量子安全移动存储介质

密钥协商充注协议详细设计详细设计

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

[1 引言 3](#_Toc11176)

[1.1 编写目的 3](#_Toc28585)

[2 量子移动存储设备C2S协商密钥 3](#_Toc24651)

[2.1 量子移动存储设备相关接口定义 3](#_Toc8739)

[2.1.1 密钥协商 3](#_Toc1111)

[2.1.2 获取密钥句柄 3](#_Toc32181)

[2.1.3 导出密钥 4](#_Toc11288)

[2.2 量子云控系统相关接口定义 4](#_Toc8745)

[2.2.1 请求密钥 4](#_Toc2614)

[2.3 流程图 6](#_Toc18817)

[3 量子移动存储设备C2C协商密钥 6](#_Toc25278)

[3.1 量子移动存储设备相关接口定义 6](#_Toc6492)

[3.1.1 获取认证同步码 6](#_Toc6002)

[3.1.2 认证同步 8](#_Toc31889)

[3.1.3 获取密钥句柄 8](#_Toc8065)

[3.1.4 导出密钥 9](#_Toc11899)

[3.2 流程图 10](#_Toc3608)

[4 量子移动存储设备C2C在线充注密钥 10](#_Toc11728)

[4.1 量子移动存储设备相关接口定义 10](#_Toc9838)

[4.1.1 密钥协商 10](#_Toc15092)

[4.2 量子云控系统相关接口定义 11](#_Toc12597)

[4.2.1 获取清理链路 11](#_Toc26152)

[4.2.2 提交清理关系 12](#_Toc9883)

[4.2.3 获取链路关系 13](#_Toc5134)

[4.2.4 创建充注任务 14](#_Toc6460)

[4.2.5 请求密钥 15](#_Toc21328)

[4.2.6 提交任务 16](#_Toc29104)

[4.2.7 回滚任务 17](#_Toc29800)

[4.3 流程图 18](#_Toc18343)

[5 量子移动存储设备C2S在线充注密钥 18](#_Toc7397)

[5.1 量子移动存储设备相关接口定义 18](#_Toc19622)

[5.1.1 密钥协商 18](#_Toc6562)

[5.2 量子云控系统相关接口定义 19](#_Toc7649)

[5.2.1 创建充注任务 19](#_Toc4029)

[5.2.2 请求密钥 20](#_Toc15823)

[5.2.3 提交任务 21](#_Toc27226)

[5.2.4 回滚任务 22](#_Toc15204)

[5.3 流程图 23](#_Toc4984)

软件概要设计说明书

# 引言

## 编写目的

给出量子安全移动存储介质密钥协商充注协议说明。

# 量子移动存储设备C2S协商密钥

## 量子移动存储设备相关接口定义

### 密钥协商

原型： int QCard\_RequestCTSKeyByApp(char \*pcAddr，

char \*pcStoreId,

char \*pcAppName,

char \*pcConName,

unsigned long ulSoftKeyLen,

unsigned char \*pucKey,

unsigned char \*pucSoftKey,

char \*\*pcFlag,

char \*pcCheckCode);

描述：获取密钥句柄

参数：pcAddr [in] 服务端地址

pcStoreId [in] 设备序列号

pcAppName [in] 应用名称

pcConName [in] 容器名称

ulSoftKeyLen [in] 软加密算法密钥长度

pucKey [out] 协商出的密钥(16字节)

pucSoftKey [out] 软加密算法密钥

pcFlag [out] 协商数据

pcCheckCode [out] 协商数据校验码

返回值：0 成功；

非0 失败，错误代码。

### 获取密钥句柄

原型： int QCard\_ClientKeyInit (QHANDLE hStoreHandle，

char \*pcCheckCode,

char \*pcFlag,

char \*ulAlgId,

QCard\_BLOCKCIPHERPARAM KeyParam,

char \*pcAppName,

char \*pcContainerName,

unsigned long \* pcPin,

unsigned long ulSafeTactics,

KEYHANDLE \*phKeyHandle);

