

Table 190: Asynchronous Response Header Structure

Asynchronous Response Batch Item		
----------------------------------	--	--

Object	REQUIRED in Message	Comment
Batch Item	Yes	Structure, see 6.15
Operation	Yes, if not a failure	See 6.2
Unique Batch Item ID	No	REQUIRED if <i>Batch Count</i> > 1, see 6.4
Result Status	Yes	See 6.9
Result Reason	No	Only present if Result Status is not <i>Pending</i> or <i>Success</i> , see 6.10
Result Message	No	Only present if Result Status is not <i>Pending</i> or <i>Success</i> , see 6.11
Asynchronous Correlation Value	Yes	Only present if Result Status is <i>Pending</i> , see 6.8
Response Payload	Yes, if not a failure	Structure, contents depend on the Operation, see 4 and 5
Message Extension	No	See 6.16

Table 191: Asynchronous Response Batch Item Structure

1628

1629 **8 Authentication**

1630 The mechanisms used to authenticate the client to the server and the server to the client are not part of
1631 the message definitions, and are external to the protocol. The KMIP Server SHALL support authentication
1632 as defined in **[KMIP-Prof]**.

1633 **9 Message Encoding**

1634 To support different transport protocols and different client capabilities, a number of message-encoding
1635 mechanisms are supported.

1636 **9.1 TTLV Encoding**

1637 In order to minimize the resource impact on potentially low-function clients, one encoding mechanism to
1638 be used for protocol messages is a simplified TTLV (Tag, Type, Length, Value) scheme.

1639 The scheme is designed to minimize the CPU cycle and memory requirements of clients that need to
1640 encode or decode protocol messages, and to provide optimal alignment for both 32-bit and 64-bit
1641 processors. Minimizing bandwidth over the transport mechanism is considered to be of lesser importance.

1642 **9.1.1 TTLV Encoding Fields**

1643 Every Data object encoded by the TTLV scheme consists of four items, in order:

1644 **9.1.1.1 Item Tag**

1645 An Item Tag is a three-byte binary unsigned integer, transmitted big endian, which contains a number that
1646 designates the specific Protocol Field or Object that the TTLV object represents. To ease debugging, and
1647 to ensure that malformed messages are detected more easily, all tags SHALL contain either the value 42
1648 in hex or the value 54 in hex as the high order (first) byte. Tags defined by this specification contain hex
1649 42 in the first byte. Extensions, which are permitted, but are not defined in this specification, contain the
1650 value 54 hex in the first byte. A list of defined Item Tags is in Section 9.1.3.1

1651 **9.1.1.2 Item Type**

1652 An Item Type is a byte containing a coded value that indicates the data type of the data object. The
1653 allowed values are:

Data Type	Coded Value in Hex
Structure	01
Integer	02
Long Integer	03
Big Integer	04
Enumeration	05
Boolean	06
Text String	07
Byte String	08
Date-Time	09
Interval	0A

1654 **Table 192: Allowed Item Type Values**

1655 **9.1.1.3 Item Length**

1656 An Item Length is a 32-bit binary integer, transmitted big-endian, containing the number of bytes in the
1657 Item Value. The allowed values are:

1658

Data Type	Length
Structure	Varies, multiple of 8
Integer	4
Long Integer	8
Big Integer	Varies, multiple of 8
Enumeration	4
Boolean	8
Text String	Varies
Byte String	Varies
Date-Time	8
Interval	4

Table 193: Allowed Item Length Values

1659

1660 If the Item Type is Structure, then the Item Length is the total length of all of the sub-items contained in
1661 the structure, including any padding. If the Item Type is Integer, Enumeration, Text String, Byte String, or
1662 Interval, then the Item Length is the number of bytes excluding the padding bytes. Text Strings and Byte
1663 Strings SHALL be padded with the minimal number of bytes following the Item Value to obtain a multiple
1664 of eight bytes. Integers, Enumerations, and Intervals SHALL be padded with four bytes following the Item
1665 Value.

1666 **9.1.1.4 Item Value**

1667 The item value is a sequence of bytes containing the value of the data item, depending on the type:

- 1668 • Integers are encoded as four-byte long (32 bit) binary signed numbers in 2's complement
1669 notation, transmitted big-endian.
- 1670 • Long Integers are encoded as eight-byte long (64 bit) binary signed numbers in 2's complement
1671 notation, transmitted big-endian.
- 1672 • Big Integers are encoded as a sequence of eight-bit bytes, in two's complement notation,
1673 transmitted big-endian. If the length of the sequence is not a multiple of eight bytes, then Big
1674 Integers SHALL be padded with the minimal number of leading sign-extended bytes to make the
1675 length a multiple of eight bytes. These padding bytes are part of the Item Value and SHALL be
1676 counted in the Item Length.
- 1677 • Enumerations are encoded as four-byte long (32 bit) binary unsigned numbers transmitted big-
1678 endian. Extensions, which are permitted, but are not defined in this specification, contain the
1679 value 8 hex in the first nibble of the first byte.
- 1680 • Booleans are encoded as an eight-byte value that SHALL either contain the hex value
1681 0000000000000000, indicating the Boolean value *False*, or the hex value 0000000000000001,
1682 transmitted big-endian, indicating the Boolean value *True*.

- 1683 • Text Strings are sequences of bytes that encode character values according to the UTF-8
1684 encoding standard. There SHALL NOT be null-termination at the end of such strings.
- 1685 • Byte Strings are sequences of bytes containing individual unspecified eight-bit binary values, and
1686 are interpreted in the same sequence order.
- 1687 • Date-Time values are POSIX Time values encoded as Long Integers. POSIX Time, as described
1688 in IEEE Standard 1003.1 [IEEE1003-1], is the number of seconds since the Epoch (1970 Jan 1,
1689 00:00:00 UTC), not counting leap seconds.
- 1690 • Intervals are encoded as four-byte long (32 bit) binary unsigned numbers, transmitted big-endian.
1691 They have a resolution of one second.
- 1692 • Structure Values are encoded as the concatenated encodings of the elements of the structure. All
1693 structures defined in this specification SHALL have all of their fields encoded in the order in which
1694 they appear in their respective structure descriptions.

1695 9.1.2 Examples

1696 These examples are assumed to be encoding a Protocol Object whose tag is 420020. The examples are
1697 shown as a sequence of bytes in hexadecimal notation:

- 1698 • An Integer containing the decimal value 8:
1699 42 00 20 | 02 | 00 00 00 04 | 00 00 00 08 00 00 00 00
- 1700 • A Long Integer containing the decimal value 123456789000000000:
1701 42 00 20 | 03 | 00 00 00 08 | 01 B6 9B 4B A5 74 92 00
- 1702 • A Big Integer containing the decimal value 12345678900000000000000000000000:
1703 42 00 20 | 04 | 00 00 00 10 | 00 00 00 00 03 FD 35 EB 6B C2 DF 46 18 08
1704 00 00
- 1705 • An Enumeration with value 255:
1706 42 00 20 | 05 | 00 00 00 04 | 00 00 00 FF 00 00 00 00
- 1707 • A Boolean with the value *True*:
1708 42 00 20 | 06 | 00 00 00 08 | 00 00 00 00 00 00 00 01
- 1709 • A Text String with the value "Hello World":
1710 42 00 20 | 07 | 00 00 00 0B | 48 65 6C 6C 6F 20 57 6F 72 6C 64 00 00 00
1711 00 00
- 1712 • A Byte String with the value { 0x01, 0x02, 0x03 }:
1713 42 00 20 | 08 | 00 00 00 03 | 01 02 03 00 00 00 00 00
- 1714 • A Date-Time, containing the value for Friday, March 14, 2008, 11:56:40 GMT:
1715 42 00 20 | 09 | 00 00 00 08 | 00 00 00 00 47 DA 67 F8
- 1716 • An Interval, containing the value for 10 days:
1717 42 00 20 | 0A | 00 00 00 04 | 00 0D 2F 00 00 00 00 00
- 1718 • A Structure containing an Enumeration, value 254, followed by an Integer, value 255, having tags
1719 420004 and 420005 respectively:
1720 42 00 20 | 01 | 00 00 00 20 | 42 00 04 | 05 | 00 00 00 04 | 00 00 00 FE
1721 00 00 00 00 | 42 00 05 | 02 | 00 00 00 04 | 00 00 00 FF 00 00 00 00

1722 **9.1.3 Defined Values**

1723 This section specifies the values that are defined by this specification. In all cases where an extension
1724 mechanism is allowed, this extension mechanism is only able to be used for communication between
1725 parties that have pre-agreed understanding of the specific extensions.

1726 **9.1.3.1 Tags**

1727 The following table defines the tag values for the objects and primitive data values for the protocol
1728 messages.

Tag	
Object	Tag Value
(Unused)	000000 - 420000
Activation Date	420001
Application Data	420002
Application Namespace	420003
Application Specific Information	420004
Archive Date	420005
Asynchronous Correlation Value	420006
Asynchronous Indicator	420007
Attribute	420008
Attribute Index	420009
Attribute Name	42000A
Attribute Value	42000B
Authentication	42000C
Batch Count	42000D
Batch Error Continuation Option	42000E
Batch Item	42000F
Batch Order Option	420010
Block Cipher Mode	420011
Cancellation Result	420012
Certificate	420013
Certificate Identifier	420014
Certificate Issuer	420015
Certificate Request	420016
Certificate Request Type	420017
Certificate Subject	420018
Certificate Subject Alternative Name	420019
Certificate Subject	42001A

Tag	
Object	Tag Value
Distinguished Name	
Certificate Type	42001B
Certificate Value	42001C
Common Template-Attribute	42001D
Compromise Date	42001E
Compromise Occurrence Date	42001F
Contact Information	420020
Credential	420021
Credential Type	420022
Credential Value	420023
Criticality Indicator	420024
CRT Coefficient	420025
Cryptographic Algorithm	420026
Cryptographic Domain Parameters	420027
Cryptographic Length	420028
Cryptographic Parameters	420029
Cryptographic Usage Mask	42002A
Custom Attribute	42002B
D	42002C
Deactivation Date	42002D
Derivation Data	42002E
Derivation Method	42002F
Derivation Parameters	420030
Destroy Date	420031
Digest	420032
Digest Value	420033
Encryption Key Information	420034
G	420035
Hashing Algorithm	420036
Initial Date	420037
Initialization Vector	420038
Issuer	420039
Iteration Count	42003A
IV/Counter/Nonce	42003B
J	42003C

