ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0110—2021

密钥管理互操作协议规范

Key management interoperability protocol specification

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：三未信安科技股份有限公司、北京数字认证股份有限公司、北京信安世纪科技股份有限公司、上海众人网络安全技术有限公司、中金金融认证中心有限公司、兴唐通信科技有限公司、成都卫士通信息产业股份有限公司、北京赛博兴安科技有限公司、北京融通高科科技发展有限公司、北京数码视讯科技股份有限公司、北京江南天安科技有限公司、北京宏思电子技术有限责任公司、北京智芯微电子科技有限公司、数安时代科技股份有限公司、格尔软件股份有限公司、山东大学、中国移动通信集团设计院有限公司、暨南大学。

本文件主要起草人：高志权、董坤朋、鹿淑煜、刘晓东、李向锋、汪宗斌、李坤、刘海涛、姜晓新、成明、韩浩、王亚伟、张向辉、马晓艳、王妮娜、罗俊、张旭、张妍、张钊、张永强、谭武征、张高山。

引　言

在密码系统中，密钥的生成、使用和管理至关重要，密钥的安全是密码系统安全的基础。密钥管理是指根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。在密码应用方案中，应用服务器、数据库系统、云计算平台、大数据平台等多种环境中需要对数据进行加密保护，都需要使用密钥管理系统对数据加密密钥等密钥的全生命周期进行安全管理，亟需定义统一的密钥管理接口规范。

本文件目标是为密码应用系统和密钥管理系统之间通信制定统一的密钥管理协议。通过该密钥管理协议，解决需要使用密钥的应用系统与生成和管理这些密钥的密钥管理系统之间的通信标准化问题。

本文件制定的密钥管理协议为密钥管理系统的开发、使用及检测提供依据和指导，有利于提高密钥管理系统的产品化和规范化。

密钥管理互操作协议规范

1 范围

本文件规定了密钥客户端和密钥管理服务端之间通信的密钥管理协议，通过该协议完成密钥管理服务端中对象的生成、存储和状态转换等操作，并规定了协议应用的安全要求。

不涉及密钥管理服务端的内部逻辑结构和安全性设计，也不涉及密钥客户端的业务逻辑。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 35276 信息安全技术 SM2密码算法使用规范

GM/T 0024 SSL VPN技术规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

归档 archive

将不会被频繁访问的信息放进长期存储区。

3.2

授权 authorization

授予实体的访问权限；表达了对执行某项安全功能或活动的“正式”许可。

3.3

失信 compromise

未经授权泄露、篡改、替换或使用敏感数据(例如密钥材料和与安全相关的其他信息)。

3.4

消息摘要 message digest

消息经过密码杂凑运算得到的结果。

3.5

密钥封装(封装) key wrapping(wrapping)

一种对密钥进行加密、MAC/签名或加密与MAC/签名都执行的一种方法。

3.6

配置文件　profile

对对象、属性、操作、消息元素和认证方法的一种规范说明，这些对象、属性、操作、消息元素和认证方法将用于特定背景下的密钥管理服务与客户端之间的互动。

3.7

恢复　recover

复原已被存档长期保存的信息。

3.8

拆分密钥　split key

使用秘密共享技术把一个密钥拆分成 n 个密钥分量的过程，其中每个密钥分量都不能单独推算出原密钥，而组合到一起可以重建出原密钥。如果需要 k 个密钥分量（$k \leqslant n$）才能重建原密钥，那么若只知道 $k-1$ 个密钥分量，无法获取原密钥的密钥信息。

3.9

添加变量　salt

作为单向或加密函数的二次输入而加入的随机变量，可用于导出口令验证数据。

3.10

密钥派生　key derivation

使用伪随机函数从主密钥、口令或密码短语的秘密值导出一个或多个秘密密钥。可用于将密钥扩展为更长的密钥或获得所需格式的密钥。

3.11

XTS 加密模式　XEX-based tweaked-codebook mode with ciphertext stealing

基于 XEX（XOR-ENCRYPT-XOR）的密文挪用算法的可调整的密码本模式，该加密模式主要用于以数据单元（包括扇区、逻辑磁盘块等）为基础结构的存储设备中静止状态数据的加密。

3.12

被管理对象　managed object

密钥管理服务端管理的对象，包括对称密钥、非对称密钥、证书、秘密数据、不透明对象等。

4　缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法标记（Abstract Syntax Notation One）

CA：证书认证机构（Certification Authority）

CRL：证书撤销列表（Certificate Revocation List）

CRT：中国剩余定理（Chinese Remainder Theorem）

CTR：计数器（Counter）

DER：可区分编码规则（Distinguished Encoding Rules）

DNS：域名系统（Domain Name System）

GCM：Galois 计数器模式（Galois Counter Mode）

HMAC：带密钥的杂凑算法（Keyed-Hash Message Authentication Code）

IP：互联网协议（Internet Protocol）

ISO：国际标准化组织（International Organization for Standardization）

IV：初始化向量（Initialization Vector）

KMIP：密钥管理互操作协议（Key Management Interoperability Protocol）

MAC:消息鉴别码(Message Authentication Code)
PKCS:公钥加密标准(Public Key Cryptography Standards)
PKI:公钥基础设施(Public Key Infrastructure)
PSS:概率签名格式(Probabilistic Signature Scheme)
RNG:随机数发生器(Random Number Generator)
RSA:一种非对称密码算法(RSA algorithm)
TTLV:标签,类型,长度,值(tag,type,length,value)
URI:统一资源标识符(Uniform Resource Identifier)
URL:统一资源定位符(Uniform Resource Locator)
XTS:一种分组密码加密模式(XEX-based tweaked-codebook mode with ciphertext stealing)

5 概述

本文件旨在定义一套密钥客户端和密钥管理服务端之间的通信协议规范,通过该协议可以完成密钥管理服务端中对象的创建、存储、使用和销毁等操作。这些对象在本文件中统称被管理对象。本文件中被管理对象包括对称密钥、非对称密钥、数字证书等。被管理对象具有一系列属性,属性信息存储在密钥管理服务中,通过密钥管理服务可以对这些属性进行添加、修改或删除操作。密钥管理服务端可以支持的对象管理操作包括生成加密密钥、导入密码对象、查询对象、获取对象以及销毁对象等。标准应用示例和主要应用场景详见附录 A。

6 密钥管理互操作协议

6.1 协议模型

密钥管理互操作协议的交互模型如图 1 所示。

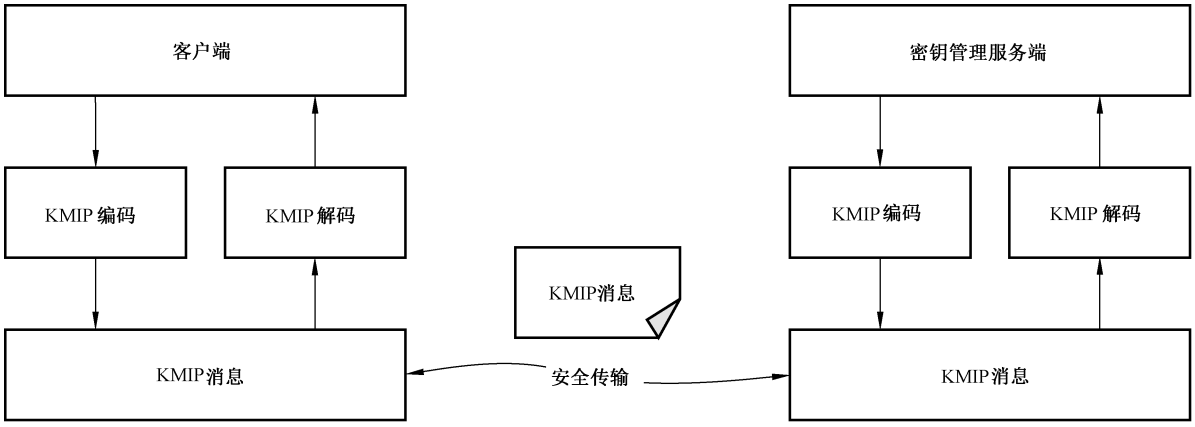


图 1 密钥管理互操作协议交互模型

如图 1 所示,客户端向密钥管理服务端发送请求消息,请求消息中应包含用于进行客户端身份认证、操作标识、操作参数等信息。密钥管理服务端按照请求消息进行相应操作并将操作结果作为响应消息返回给客户端。响应消息中包含结果状态和结果数据。本文件描述的协议具备以下特性:

a) 消息与消息之间是无关的,实现者无须维持消息相关状态。具体消息的数据格式和编解码见 6.5。

b) 消息中可以包含单个操作请求或响应，也可包含多个操作请求或响应。
c) 消息可以为同步消息或异步消息。消息的形式与具体操作和实现有关。
d) 根据操作的不同或操作目标对象的不同，可以分为：
1) 无须认证直接操作，例如对公共对象的查询等操作；
2) 需要进行认证方可操作，例如对私有对象的创建、获取等。

6.2 对象

6.2.1 对象类型

以下小节描述客户端和密钥管理服务端之间传递的对象。

被管理对象是密钥管理操作(见 6.4)的对象。被管理对象包括密码对象(包含密钥材料的对象，例如证书、密钥和秘密数据)和非密码对象(例如不透明对象)。

有些对象类型只用于协议本身，不作为被管理对象，称为基础对象。

对象描述中引用到的原始数据类型包括：

——整数(Integer)；
——长整数(Long Integer)；
——大整数(Big Integer)；
——枚举(Enumeration)，从预定义的数值表中选择；
——布尔(Boolean)，True 为真，False 为假；
——文本串(Text String)，可读的文本字符串；
——字节串(Byte String)，未编码的字节值序列；
——日期-时间(Date-Time)，日期和时间，单位为秒；
——间隔(Interval)，以秒为单位的时间长度；
——结构(Structures)，由原始数据类型或子结构的有序列表组成。

6.2.2 基础对象

6.2.2.1 属性

属性对象是用于发送和接收被管理对象属性的结构，如表 1 所示。属性名是用来标识属性的文本串。属性索引是由密钥管理服务分配的索引号。属性索引用于标识特定的实例。属性索引从 0 开始。在添加或删除其他实例时，属性的属性索引不应更改。单实例属性(对象只有一个实例的属性)应该具有属性索引为 0 的属性。根据属性不同，属性值可以是原始数据类型，也可以是结构化对象。

当属性结构用于指定或返回属性的特定实例，且在未指定属性索引的情况下，应假定为 0。

表 1 属性对象结构

对象	编码	是否必需
属性	结构	
属性名称	文本串	是，具体属性及说明见 6.3
属性索引	整型	否
属性值	各不相同，取决于属性(参考 6.3)	是，通知操作除外(见 6.4.2.2)

6.2.2.2 凭证

凭证是一个用于识别客户端的结构，如表 2 所示。凭证(例如用户名和口令、令牌等)并不由密钥管

理服务端管理，它主要用于认证客户端。

表 2　凭证对象结构

对象	编码	是否必需
凭证	结构	
凭证类型	枚举型，见 6.5.3.2.1 凭证类型枚举	是
凭证值	各不相同，取决于凭证类型	是

如果凭证中的凭证类型是用户名和口令，则凭证值的结构，如表 3 所示。用户名字段标识客户端，口令字段对客户端进行认证。

表 3　用户名和口令凭证的凭证值结构

对象	编码	是否必需
凭证值	结构	
用户名	文本串	是
口令	文本串	否

如果凭证中的凭证类型是设备，则凭证值的结构，如表 4 所示。设备序列号、网络标识符、机器标识符和媒介标识符的组合是唯一的。服务端实现可以执行针对单个字段的唯一性策略。还可以使用共享密码对客户端进行认证。客户应至少提供一个字段。

表 4　设备凭证的凭证值结构

对象	编码	是否必需
凭证值	结构	
设备序列号	文本串	否
密码	文本串	否
设备标识	文本串	否
网络标识	文本串	否
机器标识	文本串	否
媒介标识	文本串	否

如果凭证中的凭证类型为认证，则凭证值结构如表 5 所示。随机值的取值从随机值对象的密钥管理服务端中获得。如果服务端不能从客户端验证认证数据，则认证凭证对象可以包含来自客户端的度量或第三方的声明。任何类型的认证数据(认证度量或认证声明)对于服务端都不是必需的，但客户应在认证度量或认证声明字段中提供认证数据。

表 5　认证凭证的凭证值结构

对象	编码	是否必需
凭证值	结构	
随机值	结构，见 6.2.2.14 随机值	是

表 5　认证凭证的凭证值结构（续）

对象	编码	是否必需
认证类型	枚举，见 6.5.3.2.36 认证类型枚举	是
认证度量	字节串	否
认证声明	字节串	否

6.2.2.3　密钥块

密钥块对象结构，如表 6 所示。用于封装与密钥密切相关的所有信息。它包含的密钥值有以下格式类型：

——Raw，只包含加密密钥材料的密钥，编码为一个字节串；

——Opaque，编码密钥，其编码对密钥管理服务端来说是未知的，它被编码为一个字节串；

——PKCS1，编码私钥，表示为 DER-encoded ASN.1 PKCS＃1 对象；

——PKCS8，编码私钥，表示为 DER-encoded ASN.1 PKCS＃8 对象，支持 RSAPrivateKey 语法和 EncryptedPrivateKey；

——X.509，编码的对象，表示为 DER-encoded ASN.1 X.509 对象；

——SM2PrivateKey，编码的 SM2 私钥，格式符合 GB/T 35276；

——透明密钥类型，指定算法结构，其中包含了各种密钥类型的定义值，如 6.2.2.7；

——Extensions，这些是特定于供应商的扩展，允许用于专有或遗留的密钥格式。

密钥块可能包含密钥压缩类型，后者表示椭圆曲线公钥的格式。默认情况下，公钥是未压缩的。

密钥块还包含密钥值字段范围内的密钥加密算法和加密长度。

如果密钥值字段内的密钥已经封装（即加密、MAC/签名，或两者都有），密钥块应包含密钥封装数据结构。

表 6　密钥块对象结构

对象	编码	是否必需
密钥块	结构	
密钥格式类型	枚举，见 6.5.3.2.3	是
密钥压缩类型	枚举，见 6.5.3.2.2	否
密钥值	字节串：封装的密钥值； 结构：明文密钥值，见 6.2.2.4	否
加密算法	枚举，见 6.5.3.2.13	是。只有当可从密钥值中获取此信息时，才可以省略。不适用于秘密数据（见 6.2.3.6）或不透明对象（见 6.2.3.7）。如显示，加密长度也应显示
加密长度	整型	是。只有当可从密钥值中获取此信息时，才可以省略。不适用于机密数据（见 6.2.3.6）或不透明对象（见 6.2.3.7）。如显示，加密算法也应显示
密钥封装数据	结构，见 6.2.2.5	否。只有密钥封装是显示

6.2.2.4 密钥值

密钥值只在密钥块中使用，并且是字节串或结构，如表 7 所示。

——密钥值结构包含密钥材料，无论是字节串、透明的密钥结构（见 6.2.2.7），还是与密钥材料相关联并封装的可选属性信息。这个属性信息不同于被管理对象的相关属性，因为它被密封在（可能是封装）密钥材料本身，并且可通过获取属性操作获得。

——密钥值字节串是封装的 TTLV 编码（见附录 B）的密钥值结构，或是字节串密钥材料字段的未编码的值。

表 7 密钥值对象结构

对象	编码	是否必需
密钥值	结构	
密钥材料	字节串：原始的、不透明的、PKCS1、PKCS8、ECPrivateKey 或扩展密钥格式类型； 结构：透明、拓展密钥格式类型	是
属性	属性对象，见 6.2.2.1	否。可能重复

6.2.2.5 密钥封装数据

密钥封装数据结构，如表 8 所示。只用于密钥块内部，密钥块还可以提供关于用于封装密钥值的加密密钥封装机制的可选信息。

表 8 密钥封装数据对象结构

对象	编码	是否必需
密钥封装数据	结构	
封装方法	枚举，见 6.5.3.2.4	是
加密密钥信息	结构，见下文	否。对应用于加密密钥值的密钥
MAC/签名密钥信息	结构，见下文	否。对应的对称密钥用于 MAC 密钥值，或私钥用于签名密钥值
MAC/签名	字节串	否
IV/计数器/随机值	字节串	否
编码选项	枚举，见 6.5.3.2.32	否。指定编码密钥值字节串。如不显示，封装的密钥值结构应为 TTLV 编码

加密密钥信息结构，如表 9 所示，MAC/签名密钥信息，如表 10 所示。

表 9 加密密钥信息对象结构

对象	编码	是否必需
加密密钥信息	结构	
唯一标识符	文本串，见 6.3.2	是
密码参数	结构，见 6.3.7	否

表 10　MAC/签名密钥信息对象结构

对象	编码	是否必需
MAC/签名密钥信息	结构	
唯一标识符	文本串，见 6.3.2	是。可以是用于 MAC 的对称密钥的唯一标识符，也可以是用于签名的私钥（或其对应的公钥）的唯一标识符
密码参数	结构，见 6.3.7	否

6.2.2.6　密钥封装规格

密钥封装规格定义为提供返回封装密钥的选项，如表 11 所示。如果客户要求服务端返回封装好的密钥，则“密钥封装规格”应包含在操作请求中。如果在加密密钥信息和/或密钥封装规格的 MAC/签名密钥信息中指定了加密参数，则服务端将验证它们是否与相应密钥的加密参数属性的实例相匹配。如果省略加密参数，则服务端应使用相应密钥加密参数属性的最小属性索引。如果对应的密钥没有加密参数属性，或发现不匹配，则返回错误。

表 11　密钥封装规格对象结构

对象	编码	是否必需
密钥封装规格	结构	
封装方式	枚举，见 6.5.3.2.4	是
加密密钥信息	结构，见 6.2.2.5	否，MAC/签名密钥信息省略时显示
MAC/签名密钥信息	结构，见 6.2.2.5	否，加密密钥信息省略时显示
属性名称	文本串	否，可能重复
编码选项	枚举，见 6.5.3.2.32	否。如编码选项不显示，则封装的密钥值将以 TTLV 编码

6.2.2.7　透明密钥

6.2.2.7.1　透明密钥结构

透明密钥结构描述获取密钥材料的必要参数，在密钥值结构中使用。在其他标准中指定的参数映射如表 12 所示。

表 12　参数映射

对象	描述	映像
P	RSA 模的素因子	[PKCS#1]中的 p
Q	RSA 模的素因子	[PKCS#1]中的 q
N	RSA 模 PQ，P 和 Q 是不同的素数	[PKCS#1]中的 n
d	RSA 私钥指数	[PKCS#1]中的 d
e	RSA 公钥指数	[PKCS#1]中的 e

表 12　参数映射（续）

对象	描述	映像
dP	CRT 格式中主因子 P 的 RSA 私钥指数，即 d mod (P-1)	[PKCS#1]中的 dP
dQ	CRT 格式中主因子 Q 的 RSA 私钥指数，即 d mod (Q-1)	[PKCS#1]中的 dQ
qInv	CRT 系数，即 Q-1 mod P	[PKCS#1]中的 qInv
D	椭圆曲线私钥	见 GB/T 32918
Q 字符串	椭圆曲线公钥	见 GB/T 32918

6.2.2.7.2　透明对称密钥

如果密钥块中的密钥格式类型为透明对称密钥，那么密钥材料是如表 13 所示的结构。

表 13　透明对称密钥的密钥材料对象结构

对象	编码	是否必需
密钥材料	结构	
密钥	字节串	是

6.2.2.7.3　透明 RSA 私钥

如果密钥块中的密钥格式类型是透明的 RSA 私钥，那么密钥材料是如表 14 所示的结构。

表 14　透明 RSA 私钥的密钥材料对象结构

对象	编码	是否必需
密钥材料	结构	
N	大整数	是
d	大整数	否
e	大整数	否
P	大整数	否
Q	大整数	否
dP	大整数	否
dQ	大整数	否
qInv	大整数	否

至少存在以下之一（参考[PKCS#1]）：

——d；

——P 和 Q；

——dP 和 dQ。

6.2.2.7.4 透明 RSA 公钥

如果密钥块中的密钥格式类型是透明的 RSA 公钥，那么密钥材料对象结构如表 15 所示。

表 15 透明 RSA 公钥的密钥材料对象结构

对象	编码	是否必需
密钥材料	结构	
N	大整数	是
e	大整数	是

6.2.2.7.5 透明 SM2 私钥

如果密钥块中的密钥格式类型是透明的 SM2 私钥，那么密钥材料对象结构如表 16 所示。

表 16 透明 SM2 私钥的密钥材料对象结构

对象	编码	是否必需
密钥材料	结构	
推荐曲线	枚举，见 6.5.3.2.5	是
D	大整数	是

6.2.2.7.6 透明 SM2 公钥

如果密钥块中的密钥格式类型是透明的 SM2 公钥，那么密钥材料对象结构如表 17 所示。

表 17 透明 SM2 公钥的密钥材料对象结构

对象	编码	是否必需
密钥材料	结构	
推荐曲线	枚举，见 6.5.3.2.5	是
Q String	字节串	是

6.2.2.8 属性集

属性集对象用于在请求中提供所需的多个属性/属性集合的值和/或名称，并在响应中返回实际的属性值。属性集对象可用于各种操作。

属性集、通用属性集、私钥属性集和公钥属性集结构的定义是相同的。属性集对象结构如表 18 所示。

表 18 属性集对象结构

对象	编码	是否必需
属性集，通用属性集、私钥属性集、公钥属性集	结构	
名称	结构，见 6.3.3	否，可重复
属性	属性对象，见 6.2.2.1	否，可重复

6.2.2.9 扩展信息

扩展信息对象是一个结构，如表 19 所示，在扩展范围内用项标签值描述对象。扩展名是用来命名对象(如表 253 所示)的文本串。扩展标记是对象的项标签值(如表 253 所示)。扩展类型是对象的项类型值(如表 B.1 所示)。

表 19 扩展信息对象结构

对象	编码	是否必需
扩展信息	结构	
扩展名	文本串	是
扩展标签	整型	否
扩展类型	整型	否

6.2.2.10 数据

数据对象用于在客户端和服务端之间传递数据的加密操作中的请求和响应。数据结构如表 20 所示。

表 20 数据对象结构

对象	编码
数据	字节串

6.2.2.11 数据长度

数据长度用于加密操作中的请求，以指示响应中预期的数据量，如表 21 所示。

表 21 数据长度结构

对象	编码
数据长度	整型

6.2.2.12 签名数据

签名数据用于密码操作中的请求和响应，这些操作将在客户端和服务端之间传递签名数据。如表 22 所示。

表 22 签名数据结构

对象	编码
签名数据	字节串

6.2.2.13 MAC 数据

MAC 数据用于密码操作中的请求和响应，这些操作将在客户端和服务端之间传递 MAC 数据。如表 23 所示。

表 23　MAC 数据结构

对象	编码
MAC 数据	字节串

6.2.2.14　随机值

随机值对象是服务端用来向客户端发送随机值的结构，如表 24 所示。随机值标识符由服务端分配，用于标识随机值对象。随机数值包括服务端创建的随机数据。

表 24　随机值结构

对象	编码	是否必需
随机数	结构	
随机数 ID	字节串	是
随机数值	字节串	是

6.2.2.15　相关值

相关值用于支持多步(流)密码操作的请求和响应。对于一个跨多个请求执行的操作来说，这是由服务端生成的，并在第一个响应中返回。如表 25 所示。

表 25　相关值结构

对象	编码
相关值	字节串

6.2.2.16　初始指示符

初始指示符用于支持多步(流)密码操作中的请求。这是在第一个请求中提供的，值为 True，用于跨多个执行操作的请求。如表 26 所示。

表 26　初始指示符结构

对象	编码
初始指示符	布尔

6.2.2.17　完成指示符

完成指示符用于支持多步(流)密码操作中的请求。这是在最后一个请求中提供的，值为 True，用于跨多个执行操作的请求。如表 27 所示。

表 27　完成指示符结构

对象	编码
完成指示符	布尔

6.2.2.18 随机数发生器(RNG)参数

RNG 参数基础对象是一个包含强制 RNG 算法和一组描述随机数发生器的可选字段的结构。特定字段仅适用于某些类型的 RNG。如表 28 所示。

应指定 RNG 算法。如果 RNG 算法未知或者不想提供具体细节时,应使用未指定的枚举。

表 28 RNG 参数结构

对象	编码	是否必需
随机数发生器参数	结构	
随机数发生器算法	枚举,见 6.5.3.2.37	是

6.2.2.19 配置文件信息

配置文件信息基础对象是一个包含受支持配置文件的详细信息的结构。特定字段仅适用于某些类型的配置文件。如表 29 所示。

表 29 配置文件信息结构

对象	编码	是否必需
配置文件信息	结构	
配置文件名称	枚举,见 6.5.3.2.40	是
服务器 URI	文本串	否
服务器端口	整型	否

6.2.2.20 验证信息

验证信息基础对象是一个包含正式验证的详细信息的结构。特定字段仅适用于某些类型的验证。如表 30 所示。

表 30 验证信息结构

对象	编码	是否必需
验证信息	结构	
验证机构类型	枚举,见 6.5.3.2.38	是
验证机构国家	文本串	否
验证机构 URI	文本串	否
验证主版本	整型	是
验证次版本	整型	否
验证类型	枚举,见 6.5.3.2.39	是
验证级别	整型	是
验证证书编号	文本串	否
验证证书 URI	文本串	否
验证供应商 URI	文本串	否
验证配置文件	文本串(可能重复)	否

提供验证机构以及验证主版本、验证类型和验证级别，以唯一标识符给定验证机构的验证。如果没有提供验证证书 URI，则服务端应该包括一个验证供应商 URI，从中可以获得与验证相关的信息。验证机构国家是两个字母的 ISO 国家代码。

6.2.2.21 能力信息

能力信息基础对象是包含所支持能力的详细信息结构。如表 31 所示。

表 31 能力信息结构

对象	编码	是否必需
能力信息	结构	
流化能力	布尔	否
异步能力	布尔	否
证明能力	布尔	否
批量撤销能力	布尔	否
批量持续能力	布尔	否
解封装模式	枚举，见 6.5.3.2.41	否
销毁操作	枚举，见 6.5.3.2.42	否
粉碎算法	枚举，见 6.5.3.2.43	否
随机数发生器模式	枚举，见 6.5.3.2.44	否

6.2.2.22 加密验证附加数据

加密验证附加数据对象用于需要客户端提供可选的附加数据，用于验证加密和解密操作。如表 32 所示。

表 32 加密验证附加数据

对象	编码	是否必需
加密验证附加数据	字节串	否

6.2.2.23 加密验证完整性标签

加密验证完整性标签对象用于验证加密模式下加密和解密的数据的完整性。它是加密过程的输出和解密过程的输入。如表 33 所示。

表 33 加密验证完整性标签

对象	编码	是否必需
加密验证完整性标签	字节串	否

6.2.3 被管理对象

6.2.3.1 证书

数字证书是一种被管理的密码对象。如表 34 所示。

表 34　证书对象结构

对象	编码	是否必需
证书	结构	
证书类型	枚举,见 6.5.3.2.6	是
证书值	字节串	是

6.2.3.2　对称密钥

对称密钥是一种被管理的密码对象。如表 35 所示。

表 35　对称密钥对象结构

对象	编码	是否必需
对称密钥	结构	
密钥块	结构,见 6.2.2.3	是

6.2.3.3　公钥

非对称密钥对的公钥部分是一种被管理的密码对象。这只是公钥,而不是证书。如表 36 所示。

表 36　公钥对象结构

对象	编码	是否必需
公钥	结构	
密钥块	结构,见 6.2.2.3	是

6.2.3.4　私钥

非对称密钥对的私钥部分是一种被管理的密码对象。如表 37 所示。

表 37　私钥对象结构

对象	编码	是否必需
私钥	结构	
密钥块	结构,见 6.2.2.3	是

6.2.3.5　拆分密钥

拆分密钥是一种被管理的密码对象。为了保密,通常将对称密钥或私钥拆分成多个部分,每个部分可以分配给几个密钥持有者,用于额外的安全性。“密钥分量”字段指示拆分的总数,“拆分密钥阈值”字段指示重建整个密钥所需的最少部分数。“密钥分量标识符”指示密码对象中包含哪个密钥部分,应至少为 1,并且小于或等于密钥分量的个数。如表 38 所示。

表 38　拆分密钥对象结构

对象	编码	是否必需
拆分密钥	结构	
密钥分量	整型	是
密钥分量标识符	整型	是
拆分密钥阈值	整型	是
拆分密钥方法	枚举，见 6.5.3.2.8	是
素域尺寸	大整数	否，只有在拆分密钥方法为多项式共享素域时为是
密钥块	结构，见 6.2.2.3	是

有三种密钥拆分方法用于密钥共享：第一个是基于异或，另外两个是基于多项式秘密共享。

假定 L 为表示所有秘密所需比特位的最小值：

——当使用异或方法时：密钥分量的长度是 L 比特位，拆分密钥阈值就是密钥分量的总数，所有密钥分量通过异或重组成密钥。

——当使用多项式共享素域方法时，秘密共享是在域 GF(素数域大小)，表示为整型，素域的大小是一个比 2^L 大的素数。

——当使用多项式共享 GF(2^{16})方法时，此处秘密共享是在域 GF(2^{16})。密钥块的值中的密钥材料是以一个 L 长度的比特串。并且当 L 大于 2^{16} 时，秘密共享使用每 16 比特一个片的集合表示。密钥块的值中的密钥材料是将所有秘密片段串起来。