描述：获取密钥句柄，通过密钥句柄可以对业务数据进行加解密

参数： hStoreHandle [in] 安全存储区句柄

pcCheckCode [in] 校验码

pcFlag [in] 密钥标记位

ulAlgId [in] 算法标示,见附录B

KeyParam [in] 分组密钥算法相关参数度,见附录C

pcAppName [in] 应用名称

pcContainerName [in] 容器名称

pcPin [in] 应用用户PIN

ulSafeTactics [in] 安全策略，见附录D

phKeyHandle [out] 密钥句柄

返回值：0 成功；

非0 失败，错误代码。

备注： 初始化资源成功后，方可调用获取密钥句柄接口。该接口用于CTS密钥模式，

服务端从管理端获取到密钥标记位和校验码后，交由客户端获取密钥句柄。

密钥句柄使用完后记得关闭。

### 导出密钥

原型： void QCard\_ExportKey (QHANDLE hStoreHandle,

KEYHANDLE hKeyHandle，

unsigned char \*pucKey,

unsigned long \*pulKeyLen);

描述：导出密钥

参数： hStoreHandle [in] 安全存储区句柄

hKeyHandle [in] 密钥句柄

pucKey [in out] 密钥缓冲区指针，可以为NULL，用于获取密钥长度

pulKeyLen [in out] 输入时表示数据缓冲区长度，输出时表示结果数据实际长度

返回值：0 成功；

非0 失败，错误代码。

## 量子云控系统相关接口定义

### 请求密钥

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 |
| containerName | String | 非空 | 容器名 |
| keyLen | String | 非空 | 软加密密钥长度 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"协商密钥成功","data":{"checkCode":"++dwnFr5X5MBviV+O+zahg==","flag":{"storeId":"3430483533185D3A","unitId":"ec8aef854bb14eb186b3dda711f6c3e4","blockId":"bea2f5d1a5134c17b9a24fdf3205e56f","offsetIndex":384,"encodeType":"SMS4\_MAC","keyLen":16,"softQkeyLen":16,"encSoftQkey":"gP7WO1eolJ/AatjAlkTWF9A293JOC6q+2Yhl0qd04MA=","errorCode":"0","errorMsg":""},"softQkey":"PSOGRma4rJSXg0l+nXfHKg==","qkey":"kLJbyn9JJ1oJhUsWCdow0Q=="}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | String | 数据 |
| checkCode | String | 校验码，该值等于使用flag协商出的量子密钥对flag数据进行SM4\_MAC运算 |
| flag | String | 协商数据 |
| storeId | String | 设备序列号 |
| unitId | String | 密钥批次号 |
| blockId | String | 密钥块号 |
| offsetIndex | Int32 | 密钥偏移量 |
| encodeType | String | 加密算法 |
| keyLen | Int32 | 密钥长度 |
| softQkeyLen | Int32 | 软加密密钥长度 |
| encSoftQkey | String | 软加密密钥密文，该值等于该值等于使用flag协商出的量子密钥对softQkey数据进行SM4\_CBC加密运算 |
| errorCode | Int32 | 错误码 |
| errorMsg | String | 错误消息 |
| softQkey | String | 软加密密钥 |

## 流程图



1. 密钥协商流程图

# 量子移动存储设备C2C协商密钥

## 量子移动存储设备相关接口定义

### 获取认证同步码

原型： int QCard\_ReadAuthSynFlag(QHANDLE hStoreHandle，

char \*pcOtherStoreId,

char \*pcAppName,

char \*pcContainerName,

unsigned long \* pcPin,

unsigned char \*pcFlag,

unsigned long pulFlagLen);