Tag	
Object	Tag Value
Key	42003D
Key Block	42003E
Key Compression Type	42003F
Key Format Type	420040
Key Material	420041
Key Part Identifier	420042
Key Value	420043
Key Wrapping Data	420044
Key Wrapping Specification	420045
Last Change Date	420046
Lease Time	420047
Link	420048
Link Type	420049
Linked Object Identifier	42004A
MAC/Signature	42004B
MAC/Signature Key Information	42004C
Maximum Items	42004D
Maximum Response Size	42004E
Message Extension	42004F
Modulus	420050
Name	420051
Name Type	420052
Name Value	420053
Object Group	420054
Object Type	420055
Offset	420056
Opaque Data Type	420057
Opaque Data Value	420058
Opaque Object	420059
Operation	42005A
Operation Policy Name	42005B
P	42005C
Padding Method	42005D
Prime Exponent P	42005E
Prime Exponent Q	42005F

Tag	
Object	Tag Value
Prime Field Size	420060
Private Exponent	420061
Private Key	420062
Private Key Template-Attribute	420063
Private Key Unique Identifier	420064
Process Start Date	420065
Protect Stop Date	420066
Protocol Version	420067
Protocol Version Major	420068
Protocol Version Minor	420069
Public Exponent	42006A
Public Key	42006B
Public Key Template-Attribute	42006C
Public Key Unique Identifier	42006D
Put Function	42006E
Q	42006F
Q String	420070
Query Function	420071
Recommended Curve	420072
Replaced Unique Identifier	420073
Request Header	420074
Request Message	420075
Request Payload	420076
Response Header	420077
Response Message	420078
Response Payload	420079
Result Message	42007A
Result Reason	42007B
Result Status	42007C
Revocation Message	42007D
Revocation Reason	42007E
Revocation Reason Code	42007F
Role Type	420080
Salt	420081
Secret Data	420082
Secret Data Type	420083

Tag	
Object	Tag Value
Serial Number	420084
Server Information	420085
Split Key	420086
Split Key Method	420087
Split Key Parts	420088
Split Key Threshold	420089
State	42008A
Storage Status Mask	42008B
Symmetric Key	42008C
Template	42008D
Template-Attribute	42008E
Time Stamp	42008F
Unique Batch Item ID	420090
Unique Identifier	420091
Usage Limits	420092
Usage Limits Byte Count	420093
Usage Limits Object Count	420094
Usage Limits Total Bytes	420095
Usage Limits Total Objects	420096
Validity Date	420097
Validity Indicator	420098
Vendor Extension	420099
Vendor Identification	42009A
Wrapping Method	42009B
X	42009C
Y	42009D
(Reserved)	42009E - 42FFFF
(Unused)	430000 - 53FFFF
Extensions	540000 - 54FFFF
(Unused)	550000 - FFFFFFFF

Table 194: Tag Values

1730 **9.1.3.2 Enumerations**

1731 The following tables define the values for enumerated lists.

1732 **9.1.3.2.1 Credential Type Enumeration**

Credential Type	
Name	Value
Username & Password	00000001
Token	00000002
Biometric Measurement	00000003
Certificate	00000004
Extensions	8XXXXXXXX

1733 **Table 195: Credential Type Enumeration**

1734 **9.1.3.2.2 Key Compression Type Enumeration**

Key Compression Type	
Name	Value
EC Public Key Type Uncompressed	00000001
EC Public Key Type X9.62 Compressed Prime	00000002
EC Public Key Type X9.62 Compressed Char2	00000003
EC Public Key Type X9.62 Hybrid	00000004
Extensions	8XXXXXXXX

1735 **Table 196: Key Compression Type Enumeration**

1736 **9.1.3.2.3 Key Format Type Enumeration**

Key Format Type	
Name	Value
Raw	00000001
Opaque	00000002
PKCS#1	00000003
PKCS#8	00000004
X.509	00000005
ECPrivateKey	00000006
Transparent Symmetric Key	00000007
Transparent DSA Private Key	00000008
Transparent DSA Public Key	00000009

Transparent RSA Private Key	0000000A
Transparent RSA Public Key	0000000B
Transparent DH Private Key	0000000C
Transparent DH Public Key	0000000D
Transparent ECDSA Private Key	0000000E
Transparent ECDSA Public Key	0000000F
Transparent ECDH Private Key	00000010
Transparent ECDH Public Key	00000011
Transparent ECMQV Private Key	00000012
Transparent ECMQV Public Key	00000013
Extensions	8XXXXXXXX

1737 **Table 197: Key Format Type Enumeration**

1738 **9.1.3.2.4 Wrapping Method Enumeration**

Wrapping Method	
Name	Value
Encrypt	00000001
MAC/sign	00000002
Encrypt then MAC/sign	00000003
MAC/sign then encrypt	00000004
TR-31	00000005
Extensions	8XXXXXXXX

1739 **Table 198: Wrapping Method Enumeration**

1740 **9.1.3.2.5 Recommended Curve Enumeration for ECDSA, ECDH, and ECMQV**

1741 Recommended curves are defined in NIST FIPS PUB 186-3.

Recommended Curve Enumeration	
Name	Value
P-192	00000001
K-163	00000002
B-163	00000003
P-224	00000004
K-233	00000005
B-233	00000006
P-256	00000007
K-283	00000008
B-283	00000009
P-384	0000000A
K-409	0000000B
B-409	0000000C
P-521	0000000D
K-571	0000000E
B-571	0000000F
Extensions	8XXXXXXXX

1742 **Table 199: Recommended Curve Enumeration for ECDSA, ECDH, and ECMQV**

1743 **9.1.3.2.6 Certificate Type Enumeration**

Certificate Type	
Name	Value
X.509	00000001
PGP	00000002
Extensions	8XXXXXXXX

1744 **Table 200: Certificate Type Enumeration**

1745 **9.1.3.2.7 Split Key Method Enumeration**

Split Key Method	
Name	Value
XOR	00000001
Polynomial Sharing GF(2 ¹⁶)	00000002
Polynomial Sharing Prime Field	00000003
Extensions	8XXXXXXXX

1746 **Table 201: Split Key Method Enumeration**

1747 **9.1.3.2.8 Secret Data Type Enumeration**

Secret Data Type	
Name	Value
Password	00000001
Seed	00000002
Extensions	8XXXXXXXX

1748 **Table 202: Secret Data Type Enumeration**

1749 **9.1.3.2.9 Opaque Data Type Enumeration**

Opaque Data Type	
Name	Value
Extensions	8XXXXXXXX

1750 **Table 203: Opaque Data Type Enumeration**

1751 **9.1.3.2.10 Name Type Enumeration**

Name Type	
Name	Value
Uninterpreted Text String	00000001
URI	00000002
Extensions	8XXXXXXXX

1752 **Table 204: Name Type Enumeration**

1753 **9.1.3.2.11 Object Type Enumeration**

Object Type	
Name	Value
Certificate	00000001
Symmetric Key	00000002
Public Key	00000003
Private Key	00000004
Split Key	00000005
Template	00000006
Secret Data	00000007
Opaque Object	00000008
Extensions	8XXXXXXXX

1754 **Table 205: Object Type Enumeration**

1755 **9.1.3.2.12 Cryptographic Algorithm Enumeration**

Cryptographic Algorithm	
Name	Value
DES	00000001
3DES	00000002
AES	00000003
RSA	00000004
DSA	00000005
ECDSA	00000006
HMAC-SHA1	00000007
HMAC-SHA224	00000008
HMAC-SHA256	00000009
HMAC-SHA384	0000000A
HMAC-SHA512	0000000B
HMAC-MD5	0000000C
DH	0000000D
ECDH	0000000E
ECMQV	0000000F
Extensions	8XXXXXXXX

1756

Table 206: Cryptographic Algorithm Enumeration

1757 **9.1.3.2.13 Block Cipher Mode Enumeration**

Block Cipher Mode	
Name	Value
CBC	00000001
ECB	00000002
PCBC	00000003
CFB	00000004
OFB	00000005
CTR	00000006
CMAC	00000007
CCM	00000008
GCM	00000009
CBC-MAC	0000000A
XTS	0000000B
AESKeyWrapPadding	0000000C
NISTKeyWrap	0000000D
X9.102 AESKW	0000000E
X9.102 TDKW	0000000F
X9.102 AKW1	00000010
X9.102 AKW2	00000011
Extensions	8XXXXXXXX

Table 207: Block Cipher Mode Enumeration

1758

1759 **9.1.3.2.14 Padding Method Enumeration**

Padding Method	
Name	Value
None	00000001
OAEP	00000002
PKCS5	00000003
SSL3	00000004
Zeros	00000005
ANSI X9.23	00000006
ISO 10126	00000007
PKCS1 v1.5	00000008
X9.31	00000009
PSS	0000000A
Extensions	8XXXXXXXX

Table 208: Padding Method Enumeration

1760

1761 9.1.3.2.15 Hashing Algorithm Enumeration

Hashing Algorithm	
Name	Value
MD2	00000001
MD4	00000002
MD5	00000003
SHA-1	00000004
SHA-224	00000005
SHA-256	00000006
SHA-384	00000007
SHA-512	00000008
Extensions	8XXXXXXXX

1762 Table 209: Hashing Algorithm Enumeration

1763 **9.1.3.2.16 Role Type Enumeration**

Role Type	
Name	Value
BDK	00000001
CVK	00000002
DEK	00000003
MKAC	00000004
MKSMC	00000005
MKSMI	00000006
MKDAC	00000007
MKDN	00000008
MKCP	00000009
MKOTH	0000000A
KEK	0000000B
MAC16609	0000000C
MAC97971	0000000D
MAC97972	0000000E
MAC97973	0000000F
MAC97974	00000010
MAC97975	00000011
ZPK	00000012
PVKIBM	00000013
PVKPVV	00000014
PVKOTH	00000015
Extensions	8XXXXXXXX

Table 210: Role Type Enumeration

1764
 1765 Note that while the set and definitions of role types are chosen to match TR-31 there is no necessity to
 1766 match binary representations.

1767 **9.1.3.2.17 State Enumeration**

State	
Name	Value
Pre-Active	00000001
Active	00000002
Deactivated	00000003
Compromised	00000004
Destroyed	00000005
Destroyed Compromised	00000006

Extensions	8XXXXXXXX
------------	-----------

1768

Table 211: State Enumeration

1769 **9.1.3.2.18 Revocation Reason Code Enumeration**

Revocation Reason Code	
Name	Value
Unspecified	00000001
Key Compromise	00000002
CA Compromise	00000003
Affiliation Changed	00000004
Superseded	00000005
Cessation of Operation	00000006
Privilege Withdrawn	00000007
Extensions	8XXXXXXXX

1770

Table 212: Revocation Reason Code Enumeration

1771 **9.1.3.2.19 Link Type Enumeration**

Link Type	
Name	Value
Certificate Link	00000101
Public Key Link	00000102
Private Key Link	00000103
Derivation Base Object Link	00000104
Derived Key Link	00000105
Replacement Object Link	00000106
Replaced Object Link	00000107
Extensions	8XXXXXXXX

1772

Table 213: Link Type Enumeration

1773

Note: Link Types start at 101 to avoid any confusion with Object Types.