——秘密共享在域 GF(2^{16})中完成，GF(2^{16})是 GF(2^8)的扩展：
GF(2^{16})≈GF(2^8)[y]/(y^2+y+m)，其中的 m 在之后定义。这个域的一个元素由一个线性组合 $uy+v$ 组成，其中的 u 和 v 是更小的域 GF(2^8)的元素。

6.2.3.6　秘密数据

秘密数据是一种被管理的密码对象，它包含一个非密钥或证书的共享秘密值(例如口令)。秘密数据对象的密钥块包含秘密数据类型的密钥值。这个密钥值可以被封装。如表 39 所示。

表 39　秘密数据对象结构

对象	编码	是否必需
秘密数据	结构	
秘密数据类型	枚举，见 6.5.3.2.9	是
密钥块	结构，见 6.2.2.3	是

6.2.3.7　不透明对象

不透明数据对象是一种密钥管理服务端无法识别的被管理对象。可以使用自定义属性来存储和检索此对象的上下文信息。如表 40 所示。

表 40　不透明对象结构

对象	编码	是否必需
不透明对象	结构	
不透明数据类型	枚举，见 6.5.3.2.10	是
不透明数据值	字节串	是

6.3　属性

6.3.1　概述

以下小节描述与被管理对象关联的属性。对象具有多个实例的属性称为多实例属性。属性的所有实例应该具有不同的值。另外，对象最多只有一个实例的属性称为单实例属性。客户端通过“获取属性”操作从服务端获取属性。某些属性能够通过“添加属性”操作进行设置，或者通过“修改属性”操作进行更新。如果某些属性不再适用于被管理对象，则可以通过“删除属性”操作将其删除。只读属性是不应被任何服务端或客户端修改的属性，并且不应被客户端删除。

当服务端返回属性（如，“获取属性”操作）时，返回的属性值对于不同的客户端可能有所不同（如，根据服务端的策略，不同客户端的密码用途掩码值可能不同）。

每个小节中的第一个表包含第一行中的属性名称。该名称是使用“获取属性”，“获取属性列表”，“添加属性”，“修改属性”和“删除属性”操作，来管理属性时使用的规范名称。

服务端如果没收到客户端请求不应删除属性，直到被管理对象被销毁。在对象被销毁之后，服务端可能会保留对象属性中的一些值，这具体取决于对象类型和服务端策略。

每个小节中的第二个表格列出了某些属性特征（例如，“必须有值”）；如表 41 所示说明了可能出现在这些表中的每个特征的含义。服务端策略可以进一步限制这些属性特征。

表 41　属性规则

属性特征	含义
必须有值	所有被管理对象都是这个属性应用的对象类型，一旦对象被创建或注册，它将始终具有这个属性，直到对象被销毁为止
初始化设置方	哪一方设置属性的初值（如果属性从未被设置，或者所有属性值都被删除）
服务端可修改	是否允许服务端更改属性的现有值，而不从客户端接收请求
客户端可修改	一旦设置了属性值，客户端能否更改属性值的现有值
客户端可删除	客户端能否删除属性的实例
允许多实例	是否允许多个属性实例
何时隐式设置	即使在操作请求本身没有指定属性，哪些操作也可以设置此属性
适用对象类型	哪些被管理对象可以设置此属性

6.3.2　唯一标识符

唯一标识符是由密钥管理服务端生成的唯一标识管理对象。它仅在由单个密钥管理服务端管理的标识符空间内是全局唯一的，以便允许此类对象的密钥管理域导出。此属性应由密钥管理服务端在创

建或注册时分配,在对象被销毁之前不应更改或删除。如表 42 与表 43 所示。

表 42　唯一标识符属性

对象	编码	是否必需
唯一标识符	文本串	是

表 43　唯一标识符属性规则

属性特征	规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥,创建密钥对,注册,派生密钥,更新对称密钥,更新密钥对
适用对象类型	所有对象

6.3.3　名称

名称属性用于识别和定位对象,该属性由客户端分配。名称属性的值应方便理解。密钥管理服务端可以指定客户端创建有效名称的规则。客户端可以自定义标准未指定的命名规则。名称在给定的密钥管理域内应该是唯一的,不要求全局唯一。如表 44 与表 45 所示。

表 44　名称属性结构

对象	编码	是否必需
名称	结构	
名称值	文本串	是
名称类型	枚举,见 6.5.3.2.11	是

表 45　名称属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端
服务端可修改	是
客户端可修改	是
客户端可删除	是
允许多实例	是
何时隐式设置	更新对称密钥,更新密钥对
适用对象类型	所有对象

6.3.4 对象类型

对象类型(例如:公钥、私钥、对称密钥等)在创建或注册对象时由服务端设置;在对象被销毁之前不应被更改或删除。如表 46 与表 47 所示。

表 46 对象类型属性

对象	编码
对象类型	枚举,见 6.5.3.2.12

表 47 对象类型属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥,创建密钥对,注册,派生密钥,更新对称密钥,更新密钥对
适用对象类型	所有对象

6.3.5 密码算法

对象的密码算法。证书对象的密码算法,标识证书中包含的公钥算法。用于签署证书的数字签名算法,在 6.3.14 中定义的数字签名算法属性中进行标识。当对象被创建或注册时,该属性应由服务端设置,然后在对象被销毁之前不应被更改或删除。如表 48 与表 49 所示。

表 48 加密算法属性

对象	编码
密码算法	枚举,见 6.5.3.2.13

表 49 加密算法属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥,创建密钥对,注册,派生密钥,更新对称密钥,更新密钥对
适用对象类型	密钥,证书

6.3.6 加密长度

对于被管理对象的密钥，加密长度是明文加密密钥材料的长度(以位为单位)；对于证书而言，加密长度是指证书内的公钥长度(以位为单位)。创建或注册对象时，该属性应由服务端设置，在对象被销毁之前不应被更改或删除。如表 50 与表 51 所示。

表 50 加密长度属性

对象	编码
加密长度	整型

表 51 加密长度属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，更新对称密钥，更新密钥对
适用对象类型	密钥，证书

6.3.7 密码参数

密码参数属性是一个结构，如表 52 与表 53 所示，它包含一组描述某些密码参数可选字段，在对象执行密码操作时使用。特定字段可能仅适用于特定类型的被管理对象。证书对象的密码参数属性，标识证书中包含的公钥密码参数。

密码算法属性也用于指定密码操作的参数。对于涉及数字签名的操作，可以指定数字签名算法，也可以指定加密算法和杂凑算法的组合。

对于一个使用 IV 的加密算法，可以用服务端生成一个随机的 IV。生成的随机 IV 在响应加密操作中返回。

IV 的长度是初始向量的长度(以位为单位)。在指定的分组密码模式支持可变的 IV 长度时，应提供此参数。

标签长度是认证标签的长度(以字节为单位)。当分组密码模式为 GCM 或 CCM 时，应提供该参数。

对于一个给定的加密密钥，与计数器操作模式（如 CTR 和 GCM）一起使用的 IV 不能重复。

初始计数器值对于 CTR 模式来说就是开始计数的值。

表 52　密码参数属性结构

对象	编码	是否必需
密码参数	结构	
分组密码模式	枚举,见 6.5.3.2.14	否
填充方法	枚举,见 6.5.3.2.15	否
杂凑算法	枚举,见 6.5.3.2.16	否
密钥角色类型	枚举,见 6.5.3.2.17	否
数字签名算法	枚举,见 6.5.3.2.7	否
密码算法	枚举,见 6.5.3.2.13	否
随机 IV	布尔	否
IV 长度	整型	否,除非分组密码模式支持变 IV 长度
标签长度	整型	否,除非分组密码模式是 GCM
固定字段长度	整型	否
调用字段长度	整型	否
计数器长度	整型	否
初始计数器值	整型	否
盐长度	整型	否
填充字段	整型	否(如果省略,默认为 PSS 填充中的标准单字节预告)

表 53　密码参数属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端
服务端可修改	否
客户端可修改	是
客户端可删除	是
允许多实例	是
何时隐式设置	更新对称密钥,更新密钥对
适用对象类型	密钥,证书

密钥类型定义如表 54 所示。

表 54　密钥类型定义

密钥类型	定义
BDK	基础派生密钥(Base Derivation Key)
CVK	卡验证密钥(Card Verification Key)
DEK	数据加密密钥[Data Encryption Key (通用数据加密)]
MKAC	IC 卡应用密文主密钥(EMV/chip card Master Key:Application Cryptograms)
MKSMC	IC 卡安全报文加密主密钥(EMV/chip card Master Key:Secure Messaging for Confidentiality)
MKSMI	IC 卡安全报文认证主密钥(EMV/chip card Master Key:Secure Messaging for Integrity)
MKDAC	IC 卡数据认证主密钥(EMV/chip card Master Key:Data Authentication Code)
MKDN	IC 卡动态数主密钥(EMV/chip card Master Key:Dynamic Numbers)
MKCP	IC 卡个人化主密钥(EMV/chip card Master Key:Card Personalization)
MKOTH	其他 IC 卡主密钥(EMV/chip card Master Key:Other)
KEK	密钥加密(封装)密钥(Key Encryption or Wrapping Key)
MAC16609	ISO 16609 MAC 算法 1
MAC97971	ISO 9797-1 MAC 算法 1
MAC97971	ISO 9797-1 MAC 算法 1(见 GB/T 15852.1)
MAC97972	ISO 9797-1 MAC 算法 2(见 GB/T 15852.1)
MAC97973	ISO 9797-1 MAC 算法 3 (即 X9.19 零售 MAC)
MAC97974	ISO 9797-1 MAC 算法 4(见 GB/T 15852.1)
MAC97975	ISO 9797-1 MAC 算法 5(见 GB/T 15852.1)
ZPK	PIN 加密密钥(PIN Block Encryption Key)
PVKPVV	PIN 验证密钥(PIN Verification Key,VISA PVV 算法)
PVKOTH	PIN 验证密钥(PIN Verification Key,其他算法)

6.3.8　密码算法域参数

密码算法域参数属性是一个结构,如表 55 所示,其中包含一组可选字段,这些字段可能需要在创建密钥对请求有效载荷中指定。特定的字段可能只涉及某些类型的被管理对象。密码算法域参数属性规则,如表 56 所示。

推荐曲线适用于椭圆曲线算法,见 GB/T 32918。

表 55　密码算法域参数属性结构

对象	编码	是否必需
密码算法域参数	结构	是
推荐曲线	枚举,见 6.5.3.2.5	否

表 56　密码算法域参数属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	更新密钥对
适用对象类型	非对称密钥

6.3.9　证书类型

证书类型属性表示一类证书(例如 X.509)。如表 57 与表 58 所示。

证书类型值应该由服务端在创建或注册证书时设置,并且在对象销毁之前不应更改或删除。

表 57　证书类型属性

对象	编码	
证书类型	枚举,见 6.5.3.2.6	

表 58　证书类型属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注册
适用对象类型	证书

6.3.10　证书长度

证书长度属性是证书对象的字节长度。证书长度应该由服务端在创建或注册对象时设置,并且在对象销毁之前不应更改或删除。如表 59 与表 60 所示。

表 59　证书长度属性

对象	编码
证书长度	整型

表 60　证书长度属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注册
适用对象类型	证书

6.3.11　X.509 证书标识符

X.509 证书标识符属性是一种结构，如表 61 与表 62 所示，用于提供 X.509 公钥证书的标识。X.509 证书标识符包含颁发者可识别名(即来自 X.509 证书的颁发者字段)和证书序列号(即来自 X.509 证书的序列号字段)。当 X.509 证书被创建或注册时，X.509 证书标识符应该由服务端设置，并且在对象销毁之前不应更改或删除。

表 61　X.509 证书标识符属性结构

对象	编码	是否必需
X.509 证书标识符	结构	
颁发者可识别名	字节串	是
证书序列号	字节串	是

表 62　X.509 证书标识符属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注册
适用对象类型	X.509 证书

6.3.12 X.509 证书主体

X.509 证书主体属性是用于识别 X.509 证书主体的结构，如表 63 与表 64 所示。X.509 证书主体包含主体可识别名(即来自 X.509 证书的主体字段)。可以包含一个或多个替换名(例如电子邮件地址，IP 地址，DNS 名称)作为 X.509 证书主体(即来自 X.509 证书中的主体替换名扩展)。X.509 证书主体应该由服务端根据 X.509 证书注册(作为注册操作的一部分)时提取的信息进行设置，并且在对象被销毁之前不应被改变或删除。

如果主体替换名扩展包含在 X.509 证书中，并且在 X.509 证书本身中被标记为关键项，则可以发布主体字段留空的 X.509 证书。因此，主体可识别名可以为空字符串。

表 63 X.509 证书主体属性结构

对象	编码	是否必需
X.509 证书主体	结构	
主体可识别名	字节串	是，但可能为空字符串
主体替换名	字节串	是，如果主体可识别名为空字符串。可能重复

表 64 X.509 证书主体属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注册
适用对象类型	X.509 证书

6.3.13 X.509 证书颁发者

X.509 证书颁发者属性是用于标识包含颁发者可识别名(即来自 X.509 证书的颁发者字段)的 X.509 证书颁发者的结构，如表 65 与表 66 所示。它可以包含一个或多个替换名(例如电子邮件地址，IP 地址，DNS 名称)作为证书颁发者(即来自 X.509 证书中的颁发者替换名扩展)。服务端应根据从 X.509 证书中提取的信息设置这些值，这些证书是作为注册操作的一部分发送。在销毁对象之前，不应更改或删除这些值。

表 65 X.509 证书颁发者属性结构

对象	编码	是否必需
X.509 证书颁发者	结构	
颁发者可识别名	字节串	是
颁发者替换名	字节串	否，可能重复

表 66　X.509 证书颁发者属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注册
适用对象类型	X.509 证书

6.3.14　数字签名算法

数字签名算法属性标识是与数字签名对象(例如证书)相关联的数字签名算法,如表 67 与表 68 所示。当对象被创建或注册时,该属性应该由服务端设置,并且在对象被销毁之前不应被更改或删除。

表 67　数字签名算法属性

对象	编码
数字签名算法	枚举,见 6.5.3.2.7

表 68　数字签名算法属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否(对 X.509 证书)
何时隐式设置	注册
适用对象类型	证书

6.3.15　摘要

摘要属性是一个结构,如表 69 与表 70 所示,其包括密钥或秘密数据(即密钥材料的摘要)、证书(即证书值的摘要)或不透明对象(即不透明数据值的摘要)的摘要值。如果密钥材料是一个字节字符串,那么摘要值应该计算在这个字节字符串上。如果密钥材料是一个结构,那么摘要值应根据 TTLV 编码(见附录 B)在该密钥材料结构上进行计算。摘要属性中的密钥格式类型字段指示管理对象的格式,摘要值是从该管理对象计算得出的。可以使用 6.5.3.2.16 中列出的不同算法和/或 6.5.3.2.3 中列出的密

钥格式类型来计算多个摘要。如果这个属性存在，那么它应该有一个用 GB/T 32905 SM3 杂凑算法计算的强制属性实例。对于由客户端注册的对象，服务端应该使用注册对象的密钥格式类型，来计算强制属性实例的摘要。在所有其他情况下，只要它能够以相同格式向客户端提供对象，服务端可以在计算强制属性实例的摘要时，使用任何密钥格式类型，摘要是静态的，并应该在对象创建或注册时由服务端设置，前提是服务端可以访问密钥材料或摘要值（可能通过带外机制获取）。

表 69　摘要属性结构

对象	编码	是否必需
摘要	结构	
密码杂凑算法	枚举，见 6.5.3.2.16	是
摘要值	字节串	是，如果服务端可以访问摘要值或密钥材料（用于密钥和秘密数据），证书值（用于证书）或不透明数据值（用于不透明对象）
密钥格式类型	枚举，见 6.5.3.2.3	是的，如果管理对象是密钥或秘密数据对象

表 70　摘要属性规则

属性特征	属性规则
必须有值	是，如果服务端可以访问摘要值、密钥材料（用于密钥和秘密数据）、证书值（用于证书）或不透明数据值（用于不透明对象）
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	是
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，更新对称密钥，更新密钥对
适用对象类型	所有密码对象，不透明对象

6.3.16　密码用途掩码

密码用途掩码属性定义了密钥的用途。掩码向客户端指示哪些密码功能可以使用密钥执行，哪些不应执行。如下列：

——签名；
——验签；
——加密；
——解密；
——密钥封装；
——密钥解封装；
——导出；
——生成 MAC；
——验证 MAC；

——派生密钥；
——防抵赖；
——密钥协商；
——证书签发；
——CRL 签发；
——生成密码；
——验证密码；
——传输加密；
——传输解密；
——传输封装；
——传输解封装。

此列表考虑了可能会出现在 X.509 证书中的密钥用法扩展值。但是，该列表不考虑可能会出现在密钥用法扩展中的额外用法。

X.509 证书中密钥用法值应按照以下方式映射到密码用途掩码值，如表 71 所示。密码用途掩码属性与规则，如表 72 与表 73 所示。

表 71　X.509 密钥用法到密码用途掩码的对应

X.509 密钥用法到密码用途对应	
X.509 密钥用法	密码用途
digitalSignature	签名或验签
contentCommitment	防抵赖（不可否认性）
keyEncipherment	密钥封装或密钥解封装
dataEncipherment	加密或解密
keyAgreement	密钥协商
keyCertSign	证书签发
cRLSign	CRL 签发
encipherOnly	只加密
decipherOnly	只解密

表 72　密码用途掩码属性

对象	编码
密码用途掩码	整型

表 73　密码用途掩码属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端或客户端
服务端可修改	是

表 73　密码用途掩码属性规则（续）

属性特征	属性规则
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建，创建密钥对，注册，派生密钥，更新密钥，更新密钥对
适用对象类型	所有密码对象

6.3.17　租约时间

“租约时间”属性定义了被管理对象的时间间隔，如表 74 和表 75 所示，超出该时间间隔，客户端不应使用该对象，除非获取到另一个租约。该属性始终保存租约允许的初始时间长度，而不是实际的剩余时间。一旦租约到期，客户端只能通过调用“租约获取”操作进行续约。服务端应在此属性中存储它能够服务的最大租约时间，而且客户端获取的租约（通过“租约获取”操作）要小于或等于最大租约时间。该属性对于客户端是只读的。它只能由服务端修改。

表 74　租约时间属性

对象	编码
租约时间	间隔

表 75　租约时间属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	是
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，更新对称密钥，更新密钥对
适用对象类型	所有密码对象

6.3.18　使用限制

使用限制属性是一种限制被管理对象使用的机制。它仅适用于能够用于实施密码保护的被管理对象，并且仅影响该保护（例如加密，签名等）应用的用法。该属性并不一定适用于所有被管理对象，因为根据客户端/服务端策略，某些对象可以无限制地用于加密保护数据。用于处理密码保护数据（例如解密，验证等）的用途不受限制。使用限制属性具有以下三个字段：

——使用限制总数，允许被管理对象的使用限制单位总数。这是被管理对象整个生命周期的限制总值，并且一旦被管理对象开始用于实施密码保护，该值就不应被更改；

——使用限制计数，当前剩余的被管理对象的使用限制单位数量；

——使用限制单位，此结构指定使用限制的数量类型（如，字节，对象）。

在初始设置属性时（通常在对象创建或注册期间），使用限制计数被设置为对象使用寿命允许的使用限制总数值，并且在使用对象时递减。如果在创建新对象的操作中指定了该属性，则服务端应忽略使用限制计数值。通过“修改属性”操作所做的更改反映了“使用限制总数”值的更正，但一旦“使用限制计数”值由“获取使用配额”操作更改，它们不应再被更改。使用限制计数值不应由客户端通过添加属性或修改属性操作设置或修改。使用限制属性结构和规则，如表 76 和表 77 所示。

表 76　使用限制属性结构

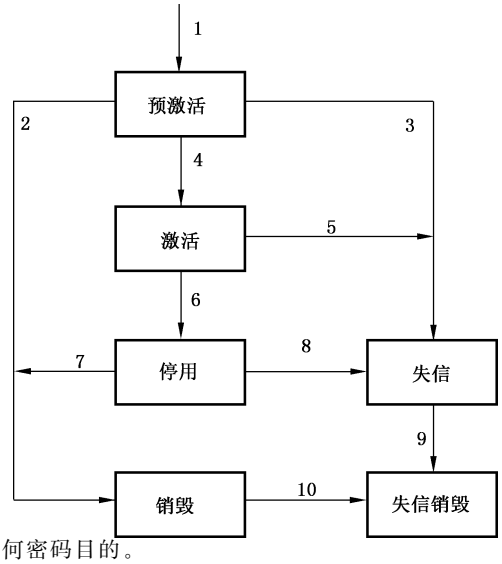
对象	编码	是否必需
使用限制	结构	
使用限制总数	长整型	是
使用限制计数	长整型	是
使用限制单位	枚举，见 6.5.3.2.31	是

表 77　使用限制属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端（总数、计数和单位） 客户端（总数和/或单位）
服务端可修改	是
客户端可修改	是（仅总数和/或单位，只要“获取使用配额”操作尚未执行）
客户端可删除	是，只要“获取使用配额”操作尚未执行
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，更新对称密钥，更新密钥对，获取使用配额
适用对象类型	密钥

6.3.19　状态

该属性表示密钥管理服务端已知的对象状态。状态属性与规则，如表 78 与表 79 所示。不应通过对此属性使用修改属性操作来更改状态。该状态只能由服务端作为其他操作或其他服务端进程的一部分进行更改。在任何给定时间，对象应处于图 2 所示状态之一。（注意：这些状态对应于[SP800-57-1]中描述的状态）。



预激活：对象存在，不应用于任何密码目的。

激活：在用于任何密码目的之前，对象应该被转换为激活状态。该对象只能用于其密码用途掩码属性所允许的所有密码目的。如果设置了生效日期(见 6.3.21)属性，那么在生效日期之前，该对象不能应用于密码目的。如果设置了失效日期(见 6.3.22)属性，则该对象在失效日期之后不能应用于密码目的。

停用：对象不应用于实施密码保护(例如，加密，签名，密钥封装，生成 MAC，派生密钥)。该对象只能用于“密码用途掩码”属性所允许的密码目的。该对象只能用于处理已受密码机制保护的信息(例如，解密，签名验证，密钥解封装，在特殊情况下且授予特别许可时的 MAC 验证。)

失信：该对象不能用于实施密码保护(例如，加密，签名，密钥封装，生成 MAC，派生密钥)。该对象只能用于处理已受密码机制保护的信息(例如，在可信的客户端使用已失信的管理对象进行解密，签名验证，密钥解封装，验证 MAC)。该对象只能用于“密码用途掩码”属性所允许的密码目的。

销毁：对象不应用于任何密码目的。

失信销毁：对象不应用于任何密码目的；但是，为了审计或安全目的，应保留其失信状态。

状态转换发生如下。

a) “1”从不存在的密钥到预激活状态的转换是由对象的创建引起的。当一个对象被创建或注册时，它会自动从不存在状态到预激活状态。但是，如果创建或注册对象的操作包含已经发生的激活日期，则状态会立即从预激活转换为激活。在这种情况下，服务端应该将激活日期属性设置为请求中指定的值，或者根据服务端策略使尝试创建或注册对象的请求失败。如果操作包含未来的激活日期属性或不包含激活日期，则被管理对象在密钥管理服务端中以预激活状态进行初始化。

b) “2”从预激活到销毁的转换是由发出销毁操作的客户端引起的。当(且如果)服务端策略规定时，服务端销毁对象。

c) “3”从预激活到失信状态的转换是由客户端发出注销操作引起的，该注销操作包含失信注销原因。

d) “4”从预激活到激活的转换应以三种方式之一进行：

   1) 激活日期已到；

   2) 客户端成功发出修改属性操作，将激活日期修改为过去的日期或当前日期；

   3) 客户端在对象上发出激活操作，服务端应将激活日期设置为收到激活操作的时间。

e) “5”从激活到失信的转换是由客户端发出注销操作引起的，该注销操作包含失信注销原因。

f) “6”从激活状态到停用状态的转换有三种方式：

   1) 该对象的停用日期已到；

   2) 客户发出注销操作，该注销操作包含失信注销原因；

   3) 客户端成功发出修改属性操作，将停用日期修改为过去的日期或当前日期。

g) “7”从停用到销毁的转换是由客户端或服务端根据服务端策略发出销毁操作引起的。当(且如果)服务端策略规定时，服务端销毁对象。

h) “8”从停用到失信的转换是由客户端发出注销操作引起的，该注销操作包含失信注销原因。

i) “9”从失信到失信销毁的转换是由客户端发出销毁操作或由服务端根据服务端策略引起的。当(且如果)服务端策略规定时，服务端销毁对象。

j) “10”从销毁到失信销毁的转换是由于客户端发出注销操作引起的，该注销操作包含失信注销原因。

图 2　密码对象状态及转换

表 78　状态属性

对象	编码
状态	枚举，见 6.5.3.2.18

表 79　状态属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	是
客户端可修改	否，但只能由服务端响应某些请求（请参阅上文）
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，激活，注销，销毁，更新对称密钥，更新密钥对
适用对象类型	所有密码对象

6.3.20　初始化日期

初始化日期属性包含密钥管理对象在服务端上首次创建或注册的日期和时间。如表 80 与表 81 所示。这个时机对应于状态转换“1”，见图 2。当创建或注册对象时，该属性应由服务端设置，然后在对象被销毁之前不应被更改或删除。当非密码对象第一次注册时，此属性也会被服务端设置。

表 80　初始化日期属性

对象	编码
初始化日期	日期-时间

表 81　初始化日期属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，激活，注销，销毁，更新对称密钥，更新密钥对
适用对象类型	所有对象

6.3.21 激活日期

激活日期属性包含被管理对象可以开始使用的日期和时间，如表 82 与表 83 所示。这个时机对应于状态转换“4”，见图 2。在到达激活日期之前，该对象不应用于任何加密目的。一旦从预激活状态转换到激活状态，则此属性在对象被销毁之前不应被更改或删除。

表 82 激活日期属性

对象	编码
激活日期	日期-时间

表 83 激活日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端或客户端
服务端可修改	是，只有在预激活状态
客户端可修改	是，只有在预激活状态
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，激活，注销，销毁，更新对称密钥，更新密钥对
适用对象类型	所有密码对象

6.3.22 生效日期

生效日期属性是被管理对象可以开始用于处理加密保护信息（例如解密或解封装）的日期和时间，如表 84 和表 85 所示。具体允许操作属性取决于其密码用途掩码属性的值。在达到生效日期之前，该对象不应用于加密目的。此值可以等于或晚于激活日期，但不能在激活日期之前。一旦生效日期到达，则此属性在对象被销毁之前不应被改变或删除。

表 84 生效日期属性

对象	编码
生效日期	日期-时间

表 85 生效日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端或客户端
服务端可修改	是，只有处于“预激活”或“激活”状态，并且生效日期未到达

表 85　生效日期属性规则（续）

属性特征	属性规则
客户端可修改	是，只有处于“预激活”或“激活”状态，并且生效日期未到达
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，注册，派生密钥，更新对称密钥
适用对象类型	对称密钥，对称密钥的拆分密钥

6.3.23　失效日期

失效日期属性是被管理对象不能用于处理加密保护信息（例如：加密或封装）的日期和时间，如表 86 和表 87 所示。具体允许操作属性取决于其密码用途掩码属性的值。该值可能等于或早于，但不应晚于停用日期。一旦到达失效日期，则此属性在对象被销毁之前不应更改或删除该属性。

表 86　失效日期属性

对象	编码
失效日期	日期-时间

表 87　失效日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端或客户端
服务端可修改	是，只有在处于预活动状态或激活状态，并且只要失效日期尚未到达
客户端可修改	是，只有在处于预活动状态或激活状态，并且只要失效日期尚未到达
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，注册，派生密钥，更新对称密钥
适用对象类型	对称密钥，对称密钥的拆分密钥

6.3.24　停用日期

停用日期属性是被管理对象除了解密、签名验证或解封装外，不应用于任何目的的日期和时间，并且只能在特殊情况下且授予特殊许可时才允许使用，如表 88 和表 89 所示。这一时机对应于状态转换“6”，见图 2。除非对象处于“预激活”或“激活”状态，否则在对象被销毁之前不应改变或删除此属性。

表 88　停用日期属性

对象	编码
停用日期	日期-时间

表 89　停用日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端或客户端
服务端可修改	是,只有在预激活状态或激活状态
客户端可修改	是,只有在预激活状态或激活状态
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥,创建密钥对,注册,派生密钥,销毁,更新对称密钥,更新密钥对
适用对象类型	所有密码对象

6.3.25　销毁日期

销毁日期属性是被管理对象被销毁的日期和时间,如表 90 和表 91 所示。这一时机对应于状态转换“2”“7”或“9”,见图 2。当接收到销毁操作或由于服务端策略或带外管理操作而导致对象销毁时,由服务端设置该值。

