

SZSD

数 字 山 东 工 程 标 准

SZSD01 0003—2024

电子政务外网量子加密技术要求与实施 指南

Technical Requirements and Implementation Guidelines for Quantum Encryption in
E-government Extranet

2024 - 04 - 15 发布

2024 - 06 - 01 实施

济南市大数据局 发 布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 基本原则 2

 5.1 概述 2

 5.2 遵循国家密码管理原则 2

 5.3 等级保护合规性原则 3

 5.4 层级化管理原则 3

 5.5 准入测试原则 3

 5.6 备案原则 3

6 应用架构 3

 6.1 应用架构图 3

 6.2 量子密钥生成层 4

 6.3 量子密钥传输层 4

 6.4 量子密钥管理层 4

 6.5 量子密钥应用层 4

7 部署方式 4

 7.1 概述 4

 7.2 分支机构与中心部署 6

 7.3 终端系统部署 6

 7.4 量子安全服务部署 6

 7.5 业务系统部署 6

8 技术与管理要求 7

 8.1 功能要求 7

 8.2 性能要求 7

 8.3 接口要求 7

 8.4 管理要求 8

9 实施与应用 9

 9.1 应用场景 9

 9.2 密钥充注场景 9

 9.3 终端安全应用场景 10

 9.4 业务系统密码应用场景 10

参 考 文 献 11

前 言

本文件按照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。

本文件由济南大数据局提出、归口，并组织实施。

本文件起草单位：济南市大数据局、安徽问天量子科技股份有限公司、中电信量子信息科技集团有限公司、中国电信股份有限公司济南分公司、山东建筑大学。

本文件主要起草人：王越，李宁，高明阳，苗春华，刘婧婧，施红旗，王新莲，洪泰辉，赵林，杨蕾。

电子政务外网量子加密技术要求与实施指南

1 范围

本文件规定了电子政务外网系统量子加密的基本原则、应用架构、部署流程、技术要求和应用指南。

本文件适用于量子密码技术在省级、市级电子政务外网业务场景的应用。特别是量子密钥在认证、机密性保障、防篡改的防护等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
- GM/T 0014-2012 数字证书认证系统密码协议规范
- GM/T 0016-2012 智能密码钥匙密码应用接口规范
- GM/T 0018-2012 密码设备应用接口规范
- GM/T 0022-2014 IPSec VPN技术规范
- GM/T 0024-2014 SSL VPN技术规范
- GM/T 0028-2014 密码模块安全技术要求
- GM/T 0051-2016 密码设备管理 对称密钥管理技术规范
- GM/T 0103-2021 随机数发生器总体框架
- GM/T 0108-2021 骗态BB84量子密钥分配产品技术规范
- SZSD01 0014—2020 电子政务外网认证量子通信应用规范
- ISO/IEC 7816 识别卡 集成电路卡

3 术语和定义

下列术语和定义适用于本文件。

3.1

量子安全模块 quantum cryptographic module

适用于终端的量子密钥存储与安全算法模块，包括量子SIM卡、TF卡、U盾、软件密码模块和PCIE密码卡。

3.2

密钥管理系统 key management system

密钥生成、存储、分发、销毁、归档等生命周期的管理系统。

3.3

密钥池 key Pool

具有密钥存储和分发能力的安全模块。

3.4

密钥充注机 key filling machine

对密码模块中的密钥进行加注的设备。

3.5

量子随机数发生器 quantum random number generator

基于量子力学原理所保证的真随机数生成设备。

3.6

量子密钥分配终端 quantum key distribution product

具有量子密钥分发功能的设备。

3.7

密钥更新周期 key update cycle

密钥更新的时间间隔。

3.8

加密延时 encryption delay

密码设备利用密钥和加密算法对数据加密或解密过程所耗费的时间。

3.9

会话密钥 session key

会话密钥包括数据加密密钥和校验密钥。其中数据加密密钥用于数据的加密和解密, 校验密钥用于数据的完整性计算和校验。

3.10

认证密钥 authentication key

用于身份鉴别的密钥对, 包括签名密钥对和加密密钥对, 其中签名密钥对由安全设备自身密码模块产生, 加密密钥对应通过 CA 认证中心向 KMC 申请。用于握手过程中客户端身份鉴别。

