第三章 采购需求

一、项目基本信息

1、项目名称及编号：海南省购买信息化服务量子保密通信服务（项目编号：HNYH2019-19-0111）

2、采购预算：2700 万元（人民币贰仟柒佰万元整）包含所有费用，报价超出采购预算的视为无效报价。

3、采购单位：海南省大数据管理局

二、用户需求

1.建设目标

启动海南量子通信政务项目，以购买量子保密通信服务的方式，进一步覆盖省直及各厅局单位，为党政机关的政务办公、数据传输、视频会议等业务应用提供更高的信息安全保障。

以本次项目为基础，将服务范围逐步拓展到军民融合、金融、能源、数据中心、航空航天、军工等领域，为海南创新发展提供信息安全保障。

2.服务周期与地点

服务周期： 三年

服务地点：海南省海口市

3.服务内容及技术要求

3.1 项目范围

购买量子保密通信服务，在电子政务外网用户中，选择 20 个对信息安全要求高的省直部门接入海口量子保密通信城域网。由服务承接单位配合查勘选点。

3.2 服务内容

主要的服务内容如下

▲密钥更新服务

支持客户各业务接入点之间定期更新量子密钥的服务需求：

1）密钥取用的频率最低为 1 次/小时、最高可达 1 次/秒；

2）每次取用密钥长度为 1KB-63KB 可选（更新频率视选取的密钥长度决定）；

3）同时支持量子密钥、IKE 密钥的双重密钥保障机制。

▲硬件维修更换服务

客户购买/租赁的设备在维护期（含质保期和维保期，下同）内发生硬件故障时，服务承接单位在规定时限内为客户提供规定的硬件维修更换服务。

▲技术咨询服务

客户在使用过程中遇到疑问或技术帮助时，通过电话、传真、电子邮件等向服务承接单位提出技术咨询服务请求，服务承接单位应提供咨询服务，并尽最大努力、最大限度满足客户需求。

▲现场支持服务

对于电话支持不能解决的问题，服务承接单位根据客户协议规定的时限安排相关技术服务人员到现场提供支持服务。

当客户对现有量子通信系统存在变更/优化等需求，需要技术服务工程师到现场协助时，适用该项服务。系统变更不包括系统结构的变化，一般为设备维修、设备到货上架、设备连线等内容。若出现系统结构或系统解决方案的变化时，双方协商确认具体服务内容及服务报价。

▲系统升级服务

为修复系统软、硬件 bug 或潜在的系统运行风险，服务承接单位提供系统软、硬件升级服务以及客户提出系统软件新增功能或硬件升级等相关服务，新增功能需双方协商确认具体服务内容及服务报价。

▲系统状态巡检

服务承接单位按照一定时间周期对系统进行状态巡检，根据性能指标确定当前系统整体运行状态，排查系统潜在的故障，降低系统运行风险。

▲线上配置规范

服务承接单位根据客户的软硬件资源及功能需求列表，提供标准配置规范，提供最佳配置推荐，减少运行配置隐患，提升系统稳定性。

在对现有系统进行配置、拓扑变更时，服务承接单位需要对变更项评估变更风险，并与客户沟通确认。确认后方可实施，必要时在服务承接单位测试环境进行验证，验证通过，方可在现场与客户工程师共同完成变更操作。

▲重保支撑服务

在客户出现重要的业务时刻,根据合同或协议约定，服务承接单位可提供合同或协议约定的重保支撑服务内容。

重保支撑服务主要包括以下内容:

1）巡检服务：服务承接单位根据客户申请及双方协商的服务内容和巡检时间，对客户正在运行的量子通信网络进行全面健康检查，排除潜在隐患。巡检周期根据服务内容及协议而定。