表 90　销毁日期属性

对象	编码
销毁日期	日期-时间

表 91　销毁日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	销毁
适用对象类型	所有密码对象,不透明对象

6.3.26　失信发生日期

失信发生日期属性是被管理对象第一次被认定为失信的日期和时间,如表 92 和表 93 所示。如果不可能估计何时发生失信,那么该值应该设置为该对象的初始化日期。

表 92　失信发生日期属性

对象	编码
失信发生日期	日期-时间

表 93　失信发生日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注销
适用对象类型	所有密码对象,不透明对象

6.3.27　失信日期

失信日期属性包含被管理对象进入失信状态的日期和时间,如表 94 或表 95 所示。此时机对应于状态转换“3”“5”“8”或“10”,见图 2。这个时间表明密钥管理服务端何时意识到对象失信,而不一定是在失信发生时。当服务端接收到具有失信注销原因的注销操作,或由于服务端策略或带外管理操作时,由服务端设置该属性。

表 94　失信日期属性

对象	编码
失信日期	日期-时间

表 95　失信日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	否
客户端可修改	否

表 95　失信日期属性规则（续）

属性特征	属性规则
客户端可删除	否
允许多实例	否
何时隐式设置	注销
适用对象类型	所有密码对象，不透明对象

6.3.28　注销原因

注销原因属性是用于指示被管理对象为什么被注销（例如，“销毁”“过期”“不再使用”等）的一个结构，如表 96 和表 97 所示。该属性作为注销操作的一部分，仅能由服务端设置。

注销原因是专门用于审计追踪/记录的目的，可能包含关于为什么该对象被注销附加信息的可选字段（例如，“笔记本电脑遗失”或“机器退役”）。

表 96　注销原因属性结构

对象	编码	是否必需
注销原因	结构	
注销原因码	枚举，见 6.5.3.2.19	是
注销信息	文本串	否

表 97　注销原因属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	是
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注销
适用对象类型	所有密码对象，不透明对象

6.3.29　归档日期

归档日期属性是被管理对象归档存储的日期和时间，如表 98 和表 99 所示。该值作为归档操作的一部分，由服务端设置。每当执行恢复操作时，服务端都应删除此属性。

表 98　归档日期属性

对象	编码
归档日期	日期-时间

表 99　归档日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	激活
适用对象类型	所有对象

6.3.30　对象组

对象是对象组的一部分。一个对象可能属于多个对象组，如表 100 和表 101 所示。要将对象分配给一个对象组，应该设置此属性为对象组名称。“默认值”是对象组的保留文本字符串。

表 100　对象组属性

对象	编码
对象组	文本串

表 101　对象组属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	是
允许多实例	是
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，更新密钥对
适用对象类型	所有对象

6.3.31 未使用

未使用属性是一个布尔属性，它表示该对象从未提供给客户端使用，如表 102 和表 103 所示。当在服务端上创建新对象时，未使用属性应设置为真。一旦将对象提供给客户端使用后，服务端就会将该属性值更改为假。

表 102 未使用属性

对象	编码
未使用	布尔

表 103 未使用属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，更新密钥对
适用对象类型	所有密码对象

6.3.32 链接

链接属性是用于创建从一个被管理对象到另一个紧密相关的目标被管理对象的结构，如表 104 和表 105 所示。该链接具有类型，并且允许的类型不同，具体取决于被管理对象的对象类型，如下所示。该链接的对象标识符标识唯一的被管理对象目标。该链接包含有关被管理对象之间的关联信息(如，与公钥相对应的私钥；证书链中证书的签发者证书；派生对称密钥与其导出的原始密钥)。

根据被管理对象的对象类型，链接类型的值如下。

——私钥链接：对应于公钥的私钥。

——公钥链接：私钥对象对应的公钥。对于证书对象为证书中包含的公钥。

——证书链接：对于证书对象为证书链中证书的签发者证书。对于公钥对象对应为包含相同公钥的证书。

——派生基础对象链接：对于派生的对称密钥或秘密数据对象，对应从中导出当前对称密钥的对象。

——派生密钥链接：从当前对象导出的对称密钥或密钥数据对象。

——被替换对象链接：对称密钥，非对称私钥或不对称公钥对象对应于由当前密钥重建产生的密钥。对于证书对象对应于重新认证产生的证书。请注意，每个被管理对象只能有一个这样的替换对象。

——替换对象链接：对称密钥，不对称私钥或不对称公钥对象对应于重新创建以获取当前密钥的密钥。对于证书对象对应于重新认证获得当前证书的证书。

——父链接：对于所有对象类型对应于对象对应的所有者，容器或其他父对象。

——子链接：对于所有对象类型对应于对象相对应的从属，派生或其他子对象。

——上一个链接：对于所有对象类型对应于此对象的上一个对象。

——下一个链接：对于所有对象类型对应于此对象的下一个对象。

链接属性应该存在于由服务端存储证书链和证书链中的证书的私钥和公钥中。

密码对象有可能具有链接属性的多个实例(例如，私钥具有到关联证书的链接以及相关联的公钥；证书对象具有到公钥和签发证书认证机构的证书)。

管理对象也可能没有与相关密码对象的链接。这可能发生在服务端或客户端无法使用相关密钥材料的情况下(例如，用服务端注册 CA 签名证书，以相应的方式保存对应的私钥)。

管理对象也可能不具有到相关密码对象的链接。这可能发生在相关联的密钥材料对服务端或客户端不可用的情况下(例如，与服务端注册 CA 签署者证书，其中相应的私钥以不同的方式保存)。

表 104　链接属性结构

对象	编码	是否必需
链接	结构	
链接类型	枚举，见 6.5.3.2.20	是
链接对象标识符，见 6.3.1	文本串	是

表 105　链接属性规则

属性特征	属性规则
必须有值	没有
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	是
允许多实例	是
何时隐式设置	创建密钥对，更新密钥对
适用对象类型	所有密码对象

6.3.33　应用特定信息

应用特定信息属性是用于存储使用管理对象的特定应用(一个或多个)数据结构，如表 106 和表 107 所示。它由以下字段组成：应用程序命名空间和具体应用程序命名空间的应用程序数据。

客户端可以请求设置(即使用在服务端上导致新的被管理对象的任何操作或添加/修改现有被管理对象的属性)具有应用程序命名空间的此属性的实例，同时省略应用程序数据。在这种情况下，如果服务端支持此命名空间(如 6.4.1.24 中的查询操作所示)，则应返回合适的应用程序数据值。如果服务端不支持此命名空间，则会返回一个错误。

表 106　应用特定信息属性结构

对象	编码	是否必需
应用程序特定信息	结构	
应用程序命名空间	文本串	是
应用程序数据	文本串	否

表 107　应用特定信息属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端(仅在客户端请求中忽略应用程序数据时)
服务端可修改	是(仅在客户端请求中忽略了应用程序数据)
客户端可修改	是
客户端可删除	是
允许多实例	是
何时隐式设置	更新对称密钥,更新密钥对
适用对象类型	所有对象

6.3.34　联系信息

联系信息属性是可选的,其内容仅用于联系目的,如表 108 和表 109 所示。它不用于策略执行。该属性由客户端或服务端设置。

表 108　联系信息属性

对象	编码
联系信息	文本串

表 109　联系信息属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	是
允许多实例	否
何时隐式设置	创建对称密钥,创建密钥对,注册,派生密钥,更新对称密钥,更新密钥对
适用对象类型	所有对象

6.3.35 最后修改日期

最后更改日期属性包含指定对象上次修改的日期和时间，如表 110 和表 111 所示。

表 110 最后修改日期属性

对象	编码
最后修改日期	日期-时间

表 111 最后修改日期属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	是
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，注册，派生密钥，激活，注销，销毁，归档，恢复，更新对称密钥，更新密钥对，添加属性，修改属性，删除属性，获取使用配额
适用对象类型	所有对象

6.3.36 自定义属性

自定义属性是用于特定供应商的客户端或服务端定义的属性。它由客户端或由服务端创建，由客户端解释，如表 112 和表 113 所示。客户端创建的所有自定义属性都应遵循命名方案，其中属性的名称应具有前缀“x-”。密钥管理服务端创建的所有自定义属性都应遵循命名方案，其中属性的名称应具有前缀“y-”。服务端不接受客户端创建或修改属性的名称前缀为“y-”的属性。标签类型自定义属性无法识别特定属性；因此这样一个属性只能出现在属性结构中，其名称如第 6.2.2.1 的定义。

表 112 自定义属性

对象	编码	备注
自定义属性	任何数据类型或结构。如果是结构，那么结构应该不包括子结构	属性的名称应以“x-”或“y-”开头

表 113 自定义属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	是，对于服务端创建的属性

表 113　自定义属性规则（续）

属性特征	属性规则
客户端可修改	是，对于客户端创建的属性
客户端可删除	是，对于客户端创建的属性
允许多实例	是
何时隐式设置	创建对称，创建密钥对，注册，派生密钥，激活，注销，销毁，更新对称密钥，更新密钥对
适用对象类型	所有对象

6.3.37　别名

别名属性用于标识和定位对象，如表 114 和表 115 所示。这个属性是由客户端分配的，而别名是为了方便理解和记忆一个对象。密钥管理服务端可以指定客户端创建有效的别名的规则。客户可以通过本文件规定的机制获知这些规则。在给定的密钥管理域中，别名可能不是唯一的。

表 114　别名属性结构

对象	编码	是否必需
别名	结构	
别名值	文本串	是
别名类型	枚举，见 6.5.3.2.34	是

表 115　别名属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端
服务端可修改	是(只有当没有值时)
客户端可修改	是
客户端可删除	是
允许多实例	是
适用对象类型	所有对象

6.3.38　密钥值存在标记

密钥值存在标记属性是由服务端创建的密码对象的可选属性，如表 116 和表 117 所示。客户端不应在注册请求中指定它。如果密钥值在注册请求中的密钥块中不存在，则此属性由服务端创建。密钥值存在标记的值不能由客户端或服务端修改。密钥值存在标记属性可用作定位操作的一部分。此属性不适用于证书，公钥或不透明对象。

表 116　密钥值存在标记属性

对象	编码	是否必需
密钥值存在标记	布尔	否

表 117　密钥值存在标记属性规则

属性特征	属性规则
必须有值	否
初始化设置方	服务端
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	注册操作时
适用对象类型	对称密钥,私钥,拆分密钥,秘密数据

6.3.39　密钥值位置

密钥值位置是密钥对象的可选属性,如表 118 和表 119 所示。当注册请求中的密钥块中缺少密钥值时,此属性由客户端指定。密钥值位置用于指示注册对象中缺少密钥值的位置。此属性不适用于证书,公钥或不透明对象。

表 118　密钥值位置结构

对象	编码	是否必需
密钥值位置	结构	
密钥值位置值	文本串	是
密钥值位置类型	枚举,见 6.5.3.2.35	是

表 119　密钥值位置属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端
服务端可修改	否
客户端可修改	是
客户端可删除	是
允许多实例	是
何时隐式设置	从不
适用对象类型	对称密钥,私钥,拆分密钥,秘密数据

6.3.40 初始创建日期

初始创建日期属性包含对象最初创建的日期和时间，这个时间可能与将对象注册到密钥管理服务端的时间不同，如表 120 和表 121 所示。

由客户端注册的对象此属性是可选的。该初始创建日期可以通过客户端注册操作过程中进行设置。如果在注册操作期间客户端未设置此属性，则可以稍后通过该对象的“添加属性”操作来操作。

由于创建，创建密钥对，导出密钥，更新密钥或更新密钥对操作在服务端上是强制创建对象的，所以在这种情况下，初始创建日期应由服务端设置，并且与初始化日期属性相同。

在所有情况下，一旦创建初始创建日期，它不应被删除或更新。

表 120 初始创建日期属性

对象	编码
原创创建日期	日期-时间

表 121 初始创建日期属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端(当服务端生成对象时)
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥，创建密钥对，派生密钥，更新对称密钥，更新密钥对
适用对象类型	所有对象

6.3.41 随机数发生器

随机数发生器属性包含在创建管理密码对象的过程中使用的随机数发生器的详细信息，如表 122 和表 123 所示。由客户端注册的被管理对象此属性是可选的。该属性可以通过客户端注册操作过程中进行设置。如果客户端在注册操作期间没有设置此属性，则可以在稍后通过该对象的“添加属性”操作来进行此操作。

由于创建密钥，创建密钥对，导出密钥，更新密钥或更新密钥对操作，在服务端上是强制创建对象的。在这种情况下，随机数发生器属性应由服务端根据使用的随机数发生器设置。如果随机数发生器的具体细节未知，则 RNG 参数结构中的 RNG 算法应设置为未指定。

该随机数发生器属性不应从在密钥更新、密钥对更新操作的原始对象间复制。

在所有情况下，一旦设置了此属性，此属性将不应被删除或更新。

表 122 随机数发生器属性

对象	编码
随机数发生器	RNG 参数，见 6.2.2.18

表 123　随机数发生器属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端(当客户端生成对象并注册时)或服务端(服务端生成对象时)
服务端可修改	否
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	创建对称密钥,创建密钥对,派生密钥,更新对称密钥,更新密钥对
适用对象类型	所有密码对象

6.3.42　PKCS＃12 别名

PKCS＃12 别名属性是可选的,如表 124 和表 125 所示。如果以 PKCS＃12 密钥格式类型在注册私钥时提供,则它向服务端提供该私钥及其应在密钥材料中出现的相关证书链下的别名或别名(见 RFC7292)。如果没有提供这样的别名或别名,服务端应记录它为该密钥材料中的第一个私钥中出现的别名或别名。

当以 PKCS＃12 密钥格式类型发送获取请求时,此属性告知服务端在编码应答时应采用的别名或别名。如果此属性对于获取请求所发送的对象是空缺的,服务端宜采用别名或别名。由于 PKCS＃12 别名是在 ASN.1 中以忽略大小写的匹配规则定义的,所以客户端和服务端宜采用小写文本字符串。

表 124　PKCS＃12 别名属性

对象	编码
PKCS＃12 别名	文本串

表 125　PKCS＃12 别名属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	否
客户端可修改	是
客户端可删除	是
允许多实例	否
适用对象类型	所有密码对象

6.3.43　描述

描述属性是可选的,其内容仅用于提供信息,如表 126 和表 127 所示。它不用于策略执行。该属性

由客户端或服务端设置。

表 126　描述属性

对象	编码
描述	文本串

表 127　描述属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	是
允许多实例	否
适用对象类型	所有对象

6.3.44　备注

备注属性是可选的，其内容仅用于提供信息，如表 128 和表 129 所示。它不用于策略执行。该属性由客户端或服务端设置。

表 128　备注属性

对象	编码
备注	文本串

表 129　备注属性规则

属性特征	属性规则
必须有值	否
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	是
允许多实例	否
适用对象类型	所有对象

6.3.45　敏感

敏感属性如果为真，则服务端应禁止（通过获取操作）获取该对象值，除非将其由另一个密钥封装。

如果客户端未提供该值，服务端应将此值设置为假，如表 130 和表 131 所示。

表 130　敏感属性

对象	编码
敏感	布尔

表 131　敏感属性规则

属性特征	属性规则
必须有值	是
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	否
允许多实例	否
何时隐式设置	当对象被创建或注册时
适用对象类型	所有对象

6.3.46　始终敏感

如果敏感属性一直为真，服务端应设置始终敏感值为真；如果敏感属性曾被设置为假，则此值为假，如表 132 和表 133 所示。

表 132　始终敏感属性

对象	编码
始终敏感	布尔

表 133　始终敏感属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	是
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	敏感属性设置或改变时
适用对象类型	所有对象

6.3.47　可提取

如果为假，服务端应始终禁止(通过获取操作)获取该对象值，如表 134 和表 135 所示。如果该值不

是由客户端提供的，服务端应将该值设置为真。

表 134　可提取属性

对象	编码
可提取	布尔

表 135　可提取属性规则

属性特征	属性规则
必须有值	是
初始化设置方	客户端或服务端
服务端可修改	是
客户端可修改	是
客户端可删除	否
允许多实例	否
何时隐式设置	当对象被创建或注册时
适用对象类型	所有对象

6.3.48　从未提取

如果提取属性一直为假，服务端应将此值设置为真；如果提取曾经被设置为真，则设置此值为假，如表 136 和表 137 所示。

表 136　从未提取属性

对象	编码
从未提取	布尔

表 137　从未提取属性规则

属性特征	属性规则
必须有值	是
初始化设置方	服务端
服务端可修改	是
客户端可修改	否
客户端可删除	否
允许多实例	否
何时隐式设置	提取属性设置或改变时
适用对象类型	所有对象

6.4 操作

6.4.1 客户端到服务端的操作

6.4.1.1 概述

本条定义了密钥管理客户端可请求的操作。所有的对象管理操作都是在请求中从客户端发送到服务端的，并在从服务端到客户端的应答中获得结果。多个操作可结合在一个批处理中，结果是只有一个请求应答。

如下的操作受到被称为 ID 占位符机制的影响。

密钥管理服务应实现一个称为 ID 占位符的临时变量。此值包含一个唯一标识符。它是存储在服务端内部的一个变量，它仅当执行一个批处理操作时有效并保存。一旦批处理操作完成，该 ID 占位符就应由服务端抛弃并且(或者)使之失效，从而使后续请求不会看到这一之前的 ID 占位符有效。

ID 占位符是从创建对称密钥、创建公私钥对、注册、派生密钥、更新对称密钥、更新公私钥对、定位和恢复操作的应答中返回的唯一标识符获取的。如果这些操作的任何一个成功完成，则服务端应复制此唯一标识符到 ID 占位符变量中，将其保持直到完成批处理操作的其余操作，或批处理中的一个后续操作导致 ID 占位符被替换。如果批处理错误继续选项被设置为停止且批处理顺序选项设置为真，则批处理请求中的后续操作可通过利用 ID 占位符，省略请求载荷中的唯一标识符。

对于任何对已经存储在服务端中的管理对象进行的操作，任何被归档的对象都应首先通过恢复操作使之可用(见 6.4.1.22)，才可被使用(例如在线对象)。

多步密码算法操作(其数据流跨越从客户端到服务端的多个请求的操作)是可选地由包含相关值(见 6.2.2.15)、初始指示符(见 6.2.2.16)和完成指示符(见 6.2.2.17)请求参数的那些密码算法操作支持的。

对于多步密码算法操作，执行下列过程。

a) 在第一个请求中：
   1) 提供值为真的初始指示符；
   2) 提供其他所需参数；
   3) 保留应答中返回的相关值用于后续请求；
   4) 使用应答的数据输出(如果有)。
b) 在后续请求中：
   1) 提供来自上一个应答的相关值；
   2) 提供其他所需参数；
   3) 使用应答的下一块数据输出(如果有)。
c) 在最终请求中：
   1) 提供来自上一个应答的相关值；
   2) 提供其值为真的完成指示符；
   3) 使用应答的数据输出(如果有)。

单步密码协议操作(提供一个输入且返回一个应答的操作)执行下列过程。

a) 在请求中：
   1) 不提供初始指示符、完成指示符或相关值，或提供初始指示符、完成指示符但不提供相关值；
   2) 提供其他所需参数；

3) 使用应答的数据输出。

在密码协议执行中总是有数据参与,除非初始指示符或完成指示符为真时。

操作结果错误类型和错误处理按照附录 C。

6.4.1.2 创建对称密钥

创建对称密钥请求服务端产生新的作为管理对象的对称密钥(见 6.4.1.4),该请求包含有关所要产生对象类型的信息,以及某些分配给该对象的属性(例如:密码算法、密码长度等),如表 138 所示。

应答包含所产生对象的唯一标识符。服务端应将此操作返回的唯一标识符复制到 ID 占位符变量,如表 139 所示。

表 138 创建对称密钥请求载荷

对象	是否必需	描述
对象类型,见 6.3.4	是	决定所产生对象的类型
属性集,见 6.2.2.8	是	指定用于与新的对象关联的属性集

表 139 创建对称密钥应答载荷

对象	是否必需	描述
对象类型,见 6.3.4	是	所产生对象的类型
唯一标识符,见 6.3.2	是	新产生对象的唯一标识符
属性集,见 6.2.2.8	否	可选的对象属性列表,其值在请求中未予指定,但已经由密钥管理服务端隐含设置

表 140 指出了在采用属性集对象的创建请求中应包含的属性。

表 140 创建对称密钥属性要求

属性	要求
密码算法,见 6.3.5	是
密码用途掩码,见 6.3.16	是

6.4.1.3 创建公私钥对

创建公私钥对请求服务端生成新的公私钥对并注册两个新的密码被管理对象,该请求包含分配给该对象的属性(例如密码算法、密码长度等)。可通过在请求中指定通用对象为公私钥同时指定属性名称,如表 141 所示。

对于公私钥非通用的属性(例如名称、密码算法应用掩码)可在请求中使用私钥属性集和公钥属性集来指定,它们优先于通用属性集对象。

对于私钥,服务端应产生一个指向公钥的链接类型公钥的链接属性。对于公钥,服务端应产生一个指向私钥的链接类型私钥的链接属性。应答包含两个所产生对象的唯一标识符。ID 占位符值应设置为私钥的唯一标识符。

表 141　创建公私钥对请求载荷

对象	是否必需	描述
通用属性集	否	指定与既应用于私钥对象也应用于公钥对象的新对象关联的需要的属性集
私钥属性集	否	指定与应用于私钥对象的新对象关联的属性集。适用优先顺序
公钥属性集	否	指定与应用于公钥对象的新对象关联的属性集。适用优先顺序

对于允许多值的属性，应使用在通用、私钥和公钥属性集中出现值的联合变量，如表 142 所示。对于仅允许单值的属性，优先顺序如下：

a)　在私钥和公钥属性集中直接指定的属性；

b)　通用属性集中直接指定的属性。

如果在通用、私钥或公钥属性集中有多个属性，作为发生冲突的只允许一个值的属性的最后一个值优先。

表 142　创建公私钥对应答载荷

对象	是否必需	描述
私钥唯一标识符，见 6.3.2	是	新产生的私钥对象的唯一标识符
公钥唯一标识符，见 6.3.2	是	新产生的公钥对象的唯一标识符
私钥属性集，见 6.2.2.8	否	可选的私钥对象属性列表，其值在请求中未予指定，但已经由密钥管理服务端隐含设置
公钥属性集，见 6.2.2.8	否	可选的公钥对象属性列表，其值在请求中未予指定，但已经由密钥管理服务端隐含设置

表 143 表明哪些属性应包含在使用属性集对象的创建公私钥对请求中，以及对于私钥和公钥哪些属性应具有相同值。

表 143　创建公私钥对属性要求

属性	是否必需	对于私钥和公钥应有相同的值
密码算法，见 6.3.5	是	是
密钥长度，见 6.3.6	否	是
密码用途掩码，见 6.3.16	是	否
密码算法域参数，见 6.3.8	否	是
密码参数，见 6.3.7	否	是

6.4.1.4　注册

注册请求服务端注册一个由客户端生成的或通过其他方法获取的被管理对象，让服务端来管理该对象。请求中参数与创建操作类似，但包含了由服务端存储的对象本身。该请求包含了有关所要注册对象类型的信息，以及分配给该对象的属性（例如，密码算法、密码算法长度等）。这些信息应通过使用

属性集对象来指定，如表 144 所示。

应答包含由服务端分配给所注册对象的唯一标识符。服务端应复制通过此操作返回的唯一标识符到 ID 占位符变量。该对象的初始日期属性应设置为当前时间，如表 145 所示。

表 144　注册请求载荷

对象	是否必需	描述
对象类型，见 6.3.4	是	决定所要注册对象的类型
属性集，见 6.2.2.8	是	指定用于与新的对象关联的属性集
证书、对称密钥、私钥、公钥、拆分密钥、秘密数据或不透明对象，见 6.2.2.22	是	所要注册的对象，对象及属性可包封

表 145　注册响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	新注册对象的唯一标识符
属性集，见 6.2.2.8	否	可选的对象属性列表，其值在请求中未予指定，但已经由密钥管理服务端隐含设置

如果要注册被管理对象，则注册请求中应直接或通过属性集中包含的属性如表 146 所示。

表 146　注册属性要求

属性	是否必需
密码算法，见 6.3.5	是，仅当此信息已经封装在密钥块中时可省略。不适用于私钥。如果存在，则下面的密码算法长度也应存在
密钥长度，见 6.3.6	是，仅当此信息已经封装在密钥块中时可省略。不适用于秘密数据。如果存在，则上面的密码算法也应存在
证书长度，见 6.3.10	是，仅用于证书
密码用途掩码，见 6.3.16	是
数字签名算法，见 6.3.14	是，仅当此信息封装在证书对象中时可省略。只适用于证书

6.4.1.5　更新对称密钥

此请求用于对现有对称密钥生成替换密钥。它类似于创建操作，除替换密钥的属性是从现有密钥复制而来以外，其例外是 6.3.41 的随机数发生器中所列属性。由于替换密钥占用了现有密钥的名称属性，对给定密钥宜仅执行一次密钥更新。更新对称密钥请求载荷，如表 149 所示。

服务端应将为此操作返回的替换密钥的唯一标识符复制到 ID 占位符变量。对于现有密钥，服务端应生成一个指向替换密钥的链接类型替换对象的链接属性。对于替换密钥，服务端应生成一个指向现有密钥的链接类型替换密钥的链接属性。更新对称密钥响应载荷，如表 150 所示。

可使用一个偏移量来表示替换密钥的初始化日期与激活日期之差。如果没有指定偏移量，就从现

有密钥复制激活日期、生效日期、失效日期和停用日期值。如果设置了偏移量，且存在现有密钥的各个日期，则替换密钥的各个日期基于现有密钥的日期设置，如表147所示。

表147　更新对称密钥时通过偏移量计算新日期

现有密钥中的属性	替换密钥中的属性
初始日期(IT1)	初始日期(IT2)＞IT1
激活日期（AT1）	激活日期(AT2)＝IT2＋Offset
生效日期（CT1）	生效日期＝CT1＋(AT2－AT1)
失效日期（TT1）	失效日期＝TT1＋(AT2－AT1)
停用日期(DT1)	停用日期＝DT1＋(AT2－AT1)

当生成替换密钥时需要专门处理的属性如表148所示。

表148　更新对称密钥属性要求

属性	处理
初始日期，见6.3.20	设置为当前时间
销毁日期，见6.3.25	不设置
失信发生日期，见6.3.26	不设置
失信日期，见6.3.27	不设置
注销原因，见6.3.28	不设置
唯一标识符，见6.3.2	生成新值
使用限制，见6.3.18	该值从现有密钥总数值复制，并将现有密钥的计数值设置为总数值
名称，见6.3.3	设置为现有密钥的名称；所有名称属性从现有密钥中清除
状态，见6.3.19	基于属性值设置日期，如表147所示
摘要，见6.3.15	依替换密钥值重新计算
链接，见6.3.32	设置指向作为替换密钥的现有密钥
最后修改时间，见6.3.35	设置为当前时间
随机数发生器，见6.3.41	设置为生成新管理对象所用的随机数发生器。不从原对象中复制

表149　更新对称密钥请求载荷

对象	是否必需	描述
唯一标识符，6.3.2	否	确定被重置密钥的现有对称密钥。如果省略，则ID占位符值被服务端用作唯一标识符
偏移量	否	一个时间间隔对象，用来表示所要生成的替换密钥的初始化日期与生效日期之差
属性集，见6.2.2.8	否	指定对象属性需使用独立属性集

表 150　更新对称密钥响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	新生成的替换对称密钥的唯一标识符
属性集，见 6.2.2.8	否	可选的对象属性列表，其值在请求中未予指定，但已经由密钥管理服务端隐含设置

6.4.1.6　更新公私钥对

该请求用于为现有公私钥对生成替换密钥对。它类似于创建公私钥对操作，只是替换密钥对的属性中除了 6.3.41 随机数产生中列举的属性以外都是从现有密钥对复制过来。由于替换密钥对占用了现有公私钥对的名称属性，对给定密钥对宜仅执行一次公私钥更新。更新密钥对请求载荷如表 153 所示。

对于现有的公钥和私钥，服务端应分别创建指向替换公钥和私钥的链接类型来替换密钥的链接属性。对于替换公钥和私钥，服务端应分别创建指向现有公钥和私钥的链接类型来替换密钥的链接属性。服务端应将此操作返回的替换私钥的私钥唯一标识符复制到 ID 占位符变量中。更新密钥对响应载荷如表 154 所示。

可使用偏移量来表示替换密钥对初始化日期和激活日期之间的差别。如果没有特别注明偏移量，激活日期和停用日期从现有密钥对复制。如果设置了偏移量并且现有密钥对也有相应的日期存在，则替换密钥对的日期应基于现有密钥对的日期按如表 151 所示方式设置。

表 151　根据偏移量计算更新密钥对的新日期

现有密钥对属性	替换密钥对属性
初始日期（IT1）	初始日期(IT2)＞IT1
激活日期(AT1)	激活日期(AT2)＝IT2＋Offset
停用日期(DT1)	停用日期(DT2)＝DT1＋(AT2－AT1)

