ICS 19 020

M731

T/GXDSL

团　　体　　标　　准

T/GXDSL 001—2025

量子通信网络设备接口技术规范

Technical Specifications for the Interfaces of Quantum Communication Network Equipment

2025 - 3 - 7 发布　　2025 - 3 - 7 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：广西研科院高新技术有限公司，安徽问天量子科技股份有限公司，广西产学研科学研究院，中国科学技术大学，国防科技大学，西安交通大学，广西蓝脑科技有限公司，合肥量芯科技有限公司，合肥富地智飞科技有限公司，中国联通南宁市分公司，广西景灿通信科技有限公司，山东大学(乐陵)人工智能研究院，清华大学零一学院，西安蓝脑科技有限公司，成都锦城学院，西北农林科技大学，海南大学，重庆大学，西安欧亚学院，西北大学，西那瓦国际大学(泰国)，西安理工大学，上海信昊信息科技有限公司，上海工程技术大学，广西科技大学，广西立新科技产业有限公司。

本文件主要起草人：庄文斌，郝鹏磊，刘婧婧，曹渊，朱敏波，朱进山，韦新，东晨，陈世卿，王建，李征骥，李三雁，张志敏，王博知，韦博鲲，段玉聪，路建国，宋永端，杨猛，赵闪光，郑小伟，李学平, 熊文阔，龚才春，赵国帅，周伯韬，周建伟，李高健，李奇，包奇，张健，陶震，朱惠英，王钊锦，李树衡，蔡伟逸。

本文件为首次发布。

量子通信网络设备接口技术规范

1 范围

本标准规定了量子通信网络设备接口的通用技术要求，包括QKD与QKS之间的应用接口、QKS与APP之间的输出接口的连接方式、协议说明。

本标准适用于量子密钥分发（QKD）设备、量子密钥管理设备（QKS）、量子密钥应用设备（APP）等核心组件的设计、研发、集成及部署，也可用于指导量子通信网络系统的检测。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。

DL/T 2399—2021 电力量子保密通信系统密钥交互接口技术规范

GB/T 15843.2—2024 网络安全技术 实体鉴别 第2部分：采用鉴别式加密的机制（即将实施，预计实施日期：2025-04-01）

GM/T 0006—2023 密码应用标识规范

GM/T 0050—2016 密码设备管理 设备管理技术规范

YD/T 4301—2023 量子保密通信网络架构

YD/T 4410.1—2023 量子密钥分发（QKD）网络Ak接口技术要求 第1部分：应用程序接口（API）

3 术语和定义

3.1 经典信道 Classical Channel

传输经典信号的信道。。[引用标准：YD/T 4301—2023，3.1]

3.2 量子信道 Quantum Channel

用于传输量子信号的通信信道。。[引用标准：YD/T 4301—2023，3.8]

3.3 量子密钥 Quantum Key

以量子态为信息载体，基于量子不可克隆、不可分割定理，通过量子信道与经典信道协商出的对称随机比特序列。[引用标准：DL/T 2399—2021，3.4]

3.4 量子保密通信系统 Quantum Secure Communication System

基于量子密钥分发和密码技术实现安全通信的系统，系统主要包括量子密钥应用设备、量子密钥管理设备及量子密钥生成设备。[引用标准：DL/T 2399—2021，3.7]

3.5 量子密钥生成设备 Quantum Key Generation Device

通过量子信道与经典信道协商生成量子密钥的设备。[引用标准：DL/T 2399—2021，3.8]

3.6 量子密钥管理设备 Quantum Key Management Device

由量子密钥生成设备获取量子密钥，进行密钥管理，并向量子密钥应用设备提供量子密钥的设备。实际系统中，量子密钥管理设备通常可独立存在，也可与量子密钥生成设备集成。[引用标准：DL/T 2399—2021，3.9]如QKS设备。

3.7 量子密钥应用设备 Quantum Key Application Device

应用量子密钥进行加解密或认证的设备。[引用标准：DL/T 2399—2021，3.10]

4 连接方式

量子保密通信系统通常由量子密钥分发设备（QKD）、量子密钥管理设备（QKS）、量子密钥应用设备（APP）、量子密钥管控中心和量子网络管理系统组成。本规范描述QKD与QKS之间的应用接口和QKS与APP之间的输出接口。QKD与QKS之间通过网口连接，采用TCP长连接方式，端口号为5551；QKS与APP之间同样通过网口连接，采用TCP长连接方式，端口号为13579。这些接口在系统中的位置如下图所示。