3.11

密钥加密密钥 key encryption key

通信设备双方预置或者通过算法生成的密钥, 用于对会话密钥进行加密保护。

4 缩略语

QKD: 量子密钥分发 (Quantum Key Distribution)

VPN: 虚拟专用网 (Virtual Private Network)

CA: 电子认证服务 (Certificate Authority)

KMC: 密钥管理中心 (Key Management Center)

SKF: 安全钥匙函数 (Secure Key Function)

SDF: 安全设备函数 (Secure Device Function)

5 基本原则

5.1 概述

电子政务外网量子加密技术要求与实施, 主要是依托现有电子政务外网网络和政务办公应用技术设施, 建设并部署实施量子通讯密钥基础设施, 实现基于电子政务外网政务应用环境的数据量子密钥加密传输, 进一步提升党政机关网上、掌上政务办公安全保障水平。

5.2 遵循国家密码管理原则

应遵循《密码法》、《网络安全法》、《数据安全法》、《关键信息基础设施安全保护条例》、《商用密码应用安全性评估管理办法（试行）》、《商用密码管理条例》、《商用密码产品使用管理规定》、《信息系统密码应用基本要求》以及相关密码管理制度。

5.3 等级保护合规性原则

量子安全服务体系的部署实施应满足等保相关安全原则。遵循GB/T 39786 信息安全技术 信息系统密码应用基本要求。满足物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等。

5.4 层级化管理原则

建立全局的政务外网安全管理体系，包括市级和区县级的管理体系，各级政务外网建设运维单位分别负责该级量子安全服务体系的管理，并按照层级化管理方式层层负责，也可以根据实际情况集中统一管理，如市级可以集中统一管理本市的各级量子安全服务体系，确保政务外网系统安全保障措施的规范统一。