替换密钥对的属性，不是从现有的密钥对复制，而是以特定的方式处理的，如表 152 所示。

表 152　更新密钥对属性需求

属性	动作
私钥唯一标识符，见 6.3.2	生成新值
公钥唯一标识符，见 6.3.2	生成新值
名称，见 6.3.3	设置为现有公钥/私钥的名称；删除现有公钥/私钥的所有名称属性
摘要，见 6.3.15	从新的公私钥重新计算替换公钥和私钥
使用限制，见 6.3.18	总字节数/总对象值从现有密钥对中复制，而字节数/对象计数值设置为总字节数/总对象数
状态，见 6.3.19	根据属性值(如日期)进行设置
初始日期，见 6.3.20	设置为当前时间
销毁日期，见 6.3.25	没有设置

表 152　更新密钥对属性需求（续）

属性	动作
失信发生日期，见 6.3.26	没有设置
失信日期，见 6.3.27	没有设置
注销原因，见 6.3.28	没有设置
链接，见 6.3.32	设置为指定现有的公/私钥作为已更换的公钥/私钥
最后更改日期，见 6.3.35	设置为当前时间
随机数发生器，见 6.3.41	设置为用于创建新管理对象的随机数发生器。不从原始对象复制

表 153　更新密钥对请求载荷

对象	是否必需	描述
私钥唯一标识符，见 6.3.2	否	确定要更新密钥的现有非对称密钥对。如果省略，则 ID 占位符被服务端替代
偏移量	否	代表要创建的替换密钥对的初始化日期和激活日期之间的差异的间隔对象
通用属性集，见 6.2.2.8	否	在适用于公私钥对象的各个属性中指定所需的属性
私钥属性集，见 6.2.2.8	否	代表应用于私钥对象的属性。优先级顺序应用
公钥属性集，见 6.2.2.8	否	代表与应用于公钥对象的属性。优先级顺序应用

表 154　更新密钥对响应载荷

对象	是否必需	描述
私钥唯一标识符，见 6.3.2	是	新创建的替换私钥对象的唯一标识符
公钥唯一标识符，见 6.3.2	是	新创建的替换公钥对象的唯一标识符
私钥属性集，见 6.2.2.8	否	可选的私钥对象属性列表，其值在请求中未予指定，但已经由密钥管理服务端隐含设置
公钥属性集，见 6.2.2.8	否	可选的公钥对象属性列表，其值在请求中未予指定，但已经由密钥管理服务端隐含设置

对于多实例属性，使用在通用、私钥和公钥属性集中的属性值的联合。对于单实例属性，优先级顺序如下：

a）　在私钥和公钥属性集中显式指出的属性；

b）　在通用属性集中显式指出。

如果公共、私有或公钥属性集中有多个模板，那么单实例属性的后续值将优先。

6.4.1.7　派生密钥

该请求用于从密钥管理服务端已知的密钥或秘密数据对象中，派生出对称密钥或秘密数据对象。该请求应仅适用于被管理的密码对象，此密码对象在指定管理对象的密码使用掩码属性中包含了其派

生密钥位(即,能够用于密钥派生)。若对一个未包含此位的对象进行操作,则服务端应返回错误。派生密钥请求载荷,如表 155 所示。

请求中的字段指定了用于派生的密钥或秘密数据对象的唯一标识符(例如有的派生方法可使用多个密钥或秘密数据对象来派生出结果)、用于派生的方法、指定方法所需的任何参数。方法作为枚举变量指定。目前定义的派生方法包括:

——PBKDF2,此方法用于从密码或密码短语中派生对称密钥,PBKDF2 方法在[PKCS＃5]和[RFC2898]中发布;

——HASH,该方法通过计算派生密钥或派生数据上的杂凑来获得密钥;

——HMAC,该方法通过在派生数据上计算 HMAC 来获得密钥;

——ENCRYPT,此方法通过加密派生数据来获取密钥;

——扩展。

服务端应执行派生函数,然后将派生对象注册为新的被管理对象,为响应中的新对象返回新的唯一标识符。服务端应将此操作返回的唯一标识符复制到 ID 占位符变量中。

对于由密钥和秘密数据派生得到的密钥和秘密数据对象,服务端应创建一个链接类型派生密钥的链接属性,指向由本操作派生得到的对称密钥或秘密数据对象。对于由本操作派生得到的对称密钥或秘密数据对象,服务端应创建一个链接类型派生基础对象的链接属性,指向由密钥或秘密数据对象派生得到的密钥或秘密数据对象。派生密钥响应载荷,如表 156 所示。

表 155　派生密钥请求载荷

对象	是否必需	描述
对象类型,见 6.3.4	是	确定要创建的对象的类型
唯一标识符,见 6.3.2	是,可重复	确定要用于派生新密钥的对象或对象集。在此操作中,ID 占位符的当前值不能用于代替唯一标识符
派生方法,见 6.5.3.2.21	是	用于导出新密钥的方法的枚举对象
派生参数,见下文	是	包含指定派生方法所需参数的结构对象
属性集,见 6.2.2.8	是	使用单个属性指定与新对象关联的所需属性集;长度和算法总是被指定用于创建对称密钥

表 156　派生密钥响应载荷

对象	是否必需	描述
唯一标识符,见 6.3.2	是	新派生的密钥或秘密数据对象的唯一标识符
属性集,见 6.2.2.8	否	可选的对象属性列表,其值在请求中未予指定,但已经由密钥管理服务端隐含设置

除了 PBKDF2 增加了 2 个另外的参数项,其余派生方法的派生参数包含的参数项如表 157 所示。

表 157　派生参数结构(PBKDF2 除外)

对象	编码	是否必需
派生参数	结构	是
密码参数,见 6.3.7	结构	是,除了 HMAC 派生密钥
初始向量	字节字符串	否,取决于 PRF 和操作模式:若未提供此项则设 IV 值为空
派生数据	字节字符串	是,除非提供了秘密数据对象的唯一标识符

若使用杂凑派生方法来派生密钥，则客户端需在密码参数中指明杂凑算法；同理，若使用 GB/T 32907 中定义的 SM4 密码算法来派生密钥，则客户端需指明分组密码加密模式。服务端应核验指定模式匹配相应密钥的密码参数集中的一个实例。若省略了密码参数，则服务端应通过指定密钥的最小属性索引来选择密码参数。若对应密钥不含任何密码参数属性，或无任何匹配项，则返回错误。

派生数据是用于加密、杂凑或 HMAC 的明文数据。

派生数据可由客户端通过派生数据域来显式地提供，或通过提供密码数据对象的唯一标识符来隐式地提供。若两种均已提供，则应返回错误。

PBKDF2 派生方法增加了另外 2 个参数，如表 158 所示。

表 158　PBKDF2 派生参数结构

对象	编码	是否必需
派生参数	结构	是
密码参数，见 6.3.7	结构	是，除了 HMAC 派生密钥
初始向量	字节字符串	否，取决于 PRF 和操作模式：若未提供此项则设 IV 值为空
派生数据	字节字符串	是，除非提供了秘密数据对象的唯一标识符
盐	字节字符串	是
迭代次数	整型	是

6.4.1.8　定位

此操作请求服务端根据请求中指定的属性搜索一个或多个被管理对象。在请求中不宜指定属性索引值。提供的属性索引值应被服务端忽略。此请求可包含一个最大项域，此域指定了需返回对象的最大数量。若最大项域已忽略，则服务端可返回所有匹配的对象，或因资源有限而设置内部最大限制值。此请求可包含一个偏移项域，此域指定了需跳过的对象数量，以满足请求设定的鉴别标准。偏移项为 0 时则等同于忽略此偏移项域。若请求中同时指定了偏移项和最大数量项，则服务端跳过偏移项并返回最大项的对象。

若不止一个对象满足请求中的鉴别标准，则返回可包括不同管理对象的唯一标识符。返回的对象应匹配请求中所有的属性。若无对象匹配，则返回空的载荷。若请求未指定任何属性，所有对象都应被视为匹配定位请求。响应可包含定位项，此项为满足鉴别标准的对象数量。

服务端返回一列已发现对象的唯一标识符，可使用获取操作来取回。若对象已被归档，则恢复和获取操作是需使用的以得到这些对象。若返回给客户端一个唯一标识符，则服务端应将此操作返回的唯一标识符复制给 ID 占位符变量。若定位操作匹配不止一个对象，且最大项的值被请求所忽略，或被设为大于 1 的某个值，则服务端应清空 ID 占位符，使得后续与定位有关联，且并未明确指定唯一标识符的操作都失败。这样确保了这些操作应仅当定位操作返回单个对象时才可执行。

定位请求中的数据属性（初始数据、激活数据等）用于指定定位的时间或时间范围。若请求中使用了给定数据属性的单个实例，则具有相同数据属性的对象被认为是匹配的候补对象。若使用了相同数据属性的 2 个实例（具有 2 个不同值来指定范围），则对于数据属性在一定范围内的对象，被认为是匹配的候补对象。若数据属性被设定为其可能的最大值，则它等价于一个未定义的属性。

当请求中指定了密码使用掩码属性时，候选对象将通过请求掩码和候选对象掩码进行逻辑与操作，其结果与请求掩码进行比较。

当请求中指定了使用限制属性时，匹配候选对象应具有使用限制次数和使用限制总数，其中使用限制总数与请求中指定的值一致或比请求中指定的值更大。

当请求中指定了对象组属性和对象组成员标识，且对象组成员的指定值为“组成员未使用”时，匹配候选对象应在对象组中为未使用对象(见 6.3.31)。若组中不含更多的未使用对象时，服务端可基于服务端策略选择产生一个新的备用对象。若对象组成员的指定值为“组成员缺省”，则服务端根据服务端策略定位此缺省对象。

定位请求载荷与响应载荷，分别如表 159 和表 160 所示。

存储状态掩码字段(见 6.5.3.3.2)用于指明定位哪种对象：在线对象和/或存档对象。

表 159　定位请求载荷

对象	是否必需	描述
最大项目数量	否	代表服务端可能返回的对象标识符的最大数量的整数对象
偏移项目数量	否	代表可跳过的满足请求中指定的标识条件的对象标识符数量
存储状态掩码，见 6.5.3.3.2	否	一个整数对象(用作位掩码)，用于代表是否只是在线对象，仅归档对象或同时在线和归档对象。如果省略，则仅假定为在线
对象组成员，见 6.5.3.2.33	否	代表对象组成员类型的枚举对象
属性，见 6.3	否，可重复	指定一个属性及其所需的值，以匹配候选对象中的属性(根据上面定义的匹配规则)

表 160　定位响应载荷

对象	是否必需	描述
定位项目	否	指示满足请求中指定的标识条件的对象标识符数量的整数对象。 如果服务端不能或不愿意确定匹配的项目的总计数，则可选择从响应中省略该值。 即使请求中不存在偏移项，服务端也可选择返回“已定位项”值
唯一标识符，见 6.3.2	否，可重复	定位对象的唯一标识符

6.4.1.9　检查

此操作请求服务端根据请求中指定的值检查被管理对象的使用情况。此操作宜仅在放置在一组批处理操作中时使用，通常在定位、创建对称密钥、创建公私钥对、派生密钥、更新密钥或更新密钥对操作之后执行，该操作之后执行获取操作。

如果服务端根据指定的属性确定允许客户端使用该对象，则服务端将返回对象的唯一标识符。

如果服务端根据指定的属性确定客户端不准许使用对象，则服务端将清空 ID 占位符，并且不返回唯一标识符，并且该操作返回请求中指定的导致服务端策略拒绝的属性集。只应返回导致服务端确定客户端不准许使用对象的属性，以便客户端确定如何处理。

在包括检查操作的批处理操作中宜设置批处理顺序选项为真。在这种类型的批处理中客户端宜只能使用停止和撤销批处理错误的配置选项值。请求中可指定额外属性限制如下。

——使用限制(见 6.3.18)请求中可包括客户端认为有必要完成其所需功能的使用数量。这并不要求后续的获取使用分配操作请求该数量。这仅仅意味着客户端在确保所指定数量是可用的。

——密码用途掩码，用来指定客户端打算使用于对象的密码操作。这允许服务端确定策略是否允许客户端在对象上执行这些操作。

租约时间—指定需要的租借时间(见 6.3.17)。客户端可使用该值确定服务端是否允许客户端按照

指定租约时间或更长时间使用对象。在检查操作中包括该值并不会实际上导致服务端批准该租约，而仅仅意味着如果被后续的批处理化的获取租约操作请求的话，所请求的该租约时间可被批准。

检查请求载荷与相应载荷，分别如表 161 和表 162 所示。

表 161　检查请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定被检查的对象。如果忽略，服务端采用 ID 占位符的值作为唯一标识符
使用限制，见 6.3.18	否	指定被用来对照检查服务端策略的被保护的使用限制单元的数量
密码用途掩码，见 6.3.16	否	指定客户端打算使用于对象的密码操作
租约时间，见 6.3.17	否	指定客户端要求服务端保证服务端策略有效的租约时间值

表 162　检查响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是，除非失败请求	对象的唯一标识符
使用限制，见 6.3.18	否	如果请求内容中指定的使用限制值大于服务端策略允许值，由服务端返回
密码用途掩码，见 6.3.16	否	如果请求内容中指定的密码用途掩码由于违反策略被服务端拒绝，由服务端返回
租约时间，见 6.3.17	否	如果请求内容中指定的租约时间值大于服务端可能批准的有效租约时间，由服务端返回

6.4.1.10　获取

此操作请求服务端返回由其唯一标识符指定的被管理对象。响应包含对象的唯一标识符以及对象本身，可使用请求中指定的封装密钥来进行封装。获取请求载荷与响应载荷，分别如表 163 和表 164 所示。

下面的密钥格式要求应由客户端指定；当客户端请求服务端以特定格式返回一个对象时限制措施生效：

——如果客户端以指定格式注册一个密钥，服务端应能够在获取操作中以密钥注册时的相同格式返回密钥；

——服务端可支持任何其他格式转换。

表 163　获取请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定要请求的对象。如果省略，则 ID 占位符值由服务端用作唯一标识符
密钥格式类型，见 6.5.3.2.3	否	确定要返回的密钥格式类型
密钥封装类型，见 6.5.3.2.3	否	确定返回密钥值的密钥封装类型
密钥压缩类型，见 6.5.3.2.2	否	确定椭圆曲线公钥的压缩方法
密钥封装规格，见 6.2.2.6	否	指定用于封装返回的对象的密钥和其他信息

表 164　获取响应载荷

对象	是否必需	描述
对象类型，见 6.3.4	是	对象的类型
唯一标识符，见 6.3.2	是	对象的唯一标识符
证书，对称密钥，私钥，公钥，拆分密钥，秘密数据或不透明对象，见 6.2.2.22	是	返回的对象

6.4.1.11　获取属性

此操作请求与被管理对象的一个或多个属性相关联。该对象由其唯一标识符指定，属性由请求中的名称指定。如果指定的属性具有多个实例，则返回所有实例。如果指定的属性不存在（即没有值），则不应在返回的响应中出现。如果请求的属性不存在，则响应应仅由唯一标识符组成。如果在请求中没有指定属性名称，则所有属性应被视为与获取属性请求相匹配。相同的属性名称在请求中出现的次数不应多于一次。获取属性请求载荷与响应载荷，分别如表 165 和表 166 所示。

表 165　获取属性请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定正在请求其属性的对象。如果省略，则 ID 占位符值由服务端用作唯一标识符
属性，见 6.2.2.1	否，可重复	指定与对象关联的属性的名称

表 166　获取属性响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符
属性，见 6.2.2.1	否，可重复	与该对象关联的请求属性

6.4.1.12　获取属性列表

此操作请求与被管理对象相关联的属性名称列表。该对象由其唯一标识符指定。获取属性列表请求载荷与响应载荷，分别如表 167 和表 168 所示。

表 167　获取属性列表请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定正在请求其属性名称的对象。如果省略，则 ID 占位符值由服务端用作唯一标识符

表 168　获取属性列表响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符
属性，见 6.2.2.1	是，可重复	与对象关联的可用属性的名称

6.4.1.13 添加属性

此操作请求服务端添加与被管理对象关联的新属性实例并设置其值。请求包含属性所属的被管理对象的唯一标识符,以及属性名称和值。单实例时,此为如何创建属性的值。多实例时,此为如何创建属性的第一个和后续的值。现有属性值应只能通过修改属性操作进行更改。只读属性不应使用添加属性操作添加。属性索引不应在请求中指定。响应返回一个新的属性索引,如果添加的属性实例的索引为0,则可省略属性索引。多个添加属性请求可包含在单个批处理请求中用来添加多个属性。添加属性请求载荷与响应载荷,分别如表169和表170所示。

表169 添加属性请求载荷

对象	是否必需	描述
唯一标识符,见6.3.2	否	对象的唯一标识符。如果省略,则ID占位符值由服务端用作唯一标识符
属性,见6.2.2.1	是	指定要作为对象的属性添加的属性

表170 添加属性响应载荷

对象	是否必需	描述
唯一标识符,见6.3.2	是	对象的唯一标识符
属性,见6.2.2.1	是	与对象关联的添加属性

6.4.1.14 修改属性

此操作请求服务端修改与被管理对象相关联的现有属性实例的值。请求载荷包含要修改属性的被管理对象的唯一标识符,属性名称,可选属性索引和新值。如果在请求中没有指定属性索引,则属性索引设定为0。只有现有的属性可以通过此操作进行更改。新属性应通过添加属性操作添加。只有指向的属性实例值应被修改。如索引值指向不存在的属性对象时应返回一个错误。响应载荷返回修改后的属性(新值)和属性索引(如果为0可省略)。多条修改请求可以合并成一个批处理请求修改多个属性值。修改属性操作的请求载荷与响应载荷,分别如表171和表172所示。

表171 修改属性请求载荷

对象	是否必需	描述
唯一标识符,见6.3.2	否	对象的唯一标识符。如果省略,则服务端将ID的占位符值用作唯一标识符
属性,见6.2.2.1	是	与对象关联要修改的属性

表172 修改属性响应载荷

对象	是否必需	描述
唯一标识符,见6.3.2	是	对象的唯一标识符
属性,见6.2.2.1	是	与对象关联的修改后的属性

6.4.1.15 删除属性

此操作请求服务端删除与被管理对象相关联的属性。请求载荷包含要删除其属性的被管理对象的唯一标识符,属性名称和可选属性索引。如果在请求中没有指定属性索引,则属性索引设定为0。必须赋值的属性不应被此操作删除。尝试删除不存在的属性或索引值指向不存在的属性对象时应返回一个错误。响应载荷返回被删除的属性和属性索引(如果为0可省略)。多条删除请求可合并成一个批处理请求删除多个属性值。删除属性操作的请求载荷与响应载荷,分别如表173和表174所示。

表173 删除属性请求载荷

对象	是否必需	描述
唯一标识符,见6.3.2	否	确定其属性被删除的对象。如果省略,服务端用ID占位符值作唯一标识符
属性,见6.2.2.1	是	与对象关联的要删除的属性名称
属性索引,见6.2.2.1	否	要删除的属性索引

表174 删除属性响应载荷

对象	是否必需	描述
唯一标识符,见6.3.2	是	对象的唯一标识符
属性,见6.2.2.1	是	与对象关联的已删除属性

6.4.1.16 获取租约

此操作请求服务端为指定的被管理对象获取新的租约期。租约期是一个区间值,用于确定客户端内关于该对象的内部缓存到期并更新的间隔值。如果租约期的返回值为0,则服务端设定租约间隔无效,客户端可不受任何租期限制使用该对象。如果客户端的租期到期,则客户端不应使用相关的密码对象,直到获取新的租约。如果服务端设定不应为指定的密码对象发出新的租约,那么服务端对获取此租约请求响应一个错误。

操作的响应载荷包含对象的最后更改日期属性的当前值。客户端可通过比较先前获取属性的时间来确定客户端缓存的属性是否需要刷新。

获取租约操作的请求载荷与响应载荷,分别如表175和表176所示。

表175 获取租约请求载荷

对象	是否必需	描述
唯一标识符,见6.3.2	否	确定获得租约的对象。如果省略,服务端用ID占位符值作唯一标识符

表176 获取租约响应载荷

对象	是否必需	描述
唯一标识符,见6.3.2	是	对象的唯一标识符
租约时间,见6.3.17	是	确定在需要获得新租约之前可以使用对象的时间量(以秒为单位)
最后更改日期,见6.3.35	是	对指定对象的任何属性进行最新更改的日期和时间

6.4.1.17 获取使用配额

此操作请求服务端从当前使用限制值获取配额，允许客户端使用被管理对象来执行密码保护。该配额仅适用于能够用于应用保护的被管理对象(例如用于加密的对称密钥，用于签名的私钥等)，并且仅当被管理对象具有使用限制属性时才有效。用于处理加密保护信息(例如解密，验证等)的用途不受限制，不能分配。客户端除非已获取使用配额，否则不能使用具有使用限制属性的被管理对象进行密码保护。只有在被管理对象启用保护的时间内(即在激活日期之后和失效日期之前)，才需要请求配额的操作。如果对无使用限制属性的对象请求操作，或者对不是可以应用密码保护的对象请求操作，则服务端应返回错误。

请求的字段指定了客户端需要保护的次数。如果请求的次数不可用或者被管理对象此时不能用于密码保护，服务端应返回错误。服务端应假设配额数量会使用完。当配额数量使用完后，客户端不应继续使用被管理对象进行密码保护除非得到新配额。

获取使用配额操作的请求载荷与响应载荷，分别如表 177 和表 178 所示。

表 177 获取使用配额请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定正在请求使用分配的对象。如果省略，服务器端用 ID 占位符值作唯一标识符
使用限制计数，见 6.3.18 中的使用限制计数字段	是	要保护的使用限制单位数

表 178 获取使用配额响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符

6.4.1.18 激活

此操作请求服务端激活被管理对象。该操作只应在“预激活”状态的对象上执行，将其状态更改为“激活”，并将其激活日期设置为当前日期和时间。激活操作的请求载荷与响应载荷，分别如表 179 和表 180 所示。

表 179 激活请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定被激活的对象。如果省略，如果省略，服务端用 ID 占位符值作唯一标识符

表 180 激活响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符

6.4.1.19 注销

此操作请求服务端注销被管理对象或不透明对象。请求包含注销的原因(例如“密钥失信”,“终止操作”等)。发出该请求前应进行鉴别和授权校验。只有对象所有者或获得安全授权的操作员才可发出此请求。该操作产生两种结果。如果注销原因是密钥失信或CA失信,则将对象置为“失信”状态,日期设置为当前日期和时间。如果请求中有“失信发生日期”则直接赋值,如果请求中未提供,则将“失信发生日期”设置为对象的初始日期。如果注销原因既不是密钥失信也不是CA失信,则将对象置于“停用”状态,并且将“停用日期”设置为当前日期和时间。注销操作的请求载荷与响应载荷,分别如表181和表182所示。

表181 注销请求载荷

对象	是否必需	描述
唯一标识符,见6.3.2	否	确定被注销的对象。如果省略,服务器端用ID占位符值作唯一标识符
注销原因,见6.3.28	是	注销的原因
失信发生日期,见6.3.26	否	仅用于注销原因是“密钥失信”或“CA失信”,不适用于其他注销原因

表182 注销响应载荷

对象	是否必需	描述
唯一标识符,见6.3.2	是	对象的唯一标识符

6.4.1.20 销毁

此操作用于向服务端表示销毁指定被管理对象的密钥材料。密钥材料的元数据可由服务器端保留(例如,用于确保过期或注销的签名私钥不再可用)。发出该请求前应进行鉴别和授权校验。只有对象所有者或获得安全授权的操作员才可发出此请求。密码对象只在“预激活”和“停用”状态下可被销毁。

销毁操作的请求载荷与响应载荷,分别如表183和表184所示。

表183 销毁请求载荷

对象	是否必需	描述
唯一标识符,见6.3.2	没有	确定被销毁的对象。如果省略,服务器端用ID占位符值作唯一标识符

表184 销毁响应载荷

对象	是否必需	描述
唯一标识符,见6.3.2	是	对象的唯一标识符

6.4.1.21 归档

此操作用于指定被管理对象可以归档。对象归档的实际时间，归档的位置或归档的级别由密钥管理服务端中的策略确定，不由客户端指定。请求包含被管理对象的唯一标识符。发出该请求前应进行鉴别和授权校验。只有对象所有者或获得安全授权的操作员才可发出此请求。归档请求只是一个客户端意向，密钥管理服务端才能实施对象的归档。

归档操作的请求载荷与响应载荷，分别如表 185 和表 186 所示。

表 185 归档请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定要归档的对象。如果省略，服务器端用 ID 占位符值作唯一标识符

表 186 归档响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符

6.4.1.22 恢复

此操作将对已归档的被管理对象执行恢复操作。这个请求可能需要异步轮询获得响应，因为已归档对象恢复时会导致延迟。一旦获得响应，被管理对象就立即上线，可被获得（例如，执行一个获取操作）。发出该请求前应进行鉴别和授权校验。恢复操作的请求载荷与响应载荷，分别如表 187 和表 188 所示。

表 187 恢复请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	没有	确定正在恢复的对象。如果省略，服务器端用 ID 占位符值作唯一标识符

表 188 恢复响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符

6.4.1.23 验证证书

此操作请求服务端验证证书链，并返回其有效性信息。每个请求中只包含单个证书链。在服务端支持此操作是可选的。如果服务端不支持此操作，则返回错误。请求可包含一个证书对象列表，以及（或者）指向被管理证书对象的唯一标识符的列表。两个列表组成一个可验证的证书链。请求也可包含一个数据表示证书链中所有的证书都需要验证有效性。有效性验证的方式取决于服务端和协议的需求。与之类似，信任根和证书链的验证顺序也由服务端决定。

验证证书的请求载荷与响应载荷，分别如表 189 和表 190 所示。

表 189　验证证书请求载荷

对象	是否必需	描述
证书，见 6.2.2.1	否，可重复	一个或多个证书
唯一标识符，见 6.3.2	否，可重复	一个或多个证书对象的唯一标识符
有效期	否	证书链有效的日期-时间对象，如果省略，设定为当前日期-时间

表 190　验证证书响应载荷

对象	是否必需	描述
有效性标识，见 6.5.3.2.23	是	一个枚举对象，标识证书链有效、非法或者未知

6.4.1.24　查询

该操作用于客户端向服务端查询其功能和协议机制。该查询操作开放给未鉴别客户端调用。请求中的查询功能字段应包含以下一个或多个项目：

——查询操作，
——查询对象，
——查询服务端信息，
——查询应用程序命名空间，
——查询扩展列表，
——查询扩展映射，
——查询证明类型，
——查询 RNG(随机数发生器)，
——查询验证，
——查询配置文件，
——查询功能，
——查询客户端注册方法。

如果没有任何值要返回则响应载荷为空。

查询操作的请求载荷与响应载荷，分别如表 191 和表 192 所示。

表 191　查询请求载荷

对象	是否必需	描述
查询功能，见 6.5.3.2.24	是，可重复	确定要查询的信息

表 192　查询响应载荷

对象	是否必需	描述
操作，见 6.5.3.2.27	否，可重复	服务端支持的操作
对象类型，见 6.3.4	否，可重复	服务端支持的被管理对象类型

表 192　查询响应载荷（续）

对象	是否必需	描述
供应商标识	否	如果请求查询服务端信息，则返回。供应商标识应该是唯一标识供应商的文本字符串
服务端信息	否	包含客户端可能感兴趣的特定供应商的信息
应用程序命名空间，见 6.3.33	否，可重复	服务端支持的应用程序命名空间
扩展信息，见 6.2.2.9	否，可重复	如果服务端请求并支持查询扩展列表或查询扩展映射，则应返回
证明类型，见 6.5.3.2.36	否，可重复	服务端支持的证明类型
RNG 参数，见 6.2.2.18	否，可重复	服务端支持的 RNG
配置文件信息，见 6.2.2.19	否，可重复	服务端支持的配置文件
验证信息，见 6.2.2.20	否，可重复	服务端支持的验证
性能信息，见 6.2.2.21	否，可重复	服务端支持的性能
客户注册方法，见 6.5.3.2.45	否，可重复	服务端支持的客户端注册方法

6.4.1.25　版本查询

此操作用于客户端确定服务端支持的协议版本列表。请求中包含客户端支持的协议版本的可选列表。协议版本按照优先级顺序排列。

响应中包含服务端支持的协议版本列表。协议版本按优先级顺序排列。如果在请求中客户端向服务端提供支持的协议版本列表，则服务端应仅返回客户端和服务端都支持的协议版本。服务端应列出客户端和服务端都支持的所有协议版本。

如果在请求头中指定的协议版本未在请求载荷中指定，并且服务端不支持请求载荷指定的协议版本，则服务端应在响应返回一个空列表。如果在请求载荷中未指定协议版本，服务端应返回服务端支持的所有协议版本。

版本查询操作的请求载荷与响应载荷，分别如表 193 和表 194 所示。

表 193　版本查询请求载荷

对象	是否必需	描述
协议版本，见 6.5.1.1	否，可重复	客户端支持的协议版本列表，以优先级顺序排列

表 194　版本查询响应载荷

对象	是否必需	描述
协议版本，见 6.5.1.1	否，可重复	服务端支持的协议版本列表，以优先级顺序排列

6.4.1.26　取消

此操作请求服务端取消未完成的异步操作。请求中应指定原始操作的相关值（见 6.5.1.8）。服务端应返回以下值之一的“取消结果”作为响应：

已取消——取消操作成功；

无法取消——取消操作无法进行；
动作已完成——在取消之前，原始操作已完成；
动作已失败——在取消之前，原始操作已失败；
不可用——指定的相关值与最近待处理或完成的异步操作不匹配。
对此操作的响应不能是异步的。
取消操作的请求载荷与响应载荷，分别如表 195 和表 196 所示。

