

项目服务清单如下：

序号	名称	单位	数量	要求/备注
1	加油机智慧数据采集终端—报税口采集模块	台	990	包含采集报税口模块、采集编码器模块、采集抬挂枪模块，含辅材及安装。
	加油机智慧数据采集终端—编码器采集模块			
	加油机智慧数据采集终端——抬挂枪采集模块			
2	液位仪智慧数据采集传输终端	台	264	采集液位仪数据，含辅材及安装
3	加油机智慧数据传输终端	台	264	采集加油站进销存数据传输云平台，含辅材及安装
4	加油站诚信经营综合数据防控监管系统	套	1	含首页、加油站信息管理、设备管理、运营管理、数据中心、预警管理、监控中心、系统管理、个人中心、下载管理等多项功能。
5	密码安全服务平台	台	1	具备密码服务、密码设备、密钥管理、态势感知等功能；集中提供完整的、统一的、可定制的安全服务体系，其中包括身份认证服务、访问控制服务、签名验签服务、加解密服务。
6	数字证书认证系统	台	1	基于 SM2 算法签发数字证书，提供数字证书申请、审核、更新、注销等数字证书全生命周期管理，须实现用户身份鉴别
7	综合安全网关	台	1	基于密码技术构建国密协议的数据安全传输通道，保证通信过程中数据的机密性和完整性
8	安全密码模块	台	1	通过密钥分割和协同签名技术，须实现物联网终端设备身份鉴别，提供身份认证、加解密、签名验签等功能
9	签名验签服务器	台	1	提供加解密，签名和验签等功能，须实现身份鉴别，保证数据完整性和机密性
10	安全运维服务器（国密堡垒机）	台	1	提供符合国密协议要求的安全运维管理，集成国密算法须实现双因子身份鉴别并对关键数据进行完整性校验及抗抵赖验证
11	智能密码钥匙	个	20	智能密码钥匙存储数字证书，标示用户身

				份，为本系统业务用户及运维、管理人员均配发数字证书
12	国密浏览器	套	20	用户通过国密浏览器与综合安全网关、安全运维服务器构建基于国密算法 SSL 协议的网络通道，保证通信过程中数据的机密性和完整性

项目主要技术参数及要求如下：

加油站诚信经营综合数据防控监管系统

序号	功能	功能需求
1	首页	1、可汇总展示辖区内加油站设备数量信息、销售统计信息和储油罐进出油信息。 2、可实现通过折线图、柱状图等形式分区域展示辖区内加油站销售统计情况。 3、可实现通过 GIS 地图展示区域内的加油站分布情况，可点击查看加油站基础信息及设备信息。
2	加油站信息管理	1、加油站信息查询：可实现加油站基础信息查询功能，可实现加油站信息编辑功能，可实现加油站信息页面新增和批量导入功能，可实现加油站撤站管理； 2、加油机信息查询：可实现加油机基础信息查询功能，可实现加油机信息编辑功能，可实现加油机信息页面新增和批量导入功能； 3、加油枪信息查询：可实现加油枪基础信息查询功能，可实现加油枪信息编辑功能，可实现加油枪使用状态显示功能； 4、液位仪信息查询：可实现液位仪基础信息查询功能，可实现液位仪信息编辑功能，可实现液位仪信息页面新增和批量导入功能；
3	设备管理	1、加油机数据采集设备信息查询：可实现加油机数据采集设备信息查询功能，可实现加油机数据采集设备手动新增管理功能； 2、加油机路由设备信息查询：可实现加油机路由设备信息查询

