# 采购需求

## 一、项目概况

根据《关于规范和加强我市重要网络和信息系统密码应用与安全性评估工作的通知》提出，非涉密的关键信息基础设施、网络安全等级保护第三级以上网络(含信息系统)、政务信息系统，以及法律、行政法规和国家有关规定要求使用商用密码进行保护的其他网络和信息系统，应当落实密码应用相关要求，包括密码应用方案编制与评估、密码保障系统建设、密码应用测评、密码应用安全性评估等工作。

2023 年,市局印发《关于进一步加强公安传输网络建设管理工作的通知》(沪公科传发〔2023〕100 号)，要求增强传输网络健壮性和可靠性,完成普陀分局融合承载网汇聚层设备冗余建设，解决融合承载网单点故障隐患。

根据分局应用系统密码使用需求，新增密码软硬件产品，统筹开展分局密码应用体系建设。此外，同步完成邮件等基础信息系统的改造工作及加强分局基础传输网络的建设管理工作。

## 二、建设目标

完成普陀分局公安信息网、公安移动信息网和视频传输网密码应用体系建设，为各应用系统提供密码资源服务，满足密码应用安全性评估要求。

完成基础信息系统改造及配套软硬件建设，进一步提升基础信息系统安全防护水平。

采购部署融合承载网汇聚层设备，解决普陀分局融合承载网单点故障隐患。

## 三、建设依据

1、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）；

2、《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）；

3、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；

4、《信息系统密码应用基本要求》（GM/T 0054-2018）；

5、《电子文件密码应用技术规范》（GM/T 0055-2018）；

6、《电子文件密码应用指南》（GM/T 0071-2018）。

## 四、建设内容

4、1 本项目主要建设内容包括三部分：

4．1．1 基础信息系统改造

（1）采购 1 套邮件系统；

（2）采购一套时钟同步系统替换视频传输网中现有 GPS 时钟同步系统。同时，新增一套时钟同步系统，部署在公安信息网中；

4．1．2 融合承载网汇聚层设备采购

采购部署一套融合承载网汇聚层设备，解决普陀分局融合承载网单点故障隐患；

4．1．3 普陀分局密码应用体系建设

按照《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021），在公安信息网、视频传输网、移动信息网中开展密码应用体系建设，部署安全认证网关、签名验签服务器、安全加密存储备份网关密码模块、密钥管理系统、SSL VPN 等设备，为应用业务应用提供统一的安全密码服务。

4、2 设备清单

| 序号 | 项目 | 单位 | 数量 |
|---|---|---|---|
| **(1)公安信息网** | | | |
| 1 | 密码服务平台 | 套 | 1 |
| 2 | 安全认证网关服务组件（授权） | 套 | 3 |
| 3 | 签名验签服务组件（授权） | 套 | 6 |
| 4 | 密钥管理服务组件（授权） | 套 | 5 |
| 5 | 安全加密存储备份网关组件（授权） | 套 | 4 |
| 6 | 云服务器密码机 | 台 | 1 |
| 7 | 完整性保护 | 套 | 1 |
| **(2)公安移动信息网** | | | |
| 1 | 安全认证网关 | 台 | 1 |
| 2 | 服务器密码机 | 台 | 1 |
| 3 | 签名验签服务器 | 台 | 1 |
| 4 | 完整性保护工具 | 套 | 1 |
| 5 | SSL VPN | 台 | 1 |
| **(3)视频传输网** | | | |
| 1 | 安全认证网关 | 台 | 2 |
| 2 | 服务器密码机 | 台 | 2 |
| 3 | 安全加密存储备份网关密码模块 | 套 | 1 |
| 4 | 签名验签服务器 | 台 | 1 |
| 5 | 密钥管理系统 | 套 | 1 |
| 6 | 完整性保护工具 | 套 | 1 |
| **(4)基础信息系统改造** | | | |
| 1 | 邮件系统软件（含 3500 个客户端授权） | 套 | 1 |
| 2 | 时钟同步系统 | 台 | 2 |
| 3 | HBA 卡 | 块 | 2 |
| 4 | 操作系统 | 套 | 16 |
| 5 | 中间件 | 套 | 4 |
| 6 | 数据库 | 套 | 5 |
| **(5) 融合承载网** | | | |
| 1 | 电子架 | 套 | 1 |

| | | | |
|---|---|---|---|
| 2 | 光子架 | 套 | 1 |
| 3 | 光监控板卡 | 块 | 1 |
| 4 | 电源组件 | 套 | 2 |