1774 **9.1.3.2.20 Derivation Method Enumeration**

Derivation Method	
Name	Value
PBKDF2	00000001
HASH	00000002
HMAC	00000003
ENCRYPT	00000004
NIST800-108-C	00000005
NIST800-108-F	00000006
NIST800-108-DPI	00000007
Extensions	8XXXXXXXX

1775 **Table 214: Derivation Method Enumeration**

1776 **9.1.3.2.21 Certificate Request Type Enumeration**

Certificate Request Type	
Name	Value
CRMF	00000001
PCKS#10	00000002
PEM	00000003
PGP	00000004
Extensions	8XXXXXXXX

1777 **Table 215: Certificate Request Type Enumeration**

1778 **9.1.3.2.22 Validity Indicator Enumeration**

Validity Indicator	
Name	Value
Valid	00000001
Invalid	00000002
Unknown	00000003
Extensions	8XXXXXXXX

1779 **Table 216: Validity Indicator Enumeration**

1780 **9.1.3.2.23 Query Function Enumeration**

Query Function	
Name	Value
Query Operations	00000001
Query Objects	00000002
Query Server Information	00000003

Query Application Namespaces	00000004
Extensions	8XXXXXXXX

1781

Table 217: Query Function Enumeration

1782 **9.1.3.2.24 Cancellation Result Enumeration**

Cancellation Result	
Name	Value
Canceled	00000001
Unable to Cancel	00000002
Completed	00000003
Failed	00000004
Unavailable	00000005
Extensions	8XXXXXXXX

1783

Table 218: Cancellation Result Enumeration

1784 **9.1.3.2.25 Put Function Enumeration**

Put Function	
Name	Value
New	00000001
Replace	00000002
Extensions	8XXXXXXXX

1785

Table 219: Put Function Enumeration

Operation	
Name	Value
Create	00000001
Create Key Pair	00000002
Register	00000003
Re-key	00000004
Derive Key	00000005
Certify	00000006
Re-certify	00000007
Locate	00000008
Check	00000009
Get	0000000A
Get Attributes	0000000B
Get Attribute List	0000000C
Add Attribute	0000000D
Modify Attribute	0000000E
Delete Attribute	0000000F
Obtain Lease	00000010
Get Usage Allocation	00000011
Activate	00000012
Revoke	00000013
Destroy	00000014
Archive	00000015
Recover	00000016
Validate	00000017
Query	00000018
Cancel	00000019
Poll	0000001A
Notify	0000001B
Put	0000001C
Extensions	8XXXXXXX

Table 220: Operation Enumeration

1788 **9.1.3.2.27 Result Status Enumeration**

Result Status	
Name	Value
Success	00000000
Operation Failed	00000001
Operation Pending	00000002
Operation Undone	00000003
Extensions	8XXXXXXXX

1789 **Table 221: Result Status Enumeration**

1790 **9.1.3.2.28 Result Reason Enumeration**

Result Reason	
Name	Value
Item Not Found	00000001
Response Too Large	00000002
Authentication Not Successful	00000003
Invalid Message	00000004
Operation Not Supported	00000005
Missing Data	00000006
Invalid Field	00000007
Feature Not Supported	00000008
Operation Canceled By Requester	00000009
Cryptographic Failure	0000000A
Illegal Operation	0000000B
Permission Denied	0000000C
Object archived	0000000D
Index Out of Bounds	0000000E
General Failure	0000100
Extensions	8XXXXXXXX

1791 **Table 222: Result Reason Enumeration**

1792 **9.1.3.2.29 Batch Error Continuation Enumeration**

Batch Error Continuation	
Name	Value
Continue	00000001
Stop	00000002
Undo	00000003

Extensions	8XXXXXXXX
------------	-----------

1793

Table 223: Batch Error Continuation Enumeration

1794 **9.1.3.3 Bit Masks**

1795 **9.1.3.3.1 Cryptographic Usage Mask**

Cryptographic Usage Mask	
Name	Value
Sign	00000001
Verify	00000002
Encrypt	00000004
Decrypt	00000008
Wrap Key	00000010
Unwrap Key	00000020
Export	00000040
MAC Generate	00000080
MAC Verify	00000100
Derive Key	00000200
Content Commitment (Non Repudiation)	00000400
Key Agreement	00000800
Certificate Sign	00001000
CRL Sign	00002000
Generate Cryptogram	00004000
Validate Cryptogram	00008000
Translate Encrypt	00010000
Translate Decrypt	00020000
Translate Wrap	00040000
Translate Unwrap	00080000
Extensions	XXX00000

1796

Table 224: Cryptographic Usage Mask

1797 This list takes into consideration values which MAY appear in the Key Usage extension in an X.509
 1798 certificate.

1799 **9.1.3.3.2 Storage Status Mask**

Storage Status Mask	
Name	Value
On-line storage	00000001
Archival storage	00000002
Extensions	XXXXXXXX0

1800

Table 225: Storage Status Mask

1801 **9.2 XML Encoding**

1802 An XML Encoding has not yet been defined.

1803 **10 Transport**

1804 A KMIP Server SHALL establish and maintain channel confidentiality and integrity, and prove server
1805 authenticity for KMIP messaging.

1806 If a KMIP Server uses TCP/IP for KMIP messaging, then it SHALL support SSL v3.1/TLS v1.0 or later and
1807 may support other protocols as specified in **[KMIP-Prof]**.

1808 11 Error Handling

1809 This section details the specific Result Reasons that SHALL be returned for errors detected.

1810 11.1 General

1811 These errors MAY occur when any protocol message is received by the server.

Error Definition	Action	Result Reason
Protocol major version mismatch	Response message containing a header and a Batch Item without Operation, but with the Result Status field set to Operation Failed	Invalid Message
Error parsing batch item or payload within batch item	Batch item fails; Result Status is Operation Failed	Invalid Message
The same field is contained in a header/batch item/payload more than once	Result Status is Operation Failed	Invalid Message
Same major version, different minor versions; unknown fields/fields the server does not understand	Ignore unknown fields, process rest normally	N/A
Same major & minor version, unknown field	Result Status is Operation Failed	Invalid Field
Client is not allowed to perform the specified operation	Result Status is Operation Failed	Permission Denied
Operation is not able to be completed synchronously and client does not support asynchronous requests	Result Status is Operation Failed	Operation Not Supported
Maximum Response Size has been exceeded	Result Status is Operation Failed	Response Too Large

1812 **Table 226: General Errors**

1813 11.2 Create

Error Definition	Result Status	Result Reason
Object Type is not recognized	Operation Failed	Invalid Field
Templates that do not exist are given in request	Operation Failed	Item Not Found
Incorrect attribute value(s) specified	Operation Failed	Invalid Field
Error creating cryptographic object	Operation Failed	Cryptographic Failure
Trying to set more instances than the server supports of an attribute that	Operation Failed	Index Out of Bounds

MAY have multiple instances		
Trying to create a new object with the same Name attribute value as an existing object	Operation Failed	Invalid Field
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
Template object is archived	Operation Failed	Object Archived

1814 **Table 227: Create Errors**

1815 **11.3 Create Key Pair**

Error Definition	Result Status	Result Reason
Templates that do not exist are given in request	Operation Failed	Item Not Found
Incorrect attribute value(s) specified	Operation Failed	Invalid Field
Error creating cryptographic object	Operation Failed	Cryptographic Failure
Trying to create a new object with the same Name attribute value as an existing object	Operation Failed	Invalid Field
Trying to set more instances than the server supports of an attribute that MAY have multiple instances	Operation Failed	Index Out of Bounds
REQUIRED field(s) missing	Operation Failed	Invalid Message
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
Template object is archived	Operation Failed	Object Archived

1816 **Table 228: Create Key Pair Errors**

1817 **11.4 Register**

Error Definition	Result Status	Result Reason
Object Type is not recognized	Operation Failed	Invalid Field
Object Type does not match type of cryptographic object provided	Operation Failed	Invalid Field
Templates that do not exist are given in request	Operation Failed	Item Not Found
Incorrect attribute value(s) specified	Operation Failed	Invalid Field
Trying to register a new object with the same Name attribute value as an	Operation Failed	Invalid Field

existing object		
Trying to set more instances than the server supports of an attribute that MAY have multiple instances	Operation Failed	Index Out of Bounds
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
Template object is archived	Operation Failed	Object Archived

1818

Table 229: Register Errors

1819 **11.5 Re-key**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Object specified is not able to be re-keyed	Operation Failed	Permission Denied
Offset field is not permitted to be specified at the same time as any of the Activation Date, Process Start Date, Protect Stop Date, or Deactivation Date attributes	Operation Failed	Invalid Message
Cryptographic error during re-key	Operation Failed	Cryptographic Failure
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
Object is archived	Operation Failed	Object Archived

1820

Table 230: Re-key Errors

1821 **11.6 Derive Key**

Error Definition	Result Status	Result Reason
One or more of the objects specified do not exist	Operation Failed	Item Not Found
One or more of the objects specified are not of the correct type	Operation Failed	Invalid Field
Templates that do not exist are given in request	Operation Failed	Item Not Found
Invalid Derivation Method	Operation Failed	Invalid Field
Invalid Derivation Parameters	Operation Failed	Invalid Field
Ambiguous derivation data provided both with Derivation Data and Secret Data object.	Operation Failed	Invalid Message
Incorrect attribute value(s) specified	Operation Failed	Invalid Field
One or more of the specified objects are not able to be used to derive a new key	Operation Failed	Invalid Field
Trying to derive a new key with the same Name attribute value as an existing object	Operation Failed	Invalid Field
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
One or more of the objects is archived	Operation Failed	Object Archived

1822 **Table 231: Derive Key Errors-**

1823 **11.7 Certify**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Object specified is not able to be certified	Operation Failed	Permission Denied
The Certificate Request does not contain a signed certificate request of the specified Certificate Request Type	Operation Failed	Invalid Field
Server does not support operation	Operation Failed	Operation Not Supported
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported

Object is archived	Operation Failed	Object Archived
--------------------	------------------	-----------------