5.5 准入测试原则

政务外网量子安全服务技术体系相关产品在入网前应通过由国家电子政务外网管理中心统一组织的准入测试。

5.6 备案原则

业务单位成功申请并接入量子安全服务体系之后，本级政务外网建设运维单位应登记备案并上报上级建设运维单位，量子安全模块应妥善保管，丢失及时报备。

6 应用架构

6.1 应用架构图

电子政务外网的量子密钥应用架构包括量子密钥生成、量子密钥传输、量子密钥管理、量子密钥应用。电子政务外网的量子密钥应用架构如图1所示。

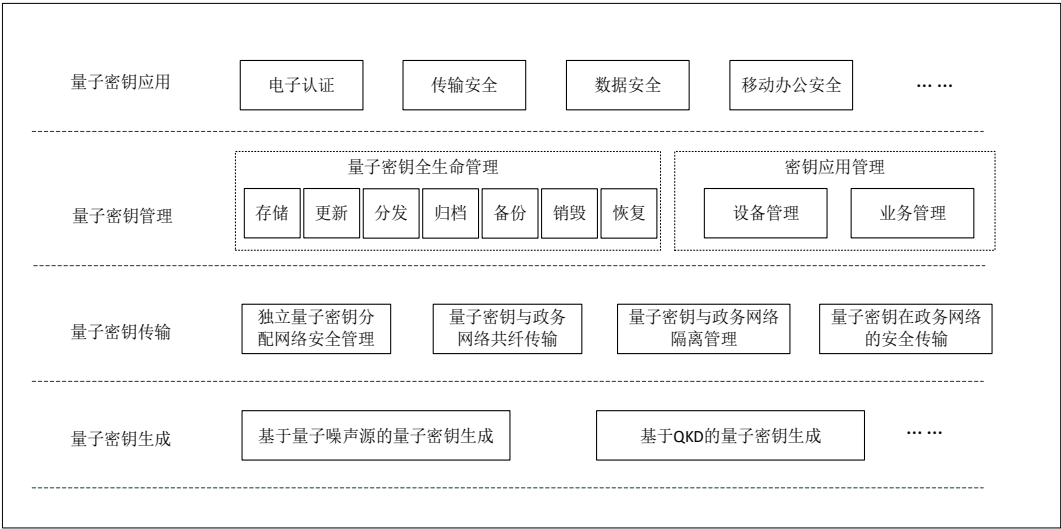


图1 政务外网的量子密钥应用架构图

6.2 量子密钥生成层

量子密钥生成层通过量子物理特性生成量子密钥，包括本地量子随机数发生器生成密钥和异地QKD设备生成量子密钥。

6.3 量子密钥传输层

量子密钥传输层独立于量子密钥分配网络，通过独立网络分配、共纤传输、隔离管理和融合管理等方式进行密钥的分发。

6.4 量子密钥管理层

量子密钥管理层实现密钥的存储、更新、分发、归档、备份、销毁和恢复等，同时进行密钥设备管理和业务管理。

6.5 量子密钥应用层

量子密钥应用层实现电子认证、传输安全保障、数据安全防护等。

7 部署方式

7.1 概述

山东省政务外网接入分三层级:包括省级、市级、县(市、区)级电子政务外网城域网。

接入方式:包括专线、VPN 两种方式，专线、VPN。

接入设备包括:

a) 以专线方式接入电子政务外网的接入部门，应通过网络设备或者安全设备等方式接入电子政务外网；

b) 不具备专线接入条件的接入部门，应通过 VPN 网关或 VPN 终端等方式接入电子政务外网县级及以下接入部门直接接入市级电子政务外网，VPN可使用IPSec和SSL协议。