4、3 技术参数要求

4．3．1 公安信息网

**（1）密码服务平台**

| 指标项 | 技术要求 | |
|---|---|---|
| 资质 | 密码产品型号证书 | 具有国家密码管理局颁发的商用密码产品认证 |
| 主要功能 | 支持 SM2、SM3、SM4 算法，具有密码运算服务、密钥管理等功能 | |
| | 支持密码密钥资源隔离 | |
| | 支持标准 API 接口为业务应用加密解密、签名/验签、杂凑运算、消息鉴别码的产生和验证等通用密码服务 | |
| | 支持 AK/SK 机制验证密码服务请求发送者的身份 | |
| | 支持配置国际或国密 SSL 方式调用密码服务 | |
| | 支持微服务架构 | |
| | 支持接入多厂商的异构云密码机设备及管理。支持管理异构云密码机认证凭证、查看认证状态等操作 | |
| | 支持虚拟密码机开通管理功能 | |
| | ▲支持通过在密码服务关联中管理节点组和服务节点组的方式，可对密码资源进行动态调整。（提供第三方出具的检测证明或官网截图或产品说明书或产品截图） | |
| | 支持按场景创建不同模式的密码服务，需支持共享服务、专享服务、平台公共服务三种服务类型 | |
| | 支持租户管理的功能 | |
| | 支持租户管理员管理，用于租户级的管理操作，并支持管理租户子管理员 | |
| | ▲支持产生平台使用情况的可视化大屏。（提供第三方出具的检测证明或官网截图或产品说明书或产品截图） | |
| | ▲支持按场景创建不同模式的密码服务，至少支持共享服务、专享服务、平台公共服务三种服务类型。（提供第三方出具的检测证明或官网截图或产品说明书或产品截图） | |
| | 支持通过虚拟化技术结合硬件密码机资源，为业务应用提供多种虚拟密码服务 | |

| | |
|---|---|
| | 支持对密码资源设备的监控，包括云服务器密码机、服务器密码机、金融密码机、密码产品设备，至少支持设备可用性、CPU、内存、磁盘的监控 |
| 性能 | 最大可支持租户数：≥1000 个<br>最大可接入应用数量：≥5000 个<br>最大密码服务节点数量：≥2000 个<br>服务平均响应时间≤100ms<br>安全认证服务（指标）：<br>1）新建连接数（单向）：≥8000 次/秒<br>2）新建连接数（双向）：≥3500 次/秒<br>3）每秒交易数（TPS）：≥20000 次/秒<br>签名验签服务（指标）：<br>1）SM2 签名性能：≥2500 次/秒<br>2）SM2 验签性能：≥2000 次/秒<br>数据加密服务（指标）：<br>1）SM4 对称加解密（8K）：≥8000 次/秒或 500Mb/秒<br>2）HMAC 计算（SM3）：≥8500 次/秒<br>3）主密钥生成（SM4）：≥300 个/秒 |

**（2）安全认证网关服务（授权）**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持 SM1、SM2、SM3、SM4 算法 |
| | 支持密钥协商、身份认证、SSL 隧道加密等功能 |
| | 支持基于数字证书实现用户访问业务系统时的安全身份认证 |
| | 支持双向身份验证功能，支持动态黑名单 |
| | 支持多种业务应用 |
| | 支持 B/S 应用 |