		功能，可实现加油机路由设备手动新增管理功能； 3、液位仪路由设备信息查询：可实现液位仪路由设备信息查询功能，可实现液位仪路由设备手动新增管理功能； 4、升级管理：可实现加油机数据采集设备、加油机路由设备、液位仪路由设备远程升级功能。
4	运营管理	1、一户式查询：可实现通过加油站查询，聚合显示加油站基础信息、销售统计、设备基础信息及设备在线状态显示功能； 2、操作员管理：可实现新增、查询、编辑区域操作员功能，操作员权限对应登录 H5 安装、巡检平台权限； 3、加油机主板查询：可实现查询显示加油机编号、税控微处理器编号、编码器身份信息功能，与手持加油机数据采集器（POS 机）读取数据一致； 4、加油站营业异常：可实现新增、查询、关停加油站经营异常情况功能； 5、加油机报税口连接设备告警：可实现加油机报税口连接设备离线告警查询功能； 6、加油机路由设备告警：可实现加油机路由设备离线告警查询功能； 7、液位仪路由设备告警：可实现液位仪路由设备离线告警查询功能；
5	数据中心	1、加油站报税口交易明细查询：实现加油站报税口交易明细（交易金额、交易油量、交易单价、累计金额、累计油量、交易时间等数据）查询功能，实现查询结果一键导出功能； 2、报税口交易日报：实现报税口日报查询功能，实现查询结果一键导出功能； 3、报税口交易月报：实现报税口月报查询功能，实现查询结果一键导出功能； 4、加油站编码器交易明细查询：实现加油站编码器交易明细（交易金额、交易油量、交易单价、累计金额、累计油量、交易时

		间等数据）查询功能。 5、编码器交易日报：实现编码器交易日报查询功能，实现查询结果一键导出功能； 6、编码器交易月报：实现编码器交易月报查询功能，实现查询结果一键导出功能； 7、液位仪数据查询：可实现储油罐液位明细数据查询功能，可实现查询结果一键导出功能； 8、液位仪日报：实现液位仪日报查询功能，实现查询结果一键导出功能； 9、液位仪月报：实现液位仪月报查询功能，实现查询结果一键导出功能；
6	预警管理	1、预警生成设置：可实现告警阈值设置功能，可实现告警信息启停管理功能； 2、加油机路由器告警查询：可实现加油机路由器告警记录查询功能，实现查询结果的一键导出； 3、加油机采集器告警查询：可实现加油机采集器告警记录查询功能，实现查询结果的一键导出； 4、液位仪路由器告警查询：可实现液位仪路由器告警记录查询功能，实现查询结果的一键导出。
7	监控中心	可实现数据可视化大屏显示功能。
8	系统管理	1、用户管理：可实现新增、编辑、启用、停用用户账户功能，可实现查询结果一键导出功能； 2、角色管理：可实现新增、编辑、启用、停用用户角色功能，可实现查询结果一键导出功能； 3、部门管理：可实现新增、编辑、启用、停用、删除部门功能，可实现查询结果一键导出功能； 4、岗位管理：可实现新增、编辑、启用、停用、删除岗位功能，可实现查询结果一键导出功能； 5、日志管理：可实现系统操作日志查询功能，可实现系统登录

		日志查询功能。
9	个人中心	可实现个人信息用户姓名、手机号、登录密码编辑修改功能。
10	移动端	1、可实现兼容手机浏览器访问页面； 2、可实现展示加油站基础信息、加油站流水信息、加油站订单汇总信息功能； 3、可实现采集设备安装设置功能； 4、可实现加油站巡检功能，包括实时显示加油站交易流水，加油站设备在线状态功能，加油站储油罐实时液位状态信息。
11	数据应用安全	▲系统支持与密码安全服务平台进行无缝对接，有效保证系统身份认证的合法性、关键敏感数据的机密性和完整性，密码安全服务平台应具备商用密码产品认证证书。

加油机智慧数据采集终端

序号	名称	配置需求
1	设备	机箱材质：金属外壳
		无线通信：采用无线扩频技术
		供电范围：(DC5V-DC12V)
		在线监测：通过定时发送心跳包，监测设备是否掉线。
		使用环境：▲温度及优于：-40℃到+55℃(需提供防爆证测试证明)
2	数据采集接口	支持国家税务总局税控协议约定的串口参数，可直连加油机税控口采集数据
		RS232 数据采集接口： 接口数量：至少 2 路； 接口形式：DB-9 母型插座 或 XH2.54-3P 接口。 通信速率：支持 1200-115200 bps 通信状态指示：支持通信状态指示 静电防护：满足静电防护要求；
		RS485 数据采集接口 接口数量：至少 1 路； 接口形式：RJ45；