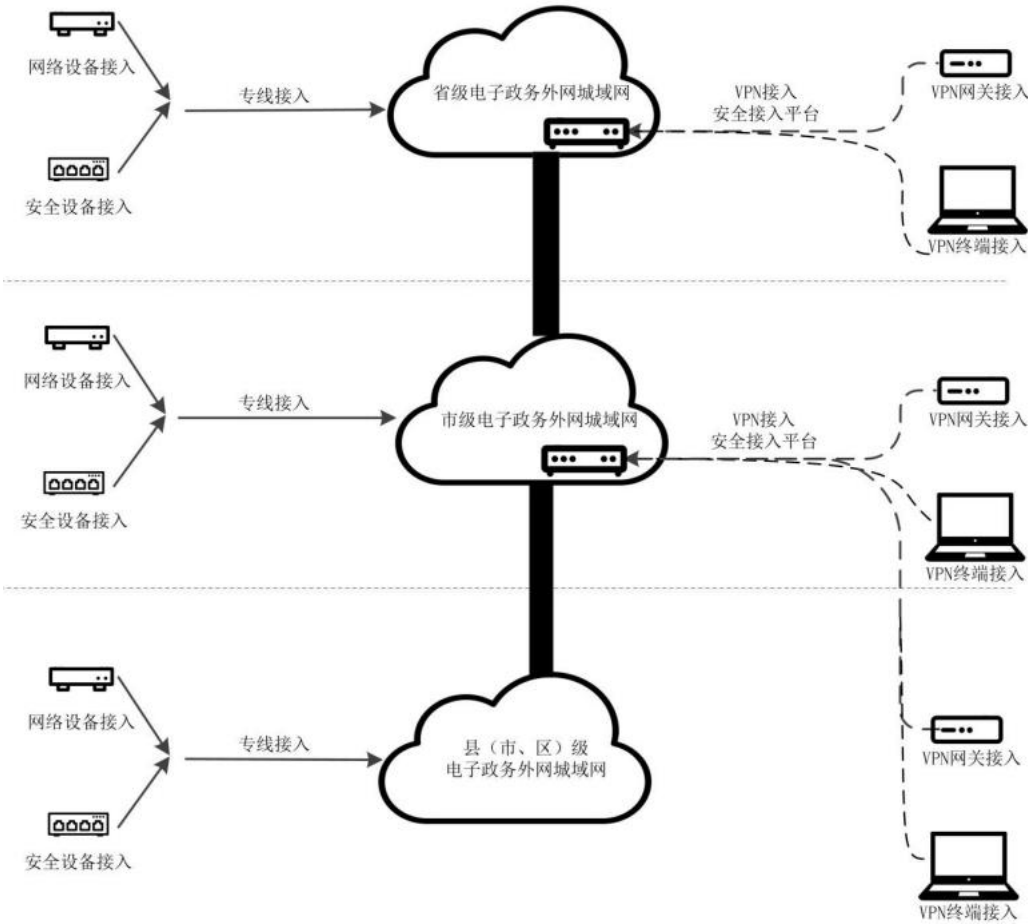


图2 接入框图

电子政务外网的量子密钥部署是在图2接入框图的基础上增加量子密钥应用与管理要求，部署上包括分支机构与中心部署、终端系统部署、量子安全服务部署、业务系统部署，部署方案见图3。

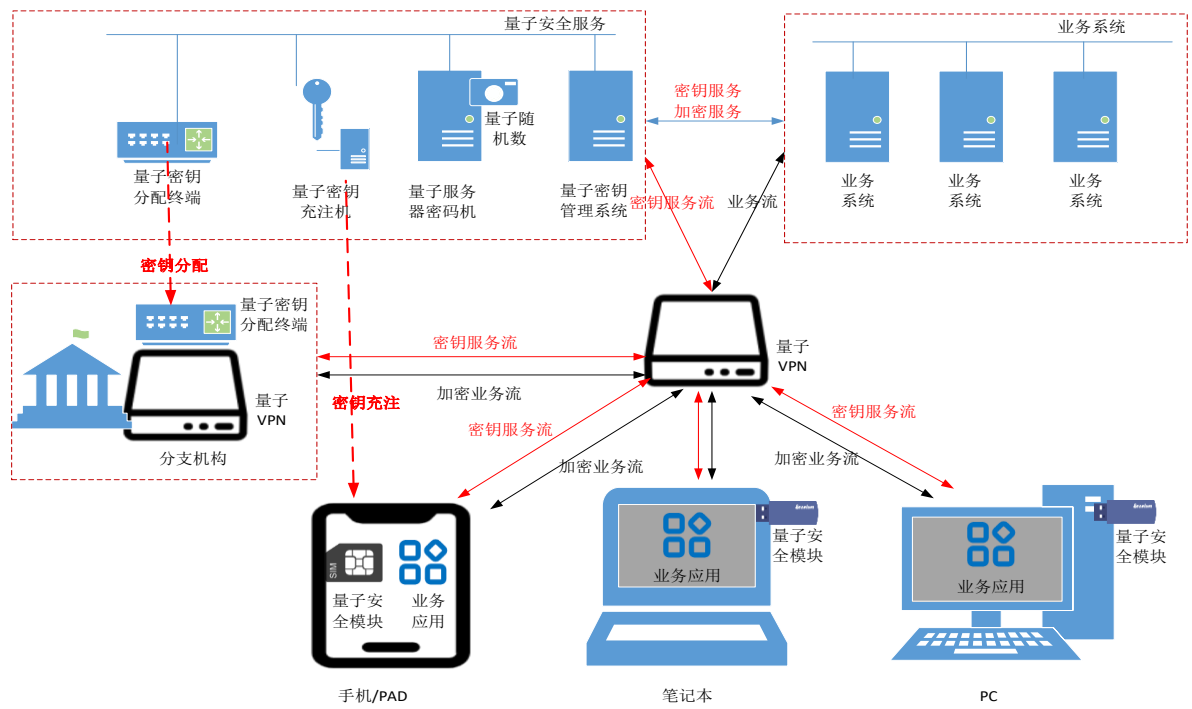


图3 部署方案图

7.2 分支机构与中心部署

在分支机构和中心分别部署量子密钥分配终端和量子VPN设备，将分支机构内部网络与中心业务系统联通。当分支机构与中心之间进行通信时，分支机构量子VPN设备首先从量子密钥分配终端获取密钥，同时中心部署的量子VPN设备也从另一端的量子密钥分配终端中获取相同的密钥，通信过程中两台量子VPN设备之间使用共同的密钥完成身份认证、完整性保护和数据加解密等服务。

