文件标识

量子云控管理系统

CTS 协商概要说明

编制_____日期

审核_____日期

标准化_____日期

批准_____日期

变更记录

版本	变更单号	变更原因	变更内容	变更人	日期

目录

软件概要设计说明书

1 引言

1.1 编写目的

说明编写这份概要设计说明书的目的，指出预期的读者。

1.2 项目背景

说明：

a) 待开发软件系统的名称；

b) 列出本项目的任务提出者、开发者、用户。

1.3 术语定义

1.4 参考资料

列出要用到的参考资料，如：

a) 本项目的经核准的计划任务书或合同、上级机关的批文；

b) 属于本项目的其他已发表的文件；

c) 本文件中各处引用的文件、资料，包括所要用到的软件开发标准。

列出这些文件的标题、文件编号、发表日期和出版单位，说明能够得到这些文件资料的来源。

2 量子云控服务端管理

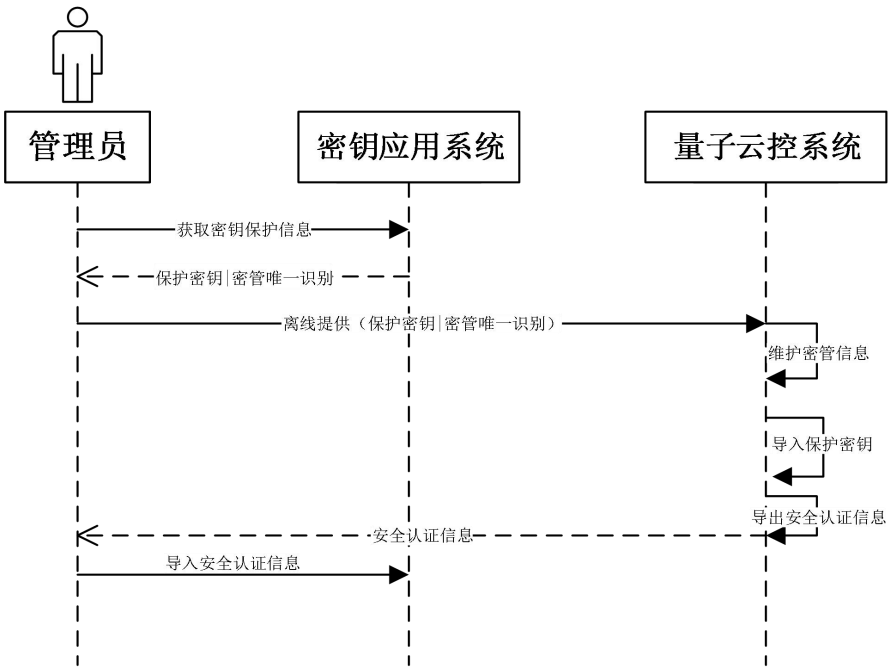
主要包含：安全认证密钥管理、量子安全存储设备注册、量子密钥充注以及量子会话密钥协商

2.1 安全认证密钥管理

2.1.1 功能描述

由密管系统提供分发保护密钥（SM2 加密公钥）的 pem 格式文件、密管系统唯一标识，在量子云控维护密管系统基础信息并且导入保护密钥文件，生成安全认证信息、密钥加密密钥（KEK）、以及提供导出安全认证信息、密钥加密密钥。

业务流程，如下图所示：



离线分发安全通道认证信息：

1) 密管系统生成加密密钥对作为保护密钥，加密公钥（SM2 加密公钥）转成 pem 格式以文件方式提供给量子随机数源，同时需提供密管系统的唯一标识；
2) 量子云控维护密管系统基础信息，导入保护密钥并且生成安全认证密钥，以主密钥加密存储；
3) 量子云控提供导出与密管系统建立安全认证信息，包含：量子云控唯一标识、KEK 密钥，安全认证密钥密钥、密钥的校验信息；
4) 密管系统导入与量子云控之间安全认证信息、密钥加密密钥。