1824

Table 232: Certify Errors

1825 **11.8 Re-certify**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Object specified is not able to be certified	Operation Failed	Permission Denied
The Certificate Request does not contain a signed certificate request of the specified Certificate Request Type	Operation Failed	Invalid Field
Server does not support operation	Operation Failed	Operation Not Supported
Offset field is not permitted to be specified at the same time as any of the Activation Date or Deactivation Date attributes	Operation Failed	Invalid Message
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
Object is archived	Operation Failed	Object Archived

1826

Table 233: Re-certify Errors

1827 **11.9 Locate**

Error Definition	Result Status	Result Reason
Non-existing attributes, attributes that the server does not understand or templates that do not exist are given in the request	Operation Failed	Invalid Field

1828

Table 234: Locate Errors

1829 **11.10 Check**

Error Definition	Result Status	Result Reason
Object does not exist	Operation Failed	Item Not Found
Object is archived	Operation Failed	Object Archived

1830

Table 235: Check Errors

1831 **11.11 Get**

Error Definition	Result Status	Result Reason
Object does not exist	Operation Failed	Item Not Found
Wrapping key does not exist	Operation Failed	Item Not Found
Object with Wrapping Key ID exists, but it is not a key	Operation Failed	Illegal Operation
Object with Wrapping Key ID exists, but it is not able to be used for wrapping	Operation Failed	Permission Denied
Object with MAC/Signature Key ID exists, but it is not a key	Operation Failed	Illegal Operation
Object with MAC/Signature Key ID exists, but it is not able to be used for MACing/signing	Operation Failed	Permission Denied
Object exists but cannot be provided in the desired Key Format Type and/or Key Compression Type	Operation Failed	Key Format Type and/or Key Compression Type Not Supported
Object exists and is not a Template, but the server only has attributes for this object	Operation Failed	Illegal Operation
Cryptographic Parameters associated with the object do not exist or do not match those provided in the Encryption Key Information and/or Signature Key Information	Operation Failed	Item Not Found
Object is archived	Operation Failed	Object Archived

1832 **Table 236: Get Errors**

1833 **11.12 Get Attributes**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
An Attribute Index is specified, but no matching instance exists.	Operation Failed	Item Not Found
Object is archived	Operation Failed	Object Archived

1834 **Table 237: Get Attributes Errors**

1835 **11.13 Get Attribute List**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found

Object is archived	Operation Failed	Object Archived
--------------------	------------------	-----------------

1836

Table 238: Get Attribute List Errors1837 **11.14 Add Attribute**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Attempt to add a read-only attribute	Operation Failed	Permission Denied
Attempt to add an attribute that is not supported for this object	Operation Failed	Permission Denied
The specified attribute already exists	Operation Failed	Illegal Operation
New attribute contains Attribute Index	Operation Failed	Invalid Field
Trying to add a Name attribute with the same value that another object already has	Operation Failed	Illegal Operation
Trying to add a new instance to an attribute with multiple instances but the server limit on instances has been reached	Operation Failed	Index Out of Bounds
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted from the client request	Operation Failed	Application Namespace Not Supported
Object is archived	Operation Failed	Object Archived

1838

Table 239: Add Attribute Errors1839 **11.15 Modify Attribute**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
A specified attribute does not exist (i.e., it needs to first be added)	Operation Failed	Invalid Field
An Attribute Index is specified, but no matching instance exists.	Operation Failed	Item Not Found
The specified attribute is read-only	Operation Failed	Permission Denied
Trying to set the Name attribute value to a value already used by another object	Operation Failed	Illegal Operation
The particular Application Namespace is not supported, and Application Data cannot be generated if it was omitted	Operation Failed	Application Namespace Not Supported

from the client request		
Object is archived	Operation Failed	Object Archived

Table 240: Modify Attribute Errors

1840

1841 **11.16 Delete Attribute**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Attempt to delete a read-only/REQUIRED attribute	Operation Failed	Permission Denied
Attribute Index is specified, but the attribute does not have multiple instances (i.e., no Attribute Index is permitted to be specified)	Operation Failed	Item Not Found
No attribute with the specified name exists	Operation Failed	Item Not Found
Object is archived	Operation Failed	Object Archived

Table 241: Delete Attribute Errors

1842

1843 **11.17 Obtain Lease**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
The server determines that a new lease is not permitted to be issued for the specified cryptographic object	Operation Failed	Permission Denied
Object is archived	Operation Failed	Object Archived

Table 242: Obtain Lease Errors

1844

1845 **11.18 Get Usage Allocation**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Object has no Usage Limits attribute, or the object is not able to be used for applying cryptographic protection	Operation Failed	Illegal Operation
Both Usage Limits Byte Count and Usage Limits Object Count fields are specified	Operation Failed	Invalid Message
Neither the Byte Count or Object Count is specified	Operation Failed	Invalid Message

A usage type (Byte Count or Object Count) is specified in the request, but the usage allocation for the object MAY only be given for the other type	Operation Failed	Operation Not Supported
Object is archived	Operation Failed	Object Archived

1846

Table 243: Get Usage Allocation Errors

1847 **11.19 Activate**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Unique Identifier specifies a template or other object that is not able to be activated	Operation Failed	Illegal Operation
Object is not in Pre-Active state	Operation Failed	Permission Denied
Object is archived	Operation Failed	Object Archived

1848

Table 244: Activate Errors

1849 **11.20 Revoke**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Revocation Reason is not recognized	Operation Failed	Invalid Field
Unique Identifier specifies a template or other object that is not able to be revoked	Operation Failed	Illegal Operation
Object is archived	Operation Failed	Object Archived

1850

Table 245: Revoke Errors

1851 **11.21 Destroy**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Object exists, but has already been destroyed	Operation Failed	Permission Denied
Object is not in Deactivated state	Operation Failed	Permission Denied
Object is archived	Operation Failed	Object Archived

1852

Table 246: Destroy Errors

1853 **11.22 Archive**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found
Object is already archived	Operation Failed	Object Archived

1854 **Table 247: Archive Errors**

1855 **11.23 Recover**

Error Definition	Result Status	Result Reason
No object with the specified Unique Identifier exists	Operation Failed	Item Not Found

1856 **Table 248: Recover Errors**

1857 **11.24 Validate**

Error Definition	Result Status	Result Reason
The combination of Certificate Objects and Unique Identifiers does not specify a certificate list	Operation Failed	Invalid Message
One or more of the objects is archived	Operation Failed	Object Archived

1858 **Table 249: Validate Errors**

1859 **11.25 Query**

1860 N/A

1861 **11.26 Cancel**

1862 N/A

1863 **11.27 Poll**

Error Definition	Result Status	Result Reason
No outstanding operation with the specified Asynchronous Correlation Value exists	Operation Failed	Item Not Found

1864 **Table 250: Poll Errors**

1865 **11.28 Batch Items**

1866 These errors MAY occur when a protocol message with one or more batch items is processed by the
1867 server. If a message with one or more batch items was parsed correctly, then the response message
1868 SHOULD include response(s) to the batch item(s) in the request according to the table below.

1869

Error Definition	Result Status	Result Reason
Processing of batch item fails with Batch Error Continuation Option set to Stop	Batch item fails. Responses to batch items that have already been processed are returned normally. Responses to batch items that have not been processed are not returned.	See tables above, referring to the operation being performed in the batch item that failed
Processing of batch item fails with Batch Error Continuation Option set to Continue	Batch item fails. Responses to other batch items are returned normally.	See tables above, referring to the operation being performed in the batch item that failed
Processing of batch item fails with Batch Error Continuation Option set to Undo	Batch item fails. Batch items that had been processed have been undone and their responses are returned with Undone result status.	See tables above, referring to the operation being performed in the batch item that failed

1870

Table 251: Batch Items Errors

1871 12 Implementation Conformance

1872 The intention of the baseline conformance profile is for the minimal KMIP Server to support the
1873 mechanics of communication and to support a limited set of commands, such as query. The minimal
1874 KMIP Server would not need to support any particular algorithm – this would be the work of additional
1875 profiles.

1876 An implementation is a conforming KMIP Server if the implementation meets the conditions in Section
1877 12.1 .

1878 An implementation SHALL be a conforming KMIP Server.

1879 If an implementation claims support for a particular clause, then the implementation SHALL conform to all
1880 normative statements within that clause and any subclauses to that clause.

1881 12.1 Conformance clauses for a KMIP Server

1882 An implementation conforms to this specification as a KMIP Server if it meets the following conditions:

- 1883 1. Supports the following objects:
 - 1884 a. Attribute (see 2.1.1)
 - 1885 b. Credential (see 2.1.2)
 - 1886 c. Key Block (see 2.1.3)
 - 1887 d. Key Value (see 2.1.4)
 - 1888 e. Template-Attribute Structure (see 2.1.8)
- 1889 2. Supports the following attributes:
 - 1890 a. Unique Identifier (see 3.1)
 - 1891 b. Name (see 3.2)
 - 1892 c. Object Type (see 3.3)
 - 1893 d. Cryptographic Algorithm (see 3.4)
 - 1894 e. Cryptographic Length (see 3.5)
 - 1895 f. Cryptographic Parameters (see 3.6)
 - 1896 g. Digest (see 3.12)
 - 1897 h. Default Operation Policy (see 3.13.2)
 - 1898 i. Cryptographic Usage Mask (see 3.14)
 - 1899 j. State (see 3.17)
 - 1900 k. Initial Date (see 3.18)
 - 1901 l. Activation Date (see 3.19)
 - 1902 m. Deactivation Date (see 3.22)
 - 1903 n. Destroy Date (see 3.23)
 - 1904 o. Compromise Occurrence Date (see 3.24)
 - 1905 p. Compromise Date (see 3.25)
 - 1906 q. Revocation Reason (see 3.26)
 - 1907 r. Archive Date (see 3.27)
- 1908 3. Supports the following client-to-server operations:
 - 1909 a. Locate (see 4.8)
 - 1910 b. Check (see 4.9)
 - 1911 c. Get (see 4.10)
 - 1912 d. Get Attribute (see 4.11)

- 1913 e. Get Attribute List (see 4.12)
- 1914 f. Add Attribute (see 4.13)
- 1915 g. Modify Attribute (see 4.14)
- 1916 h. Delete Attribute (see 4.15)
- 1917 i. Activate (see 4.18)
- 1918 j. Revoke (see 4.19)
- 1919 k. Destroy (see 4.20)
- 1920 l. Query (see 4.24)
- 1921 4. Supports the following message contents:
 - 1922 a. Protocol Version (see 6.1)
 - 1923 b. Operation (see 6.2)
 - 1924 c. Maximum Response Size (see 6.3)
 - 1925 d. Unique Batch Item ID (see 6.4)
 - 1926 e. Time Stamp (see 6.5)
 - 1927 f. Asynchronous Indicator (see 6.7)
 - 1928 g. Result Status (see 6.9)
 - 1929 h. Result Reason (see 6.10)
 - 1930 i. Result Message (see 6.11)
 - 1931 j. Batch Order Option (see 6.12)
 - 1932 k. Batch Error Continuation Option (see 6.13)
 - 1933 l. Batch Count (see 6.14)
 - 1934 m. Batch Item (see 6.15)
- 1935 5. Supports Message Format (see 7)
- 1936 6. Supports Authentication (see 8)
- 1937 7. Supports the TTLV encoding (see 9.1)
- 1938 8. Supports the transport requirements (see 10)
- 1939 9. Supports Error Handling (see 11) for any supported object, attribute, or operation
- 1940 10. Optionally supports any clause within this specification that is not listed above
- 1941 11. Optionally supports extensions outside the scope of this standard (e.g., vendor extensions,
- 1942 conformance profiles) that do not contradict any requirements within this standard
- 1943 12. Supports at least one of the profiles defined in the KMIP Profiles Specification **[KMIP-Prof]**.