7.3 终端系统部署

终端设备部署量子安全模块，量子安全模块以离线的方式提前通过量子密钥充注机获取量子密钥。当终端与业务系统之间进行入网认证、数据传输等业务时，使用量子安全模块内的密钥进行身份认证、完整性保护和数据加解密等。

7.4 量子安全服务部署

量子安全服务由量子密钥管理设备（如量子密钥管理系统或密钥服务平台）、量子服务器密码机和量子密钥充注机组成，应放置在安全的管理区。量子密钥充注机为量子安全模块提供量子密钥的充注，在量子安全模块使用之前以离线方式充注一定量的量子密钥。量子密钥充注机的密钥来源自量子服务器密码机。量子服务器密码机是密钥的存储设备，为身份认证、安全传输和数据存储安全提供密码服务。量子密钥管理设备在业务期间提供密钥的全生命周期管理。

7.5 业务系统部署

业务系统应用量子安全服务时需要先向量子安全服务系统进行申请，由量子密钥管理设备管理员登记业务系统的用户、单位、应用相关信息，并分配授权凭证。在业务应用过程中，通过接口调用量子安全服务提供的密钥申请、密码运算等功能。

8 技术与管理要求

8.1 功能要求

8.1.1 身份鉴别功能

采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性，包括终端设备身份鉴别和登录用户角色鉴别。

8.1.2 数据机密性

采用密码技术保证通信过程中的敏感信息或通信报文的机密性，保证服务端与终端业务数据存储的机密性，防止数据被非法窃取导致的信息泄露。

8.1.3 数据完整性

采用密码技术保证通信过程中数据的完整性，网络边界访问控制信息的完整性，业务存储数据、日志审计信息的完整性等。

8.1.4 不可抵赖性

在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；如采用密码技术保证事件过程、操作事项、通信内容的不可抵赖性。

8.2 性能要求

8.2.1 加密带宽

终端加密带宽 $\geq 2\text{Mbps}$ 。

8.2.2 加密延时

加密延时 $\leq 50\text{ms}$ 。

8.2.3 并发连接数

中心端量子VPN并发连接数 ≥ 1000 个。

8.2.4 密钥更新周期：

密钥更新周期：60-3600秒或一次一密。

8.3 接口要求

8.3.1 硬件接口要求

量子安全模块主要包括量子SIM卡、量子TF卡、量子U盾和量子PCIE密码卡，应分别满足以下接口要求：

- a) 量子SIM卡接口满足ISO/IEC 7816接口规范；
- b) 量子TF卡接口符合Micro SD接口规范；
- c) 量子U盾满足USB接口规范；
- d) 量子PCIE密码卡满足PCIE接口规范。

量子安全服务主要包括量子密钥充注机、量子服务器密码机、量子密钥管理设备，应满足

- a) 应具有RJ45电接口或光网络接口；
- b) 应具有USB接口。

量子VPN应满足：

- a) 应具有RJ45电接口或光网络接口；
- b) 应具有USB接口。

量子密钥分配终端应满足：

- a) 应具有RJ45电接口或光网络接口；
- b) 应具有USB接口；
- c) 应具有FC/PC量子光接口。

8.3.2 软件接口要求

软件接口主要包括终端量子安全模块接口和量子服务器密码机接口，应分别满足以下要求：

- a) 量子安全模块接口应满足国密SKF接口规范,GM/T 0016-2012 智能密码钥匙密码应用接口规范，其中PCIE密码卡应满足国密SDF接口规范，GM/T 0018-2012 密码设备应用接口规范；
- b) 量子服务器密码机接口应满足国密SDF接口规范，GM/T 0018-2012 密码设备应用接口规范。