描述：获取认证同步码

参数： hStoreHandle [in] 安全存储区句柄

pcOtherStoreId [in] 另一端设备序列号

pcAppName [in] 应用名

pcContainerName [in] 容器名

pcPin [in] 用户PIN码

pcFlag [in, out] 认证同步码缓冲区指针，可以为NULL，用于数据实际长度

pulFlagLen [in, out] 输入时表示数据缓冲区长度，输出时表示结果数据实际长度

返回值：0 成功；

非0 失败，错误代码。

备注： 初始化资源成功后，方可调用获取密钥句柄接口。该接口用于CTC密钥模式协商。

认证同步码格式:

|  |
| --- |
| {"checkCode":"0KqEy9S+KVUTN/1q9NSt51KOSv74n9OJgY2wutLQIpE=","flag":{"storeId":"343048353318665D","unitId":"860994ca46a9469c972668ff1ef9d47d","blockId":"d960a6fda71f461f98d3b9502b7a2344","offsetIndex":0,  "encdeType":"SGD\_SM1\_ECB","keyLen":16,"random":"2PEXuyYGX3vElkzdy5xK7A==","code":0,"errorMsg":""}} |

认证同步码数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| checkCode | String | 校验码，该值等于使用flag协商出的量子密钥对flag数据进行SM3运算后，进行SM1\_ECB加密操作的结果 |
| flag | String | 协商数据 |
| storeId | String | 设备序列号 |
| unitId | String | 密钥批次号 |
| blockId | String | 密钥块号 |
| offsetIndex | Int32 | 密钥偏移量 |
| encodeType | String | 加密算法 |
| keyLen | Int32 | 密钥长度 |
| random | String | 随机数，该值使用使用flag协商出的量子密钥进行SM1\_ECB解密操作的结果的软加密密钥 |
| code | Int32 | 错误码 |
| errorMsg | String | 错误消息 |

### 认证同步

原型： int QCard\_AuthSynFlag(QHANDLE hStoreHandle，

char \*pcOtherStoreId,

char \*pcAppName,

char \*pcContainerName,

unsigned char \*pcFlag);

描述：获取认证同步码

参数： hStoreHandle [in] 安全存储区句柄

pcOtherStoreId [in] 另一端设备序列号

pcAppName [in] 应用名

pcContainerName [in] 容器名

pcFlag [in, out] 认证同步码

返回值：0 成功；

非0 失败，错误代码。

备注： 初始化资源成功后，方可调用获取密钥句柄接口。该接口用于CTC密钥模式协商。如果Flag包含的密钥偏移量比本地偏移量大，则同步偏移量，否则不同步。

### 获取密钥句柄

原型： int QCard\_AuthSynFlagKeyInit (QHANDLE hStoreHandle，

char \*pcFlag,

char \*ulAlgId,

QCard\_BLOCKCIPHERPARAM KeyParam,

char \*pcAppName,

char \*pcContainerName,

unsigned long \* pcPin,

unsigned long ulSafeTactics,

KEYHANDLE \*phKeyHandle);

描述：获取密钥句柄

参数： hStoreHandle [in] 安全存储区句柄

pcFlag [in] 密钥标记位

ulAlgId [in] 算法标示,见附录B

KeyParam [in] 分组密钥算法相关参数度,见附录C

pcAppName [in] 应用名称

pcContainerName [in] 容器名称

pcPin [in] 应用用户PIN

ulSafeTactics [in] 安全策略，见附录D

phKeyHandle [out] 密钥句柄

返回值：0 成功；

非0 失败，错误代码。

备注： 初始化资源成功后，方可调用获取密钥句柄接口。该接口用于CTC密钥获取。

### 导出密钥

原型： void QCard\_ExportKey (QHANDLE hStoreHandle,

KEYHANDLE hKeyHandle，

unsigned char \*pucKey,

unsigned long \*pulKeyLen);