1944
1945
1946

A. Attribute Cross-reference

The following table of Attribute names indicates the Managed Object(s) for which each attribute applies. This table is not normative.

Attribute Name	Managed Object							
	Certificate	Symmetric Key	Public Key	Private Key	Split Key	Template	Secret Data	Opaque Object
Unique Identifier	x	x	x	x	x	x	x	x
Name	x	x	x	x	x	x	x	x
Object Type	x	x	x	x	x	x	x	x
Cryptographic Algorithm	x	x	x	x	x	x		
Cryptographic Domain Parameters			x	x		x		
Cryptographic Length	x	x	x	x	x	x		
Cryptographic Parameters	x	x	x	x	x	x		
Certificate Type	x							
Certificate Identifier	x							
Certificate Issuer	x							
Certificate Subject	x							
Digest	x	x	x	x	x		x	
Operation Policy Name	x	x	x	x	x	x	x	x
Cryptographic Usage Mask	x	x	x	x	x	x	x	
Lease Time	x	x	x	x	x		x	x
Usage Limits		x	x	x	x	x		
State	x	x	x	x	x		x	
Initial Date	x	x	x	x	x	x	x	x
Activation Date	x	x	x	x	x	x	x	
Process Start Date		x			x	x		
Protect Stop Date		x			x	x		
Deactivation Date	x	x	x	x	x	x	x	x
Destroy Date	x	x	x	x	x		x	x
Compromise Occurrence Date	x	x	x	x	x		x	x
Compromise Date	x	x	x	x	x		x	x
Revocation Reason	x	x	x	x	x		x	x
Archive Date	x	x	x	x	x	x	x	x

	Managed Object							
Object Group	x	x	x	x	x	x	x	x
Link	x	x	x	x	x		x	
Application Specific Information	x	x	x	x	x	x	x	x
Contact Information	x	x	x	x	x	x	x	x
Last Change Date	x	x	x	x	x	x	x	x
Custom Attribute	x	x	x	x	x	x	x	x

1947

Table 252: Attribute Cross-reference

B. Tag Cross-reference

1949 This table is not normative.

Object	Defined	Type	Notes
Activation Date	3.19	Date-Time	
Application Data	3.30	Text String	
Application Namespace	3.30	Text String	
Application Specific Information	3.30	Structure	
Archive Date	3.27	Date-Time	
Asynchronous Correlation Value	6.8	Byte String	
Asynchronous Indicator	6.7	Boolean	
Attribute	2.1.1	Structure	
Attribute Index	2.1.1	Integer	
Attribute Name	2.1.1	Text String	
Attribute Value	2.1.1	*	type varies
Authentication	6.6	Structure	
Batch Count	6.14	Integer	
Batch Error Continuation Option	6.13 , 9.1.3.2.29	Enumeration	
Batch Item	6.15	Structure	
Batch Order Option	6.12	Boolean	
Block Cipher Mode	3.6 , 9.1.3.2.13	Enumeration	
Cancellation Result	4.25 , 9.1.3.2.24	Enumeration	
Certificate	2.2.1	Structure	
Certificate Identifier	3.9	Structure	
Certificate Issuer	3.9	Structure	
Certificate Request	4.6 , 4.7	Byte String	
Certificate Request Type	4.6 , 4.7 , 9.1.3.2.21	Enumeration	
Certificate Subject	3.10	Structure	
Certificate Subject Alternative Name	3.10	Text String	
Certificate Subject Distinguished Name	3.10	Text String	
Certificate Type	2.2.1 , 3.8 , 9.1.3.2.6	Enumeration	
Certificate Value	2.2.1	Byte String	
Common Template-Attribute	2.1.8	Structure	
Compromise Occurrence Date	0	Date-Time	
Compromise Date	3.25	Date-Time	
Contact Information	3.31	Text String	
Credential	2.1.2	Structure	
Credential Type	2.1.2 , 9.1.3.2.1	Enumeration	
Credential Value	2.1.2	Byte String	

Object	Defined	Type	Notes
Criticality Indicator	6.16	Boolean	
CRT Coefficient	2.1.7	Big Integer	
Cryptographic Algorithm	3.4 , 9.1.3.2.12	Enumeration	
Cryptographic Length	3.5	Integer	
Cryptographic Parameters	3.6	Structure	
Cryptographic Usage Mask	3.14 , 9.1.3.3.1	Integer	Bit mask
Custom Attribute	3.33	*	type varies
D	2.1.7	Big Integer	
Deactivation Date	3.22	Date-Time	
Derivation Data	4.5	Byte String	
Derivation Method	4.5 , 9.1.3.2.20	Enumeration	
Derivation Parameters	4.5	Structure	
Destroy Date	3.23	Date-Time	
Digest	3.12	Structure	
Digest Value	3.12	Byte String	
Encryption Key Information	2.1.5	Structure	
Extensions	9.1.3		
G	2.1.7	Big Integer	
Hashing Algorithm	3.6 , 3.12 , 9.1.3.2.15	Enumeration	
Initial Date	3.18	Date-Time	
Initialization Vector	4.5	Byte String	
Issuer	3.9	Text String	
Iteration Count	4.5	Integer	
IV/Counter/Nonce	2.1.5	Byte String	
J	2.1.7	Big Integer	
Key	2.1.7	Byte String	
Key Block	2.1.3	Structure	
Key Compression Type	9.1.3.2.2	Enumeration	
Key Format Type	2.1.4 , 9.1.3.2.3	Enumeration	
Key Material	2.1.4 , 2.1.7	Byte String / Structure	
Key Part Identifier	2.2.5	Integer	
Key Value	2.1.4	Byte String / Structure	
Key Wrapping Data	2.1.5	Structure	
Key Wrapping Specification	2.1.6	Structure	
Last Change Date	3.32	Date-Time	
Lease Time	3.15	Interval	
Link	3.29	Structure	

Object	Defined	Type	Notes
Link Type	3.29 , 9.1.3.2.19	Enumeration	
Linked Object Identifier	3.29	Text String	
MAC/Signature	2.1.5	Byte String	
MAC/Signature Key Information	2.1.5	Text String	
Maximum Items	4.8	Integer	
Maximum Response Size	6.3	Integer	
Message Extension	6.16	Structure	
Modulus	2.1.7	Big Integer	
Name	3.2	Structure	
Name Type	3.2 , 9.1.3.2.10	Enumeration	
Name Value	3.2	Text String	
Object Group	3.28	Text String	
Object Type	3.3 , 9.1.3.2.11	Enumeration	
Offset	4.4 , 4.7	Interval	
Opaque Data Type	2.2.8 , 9.1.3.2.9	Enumeration	
Opaque Data Value	2.2.8	Byte String	
Opaque Object	2.2.8	Structure	
Operation	6.2 , 9.1.3.2.26	Enumeration	
Operation Policy Name	3.13	Text String	
P	2.1.7	Big Integer	
Padding Method	3.6 , 9.1.3.2.14	Enumeration	
Prime Exponent P	2.1.7	Big Integer	
Prime Exponent Q	2.1.7	Big Integer	
Prime Field Size	2.2.5	Big Integer	
Private Exponent	2.1.7	Big Integer	
Private Key	2.2.4	Structure	
Private Key Template-Attribute	2.1.8	Structure	
Private Key Unique Identifier	4.2	Text String	
Process Start Date	3.20	Date-Time	
Protect Stop Date	3.21	Date-Time	
Protocol Version	6.1	Structure	
Protocol Version Major	6.1	Integer	
Protocol Version Minor	6.1	Integer	
Public Exponent	2.1.7	Big Integer	
Public Key	2.2.3	Structure	
Public Key Template-Attribute	2.1.8	Structure	
Public Key Unique Identifier	4.2	Text String	
Put Function	5.2 , 9.1.3.2.25	Enumeration	

Object	Defined	Type	Notes
Q	2.1.7	Big Integer	
Q String	2.1.7	Byte String	
Query Function	4.24 , 9.1.3.2.23	Enumeration	
Recommended Curve	2.1.7 , 9.1.3.2.5	Enumeration	
Replaced Unique Identifier	5.2	Text String	
Request Header	7.2 , 7.3	Structure	
Request Message	7.1	Structure	
Request Payload	4 , 5 , 7.2 , 7.3	Structure	
Response Header	7.2 , 7.3	Structure	
Response Message	7.1	Structure	
Response Payload	4 , 7.2 , 7.3	Structure	
Result Message	6.11	Text String	
Result Reason	6.10 , 9.1.3.2.28	Enumeration	
Result Status	6.9 , 9.1.3.2.27	Enumeration	
Revocation Message	3.26	Text String	
Revocation Reason	3.26	Structure	
Revocation Reason Code	3.26 , 9.1.3.2.18	Enumeration	
Role Type	3.6 , 9.1.3.2.16	Enumeration	
Salt	4.5	Byte String	
Secret Data	2.2.7	Structure	
Secret Data Type	2.2.7 , 9.1.3.2.8	Enumeration	
Serial Number	3.9	Text String	
Server Information	4.24	Structure	contents vendor-specific
Split Key	2.2.5	Structure	
Split Key Method	2.2.5 , 9.1.3.2.7	Enumeration	
Split Key Parts	2.2.5	Integer	
Split Key Threshold	2.2.5	Integer	
State	3.17 , 9.1.3.2.17	Enumeration	
Storage Status Mask	4.8 , 9.1.3.3.2	Integer	Bit mask
Symmetric Key	2.2.2	Structure	
Template	2.2.6	Structure	
Template-Attribute	2.1.8	Structure	
Time Stamp	6.5	Date-Time	
Transparent*	2.1.7	Structure	
Unique Identifier	3.1	Text String	
Unique Batch Item ID	6.4	Byte String	
Usage Limits	3.16	Structure	
Usage Limits Byte Count	3.16	Big Integer	

Object	Defined	Type	Notes
Usage Limits Object Count	3.16	Big Integer	
Usage Limits Total Bytes	3.16	Big Integer	
Usage Limits Total Objects	3.16	Big Integer	
Validity Date	4.23	Date-Time	
Validity Indicator	4.23 , 9.1.3.2.22	Enumeration	
Vendor Extension	6.16	Structure	contents vendor-specific
Vendor Identification	4.24 , 6.16	Text String	
Wrapping Method	2.1.5 , 9.1.3.2.4	Enumeration	
X	2.1.7	Big Integer	
Y	2.1.7	Big Integer	

Table 253: Tag Cross-reference

1950

1951
1952
1953

C. Operation and Object Cross-reference

The following table indicates the types of Managed Object(s) that each Operation accepts as input or provide as output. This table is not normative.