表 195　取消请求载荷

对象	是否必需	描述
异步相关值，见 6.5.1.8	是	要取消的请求

表 196　取消响应载荷

对象	是否必需	描述
异步相关值，见 6.5.1.8	是	在请求中指定
取消结果，见 6.5.3.2.25	是	枚举表示取消结果

6.4.1.27　轮询

此操作用于向服务端轮询获得未完成异步操作的状态。请求中应指定原始操作的相关值（见 6.5.1.8）。对此操作的响应不能是异步的。轮询操作的请求载荷，如表 197 所示。

表 197　轮询请求载荷

对象	是否必需	描述
异步相关值，见 6.5.1.8	是	指定要轮询的请求

服务端应返回的响应为两者之一：
——如果操作未完成，响应不包含载荷和一个“挂起中”的结果状态；
——如果操作已完成，响应包含相应的载荷。如果操作同步完成响应显示应与已完成一致。

6.4.1.28　加密

此操作请求服务端用被管理对象作为加密密钥对提供的数据执行加密操作。此操作是可选操作。

请求包含密码参数信息（加密模式和补齐方式），待加密的数据，用到的 IV/计数器/随机值。密码参数可省略，在被管理的密码对象相关属性中指定。如果密码参数指定服务端可以产生随机的 IV 提供给客户端或者加密算法不需要 IV/计数器/随机值，IV/计数器/随机值也可省略。服务端不保存和管理 IV/计数器/随机值。

如果被管理对象有使用限制属性，那么在执行加密操作前服务端应从现有的使用限制中获取一个配额。如果无法获取配额，则返回“操作失败”的结果状态和“未获取授权”的原因。

响应包含用作密钥的被管理对象的唯一标识符和加密操作的结果。操作成功或者失败（如果失败，失败原因）显示在响应头的结果状态字段中。

加密操作的请求载荷与响应载荷，分别如表 198 和表 199 所示。

表 198　加密请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	被管理对象的唯一标识符，用作加密密钥。如果省略，服务端用 ID 占位符值作为唯一标识符
密码参数，见 6.3.7	否	加密用到的密码参数（分组算法加密模式，补齐方式，随机 IV）。如果省略，则使用被管理对象相关联的最低属性索引设定的密码参数。 如果被管理对象无相关联的密码参数，并且算法需要参数，则操作将返回“操作失败”的结果状态
数据	单步操作时是，多步操作时否	待加密的明文数据（作为字节串）
IV/计数器/随机值	否	要使用的初始向量，计数器或随机数
相关值，见 6.2.2.15	否	指向现有的序列流或分步密码操作（调用前一个密码操作的返回）
初始指示符，见 6.2.2.16	否	布尔值
完成指示符，见 6.2.2.17	否	布尔值
认证加密附加数据，见 6.2.2.22	否	通过认证加密标签认证的附加数据。如果在多步加密中提供，则必须在初始加密请求中提供此数据

表 199　加密响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	被管理对象的唯一标识符，用作加密密钥
数据	单步操作时是，多步操作时否	加密后的密文数据（作为字节串）
IV/计数器/随机值	否	如果在请求中没有提供加密参数指定的随机 IV 和 IV/计数器/随机值的值，则算法需要提供 IV/计数器/随机值
相关值，见 6.2.2.15	否	指向序列流或在执行加密操作的后续调用中要提供的分步操作值
认证加密标签，见 6.2.2.23	否	验证解密数据所需的标签。认证加密密码在完成最后一个明文的加密时返回

6.4.1.29　解密

该操作请求服务端使用被管理对象作为解密密钥对所提供的数据执行解密操作。此操作是可选操作。请求包含密码参数信息（加密模式和补齐方式），待解密的数据，用到的 IV/计数器/随机值。密码参数可省略，因为他们可以在被管理的密码对象相关属性中指定。如果算法不需要 IV/计数器/随机值也可被省略。响应包含用作密钥的被管理对象的唯一标识符和解密操作的结果。操作成功或者失败（如果失败，失败原因）显示在响应头的结果状态字段中。

解密操作的请求载荷与响应载荷，分别如表 200 和表 201 所示。

表 200　解密请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	被管理对象的唯一标识符，作为解密密钥。如果省略，服务端用 ID 占位符作为唯一标识符
密码参数，见 6.3.7	否	与特定解密方法相对应的密码参数。如果省略，则使用与具有最低属性索引的被管理对象相关联的加密参数。 如果没有与被管理对象相关联的加密参数，并且算法需要参数，则操作将返回，并显示“操作失败的结果状态”
数据	单步操作时是，多步操作时否	要解密的数据（作为字节串）
IV/计数器/随机值	否	要使用的初始向量，计数器或随机数
相关值，见 6.2.2.15	否	指向现有的序列流或分步密码操作（调用前一个密码操作的返回）
初始指示符，见 6.2.2.16	否	布尔值
完成指示符，见 6.2.2.17	否	布尔值
认证加密附加数据，见 6.2.2.22	否	应通过认证加密标签进行认证的附加数据。如果是多步解密方式提供，则必须在初始解密请求中提供此数据
认证加密标签，见 6.2.2.23	否	指定验证解密数据所需的标签。如果以多步解密方式提供，则必须在初始解密请求中提供此数据

表 201　解密响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	被管理对象的唯一标识符，用于解密密钥
数据	单步操作时是，多步操作时否	解密后的明文数据（作为字节串）
相关值，见 6.2.2.15	没有	指向序列流或在执行加密操作的后续调用中要提供的分步操作值

6.4.1.30　签名

此操作请求服务端使用被管理对象作为签名密钥对提供的数据执行签名操作。此操作是可选操作。请求包含密码参数（数字签名算法或密码算法和杂凑算法）以及要签名的数据。密码参数可省略，因为可以从被管理对象的关联属性中指定。如果被管理对象有使用限制属性，那么在执行签名操作前服务端应从现有的使用限制中获取一个配额。如果无法获取配额，则返回“操作失败”的结果状态和失败原因“未获取授权”。响应包含用作密钥的被管理对象的唯一标识符和签名操作的结果。操作成功或者失败（如果失败，失败原因）显示在响应头的结果状态字段中。

签名操作请求载荷与响应载荷，分别如表 202 和表 203 所示。

表 202　签名请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	被管理对象的唯一标识符，用于签名密钥。如果省略，服务端用 ID 占位符作为唯一标识符
密码参数，见 6.3.7	否	标识签名生成方法对应的密码参数（数字签名算法或密码算法和 HASH 算法）。如果省略，则使用被管理对象相关联的最低属性索引设定的密码参数。 如果被管理对象无相关联的密码参数，并且算法需要参数，则操作将返回“操作失败”的结果状态
数据	除非提供了摘要数据对于单步操作时是。多步操作时否	要签名的数据（作为字节串）
摘要数据	否	要签名的摘要数据（作为字节串）
相关值，见 6.2.2.15	否	指向现有的序列流或分步密码操作（调用前一个密码操作的返回）
初始指示符，见 6.2.2.16	否	布尔值
完成指示符，见 6.2.2.17	否	布尔值

表 203　签名响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	被管理对象的唯一标识符，用于签名密钥
签名数据	单步操作时是，多步操作时否	签名数据（作为字节串）
相关值，见 6.2.2.15	没有	指向序列流或在执行加密操作的后续调用中要提供的分步操作值

6.4.1.31　验签

该操作请求服务端使用被管理对象作为签名验证操作的密钥对提供的数据执行签名验证操作。此操作是可选操作。该请求包含关于加密参数（数字签名算法或加密算法和杂凑算法）和要验证的签名的信息，并且可包含传递给签名操作的数据（对于那些需要原始数据来验证签名的算法）。可从请求中省略加密参数，因为它们可以被指定为被管理对象的关联属性。响应包含所使用的被管理密钥的唯一标识符，以及从签名中恢复的可选数据（用于支持签名的数据恢复的签名算法）。该签名的有效性由有效性指标字段表示。该操作的成功或失败由响应头中的结果状态（如果失败，失败原因）来表示。

验签请求载荷与响应载荷，分别如表 204 和表 205 所示。

表 204　验签请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	用于验证签名操作的被管理密钥对象的唯一标识符。如果省略，则 ID 占位符将被服务端用作唯一标识符
密码参数，见 6.3.7	否	与要求的特定签名验证方法相对应的加密参数（数字签名算法或加密算法和杂凑算法）。如果省略，则使用与具有最低属性索引的被管理对象相关联的加密参数。 如果没有与被管理对象相关联的加密参数，并且算法需要参数，则操作将返回 失败状态
数据	否	已签名的数据（作为字节串）
摘要数据	否	要验证的摘要数据（作为字节串）
签名数据	单步操作时是，多步操作时否	要验证的签名（作为字节串）
相关值，见 6.2.2.15	否	指定现有的流或部分加密操作
初始指示符，见 6.2.2.16	否	初始操作为布尔值
完成指示符，见 6.2.2.17	否	最终操作为布尔值

表 205　验签响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	用于验证签名操作的被管理密钥对象的唯一标识符
有效性指标，见 6.5.3.2.23	是	一个枚举对象，指示签名是有效的，无效的还是未知的
数据	否	对于支持来自签名的数据恢复的签名算法，可选恢复数据（作为字节串）
相关值，见 6.2.2.15	否	指定在执行加密操作的此操作的后续调用中要提供的流或部分值

6.4.1.32　MAC 计算

此操作请求服务端使用被管理对象作为 MAC 操作的密钥对所提供的数据执行消息认证码（MAC）操作。此操作是可选操作。该请求包含有关加密参数（加密算法）和要做 MAC 计算的数据的信息。可从请求中省略加密参数，因为它们可以被指定为被管理对象的关联属性。响应包含用作密钥的被管理对象的唯一标识符和 MAC 计算的结果。该操作的成功或失败由响应头中的结果状态（如果失败，失败原因）来表示。

MAC 请求载荷与响应载荷，分别如表 206 和表 207 所示。

表 206　MAC 计算请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	用于 MAC 操作的被管理密钥对象的唯一标识符。如果省略，则 ID 占位符将被服务端用作唯一标识符
密码参数，见 6.3.7	否	与所要求的特定 MAC 方法对应的加密参数(加密算法)。如果省略，则使用与具有最低属性索引的被管理对象相关联的加密参数。 如果没有与被管理对象相关联的加密参数，并且算法需要参数，则操作将返回 失败状态
数据	单步操作时是，多步操作时否	用于 MAC 计算的数据(作为字节串)
相关值，见 6.2.2.15	否	指定现有的流或部分加密操作
初始指示符，见 6.2.2.16	否	初始操作为布尔值
完成指示符，见 6.2.2.17	否	最终操作为布尔值

表 207　MAC 计算响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	用于 MAC 操作的被管理密钥对象的唯一标识符
MAC 值	单步操作时是，多步操作时否	MAC 计算结果(作为字节串)
相关值，见 6.2.2.15	没有	指定在执行加密操作的此操作的后续调用中要提供的流或部分值

6.4.1.33　MAC 验证

此操作请求服务端使用被管理对象作为 MAC 验证操作的密钥，对所提供的数据执行 MAC 验证操作。此操作是可选操作。该请求包含关于加密参数(加密算法)和要做 MAC 验证的数据的信息，并且可包含传递给 MAC 操作的数据(对于需要原始数据来验证 MAC 的那些算法)。可从请求中省略加密参数，因为它们可以被指定为被管理对象的关联属性。响应包含了作为密钥的被管理对象的唯一标识符，以及 MAC 验证操作的结果。MAC 的有效性由“有效性指示符”字段表示。该操作的成功或失败由响应头中的结果状态(如果失败，失败原因)来表示。

MAC 验证请求载荷与响应载荷，分别如表 208 和表 209 所示。

表 208　MAC 验证请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	用于 MAC 验证操作的被管理密钥对象的唯一标识符。如果省略，则 ID 占位符值将被服务端用作唯一标识符

表 208　MAC 验证请求载荷（续）

对象	是否必需	描述
密码参数，见 6.3.7	否	与所要求的特定 MAC 方法对应的加密参数（加密算法）。如果省略，则使用与具有最低属性索引的被管理对象相关联的加密参数。 如果没有与被管理对象相关联的加密参数，并且算法需要参数，则操作将返回 失败状态
原始数据	否	要进行 MAC 验证的数据（作为字节串）
待验证的 MAC 值	单步操作时是，多步操作时否	MAC 值（作为字节串）
相关值，见 6.2.2.15	否	指定现有的流或部分加密操作（如前面调用此操作所返回的那样）
初始指示符，见 6.2.2.16	否	初始操作为布尔值
完成指示符，见 6.2.2.17	否	最终操作为布尔值

表 209　MAC 验证响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	被管理对象的唯一标识符是用于验证操作的密钥
有效性指示符，见 6.5.3.2.23	是	指示 MAC 是否有效，无效或未知的枚举对象
相关值，见 6.2.2.15	否	指定在执行加密操作的此操作的后续调用中要提供的流或部分值

6.4.1.34　获取随机数

此操作请求服务端返回一个随机数发生器（RNG）的输出值。请求包含输出随机数的数据量。响应包含输出的随机数。操作的成功或失败由响应头中的结果状态（如果失败，失败原因）表示。

获取随机数请求载荷与响应载荷，分别如表 210 和表 211 所示。

表 210　获取随机数请求载荷

对象	是否必需	描述
数据长度	是	随机数发生器输出返回的数据量（以字节为单位）

表 211　获取随机数响应载荷

对象	是否必需	描述
数据	是	随机数发生器输出

6.4.1.35 密码杂凑运算

此操作请求服务端对提供的数据执行密码杂凑运算。此操作是可选操作。请求信息包含有关加密参数(密码杂凑算法)和要进行密码杂凑的数据。响应包含杂凑操作的结果。操作的成功或失败由响应头中的结果状态(如果失败,失败原因)表示。

密码杂凑运算请求载荷与响应载荷,分别如表 212 和表 213 所示。

表 212 密码杂凑运算请求载荷

对象	是否必需	描述
密码参数,见 6.3.7	是	与要求的特定杂凑方法相对应的加密参数(杂凑算法)
数据	单步操作时是,多步操作时否	要进行杂凑的数据(作为字节串)
相关值,见 6.2.2.15	否	指定现有的流或部分加密操作
初始指示符,见 6.2.2.16	否	初始操作为布尔值
完成指示符,见 6.2.2.17	否	最终操作为布尔值

表 213 密码杂凑运算响应载荷

对象	是否必需	描述
数据	单步操作时是,多步操作时否	杂凑数据(作为字节串)
相关值,见 6.2.2.15	否	指定在执行加密操作的此操作的后续调用中要提供的流或部分值

6.4.1.36 创建拆分密钥

此操作请求服务端生成一个新的拆分密钥,并将所有拆分后的分量注册为单独的新的密码对象。该请求包含要分配给对象的属性(例如,密钥分量,密钥阈值,拆分密钥方法,加密算法,加密长度等)。请求可包含客户端请求由服务端拆分的现有密码对象的唯一标识符。如果请求中提供的属性与提供的密钥不匹配,那么密钥的属性优先。响应中包含所有已创建对象的唯一标识符。ID 占位符的值应被设置成密钥分量标识符为 1 的唯一标识符。

创建拆分密钥请求载荷与响应载荷,分别如表 214 和表 215 所示。

表 214 创建拆分密钥请求载荷

对象	是否必需	描述
对象类型,见 6.3.4	是	确定要创建的对象的类型
唯一标识符,见 6.3.2	否	要拆分的密钥唯一标识符
密钥分量数量	是	分量总数
密钥分量阈值	是	重建整个密钥所需的最少分量数
拆分方法	是	见 6.2.3.5
素域大小	否	
属性集,见 6.2.2.8	是	使用属性集指定所需的对象属性

表 215　创建拆分密钥响应载荷

对象	是否必需	描述
唯一标识符，见 6.2.2.1	是，可重复	新创建对象的唯一标识符列表
属性集，见 6.2.2.8	否	对象属性的可选列表，其值在请求中未指定，但已由密钥管理服务端隐式设置

6.4.1.37　拆分密钥合成

此操作请求服务端将密钥分量列表合成到单个被管理对象中。请求中唯一标识符的数量应不少于密钥分量中定义的拆分密钥的阈值。该请求包含客户端请求将拆分密钥对象组合形成的被管理对象的对象类型。如果形成的对象类型是秘密数据，则客户端可在请求中包括秘密数据类型。响应包含将拆分密钥组合得到的对象的唯一标识符。服务端应将此操作返回的唯一标识符复制到 ID 占位符变量中。

拆分密钥合成请求载荷与响应载荷，分别如表 216 和表 217 所示。

表 216　拆分密钥合成请求载荷

对象	是否必需	描述
对象类型，见 6.3.4	是	确定要创建的对象的类型
唯一标识符，见 6.3.2	是，可重复	确定要组合的密钥分量。标识符的最小数量由每个拆分密钥中的“密钥分量阈值”字段指定
秘密数据类型	否	确定所拆分的密钥是哪种秘密数据类型
属性集，见 6.2.2.8	否	使用属性集指定所需的对象属性

表 217　拆分密钥合成响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	通过组合密钥分量获得的密钥对象的唯一标识符
属性集，见 6.2.2.8	否	对象属性的可选列表，其值在请求中未指定，但已由密钥管理服务端隐式设置

6.4.1.38　导出

此操作请求服务端返回由其唯一标识符指定的被管理对象及其属性。密钥格式类型、密钥封装类型、密钥压缩类型和密钥封装规范应具有与“获取”操作相同的语义。如果被管理对象已被销毁，那么指定的被管理对象的密钥材料不会在响应中返回。服务端应将此操作返回的唯一标识符复制到 ID 占位符变量中。应强制执行特定的身份验证和授权来执行此请求。只有对象所有者或授权的安全人员才能发出此请求。

导出请求载荷与响应载荷，如表 218 和表 219 所示。

表 218　导出请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	否	确定要请求的对象。如果省略，则 ID 占位符值将被服务端用作唯一标识符
密钥格式类型，见 6.5.3.2.3	否	确定要返回的密钥格式类型
密钥封装类型，见 6.5.3.2.3	否	确定返回密钥值的密钥封装类型
密钥压缩类型，见 6.5.3.2.2	否	确定椭圆曲线公钥的压缩方法
密钥封装规格，见 6.2.2.6	否	指定用于封装返回对象的密钥和其他信息

表 219　导出响应载荷

对象	是否必需	描述
对象类型，见 6.3.4	是	对象的类型
唯一标识符，见 6.3.2	是	对象的唯一标识符
属性，见 6.2.2.1	是，重复	所有对象的属性
证书，对称密钥，私钥，公钥，拆分密钥，秘密数据或不透明对象，见 6.2.2.22	是	与“获取”操作相同的方式返回对象值

6.4.1.39　导入

此操作请求服务端导入由其唯一标识符指定的被管理对象。该请求指定要导入的对象以及要分配给对象的所有属性。“初始设置”和“隐式设置”的每个属性的属性规则不应被强制执行，因为所有属性必须设置为提供的值，而不是任何服务端生成的值。应强制执行特殊的身份验证和授权来执行此请求。只有对象所有者或授权的安全人员才能发出此请求。响应包含请求或服务端分配的唯一标识符。服务端应将此操作返回的唯一标识符复制到 ID 占位符变量中。

导入请求载荷与响应载荷，如表 220 和表 221 所示。

表 220　导入请求载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	要导入的对象的唯一标识符
是否替代	否	一个布尔值。如果指定为 True，那么具有相同唯一标识符的任何现有对象都将被此操作替换。如果缺少或为 False，则如果存在具有相同唯一标识符的现有对象，则操作将失败
密钥封装类型，见 6.5.3.2.46	否	如果未封装，则服务端在存储之前应解除对象，如果封装密钥不可用，则返回错误。否则，服务端应按照提供的方式存储对象
属性，见 6.2.2.1	是，重复	所有对象的属性
证书，对称密钥，私钥，公钥，拆分密钥，秘密数据或不透明对象，见 6.2.2.22	是	导入的对象值与注册操作相同

表 221　导入响应载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符

6.4.2　服务端到客户端操作

6.4.2.1　概述

服务端到客户端操作被服务端用来通过普通的客户机-服务端和请求-响应机制之外的手段向客户端发送信息或被管理对象。这些操作用于主动将被管理对象直接发送到客户端，而不需要客户端的特定请求。

6.4.2.2　通知

此操作用于通知客户端导致对象属性更改的事件。此操作只能由服务端通过普通客户端请求/响应协议之外的手段发送到客户端，通过未指定的配置或管理机制使用服务端已知的信息。它包含应用通知的对象唯一标识符，以及已更改值并触发通知的属性列表。其消息使用与请求消息相同的格式(见 6.5.2，表 247)，但不准许使用最大响应大小，异步指示符，批处理错误附加选项和批处理顺序选项字段。客户端应以不包含有效载荷的响应消息(见 6.5.2，表 248)的形式发送响应，除非客户端和服务端都具有客户端无法响应的先验知识(通过带外机制获取)。

通知消息载荷，如表 222 所示。

表 222　通知消息载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符
属性，见 6.3	是，可重复	属性已更改。至少包括最后更改日期属性。如果属性被删除，则属性结构(见 6.2.2.1)不应包含“属性值”字段

6.4.2.3　推送

此操作用于将被管理对象“推送”到客户端。此操作只能由服务端通过普通客户端请求/响应协议之外的手段发送到客户端，通过未指定的配置或管理机制使用服务端已知的信息。它包含正在发送的对象唯一标识符，以及对象本身。消息使用与请求消息相同的格式(见 6.5.2，表 247)，但不准许使用最大响应大小，异步指示符，批处理错误继续选项和批处理顺序选项字段。客户端应以不包含有效载荷的响应消息(见 6.5.2，表 248)的形式发送响应，除非客户端和服务端都具有客户端无法响应的先验知识(通过带外机制获取)。

“推送功能”字段代表“被推送”的对象是否是一个新的对象，或者是客户端已经知道的替代对象。“推送功能”应包含以下值之一：

新建——表示对象不是替代另一个对象。

替换——表示对象是另一个对象的替代，并且替换的唯一标识符字段存在并且包含被替换对象的标识。如果客户端不存在具有替换的唯一标识符的对象，则客户端便认为“推送功能”中包含“新建”值。

属性字段包含服务端与对象一起发送的一个或多个属性。服务端可包括对象的属性，以指定对象

如何被客户端使用。服务端可包括授予租约给客户端的租约时间属性。如果被管理对象是封装密钥，那么密钥封装规范在通过带外机制传输之前应进行交换。

处理消息载荷，如表 223 所示。

表 223　推送消息载荷

对象	是否必需	描述
唯一标识符，见 6.3.2	是	对象的唯一标识符
推送功能，见 6.5.3.2.26	是	表示推送消息的功能
替换唯一标识符，见 6.3.2	否	替换对象的唯一标识符。如果推送功能是替换，将存在
证书，对称密钥，私钥，公钥，拆分密钥，秘密数据或不透明对象，见 6.2.2.22	是	该对象被发送到客户端
属性，见 6.3	否，可重复	服务端希望附加属性与对象一起发送

6.4.2.4　查询

该操作是由服务端询问客户端以确定其性能和协议机制。查询操作应由未经身份验证的服务端调用，以查询客户端特性和功能。请求中的“请求功能”字段应包含以下一个或多个项目：

——查询操作；
——查询对象；
——查询服务端信息；
——查询扩展列表；
——查询扩展映射；
——查询证明类型；
——查询随机数发生器；
——查询验证；
——查询配置文件；
——查询能力；
——查询客户端注册方法。

如果没有值返回，响应载荷为空。

查询请求载荷和响应载荷，如表 224 和表 225 所示。

表 224　查询请求载荷

对象	是否必需	描述
查询功能，见 6.5.3.2.24	是，可重复	确定要查询的信息

表 225　查询响应载荷

对象	是否必需	描述
操作，见 6.5.3.2.27	否，可重复	指定客户端支持的操作
对象类型，见 6.3.4	否，可重复	指定客户端支持的被管理对象类型

表 225　查询响应载荷（续）

对象	是否必需	描述
供应商标识	否	如果要求查询服务端信息，则返回。供应商标识应是唯一标识供应商的文本字符串
服务端信息	否	包含针对查询的供应商特定的信息
扩展信息，见 6.2.2.9	否，可重复	如果客户端请求并支持查询扩展列表或查询扩展映射，则返回
证明类型，见 6.5.3.2.36	否，可重复	指定客户端支持的认证类型
RNG 参数，见 6.2.2.18	否，可重复	指定客户端支持的 RNG
配置文件信息，见 6.2.2.19	否，可重复	指定客户端支持的配置文件
验证信息，见 6.2.2.20	否，可重复	指定客户端支持的验证
能力信息，见 6.2.2.21	否，可重复	指定客户端支持的能力
客户端注册方法，见 6.5.3.2.45	否，可重复	指定客户端支持的客户端注册方法

6.4.2.5　版本查询

服务端使用此操作来确定客户端支持的协议版本列表。请求载荷中要包含服务端支持的协议版本的可选列表，并按优先顺序进行排列。响应载荷要包含客户端支持的协议版本列表，并按优先级递减顺序排列。如果服务端向客户端提供了请求载荷中支持的协议版本列表，则客户端只需要返回客户端和服务端都支持的协议版本即可。客户端要列出客户端和服务端支持的所有协议版本。如果请求载荷中没有在请求报头中指定协议版本，且客户端不支持请求载荷中指定的任何协议版本，则客户端在响应载荷中返回一个空列表。如果请求载荷中没有指定协议版本，则客户端返回客户端支持的所有协议版本。

版本查询请求载荷和响应载荷，如表 226 和表 227 所示。

表 226　版本查询请求载荷

对象	是否必需	描述
协议版本，见 6.5.1.1	否，可重复	服务端支持的协议版本列表，按照优先级顺序递减排列

表 227　版本查询响应载荷

对象	要求	描述
协议版本，见 6.5.1.1	否，可重复	客户端支持的协议版本列表，按照优先级顺序递减排列

6.5　消息

6.5.1　消息元素

6.5.1.1　协议版本

该字段包含协议的版本号，确保通信方能够完全理解协议。版本号应分为主版本和次要版本两个部分。服务端和客户端应支持与主版本相同的协议版本的向后兼容性。支持与不同主版本的向后兼容性是可选的。消息头中的协议版本结构，如表 228 所示。

表 228　消息头中的协议版本结构

对象	编码
协议版本	结构
主版本	整型
次要版本	整型

6.5.1.2　操作

该字段表示正在请求的操作或返回响应的操作。操作在 6.4 和 6.5 中定义。批处理操作，如表 229 所示。

表 229　批处理操作

对象	编码
操作	枚举，见 6.5.3.2.27

6.5.1.3　最大响应长度

这是一个包含在请求消息中的可选字段，用于指示请求者能够处理的响应消息的最大长度(以字节为单位)。它应只包含于可能返回大量回复的请求中。消息请求头中的最大响应长度，如表 230 所示。

表 230　消息请求头中的最大响应长度

对象	编码
最大响应长度	整型

6.5.1.4　唯一批处理项 ID

这是请求中包含的可选字段，用于请求和响应之间的关联。如果请求消息中有唯一批处理项 ID，则对应该请求的响应消息中需要有相同的唯一批处理项 ID。在批处理项中唯一的批处理项 ID，如表 231 所示。

表 231　批处理项中唯一的批处理项 ID

对象	编码
唯一批处理项 ID	字节串

6.5.1.5　时间戳

这是客户端请求中包含的可选字段。在服务端请求和响应中需要它。时间戳主要用于确保客户端在合理的时间内执行操作(例如，如果客户端请求带的时间戳时间与服务端时间相差太大的情况下，服务端可以拒绝该请求)。注意：时间戳可以在没有实时时钟的客户端使用，但会有一个倒数计时器，通过减法来获取有用的当前时间信息。消息头中的时间戳，如表 232 所示。

表 232　消息头中的时间戳

对象	编码
时间戳	日期-时间

6.5.1.6　身份鉴别

这用于对请求者进行身份鉴别。它是一个可选的信息项，具体取决于所发出的请求类型和服务端策略。服务端可以在没有请求的情况下进行身份鉴别，也可以在请求的子集或者所有请求上进行身份鉴别，具体选择可通过策略定义。用于查询服务端特征和功能的查询操作不需要身份鉴别。身份鉴别可包括一个或多个身份凭证。认证机制在 7.4 中进行了描述和讨论。消息头中的身份认证结构，如表 233 所示。

表 233　消息头中的身份认证结构

对象	编码
身份鉴别	结构
身份凭证，可重复	结构，见 6.2.2.2

6.5.1.7　异步指示器

布尔型，用于指示客户端是否能够接受异步响应。如果客户端能够处理异步响应，它的布尔值为 True，否则为 False。如果请求中不存在该项，则假定为 False。如果客户端表示无法处理异步响应，服务端将同步处理请求。消息请求头中的异步指示器，如表 234 所示。