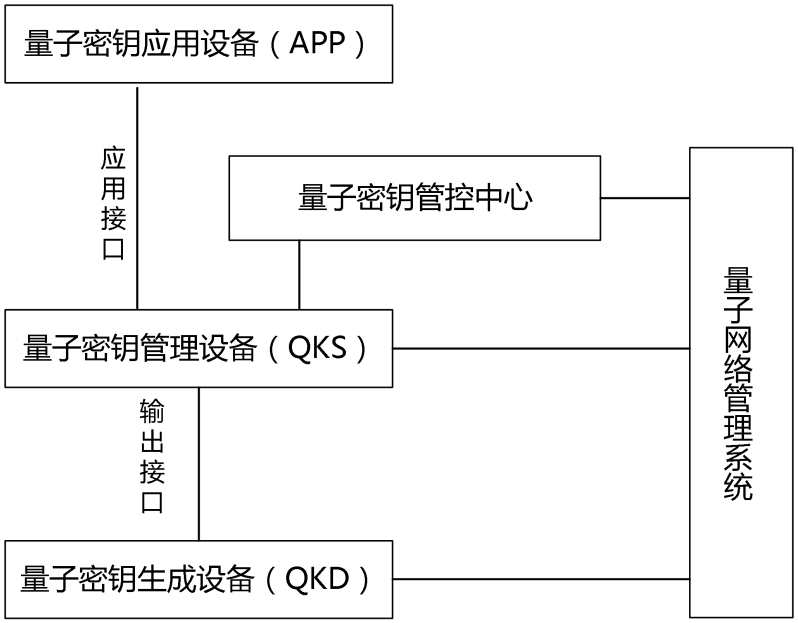

图 1 量子通信网络设备接口示意图

4.1 基本要求

在通用设计方面，本协议采用大端字节序，编码设计时考虑兼容不同平台、操作系统、硬件（含不同厂家密码卡、安全芯片）、软件算法，同时建议设备间时间同步（非必需）。在安全设计方面，要求两个实体设备之间进行身份认证，采用SM4_CBC和SM3_HMAC保证数据的机密性和完整性，其它说明如下：

a) 鉴于量子保密通信网络的特殊性，本规范采用对称密钥进行实体间的身份认证，采用 GB/T 15843.2—2024《网络安全技术 实体鉴别 第 2 部分：采用鉴别式加密的机制》7.3.3 节三次传递鉴别机制。

b) 实体间若采用长连接方式，双方应建立并长期保持该连接，若采用短连接方式，单次数据发送后即断开连接，需要发送数据时重新启动连接。

c) 认证密钥更新要求：认证密钥在实体双方进行身份认证时使用，相对来说使用次数小，加密信息量较少，更换周期长，一般可采用人工方式更新。

d) 业务（会话）密钥更新要求：用于加密设备之间的通信数据，使用比较频繁，加密数据量大，应及时进行更换，更新周期通常与业务需求相关，可自行定义。对于不能中断的业务密钥更新时应无感更新。

4.2 交互流程

4.2.1 QKD 与 QKS 之间的应用接口交互流程

QKD向QKS输出量子密钥，主要包含以下操作：设备入网、状态上报、会话创建、密钥推送、会话销毁、设备离网，示意图如下。

图 2 QKD 与 QKS 协议交互流程

如上图所示，展示了QKD与QKS间的交互流程，相关接口协议说明如下表。

表 1 QKD 与 QKS 交互接口协议列表

序号	名称	描述	物理连接	备注
1	设备入网	QKD 与 QKS 进行身份认证并建立数据加密传输通道	网口	必选
2	状态上报	QKD 定时向 QKS 上报状态，可作为心跳使用	网口	推荐

3	会话创建	QKD 以链路为单位与 QKS 建立量子密钥推送的服务会话，一台设备可以有多个服务会话	网口	必选
4	密钥推送	QKD 一链路为单位向 QKS 推送密钥，通常一个服务会话会包含多次推送	网口	必选
5	会话销毁	QKD 销毁与 QKS 间的指定链路会话	网口	推荐
6	设备离网	QKD 断开与 QKS 间的连接，并销毁连接对象	网口	必选