		通信速率：支持 1200-115200 bps 通信状态指示：支持通信状态指示 静电防护：满足静电防护要求
		提枪信号采集接口（需提供设备图片） 接口数量：至少 6 路； 通信状态指示：支持通信状态指示
		编码器采集接口（需提供设备图片） 接口数量：至少 6 路； 通信状态指示：支持通信状态指示
3	数据传输接口	SMA 天线接口
		支持安全加密传输
		指示灯：PWR-LED TXD-LED RXD-LED
		无线局域组网，可应急实现无线电静默
4	主处理器	工业级
		支持掉电存储配置参数
		抗电磁干扰，需提供证明材料。
5	资质	▲供应商或原厂商所投产品具有防爆功能。其中防爆标志不得低于 IIC 标准（C>B>A）（需提供防爆合格证复印件证明，并附查询地址）
6	无线发射功率	$\leq 2\text{w}$
7	兼容加密报税口	支持兼容采集 2019 年以后生产的新型加油机的密文税控芯片数据，支持、兼容 2019 年以后生产燃油加油机防作弊系统。
8	电磁环境控制	▲本项完成电磁兼容测试，取得电磁兼容测试报告，包括静电放电抗扰度、射频电磁场辐射抗扰度、电快速瞬变脉冲群抗扰度、浪涌（冲击）抗扰度、工频磁场抗扰度、电压暂降、短时中断和电压变化的抗扰度。保证其中每一项在 A 级/类别的测试中结论是“合格”或“符合”。不得缺项或少项。（需提供 CNAS 认证标志的检验报告）。
9	数据加密	▲应具备安全密码模块功能，采用数据加密传输，支持国密加密算法。安全密码模块应具备商用密码产品认证证书。

加油机智慧数据传输终端

序号	类型	项目	配置需求
----	----	----	------

1	基础要求	协议支持	集成 MQTT/TCP 协议，能接入各通讯运营商物联网平台
2		数据解析 转发要求	支持国家税务总局税控协议解析，可将采集数据解析重新打包上传物联网平台
3		在线监测支持	心跳包技术，智能防掉线，支持在线检测，在线维持，掉线自动重拨，确保设备永远在线
4		参数配置	应支持网络远程参数配置，并且将配置好的参数保存内部的永久存储器件内（一般为 FLASH 或 EEPROM 等）。当上电时，自动按照设置好的参数进行工作
5	功能要求	异常恢复	当发生异常或者死机时，应可进行重启操作
6		云平台对接	支持与云平台对接
7		升级	支持网络远程升级；更新失败后具备恢复机制
8	硬件要求	主处理器	三级流水结构处理 支持在线 IAP 内置看门狗
9		通信接口	接口标准：支持 RS232 和 RS485 保护：15KV ESD/保护
10		供电	供电输入电压范围 220V±5% 工作湿度 20-90%RH 无冷凝
11		联网模组	频段国内全网通：为保持数据连续性、完整性、及时性，可同时支持多家通讯公司
12		资质	▲供应商或原厂商所投产品具有防爆功能。其中防爆标志不得低于 IIC 标准（C>B>A）（需提供防爆合格证复印件证明，并附查询地址）
13		电磁环境控制	▲本项完成电磁兼容测试，取得电磁兼容测试报告，包括静电放电抗扰度、射频电磁场辐射抗扰度、电快速瞬变脉冲群抗扰度、浪涌（冲击）抗扰度、工频磁场抗扰度、电压暂降、短时中断和电压变化的抗扰度。保证其中每一项在 A 级/类别 的测试中结论是“合格”或“符合”。不得缺项或少项。（需提供 CNAS 认证标志的检验报告）。
14		数据加密	▲应具备安全密码模块功能，采用数据加密传输，支持国密加密算法。安全密码模块应具备商用密码产品认证证书。
15	性能要求	操作性	上电启动到工作状态，时延不超过 30s
16		发射功率	≤3W
17		工作环境	湿度：20%~90%无凝露