2）现场备件服务：根据服务约定，按照现场设备的一定比例提供备件，以保证客户系统正常运行。

3）现场值守服务：在客户出现重要业务时刻时，服务承接单位根据客户服务申请，安排人员值守，并在值守期间进行应急处理。

备注：服务协议中重保需明确指出或标注重保支撑次数、时长。

▲客户人员培训

服务承接单位对客户提供培训服务，针对客户的不同技术人员、用户提供不同类型的服务，达到用户可自行操作、使用系统，技术支持/维护人员可对系统进行日常的维护。

▲网管支撑服务

1）网络性能指标

成码率：城域网各节点之间，以及城域网 QKD 设备链路之间，支持 30 秒、小时、天平均成码率上报。

密钥消耗量：用户节点支持 30 秒、小时、天消耗密钥量上报；配对用户节点之间支持 30 秒、小时、天消耗密钥量上报。

配对密钥量：用户节点支持 30 秒、小时、天配对可使用的中继密钥量上报；城域网各节点之间支持 30 秒、小时、天配对生成密钥量上报。

2）设备网元信息

支持按照设备类型每天统计全网设备数量。

支持每天汇总全网设备信息情况，包括如下信息：站点名称、设备名称、设备类型、设备型号、机箱编号、网元软件版本、插板型号、插板软件版本。

3）故障告警统计

支持按照告警级别实时统计系统告警数量。

支持实时统计涉及故障的设备与全网设备数量的占比。

3.3 技术路线

依托海口量子保密通信城域网，为政务单位提供量子保密通信接入服务，实现政务单位与大数据局之间通信数据的安全传输，提高数据传输安全等级。依据各政务单位需求，结合量子密钥的网络传输与最新的 IPSecVPN 协议对网络层进行二次加密封装，建立各政务单位至大数据局间数据网络加密传输隧道。

整个网络分为经典的数据传输网和量子密钥交换网络。其中：传统的数据传输网为海南省现有的电子政务网络；在不改变原有数据传输网络的情况下，叠加组建一张量子密钥交换网络。指定业务数据流向至量子安全加密路由器，在数据传输请求端和服务端建立量子加密通道，保证端到端数据传输安全。采用此方式，不影响现有数据传输的整体网络结构，相当于在现有网络基础上再加一把量子“锁”。各接入单位使用量子安全加密路由器（或量子 VPN 设备）使用量子密钥对数据进行加密，通过传统的 IP 网络进行数据加密传输。由量子通信城域网对量子网关设备产生的密钥进行网络分发，为量子 VPN 设备提供加解密密钥，实现数据传输的安全。

4.功能需求

4.1 政务云服务访问加密需求

采用量子保密通信技术对现有政务光缆网络链路加密提升整体政务外网的数据传输的安全性，提升对政务云服务访问数据传输的安全性，对海南省电子政务外网的网络安全具有重要意义。

4.2 量子密钥分发需求

本项目的量子密钥分发需求如下：

1）采用裸光纤实现量子密钥分发；

2）可支持任意用户节点间的量子密钥分发；

3）提供基本管理功能，设备兼容 SNMP 协议。

量子信息学是量子力学、计算机科学、信息与通信工程组成的交叉学科，拥有许多经典通信无法比拟的优势。在经典信息领域，基本的信息处理单位是比特。相对的在量子信息学中，基本的信息处理单位是量子比特。量子比特的本质是编码的量子态，拥有许多不同于经典比特的独特性质，例如叠加性、相干性等等。

由于量子态的性质和演化遵循的规律和经典物理有着显著的区别，所以将信息编码在量子态上将对信息的存储、传输和处理将产生巨大的变化。

量子密钥分发是量子信息学的重要分支，也是目前量子信息领域中实用化最为成熟的技术。量子密钥分发能够安全的将对称密钥分发给合法的通信双方，其安全性基于量子物理原理:

1）单量子不可再分。量子是物理量变化的最小单元，单个量子不可分割。量子密钥分发若采用单个量子（通常为单光子）作为信息载体，则攻击者无法通过窃取单量子一部分并测量其状态的方法来获得密钥信息。

2）未知单量子态无法精确测量。根据海森堡测不准原理（现在多称为不确定性原理），量子的一对非对易物理量不能被同时测准。在量子密钥分发双方随机选择非对易物理量的其一进行编解码时，攻击者即使截取了量子信号，也无法有效测准单量子的状态。如果攻击者根据测量结果重新制备一个量子发送给接收方，将不可避免地改变单量子状态，导致解码结果与编码不一致。量子密钥分发双方可通过检测误码率来判断攻击行为及其强度，并在后处理中进行消除。