4.2.2 QKS 与 APP 之间的输出接口交互流程

APP向QKS获取量子密钥，主要包含以下操作：设备入网、状态上报、量子密钥服务申请、量子密钥申请、量子密钥服务撤销、设备离网，示意图如下。

图 3 APP 与 QKS 协议交互流程

如上图所示，展示了APP与QKS间的交互流程，相关接口协议说明如下表。

表 2 APP 与 QKS 交互接口协议列表

序号	名称	接口名称	描述	物理连接	备注
1	设备入网	qcf_app_login	APP 与 QKS 进行身份认证并建立数据加密传输通道	网口	必选

2	状态上报	qcf_app_upload_status	APP 定时向 QKS 上报状态，可作为心跳使用	网口	推荐
3	量子密钥服务申请	qcf_app_open_session	APP 与 QKS 建立量子密钥申请服务的会话，一台设备可以有多个服务会话	网口	必选
4	量子密钥申请	qcf_app_get_key	APP 向 QKS 申请密钥，通常一个服务会话会包含多次申请	网口	必选
5	量子密钥服务撤销	qcf_app_close_session	APP 销毁与 QKS 间的指定服务会话	网口	推荐
6	设备离网	qcf_app_logout	APP 断开与 QKS 间的连接，并销毁连接对象	网口	必选

5 协议说明

5.1 QKD 与 QKS 之间的应用接口交互协议说明

5.1.1 协议格式

通信协议报文格式包含消息头、消息体和消息尾。

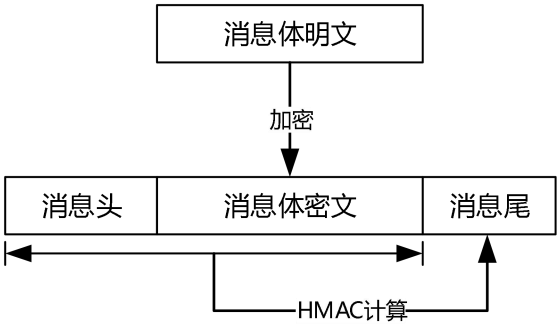

图 4 数据格式及加密机制

如上图所示，消息体明文数据进行SM4加密后得到消息体密文，消息头与消息体密文组合后共同计算HMAC得到校验值，校验值填充至消息尾，解密为上述过程的逆操作。

a) 消息头

消息头主要定义了报文的基本信息，包括协议标识、版本号、消息ID等，如下表所示。

表 3 消息头格式定义

名称	长度（字节）	说明
协议标识	4	唯一标识一个协议，主要用于区分协议，固定为 0xA1A2A3A4
版本号	1	0x01
安全模式	1	高 4 位表示加解密算法，低四位表示 MAC 算法，当该值为 0 时表示不加密并采用 SM3 作为 MAC 算法，当该值为 0x11 时表示采用 SM4_CBC+SM4_HMAC 算法套件
保留	2	保留,置零 0x00
接收方ID	4	消息接收方设备 ID

发送方ID	4	消息发送方设备 ID
消息ID	8	从 1 递增，重建清零
功能标识	2	0x00A1：设备入网 0x00A2：状态上报 0x00A3：会话创建 0x00A4：密钥推送 0x00A5：会话销毁 0x00A6：设备离网
消息体长度	4	消息体长度，若加密则为加密后的消息体长度

a) 消息尾

消息尾主要定义了报文的校验信息，包含校验值长度、校验值，如下表所示。

表 4 消息尾格式定义

名称	长度（字节）	说明
校验值长度	4	校验值长度
校验值	N	根据消息头和消息体计算得到的 HMAC 校验值

b) 消息体

消息体主要定义了报文的具体内容用于承载业务数据，业务不同，承载的数据也不同，在数据传输中，消息体需进行加密保护。

在采用对称密钥加密时通常会涉及IV和数据填充，对其规定如下：

1) 加密 IV 通过计算当前数据包消息头的 MAC 值获得，取前 16 字节。由于消息 ID 不同，每一包的 IV 也将不同。
2) 加密填充方法参考 GM/T 0050—2016《密码设备管理 设备管理技术规范》标准 8.1 节描述，采用第一个字节为 0x80，其后为 0x00，填充到分组长度的整数倍（消息头明文长度为分组长度整数倍时也应进行填充）。

5.1.2 设备入网

设备入网是QKD与QKS之间、QKS与APP之间建立安全传输通道的过程，其主要包含身份认证和加密通道的建立。通常QKD或APP启动并完成配置后，即开始自动向QKS发起设备入网申请，若申请失败，则再次申请（申请时间间隔可配置，默认为30秒）。