**（3）签名验签服务（授权）**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持国产密码算法 SM2、SM3、SM4 |

| | |
|---|---|
| | 通过数字签名技术对电子门禁系统进出记录、视频监控音像记录系统、重要结构化或非结构化数据进行完整性保护 |
| | 支持基于数字证书的身份认证，提供数据签名与签名验证功能、数字信封功能，实现数据的完整性和行为的不可否认性保护 |
| | 支持数据签名与签名验证功能，支持 pkcs1/Pkcs7 attach/Pkcs7 detach/xml Sign 等多种格式的数字签名和数字签名验证功能 |
| | 支持文件数据签名与签名验证功能 |

**（4）密钥管理系统（授权）**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持 SM2、SM3、SM4 算法，具有密钥生成、分发、存储、管理等功能；提供密钥生命周期管理，提供创建密钥，禁用密钥，删除密钥，导入密钥（密钥来源为外部导入），查看密钥轮转历史，搜索指定密钥等功能 |
| | 支持服务设备动态扩展，满足密码服务能力使用要求 |
| | 支持服务设备动态扩展，满足密码服务能力使用要求 |

**（5）安全加密存储备份网关（授权）**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持 SM2、SM3、SM4 算法具有文件加密传输、密钥管理等功能 |
| | 支持为多个应用提供加密服务，且应用拥有独立的文件视图 |
| | 支持同时访问文件明文和密文，支持密文的导入导出 |
| | 支持多种存储设备，包括 NFS 存储、SAN 存储、GlusterFS 等分布式存储 |
| | 单节点支持配置多个不同的存储设备，支持为不同应用分配独立的存储设备 |
| | 支持使用接口 API 访问 NFS 和 GlusterFS 存储 |
| | 支持一文一密钥加密。 |
| | 支持为非结构化文件数据（文本文件/办公文件/音视频文件/图形图像文件）、半结构化数据（XML 文件）、结构化文件数据（数据库）提供存储加密服务 |

**（6）云服务密码机**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持 SM2、SM3、SM4 等国密算法 |

| | |
|---|---|
| | 支持密钥生命周期管理，包括对称密钥管理，非对称密钥管理；设备的密钥管理和密码运算功能均由设备内的密码卡完成 |
| | 支持虚拟密码机用户独立进行密钥管理；支持虚拟密码机及密码机集群之间密钥同步 |
| | 支持符合 GM/T 0018 密码设备应用接口和 GM/T 0019 通用密码服务接口 |
| | 支持虚拟密码机用户独立进行密钥管理 |
| | 支持虚拟密码机集群的密钥的自动同步功能 |
| | 数据加密和解密：支持 SM1、SM4、AES、3DES 算法的 ECB/CBC/CTR/GCM 等模式的数据加密和解密运算 |
| | 支持对虚拟密码机密钥的备份/恢复，利用门限算法将备份密钥的分量存入硬件介质，实现备份/恢复的高安全性 |
| 性能要求 | 单台设备可虚拟≥16 个虚拟密码机 |
| | SM4 加解密≥600Mbps |
| | SM2 密钥对生成≥13000 对/秒 |
| | SM2 签名≥16000 次/秒；SM2 验证≥15000 次/秒 |
| | SM3≥700Mbps |
| 资质 | 提供国家密码管理局颁发的产品证书 |

**（7）完整性保护工具**

基于签名验证服务开发的文件签名和验证的软件，可以对服务器重要文件、关键执行程序、第三方软件的控制文件以及日志文件进行完整性保护。该工具需无缝对接签名验签服务器及签名验签服务（授权）。

4．3．2 公安移动信息网

**（1）安全认证网关**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持 SM1、SM2、SM3、SM4 算法 |
| | 支持密钥协商、身份认证、SSL 隧道加密等功能 |
| | 支持基于数字证书实现用户访问业务系统时的安全身份认证 |
| | 支持双向身份验证功能，支持动态黑名单 |
| | ▲安全认证网关需支持包括随机数自检、SM1/2/3/4/9 算法自检、密钥完整性自检、 |