Operation	Managed Objects							
	Certificate	Symmetric Key	Public Key	Private Key	Split Key	Template	Secret Data	Opaque Object
Create	N/A	Y	N/A	N/A	N/A	Y	N/A	N/A
Create Key Pair	N/A	N/A	Y	Y	N/A	N/A	N/A	N/A
Register	Y	Y	Y	Y	Y	Y	Y	Y
Re-Key	N/A	Y	N/A	N/A	N/A	Y	N/A	N/A
Derive Key	N/A	Y	N/A	N/A	N/A	Y	Y	N/A
Certify	Y	N/A	Y	N/A	N/A	Y	N/A	N/A
Re-certify	Y	N/A	N/A	N/A	N/A	Y	N/A	N/A
Locate	Y	Y	Y	Y	Y	Y	Y	Y
Check	Y	Y	Y	Y	Y	N/A	Y	Y
Get	Y	Y	Y	Y	Y	Y	Y	Y
Get Attributes	Y	Y	Y	Y	Y	Y	Y	Y
Get Attribute List	Y	Y	Y	Y	Y	Y	Y	Y
Add Attribute	Y	Y	Y	Y	Y	Y	Y	Y
Modify Attribute	Y	Y	Y	Y	Y	Y	Y	Y
Delete Attribute	Y	Y	Y	Y	Y	Y	Y	Y
Obtain Lease	Y	Y	Y	Y	Y	N/A	Y	N/A
Get Usage Allocation	N/A	Y	Y	Y	N/A	N/A	N/A	N/A
Activate	Y	Y	Y	Y	Y	N/A	Y	N/A
Revoke	Y	Y	N/A	Y	Y	N/A	Y	Y
Destroy	Y	Y	Y	Y	Y	Y	Y	Y
Archive	Y	Y	Y	Y	Y	Y	Y	Y
Recover	Y	Y	Y	Y	Y	Y	Y	Y
Validate	Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Query	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Cancel	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Poll	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Notify	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Put	Y	Y	Y	Y	Y	Y	Y	Y

1954

Table 254: Operation and Object Cross-reference

1955 **D. Acronyms**

1956 The following abbreviations and acronyms are used in this document:

- 1957 3DES - Triple Data Encryption Standard specified in ANSI X9.52
- 1958 AES - Advanced Encryption Standard specified in FIPS 197
- 1959 ASN.1 - Abstract Syntax Notation One specified in ITU-T X.680
- 1960 BDK - Base Derivation Key specified in ANSI X9 TR-31
- 1961 CA - Certification Authority
- 1962 CBC - Cipher Block Chaining
- 1963 CCM - Counter with CBC-MAC specified in NIST SP 800-38C
- 1964 CFB - Cipher Feedback specified in NIST SP 800-38A
- 1965 CMAC - Cipher-based MAC specified in NIST SP 800-38B
- 1966 CMC - Certificate Management Messages over CMS specified in RFC 5275
- 1967 CMP - Certificate Management Protocol specified in RFC 4210
- 1968 CPU - Central Processing Unit
- 1969 CRL - Certificate Revocation List specified in RFC 5280
- 1970 CRMF - Certificate Request Message Format specified in RFC 4211
- 1971 CRT - Chinese Remainder Theorem
- 1972 CTR - Counter specified in NIST SP 800-38A
- 1973 CVK - Card Verification Key specified in ANSI X9 TR-31
- 1974 DEK - Data Encryption Key
- 1975 DER - Distinguished Encoding Rules specified in ITU-T X.690
- 1976 DES - Data Encryption Standard specified in FIPS 46-3
- 1977 DH - Diffie-Hellman specified in ANSI X9.42
- 1978 DNS - Domain Name Server
- 1979 DSA - Digital Signature Algorithm specified in FIPS 186-3
- 1980 DSKPP - Dynamic Symmetric Key Provisioning Protocol
- 1981 ECB - Electronic Code Book
- 1982 ECDH - Elliptic Curve Diffie-Hellman specified in ANSI X9.63 and NIST SP 800-56A
- 1983 ECDSA - Elliptic Curve Digital Signature Algorithm specified in ANSX9.62
- 1984 ECMQV - Elliptic Curve Menezes Qu Vanstone specified in ANSI X9.63 and NIST SP 800-56A
- 1985 FIPS - Federal Information Processing Standard
- 1986 GCM - Galois/Counter Mode specified in NIST SP 800-38D
- 1987 GF - Galois field (or finite field)
- 1988 HMAC - Keyed-Hash Message Authentication Code specified in FIPS 198-1 and RFC 2104
- 1989 HTTP - Hyper Text Transfer Protocol
- 1990 HTTP(S) - Hyper Text Transfer Protocol (Secure socket)
- 1991 IEEE - Institute of Electrical and Electronics Engineers

1992	IETF	- Internet Engineering Task Force
1993	IP	- Internet Protocol
1994	IPsec	- Internet Protocol Security
1995	IV	- Initialization Vector
1996	KEK	- Key Encryption Key
1997	KMIP	- Key Management Interoperability Protocol
1998	MAC	- Message Authentication Code
1999	MKAC	- EMV/chip card Master Key: Application Cryptograms specified in ANSI X9 TR-31
2000	MKCP	- EMV/chip card Master Key: Card Personalization specified in ANSI X9 TR-31
2001	MKDAC	- EMV/chip card Master Key: Data Authentication Code specified in ANSI X9 TR-31
2002	MKDN	- EMV/chip card Master Key: Dynamic Numbers specified in ANSI X9 TR-31
2003	MKOTH	- EMV/chip card Master Key: Other specified in ANSI X9 TR-31
2004	MKSMC	- EMV/chip card Master Key: Secure Messaging for Confidentiality specified in X9 TR-31
2005	MKSMI	- EMV/chip card Master Key: Secure Messaging for Integrity specified in ANSI X9 TR-31
2006	MD2	- Message Digest 2 Algorithm specified in RFC 1319
2007	MD4	- Message Digest 4 Algorithm specified in RFC 1320
2008	MD5	- Message Digest 5 Algorithm specified in RFC 1321
2009	NIST	- National Institute of Standards and Technology
2010	OAEP	- Optimal Asymmetric Encryption Padding specified in PKCS#1
2011	OFB	- Output Feedback specified in NIST SP 800-38A
2012	PBKDF2	- Password-Based Key Derivation Function 2 specified in RFC 2898
2013	PCBC	- Propagating Cipher Block Chaining
2014	PEM	- Privacy Enhanced Mail specified in RFC 1421
2015	PGP	- Pretty Good Privacy specified in RFC 1991
2016	PKCS	- Public-Key Cryptography Standards
2017	PKCS#1	- RSA Cryptography Specification Version 2.1 specified in RFC 3447
2018	PKCS#5	- Password-Based Cryptography Specification Version 2 specified in RFC 2898
2019	PKCS#8	- Private-Key Information Syntax Specification Version 1.2 specified in RFC 5208
2020	PKCS#10	- Certification Request Syntax Specification Version 1.7 specified in RFC 2986
2021	POSIX	- Portable Operating System Interface
2022	RFC	- Request for Comments documents of IETF
2023	RSA	- Rivest, Shamir, Adelman (an algorithm)
2024	SCEP	- Simple Certificate Enrollment Protocol
2025	SHA	- Secure Hash Algorithm specified in FIPS 180-2
2026	SP	- Special Publication
2027	SSL/TLS	- Secure Sockets Layer/Transport Layer Security
2028	S/MIME	- Secure/Multipurpose Internet Mail Extensions
2029	<u>TDEA</u>	- see 3DES

- 2030 TCP - Transport Control Protocol
- 2031 TTLV - Tag, Type, Length, Value
- 2032 URI - ~~Uniform~~ Resource Identifier
- 2033 UTC - Universal Time Coordinated
- 2034 UTF - Universal Transformation Format 8-bit specified in RFC 3629
- 2035 XKMS - XML Key Management Specification
- 2036 XML - Extensible Markup Language
- 2037 XTS - XEX Tweakable Block Cipher with Ciphertext Stealing specified in NIST SP 800-38E
- 2038 X.509 - Public Key Certificate specified in RFC 5280
- 2039 ZPK - PIN Block Encryption Key specified in ANSI X9 TR-31

Deleted: Unique

E. List of Figures and Tables

2041	Figure 1: Cryptographic Object States and Transitions	43
2042		
2043	Table 1: Attribute Object Structure	14
2044	Table 2: Credential Object Structure	15
2045	Table 3: Key Block Object Structure	16
2046	Table 4: Key Value Object Structure	17
2047	Table 5: Key Wrapping Data Object Structure	18
2048	Table 6: Encryption Key Information Object Structure	18
2049	Table 7: MAC/Signature Key Information Object Structure	18
2050	Table 8: Key Wrapping Specification Object Structure	19
2051	Table 9: Key Material Object Structure for Transparent Symmetric Keys	19
2052	Table 10: Key Material Object Structure for Transparent DSA Private Keys	19
2053	Table 11: Key Material Object Structure for Transparent DSA Public Keys	20
2054	Table 12: Key Material Object Structure for Transparent RSA Private Keys	20
2055	Table 13: Key Material Object Structure for Transparent RSA Public Keys	21
2056	Table 14: Key Material Object Structure for Transparent DH Private Keys	21
2057	Table 15: Key Material Object Structure for Transparent DH Public Keys	21
2058	Table 16: Key Material Object Structure for Transparent ECDSA Private Keys	22
2059	Table 17: Key Material Object Structure for Transparent ECDSA Public Keys	22
2060	Table 18: Key Material Object Structure for Transparent ECDH Private Keys	22
2061	Table 19: Key Material Object Structure for Transparent ECDH Public Keys	22
2062	Table 20: Key Material Object Structure for Transparent ECMQV Private Keys	23
2063	Table 21: Key Material Object Structure for Transparent ECMQV Public Keys	23
2064	Table 22: Template-Attribute Object Structure	23
2065	Table 23: Certificate Object Structure	24
2066	Table 24: Symmetric Key Object Structure	24
2067	Table 25: Public Key Object Structure	24
2068	Table 26: Private Key Object Structure	24
2069	Table 27: Split Key Object Structure	25
2070	Table 28: Template Object Structure	26
2071	Table 29: Secret Data Object Structure	27
2072	Table 30: Opaque Object Structure	27
2073	Table 31: Attribute Rules	28
2074	Table 32: Unique Identifier Attribute	29
2075	Table 33: Unique Identifier Attribute Rules	29
2076	Table 34: Name Attribute Structure	29
2077	Table 35: Name Attribute Rules	29
2078	Table 36: Object Type Attribute	30
2079	Table 37: Object Type Attribute Rules	30