5.1.2.1 认证流程

本协议规定身份认证采用GB/T 15843.2—2024《网络安全技术 实体鉴别 第2部分：采用鉴别式加密的机制》7.3.3节三次传递鉴别机制。

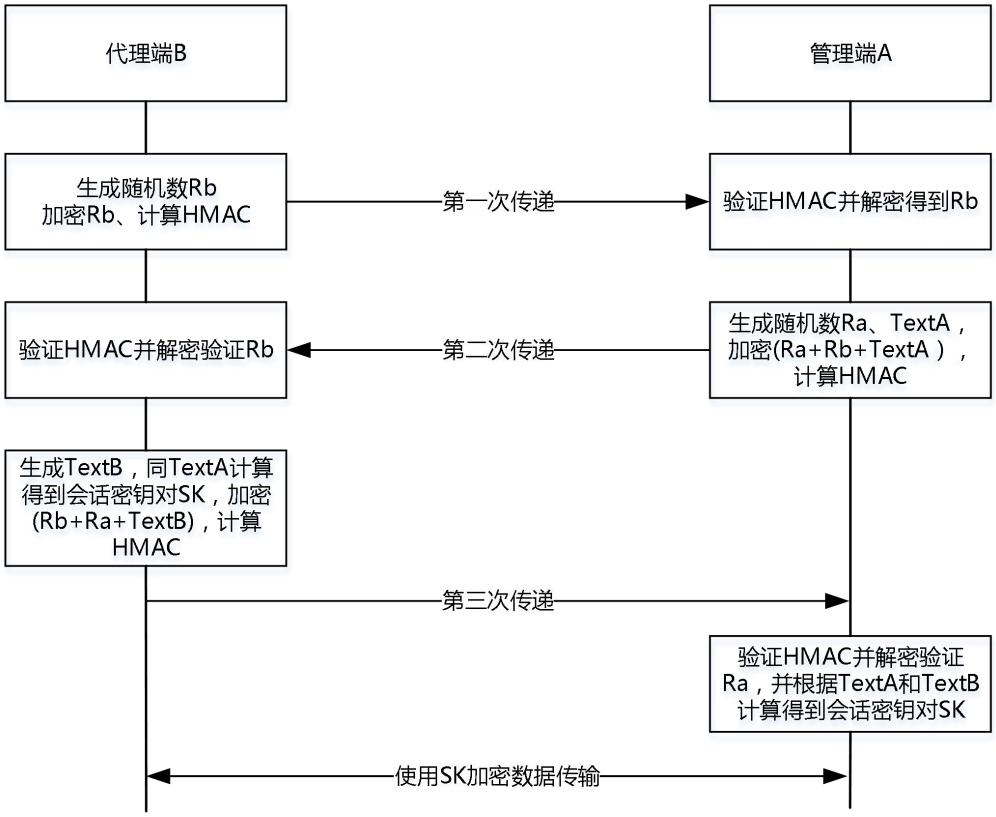

图 5　基于对称密钥的安全通道协议及三次传递鉴别

基于对称密钥的身份认证如图所示，通信双方预置对称密钥，并将对称密钥分成2个部分，每个部分2组密钥。第1部分是A到B方向，K^{1}_{AB}用于加密PDU消息敏感数据，K^{2}_{AB}用于计算安全通道整个数据格式的HMAC；第2部分是B到A方向，K^{1}_{BA}用于加密PDU消息敏感数据，K^{2}_{BA}用于计算安全通道整个数据格式的HMAC。

a) 代理端 B 产生成随机数 R_b，使用K^{1}_{BA}加密 R_b, K^{2}_{BA}计算 HMAC,组织数据发送至管理端 A；
b) 管理端 A 使用K^{2}_{BA}验证报文完整性，K^{1}_{BA}解密得到 R_b，之后生成随机数 R_a和 TextA，使用K^{1}_{AB}加密(R_bR_aTextA)，K^{2}_{AB}计算 HMAC，组织数据发送至代理端 B；
c) 代理端 B 使用K^{2}_{AB}验证报文完整性，K^{1}_{AB}解密得到(R_aR_bTextA)，验证 R_b一致性后生成 TextB，同时使用 TextA 和 TextB 生成会话密钥对 SK，之后使用K^{1}_{BA}加密(R_bR_aTextB)，K^{2}_{BA}计算 HMAC，组织数据发送至管理端 A，；
d) 管理端 A 使用K^{2}_{BA}验证报文完整性，K^{1}_{BA}解密得到(R_bR_aTextB)，验证 R_a一致性后，使用 TextA 和 TextB 生成会话密钥对 SK。

注：关于TextA包含16字节随机数A1+16字节随机数A2，TextB包含16字节随机数B1+16字节随机数B2，会话密钥SK由数据加密密钥和HMAC计算密钥组成，数据加密密钥为（A1⊕B1），HMAC计算密钥为（A2⊕B2）。

5.1.2.2　消息格式

入网协商第一帧消息体格式如下表。

表 5　入网协商第一帧消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-入网协商第一帧
设备标识	4	QKD设备ID
协商数据B的长度	2	协商数据B的长度，暂固定为32
协商数据B	N	B端产生的协商随机数R_b