表 234　消息请求头中的异步指示器

对象	编码
异步指示器	布尔

6.5.1.8　异步相关值

异步相关值是在正在进行的操作的即时响应中返回的，并且需要异步轮询。服务端决定哪些操作是同步执行还是异步执行的(见 6.5.1.7)。在与原始操作相关的任何后续轮询或取消操作中应指定服务器生成的相关值。响应批处理中的异步相关值，如表 235 所示。

表 235　响应批处理中的异步相关值

对象	编码
异步相关值	字节串

6.5.1.9　结果状态

结果状态是在响应消息中发送的，代表请求成功或失败。可以在此字段中设置以下值：

成功——请求的操作成功完成；

操作挂起——请求的操作正在进行中，需要通过异步轮询获取实际结果。结果状态的后续轮询应使用异步相关值；

操作撤销——请求的操作被执行，但必须被撤销（即：由于批处理错误继续选项，见 6.5.1.13 和6.5.2 被设置为撤销）；

操作失败——请求的操作失败。

响应批处理中的异步相关值，如表 236 所示。

表 236　结果状态载荷

对象	编码
结果状态	枚举，见 6.5.3.2.28

6.5.1.10　结果原因

此字段表示失败的原因或部分成功时需要修改的内容，在返回失败结果状态的响应中出现。在这种情况下，结果原因按照附录 B 规定进行设置。任何返回成功结果状态的响应都是可选的。为此字段定义了以下值：

未找到项——未找到请求对象或请求对象不存在；

响应超长——对请求的响应超出请求中的最大响应长度；

身份认证不成功——请求中的身份认证信息无法验证，或未找到；

无效消息——请求消息未被服务端理解；

不支持操作——服务端不支持请求消息请求的操作；

缺少数据——操作需要请求中的其他信息，但是不存在需要的其他消息；

无效字段——请求中的某些数据项具有无效值；

功能不支持——不支持请求中指定的可选功能；

请求者取消操作——操作是异步的，在操作未成功完成之前被取消；

加密失败——由于加密错误，操作失败；

非法操作——客户端请求了无法用指定参数执行的操作；

拒绝许可——客户端没有执行请求操作的权限；

对象已归档——在执行操作之前，应从存档中恢复对象；

超出范围的索引——客户端尝试设置的实例多于它所支持的数量；

不支持应用程序命名空间——不支持特定应用程序命名空间，如果客户端请求中省略了该字段，则服务端无法生成应用程序特定信息属性的应用程序数据字段；

密钥格式类型和/或密钥压缩类型不支持——对象存在，但服务端无法提供需要的密钥格式类型或者密钥压缩类型；

一般故障——除了上述定义的原因之外，请求失败。

响应批处理的结果原因，如表 237 所示。

表 237　响应批处理的结果原因

对象	编码
结果原因	枚举，见 6.5.3.2.29

6.5.1.11 返回消息

此字段可以在响应中返回，包含一个描述更详细的错误消息，可以提供给最终用户，或者用于日志和审计目的。响应批处理的结果消息，如表 238 所示。

表 238 响应批处理的结果消息

对象	编码
返回消息	文本串

6.5.1.12 批处理顺序选项

布尔值，用于请求中批处理计数大于 1 的请求。如果为 True，则批处理操作将按照请求中显示的顺序执行。如果为 False，则服务端可以选择以任何顺序执行批处理操作。如果未指定，则假定为 False（没有隐含排序）。服务端对此功能的支持是可选的，但是如果服务端不支持这个特性，并且请求中批处理顺序选项被设置为 True，那么整个请求将被拒绝。消息请求头中的批处理顺序选项，如表 239 所示。

表 239 消息请求头中的批处理顺序选项

对象	编码
批处理顺序选项	布尔

6.5.1.13 批处理错误继续选项

如果批处理计数大于 1，则此选项才会出现。此选项应具有以下三个值中的一个：

撤销——如果请求中的任何操作失败，则服务端将撤销所有以前的操作。

停止——如果操作失败，则服务端不会继续处理请求中的后续操作。完成的操作不可撤销。

继续——为失败操作返回错误值，并继续处理请求中的后续操作。

如果未指定，则假定为停止。服务端对此功能的支持是可选的，但是如果服务端不支持该功能，并且收到包含有不同于默认值（停止）的批量错误的请求，那么整个请求将被拒绝。消息请求头中的批处理错误继续选项，如表 240 所示。

表 240 消息请求头中的批处理错误继续选项

对象	编码
批处理错误继续选项	枚举，见 6.5.3.2.30

6.5.1.14 批处理项数量

此字段是必须的，包含消息中的批处理项的数量。如果仅请求单个操作，则批处理项计数应设置为 1。消息有效载荷跟在消息头后面，包含一个或多个批处理项。消息头中的批处理项数量，如表 241 所示。

表 241 消息头中的批处理项数量

对象	编码
批处理项数量	整型

6.5.1.15 批处理项

该字段由一个结构组成，包含一个在批处理中保存各个请求或响应的结构，并且是必需的。批处理项的内容见 6.5.2 中描述。消息中的批处理项，如表 242 所示。

表 242 消息中的批处理项

对象	编码
批处理项	结构

6.5.1.16 消息扩展

消息扩展是可选结构，可以附加到任何批处理项。它用于扩展协议消息，以增加供应商指定的扩展。消息扩展是一种结构，该结构包含供应商标识、关键性指示符和供应商扩展字段。供应商标识是唯一标识供应商的文本字符串，客户端可指定是否可解析该扩展项。如果客户端或者服务端接收到含有无法解析的消息扩展项的协议消息，其操作取决于关键性指示符。如果为 True(即关键性)，接收方无法解析扩展项，则接收方应拒绝整个消息。如果指示符是 False(即非关键性)，且接收方无法解析扩展项，则接收方可处理消息的其余部分，扩展项可当作不存在。供应商扩展结构包含供应商的特定扩展。批处理项中的消息扩展结构，如表 243 所示。

表 243 批处理项中的消息扩展结构

对象	编码
消息扩展	结构
供应商标识	文本串
关键性指示符	布尔
供应商扩展	结构

6.5.1.17 认证能力指示符

认证能力指示符代表客户端是否能够创建一个认证凭证对象。如果客户端能够创建一个认证凭证对象，则它的布尔值为 True，否则为 False。如果不存在，则假定值为 False。如果客户端指示无法创建认证凭证对象，但又发起了需要认证的操作(例如获取操作)，那么服务端将响应失败。消息请求头中的认证能力指示符，如表 244 所示。

表 244 消息请求头中的认证能力指示符

对象	编码
认证能力指示符	布尔

6.5.1.18 客户端相关值

客户端相关值是一个字符串，可以被客户端添加到消息，以向服务端提供附加的信息。它不具有唯一性。服务端应记录这些信息。在客户端到服务端的请求操作中提供客户端相关值。在服务端到客户端的响应操作中也提供客户端相关值。消息请求头中的客户端相关值，如表 245 所示。

表 245　消息请求头中的客户端相关值

对象	编码
客户端相关值	文本串

6.5.1.19　服务端相关值

服务端相关值由服务端提供，且是全局唯一的，由服务端记录每个请求。服务端相关值在客户端到服务端的响应操作中提供，也可在服务端到客户端的请求操作中提供。消息请求头中的服务端相关值，如表 246 所示。

表 246　消息请求头中的服务端相关值

对象	编码
服务端相关值	文本串

6.5.2　消息结构

协议中的消息由消息头、一个或多个批处理项(其中包含可选的消息载荷)和可选的消息扩展组成。消息头包含用以确定所使用的协议特征的字段(例如，异步响应)。字段内容取决于此消息是请求还是响应。消息内容包括所请求的具体操作或被回复的具体操作。

消息包含以下对象和字段。所有字段应按指定的顺序出现，分别如表 247～表 252 所示。

表 247　请求消息结构

对象	编码	是否必需
请求消息	结构	
请求消息头	结构，见表 249	是
批处理项	结构，见表 250	是，可重复

表 248　响应消息结构

对象	编码	是否必需
响应信息	结构	
响应消息头	结构，见表 251	是
批处理项	结构，见表 252	是，可重复

如果客户端能够接受异步响应，则可以在批处理请求的消息头中设置异步指示器。批处理响应可能同时包含同步和异步响应。

表 249　请求头结构

对象	是否必需	备注
请求头	是	结构
协议版本	是	见 6.5.1.1
最大响应长度	否	见 6.5.1.3
客户端相关值	否	见 6.5.1.18
异步指示器	否	见 6.5.1.7
认证能力指示符	否	见 6.5.1.17
认证类型	否,可重复	见 6.5.3.2.36
身份认证	否	见 6.5.1.6
批处理错误继续选项	否	如果省略,则假定停止,见 6.5.1.13
批处理顺序选项	否	如果省略,则假定为假,见 6.5.1.12
时间戳	否	见 6.5.1.5
批处理项数量	是	见 6.5.1.14
批处理项数量	是	见 6.5.1.14

表 250　请求批处理项结构

对象	是否必需	备注
批处理项	是	结构,见 6.5.1.15
操作	是	见 6.5.1.2
唯一批处理项 ID	否	如果批量次数>1,见 6.5.1.4
请求载荷	是	结构,内容取决于操作,见 6.4.1 和 6.4.2
消息扩展	否	见 6.5.1.16

表 251　响应头结构

对象	是否必需	备注
响应头	是	结构
协议版本	是	见 6.5.1.1
时间戳	是	见 6.5.1.5
随机数	否	见 6.2.2.14
认证类型	否,可重复	在认证过程中,如果客户端在请求中设置了认证能力指示符为 True,见 6.5.3.2.36
客户端相关值	否	见 6.5.1.18
服务端相关值	否	见 6.5.1.19
批处理项数量	是	见 6.5.1.14

表 252　响应批处理项结构

对象	是否必需	备注
批处理项	是	结构见 6.5.1.15
操作	是，如果在请求批处理项中指定	见 6.5.1.2
唯一批处理项 ID	否	如果在请求批项目中出现，见 6.5.1.4
结果状态	是	见 6.5.1.9
结果原因	是，如果结果状态为 False	如果结果状态为 False，则需要，否则可选，见 6.5.1.10
结果消息	否	如果结果状态不是等待或成功则为“可选”，见 6.5.1.11
异步相关值	否	如果结果状态为等待，见 6.5.1.8
响应载荷	是，如果不是 False	结构，内容取决于操作，见 6.4.1 和 6.4.2
消息扩展	否	见 6.5.1.16

6.5.3　消息编码

6.5.3.1　标签

表 253 所示为协议消息定义了对象和原始数据值的标签值。

表 253　标签值

名称	对象	标签值
未使用	(Unused)	000000—420000
激活日期	Activation Date	420001
应用程序数据	Application Data	420002
应用程序命名空间	Application Namespace	420003
应用程序特定信息	Application Specific Information	420004
归档日期	Archive Date	420005
异步相关值	Asynchronous Correlation Value	420006
异步指示器	Asynchronous Indicator	420007
属性	Attribute	420008
属性索引	Attribute Index	420009
属性名称	Attribute Name	42000A
属性值	Attribute Value	42000B
身份认证	Authentication	42000C
批处理项数量	Batch Count	42000D
批处理错误继续选项	Batch Error Continuation Option	42000E

表 253　标签值（续）

名称	对象	标签值
批处理项	Batch Item	42000F
批处理顺序选项	Batch Order Option	420010
分组密码模式	Block Cipher Mode	420011
取消结果	Cancellation Result	420012
证书	Certificate	420013
证书标识符	Certificate Identifier	420014
证书颁发者	Certificate Issuer	420015
证书颁发者替换名	Certificate Issuer Alternative Name	420016
证书颁发者可识别名	Certificate Issuer Distinguished Name	420017
证书请求	Certificate Request	420018
证书请求类型	Certificate Request Type	420019
证书主体	Certificate Subject	42001A
证书主体替换名	Certificate Subject Alternative Name	42001B
证书主体可识别名	Certificate Subject Distinguished Name	42001C
证书类型	Certificate Type	42001D
证书值	Certificate Value	42001E
通用属性集	Common Template-Attribute	42001F
失信日期	Compromise　Date	420020
失信发生日期	Compromise Occurrence Date	420021
联系信息	Contact Information	420022
凭证	Credential	420023
凭证类型	Credential Type	420024
凭证值	Credential Value	420025
关键性指示符	Criticality Indicator	420026
CRT 系数	CRT Coefficient	420027
密码算法	Cryptographic Algorithm	420028
密码算法域参数	Cryptographic Domain Parameters	420029
加密长度	Cryptographic Length	42002A
密码参数	Cryptographic Parameters	42002B
密码用途掩码	Cryptographic Usage Mask	42002C
自定义属性	Custom Attribute	42002D
D	D	42002E
停用日期	Deactivation Date	42002F

表 253　标签值（续）

名称	对象	标签值
派生数据	Derivation Data	420030
派生方法	Derivation Method	420031
派生参数	Derivation Parameters	420032
销毁日期	Destroy Date	420033
摘要	Digest	420034
摘要值	Digest Value	420035
加密密钥信息	Encryption Key Information	420036
G	G	420037
杂凑算法	Hashing Algorithm	420038
初始化日期	Initial Date	420039
初始向量	Initialization Vector	42003A
颁发者	Issuer	42003B
迭代次数	Iteration Count	42003C
IV/计数器/随机值	IV/Counter/Nonce	42003D
J	J	42003E
密钥	Key	42003F
密钥块	Key Block	420040
密钥压缩类型	Key Compression Type	420041
密钥格式类型	Key Format Type	420042
密钥材料	Key Material	420043
密钥分量标识符	Key Part Identifier	420044
密钥值	Key Value	420045
密钥封装规范	Key Wrapping Specification	420047
最后修改日期	Last Change Date	420048
租约时间	Lease Time	420049
链接	Link	42004A
链接类型	Link Type	42004B
链接对象标识符	Linked Object Identifier	42004C
MAC/签名	MAC/Signature	42004D
MAC/签名密钥信息	MAC/Signature Key Information	42004E
最大项目数量	Maximum Items	42004F
最大响应长度	Maximum Response Size	420050
消息扩展	Message Extension	420051
模量	Modulus	420052

表 253　标签值（续）

名称	对象	标签值
名称	Name	420053
名称类型	Name Type	420054
名称值	Name Value	420055
对象组	Object Group	420056
对象类型	Object Type	420057
偏移量	Offset	420058
不透明数据类型	Opaque Data Type	420059
不透明数据值	Opaque Data Value	42005A
不透明对象	Opaque Object	42005B
操作	Operation	42005C
操作策略名称	Operation Policy Name	42005D
P	P	42005E
填充方法	Padding Method	42005F
素数 P	Prime Exponent P	420060
素数 Q	Prime Exponent Q	420061
素域尺寸	Prime Field Size	420062
私钥指数	Private Exponent	420063
私钥	Private Key	420064
私钥属性集	Private Key Template-Attribute	420065
私钥唯一标识符	Private Key Unique Identifier	420066
生效日期	Process Start Date	420067
失效日期	Protect Stop Date	420068
协议版本	Protocol Version	420069
主版本	Protocol Version Major	42006A
次要版本	Protocol Version Minor	42006B
公钥指数	Public Exponent	42006C
公钥	Public Key	42006D
公钥属性集	Public Key Template-Attribute	42006E
公钥唯一标识符	Public Key Unique Identifier	42006F
推送功能	Put Function	420070
Q	Q	420071
Q 字符串	Q String	420072
Q 长度	Qlength	420073
查询功能	Query Function	420074

表 253　标签值（续）

名称	对象	标签值
推荐曲线	Recommended Curve	420075
替换唯一标识符	Replaced Unique Identifier	420076
请求头	Request Header	420077
请求消息	Request Message	420078
请求载荷	Request Payload	420079
响应头	Response Header	42007A
响应消息	Response Message	42007B
响应载荷	Response Payload	42007C
结果消息	Result Message	42007D
结果原因	Result Reason	42007E
结果状态	Result Status	42007F
注销信息	Revocation Message	420080
注销原因	Revocation Reason	420081
注销原因码	Revocation Reason Code	420082
密钥角色类型	Key Role Type	420083
添加变量	Salt	420084
秘密数据	Secret Data	420085
秘密数据类型	Secret Data Type	420086
序列号	Serial Number	420087
服务端信息	Server Information	420088
拆分密钥	Split Key	420089
拆分密钥方法	Split Key Method	42008A
拆分密钥分量	Split Key Parts	42008B
拆分密钥阈值	Split Key Threshold	42008C
状态	State	42008D
存储状态掩码	Storage Status Mask	42008E
对称密钥	Symmetric Key	42008F
模板	Template	420090
属性集	Template-Attribute	420091
时间戳	Time Stamp	420092
唯一批处理项 ID	Unique Batch Item ID	420093
唯一标识符	Unique Identifier	420094
使用限制	Usage Limits	420095
使用限制计数	Usage Limits Count	420096

表 253　标签值（续）

名称	对象	标签值
使用限制总数	Usage Limits Total	420097
使用限制单位	Usage Limits Unit	420098
用户名	Username	420099
有效期	Validity Date	42009A
有效性标识	Validity Indicator	42009B
供应商扩展	Vendor Extension	42009C
供应商标识	Vendor Identification	42009D
封装方法	Wrapping Method	42009E
X	X	42009F
Y	Y	4200A0
口令	Password	4200A1
设备标识	Device Identifier	4200A2
编码选项	Encoding Option	4200A3
扩展信息	Extension Information	4200A4
扩展名	Extension Name	4200A5
扩展标签	Extension Tag	4200A6
扩展类型	Extension Type	4200A7
未使用	Fresh	4200A8
机器标识	Machine Identifier	4200A9
媒体标识	Media Identifier	4200AA
网络标识	Network Identifier	4200AB
对象组成员	Object Group Member	4200AC
证书长度	Certificate Length	4200AD
数字签名算法	Digital Signature Algorithm	4200AE
证书序列号	Certificate Serial Number	4200AF
设备序列号	Device Serial Number	4200B0
颁发者可识别名	Issuer Alternative Name	4200B1
颁发者可识别名	Issuer Distinguished Name	4200B2
主体替换名	Subject Alternative Name	4200B3
主体可识别名	Subject Distinguished Name	4200B4
X.509 证书标识符	X.509 Certificate Identifier	4200B5
X.509 证书颁发者	X.509 Certificate Issuer	4200B6
X.509 证书主体	X.509 Certificate Subject	4200B7
密钥值位置	Key Value Location	4200B8

表 253　标签值（续）

名称	对象	标签值
密钥值位置值	Key Value Location Value	4200B9
密钥值位置类型	Key Value Location Type	4200BA
密钥值存在标记	Key Value Present	4200BB
原创创建日期	Original Creation Date	4200BC
PGP 密钥	PGP Key	4200BD
PGP 密钥版本	PGP Key Version	4200BE
别名	Alternative Name	4200BF
别名值	Alternative Name Value	4200C0
别名类型	Alternative Name Type	4200C1
数据	Data	4200C2
签名数据	Signature Data	4200C3
数据长度	Data Length	4200C4
随机 IV	Random IV	4200C5
MAC 值	MAC Data	4200C6
证实类型	Attestation Type	4200C7
随机数	Nonce	4200C8
随机数 ID	Nonce ID	4200C9
随机数值	Nonce Value	4200CA
证实测量	Attestation Measurement	4200CB
证实声明	Attestation Assertion	4200CC
IV 长度	IV Length	4200CD
标签长度	Tag Length	4200CE
固定字段长度	Fixed Field Length	4200CF
计数器长度	Counter Length	4200D0
初始计数器值	Initial Counter Value	4200D1
调用字段长度	Invocation Field Length	4200D2
认证能力指示符	Attestation Capable Indicator	4200D3
偏移项目数量	Offset Items	4200D4
定位项目	Located Items	4200D5
相关值	Correlation Value	4200D6
初始指示符	Init Indicator	4200D7
完成指示符	Final Indicator	4200D8
RNG 参数	RNG Parameters	4200D9
RNG 算法	RNG Algorithm	4200DA

表 253　标签值（续）

名称	对象	标签值
DRBG 算法	DRBG Algorithm	4200DB
FIPS186 变化	FIPS186 Variation	4200DC
预测阻力	Prediction Resistance	4200DD
随机数发生器	Random Number Generator	4200DE
验证信息	Validation Information	4200DF
验证机构类型	Validation Authority Type	4200E0
验证机构国家	Validation Authority Country	4200E1
验证机构 URI	Validation Authority URI	4200E2
验证主版本	Validation Version Major	4200E3
验证次版本	Validation Version Minor	4200E4
验证类型	Validation Type	4200E5
验证级别	Validation Level	4200E6
验证证书编号	Validation Certificate Identifier	4200E7
验证证书 URI	Validation Certificate URI	4200E8
验证供应商 URI	Validation Vendor URI	4200E9
验证配置文件	Validation Profile	4200EA
配置文件信息	Profile Information	4200EB
配置文件名称	Profile Name	4200EC
服务器 URI	Server URI	4200ED
服务器端口	Server Port	4200EE
流化能力	Streaming Capability	4200EF
异步能力	Asynchronous Capability	4200F0
证明能力	Attestation Capability	4200F1
解封装模式	Unwrap Mode	4200F2
销毁操作	Destroy Action	4200F3
粉碎算法	Shredding Algorithm	4200F4
随机数发生器模式	RNG Mode	4200F5
客户端注册方法	Client Registration Method	4200F6
能力信息	Capability Information	4200F7
密钥封装类型	Key Wrap Type	4200F8
批量撤销能力	Batch Undo Capability	4200F9
批量持续能力	Batch Continue Capability	4200FA
PKCS#12 别名	PKCS#12 Friendly Name	4200FB
描述	Description	4200FC

表 253　标签值（续）

名称	对象	标签值
备注	Comment	4200FD
加密验证附加数据	Authenticated Encryption Additional Data	4200FE
加密验证完整性标签	Authenticated Encryption Tag	4200FF
添加变量长度	Salt Length	420100
掩码生成器	Mask Generator	420101
掩码生成器杂凑算法	Mask Generator Hashing Algorithm	420102
P 源	P Source	420103
填充字段	Trailer Field	420104
客户端相关值	Client Correlation Value	420105
服务端相关值	Server Correlation Value	420106
摘要数据	Digested Data	420107
证书主体 CN	Certificate Subject CN	420108
证书主体 O	Certificate Subject O	420109
证书主体 OU	Certificate Subject OU	42010A
证书主体 Email	Certificate Subject Email	42010B
证书主体 C	Certificate Subject C	42010C
证书主体 ST	Certificate Subject ST	42010D
证书主体 L	Certificate Subject L	42010E
证书主体 UID	Certificate Subject UID	42010F
证书主体 Serial Number	Certificate Subject Serial Number	420110
证书主体 Title	Certificate Subject Title	420111
证书主体 DC	Certificate Subject DC	420112
证书主体 DN Qualifier	Certificate Subject DN Qualifier	420113
证书颁发者 CN	Certificate Issuer CN	420114
证书颁发者 O	Certificate Issuer O	420115
证书颁发者 OU	Certificate Issuer OU	420116
证书颁发者 Email	Certificate Issuer Email	420117
证书颁发者 C	Certificate Issuer C	420118
证书颁发者 ST	Certificate Issuer ST	420119
证书颁发者 L	Certificate Issuer L	42011A
证书颁发者 UID	Certificate Issuer UID	42011B
证书颁发者 SerialNumber	Certificate Issuer Serial Number	42011C
证书颁发者 Title	Certificate Issuer Title	42011D
证书颁发者 DC	Certificate Issuer DC	42011E

表 253　标签值（续）

名称	对象	标签值
证书颁发者 DN Qualifier	Certificate Issuer DN Qualifier	42011F
敏感	Sensitive	420120
始终敏感	Always Sensitive	420121
提取	Extractable	420122
从未提取	Never Extractable	420123
是否替代	Replace Existing	420124
（预留）	（Reserved）	420120—42FFFF
（未使用）	（Unused）	430000—53FFFF
扩展	Extensions	540000—54FFFF
（未使用）	（Unused）	550000—FFFFFF

6.5.3.2　枚举

6.5.3.2.1　凭证类型枚举

凭证类型枚举，如表 254 所示。

表 254　凭证类型

名称	值
Username and Password	00000001
Device	00000002
Attestation	00000003
扩展	8XXXXXXX

6.5.3.2.2　密钥压缩类型枚举

密钥压缩类型枚举，如表 255 所示。

表 255　密钥压缩类型

名称	值
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
SM2 Public Key Type Uncompressed	00001001
SM2 Public Key Type Compressed	00001002
扩展	8XXXXXXX

6.5.3.2.3 密钥格式类型枚举

密钥格式类型枚举，如表 256 所示。

表 256 密钥格式类型

名称	值
Raw	00000001
Opaque	00000002
PKCS#1	00000003
PKCS#8	00000004
X.509	00000005
ECPrivateKey	00000006
Transparent Symmetric Key	00000007
Transparent RSA Private Key	0000000A
Transparent RSA Public Key	0000000B
Transparent EC Private Key	00000014
Transparent EC Public Key	00000015
PKCS#12	00000016
扩展	8XXXXXXX

6.5.3.2.4 封装方法枚举

封装方式枚举，如表 257 所示。

表 257 封装方法

名称	值
Encrypt	00000001
MAC/sign	00000002
Encrypt then MAC/sign	00000003
MAC/sign then encrypt	00000004
扩展	8XXXXXXX

6.5.3.2.5 推荐曲线枚举

推荐曲线枚举，如表 258 所示。

表 258　推荐曲线

名称	值
SM2	00001045
扩展	8XXXXXXX

6.5.3.2.6　证书类型枚举

证书类型枚举，如表 259 所示。

表 259　证书类型

名称	值
X.509	00000001
扩展	8XXXXXXX

6.5.3.2.7　数字签名算法枚举

数字签名算法枚举，如表 260 所示。

表 260　数字签名算法

名称	值
SM3withSM2	00001001

6.5.3.2.8　拆分密钥方法枚举

拆分密钥方法枚举，如表 261 所示。

表 261　拆分密钥方法

名称	值
XOR	00000001
Polynomial Sharing GF(2^{16})	00000002
Polynomial Sharing Prime Field	00000003
Polynomial Sharing GF(2^{8})	00000004
扩展	8XXXXXXX

6.5.3.2.9　秘密数据类型枚举

秘密数据类型枚举，如表 262 所示。

表 262　秘密数据类型

名称	值
Password	00000001
Seed	00000002
扩展	8XXXXXXX

6.5.3.2.10　不透明数据类型枚举

不透明数据类型枚举，如表 263 所示。

表 263　不透明数据类型

名称	值
扩展	8XXXXXXX

6.5.3.2.11　名称类型枚举

名称类型枚举，如表 264 所示。

表 264　名称类型

名称	值
Uninterpreted Text String	00000001
URI	00000002
扩展	8XXXXXXX

6.5.3.2.12　对象类型枚举

对象类型枚举，如表 265 所示。

表 265　对象类型

名称	值
Certificate	00000001
Symmetric Key	00000002
Public Key	00000003
Private Key	00000004
Split Key	00000005
Secret Data	00000007
Opaque Object	00000008
扩展	8XXXXXXX

6.5.3.2.13 密码算法枚举

密码算法枚举，如表 266 所示。

表 266 密码算法

名称	值
RSA	00000004
One Time Pad	0000001B
SM1	00001001
SM2	00001002
SM3	00001003
SM4	00001004
SM7	00001005
SM9	00001006
ZUC	00001007
HMAC-SM3	00001008
扩展	8XXXXXXX

6.5.3.2.14 分组密码加密模式枚举

分组密码加密模式枚举，如表 267 所示。

表 267 分组密码加密模式

名称	值
CBC	00000001
ECB	00000002
PCBC	00000003
CFB	00000004
OFB	00000005
CTR	00000006
CMAC	00000007
CCM	00000008
GCM	00000009
CBC-MAC	0000000A
XTS	0000000B
扩展	8XXXXXXX

6.5.3.2.15 填充方法枚举

填充方式枚举，如表 268 所示。

表 268　填充方法

名称	值
None	00000001
OAEP	00000002
PKCS5	00000003
SSL3	00000004
Zeros	00000005
ISO 10126	00000007
PKCS1 v1.5	00000008
PSS	0000000A
扩展	8XXXXXXX

6.5.3.2.16　杂凑算法枚举

杂凑算法枚举，如表 269 所示。

表 269　杂凑算法

名称	值
SM3	00001001
扩展	8XXXXXXX

6.5.3.2.17　密钥角色类型枚举

密钥角色型枚举，如表 270 所示。

表 270　密钥角色类型

名称	值
BDK	00000001
CVK	00000002
DEK	00000003
MKAC	00000004
MKSMC	00000005
MKSMI	00000006
MKDAC	00000007
MKDN	00000008
MKCP	00000009
MKOTH	0000000A

表 270　密钥角色类型（续）

名称	值
KEK	0000000B
MAC16609	0000000C
MAC97971	0000000D
MAC97972	0000000E
MAC97973	0000000F
MAC97974	00000010
MAC97975	00000011
ZPK	00000012
PVKIBM	00000013
PVKPVV	00000014
PVKOTH	00000015
DUKPT	00000016
IV	00000017
TRKBK	00000018
扩展	8XXXXXXX