2080	Table 38: Cryptographic Algorithm Attribute	30
2081	Table 39: Cryptographic Algorithm Attribute Rules	30
2082	Table 40: Cryptographic Length Attribute	31
2083	Table 41: Cryptographic Length Attribute Rules	31
2084	Table 42: Cryptographic Parameters Attribute Structure	31
2085	Table 43: Cryptographic Parameters Attribute Rules	31
2086	Table 44: Role Types	32
2087	Table 45: Cryptographic Domain Parameters Attribute Structure	33
2088	Table 46: Cryptographic Domain Parameters Attribute Rules	33
2089	Table 47: Certificate Type Attribute	33
2090	Table 48: Certificate Type Attribute Rules	33
2091	Table 49: Certificate Identifier Attribute Structure	34
2092	Table 50: Certificate Identifier Attribute Rules	34
2093	Table 51: Certificate Subject Attribute Structure	34
2094	Table 52: Certificate Subject Attribute Rules	35
2095	Table 53: Certificate Issuer Attribute Structure	35
2096	Table 54: Certificate Issuer Attribute Rules	35
2097	Table 55: Digest Attribute Structure	36
2098	Table 56: Digest Attribute Rules	36
2099	Table 57: Operation Policy Name Attribute	36
2100	Table 58: Operation Policy Name Attribute Rules	37
2101	Table 59: Default Operation Policy for Secret Objects	38
2102	Table 60: Default Operation Policy for Certificates and Public Key Objects	38
2103	Table 61: Default Operation Policy for Private Template Objects	39
2104	Table 62: Default Operation Policy for Public Template Objects	39
2105	Table 63: X.509 Key Usage to Cryptographic Usage Mask Mapping	40
2106	Table 64: Cryptographic Usage Mask Attribute	40
2107	Table 65: Cryptographic Usage Mask Attribute Rules	41
2108	Table 66: Lease Time Attribute	41
2109	Table 67: Lease Time Attribute Rules	41
2110	Table 68: Usage Limits Attribute Structure	42
2111	Table 69: Usage Limits Attribute Rules	43
2112	Table 70: State Attribute	45
2113	Table 71: State Attribute Rules	45
2114	Table 72: Initial Date Attribute	45
2115	Table 73: Initial Date Attribute Rules	45
2116	Table 74: Activation Date Attribute	46
2117	Table 75: Activation Date Attribute Rules	46
2118	Table 76: Process Start Date Attribute	46
2119	Table 77: Process Start Date Attribute Rules	46
2120	Table 78: Protect Stop Date Attribute	47
2121	Table 79: Protect Stop Date Attribute Rules	47

2122	Table 80: Deactivation Date Attribute	47
2123	Table 81: Deactivation Date Attribute Rules	47
2124	Table 82: Destroy Date Attribute	48
2125	Table 83: Destroy Date Attribute Rules	48
2126	Table 84: Compromise Occurrence Date Attribute	48
2127	Table 85: Compromise Occurrence Date Attribute Rules	48
2128	Table 86: Compromise Date Attribute	49
2129	Table 87: Compromise Date Attribute Rules	49
2130	Table 88: Revocation Reason Attribute Structure	49
2131	Table 89: Revocation Reason Attribute Rules	49
2132	Table 90: Archive Date Attribute	50
2133	Table 91: Archive Date Attribute Rules	50
2134	Table 92: Object Group Attribute	50
2135	Table 93: Object Group Attribute Rules	50
2136	Table 94: Link Attribute Structure	51
2137	Table 95: Link Attribute Structure Rules	52
2138	Table 96: Application Specific Information Attribute	52
2139	Table 97: Application Specific Information Attribute Rules	52
2140	Table 98: Contact Information Attribute	52
2141	Table 99: Contact Information Attribute Rules	53
2142	Table 100: Last Change Date Attribute	53
2143	Table 101: Last Change Date Attribute Rules	53
2144	Table 102 Custom Attribute	54
2145	Table 103: Custom Attribute Rules	54
2146	Table 104: Create Request Payload	55
2147	Table 105: Create Response Payload	55
2148	Table 106: Create Attribute Requirements	56
2149	Table 107: Create Key Pair Request Payload	56
2150	Table 108: Create Key Pair Response Payload	57
2151	Table 109: Create Key Pair Attribute Requirements	57
2152	Table 110: Register Request Payload	58
2153	Table 111: Register Response Payload	58
2154	Table 112: Register Attribute Requirements	58
2155	Table 113: Computing New Dates from Offset during Re-key	59
2156	Table 114: Re-key Attribute Requirements	60
2157	Table 115: Re-key Request Payload	60
2158	Table 116: Re-key Response Payload	61
2159	Table 117: Derive Key Request Payload	62
2160	Table 118: Derive Key Response Payload	62
2161	Table 119: Derivation Parameters Structure (Except PBKDF2)	62
2162	Table 120: PBKDF2 Derivation Parameters Structure	63
2163	Table 121: Certify Request Payload	64

2164	Table 122: Certify Response Payload	64
2165	Table 123: Computing New Dates from Offset during Re-certify	65
2166	Table 124: Re-certify Attribute Requirements	65
2167	Table 125: Re-certify Request Payload	66
2168	Table 126: Re-certify Response Payload	66
2169	Table 127: Locate Request Payload	67
2170	Table 128: Locate Response Payload	67
2171	Table 129: Check Request Payload	69
2172	Table 130: Check Response Payload	69
2173	Table 131: Get Request Payload	70
2174	Table 132: Get Response Payload	70
2175	Table 133: Get Attributes Request Payload	71
2176	Table 134: Get Attributes Response Payload	71
2177	Table 135: Get Attribute List Request Payload	71
2178	Table 136: Get Attribute List Response Payload	71
2179	Table 137: Add Attribute Request Payload	72
2180	Table 138: Add Attribute Response Payload	72
2181	Table 139: Modify Attribute Request Payload	72
2182	Table 140: Modify Attribute Response Payload	72
2183	Table 141: Delete Attribute Request Payload	73
2184	Table 142: Delete Attribute Response Payload	73
2185	Table 143: Obtain Lease Request Payload	73
2186	Table 144: Obtain Lease Response Payload	74
2187	Table 145: Get Usage Allocation Request Payload	74
2188	Table 146: Get Usage Allocation Response Payload	75
2189	Table 147: Activate Request Payload	75
2190	Table 148: Activate Response Payload	75
2191	Table 149: Revoke Request Payload	75
2192	Table 150: Revoke Response Payload	75
2193	Table 151: Destroy Request Payload	76
2194	Table 152: Destroy Response Payload	76
2195	Table 153: Archive Request Payload	76
2196	Table 154: Archive Response Payload	76
2197	Table 155: Recover Request Payload	77
2198	Table 156: Recover Response Payload	77
2199	Table 157: Validate Request Payload	77
2200	Table 158: Validate Response Payload	77
2201	Table 159: Query Request Payload	78
2202	Table 160: Query Response Payload	79
2203	Table 161: Cancel Request Payload	79
2204	Table 162: Cancel Response Payload	79
2205	Table 163: Poll Request Payload	80

2206	Table 164: Notify Message Payload	81
2207	Table 165: Put Message Payload.....	82
2208	Table 166: Protocol Version Structure in Message Header	83
2209	Table 167: Operation in Batch Item	83
2210	Table 168: Maximum Response Size in Message Request Header	83
2211	Table 169: Unique Batch Item ID in Batch Item.....	83
2212	Table 170: Time Stamp in Message Header	84
2213	Table 171: Authentication Structure in Message Header.....	84
2214	Table 172: Asynchronous Indicator in Message Request Header	84
2215	Table 173: Asynchronous Correlation Value in Response Batch Item.....	84
2216	Table 174: Result Status in Response Batch Item.....	85
2217	Table 175: Result Reason in Response Batch Item	86
2218	Table 176: Result Message in Response Batch Item	86
2219	Table 177: Batch Order Option in Message Request Header.....	86
2220	Table 178: Batch Error Continuation Option in Message Request Header.....	86
2221	Table 179: Batch Count in Message Header	87
2222	Table 180: Batch Item in Message	87
2223	Table 181: Message Extension Structure in Batch Item	87
2224	Table 182: Request Message Structure	88
2225	Table 183: Response Message Structure.....	88
2226	Table 184: Synchronous Request Header Structure	88
2227	Table 185: Synchronous Request Batch Item Structure	89
2228	Table 186: Synchronous Response Header Structure.....	89
2229	Table 187: Synchronous Response Batch Item Structure	89
2230	Table 188: Asynchronous Request Header Structure.....	90
2231	Table 189: Asynchronous Request Batch Item Structure	90
2232	Table 190: Asynchronous Response Header Structure	90
2233	Table 191: Asynchronous Response Batch Item Structure	91
2234	Table 192: Allowed Item Type Values	93
2235	Table 193: Allowed Item Length Values	94
2236	Table 194: Tag Values	100
2237	Table 195: Credential Type Enumeration	101
2238	Table 196: Key Compression Type Enumeration	101
2239	Table 197: Key Format Type Enumeration	102
2240	Table 198: Wrapping Method Enumeration	102
2241	Table 199: Recommended Curve Enumeration for ECDSA, ECDH, and ECMQV	103
2242	Table 200: Certificate Type Enumeration	103
2243	Table 201: Split Key Method Enumeration	103
2244	Table 202: Secret Data Type Enumeration.....	104
2245	Table 203: Opaque Data Type Enumeration	104
2246	Table 204: Name Type Enumeration.....	104
2247	Table 205: Object Type Enumeration	104