入网协商第二帧消息体格式如下表。

表 6　入网协商第二帧消息体格式（QKS->QKD）

名称	长度（字节）	说明
消息类型	1	0x02-入网协商第二帧
协商数据A的长度	2	协商数据A的长度，本协议固定为32
协商数据A	N	A端产生的协商随机数R_a
协商数据B的长度	2	协商数据B的长度，本协议固定为32
协商数据B	N	B端的协商随机数R_b
附加数据长度	2	协商所需的附加数据长度，本协议固定为32
附加数据	N	附加数据，用于产生会话密钥对，前16字节作为数据传输加密密钥分量，后16字节作为HMAC计算密钥分量

入网协商第三帧消息体格式如下表。

表 7　入网协商第三帧消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x03-入网协商第三帧
协商数据B的长度	2	协商数据B的长度，同入网协商第一帧
协商数据B	N	B端的协商随机数R_b
协商数据A的长度	2	协商数据A的长度，同入网协商第二帧
协商数据A	N	A端的协商随机数R_a
附加数据长度	2	协商所需的附加数据长度，同入网协商第二帧
附加数据	N	附加数据，用于产生会话密钥对，前16字节作为数据传输加密密钥分量，后16字节作为HMAC计算密钥分量

当协商流程出错时，检测到错误的一方向另一方发送协商通告。入网协商通告帧消息体格式如下表。

表 8　入网协商通告帧消息体格式

名称	长度（字节）	说明
消息类型	1	0x04-入网协商通告帧
通告类型	1	0x01-入网协商第一帧应答通告 0x02-入网协商第二帧应答通告 0x03-入网协商第三帧应答通告
协商结果	4	0-成功，非0-错误（待定义）
描述长度	2	通告描述长度，长度范围0-255，若长度为0，无后续字段
描述	N	通告描述

5.1.3 状态上报

状态上报可以作为心跳使用，每隔30s上报一次，在特殊要求下（如不关心设备状态的应用场景），可不进行状态上报。当QKD连续3次未收到应答，则主动断开与QKS之间的连接；当QKS在2分钟内没有收到QKD的状态上报信息，则主动断开与QKD之间的连接。具体格式如下：

表 9 状态上报消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-状态上报
工作状态	4	0-正常，非0-异常

表 10 状态上报应答消息体格式（QKS->QKD）

名称	长度（字节）	说明
消息类型	1	0x02-状态上报应答
应答码	4	0x00

5.1.4 会话创建

当设备入网成功后，QKD即可向QKS进行会话创建申请，此消息的主要作用是QKS对QKD的策略和申请信息进行验证。

表 11 会话创建消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-会话创建
策略标识	4	本次会话的QKD策略ID
最大密钥块数	4	单次量子密钥推送的最大密钥块数，默认为1024
超时时间	4	单次量子密钥推送的超时时间，以毫秒为单位，默认为3000ms

表 12 会话创建应答消息体格式（QKS->QKD）

名称	长度（字节）	说明
消息类型	1	0x02-会话创建应答
策略标识	4	QKD策略ID
结果	4	0-成功，非0-失败

5.1.5 密钥推送

表 13 密钥推送消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-密钥推送
策略标识	4	QKD策略ID
密钥块个数	2	N个密钥块（N=1~1024，可配置）
密钥块数据	N×（4+1024）	前4字节为密钥编号，策略标识和密钥编号结合唯一标识一个密钥，最后1024字节为密钥数据（密钥编号掉电保存）

表 14　密钥推送应答消息体格式（QKS->QKD）

名称	长度（字节）	说明
消息类型	1	0x02-密钥推送应答
策略标识	4	QKD策略ID
结果	4	0-成功，非0-失败

5.1.6　会话销毁

当QKD端无需向QKS推送量子密钥时，QKD应销毁和QKS的服务会话，具体格式如下。

表 15　会话销毁消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-会话销毁
策略标识	4	本次待销毁会话的QKD策略ID

表 16　会话销毁应答消息体格式（QKS->QKD）

名称	长度（字节）	说明
消息类型	1	0x02-会话销毁应答
策略标识	4	本次销毁会话的QKD策略ID
结果	4	0-成功，非0-失败

5.1.7　设备离网

当QKD需要离网时，应向QKS发送设备离网请求，具体格式如下：

表 17　设备离网消息体格式（QKD->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-设备离网
设备标识	4	QKD设备ID