| | |
|---|---|
| | 配对一致性自检、程序完整性检测、配对数据完整性检测、身份鉴别介质接口检查。（提供第三方出具的检测证明或官网截图或产品说明书或产品截图） |
| | 支持 B/S 应用 |
| 性能 | 1、SM2 加密吞吐率≥4Gbps<br>2、SM2 每秒新建连接：单向≥ 3K<br>3、并发连接数 ≥5W<br>4、SM2 HTTP TPS≥8W |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（2）服务器密码机**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 通过标准 API 接口为安全防护措施和业务应用提供加密/解密、签名/验签、密钥生成与管理、消息鉴别码的产生和验证、数字信封等密码服务，提供基础密码计算能力 |
| | 支持国产密码算法(SM1、SM2、SM3、SM4) |
| 性能 | 1、SM4 加/解密速率≥12Mbps/12Mbps<br>2、SM2 密钥对生成速率≥2800 对/秒<br>3、加/解密速率≥4.5Mbps/4.5Mbps<br>4、SM3 运算速率≥250Mbps |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（3）签名验签服务器**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持国产密码算法 SM2、SM3、SM4 |
| | 通过数字签名技术对电子门禁系统进出记录、视频监控音像记录系统、重要结构化或非结构化数据进行完整性保护 |
| | 支持基于数字证书的身份认证，提供数据签名与签名验证功能、数字信封功能，实现数据的完整性和行为的不可否认性保护 |

| | |
|---|---|
| 性能 | SM2 签名≥2400 次/秒<br>SM2 验签≥1500 次/秒 |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（4）完整性保护工具**

基于签名验证服务开发的文件签名和验证的软件，可以对服务器重要文件、关键执行程序、第三方软件的控制文件以及日志文件进行完整性保护。该工具需无缝对接签名验签服务器及签名验签服务（授权）。

**（5）SSL VPN**

| 指标项 | 技术要求 |
|---|---|
| 主要功能 | 支持 SM1、SM2、SM3、SM4 算法 |
| | 需支持 SSL 加速、HTTP 压缩、Web 高速缓存功能、HTTP 请求和响应改写、HTTP 反向代理转发和 HTTP 重定向 |
| | 需支持证书、用户名口令认证，实现网关和客户端的双向强身份认证，最大限度地保证接入用户的合法性 |
| | 支持 SSL VPN，为应用系统提供端到网的通信安全防护支撑 |
| | 支持多种业务应用 |
| | 支持 B/S 应用 |
| 性能 | 1、SSL 加密吞吐率≥500Mbps<br>2、SSL 并发连接数≥10W<br>3、SSL 每秒新建连接数≥3000/秒 |
| 资质 | 提供国家密码管理局颁发的产品证书，相关的 SSL VPN 需符合：<br>1、GM/T 0023《IPSec VPN 网关产品规范》<br>2、GM/T 0025《SSLVPN 网关产品规范》<br>3、GM/T 0028《密码模块安全技术要求》第二级要求 |
| 其他 | 3 年质保 |

4．3．3 视频传输网

**（1）安全认证网关**

| 指标项 | 技术要求 |
| --- | --- |
| 主要功能 | 支持 SM1、SM2、SM3、SM4 算法 |
| | 支持密钥协商、身份认证、SSL 隧道加密等功能 |
| | 支持基于数字证书实现用户访问业务系统时的安全身份认证 |
| | 支持双向身份验证功能，支持动态黑名单 |
| | ▲安全认证网关需支持包括随机数自检、SM1/2/3/4/9 算法自检、密钥完整性自检、配对一致性自检、程序完整性检测、配对数据完整性检测、身份鉴别介质接口检查。（提供第三方出具的检测证明或官网截图或产品说明书或产品截图） |
| | 支持 B/S 应用 |
| 性能 | 1、SM2 加密吞吐率≥4Gbps<br>2、SM2 每秒新建连接：单向≥ 3K<br>3、并发连接数 ≥5W<br>4、SM2 HTTP TPS≥8W |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（2）服务器密码机**