2248	Table 206: Cryptographic Algorithm Enumeration	105
2249	Table 207: Block Cipher Mode Enumeration	106
2250	Table 208: Padding Method Enumeration	106
2251	Table 209: Hashing Algorithm Enumeration	107
2252	Table 210: Role Type Enumeration	108
2253	Table 211: State Enumeration	109
2254	Table 212: Revocation Reason Code Enumeration	109
2255	Table 213: Link Type Enumeration	109
2256	Table 214: Derivation Method Enumeration	110
2257	Table 215: Certificate Request Type Enumeration	110
2258	Table 216: Validity Indicator Enumeration	110
2259	Table 217: Query Function Enumeration	111
2260	Table 218: Cancellation Result Enumeration	111
2261	Table 219: Put Function Enumeration	111
2262	Table 220: Operation Enumeration	112
2263	Table 221: Result Status Enumeration	113
2264	Table 222: Result Reason Enumeration	113
2265	Table 223: Batch Error Continuation Enumeration	114
2266	Table 224: Cryptographic Usage Mask	114
2267	Table 225: Storage Status Mask	115
2268	Table 226: General Errors	117
2269	Table 227: Create Errors	118
2270	Table 228: Create Key Pair Errors	118
2271	Table 229: Register Errors	119
2272	Table 230: Re-key Errors	119
2273	Table 231: Derive Key Errors-	120
2274	Table 232: Certify Errors	121
2275	Table 233: Re-certify Errors	121
2276	Table 234: Locate Errors	121
2277	Table 235: Check Errors	121
2278	Table 236: Get Errors	122
2279	Table 237: Get Attributes Errors	122
2280	Table 238: Get Attribute List Errors	123
2281	Table 239: Add Attribute Errors	123
2282	Table 240: Modify Attribute Errors	124
2283	Table 241: Delete Attribute Errors	124
2284	Table 242: Obtain Lease Errors	124
2285	Table 243: Get Usage Allocation Errors	125
2286	Table 244: Activate Errors	125
2287	Table 245: Revoke Errors	125
2288	Table 246: Destroy Errors	125
2289	Table 247: Archive Errors	126

2290	Table 248: Recover Errors	126
2291	Table 249: Validate Errors	126
2292	Table 250: Poll Errors.....	126
2293	Table 251: Batch Items Errors.....	127
2294	Table 252: Attribute Cross-reference.....	131
2295	Table 253: Tag Cross-reference.....	136
2296	Table 254: Operation and Object Cross-reference	137
2297		

2298 F. Acknowledgements

2299 The following individuals have participated in the creation of this specification and are gratefully
2300 acknowledged:

2301 **Original Authors of the initial contribution:**

2302 David Babcock, HP
2303 Steven Bade, IBM
2304 Paolo Bezoari, NetApp
2305 Mathias Björkqvist, IBM
2306 Bruce Brinson, EMC
2307 Christian Cachin, IBM
2308 Tony Crossman, Thales/nCipher
2309 Stan Feather, HP
2310 Indra Fitzgerald, HP
2311 Judy Furlong, EMC
2312 Jon Geater, Thales/nCipher
2313 Bob Griffin, EMC
2314 Robert Haas, IBM (editor)
2315 Timothy Hahn, IBM
2316 Jack Harwood, EMC
2317 Walt Hubis, LSI
2318 Glen Jaquette, IBM
2319 Jeff Kravitz, IBM (editor emeritus)
2320 Michael McIntosh, IBM
2321 Brian Metzger, HP
2322 Anthony Nadalin, IBM
2323 Elaine Palmer, IBM
2324 Joe Pato, HP
2325 René Pawlitzek, IBM
2326 Subhash Sankuratripati, NetApp
2327 Mark Schiller, HP
2328 Martin Skagen, Brocade
2329 Marcus Streets, Thales/nCipher
2330 John Tattan, EMC
2331 Karla Thomas, Brocade
2332 Marko Vukolić, IBM
2333 Steve Wierenga, HP

2334 **Participants:**

2335 [Gordon Arnold, IBM](#)
2336 [Todd Arnold, IBM](#)
2337 [Matthew Ball, Sun Microsystems](#)
2338 [Elaine Barker, NIST](#)
2339 [Peter Bartok, Venafi, Inc.](#)
2340 [Mathias Bjorkqvist, IBM](#)
2341 [Kevin Bocek, Thales e-Security](#)
2342 [Kelley Burgin, National Security Agency](#)
2343 [Jon Callas, PGP Corporation](#)
2344 [Tom Clifford, Symantec Corp.](#)
2345 [Graydon Dodson, Lexmark International Inc.](#)
2346 [Chris Dunn, SafeNet, Inc.](#)
2347 [Paul Earsy, SafeNet, Inc.](#)
2348 [Stan Feather, HP](#)
2349 [Indra Fitzgerald, HP](#)
2350 [Alan Frindell, SafeNet, Inc.](#)

2351 [Judith Furlong, EMC Corporation](#)
2352 [Jonathan Geater, Thales e-Security](#)
2353 [Robert Griffin, EMC Corporation](#)
2354 [Robert Haas, IBM](#)
2355 [Thomas Hardjono, M.I.T.](#)
2356 [Marc Hocking, BeCrypt Ltd.](#)
2357 [Larry Hofer, Emulex Corporation](#)
2358 [Brandon Hoff, Emulex Corporation](#)
2359 [Walt Hubis, LSI Corporation](#)
2360 [Wyllys Ingersoll, Sun Microsystems](#)
2361 [Jay Jacobs, Target Corporation](#)
2362 [Glen Jaquette, IBM](#)
2363 [Scott Kipp, Brocade Communications Systems, Inc.](#)
2364 [David Lawson, Emulex Corporation](#)
2365 [Robert Lockhart, Thales e-Security](#)
2366 [Shyam Mankala, EMC Corporation](#)
2367 [Marc Massar, Individual](#)
2368 [Don McAlister, Cipheroptics](#)
2369 [Hyrum Mills, Mitre Corporation](#)
2370 [Landon Noll, Cisco Systems, Inc.](#)
2371 [René Pawlitzek, IBM](#)
2372 [Rob Philpott, EMC Corporation](#)
2373 [Bruce Rich, IBM](#)
2374 [Scott Rotondo, Sun Microsystems](#)
2375 [Anil Saldhana, Red Hat](#)
2376 [Subhash Sankuratripati, NetApp](#)
2377 [Mark Schiller, HP](#)
2378 [Jitendra Singh, Brocade Communications Systems, Inc.](#)
2379 [Servesch Singh, EMC Corporation](#)
2380 [Sandy Stewart, Sun Microsystems](#)
2381 [Marcus Streets, Thales e-Security](#)
2382 [Brett Thompson, SafeNet, Inc.](#)
2383 [Benjamin Tomhave, Individual](#)
2384 [Sean Turner, IECA, Inc.](#)
2385 [Paul Turner, Venafi, Inc.](#)
2386 [Marko Vukolic, IBM](#)
2387 [Rod Wideman, Quantum Corporation](#)
2388 [Steven Wierenga, HP](#)
2389 [Peter Yee, EMC Corporation](#)
2390 [Krishna Yellepeddy, IBM](#)
2391 [Peter Zelechowski, Election Systems & Software](#)

Deleted: TBD

G. Revision History

Revision	Date	Editor	Changes Made
ed-0.98	2009-04-24	Robert Haas	Initial conversion of input document to OASIS format together with clarifications.
ed-0.98	2009-05-21	Robert Haas	Changes to TTLV format for 64-bit alignment. Appendices indicated as non normative.
ed-0.98	2009-06-25	Robert Haas, Indra Fitzgerald	Multiple editorial and technical changes, including merge of Template and Policy Template.
ed-0.98	2009-07-23	Robert Haas, Indra Fitzgerald	Multiple editorial and technical changes, mainly based on comments from Elaine Barker and Judy Furlong. Fix of Template Name.
ed-0.98	2009-07-27	Indra Fitzgerald	Added captions to tables and figures.
ed-0.98	2009-08-27	Robert Haas	Wording compliance changes according to RFC2119 from Rod Wideman. Removal of attribute mutation in server responses.
ed-0.98	2009-09-03	Robert Haas	Incorporated the RFC2119 language conformance statement from Matt Ball; the changes to the Application-Specific Information attribute from René Pawlitzek; the extensions to the Query operation for namespaces from Mathias Björkqvist; the key roles proposal from Jon Geater, Todd Arnold, & Chris Dunn. Capitalized all RFC2119 keywords (required by OASIS) together with editorial changes.
ed-0.98	2009-09-17	Robert Haas	Replaced Section 10 on HTTPS and SSL with the content from the User Guide. Additional RFC2119 language conformance changes. Corrections in the enumerations in Section 9.
ed-0.98	2009-09-25	Indra Fitzgerald, Robert Haas	New Cryptographic Domain Parameters attribute and change to the Create Key Pair operation (from Indra Fitzgerald). Changes to Key Block object and Get operation to request desired Key Format and Compression Types (from Indra Fitzgerald). Changes in Revocation Reason code and new Certificate Issuer attribute (from Judy Furlong). No implicit object state change after Re-key or Re-certify. New Section 13 on Implementation Conformance from Matt Ball. Multiple editorial changes and new enumerations.
ed-0.98	2009-09-29	Robert Haas	(Version edited during the f2f) Moved content of Sections 8 (Authentication) and 10 (Transport), into the KMIP Profiles Specification. Clarifications (from Sean Turner) on key encoding (for Byte String) in 9.1.1.4. Updates for certificate update and renewal (From Judy

			Furlong) First set of editorial changes as suggested by Elaine Barker (changed Octet to Byte, etc). (version approved as TC Committee Draft on Sep 29 2009, counts as draft-01 version)
draft-02	2009-10-09	Robert Haas, Indra Fitzgerald	Second set of editorial changes as suggested by Elaine Barker (incl. renaming of "Last Change Date" attribute). Added list of references from Sean Turner and Judy Furlong, as well as terminology. Made Result Reasons in error cases (Sec 11) normative. Added statement on deletion of attributes by server (line 457). Added major/minor 1.0 for protocol version (line 27). Systematic use of <i>italics</i> when introducing a term for first time. Added "Editor's note" comments remaining to be addressed before public review.
draft-03	2009-10-14	Robert Haas, Indra Fitzgerald	Addressed outstanding "Editor's note" comments. Added acronyms and references.
draft-04	2009-10-21	Robert Haas, Indra Fitzgerald	Added the list of participants (Appendix F). Point to the KMIP Profiles document for a list standard application namespaces. Added Terminology (from Bob Lockhart, borrowed from SP800-57 Part 1). Modified title page.

2393