			大气压力：86~106KPa
18		可靠性	内置看门狗及多级链路检测机制，具备故障自动检测、自动恢复能力，保证设备稳定可靠运行 多重设备自检机制，确保链路畅通和告警 各接口 ESD 防护，防止静电冲击

液位仪智慧数据采集传输终端

序号	类型	项目	配置需求
1	功能要求	协议支持	集成 MQTT/TCP 协议，能接入各通讯运营商物联网平台
2		数据采集转发要求	支持主流液位仪协议解析，可将采集的液位仪数据解析重新打包上传物联网平台
3		在线监测支持	心跳包技术，智能防掉线，支持在线检测，在线维持，掉线自动重拨，确保设备永远在线
4		参数配置	应支持网络远程参数配置，并且将配置好的参数保存内部的永久存储器件内(一般为 FLASH 或 EPROM 等)。当上电时，自动按照设置好的参数进行工作
5		异常恢复	当发生异常或者死机时，应可进行重启操作
6		平台对接	支持与平台对接
7		升级	支持网络远程升级；更新失败后具备恢复机制
8	硬件要求	主处理器	三级流水结构处理 支持在线 IAP 内置看门狗
9		通信接口	采集接口标准：支持 RS232 和 RS485 采集数据输出接口：采集的液位仪数据支持 RS232 接口输出； 保护：15KV ESD/保护
10		供电	供电输入电压范围 220V±5% 工作湿度 20-90%RH 无冷凝
11		联网模组	频段国内全网通：为保持数据连续性、完整性、及时性，可同时支持多家通讯公司
12		资质	▲供应商或原厂商所投产品具有防爆功能。其中防爆标志不得低于 IIC 标准 (C>B>A) (需提供防爆合格证复印件证明，

			并附查询地址)
13		电磁环境控制	▲本项完成电磁兼容测试,取得电磁兼容测试报告,包括静电放电抗扰度、射频电磁场辐射抗扰度、电快速瞬变脉冲群抗扰度、浪涌(冲击)抗扰度、工频磁场抗扰度、电压暂降、短时中断和电压变化的抗扰度。保证其中每一项在A级/类别的测试中结论是“合格”或“符合”。不得缺项或少项。(需提供CNAS认证标志的检验报告)。
14		数据加密	▲应具备安全密码模块功能,采用数据加密传输,支持国密加密算法。安全密码模块应具备商用密码产品认证证书。
15	性能要求	操作性	上电启动到工作状态,时延不超过 30s
16		发射功率	≤3W
17		工作环境	湿度: 20%~90%无凝露 大气压力: 86~106KPa
18		可靠性	内置看门狗及多级链路检测机制,具备故障自动检测、自动恢复能力,保证设备稳定可靠运行 多重设备自检机制,确保链路畅通和告警 各接口 ESD 防护,防止静电冲击

密码安全服务平台

1	密码安全服务平台	具备密码服务、密码设备、密钥管理、态势感知等功能;集中提供完整的、统一的、可定制的安全服务体系,其中包括身份认证服务、访问控制服务、签名验签服务、加解密服务。 1、算法支持:支持国密 SM1、SM2、SM3、SM4、SM9 算法; ▲2、密码服务平台证书综合管理应包含 CA 配置、数量授权、证书管理、数量统计、存储介质管理等功能;(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) ▲3、密码服务平台密码资源管理应包含密码设备管理、宿主机管理、虚拟资源管理、镜像管理、密码服务等功能;(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制
---	----------	---