| 指标项 | 技术要求 |
| --- | --- |
| 主要功能 | 通过标准 API 接口为安全防护措施和业务应用提供加密/解密、签名/验签、密钥生成与管理、消息鉴别码的产生和验证、数字信封等密码服务，提供基础密码计算能力 |
| | 支持国产密码算法(SM1、SM2、SM3、SM4) |
| 性能 | 1、SM4 加/解密速率≥12Mbps/12Mbps<br>2、SM2 密钥对生成速率≥2800 对/秒<br>3、加/解密速率≥4.5Mbps/4.5Mbps<br>4、SM3 运算速率≥250Mbps |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（3）安全加密存储备份网关密码模块**

| 指标项 | 技术要求 |
| --- | --- |
| 主要功能 | 支持 SM2、SM3、SM4 算法具有文件加密传输、密钥管理等功能 |
| | 支持为多个应用提供加密服务，且应用拥有独立的文件视图 |
| | 支持同时访问文件明文和密文，支持密文的导入导出 |
| | 支持多种存储设备，包括 NFS 存储、SAN 存储、GlusterFS 等分布式存储 |
| | 单节点支持配置多个不同的存储设备，支持为不同应用分配独立的存储设备 |
| | 支持使用接口 API 访问 NFS 和 GlusterFS 存储 |
| | 支持一文一密钥加密 |
| | 支持为非结构化文件数据（文本文件/办公文件/音视频文件/图形图像文件）、半结构化数据（XML 文件）、结构化文件数据（数据库）提供存储加密服务 |
| 性能 | SM4 加/解密速率≥1.6Gbps/1.6Gbps，SM2 密钥对生成速率≥10000 对/秒，加/解密速率≥40Mbps/5Mbps，SM3 运算速率≥300Mbps，网关上传文件速率≥25Mbps |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（4）签名验签服务器**

| 指标项 | 技术要求 |
| --- | --- |
| 主要功能 | 支持国产密码算法 SM2、SM3、SM4 |
| | 通过数字签名技术对电子门禁系统进出记录、视频监控音像记录系统、重要结构化或非结构化数据进行完整性保护 |
| | 支持基于数字证书的身份认证，提供数据签名与签名验证功能、数字信封功能，实现数据的完整性和行为的不可否认性保护 |
| 性能 | SM2 签名≥2400 次/秒<br>SM2 验签≥1500 次/秒 |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 3 年质保 |

**（5）密钥管理系统**

| 指标项 | 技术要求 |
| --- | --- |
| 主要功能 | 支持 SM2、SM3、SM4 算法，具有密钥生成、分发、存储、管理等功能；提供密钥 |

| | |
|---|---|
| | 生命周期管理，提供创建密钥，禁用密钥，删除密钥，导入密钥（密钥来源为外部导入），查看密钥轮转历史，搜索指定密钥等功能 |
| | 支持服务设备动态扩展，满足密码服务能力使用要求 |
| | 支持服务设备动态扩展，满足密码服务能力使用要求 |
| 性能 | 密钥生成速率≥300 对 |
| 资质 | 提供国家密码管理局颁发的产品证书 |
| 其他 | 1 年质保 |

**（6）完整性保护工具**

基于签名验证服务开发的文件签名和验证的软件，可以对服务器重要文件、关键执行程序、第三方软件的控制文件以及日志文件进行完整性保护。该工具需无缝对接签名验签服务器及签名验签服务。

4．3．4 基础信息系统改造

**（1）邮件系统软件**

提供平台高安全、高性能的邮件系统。提供高可靠、高安全、高效率的办公邮件信息传输和交换。主要功能模块包括邮件收发功能、通讯录管理功能、会议与日程管理功能、邮件检索功能等几个主要部分。

**（2）时钟同步系统**

1） 需具备 CDMA 等多种方式作为外部时间源；

2） 需采用最新操作系统；

3） 需具备至少 6G 内存，64G 固态硬盘；

4） 需具备至少 4 个千兆网口、支持 8 万台以上客户端；

5） 需支持支持 IPV6；

6） 时间精度需小于 50nS；

7） 授时精度：NTP 网络授时精度小于 1ms；

8） NTP 吞吐量：需满足每秒 30000 次时间请求；

9） 需配套远程管理软件，监控 NTP 服务器状态、客户端授时偏差等；

**（3）HBA 卡**

1） 在服务器和存储装置间需支持输入/输出(I/O)处理和物理连接；

2） 服务器需支持国产化；

3) 需支持连接 FC 网络的应用，可实现高带宽高性能存储组网方案；

4) 需支持 PCIe x8 Gen3.0，需支持 I²C(Inter-integrated Circuit)和 PLDM(Platform Level Data Model)带外管理；