安全认证信息：

序号	参数	名称	类型	描述
1	keyEncryptKey	密钥加密密钥	String	以保护密钥（SM2 加密公钥）加密，通过 Base64 转码成字符串
2	keyGeneratorID	量子云控标识	String	量子云控唯一标识
3	secTunnelKeys	安全通道认证密钥	String	以保护密钥（SM2 加密公钥）加密安全认证密钥，通过 Base64 转码成字符串。
4	chkVAlg	校验算法标识	String	对密钥校验正确性算法，采用 SM3 杂凑算法

5	keyChkV	校验值	String	解密密钥时的校验码，校验值：keyChkV=H(keyEncryptKey||secTunnelKeys)

密钥加密密钥以及安全通道认证信息：


```
{
    "chkVAlg":"SGD_SM3",
    "keyChkV":"P3u/MvT6m7glkHvPlKWqpb+dfWh1nUO7NvQYTXWUe1I=",
    "keyEncryptKey":"BJqEKTNLTkTlYiOcns+7jSi8x9dkyRa4ajzgxDObP5WZb6rJniKfVoJXCackL8WjTZEDGNVysXn/UbHIrujLQDdGGmx5tF136L2xc3PLoCWgNRZHXOXb75+IcdlYURdSnQQYgqaRT7XnSH1SZRvV2FU=",
    "keyGeneratorID":"WT-QCCS100-151",
    "secTunnelKeys":"BJZSfDU92Nngegfh3Le/L4GtVQ4LRURrIWfx5+wAbeVGYBUdSRZHHKQS9LL6lO4RM1S7PdOqryBLw33mYvO5RBdVwXlV231MHHu8IAOS3wjf8LOR5WVNhOo1Aq+mA1Qo/a1J3MEgEUYIiwAJMLaLOGeuszhzWqf8v/fveW/n4kLbURVxQ+ddPzFwxvgcN25ByQ=="
}
```


安全认证密钥：

16 个字节	16 个字节	16 个字节
加密密钥（Kenc）	解密密钥(Kdec)	消息鉴别码密钥(Kmac)