		造商公章) ▲4、实现对密码设备资源的统一管理,包括签名服务器、密码机、云密码机、网关、电子签章服务器、时间戳服务器、手机盾服务器的增删改查;(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) ▲5、支持数字证书服务、密钥管理服务、签名验签服务、时间戳服务、电子签章服务、数据加解密服务、协同签名运算服务、数据链路加解密服务;(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) ▲6、密码服务平台身份认证功能应包含资源管理、角色管理授权管理功能;(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) ▲7、密码服务平台应用管理功能应包含应用接入管理和应用访问授权功能;(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) 8、支持第三方 CA 接入,实现数字证书全生命周期管理,包括个人数字证书、服务器证书的申请、更新、下载、注销等; 9、支持用户统一管理,能够在平台系统中对电子签章系统用户、移动互联网密码服务系统用户进行统一管理,包括用户的注册、修改、删除、查看; 10、支持对平台和密码设备资源的网络拓扑图自动生成功能; 11、对密码设备监控信息应包括:CPU 使用率、内存使用率、硬盘等; 12、支持日志审计、监控日志、归档日志等功能; ▲13、产品须具有国家密码管理局商用密码产品认证证书;符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求;
--	--	--

数字证书认证系统

1	数字证书认证系统	基于 SM2 算法签发数字证书，提供数字证书申请、审核、更新、注销等数字证书全生命周期管理，实现用户身份鉴别。 1、支持国际通用算法和国产 SM 系列算法；提供数字证书整个生命周期的过程管理功能。包括用户注册管理、证书/证书注销列表的生成与签发、证书/证书注销列表的存储与发布、证书状态的查询、密钥的生成与管理、过程安全审计等 2、支持证书新办、更新、吊销、挂起、解挂和证书黑名单等证书全生命周期管理； 3、支持多种证书类型模版，个人证书、机构证书、设备证书等； 4、支持证书模板自定义配置，支持国家标准规定的私有扩展及自定义扩展；证书符合国际标准 X509 V3 标准； 5、支持产生证书黑名单，包括：定时自动产生、手动实时产生，规范符合 X509 V2 标准； 6、支持手工录入、批量导入、三方应用授权集成等方式注册证书，并为用户签发数字证书； 7、支持证书签发模块、证书注册模块、系统配置模块分权管理模式； ▲8、模版管理包括证书模板管理、证书撤销列表模板管理、在线证书状态协议模板等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲9、密钥管理包含密钥生成、密钥存储、密钥传送与分发、密钥导入导出、密钥使用、密钥备份、密钥恢复、密钥归档、密钥销毁、密钥更新等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲10、证书管理包含证书注册、证书生成、证书撤销、证书更新、证书变更等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） 11、可提供证书黑名单、Ldap、OCSP 等方式数字证书身份认证服务； 12、提供基于证书的签名/验证、加密/解密等功能组件； 13、密钥独立管理体系，支持密钥自动监控、产生、分发的智能监管系统； 14、支持管理权限划分，各系统按权操作，多系统分责管理，管理员身份可鉴别； 15、支持系统管理员操作日志审查，支持操作员签名审查； 16、支持多厂家普通、蓝牙、指纹等智能 UsbKey 钥匙的无缝接入； ▲17、须具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0034 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》 18、标准机架设备，多核处理器，≥8G 内存，≥2T 硬盘，≥2 个千兆网口； ▲19、硬件平台须具有中国国家强制性产品认证证书和中国节能认证产品认证证书； 20、证书最大数量：100000；
---	----------	---