8.3.1 协议要求

协议要求主要包括以下方面：

- a) 量子VPN应满足GM/T 0024-2014 SSL VPN技术规范 或 GM/T 0022-2014 IPSec VPN技术规范；
- b) 量子密钥分配终端应满足GM/T 0108-2021 诱骗态BB84量子密钥分配产品技术规范；
- c) 量子随机数发生器应满足GM/T 0103 随机数发生器总体框架；
- d) 量子服务器密码机应满足GM/T 0028-2014 密码模块安全技术要求；
- e) 量子安全模块应满足 GM/T 0028-2014 密码模块安全技术要求；
- f) 量子U盾应满足 GM/T 0016-2012 智能密码钥匙密码应用接口规范；
- g) 量子密钥管理设备应满足GM/T 0051密码设备管理 对称密钥管理技术规范。

8.4 管理要求

8.4.1 密钥的管理

密钥管理应遵循以下要求：

- a) 量子密钥分根密钥、认证密钥和签名密钥、密钥加密密钥和会话密钥；
- b) 签名密钥对由密码安全产品自身产生,其公钥应能被导出,由外部认证机构签发签名证书；
- c) 加密密钥对由外部密钥管理机构产生并由外部认证机构签发加密证书。加密密钥对的私钥保护方法见 GM/T 0014 数字证书认证系统密码协议规范；
- d) 签名证书、加密证书和加密密钥对的私钥应能被导入密码安全产品中；
- e) 在密码安全产品中，密钥的私钥应有安全保护措施；
- f) 密钥应按设定的安全策略进行更新；
- g) 密钥可以安全形式进行备份，并在需要时能够恢复；
- h) 会话密钥产生后应保存在易失性存储器中,达到其更新条件后应立即更换,在连接断开、设备断电时应销毁。

8.4.2 管理员的管理

管理员的管理应遵循以下要求：

- a) 密码安全产品应设置系统管理员、安全员和审计员，进行三员管理；
- b) 管理员进行系统配置、密钥生成、导入、备份和恢复等操作。管理员应持有表征用户身份信息(如证书、公私密钥对)的硬件装置, 与登录口令相结合登录系统, 进行管理操作前应通过身份鉴别；
- c) 登录口令长度应不小于8个字符，应包含大小写字母和特殊字符；
- d) 使用错误口令或非法身份登录的次数限制应小于或等于8。

8.4.3 设备资源的管理

设备资源的管理应遵循以下要求：

- a) 密码安全产品的初始化, 除由厂商进行的操作外, 系统配置、密钥的生成和管理、管理员的产生等均应由用户完成；
- b) 应对密码运算部件等关键部件进行正确性检查，应对存储的密钥等敏感信息进行完整性检查；在检查不通过时应报警并停止工作。

9 实施与应用

9.1 应用场景

量子加密技术的应用场景包括密钥充注场景、终端安全应用场景、业务系统密码应用场景。

9.2 密钥充注场景

密钥充注场景应在可控环境使用量子密钥充注机对量子安全模块进行密钥加注。主要过程包括充注管理员身份认证、充注密钥申请、充注密钥写入、充注密钥校验和充注密钥使用。

9.2.1 充注管理员身份认证

量子密钥充注机登录时，通过管理员U盾向量子密钥管理设备进行身份认证，U盾内包含管理员的数字证书，通过签名验签操作校验管理员身份合法性。

9.2.2 充注密钥申请

量子密钥充注机获取量子安全模块信息，向量子密钥管理设备请求充注密钥，量子密钥管理设备从量子服务器密码机或量子保密通信网络QKD中获取充注密钥，并使用量子安全模块的加密公钥以数字信封形式封装充注密钥，保护充注密钥下发过程。充注密钥申请时，根据量子安全模块的设备类型与应用场景，可指定充注密钥长度。