描述：导出密钥

参数： hStoreHandle [in] 安全存储区句柄

hKeyHandle [in] 密钥句柄

pucKey [in out] 密钥缓冲区指针，可以为NULL，用于获取密钥长度

pulKeyLen [in out] 输入时表示数据缓冲区长度，输出时表示结果数据实际长度

返回值：0 成功；

非0 失败，错误代码。

## 流程图



1. 密钥协商流程图

# 量子移动存储设备C2C在线充注密钥

## 量子移动存储设备相关接口定义

### 密钥协商

原型： int QCard\_OnlineChargingKey(QHANDLE hStoreHandle,

char \*pcAppName,

char \*pcContainerName,

char \*pcPin,

unsigned long ulMinKeyQuantity);

描述：密钥在线充注，当密钥量低于充注密钥阀值时，进行充注

参数： hStoreHandle [in] 安全存储区句柄

pcAppName [in] 应用名称

pcContainerName [in] 容器名称

pcPin [in] 应用用户PIN

ulMinKeyQuantity [in] 充注密钥阀值

返回值：0 成功；

非0 失败，错误代码。

备注： 初始化资源成功后，方可调用密钥在线充注接口。客户端调用该接口时，需要保证与量子随机数管理系统网络通信正常。调用该接口时，设备未使用密钥量低于客户端所设置的充注密钥阀值时，接口将向管理系统发起安全充注事务。当接口返回值成功时，设备未使用密钥量高于客户端所设置的充注密钥阀值。当应用为C2C模式，该接口会查询并清理已解绑关系。

## 量子云控系统相关接口定义

### 获取清理链路

1、请求

相对路劲：/c2c/tasks/findDevRefUnbindInfos

请求方式：POST

请求格式:

|  |
| --- |
| {"appName":"RSACC","containerName":"RSACC","devAuthCode":"uciMkj+jKel8Zy17CYUfv8i9tfjmsAvl0gEDE39OUR/gvB/5dxQveMz0JX7XeLdlKdX5bxA4rlopvJMaEKUTDFNivEzjngc92Rx/7cHVynRe7hd8hug5yrlqRV0lgjOTRC0VYsumWpYYVOldEgaHTkMkJu3NbZ+gPpal+on0s7ACSutuw5GaFHUfecnSjs/7T32WNBntoRzN7VcTUQFZksGzCKNi9mqhpjWF8C6hfuoTsODuIZPk3xZ/2SqKtkBPch3hmFDrd4jJak3iBbXqm4wIqxegI9rrERerd9kaqOteAE4NzqR/QtpiRiUKs12RjnbVqkySH1N9eT2fpbM2gQ==","deviceId":"3430483533185D3A"} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| appName | String | 非空 | 应用名 |
| containerName | String | 非空 | 容器名 |
| devAuthCode | String | 非空 | 设备鉴权码，该值等于应用名，容器名，设备序列号使用设备签名密钥对签名的结果。 |
| deviceId | String | 非空 | 设备序列号 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"查询解绑设备链路信息成功","data":{"deviceId":"3430483533185D3A","unbindedPeerDevInfos":[{"taskId":"c90191ddb3af4a70be54ac12433a05c0","peerDeviceId":"343048353318665D"}]}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | String | 数据 |
| deviceId | String | 设备序列号 |
| unbindedPeerDevInfos | String | 解绑信息 |
| staskId | String | 任务ID |
| peerDeviceId | String | 对端设备序列号 |

### 提交清理关系

1、请求

相对路劲：/c2c/tasks/commitUnbindDevRefInfos

请求方式：POST

请求格式:

|  |
| --- |
| {"deviceId":"3430483533185D3A","appName":"QSWCTCECC","containerName":"QSWCTCECC","deviceTaskResultList":[{"result":1,"taskId":"c90191ddb3af4a70be54ac12433a05c0"}],"devAuthCode":"MEUCIQDgHseokJX+hraDMNTfSTu/3ezL4qjkKOE+LuzS/gCYbQIgH1ENGS7y535AP4f4C6+XtHH8+X0RRUb5Ioja9QIU3NY="} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| appName | String | 非空 | 应用名 |
| containerName | String | 非空 | 容器名 |
| deviceTaskResultList | String | 非空 | 已清理任务列表 |
| result | int32 | 非空 | 清理结果 1:清理成功 0：清理失败 |
| taskId | String | 非空 | 任务ID |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"处理任务结果成功","data":{}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | String | 数据 |