表 18　设备离网应答消息体格式（QKS->QKD）

名称	长度（字节）	说明
消息类型	1	0x02-设备离网应答
结果	4	0-成功，非0-失败

5.2　QKS 与 APP 之间的输出接口交互协议说明

5.2.1　协议格式

通信协议报文格式包含消息头、消息体和消息尾。

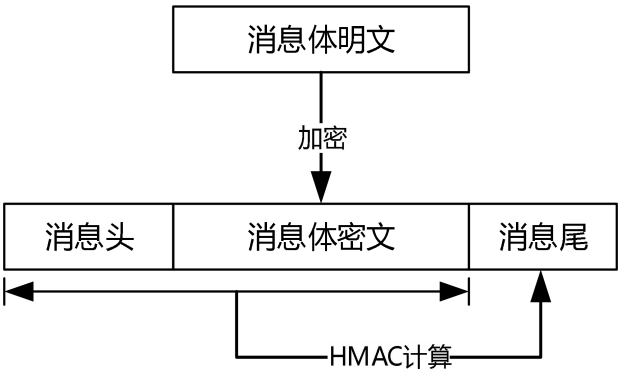

图 6　数据格式及加密机制

如上图所示，消息体明文数据进行SM4加密后得到消息体密文，消息头与消息体密文组合后共同计算HMAC得到校验值，校验值填充至消息尾，解密为上述过程的逆操作。

c)　消息头

消息头主要定义了报文的基本信息，包括协议标识、版本号、消息ID等，如下表所示。

表 19　消息头格式定义

名称	长度（字节）	说明
协议标识	4	唯一标识一个协议，固定为 0xA1B2C3D4
版本号	1	0x01
安全模式	1	0x01-表示采用 SM4-SM3 算法
保留	2	保留，置零 0x00
接收方ID	4	消息接收方设备 ID
发送方ID	4	消息发送方设备 ID
消息ID	8	从 1 递增，重建清零
功能标识	2	0x00B1：设备入网 0x00B2：状态上报 0x00B3：量子密钥服务申请 0x00B4：量子密钥申请 0x00B5：量子密钥服务撤销 0x00B6：设备离网
消息体长度	4	消息体长度，若加密则为加密后的消息体长度

d)　消息尾

消息尾主要定义了报文的校验信息，包含校验值长度、校验值，如下表所示。

表 20　消息尾格式定义

名称	长度（字节）	说明
校验值长度	4	校验值长度
校验值	N	根据消息头和消息体计算得到的 HMAC 校验值,可根据安全模式中定义的 MAC 算法获知其长度

e)　消息体

消息体主要定义了报文的具体内容用于承载业务数据，业务不同，承载的数据也不同，在数据传输中，消息体需进行加密保护。

在采用对称密钥加密时通常会涉及IV和数据填充，对其规定如下：

1) IV 通过计算当前数据包消息头的 MAC 值（默认使用 SM3 算法，取后 16 字节）获得，由于消息 ID 不同，每一包的 IV 也将不同。
2) 加密填充方法参考 GM/T 0006—2023《密码应用标识规范》标准 8.1 节描述，采用第一个字节为 0x80，其后为 0x00，填充到分组长度的整数倍（明文长度为分组长度整数倍时也应进行填充）。

5.2.2 设备入网

设备入网是APP与QKS之间建立安全传输通道的过程，其主要包含身份认证和加密通道的建立。通常APP启动并完成配置后，即开始自动向QKS发起设备入网申请，若申请失败，则再次申请（申请时间间隔可配置，默认为30秒）。

