文件标识

密钥应用服务端

接入说明

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

密钥应用服务接入说明

1 引言

1.1 编写目的

说明编写这份设计说明书的目的，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 密钥应用服务端

量子云控系统提供密钥应用服务端（S 端）的密钥使用的配置管理，包含：密钥应用服务在量子云控设置密钥应用的唯一标识、密钥应用的共享密钥、交换共享密钥功能等；

交换共享密钥要提供两种保护方式：公钥机密性保护、口令机密性保护。

密钥应用的共享密钥包含：安全认证密钥、密钥加密密钥两个部分

- 安全认证密钥：用于密钥应用系统与云控之间进行双向实体鉴别的基础上建立安全通道；

  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)

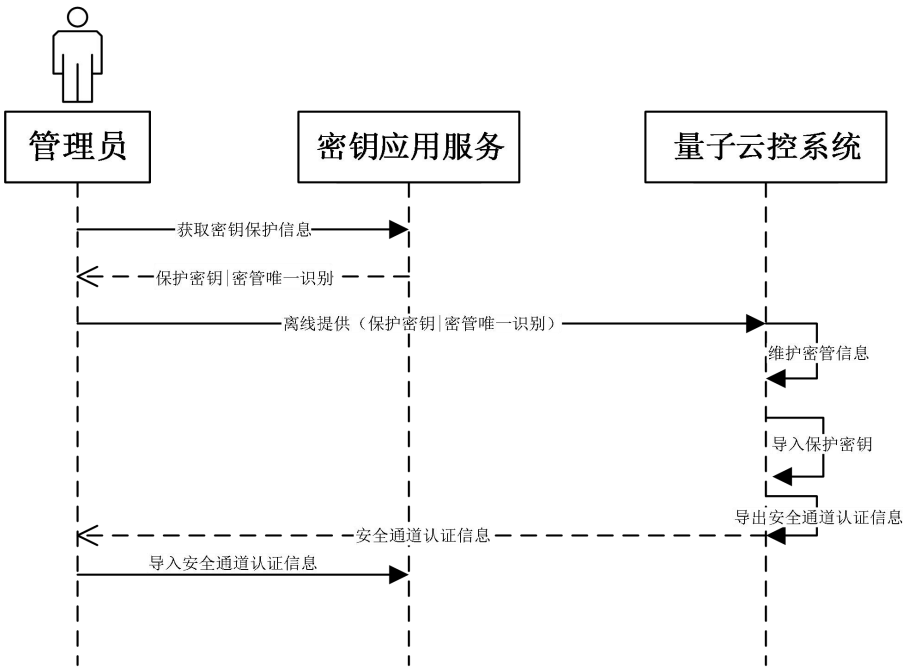
- 密钥加密密钥（KEK）:量子云控对外提供量子密钥，通过 KEK 保护后再对外提供密文量子密钥；

2.1 公钥机密性保护

2.1.1 功能描述

由密管应用服务提供分发保护密钥（SM2 加密公钥）的 pem 格式文件、密管应用服务唯一性标识，在量子云控系统维护密管应用服务基础信息并且导入保护密钥文件，生成安全通道认证信息、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、密钥提供者唯一性标识。

业务流程，如下图所示：



离线分发安全通道认证信息：

1) 密钥应用服务生成加密公私钥对作为保护密钥，加密公钥（SM2 加密公钥）转成 pem 格式以文件方式提供给量子云控系统，同时需提供密钥应用服务的唯一标识；
2) 量子云控系统维护密钥应用服务基础信息，导入保护密钥并且生成安全通道认证密钥，以主密钥加密存储；
3) 量子云控系统提供导出与密钥应用服务建立安全通道认证信息，包含：量子云控系统唯一标识、KEK 密钥，安全通道认证密钥保护密钥，安全通道认证密钥密钥、密钥的校验信息；
4) 密钥应用服务导入与量子云控系统建立安全通道认证信息以及密钥加密密钥。

安全通道认证信息：

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	量子随机数源标识	String	量子随机数源唯一标识
3	protectSecretKey	安全通道认证密钥保护密钥	String	以保护密钥（SM2 加密公钥）加密，通过 Base64 转码成字符串
3	secTunnelKeys	安全通道认证密钥	String	1、安全通道密码设备实现密码运算以

				KEK 加密； 2、安全通道软件实现密码运算以“安全通道认证密钥保护密钥”加密； 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||protectSecretKey||secTunnelKeys)

密钥加密密钥以及安全通道认证信息：


```
{
    "keyEncryptKey":
"BA2uk17oc7cgcW5JTOAN2ZqeNmCg8BrVSR4X5w2wGMSdgK8J9MafruIFPNqDg+iy44QMFf65A2I7b37vFwVvHFabdjdQJ
jkoLgGA5/fmkgRnHzQWlwixBO3ws6Ni2hsBk44Yu1A59v5jeuOPn+VzG7k=",
    "keyGeneratorID": "WT-QRNG200-0000001",
    "protectSecretKey": "+O8SQ4XgoX3wcewLRyFBYg==",
    "secTunnelKeys":
"BFke6KG7hJNsGCWNTwaSHG6je6TIaB/sDiKju3qmWJB9sCsCjxaWaUmbVQadjj2OsvMZnHu3bRCA5KzsRIfLdjBpybmgM
K9TghvCXcNv+aBCsOuS+ONrjTG7fddlLSfEgEy2mYdekt3kECPrWFkei+2tdu5oj0gfa2jIAEwbUJdJOETLz6Uj8LUlc5U
Sb+2usQ==",
     "keyChkV": "3qfD/NgOqJHojNcAaOhuAmgmFVRhp3SRRMdxD5OU4/o=",
     "chkVAlg": "SGD_SM3"
}
```


2.1.2 密钥管理

- 安全通道由软件实现加解密运算
  - 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；
  - 安全通道认证密钥保护密钥：由“密钥加密密钥”加密，算法标识 SM4_ECB，无填充；

- 安全通道认证密钥，由“安全通道认证密钥保护密钥”加密，算法标识 SM4_ECB，无填充。

■ 安全通道由密码设备实现加解密运算

- 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；
- 安全通道认证密钥，由“密钥加密密钥”加密，算法标识 SM4_ECB，无填充。

2.2 口令机密性保护

2.2.1 功能描述

维护密钥应用服务保护密钥的口令，通过口令派生保护密钥，密码算法标识是 SM3 对口令进行杂凑的结果取前 16 个字节作为保护密钥；

口令机密性保护密码示意图如下：

共享密钥使用：

1) 口令派生保护密钥：

```
protectSecretHash = SM3.digest(password);
protectSecretKey = Array.copyOfRange(protectSecretHash,0,16);
```

2) 安全认证密钥：

```
secTunnelKeys = SM4_CBC(protectSecretKey ,cipherSecTunnelKeys);
```

3) 密钥加密密钥：

```
keyEncryptKey= SM4_CBC(protectSecretKey ,cipherKeyEncryptKey);
```

2.2.2 密钥管理

安全通道由软件实现加解密运算

- 密钥加密密钥：由口令派生的保护密钥加密，加密算法 SM4_CBC，填充方式 PKCS5；
- 安全认证密钥，由口令派生的保护密钥加密，加密算法 SM4_CBC，填充方式 PKCS5。