### 获取链路关系

1、请求

相对路劲：/fillrefqkey/findFillQKeyRefTask

请求方式：POST

请求格式:

|  |
| --- |
| {"deviceId":"3430483533185D3A","systemId":"000000005","devAuthCode":"MEUCIFw2dx3UJstZ/xby+2PHgsqxhltJn1dUb9Ly4L/PMjGoAiEArGHWPqb3LYa3yP0YrunVEQTelOEwsrX7HRg4nf8eT2w="} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| systemId | String | 非空 | 系统ID |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| [{"systemId":"000000005","deviceId":"3430483533185D3A","fillStatus":"0","refId":"0a5a2643c88240b6b814cae70e4cb6eb","pdeviceId":"343048353318665D"}] |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| systemId | int | 系统ID |
| deviceId | String | 设备序列号 |
| fillStatus | String | 充注状态 0: 未充注; 1：等待充注结束; 2： 充注结束; 3：分发异常 4：等待另一端充注结束 |
| refId | String | 任务ID |
| pdeviceId | String | 对端设备序列号 |

### 创建充注任务

1、请求

相对路劲：/fillrefqkey/createFillQKeyRefTasks

请求方式：POST

请求格式:

|  |
| --- |
| {"deviceId":"343048353318665D","systemId":"000000005","pdeviceIds":"3430483533185D3A","devAuthCode":"MEYCIQD66og6XPpyfflxDpm9tWYQK4/GYVtCgu4ok0ADtcgXgwIhAKSubVtzfkb3aykohyc2GnFrIAlyHKbYCRRMlZn3b/U0"} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| systemId | String | 非空 | 系统ID |
| pdeviceIds | String | 非空 | 对端设备序列号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"创建批量链路充注任务成功","data":[{"pdeviceId":"3430483533185D3A","pdevShortNum":29,"unitId":"d76d437e6616490ba07f5052d6e2c932","fillQKyeSize":512,"cipherType":"2","distrCount":1,"perBlockSeq":0,"validDateStart":"2020-12-25 13:29:02","validDateEnd":"2023-12-25 13:29:02"}]} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | json | 数据 |
| pdeviceId | String | 对端设备序列号 |
| pdevShortNum | String | 对端设备序列号短号 |
| unitId | String | 批次号 |
| fillQKyeSize | Int32 | 充注密钥大小 |
| cipherType | String | 加密类型 0：不加密 1：公钥加密 2：对称密钥加密 |
| distrCount | Int32 | 块数量 |
| perBlockSeq | Int32 | 当前块序号 |
| validDateStart | String | 有效期始 |
| validDateStart | String | 有效期止 |

### 请求密钥

1、请求

相对路劲：/fillrefqkey/distrRefQKeyByBlock

请求方式：POST

请求格式:

|  |
| --- |
| {"deviceId":"343048353318665D","unitId":"d76d437e6616490ba07f5052d6e2c932","perBlockSeq":0,"devAuthCode":"MEYCIQCdeEX/sxHORMtIJRvdz/MlZUBy9TQ3DlF3p5r+SAa2tAIhAN3tL7gPJRpcj37jml3zNDi3cqpHzkBU9OVXk9/DbfuL"} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| unitId | String | 非空 | 批次号 |
| perBlockSeq | String | 非空 | 块序号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"创建批量链路充注任务成功","data":[{"pdeviceId":"3430483533185D3A","pdevShortNum":29,"unitId":"d76d437e6616490ba07f5052d6e2c932","fillQKyeSize":512,"cipherType":"2","distrCount":1,"perBlockSeq":0,"validDateStart":"2020-12-25 13:29:02","validDateEnd":"2023-12-25 13:29:02"}]} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | json | 数据 |
| pdeviceId | String | 对端设备序列号 |
| pdevShortNum | String | 对端设备序列号短号 |
| unitId | String | 批次号 |
| fillQKyeSize | Int32 | 充注密钥大小 |
| cipherType | String | 加密类型 0：不加密 1：公钥加密 2：对称密钥加密 |
| distrCount | Int32 | 块数量 |
| perBlockSeq | Int32 | 当前块序号 |
| validDateStart | String | 有效期始 |
| validDateStart | String | 有效期止 |

### 提交任务

1、请求

相对路劲：fillrefqkey/commitFillQKeyRefTask

请求方式：POST

请求格式:

|  |
| --- |
| {"deviceId":"343048353318665D","unitId":"d76d437e6616490ba07f5052d6e2c932","devAuthCode":"MEUCIQDabyuA/TiFt2XBIXjvikBybLJuwkNPWHpyLs5ylgs3qwIgcIRj0kKCK9PrKmq1v7Xk9bJCKVcZzmU+/pIIKhK9D0Y="} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| unitId | String | 非空 | 批次号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"提交批次充注任务成功","data":{}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |

### 回滚任务

1、请求

相对路劲：/fillrefqkey/rollbackFillQKeyRefTask

请求方式：POST

请求格式:

|  |
| --- |
| {"deviceId":"343048353318665D","unitId":"a9467cf0f3ae4cf29bdbb475e53bcc74","devAuthCode":"MEUCIF1aRTONTO7pgprxL2Mw/73ojLISCjgusyqigQETHkRpAiEAvjDsktI2p2+Fodxv6N9XlZ0dzdIRfD3EkJxcL+K+2Dc="} |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| unitId | String | 非空 | 批次号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"回滚批次充注任务成功","data":{}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |

## 流程图



1. 密钥协商流程图

# 量子移动存储设备C2S在线充注密钥

## 量子移动存储设备相关接口定义

### 密钥协商

原型： int QCard\_OnlineChargingKey(QHANDLE hStoreHandle,

char \*pcAppName,

char \*pcContainerName,

char \*pcPin,

unsigned long ulMinKeyQuantity);

描述：密钥在线充注，当密钥量低于充注密钥阀值时，进行充注

参数： hStoreHandle [in] 安全存储区句柄

pcAppName [in] 应用名称

pcContainerName [in] 容器名称

pcPin [in] 应用用户PIN

ulMinKeyQuantity [in] 充注密钥阀值

返回值：0 成功；

非0 失败，错误代码。

备注： 初始化资源成功后，方可调用密钥在线充注接口。客户端调用该接口时，需要保证与量子随机数管理系统网络通信正常。调用该接口时，设备未使用密钥量低于客户端所设置的充注密钥阀值时，接口将向管理系统发起安全充注事务。当接口返回值成功时，设备未使用密钥量高于客户端所设置的充注密钥阀值。当应用为C2C模式，该接口会查询并清理已解绑关系。

## 量子云控系统相关接口定义

### 创建充注任务

1、请求

相对路劲：/fillqkey/createFillQKeyTask

请求方式：POST

请求格式:

|  |
| --- |
| systemId=000000002&deviceId=343048353318665D&devAuthCode=MEYCIQCAA3j/FhCIeQQwrKtNvq/0nACTogj/go947T%2bq6fjGOgIhAJRV0S6syzZPG/NDwUCyjERNN%2bt9rPu39vF/Frx9F4B8 |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| systemId | String | 非空 | 系统ID |
| deviceId | String | 非空 | 设备序列号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"创建在线充注任务成功","data":{"unitId":"8fbde8dd69944b78bc6fff7b07729af3","fillQKyeSize":1024,"distrCount":1,"cipherType":"2","perBlockSeq":0,"validDateStart":"2020-12-28 16:03:28","validDateEnd":"2023-12-28 16:03:28","pdeviceId":"343048353318665D"}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | json | 数据 |
| pdeviceId | String | 设备序列号 |
| unitId | String | 批次号 |
| fillQKyeSize | Int32 | 充注密钥大小 |
| cipherType | String | 加密类型 0：不加密 1：公钥加密 2：对称密钥加密 |
| distrCount | Int32 | 块数量 |
| perBlockSeq | Int32 | 当前块序号 |
| validDateStart | String | 有效期始 |
| validDateStart | String | 有效期止 |

### 请求密钥

1、请求

相对路劲：/fillqkey/distrQKeyByBlock

请求方式：POST

请求格式:

|  |
| --- |
| deviceId=343048353318665D&unitId=8fbde8dd69944b78bc6fff7b07729af3&perBlockSeq=0&devAuthCode=MEYCIQDVwWLy%2bgC8BVQuK/BU/HjTU3nXpJ/rs7OHc8S1uHWF9QIhAKp6SFrf8dTOUudpbgZGiiCoiDi4R2vwzzuKUOOx24CQ |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| unitId | String | 非空 | 批次号 |
| perBlockSeq | String | 非空 | 块序号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"分发分块密钥成功","data":{"unitId":"8fbde8dd69944b78bc6fff7b07729af3","blockId":"4b2bf814f33a4da9b3253323e9a201b6","blockSeq":1,"blockSize":1024,"storeUnits":"1","qkContent":"CtUxbngZiag==","pdeviceId":"343048353318665D"}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |
| data | json | 数据 |
| unitId | String | 批次号 |
| blockId | String | 块号 |
| blockSeq | Int32 | 块序号 |
| blockSize | Int32 | 块大小 |
| storeUnits | String | 单位 1-byte，2-KB、3-MB |
| qkContent | String | 密钥 |
| pdeviceId | String | 设备序列号 |

### 提交任务

1、请求

相对路劲：/fillqkey/commiteTask

请求方式：POST

请求格式:

|  |
| --- |
| deviceId=343048353318665D&unitId=8fbde8dd69944b78bc6fff7b07729af3&devAuthCode=MEYCIQCbE%2b9M7ga2birNLdMgVTeb/uRnyRzB0kDVRVmDVt12sAIhALUrq1mJcFYtQPc6eJgbd6D9znrZQ3fzfb/rP20grjfx |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| unitId | String | 非空 | 批次号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"提交充注任务成功","data":{}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |

### 回滚任务

1、请求

相对路劲：/fillqkey/rollbackTask

请求方式：POST

请求格式:

|  |
| --- |
| deviceId=343048353318665D&unitId=8fbde8dd69944b78bc6fff7b07729af3&devAuthCode=MEYCIQCbE%2b9M7ga2birNLdMgVTeb/uRnyRzB0kDVRVmDVt12sAIhALUrq1mJcFYtQPc6eJgbd6D9znrZQ3fzfb/rP20grjfx |

请求数据:

|  |  |  |  |
| --- | --- | --- | --- |
| **请求参数名** | **数据类型** | **约束** | **描述** |
| deviceId | String | 非空 | 设备序列号 |
| unitId | String | 非空 | 批次号 |
| devAuthCode | String | 非空 | 鉴权码，该值等于上述信息使用设备签名密钥对签名的结果。 |

2、响应

响应格式:

|  |
| --- |
| {"code":0,"message":"回滚批次充注任务成功","data":{}} |

响应数据：

|  |  |  |
| --- | --- | --- |
| **数据项** | **数据类型** | **描述** |
| code | int | 响应码，0-操作成功，其他-操作失败 |
| message | String | 操作结果信息提示 |

## 流程图



1. 密钥协商流程图