9.2.3 充注密钥写入

量子安全模块接收充注密钥数字信封，使用加密私钥解密数字信封。

9.2.4 充注密钥校验

对充注密钥密文进行校验，判断充注密钥的完整性并将充注密钥密文导入量子安全模块存储。

9.2.5 充注密钥使用

充注密钥应用于量子安全模块入网认证、会话密钥申请等场景。充注密钥基于一次一密原则使用，被使用过的充注密钥需要进行置零操作。

9.3 终端安全应用场景

业务终端包含PC端与移动端，业务终端软件集成量子安全模块并调用量子安全模块的功能接口。主要过程包括量子安全模块安全接入、终端身份认证、会话密钥申请、数据加密与解密。

9.3.1 模块安全接入

业务终端连接量子安全模块，量子安全模块枚举内部密码应用及容器并对应用PIN做验证。

9.3.2 终端身份认证

业务终端软件通过量子安全模块提供的身份认证接口与量子密钥管理设备进行双向身份认证，并获取量子密钥管理设备分发的身份令牌。

身份认证协议使用GB/T 15843.2 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制中约定的双向认证协议。

9.3.3 会话密钥申请

业务终端创建会话密钥ID，通过量子安全模块向量子密钥管理设备申请会话密钥。会话密钥传输过程使用充注密钥加密保护，在业务终端设备上，由充注密钥解密并导入量子安全模块。

9.3.4 数据机密性与完整性保护

业务终端通过量子安全模块使用会话密钥对数据进行加解密和完整性校验。

9.4 业务系统密码应用场景

量子密钥管理设备为用户业务系统提供统一的密钥管理与密码运算能力，业务系统通过接口调用完成密钥申请、密码运算等功能。

9.4.1 业务系统注册

量子密钥管理设备为业务系统提供用户、单位、应用授权等管理功能。业务系统在申请接入量子密钥管理设备时，由量子密钥管理设备管理员登记业务系统的用户、单位、应用相关信息，并分配授权凭证。

9.4.2 密码服务使用

业务系统在调用密码服务接口时，需要携带授权凭证。密码服务接口包括会话密钥申请、数据加解密、摘要生成校验、公钥加密/私钥解密、签名验签等。

会话密钥申请由业务系统传入会话ID，量子密钥管理设备根据ID创建密钥并配置权限。业务终端在权限认证通过后可申请根据会话ID申请密钥。

业务系统调用密码运算接口只需要传入会话ID和业务数据，密钥对于业务系统可用不可见。

参 考 文 献

- [1] GB/T 39786 信息安全技术 信息系统密码应用基本要求
- [2] GM/T 0008-2012 安全芯片密码检测准则
- [3] GM/T 0014-2012 数字证书认证系统密码协议规范
- [4] GM/T 0016-2012 智能密码钥匙密码应用接口规范
- [5] GM/T 0018-2012 密码设备应用接口规范
- [6] GM/T 0020-2012 证书应用综合服务接口规范
- [7] GM/T 0022-2014 IPSecVPN技术规范
- [8] GM/T 0024-2014 SSL VPN技术规范
- [9] GM/T 0028-2014 密码模块安全技术要求
- [10] GM/T 0030-2014 服务器密码机技术规范
- [11] GM/T 0050-2016 密码设备管理 设备管理技术规范
- [12] GM/T 0051-2016 密码设备管理 对称密钥管理技术规范
- [13] GM/T 0108-2021 诱骗态BB84量子密钥分配产品技术规范
- [14] GM/T 0103 随机数发生器总体框架
- [15] SZSD01 0014—2020 电子政务外网认证量子通信应用规范
- [16] ISO/IEC 7816 识别卡 集成电路卡
- [17] 中华人民共和国网络安全法
- [18] 中华人民共和国数据安全法
- [19] 中华人民共和国密码法
- [20] 中华人民共和国个人信息保护法
- [21] 中华人民共和国网络安全法
- [22] 关键信息基础设施安全保护条例
- [23] 商用密码管理条例
- [24] 商用密码产品使用管理规定
- [25] 商用密码应用安全性评估管理办法
- [26] 政务信息系统密码应用与安全性评估工作指南
- [27] DB37/T 4630.2-2023 电子政务外网 第2部分：网络接入要求