2.1.2 密钥管理

密钥加密密钥：由保护公钥加密，密文标准[GM/T 0009-2012]标准为 C1C3C2；

安全认证密钥，由保护公钥加密，密文标准[GM/T 0009-2012]标准为 C1C3C2。

2.2 量子安全存储设备注册

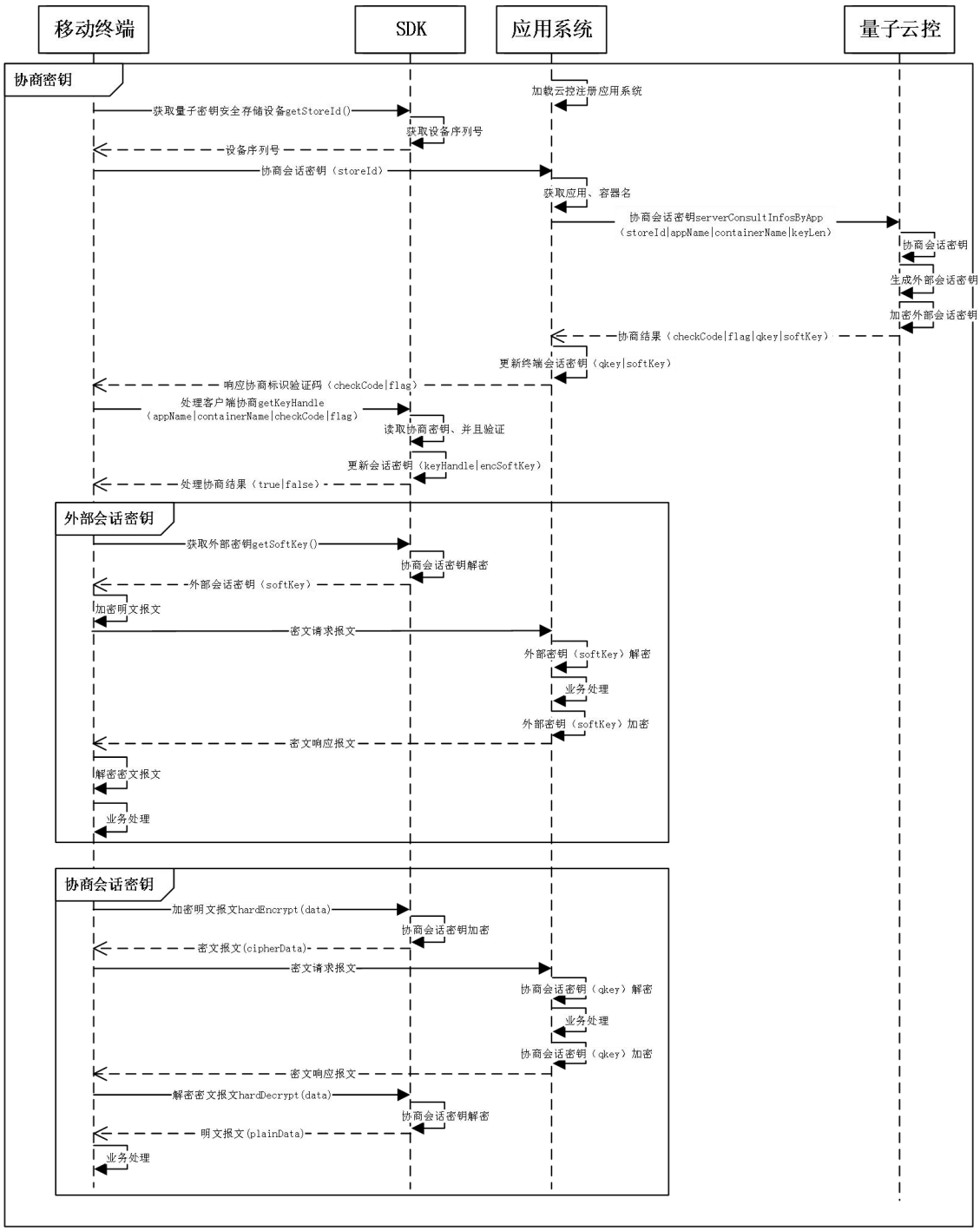
量子云控系统提供安全设备管理工具（SDMP）进行设备初始化注册应用系统

2.3 量子密钥充注

量子密钥充注量子方式：通过安全设备管理工具（SDMP）定点充注和终端 API 提供在线充注

2.4 量子会话密钥协商

业务流程如下图所示：



3 接口设计

3.1 外部接口

接口协议主要遵循 https 协议，类似 restful 方式提供。

3.1.1 密钥协商接口

1、请求

相对路劲：/qkeyapply/serverConsultInfosByApp

请求方式：post

请求参数列表:

请求参数名	数据类型	约束	描述
storeId	String	非空	设备序列号
appName	String	非空	应用名称
containerName	String	非空	容器名称
keyLen	int	非空	协商密钥量
serverId	String	非空	服务端鉴权 ID
timestamp	String	非空	时间戳
hmac	String	非空	hmac（storeId、appName、containerName、keyLen、serverId、timestamp 参与计算）

2、响应

响应数据：

数据项	数据类型	描述
code	int	响应状态码，0-操作成功，其他-操作失败
message	String	操作结果信息提示
data	jsonObject	响应数据对象

响应数据 data 对象：

数据项	数据类型	描述
checkCode	String	协商标志的消息鉴别码,SM4_MAC（flag 的 JSON 字符串）
flag	jsonObject	协商标志
storeId	String	设备序列号
unitId	String	批次号

blockId	String	密钥分块 ID
offsetIndex	int	使用偏移量
encodeType	String	消息鉴别码运算方式“SMS4_MAC”
keyLen	int	协商密钥量
encSoftQkey	String	密文外部密钥,由协商密钥加密,运算标识 SM4_CBC
softQkeyLen	int	协商的软密钥量
errorCode	String	协商结果：“0”-成功，非零-失败
errorMsg	String	协商操作提示信息
qkey	String	密文协商密钥，由安全认证解密密钥(Kdec)，运算标识 SM4_CBC
softQkey	String	密文外部密钥，由安全认证解密密钥(Kdec)，运算标识 SM4_CBC
timestamp	String	时间戳
hmac	String	hmac（checkCode、storeId、unitId、blockId、offsetIndex、encodeType、keyLen、softQkeyLen、encSoftQkey、errorCode、errorMsg、softQkey、qkey 参与计算），鉴别码运算密钥是安全认证消息鉴别码密钥(Kmac)