**（4）操作系统**

1) 支持但不限于国产化自主 cpu 平台。

2) 支持内核和核外统一访问控制安全框架 KYSEC。

3) 支持多策略融合的强制访问控制机制。

4) 内置私有数据隔离保护技术，通过该技术包括管理员在内的任何其他用户都不能进行非授权访问。

5) 内置国密算法，支持基于国密算法的加解密应用。

6) 支持可信计算 TCM/TPCM、TPM2.0。

7) 优化支持 KVM、Docker、LXC 虚拟化，以及 Ceph 、GlusterFS、OpenStack、 k8s 等原生技术生态，实现对容器、虚拟化、云平台、大数据等云原生应用的良好支持。

8) 内置支持快速块设备作为慢速块设备缓存以加速 IO。

9)支持 swap 压缩以减少 IO 并提高性能。

10)支持 FCoE 、iSCSI， 支持将 Ceph 块设备视为常规磁盘设备条目，挂载到某个目录并使用标准文件系统格式化，比如 XFS 或者 EXT4。

**（5）中间件**

1) 必须通过 Java EE5 、6 、7 、8 四个标准规范的官方兼容认证。

2) 必须通过 Jakarta EE9.1 官方兼容认证。

3) 产品应具备良好的生态环境适应能力，支持多种主流国产操作系统。

4) 内置 APM 工具，可以针对性能问题进行代码定位，提供线程剖析功能，迅速定位问题。

5) 提供内置的 JMS 服务，并支持将 TongLINK/Q 等第三方消息中间件作为消息服务代理。

6) 支持集群部署，提供集群管理工具，内置支持国密算法 (SM2/3/4) 的负载均衡模块。

7) 无需第三方 HA 软件，即可实现负载均衡模块的双机状况监控与备份切换，避免单点故障软件自身应避免存在安全漏洞威胁。

8) 内置类加载冲突检测工具，可以检测出应用部署和运行过程中哪些类存在类加载冲突问题，并能自动生成冲突检测报告，方便快速定位和解决应用类加载问题。

9) 支持在管理控制台页面上配置异步日志，保证日志输出的同时降低对应用系统性能的影响。

10） 监控服务可以选择监视信息的回放时间段，方便运维人员了解过去某段时间的系统和应用的监控情况。

**（6）数据库**

1） 产品核心功能模块的核心源码自主代码比例不低于 95%。

2） 单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等。支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移。

3） 在不少于 100 仓数据和 100 用户并发场景下，产品在不同数据库环境 7*24 小时的 TPC-C 测试中能够稳定正常运行。

4） 单表插入 100 万数据小于 1.3 秒，平均存储性能可达到 80 万条/秒以上，单库单表导入 200 万行数据小于 3 秒，批量导入性能可达到 70 万条/秒以上；支持 1GB 以上数据备份完成时间在 7 秒以内，恢复完成时间在 21 秒以内。

5） 支持数据库共享存储集群，集群规模可达 8 节点；集群具备多节点负载均衡能力;集群每个节点均支持写入，且支持多节点间的缓存一致性。

6） 在主备集群模式下，模拟不少于 3 次的主机故障场景测试，从发生故障到备用数据库服务器切换为主服务器的时间不高于 6 秒，且系统应保证服务切换期间的数据不丢失、不损坏。

4．3．5 融合承载网汇聚设备

**（1）电子架**

插框:业务板区槽位数 24;带走纤槽，电源、风扇、主控板、交叉板均为冗余设计且满配电源模块和风扇框;

主控板:配置 2 个主控板(支持 1+1 备份);

交叉板:配置 2 个交叉板(支持 1+1 备份，低阶交叉能力 160G);