综合安全网关

1	综合安全网关	基于密码技术构建国密协议的数据安全传输通道，保证通信过程中数据的机密性和完整性。 1、支持国际通用算法和国产 SM 系列算法；支持 PKI 体系；支持身份认证、访问控制、单点登录、SSL 隧道；IPSec 支持主模式和快速模式；支持 ESP 密钥交换协议；支持 NAT 穿越和双向 NAT 穿越。 ▲2、算法实现对 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法和 RSA/SHA/AES/DES/3DES 等国际通用算法的支持，实现对后量子算法的支持。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲3、身份鉴别实现基于用户名口令、数字证书、短信码、动态码等多因子认证方式；实现基于零信任架构的身份认证和安全接入功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲4、协议支持实现基于 RSA、SM2、SM9、后量子等国际和国密算法的 SSL 协议和 IPSec 协议的密钥协商、密钥交换、链路通信加密、SSL 卸载功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） 5、高强度的传输链路加密，符合 GM/T 0024 《SSL VPN 技术规范》； 6、基于角色授权，可将不同用户分配给不同角色，实现对不同用户访问权限细粒度的控制。 ▲7、访问控制支持基于角色用户机构的 RBAC 访问控制模型、基于用户属性客户端属性的 ABAC 访问控制模型、可修改超级管理员登录名基于 OB4LAC 的授权访问控制模型的功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲8、支持基于 NTLM、FORM、BASIC、CAS、OAuth2.0、OpenID 等方式和协议的单点登录功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲9、支持常用的 Radius/LDAP/AD 第三方身份认证；支持 PKI 体系的第三方证书，支持 OCSP、CRL、LDAP 有效性校验。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） 10、遵循 GM/T 0022 《IPSec VPN 技术规范》，支持与标准 IPSec VPN 产品的互联互通。 11、隧道支持主模式和快速模式、支持完全向前保密 PFS、支持 DPD 协议探测隧道状态、支持隧道断线自动重建。 12、密钥交换协议支持 ESP 协议、支持隧道模式、支持 NAT 穿越和双向 NAT 穿越。 ▲13、终端支持基于 IP 地址、MAC 地址等终端硬件信息的用户绑定功能；支持终端用户登录后的网络隔离功能，支持基于组策略、用户策略、网络白名单策略的网络隔离功能。（提供由 CNAS 或 CMA 认证的第三方检测机构
---	--------	--

		出具的测试报告的复印件并加盖制造商公章) ▲14、终端支持实现对 Windows7/10/11 主流操作系统，麒麟、统信、深度等国产操作系统，Android、iOS、鸿蒙等移动终端的支持。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) ▲15、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 16、支持多线路负载均衡、支持线路切换、线路流量负载和双机热备的功能； ▲17、须具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0023《IPSec VPN 网关产品规范、GM/T 0025《SSL VPN 网关产品规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。 ▲18、须具有网络安全专用产品安全检测证书（增强级）； 19、标准机架设备，多核处理器，≥16G 内存，≥2T 机械硬盘，≥2 个千兆网口； ▲20、硬件平台须具有中国国家强制性产品认证证书和中国节能认证产品认证证书； ▲22、产品须具备工信部颁发的电信设备进网许可证； 21、SSL VPN 性能：并发在线用户数≥10000，并发会话数≥70000，每秒新建用户数≥600，加解密速率≥2500Mbps，转发延迟<0.1ms； IPSec VPN 性能：每秒新建隧道数≥3500，并发隧道数≥12000，加解密速率≥2500Mbps，转发延迟<0.1ms
--	--	---

安全密码模块

1	安全密码模块	包含服务端和客户端，通过密钥分割和协同签名技术，实现物联网终端设备身份鉴别，提供身份认证、加解密、签名验签等功能； 1、算法支持：支持国密 SM2、SM3、SM4 算法； 2、密钥管理：密钥客户端片段生成、安全存储及销毁； 3、证书管理：集成身份认证系统（CA），支持证书在线申请、更新、注销等数字证书全生命周期管理，支持第三方 CA 认证机构； 4、扫码签名：支持扫描二维码实现数字签名； 5、推送签名：支持业务系统通过密码服务系统服务端推送签名请求到客户端，实现数字签名； 6、支持获取二维码、推送签名消息、获取签名值、验证签名等功能； 7、支持摘要运算、非对称加解密和对称加解密运算； 8、终端私钥拆分成两部分密钥因子，一部分在客户端，一部分在服务端，保证终端密钥的安全。 9、协同签名：支持与客户端配合，协同实现数字签名； 10、系统及服务监控：能够对系统服务进行监控，授权查看设备运行状态。 11、用户管理：对终端账户进行管理、统计、查询。维护账户状态，存储账户对应的设备公钥信息等。 12、管理员管理：对系统操作的管理员进行添加、删除、修改以及授权，只有授权管理员才能登陆系统进行操作。
---	--------	--