6.5.3.2.18　状态枚举

状态枚举，如表 271 所示。

表 271　状态

名称	值
Pre-Active	00000001
Active	00000002
Deactivated	00000003
Compromised	00000004
Destroyed	00000005
Destroyed Compromised	00000006
扩展	8XXXXXXX

6.5.3.2.19　注销原因代码枚举

注销原因代码枚举，如表 272 所示。

表 272　注销原因代码

名称	值
Unspecified	00000001
Key Compromise	00000002
CA Compromise	00000003
Affiliation Changed	00000004
Superseded	00000005
Cessation of Operation	00000006
Privilege Withdrawn	00000007
扩展	8XXXXXXX

6.5.3.2.20　链接类型枚举

链接类型枚举，如表 273 所示。

表 273　链接类型

名称	值
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
Parent Link	00000108
Child Link	00000109
Previous Link	0000010A
Next Link	0000010B
PKCS#12 Certificate Link	0000010C
PKCS#12 Password Link	0000010D
扩展	8XXXXXXX

6.5.3.2.21　派生方法枚举

派生方法枚举，如表 274 所示。

表 274　派生方法

名称	值
PBKDF2	00000001
HASH	00000002
HMAC	00000003
ENCRYPT	00000004
Asymmetric Key	00000008
扩展	8XXXXXXX

6.5.3.2.22　证书请求类型枚举

证书请求类型枚举，如表 275 所示。

表 275　证书请求类型

名称	值
CRMF	00000001
PKCS＃10	00000002
PEM	00000003
扩展	8XXXXXXX

6.5.3.2.23　有效指标枚举

有效指标枚举，如表 276 所示。

表 276　有效指标

名称	值
Valid	00000001
Invalid	00000002
Unknown	00000003
扩展	8XXXXXXX

6.5.3.2.24　查询功能枚举

查询功能枚举，如表 277 所示。

表 277　查询功能

名称	值
Query Operations	00000001
Query Objects	00000002
Query Server Information	00000003
Query Application Namespaces	00000004
Query Extension List	00000005
Query Extension Map	00000006
Query Attestation Types	00000007
Query RNGs	00000008
Query RNGs	00000008
Query Validations	00000009
Query Profiles	0000000A
Query Capabilities	0000000B
Query Client Registration Methods	0000000C
扩展	8XXXXXXX

6.5.3.2.25　取消结果枚举

取消结果枚举，如表 278 所示。

表 278　取消结果

名称	值
Canceled	00000001
Unable to Cancel	00000002
Completed	00000003
Failed	00000004
Unavailable	00000005
扩展	8XXXXXXX

6.5.3.2.26　推送功能枚举

推送功能枚举，如表 279 所示。

表 279　推送功能

名称	值
New	00000001
Replace	00000002
扩展	8XXXXXXX

6.5.3.2.27 操作类型枚举

操作类型枚举，如表 280 所示。

表 280 操作类型

名称	值
Create	00000001
Create Key Pair	00000002
Register	00000003
Re-key	00000004
Derive Key	00000005
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
Validate	00000017
Query	00000018
Cancel	00000019
Poll	0000001A
Notify	0000001B
Put	0000001C
Re-key Key Pair	0000001D
Discover Versions	0000001E

表 280　操作类型（续）

名称	值
Encrypt	0000001F
Decrypt	00000020
Sign	00000021
Signature Verify	00000022
MAC	00000023
MAC Verify	00000024
RNG Retrieve	00000025
HASH	00000027
Create Split Key	00000028
Join Split Key	00000029
Import	0000002A
Export	0000002B
扩展	8XXXXXXX
Re-key Key Pair	0000001D
Discover Versions	0000001E
Encrypt	0000001F
Decrypt	00000020
Sign	00000021
Signature Verify	00000022
MAC	00000023
MAC Verify	00000024
RNG Retrieve	00000025
HASH	00000027
Create Split Key	00000028
Join Split Key	00000029
Import	0000002A
Export	0000002B
扩展	8XXXXXXX

6.5.3.2.28　结果状态枚举

结果状态枚举，如表 281 所示。

表 281　结果状态

名称	值
Success	00000000
Operation Failed	00000001
Operation Pending	00000002
Operation Undone	00000003
扩展	8XXXXXXX

6.5.3.2.29　结果原因枚举

结果原因枚举，如表 282 所示。

表 282　结果原因

名称	值
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
Application Namespace Not Supported	0000000F
Key Format Type Not Supported	00000010
Key Compression Type Not Supported	00000011
Encoding Option Error	00000012
Key Value Not Present	00000013
Attestation Required	00000014
Attestation Failed	00000015

6.5.3.2.30 批处理错误延续性枚举

批处理错误延续性枚举，如表 283 所示。

表 283 批处理错误延续性

名称	值
Continue	00000001
Stop	00000002
Undo	00000003
扩展	8XXXXXXX

6.5.3.2.31 使用限制单位枚举

使用限制单位枚举，如表 284 所示。

表 284 使用限制单位

名称	值
Byte	00000001
Object	00000002
扩展	8XXXXXXX

6.5.3.2.32 编码选项枚举

编码选项枚举，如表 285 所示。

表 285 编码选项

名称	值
No Encoding	00000001
TTLV Encoding	00000002
扩展	8XXXXXXX

6.5.3.2.33 对象组成员枚举

对象组成员枚举，如表 286 所示。

表 286 对象组成员

名称	值
Group Member Fresh	00000001
Group Member Default	00000002
扩展	8XXXXXXX

6.5.3.2.34 备选名称类型枚举

备选名称类型枚举，如表 287 所示。

表 287 备选名称类型

名称	值
Uninterpreted Text String	00000001
URI	00000002
Object Serial Number	00000003
Email Address	00000004
DNS Name	00000005
X.500 Distinguished Name	00000006
IP Address	00000007
扩展	8XXXXXXX

6.5.3.2.35 密钥值位置类型枚举

密钥值位置类型枚举，如表 288 所示。

表 288 密钥值位置类型

名称	值
Uninterpreted Text String	00000001
URI	00000002
扩展	8XXXXXXX

6.5.3.2.36 认证类型枚举

认证类型枚举，如表 289 所示。

表 289 认证类型

名称	值
TPM Quote	00000001
TCG Integrity Report	00000002
SAML Assertion	00000003
扩展	8XXXXXXX

6.5.3.2.37 RNG 算法枚举

RNG 算法枚举，如表 290 所示。

表 290　RNG 算法

名称	值
Unspecified	00000001
扩展	8XXXXXXX

6.5.3.2.38　验证机构类型枚举

验证机构类型枚举，如表 291 所示。

表 291　验证机构类型

名称	值
Unspecified	00000001
Common Criteria	00000003
扩展	8XXXXXXX

6.5.3.2.39　验证类型枚举

验证类型枚举，如表 292 所示。

表 292　验证类型

名称	值
Unspecified	00000001
Hardware	00000002
Software	00000003
Firmware	00000004
Hybrid	00000005
扩展	8XXXXXXX

6.5.3.2.40　配置文件名枚举

配置文件名枚举，如表 293 所示。

表 293　配置文件名

名称	值
Baseline Server Basic KMIP v1.4	00000079
Baseline Server TLS v1.2 KMIP v1.4	0000007A
Baseline Client Basic KMIP v1.4	0000007B
Baseline Client TLS v1.2 KMIP v1.4	0000007C
HTTPS Client KMIP v1.4	00000097
HTTPS Server KMIP v1.4	00000098
扩展	8XXXXXXX

配置文件说明见附录 D

6.5.3.2.41 解封装模式枚举

解封装模式枚举，如表 294 所示。

表 294 解封装模式

名称	值
Unspecified	00000001
Processed	00000002
Not Processed	00000003
扩展	8XXXXXXX

6.5.3.2.42 销毁操作枚举

销毁操作枚举，如表 295 所示。

表 295 销毁操作

名称	值
Unspecified	00000001
Key Material Deleted	00000002
Key Material Shredded	00000003
Meta Data Deleted	00000004
Meta Data Shredded	00000005
Deleted	00000006
Shredded	00000007
扩展	8XXXXXXX

6.5.3.2.43 粉碎算法枚举

粉碎算法枚举，如表 296 所示。

表 296 粉碎算法

名称	值
Unspecified	00000001
Cryptographic	00000002
Unsupported	00000003
扩展	8XXXXXXX

6.5.3.2.44 RNG 模式枚举

RNG 模式枚举，如表 297 所示。

表 297　RNG 模式

名称	值
Unspecified	00000001
扩展	8XXXXXXX

6.5.3.2.45　客户端注册方法枚举

客户端注册方法枚举，如表 298 所示。

表 298　客户端注册方法

名称	值
Unspecified	00000001
Server Pre-Generated	00000002
Server On-Demand	00000003
Client Generated	00000004
Client Registered	00000005
扩展	8XXXXXXX

6.5.3.2.46　密钥封装类型枚举

密钥封装类型枚举，如表 299 所示。

表 299　密钥封装类型

名称	值
Not Wrapped	00000001
As Registered	00000002
扩展	8XXXXXXX

6.5.3.3　位掩码

6.5.3.3.1　密码用途掩码

密码用途掩码，如表 300 所示。

表 300　密码用途掩码

名称	值
Sign	00000001
Verify	00000002
Encrypt	00000004

表 300　密码用途掩码（续）

名称	值
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
扩展	XXX00000

6.5.3.3.2　存储状态掩码

存储状态掩码，如表 301 所示。

表 301　存储状态掩码

名称	值
On-line storage	00000001
Archival storage	00000002
扩展	XXXXXXX0

7　安全要求

7.1　密码算法

密码算法应采用国家密码管理部门批准的算法，宜使用 SM 系列密码算法。

如果签名算法使用 SM2 算法，应符合 GB/T 32918(所有部分)和 GB/T 35276。

如果密码杂凑算法使用 SM3 算法，应符合 GB/T 32905。

如果机密算法使用 SM4 算法，应符合 GB/T 32907。

7.2 密钥生成

密钥的生成是密钥管理中最基本操作，生成密钥过程和生成的密钥满足以下要求：

a) 应在安全环境中产生密钥，防止任何形式的泄露；

b) 密钥长度可根据被保护数据类型和安全期的不同有所区别；

c) 应避免弱密钥，满足随机性和不可预测性，随机性应符合 GB/T 32915；

d) 不同级别或不同类别的密钥其产生机制可有所区别。

7.3 存储安全

用户可以选择将私钥、对称密钥等敏感数据对象存储在硬件密码设备中，或者采用其他的安全措施。

主密钥或根密钥的安全性非常重要，应存储在硬件密码设备中，可采用秘密共享技术（密钥拆分）实现对主密钥或根密钥的安全管理。

7.4 传输安全

密钥客户端和密钥管理服务端应建立和保持安全信道，应确保安全信道的机密性和完整性。

密钥客户端应验证密钥管理服务端身份可靠性。

密钥管理服务端可根据安全需要验证密钥客户端身份的可靠性。

密钥客户端和密钥管理服务端通信应遵循 GM/T 0024 的规定。

7.5 身份认证

用于服务端和客户端进行身份认证的机制不是消息定义的一部分，而是外部的协议（如，客户端与服务端的安全通信协议）。

凭证（见 6.2.2.2）用于识别访问者身份，或用于对客户端的身份认证。

凭证可与建立安全信道时的客户端证书关联，以提高身份认证的安全性。

7.6 访问控制

密钥对象等只能允许授权给合法用户或应用进行操作，需要对访问者进行身份认证、对操作权限进行审核，进而确定访问者是否具备操作该对象的权限。

对象可根据安全需要设置敏感和始终敏感属性。

对象的访问者权限由创建密钥对象操作的消息中所包含的凭证（见 6.2.2.2）指定。

对象的操作权限由密码用途掩码（见 6.3.16）属性标记。不同层次或长度的密钥根据使用频率或使用范围确定相应的使用期限（见 6.3.17），或者设置不同的使用限制（见 6.3.18）属性。

部分操作（注销、销毁、归档、恢复、导入、导出等操作）应由获得安全授权的操作员才能执行。

附 录 A
（资料性）
标准应用示例

A.1 应用示例

密钥管理互操作协议应用示例如图 A.1 所示。

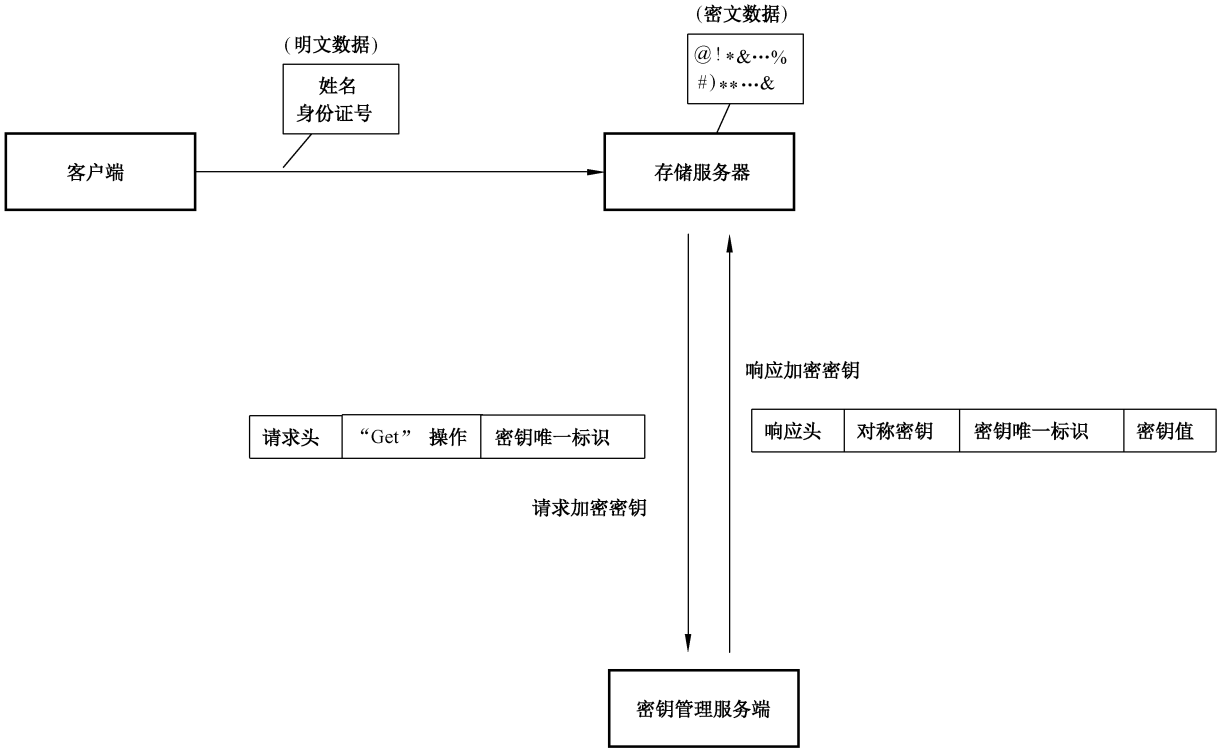


图 A.1 密钥管理互操作协议应用示例

客户端向存储服务器发送用户注册消息，请求消息中包含用户姓名、电话和身份证号等敏感信息。存储服务器接收客户端发送的消息，并调用密钥管理服务端发送 KMIP 协议报文向密钥管理服务端获取密钥。

密钥管理服务端接收 KMIP 请求，并认证存储服务器身份后使用 KMIP 协议对要响应的密钥封装后进行返回。KMIP 定义了用于交换密钥获取消息和其他密钥管理消息的标准格式。

存储服务接收密钥管理服务端的 KMIP 响应报文，解析协议中密钥，并调用 HSM 等硬件密码模块对用户注册信息进行加密后存储。

A.2 应用场景

本文件作为加密系统客户端与密钥管理服务端之间的通信标准，主要应用于加密系统加密密钥生命周期管理和统一密钥管理协议等场景。

加密系统密钥生命周期管理应用场景如图 A.2 所示。

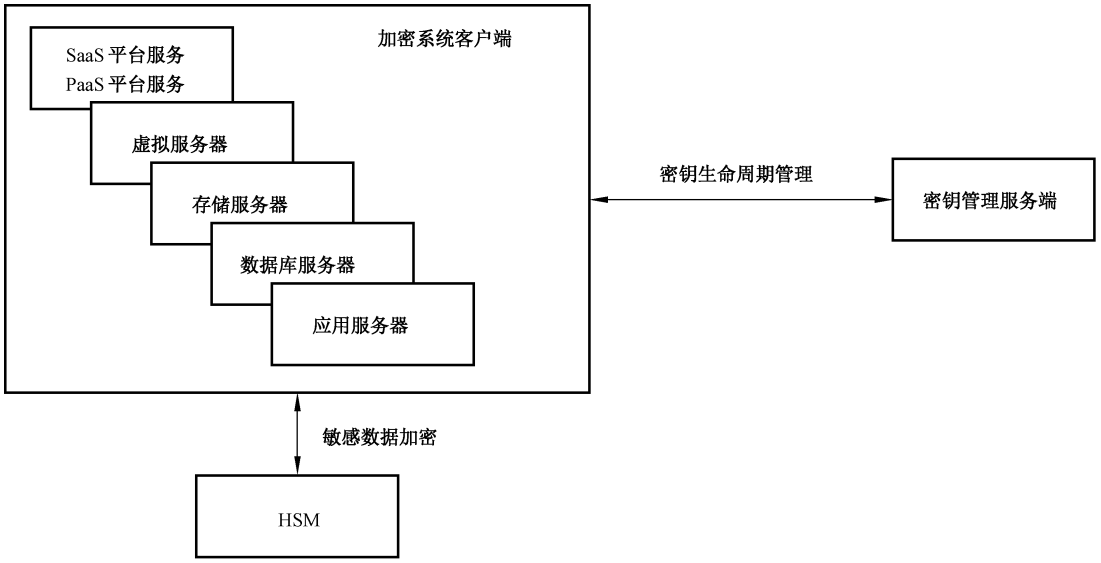


图 A.2　加密系统密钥生命周期管理

应用服务器、数据库服务器、存储服务器及云服务平台等环境中的敏感数据通过加密密钥进行保护，密钥管理服务端主要应用于如上环境加密密钥的生成、下发、注销及销毁等生命周期管理操作，解决加密系统中静态数据机密性问题。

加密系统统一密钥管理协议应用场景如图 A.3 所示。

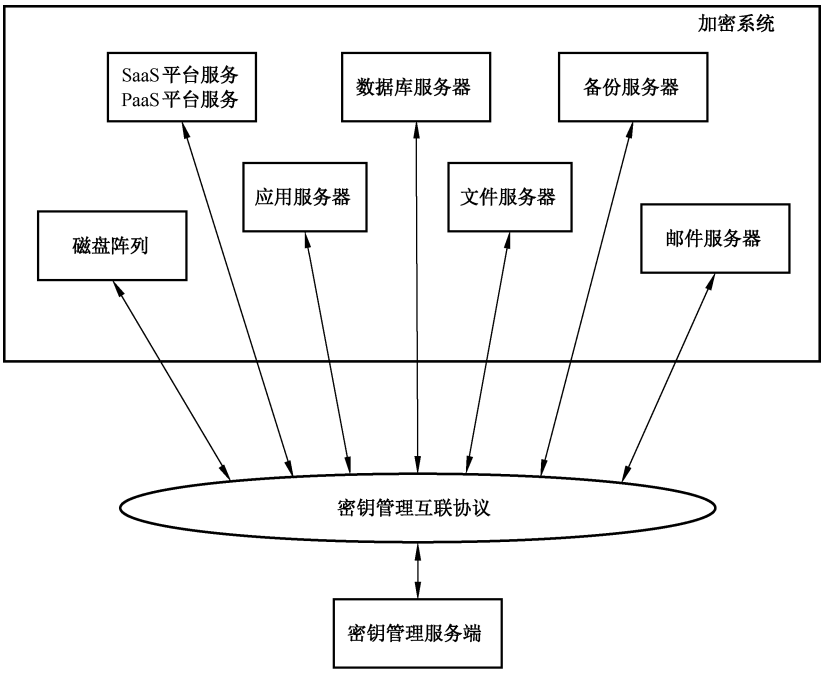


图 A.3　加密系统统一密钥管理协议

应用服务器、数据库服务器、存储服务器及云服务平台等环境中的敏感数据通过加密密钥进行保护，不同环境系统使用统一的密钥管理互操作协议连接密钥管理服务端进行加密密钥的生成及下发操作。通过加密系统和密钥管理服务之间通信的统一协议，解决了需要使用密钥的加密系统客户端与生成和管理这些密钥的密钥管理服务端之间的通信标准化问题。

附 录 B
（规范性）
TTLV 编码

B.1 概述

TTLV 方案编码的每个数据对象都包含四个项，分别为：项标签、项类型、项长度和项值。

B.2 项标签

项标签是一个三字节的二进制无符号整数，大端字节序，其中包含一个数字，用于指定 TTLV 对象表示的特定协议字段或对象。为了简化调试，并确保更容易检测到格式错误的消息，所有标记都包含十六进制中的值 42 或十六进制值 54 作为高位（第一个）字节。由本规范定义的标签在第一个字节中包含十六进制 42。在本说明书中允许但未定义的标签包含第一个字节中的值为十六进制 54。项标签列表在 6.5.3.1 进行了定义。

B.3 项类型

项类型是一个字节，包含一个指定数据对象之数据类型的编码值，如表 B.1 所示。

表 B.1 项类型值

数据类型	十六进制的编码值
结构	01
整型	02
长整型	03
大整数	04
枚举	05
布尔	06
文本串	07
字节串	08
日期-时间	09
间隔	0A

B.4 项长度

项长度是一个 32 位的二进制整数，大端字节序，包含项值中的字节数，如表 B.2 所示。

表 B.2　项长度值

数据类型	长度
结构	变长,8 的整数倍
整型	4
长整型	8
大整数	变长,8 的整数倍
枚举	4
布尔	8
文本串	变长
字节串	变长
日期-时间	8
间隔	4

如果项类型是结构,则项长度是该结构所含所有子项的总长,其中包含任何填充。如果项类型是整型、枚举型、文本串、字节串或间隔,则项长度是除填充字节之外的字节数。文本串和字节串要用最少的字节填充在项值之后,以达到 8 字节的倍数。整型、枚举型、间隔要用四字节填充到项值之后。

B.5　项值

项值是一个包含数据项的值的字节序列,具体取决于类型:

——整数被编码为 4 字节长(32 位)二进制有符号数,以 2 的补码表示,大端字节序;

——长整数被编码为 8 字节长(64 位)二进制符号,以 2 的补码表示,大端字节序;

——大整数被编码为 8 位字节的序列,以二进制补码表示,大端字节序。如果序列的长度不是八个字节的倍数,那么大整数应使用最小数量的前导符号扩展字节进行填充,以使长度达到八个字节的倍数。这些填充字节是项值的一部分,应在项长度中计数;

——枚举编码为四字节长(32 位)二进制无符号数字,大端字节序。本文件中允许但未定义的“扩展”,在第一个字节的前四位中包含十六进制的数值 8;

——布尔值编码为一个八字节值,应包含十六进制值 0000000000000000,表示布尔值 False,或十六进制值 0000000000000001,大端字节序,表示布尔值 True;

——文本串是根据 UTF-8 编码标准对字符值进行编码的字节序列。在此类字符串的末尾不应有空结束;

——字节串是包含单个未被指定的八位二进制值的字节序列,可视为以相同的顺序排列;

——日期-时间值是以长整数编码的 POSIX 时间值;

——间隔编码为四字节长(32 位)二进制无符号数,大端字节序。精度是 1 s。

结构值被编码为结构元素的级联编码。本文件定义的所有结构都应按照其各自结构描述中出现的顺序对其所有字段进行编码。

B.6　TTLV 编码示例

假设这些示例是对标签为 420020 的协议对象进行编码。这些示例以十六进制符号表示为字节序列:

——一个包含十进制值 8 的整数:

42 00 20 | 02 | 00 00 00 04 | 00 00 00 08 00 00 00 00

——一个包含十进制值 123456789000000000 的长整数：

42 00 20 | 03 | 00 00 00 08 | 01 B6 9B 4B A5 74 92 00

——一个包含十进制值 12345678900000000000000000000 的大整数：

42 00 20 | 04 | 00 00 00 10 | 00 00 00 00 03 FD 35 EB 6B C2 DF 46 18 08 00 00

——枚举值 255：

42 00 20 | 05 | 00 00 00 04 | 00 00 00 FF 00 00 00 00

——一个值为 True 的布尔值：

42 00 20 | 06 | 00 00 00 08 | 00 00 00 00 00 00 00 01

——一个值为“Hello World”的文本串：

42 00 20 | 07 | 00 00 00 0B | 48 65 6C 6C 6F 20 57 6F 72 6C 64 00 00 00 00 00

——值为{0x01,0x02,0x03}的字节串：

42 00 20 | 08 | 00 00 00 03 | 01 02 03 00 00 00 00 00

——日期-时间，包含值为 2008 年 3 月 14 日星期五，11:56:40 GMT：

42 00 20 | 09 | 00 00 00 08 | 00 00 00 00 47 DA 67 F8

——一个间隔，包含 10 天的值：

42 00 20 | 0A | 00 00 00 04 | 00 0D 2F 00 00 00 00 00

——包含枚举的结构，值为 254，后跟整数，值 255，分别具有标签 420004 和 420005：

42 00 20 | 01 | 00 00 00 20 | 42 00 04 | 05 | 00 00 00 04 | 00 00 00 FE 00 00 00 00 | 42 00 05 | 02 | 00 00 00 04 | 00 00 00 FF 00 00 00 00

附 录 C
（规范性）
错误处理

C.1 概述

本附录详细说明检测到的错误返回的具体结果原因。

C.2 一般错误

当服务端或客户端收到任何协议消息（服务端到客户端的响应操作）时，可能会发生一些错误，如表 C.1 所示。

表 C.1 一般错误

错误定义	结果状态	结果原因
主版本不匹配	响应消息包含协议头和没有操作的批处理项，但结果状态字段需要设置为“Operation Failed”	Invalid Message
解析批处理项或批处理项中有效载荷时出错	批处理项失败；结果状态为“Operation Failed”	Invalid Message
协议头/批处理项/有效载荷中多次包含相同的字段	结果状态为“Operation Failed”	Invalid Message
主版本相同，次版本不同；未知字段/服务器不理解的字段	忽略未知字段，其余正常处理	N/A
主次版本相同，未知字段	结果状态为“Operation Failed”	Invalid Field
客户端不被准许执行指定的操作	结果状态为“Operation Failed”	Permission Denied
超出最大响应长度	结果状态为“Operation Failed”	Response Too Large
服务器不支持操作	结果状态为“Operation Failed”	Operation Not Supported
消息扩展结构中的临界指示器设置为 True，但服务端不理解扩展	结果状态为“Operation Failed”	Feature Not Supported
无法解析消息	响应消息包含协议头和没有操作的批处理项，但结果状态字段需要设置为“Operation Failed”	Invalid Message
操作需要认证数据，而客户端未提供，且客户端将认证能力指示符设置为 True	结果状态为“Operation Failed”	Attestation Required
操作需要认证数据，而客户端未提供，且客户端将认证能力指示器设置为 False	结果状态为“Operation Failed”	Permission Denied
操作需要认证数据，而客户提供的认证数据不能被验证	结果状态为“Operation Failed”	Attestation Failed

C.3 创建错误

创建错误，如表 C.2 所示。

表 C.2 创建错误

错误定义	结果状态	结果原因
对象类型无法识别	Operation Failed	Invalid Field
请求不存在的模板	Operation Failed	Item Not Found
指定的属性值不正确	Operation Failed	Invalid Field
创建密码对象时出错	Operation Failed	Cryptographic Failure
试图设置的实例数量超出服务器对多实例的支持	Operation Failed	Index Out of Bounds
尝试创建与现有对象具有相同 Name 属性值的新对象	Operation Failed	Invalid Field
不支持特定应用命名空间，而且如果从客户端请求中省略，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
模板对象已存档	Operation Failed	Object Archived

C.4 创建密钥对错误

创建密钥对错误，如表 C.3 所示。

表 C.3 创建密钥对错误

错误定义	结果状态	结果原因
不存在的模板被请求	Operation Failed	Item Not Found
不正确的属性值被指定	Operation Failed	Invalid Field
创建密码对象时出错	Operation Failed	Cryptographic Failure
尝试创建和已有对象相同 Name 属性的新对象	Operation Failed	Invalid Field
尝试设置比具有多实例属性的服务端支持实例数量更多的实例	Operation Failed	Index Out of Bounds
必备的报文字段丢失	Operation Failed	Invalid Message
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
模板对象被归档	Operation Failed	Object Archived