线路侧接口:2*100G(分布在两个不同的业务槽位);

支路侧接口:(32*E1)+(30*10G)+(12*GE)+(16*STM-N);

功能授权:含 OTN、SDH 功能授权、含 800G 交叉容量授权。

**（2）光子架**

插框:业务板区槽位数 12;带走纤槽，电源、主控板均为冗余设计且满配电源和风扇;

系统控制板:配置 2 个系统控制板(支持 1+1 备份，支持时钟处理);

合/分波系统:配置 1 个合波板，1 个分波板(支持 48 个通道合、分波功能);

光放大板:配置 1 个光放板(满配光放大模块，支持光监控信道和主光信道的合、分波)。

**（3）光监控板卡**

光监控信道板:配置 1 个光监控信道板(含 2 路光监控信道，支持多光子架共用，支持线路光纤质量探测功能，支持探测能力最大 150km)

功能授权:含光监控信道板的线路光纤质量探测功能授权。

**（4）电源组件**

交流转直流供电组件，配电框、电源模块等关键部件均为冗余配置。

**五、项目工作范围与工作要求**

**5.1 工作范围**

5.1.1 中标人应按照本项目现场实际条件、招标需求及最终项目目标提供设计（或设计配合）、设备以及材料供货、安装、设备测试、调校、试运行（系统、单机）、采购人相关人员的培训及通过有关部门的验收期间提供必要的技术支持和配合、质量保证期内免费保养维修等全部工作。

5.1.2 依据本项目的工作内容与范围：中标人应包设计（或深化设计）、包设备与材料供货、包人工、包质量、包安全的方式实施本项目总承包并确保本项目最终验收顺利通过。

5.1.3 中标人应具备上海市或有关行业管理部门规定的在上海市场实施本项目所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由中标人自行负责。

**5.2 工作要求（包括但不仅限于一下要求）**

5.2.1 根据招标人的需求（要求）在采购人的指导下，负责完成系统方案与施工图深化设计以及出图工作（如有）。

5.2.2 负责编制项目实施组织设计、质量控制和技术方案、安装工艺及技术要求、施工详图等技术文件，交采购人审核后执行。

5.2.3 设备安装、线缆敷设和配合调测均应根据技术方案经过内控审核，项目各环节应按照方案实施并进行质量自验，保证项目质量符合国家和上海市有关技术标准与规范要求。

5.2.4 负责编制项目进度计划和保障措施，确保按期完成。若有变更，应及时调整进度计划。

5.2.5 负责实施方案向有关部门的报批工作，以及项目竣工后向有关部门、单位申报测试与验收工作，并确保可以满足主管部门的要求（如有）。

5.2.6 根据采购人的变更要求及实施现场的实际情况，负责完成安装方案与施工图的变更设计，并经采购人及其委托监理单位（如有）审核后实施。

5.2.7 负责设备的供应，并按合同范围、交付期限、质量标准等，保质保量按时将设备与器

材等运至项目现场、完成本项目线缆敷设和设备安装、测试、调校、系统开通、试运行等全部工作。

5.2.8 负责完成设备安装布局设计与实施、装饰与环境以及供电等工作，并协助采购人完成控制室（机房）项目验收工作。

5.2.9 协助采购人和主管部门完成项目验收工作。验收按本项目合同以及国家和上海市的有关技术标准与规范进行。

5.2.10 负责完成项目竣工图纸与资料的编制工作，并在项目完成并交付使用前提交项目竣工资料叁套（如采购人有此项要求）。

5.2.11 负责采购人相关人员的技术培训，并提供使用、操作手册，保证达到独立上岗操作与日常维护的水平。

5.2.12 负责项目售后服务（设备免费保修期和服务响应时间不低于招标文件要求）。

**六、项目管理要求**

6.1 在项目实施期间，中标人应严格执行国家、地方、行业有关本项目业务管理和安全作业的法律、法规和制度并按规定承担相应的费用。中标人因违反规定等原因造成的一切损失和责任由中标人自行承担。