		13、安全审计：能够对系统所有的操作和接口调用进行详细的记录，非授权人员不可篡改记录。 ▲14、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 15、提供 SDK 开发接口，支持物联网终端集成，支持移动端 APP、微信公众号/小程序； 16、支持双主机热备部署； ▲17、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求； ▲18、须具有网络安全专用产品安全检测证书； 19、标准机架设备，多核处理器，≥8G 内存，≥2T 机械硬盘，≥2 个千兆网口； ▲20、硬件平台须具有中国国家强制性产品认证证书和中国节能认证产品认证证书； 21、服务端协同签名运算≥5000 次/秒；验签≥8000 次/秒；最大用户数≥5000；
--	--	---

签名验签服务器

1	签名验签服务器	提供加解密，签名和验签等功能，实现身份鉴别，保证数据完整性和机密性。 1、支持身份认证、数据签名、签名验证、数据加密/解密等功能。 ▲2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256 /SHA384/SHA512/AES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲3、支持 PKCS#1/PKCS#7(attached 和 detached)/XML 的签名验签；支持二维码、条形码的签名处理；支持基于 SM2、RSA 等算法的数字信封加密、解密功能；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲4、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲5、支持服务信息功能，实现查看服务状态，系统状态，系统自检，更改服务端口，是否加密通信，服务的启动停止；支持服务测试功能，实现对签名验签，数字信封等服务功能的测试；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章） ▲6、支持应用管理功能，可管理调用签名验签服务的应用系统，包括应用的添加、删除、修改、关联证书链等功能；支持服务白名单功能，实现白名单的添加查看删除，通过连接白名单的支持，实现签名验签服务器对应用服务器的授权认证；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的
---	---------	---

		测试报告的复印件并加盖制造商公章) ▲7、支持 RSA 密钥管理、SM2 密钥管理、对称密钥管理、受信赖根证书、证书撤销列表、业务证书等管理功能；(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖制造商公章) ▲8、证书管理和验证、数字签名和验证等核心功能，要求符合《信息安全技术签名验签服务器技术规范 GB/T 38629 -2020》；(提供第三方检测报告复印件并加盖制造商公章) 9、支持标准 X509V3 数字证书格式，支持签名证书和加密证书的双证书认证体系，提供 CRL/OCSP/LDAP 等多种方式的证书有效性验证； 10、支持最大 500M 大文件、大数据的数字签名和数字信封功能； 11、可同时配置多条证书链，验证不同 CA 的用户证书；可同时支持 20 个不同的 CA； 12、提供 CRL 的自动下载功能和证书有效性验证功能； 13、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息； 14、基于 WEB 形式的图形管理界面，提供完善的配置管理、证书管理、服务管理等功能； 15、具有日志审计功能，支持第三方 SYSLOG 日志服务器； 16、支持浏览器、应用服务器、移动端的调用； ▲17、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； ▲18、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 19、提供 JAVA、C++等 API 开发接口和示例代码； ▲20、须具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0029《签名验签服务器技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求； ▲21、须具有网络安全专用产品安全检测证书； 23、标准机架设备，多核处理器，≥8G 内存，≥2T 机械硬盘，≥2 个千兆网口； ▲24、硬件平台须具有中国国家强制性产品认证证书和中国节能认证产品认证证书； 25、SM2 密钥生成≥103200 对/秒，SM2 签名≥ 202500 次/秒，SM2 验签≥ 69558 次/秒，SM2 加密≥ 41900 次/秒，SM2 解密≥50100 次/秒，SM1 加解密≥ 1850Mbps，SM4 加解密≥ 1890Mbps，SM3 摘要≥ 3800Mbps；
--	--	--