C.5 注册错误

注册错误，如表 C.4 所示。

表 C.4 注册错误

错误定义	结果状态	结果原因
对象类型无法识别	Operation Failed	Invalid Field
对象类型字段和导入时提供的密码对象的实际类型不匹配	Operation Failed	Invalid Field
不存在的模板被请求	Operation Failed	Item Not Found
不正确的属性值被指定	Operation Failed	Invalid Field
尝试使用模板结构注册包含名称属性的新模板对象	Operation Failed	Invalid Field
尝试创建和已有对象相同名称属性的新对象	Operation Failed	Invalid Field
尝试设置比具有多实例属性的服务端支持实例数量更多的实例	Operation Failed	Index Out of Bounds
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
模板对象被归档	Operation Failed	Object Archived
密钥封装包含属性名称时，不准许的编码选项	Operation Failed	Encoding Option Error
密钥格式类为 PKCS＃12，但缺少或者有重复的 PKCS＃12 密码链接	Operation Failed	Invalid Field
密钥格式类为 PKCS＃12，但 PKCS＃12 密码链接不包含 Secret Data 对象的唯一标识符或者 Secret Data 的类型不是密码	Operation Failed	Invalid Field

C.6 更新密钥错误

更新密钥错误，如表 C.5 所示。

表 C.5 更新密钥错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的密码对象无法执行密钥更新	Operation Failed	Permission Denied
激活日期、生效日期、失效日期和停用日期不能同时指定偏移字段	Operation Failed	Invalid Message
更新密钥时发生错误	Operation Failed	Cryptographic Failure

表 C.5　更新密钥错误（续）

错误定义	结果状态	结果原因
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
对象被归档	Operation Failed	Object Archived
由于没有为现有密钥指定激活日期，无法指定新的进程开始、保护停止和停用日期的偏移字段	Operation Failed	Illegal Operation
服务端不存在密钥值	Operation Failed	Key Value Not Present

C.7　更新密钥对错误

更新密钥对错误，如表 C.6 所示。

表 C.6　更新密钥对错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的密码对象无法执行密钥更新	Operation Failed	Permission Denied
激活日期、生效日期、失效日期和停用日期不能同时指定偏移字段	Operation Failed	Invalid Message
更新密钥时发生错误	Operation Failed	Cryptographic Failure
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
对象被归档	Operation Failed	Object Archived
由于没有为现有密钥指定激活日期，无法指定新的进程开始、保护停止和停用日期的偏移字段	Operation Failed	Illegal Operation
服务端不存在密钥值	Operation Failed	Key Value Not Present

C.8　派生密钥错误

派生密钥错误，如表 C.7 所示。

表 C.7　派生密钥错误

错误定义	结果状态	结果原因
指定的一个或者多个对象不存在	Operation Failed	Item Not Found
指定的一个或者多个对象的类型不正确	Operation Failed	Invalid Field
不存在的模板被请求	Operation Failed	Item Not Found
派生方法无效	Operation Failed	Invalid Field
派生参数无效	Operation Failed	Invalid Field
派生数据和秘密数据提供不确定的派生数据	Operation Failed	Invalid Message
指定的属性值不正确	Operation Failed	Invalid Field
指定的一个或者多个对象不能用于派生新的密钥	Operation Failed	Invalid Field
尝试派生和已有对象相同 Name 属性值的派生密钥	Operation Failed	Invalid Field
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
一个或者多个对象被归档	Operation Failed	Object Archived
在派生时，指定的长度超出派生方法的输出或者其他加密错误	Operation Failed	Cryptographic Failure
服务端不存在密钥值	Operation Failed	Key Value Not Present

C.9　认证错误

认证错误，如表 C.8 所示。

表 C.8　认证错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象无法认证	Operation Failed	Permission Denied
证书请求中不包含已签名的证书请求在指定的证书请求类型	Operation Failed	Invalid Field
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
对象被归档	Operation Failed	Object Archived

C.10 重新认证错误

重新认证错误，如表 C.9 所示。

表 C.9 重新认证错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象无法认证	Operation Failed	Permission Denied
证书请求中不包含已签名的证书请求在指定的证书请求类型	Operation Failed	Invalid Field
激活日期、生效日期、失效日期和停用日期不能同时指定偏移字段	Operation Failed	Invalid Message
不支持特定的应用程序命名空间，若客户端请求忽略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
对象被归档	Operation Failed	Object Archived

C.11 定位错误

定位错误，如表 C.10 所示。

表 C.10 定位错误

错误定义	结果状态	结果原因
不存在的属性，服务端无法理解的属性或者不存在的模板被请求	Operation Failed	Invalid Field

C.12 检查错误

检查错误，如表 C.11 所示。

表 C.11 检查错误

错误定义	结果状态	结果原因
对象不存在	Operation Failed	Item Not Found
对象已归档	Operation Failed	Object Archived
无法对此对象进行检查	Operation Failed	Illegal Operation
客户端不准许根据指定的属性使用对象	Operation Failed	Permission Denied

C.13 获取错误

获取错误，如表 C.12 所示。

表 C.12　获取错误

错误定义	结果状态	结果原因
对象不存在	Operation Failed	Item Not Found
包裹密钥不存在	Operation Failed	Item Not Found
具有加密密钥信息的对象存在，但它不是密钥	Operation Failed	Illegal Operation
具有加密密钥信息的对象存在，但不能用于包裹	Operation Failed	Permission Denied
具有 MAC/签名密钥信息的对象存在，但它不是密钥	Operation Failed	Illegal Operation
具有 MAC/签名密钥信息的对象存在，但不能用于 MAC/签名	Operation Failed	Permission Denied
对象存在，但不能提供所需的密钥格式类型和/或密钥压缩类型	Operation Failed	Key Format Type and/or Key Compression Type Not Supported
对象存在且不是模板，但服务端只具有此对象的属性	Operation Failed	Illegal Operation
与对象相关联的加密参数不存在或与加密密钥信息和/或签名密钥信息中提供的参数不匹配	Operation Failed	Item Not Found
对象被归档	Operation Failed	Object Archived
对象存在，但不能提供所需的编码选项	Operation Failed	Encoding Option Error
密钥封装规范包含属性名称时，不准许的编码选项	Operation Failed	Encoding Option Error
服务端不支持的密钥封装类型	Operation Failed	Not Supported
对象敏感	Operation Failed	Sensitive
对象不可提取	Operation Failed	Not Extractble

C.14　获取属性错误

获取属性错误，如表 C.13 所示。

表 C.13　获取属性错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
相同的属性名称出现不止一次	Operation Failed	Invalid Message
对象被归档	Operation Failed	Object Archived

C.15 获取属性列表错误

获取属性列表错误，如表 C.14 所示。

表 C.14 获取属性列表错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
对象被归档	Operation Failed	Object Archived

C.16 添加属性错误

添加属性错误，如表 C.15 所示。

表 C.15 添加属性错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
试图在只读属性上添加	Operation Failed	Permission Denied
试图添加此对象不支持的属性	Operation Failed	Permission Denied
指定的属性已经存在	Operation Failed	Illegal Operation
新属性包含属性索引	Operation Failed	Invalid Field
尝试添加与另一个对象已具有相同值的 Name 属性	Operation Failed	Illegal Operation
尝试向具有多个实例的属性添加新实例，但已达到实例上的服务端限制	Operation Failed	Index Out of Bounds
不支持特定应用程序命名空间，如果客户端请求中省略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
对象被归档	Operation Failed	Object Archived

C.17 修改属性错误

修改属性错误，如表 C.16 所示。

表 C.16 修改属性错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的属性不存在(它需要先添加)	Operation Failed	Invalid Field

表 C.16 修改属性错误（续）

错误定义	结果状态	结果原因
不存在匹配的属性实例	Operation Failed	Item Not Found
指定的属性是只读的	Operation Failed	Permission Denied
尝试将 Name 属性值设置为另一个对象已经使用的值	Operation Failed	Illegal Operation
不支持特定应用程序命名空间，如果客户端请求中省略了应用程序数据，则无法生成应用程序数据	Operation Failed	Application Namespace Not Supported
对象被归档	Operation Failed	Object Archived

C.18 删除属性错误

删除属性错误，如表 C.17 所示。

表 C.17 删除属性错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
尝试删除只读/REQUIRED 属性	Operation Failed	Permission Denied
不存在匹配的属性实例	Operation Failed	Item Not Found
不存在指定名称的属性	Operation Failed	Item Not Found
对象被归档	Operation Failed	Object Archived

C.19 获取租约错误

获取租约错误，如表 C.18 所示。

表 C.18 获取租约错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
服务端确定不准许为指定的密码对象发出新的租约	Operation Failed	Permission Denied
对象被归档	Operation Failed	Object Archived

C.20 获取使用配额错误

获取使用配额错误，如表 C.19 所示。

表 C.19　获取使用配额错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
对象没有使用限制属性，或者对象不能用于应用加密保护	Operation Failed	Illegal Operation
没有指定使用限制计数	Operation Failed	Invalid Message
对象被归档	Operation Failed	Object Archived
服务端无法授予请求的使用配额量	Operation Failed	Permission Denied

C.21　激活错误

激活错误，如表 C.20 所示。

表 C.20　激活错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
唯一标识符指向一个不能激活的模板或其他对象	Operation Failed	Illegal Operation
对象不处于预激活状态	Operation Failed	Permission Denied
对象被归档	Operation Failed	Object Archived

C.22　注销错误

注销错误，如表 C.21 所示。

表 C.21　注销错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
注销原因未得到承认	Operation Failed	Invalid Field
唯一标识符指向了不能被注销的模板或其他对象	Operation Failed	Illegal Operation
对象被归档	Operation Failed	Object Archived

C.23　销毁错误

销毁错误，如表 C.22 所示。

表 C.22　销毁错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
对象已被销毁	Operation Failed	Permission Denied
对象不处于预激活，已停用或受到失信状态	Operation Failed	Permission Denied
对象被归档	Operation Failed	Object Archived

C.24　归档错误

归档错误，如表 C.23 所示。

表 C.23　归档错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
对象已经存档	Operation Failed	Object Archived

C.25　恢复错误

恢复错误，如表 C.24 所示。

表 C.24　恢复错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found

C.26　验证证书错误

验证证书错误，如表 C.25 所示。

表 C.25　验证证书错误

错误定义	结果状态	结果原因
证书对象和唯一标识符的组合不能指向特定的证书列表	Operation Failed	Invalid Message
一个或多个对象被归档	Operation Failed	Object Archived

C.27　询问错误

不适用。

C.28 显示版本错误

不适用。

C.29 取消错误

不适用。

C.30 轮询错误

轮询错误，如表 C.26 所示。

表 C.26 轮询错误

错误定义	结果状态	结果原因
不存在具有指定的异步相关值的未完成的操作	Operation Failed	Item Not Found

C.31 加密错误

加密错误，如表 C.27 所示。

表 C.27 加密错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象不能用于加密	Operation Failed	Permission Denied
加密过程中的加密错误	Operation Failed	Cryptographic Failure
对象被归档	Operation Failed	Object Archived
密钥值不存在于服务端上	Operation Failed	Key Value Not Present
不存在具有指定相关值的未完成的操作	Operation Failed	Item Not Found

C.32 解密错误

解密错误，如表 C.28 所示。

表 C.28 解密错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象不能用于解密	Operation Failed	Permission Denied
解密过程中的解密错误	Operation Failed	Cryptographic Failure
对象被归档	Operation Failed	Object Archived
服务端上不存在该密钥值	Operation Failed	Key Value Not Present
不存在具有指定相关值的未完成的操作	Operation Failed	Item Not Found

C.33 签名错误

签名错误，如表 C.29 所示。

表 C.29 签名错误

错误定义	结果状态	结果原因
没有指定唯一标识符的对象存在	Operation Failed	Item Not Found
指定的对象不能用于签名	Operation Failed	Permission Denied
签名过程中的签名错误	Operation Failed	Cryptographic Failure
对象被归档	Operation Failed	Object Archived
服务端上不存在该密钥值	Operation Failed	Key Value Not Present
不存在具有指定相关值的未完成的操作	Operation Failed	Item Not Found

C.34 签名验证错误

签名验证错误，如表 C.30 所示。

表 C.30 签名验证错误

错误定义	结果状态	结果原因
指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象不能用于签名验证	Operation Failed	Permission Denied
签名验证过程中的验签错误	Operation Failed	Cryptographic Failure
对象被归档	Operation Failed	Object Archived
服务端上不存在该密钥值	Operation Failed	Key Value Not Present
不存在具有指定相关值的未完成的操作	Operation Failed	Item Not Found

C.35 MAC 计算错误

MAC 计算错误，如表 C.31 所示。

表 C.31 MAC 计算错误

错误定义	结果状态	结果原因
具有指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象不能用于计算 MAC	Operation Failed	Permission Denied
MAC 计算期间的加密错误	Operation Failed	Cryptographic Failure
对象已被归档	Operation Failed	Object Archived
指定的密钥值在服务端不存在	Operation Failed	Key Value Not Present
具有指定相关值的未完成操作不存在	Operation Failed	Item Not Found

C.36 MAC 验证错误

MAC 验证错误，如表 C.32 所示。

表 C.32 MAC 验证错误

错误定义	结果状态	结果原因
具有指定唯一标识符的对象不存在	Operation Failed	Item Not Found
指定的对象不能用于 MAC 验证	Operation Failed	Permission Denied
MAC 验证期间的加密错误	Operation Failed	Cryptographic Failure
对象被归档	Operation Failed	Object Archived
指定的密钥值在服务端不存在	Operation Failed	Key Value Not Present
具有指定相关值的未完成操作不存在	Operation Failed	Item Not Found

C.37 RNG 检索错误

RNG 检索错误，如表 C.33 所示。

表 C.33 RNG 检索错误

错误定义	结果状态	结果原因
RNG 检索期间的加密错误	Operation Failed	Cryptographic Failure

C.38 RNG 种子错误

RNG 种子错误，如表 C.34 所示。

表 C.34 RNG 种子错误

错误定义	结果状态	结果原因
RNG 种子(设置)期间的加密错误	Operation Failed	Cryptographic Failure

C.39 HASH 错误

HASH 错误，如表 C.35 所示。

表 C.35 HASH 错误

错误定义	结果状态	结果原因
HASH 计算错误	Operation Failed	Cryptographic Failure
不存在具有指定相关值的未完成的操作	Operation Failed	Item Not Found

C.40 创建拆分密钥错误

创建拆分密钥错误，如表 C.36 所示。

表 C.36　创建拆分密钥错误

错误定义	结果状态	结果原因
对象类型无法识别	Operation Failed	Invalid Field
请求中的模板不存在	Operation Failed	Item Not Found
指定的属性值不正确	Operation Failed	Invalid Field
创建密码对象时出错	Operation Failed	Cryptographic Failure
尝试设置的实例多于服务端所支持的数量	Operation Failed	Index Out of Bounds
尝试创建的对象与已存在对象具有相同的名称属性值	Operation Failed	Invalid Field
不支持特定应用程序命名空间，如果客户端请求中省略了该字段，则服务端无法生成应用程序数据字段	Operation Failed	Application Namespace Not Supported
模板对象被归档	Operation Failed	Object Archived
拆分密钥方法不支持	Operation Failed	Invalid Field
具有指定唯一标识符的对象不存在	Operation Failed	Item Not Found

C.41　拆分密钥合成错误

拆分密钥合成错误，如表 C.37 所示。

表 C.37　拆分密钥合成错误

错误定义	结果状态	结果原因
对象类型无法识别	Operation Failed	Invalid Field
请求中的模板不存在	Operation Failed	Item Not Found
指定的属性值不正确	Operation Failed	Invalid Field
创建密码对象时出错	Operation Failed	Cryptographic Failure
尝试设置的实例多于服务端所支持的数量	Operation Failed	Index Out of Bounds
尝试创建的新对象与现有对象具有相同的“名称”属性值	Operation Failed	Invalid Field
不支持特定应用程序命名空间，如果客户端请求中省略了该字段，则服务端无法生成应用程序数据字段	Operation Failed	Application Namespace Not Supported
模板对象被归档	Operation Failed	Object Archived
请求中的唯一标识符数量小于拆分密钥的阈值	Operation Failed	Cryptographic Failure
拆分密钥方法不支持	Operation Failed	Invalid Field
具有指定唯一标识符的对象不存在	Operation Failed	Item Not Found
一个或多个对象被归档	Operation Failed	Object Archived

C.42 导出错误

导出错误，如表 C.38 所示。

表 C.38 导出错误

错误定义	结果状态	结果原因
对象不存在	Operation Failed	Item Not Found
封装密钥不存在	Operation Failed	Item Not Found
具有加密密钥信息的对象，但不是密钥对象	Operation Failed	Illegal Operation
具有加密密钥信息的对象，但不能用于封装	Operation Failed	Permission Denied
具有 MAC/签名密钥信息的对象，但不是密钥对象	Operation Failed	Illegal Operation
具有 MAC/签名密钥信息的对象，但不能用于 MAC/签名	Operation Failed	Permission Denied
对象存在，但服务端无法提供需要的密钥格式类型或者密钥压缩类型	Operation Failed	Key Format Type and/or Key Compression Type Not Supported
与对象相关联的加密参数不存在，或与加密密钥信息和/或签名密钥信息中提供的参数不匹配	Operation Failed	Item Not Found
对象存在，但不能在所需的编码选项中提供	Operation Failed	Encoding Option Error
密钥封装规格包含属性名称时，编码选项不被允许	Operation Failed	Encoding Option Error
服务端不支持的密钥封装类型	Operation Failed	Not Supported

C.43 导入错误

导入错误，如表 C.39 所示。

表 C.39 导入错误

错误定义	结果状态	结果原因
“是否替代”为 false 或未指定时，替换在服务器中具有相同唯一标识符的现有对象	Operation Failed	Object Already Exists
对象类型无法识别	Operation Failed	Invalid Field
对象类型与提供的密码对象类型不匹配	Operation Failed	Invalid Field
指定的属性值不正确	Operation Failed	Invalid Field
尝试注册的新对象与现有对象具有相同“名称”属性值	Operation Failed	Invalid Field
尝试设置的实例多于服务端所支持的数量	Operation Failed	Index Out of Bounds

表 C.39　导入错误（续）

错误定义	结果状态	结果原因
不支持特定应用程序命名空间，如果客户端请求中省略了该字段，则服务端无法生成应用程序数据字段	Operation Failed	Application Namespace Not Supported
密钥封装规格包含属性名称时，编码选项不被准许	Operation Failed	Encoding Option Error
服务端不支持的字段	Operation Failed	Invalid Field

C.44　批处理项错误

当服务端处理的协议消息具有一个或多个批处理项时，可能会发生表 C.40 中这些错误。如果具有一个或多个批处理项的消息被正确解析，则应根据表 C.40，在响应消息中包含对请求中的批处理项的响应。

表 C.40　批处理项错误

错误定义	处理	结果原因
批处理项处理失败，并且批处理错误连续选项设置为停止	批处理项失败，结果状态设置为“Operation Failed”。对已处理的批处理项的响应是正常返回。对未处理的请求块的响应是不返回	请参阅上文表格中所涉及的，在批处理项中执行失败的操作
批处理项处理失败，并且批处理错误连续选项设置为继续	批处理项失败，结果状态设置为“Operation Failed”。对其他批处理项的响应是正常返回	请参阅上文表格中所涉及的，在批处理项中执行失败的操作
批处理项处理失败，并且批处理错误连续选项设置为撤销	批处理项失败，结果状态设置为“Operation Failed”。已处理的批次项目取消，并且他们的响应是返回撤销的结果状态	请参阅上文表格中所涉及的，在批处理项中执行失败的操作

附 录 D
（资料性）
配置文件示例

D.1 Baseline Server Basic KMIP v1.4

符合此配置文件的 KMIP 服务器实现：

a） 应支持本文件服务器端功能和编码定义；

b） 应支持 TLS 协商安全通道。

D.2 Baseline Server TLS v1.2 KMIP v1.4

符合此配置文件的 KMIP 服务器实现：

a） 应支持本文件服务器端功能和编码定义；

b） 应支持 TLS v1.2 协商安全通道。

D.3 Baseline Client Basic KMIP v1.4

符合此配置文件的 KMIP 客户端实现：

a） 应支持本文件客户端功能和编码定义；

b） 应支持 TLS 协商安全通道。

D.4 Baseline Client TLS v1.2 KMIP v1.4

符合此配置文件的 KMIP 客户端实现：

a） 应支持本文件客户端功能和编码定义；

b） 应支持 TLS v1.2 协商安全通道。

D.5 HTTPS Client KMIP v1.4

符合此配置文件的 KMIP 客户端实现：

a） 应支持本文件功能和编码定义；

b） 应支持使用 HTTP TLS [RFC2818]来协商安全通道；

c） 应支持如下 HTTPS 客户端条件：

1） 应使用 POST 请求方法；

2） 应该支持将值/kmip 作为目标 URI；

3） 如果消息编码是 TTLV，则应指定 Content-Type of “application/octet-stream”；

4） 如果消息编码是 XML，则应指定 Content-Type of “text/xml”；

5） 如果消息编码是 JSON，则应指定 Content-Type of “application/json”；

6） 应指定 Content-Length；

7） 应指定 Cache-Control 为“no-cache”；

8） 应以二进制格式发送 KMIP TTLV 消息作为 HTTP 请求的主体。

D.6 HTTPS Server KMIP v1.4

符合此配置文件的 KMIP 服务器端实现：

a） 应支持本文件功能和编码定义；

b) 应支持使用 HTTP TLS [RFC2818]来协商安全通道；

c) 应支持如下 HTTPS 服务端条件：

1) 如果 KMIP 响应可用，则返回 HTTP 响应代码 200；

2) 应该支持将值/kmip 作为目标 URI；

3) 如果消息编码是 TTLV，则应指定 Content-Type of “application/octet-stream”；

4) 如果消息编码是 XML，则应指定 Content-Type of “text/xml”；

5) 如果消息编码是 JSON，则应指定 Content-Type of “application/json”；

6) 应指定 Content-Length；

7) 应指定 Cache-Control 为“no-cache”；

8) 应以二进制格式发送 KMIP TTLV 消息作为 HTTP 请求的主体。

参 考 文 献

[1] [ECC-Brainpool] ECC Brainpool Standard Curves and Curve Generation v.1.0.19.10.2005, http://www.ecc-brainpool.org/download/Domain-parameters.pdf

[2] [FIPS180-4] Secure Hash Standard (SHS), FIPS PUB 186-4, March 2012, http://csrc.nist.gov/publications/fips/fips18-4/fips-180-4.pdf

[3] [FIPS186-4] Digital Signature Standard (DSS), FIPS PUB 186-4, July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[4] [FIPS197] Advanced Encryption Standard, FIPS PUB 197, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

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

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

[7] [ISO 16609] ISO, Banking—Requirements for message authentication using symmetric techniques, ISO 16609, 2012

[8] [ISO 9797-1] ISO/IEC, Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms using a block cipher, ISO/IEC 9797-1, 2011

[9] [KMIP-Prof] Key Management Interoperability Protocol Profiles Version 1.4. Edited by Tim Hudson and Robert Lockhart. Latest version: TBA

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

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

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

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

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

[15] [RFC1320] R. Rivest, The MD4 Message-Digest Algorithm, IETF RFC 1320, April 1992, http://www.ietf.org/rfc/rfc1320.txt

[16] [RFC1321] R. Rivest, The MD5 Message-Digest Algorithm, IETF RFC 1321, April 1992, http://www.ietf.org/rfc/rfc1321.txt

[17] [RFC1421] J. Linn, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, IETF RFC 1421, February 1993, http://www.ietf.org/rfc/rfc1421.txt

[18] [RFC1424] B. Kaliski, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, IETF RFC 1424, Feb 1993, http://www.ietf.org/rfc/rfc1424.txt

[19] [RFC2104] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997, http://www.ietf.org/rfc/rfc2104.txt

[20] [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels",

BCP 14,RFC 2119,March 1997.http://www.ietf.org/rfc/rfc2119.txt

[21] [RFC2898] B.Kaliski,PKCS #5:Password-Based Cryptography Specification Version 2.0,IETF RFC 2898,September 2000,http://www.ietf.org/rfc/rfc2898.txt

[22] [RFC2986] M.Nystrom and B.Kaliski,PKCS #10:Certification Request Syntax Specification Version 1.7,IETF RFC2986,November 2000,http://www.rfc-editor.org/rfc/rfc2986.txt

[23] [RFC3447] J.Jonsson,B.Kaliski,Public-Key Cryptography Standards (PKCS) #1:RSA Cryptography Specifications Version 2.1,IETF RFC 3447,Feb 2003,http://www.ietf.org/rfc/rfc3447.txt

[24] [RFC3629] F.Yergeau,UTF-8,a transformation format of ISO 10646,IETF RFC 3629,November 2003,http://www.ietf.org/rfc/rfc3629.txt

[25] [RFC3686] R.Housley,Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP),IETF RFC 3686,January 2004,http://www.ietf.org/rfc/rfc3686.txt

[26] [RFC4210] C.Adams,S.Farrell,T.Kause and T.Mononen,Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP),IETF RFC 4210,September 2005,http://www.ietf.org/rfc/rfc4210.txt

[27] [RFC4211] J.Schaad,Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF),IETF RFC 4211,September 2005,http://www.ietf.org/rfc/rfc4211.txt

[28] [RFC4880] J.Callas,L.Donnerhacke,H.Finney,D.Shaw,and R.Thayer,OpenPGP Message Format,IETF RFC 4880,November 2007,http://www.ietf.org/rfc/rfc4880.txt

[29] [RFC4949] R.Shirey,Internet Security Glossary,Version 2,IETF RFC 4949,August 2007,http://www.ietf.org/rfc/rfc4949.txt

[30] [RFC5208] B.Kaliski,Public Key Cryptographic Standards (PKCS) #8:Private-Key Information Syntax Specification Version 1.2,IETF RFC5208,May 2008,http://www.rfc-editor.org/rfc/rfc5208.txt

[31] [RFC5272] J.Schaad and M.Meyers,Certificate Management over CMS (CMC),IETF RFC 5272,June 2008,http://www.ietf.org/rfc/rfc5272.txt

[32] [RFC5280] D.Cooper,S.Santesson,S.Farrell,S.Boeyen,R.Housley,W.Polk,Internet X.509 Public Key Infrastructure Certificate,IETF RFC 5280,May 2008,http://www.ietf.org/rfc/rfc5280.txt

[33] [RFC5639] M.Lochter,J.Merkle,Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation,IETF RFC 5639,March 2010,http://www.ietf.org/rfc/rfc5639.txt

[34] [RFC6402] J.Schaad,Certificate Management over CMS (CMC) Updates,IETF RFC6402,November 2011,http://www.rfc-editor.org/rfc/rfc6402.txt

[35] [RFC6818] P.Yee,Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,IETF RFC6818,January 2013,http://www.rfc-editor.org/rfc/rfc6818.txt

[36] [SEC2] SEC 2:Recommended Elliptic Curve Domain Parameters,http://www.secg.org/collateral/sec2_final.pdf

[37] [SP800-38A] M.Dworkin,Recommendation for Block Cipher Modes of Operation-Methods and Techniques,NIST Special Publication 800-38A,December 2001,http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[38] [SP800-38B] M.Dworkin, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005, http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

[39] [SP800-38C] M.Dworkin, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, NIST Special Publication 800-38C, May 2004, http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

[40] [SP800-38D] M. Dworkin, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, Nov 2007, http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

[41] [SP800-38E] M.Dworkin, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices, NIST Special Publication 800-38E, January 2010, http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

[42] [SP800-56A] E.Barker, L.Chen, A.Roginsky and M.Smid, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A Revision 2, May 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

[43] [SP800-57-1] E.Barker, W.Barker, W.Burr, W.Polk, and M.Smid, Recommendations for Key Management-Part 1: General (Revision 3), NIST Special Publication 800-57 Part 1 Revision 3, July 2012, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

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

[45] [X.509] International Telecommunication Union (ITU)-T, X.509: Information technology-Open systems interconnection-The Directory: Public-key and attribute certificate frameworks, November 2008, http://www.itu.int/rec/recommendation.asp? lang=en&parent=T-REC-X.509-200811-1

[46] [X9.24-1] ANSI, X9.24-Retail Financial Services Symmetric Key Management-Part 1: Using Symmetric Techniques, 2009

[47] [X9.31] ANSI, X9.31: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), September 1998

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

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

[50] [X9.63] ANSI, X9.63: Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011

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

[52] [X9 TR-31] ANSI, X9 TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms, 2010

[53] [ISO/IEC 9945-2] The Open Group, Regular Expressions, The Single UNIX Specification version 2, 1997, ISO/IEC 9945-2:1993

[54] [KMIP-UG] Key Management Interoperability Protocol Usage Guide Version 1.4.Edited

by Judith Furlong.Latest version:TBA

[55] [KMIP-TC] Key Management Interoperability Protocol Test Cases Version 1.4.Edited by Tim Hudson and TBA.Latest version:TBA

[56] [RFC6151] S. Turner and L. Chen, Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms, IETF RFC6151, March 2011, http://www.rfc-editor.org/rfc/rfc6151.txt

[57] [w1979] A.Shamir,How to share a secret,Communications of the ACM,vol.22,no.11,pp.612-613,November 1979

[58] [RFC7292] K. Moriarty, M. Nystrom, S. Parkinson, A. Rusch, M. Scott. PKCS # 12: Personal Information Exchange Syntax v1.1,July 2014,https://tools.ietf.org/html/rfc7292

[59] [KMIP v1.4] OASIS,Key Management Interoperability Protocol Specification Version 1.4

索　引