6.2 中标人在投标书中承诺并经招标人认定的项目负责人及专业技术人员必须是本单位职工（在本单位缴纳社会保障金）和该项目实施现场的实际操作者，应具有类似本项目的实施经验，并应常驻项目现场。未经采购人同意，中标人不得调换或撤离上述人员。如采购人认为有必要，可要求中标人对上述人员中的部分人员作出更好的调整。

6.3 中标人在项目实施期间，应按项目实际进度与环节落实所对应项目整体及各环节管理工作，按照规范做好项目实施期间相关管理与实施记录。

6.4 中标人应严格参照执行国家与上海市有关建设工程安全文明施工管理的法律、法规和政策，积极主动落实安全文明及环境保护施工的管理和考核等有关工作，指派专人负责施工现场的安全，建立安全用电、动用明火申请批准等制度，防止隐患和落实好作业区域内的环境和原有装饰保护要求，确保作业区域周围环境的整洁和不影响正常办公区域正常工作，安全、文明实施本项目设备安装工作。

6.5 中标人在与采购人签订项目合同的同时要签订安全生产责任协议书、治安防火责任协议书、项目文明实施协议书和廉政责任书（如采购人有此项要求），中标人若违反规定违章作业等，采购人有权责令停工整改，一切损失由中标人自行承担。

6.6 在项目实施进行中，如发生人身伤害及意外，由中标人承担一切责任，采购人不承担连

带责任，并保留追诉其责任的权利。

6.7 中标人在项目实施期间必须遵守采购人的规章制度并提供实施人员名单。

6.7 各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的管理措施，并在报价中列支相应的费用清单，投标人报价中未列支上述费用清单的，上述费用视为已包含在投标人的投标总报价中。

6.9 本项目合同不得转让、不得分包。

6.10 本项目设备材料供货及安装调试将纳入监理单位（如有）、采购人的管理范围，中标人在此过程中须服从上述单位的管理协调。

**七、其他要求及申明**

7.1 投标人在进行安装方案设计时要考虑各设备的实用性、安全性、可靠性、兼容性、灵活性、先进性、开放性、扩展性、便捷性、高效节能、环保等各项因素，要选用技术先进、性能优良、使用可靠的设备和产品（不得选用已经停产或即将停产淘汰的产品），并与原有系统实现无缝对接。

7.2 本次采购不接受整体由进口产品所组成的系统。

**八、项目质量标准与验收要求**

8.1 投标人完成本项目应达到的质量标准应符合国家、地方及相关政府管理部门和行业与本项目有关的各项技术标准、规范要求，并满足采购人实际需求，标准、规范等不一致的，以要求高（严格）的为准。

8.2 本项目验收将由采购人组织进行或委托第三方进行。

8.3 本项目连续 3 次验收未获通过，采购人有权解除合同并按照合同约定的违约条款处理。

**九、知识产权及保密要求**

9.1 乙方数据、文件、资料知识产权

乙方应确保其完成本合同要求所利用、提交的所有数据、文件、资料及为完成项目而实施的其它工作没有侵犯任何人的专利权、商标权及其他知识产权。乙方保证甲方均不会因其履行合同义务而引起的在专利权、商标权以及其他知识产权方面，发生针对甲方的任何第三方的索赔。如有发生，乙方将负责处理并承担由此引起的法律责任以及包括律师费用在内的一切费用及损害赔偿。

9.2 项目保密要求

乙方为履行本合同所形成的资料、数据等成果及其他任何附加成果（包括但不限于工作中所取得的中间数据、资料等）的完整应用知识产权和使用权均属甲方所有，乙方负有保密义务。乙

方在项目服务中使用及产生的的所有资料、数据，包括但不限于本合同及附件、招标文件、工作过程资料、数据、说明等资料的所有权和过程中产生的数据、资料等知识产权、使用权、处理权均属于甲方。乙方及其任何人员不得擅自处理、发表、引用或向第三方提供或泄漏与本项目、本合同的业务活动的任何有关的资料，以及在合同履行过程中形成的制作成果或文字资料。