



# 密钥管理互操作性协议规范第 1.1 版

OASIS 标准

2013 年 1 月 24 日

# 目录

- 1 介绍
  - 1.1 术语
  - 1.2 标准文献
  - 1.3 非标准文献
- 2 对象
  - 2.1 基对象
    - 2.1.1 属性
    - 2.1.2 凭证
    - 2.1.3 密钥块
    - 2.1.4 密钥值
    - 2.1.5 密钥包装数据
    - 2.1.6 密钥包装规范
    - 2.1.7 透明密钥结构
    - 2.1.8 模板属性结构
    - 2.1.9 扩展信息
  - 2.2 受管控对象
    - 2.2.1 证书
    - 2.2.2 对称密钥
    - 2.2.3 公钥
    - 2.2.4 私钥
    - 2.2.5 分裂密钥
    - 2.2.6 模板
    - 2.2.7 秘密数据
    - 2.2.8 不透明对象
- 3 属性
  - 3.1 唯一标识符
  - 3.2 名称
  - 3.3 对象类型
  - 3.4 密码算法
  - 3.5 密码长度
  - 3.6 密码参数
  - 3.7 密码域参数
  - 3.8 证书类型
  - 3.9 证书长度
  - 3.10 X.509 证书标识符
  - 3.11 X.509 证书主体
  - 3.12 X.509 证书发行者
  - 3.13 证书标识符
  - 3.14 证书主体
  - 3.15 证书发行者
  - 3.16 数字签名算法

- 3.17 摘要
- 3.18 操作策略名称
  - 3.18.1 操作策略控制范围外的操作
  - 3.18.2 默认操作策略
- 3.19 密码用途掩码
- 3.20 租赁时间
- 3.21 用途限制
- 3.22 状态
- 3.23 初始日期
- 3.24 激活日期
- 3.25 处理开始日期
- 3.26 保护停止日期
- 3.27 失活日期
- 3.28 销毁日期
- 3.29 破坏发生日期
- 3.30 破坏日期
- 3.31 撤销理由
- 3.32 归档日期
- 3.33 对象组
- 3.34 新鲜
- 3.35 关联
- 3.36 应用特有信息
- 3.37 联系信息
- 3.38 最后改动日期
- 3.39 自定义属性
- 4 从客户端到服务器的操作
  - 4.1 创建
  - 4.2 创建密钥对
  - 4.3 注册
  - 4.4 重建密钥
  - 4.5 重建密钥对
  - 4.6 派生密钥
  - 4.7 证明
  - 4.8 重证明
  - 4.9 定位
  - 4.10 检查
  - 4.11 获得
  - 4.12 获得属性
  - 4.13 获得属性列表
  - 4.14 添加属性
  - 4.15 修改属性
  - 4.16 删除属性
  - 4.17 获得租赁
  - 4.18 获得用途分配

- 4.19 激活
- 4.20 撤销
- 4.21 销毁
- 4.22 归档
- 4.23 恢复
- 4.24 核查
- 4.25 查询
- 4.26 发现版本
- 4.27 取消
- 4.28 轮询 (Poll)
- 5 从服务器到客户端的操作
  - 5.1 通知
  - 5.2 放置 (Put)
- 6 消息的内容
  - 6.1 协议版本
  - 6.2 操作
  - 6.3 最大回应大小
  - 6.4 唯一批处理条目 ID
  - 6.5 时间戳
  - 6.6 认证
  - 6.7 异步指标
  - 6.8 异步关联值
  - 6.9 结果状态
  - 6.10 结果理由
  - 6.11 结果消息
  - 6.12 批处理顺序选项
  - 6.13 批处理错误继续选项
  - 6.14 批处理数
  - 6.15 批处理条目
  - 6.16 消息扩展
- 7 消息格式
  - 7.1 消息结构
  - 7.2 操作
- 8 认证
- 9 消息编码
  - 9.1 TTLV 编码
    - 9.1.1 TTLV 编码字段
    - 9.1.2 举例
    - 9.1.3 定义值
- 10 传输
- 11 错误处理
  - 11.1 概述
  - 11.2 创建
  - 11.3 创建密钥对

- 11.4 注册
- 11.5 重建密钥
- 11.6 重建密钥对
- 11.7 派生密钥
- 11.8 证明
- 11.9 重证明
- 11.10 定位
- 11.11 检查
- 11.12 获得
- 11.13 获得属性
- 11.14 获得属性列表
- 11.15 添加属性
- 11.16 修改属性
- 11.17 删除属性
- 11.18 获得租赁
- 11.19 获得用途分配
- 11.20 激活
- 11.21 撤销
- 11.22 销毁
- 11.23 归档
- 11.24 恢复
- 11.25 核查
- 11.26 查询
- 11.27 取消
- 11.28 轮询 (Poll)
- 11.29 批处理条目
- 12 KMIP 服务器和客户端的执行合规
  - 12.1 KMIP 服务器的执行合规
  - 12.2 KMIP 客户端的执行合规
- 附录 A 鸣谢
- 附录 B 属性的交叉引用
- 附录 C 标签的交叉引用
- 附录 D 操作和对象的交叉引用
- 附录 E 缩略语
- 附录 F 图表列表
- 附录 G 修订记录