5.2.2.1 认证流程

本协议规定身份认证采用GB/T 15843.2—2024《网络安全技术 实体鉴别 第2部分：采用鉴别式加密的机制》7.3.3节三次传递鉴别机制。

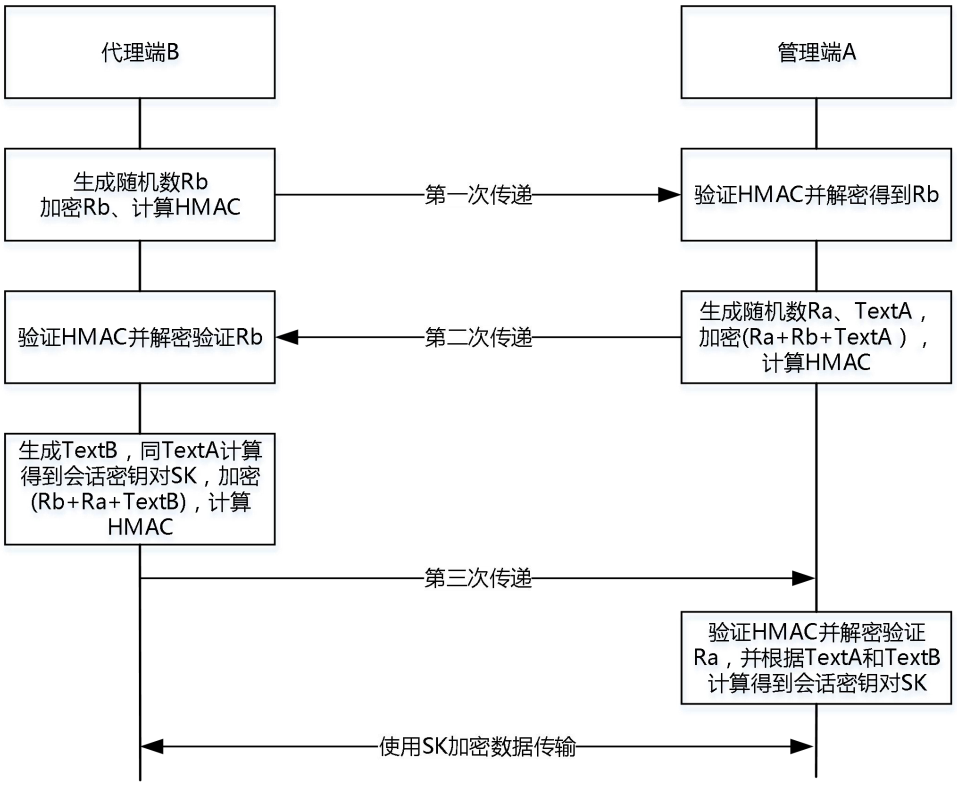

图 7 基于对称密钥的安全通道协议及三次传递鉴别

基于对称密钥的身份认证如图所示，通信双方预置对称密钥（加解密密钥为单向密钥），并将对称密钥分成2个部分，每个部分2组密钥。第1部分是A到B方向，K_{AB}^{1}用于加密PDU消息敏感数据，K_{AB}^{2}用于

计算安全通道整个数据格式的HMAC；第2部分是B到A方向，K^{1}_{BA}用于加密PDU消息敏感数据，K^{2}_{BA}用于计算安全通道整个数据格式的HMAC。

e) 代理端 B 产生成随机数 R_b，使用K^{1}_{BA}加密 R_b, K^{2}_{BA}计算 HMAC,组织数据发送至管理端 A；
f) 管理端 A 使用K^{2}_{BA}验证报文完整性，K^{1}_{BA}解密得到 R_b，之后生成随机数 R_a和 TextA，使用K^{1}_{AB}加密(R_bR_aTextA)，K^{2}_{AB}计算 HMAC，组织数据发送至代理端 B；
g) 代理端 B 使用K^{2}_{AB}验证报文完整性，K^{1}_{AB}解密得到(R_aR_bTextA)，验证 R_b一致性后生成 TextB，同时使用 TextA 和 TextB 生成会话密钥对 SK，之后使用K^{1}_{BA}加密(R_bR_aTextB)，K^{2}_{BA}计算 HMAC，组织数据发送至管理端 A，；
h) 管理端 A 使用K^{2}_{BA}验证报文完整性，K^{1}_{BA}解密得到(R_bR_aTextB)，验证 R_a一致性后，使用 TextA 和 TextB 生成会话密钥对 SK。

注：关于TextA包含16字节随机数A1+16字节随机数A2，TextB包含16字节随机数B1+16字节随机数B2，会话密钥SK由数据加密密钥和HMAC计算密钥组成，数据加密密钥为（A1⊕B1），HMAC计算密钥为（A2⊕B2）。

5.2.2.2 消息格式

入网协商第一帧消息体格式如下表。

表 21 入网协商第一帧消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-入网协商第一帧
设备标识	4	APP设备ID
协商数据B的长度	2	协商数据B的长度，暂固定为32
协商数据B	N	B端产生的协商随机数R_b

入网协商第二帧消息体格式如下表。

表 22 入网协商第二帧消息体格式（QKS->APP）

名称	长度（字节）	说明
消息类型	1	0x02-入网协商第二帧
协商数据A的长度	2	协商数据A的长度，本协议固定为32
协商数据A	N	A端产生的协商随机数R_a
协商数据B的长度	2	协商数据B的长度，本协议固定为32
协商数据B	N	B端的协商随机数R_b
附加数据长度	2	协商所需的附加数据长度，本协议固定为32
附加数据	N	附加数据，用于产生会话密钥对，前16字节作为数据传输加密密钥分量，后16字节作为HMAC计算密钥分量

入网协商第三帧消息体格式如下表。

表 23 入网协商第三帧消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x03-入网协商第三帧
协商数据B的长度	2	协商数据B的长度，同入网协商第一帧

协商数据B	N	B端的协商随机数R_b
协商数据A的长度	2	协商数据A的长度，同入网协商第二帧
协商数据A	N	A端的协商随机数R_a
附加数据长度	2	协商所需的附加数据长度，同入网协商第二帧
附加数据	N	附加数据，用于产生会话密钥对，前16字节作为数据传输加密密钥分量，后16字节作为HMAC计算密钥分量