3）未知单量子无法精确复制。量子相干叠加（同时处于多种状态）的特性使得不存在通用的方法获得任意未知单量子的多个精确一致拷贝。在量子密钥分发双方随机调制单量子态时，如果攻击者试图在截获量子信号后复制多个拷贝，将不可避免地导致复制态与初始态存在偏差，进而导致解码结果与编码不一致，量子密钥分发双方同样可进行检测发现和后处理消除。所以量子密钥分发的安全性不基于计算能力，是一种理论上可以被证明无条件安全的密钥分发方案。

本项目的量子密钥生成终端采用基于诱骗态方案的 BB84 协议，使用光子作为量子态的载体，量子态编码方式采用偏振编码方式。

4.3 量子网络管理需求

1）各站点量子网关、密钥管理机可接受集控站网元管理系统、密钥管理服务系统的统一管理；

2）各站点量子网关、密钥管理机可接受集控站网元管理服务器下发的配置消息、升级数据等。

4.4 与一期实现互联互通

本期和海南量子保密通信政务示范网一期项目（大数据二期B包项目）通过各自子网的量子网元系统实现对各自量子系统设备的管理和控制，并与已建成的海南量子保密通信政务示范网一期项目（大数据二期B包项目）实现量子密钥中继及互连互通，保证本期和一期两个子网络系统能够协同运行。

4.5 业务流量需求

1）支持各业务接入点与政务云间实现每分钟更换一次量子密钥；

2）量子密钥分发平台具备密钥缓存功能，用户业务可以通过密钥缓存池继续获取密钥，不会因量子链路的中断造成业务节点之间无法进行数据加密。

8.6 架构需求

整个网络分为经典的数据传输网和量子密钥交换网络。其中：传统的数据传输网为现有的电子政务系统网络，用来传输日常办公数据；在不改变原有数据传输网络的情况下，依托量子城域网叠加形成一张量子密钥交换网络。

1）经典传输网络

各接入单位通过量子安全路由器使用量子密钥对数据进行加密，通过传统的IP网络（互联网或专线）与省数据中心进行数据加密传输。

2）量子密钥分发网

依托量子城域网叠加形成一张量子密钥交换网络，对量子网关设备产生的密钥进行网络分发，为量子安全路由器提供加解密密钥，实现数据传输的安全。

5.项目服务交付

项目交付时，应提供接入服务开通确认单

开通服务确认书

项目编号：_____

<table>
<tr><td colspan="6">项目信息</td></tr>
<tr><td>项目名称</td><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td>站点名称</td><td colspan="2"></td><td>站点地址</td><td colspan="2"></td></tr>
<tr><td>站点联系人</td><td colspan="2"></td><td>站点联系电话</td><td colspan="2"></td></tr>
<tr><td colspan="6">服务信息</td></tr>
<tr><td>项目负责人</td><td colspan="2"></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td>服务水平</td><td colspan="5"></td></tr>
<tr><td colspan="6">测试信息</td></tr>
<tr><td rowspan="2">光纤测试</td><td>集控站/汇聚站</td><td>站点</td><td colspan="2">接入距离（光纤皮长）</td><td>衰耗（dB）</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>开通结果</td><td colspan="2">☑通过　　不通过</td><td>开通日期</td><td colspan="2">年　月　日</td></tr>
<tr><td colspan="6">备注</td></tr>
<tr><td colspan="6"></td></tr>
</table>

注意事项：

1、单位/申请人确认：以上所填写的资料完全属实，且已认真阅看并愿意接受及遵守本登记表内容及受理说明；

2、本登记表传真件有效（传真：　　）

站点签字和盖章：_____　　日期：20___年_____月____日

6.服务采购清单

本期项目采购如下服务内容，用于提升海南省电子政务外网量子保密通信服务总体服务能力。采购内容清单如下：

序号	名称	规格型号	年限（年）	数量	单位
1	应用加密服务 （包含客户站全套设备租赁）	包含服务所需的软硬件	3	20	套
2	量子保密通信城域网接入服务	包含服务所需的软硬件	3	20	套