安全运维服务器（国密堡垒机）

1	安全运维服务器（国密堡垒机）	提供符合国密协议要求的安全运维管理，集成国密算法实现双因子身份鉴别并对关键数据进行完整性校验及抗抵赖验证。 1、通过集成数字证书强身份鉴别、国密协议安全隧道以及堡垒机模块功能为一体，满足“设备与计算安全”国密身份鉴别、访问控制、链路加密及敏感数据防护等安全要求。 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、强身份认证：支持基于国密数字证书的身份认证和登录功能，支持第三方 CA。 4、通信机密性：运维人员客户端与国密堡垒机之间采用国密算法加密通信链路进行数据的传输，保证通信数据的完整性和机密性。 5、存储机密性：对关键敏感数据采用国密算法进行加密存储，保证关键敏感信息的机密性。 6、单点登录：实现与用户授权管理的无缝连接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。 7、集中账号管理：集中账号管理包含对所有服务器、网络设备账号的集中管理。账号和资源的集中管理是集中授权、认证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且还降低了管理大量用户账号的难度和工作量。 8、资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。 9、访问控制：能够提供细粒度的访问控制，最大限度保护用户资源的安全；对访问控制信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改，保证系统的安全性。 10、协议管理：支持字符型（SSH、Telnet）、图形（RDP、VNC）、数据库（Oracle、Sybase、MySQL、SQLServer、DB2 等）、文件传输（FTP、SFTP）、http、https 等多种协议类型； 11、支持基于管理代理的机制，安装在被管设备上，实现了运维服务器和被管设备之间的有效身份鉴别，并建立安全的加密信息传输通道。 12、操作审计：对访日志信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改。 13、标准机架设备，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲14、硬件平台须具有中国国家强制性产品认证证书和中国节能认证产品认证证书； ▲15、须具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求； 16、字符型协议并发会话数≥500，图形型协议并发会话数≥300，IP 管理资源授权≥500，IP 管理资源最大授权≥1000，加解密速率≥600Mbps，转发延迟<0.1ms
---	----------------	--

智能密码钥匙

1	智能密码 钥匙	智能密码钥匙存储数字证书，标示用户身份，为本系统业务用户及运维、管理人员均配发数字证书。 1、支持国产系列算法；实现密码运算与数据安全存储，具备访问控制、密钥管理及数据存储功能 2、硬件内部生成公私钥对，数字签名、私钥永不出 KEY； 3、支持数据的安全存储功能； 4、支持 Windows X86 系列操作系统（XP/Win7/Win8/Win8.1/Win10 等）、Linux(Ubuntu/Red Hat 等）等。 5、支持个性化接口定制开发； 6、无驱无软，支持驱动免安装，支持应用自动加载； 7、采用标准 USB 接口，即插即用，可支持 USB2.0 规范高速或全速模式； ▲8、产品符合国家密码管理局 GM/T 0027《智能密码钥匙技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求；具有国家密码管理局商用密码产品认证证书； 9、功率：小于 250mW 10、数据存储年限：≥10 年 ▲11、产品可在低温及高温环境下处于正常工作状态；（提供第三方测试报告复印件并加盖制造商公章） 12、存储空间：128K 13、SM2 签名≥90 次/秒；SM2 验签≥40 次/秒；SM1 加解密≥1.8Mbps；SM4 加解密≥1Mbps；SM3 摘要≥2.9Mbps； 14、擦写次数（次）≥100000 15、数据存储年限≥10（年）
---	------------	---

国密浏览器

1	国密浏览 器	用户通过国密浏览器与综合安全网关、安全运维服务器构建基于国密算法 SSL 协议的网络通道，保证通信过程中数据的机密性和完整性。 1、支持页面标签栏功能，可以提供多标签呈现形式和标签切换功能； 2、支持证书管理，可以提供 HTTPS/SSL 传输协议中根证书的与集成和证书的导入导出功能； 3、支持网络连接设置，可以提供网络代理和代理服务器配置管理功能； 4、支持基于 SM2 算法的数字证书、数字证书撤销列表（CRL）； 5、同时支持 SSL 单项及双向链接； 6、支持基于 RSA 算法的数字证书、数字证书撤销列表（CRL）； 7、支持地址栏功能，提供输入地址、网页搜索快速访问对应网址的功能； ▲8、具有国家密码管理局商用密码产品认证证书；
---	-----------	--