当协商流程出错时，检测到错误的一方向另一方发送协商通告，通告数据帧消息头安全模式字段值为0x00。入网协商通告帧消息体格式如下表。

表 24　入网协商通告帧消息体格式

名称	长度（字节）	说明
消息类型	1	0x04-入网协商通告帧
通告类型	1	0x01-入网协商第一帧应答通告 0x02-入网协商第二帧应答通告 0x03-入网协商第三帧应答通告
协商结果	2	0-成功，非0-错误（待定义）
描述长度	2	通告描述长度，长度范围0-255，若长度为0，无后续字段
描述	N	通告描述

5.2.3　状态上报

状态上报可以作为心跳使用，每隔30s上报一次，在特殊要求下（如不关心设备状态的应用场景），可不进行状态上报（不上报时，QKS在APP登录后视其始终在线）。当APP连续3次未收到应答，则主动断开与QKS之间的连接；当QKS在2分钟内没有收到APP的状态上报信息，则主动断开与APP之间的连接；若APP不进行状态上报，QKS则认为APP始终处于连接状态。具体格式如下：

表 25　状态上报消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-状态上报
工作状态	4	0-正常，非0-异常
主机版本	4	例如版本号V1.0.0.2，表示为0x01 0x00 0x00 0x02
CPU使用率	4	百分比扩大100倍后十进制展示，如：56.23%表示为5623
内存使用率	4	百分比扩大100倍后十进制展示，如：56.23%表示为5623

表 26　状态上报应答消息体格式（QKS->APP）

名称	长度（字节）	说明
消息类型	1	0x02-状态上报应答
应答码	1	0x00

5.2.4　量子密钥服务申请

当设备入网成功后，APP即可向量子密钥服务申请，此消息的主要作用是QKS对APP的策略和申请信息进行验证。

表 27　量子密钥服务申请消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-量子密钥服务申请
策略ID	4	量子密钥服务策略标识
读取模式	1	0-双端请求方式，1-单端请求单端推送方式，固定为0
申请次数	4	密钥申请总次数，当达到该次数时，撤销量子密钥服务申请
密钥长度	4	单次量子密钥申请需要的密钥长度，范围16B-1MB，16字节整数倍
超时时间	4	单次量子密钥申请的超时时间，以秒为单位，默认为3s

表 28　量子密钥服务申请应答消息体格式（QKS->APP）

名称	长度（字节）	说明
消息类型	1	0x02-量子密钥服务申请应答
策略标识	4	量子密钥服务策略唯一标识
结果	1	0-成功，非0-失败

5.2.5　量子密钥申请

表 29　量子密钥申请消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-量子密钥申请
策略标识	4	量子密钥服务策略唯一标识
密钥标识	4	密钥的唯一标识，0-由QKS自动分配，非0-获取指定标识的密钥

表 30　量子密钥申请应答消息体格式（QKS->APP）

名称	长度（字节）	说明
消息类型	1	0x02-量子密钥申请应答
策略标识	4	量子密钥服务策略唯一标识
结果	1	0-成功，非0-失败，失败无后续字段
密钥标识	4	获取密钥的唯一标识
密钥数据	N	同量子密钥服务申请中密钥长度大小

5.2.6　量子密钥服务撤销

当APP端完成量子密钥服务申请所需的密钥量或无需再获取量子密钥时，APP应向QKS撤销量子密钥服务申请，具体格式如下。

表 31　量子密钥服务撤销消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-量子密钥服务撤销申请
策略标识	4	待撤销的密钥服务策略标识

表 32　量子密钥服务撤销应答消息体格式（QKS->APP）

名称	长度（字节）	说明
消息类型	1	0x02-量子密钥服务撤销申请应答
策略标识	4	撤销的密钥服务策略标识
结果	1	0-成功，非0-失败

5.2.7　设备离网

当APP需要离网时，应向QKS发送设备离网请求，具体格式如下：

表 33　设备离网消息体格式（APP->QKS）

名称	长度（字节）	说明
消息类型	1	0x01-设备离网
设备标识	4	APP设备ID

表 34　设备离网应答消息体格式（QKS->APP）

名称	长度（字节）	说明
消息类型	1	0x02-设备离网应答
结果	1	0-成功，非0-失败

6　附则

本标准应根据量子通信网络设备接口技术的发展和应用情况，定期进行修订和更新，确保标准的先进性和适用性。

本标准自发布之日起实施。本标准由归口广西电子商务企业联合会。