需求中有修改：

（一）4.6.2，原“▲具备国家密码管理局商用密码检测中心颁发的安全认证网关商用密码产品认证证书且安全等级满足第二级要求。”现修改为：▲具备国家密码管理局商用密码检测中心颁发的服务器密码机商用密码产品认证证书且安全等级满足第二级要求。

（二）4.6.3，原“▲具备国家密码管理局商用密码检测中心颁发的身份认证系统商用密码产品认证证书且安全等级满足第二级要求。”现修改为：“▲具备国家密码管理局商用密码检测中心颁发的身份认证系统商用密码产品认证证书，满足安全等级第二级或 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》标准。”

4.6.2 服务器密码机

序号	功能指标要求
1	支持液晶屏显示。
2	▲支持保留格式加密，支持抗量子功能。（提供具有 CMA 认证或 CNAS 认证的第三方检测机构出具的检测报告并加盖原厂公章）
3	密码机 API 支持 GM/T 0018-2012《密码设备应用接口规范》定义的接口规范
4	支持物理随机源生成真随机数
5	采用三层密钥结构保障密钥及系统安全性，保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件也受备份密钥的加密保护
6	采用基于门限算法的备份密钥秘密共享机制，恢复出完整的备份密钥，确保密钥备份/恢复的安全
7	支持采用索引/标识对密钥进行管理，包括密钥的生成、存储、使用、导入/导出、删除等
8	支持基于 SM1、SM2、SM3、SM4 等商用密码算法。
9	对称密钥存储容量：≥2000 个 非对称密钥存储容量：≥1000 对 SM2 密钥对产生速率：≥3500 对/秒 SM2 签名速率：≥3000 次/秒 SM2 验签速率：≥2000 次/秒 SM3 计算 Hash 速率：≥850Mbps SM1 加解密速率：≥350Mbps SM4 加解密速率：≥450Mbps 最大并发数：≥1000
10	设备支持对用户进行管理，采用基于角色的访问控制方式，针对不同管理员给予不同的操作权限，管理员权限间彼此制衡
11	设备支持 B/S 和命令行（CLI）界面对设备进行管理

12	支持 WEB 界面提供 CPU、内存、服务状态等基本使用信息的图形化展示
13	支持基于 NTP 时间源的系统时间同步
14	支持基于 SNMP 协议的健康状态监控
序号	**非功能指标要求**
1	所投产品具备国家密码管理局颁发的商用密码产品认证证书
2	▲具备国家密码管理局商用密码检测中心颁发的服务器密码机商用密码产品认证证书且安全等级满足第二级要求。

4.6.3 身份认证系统

序号	参数指标
1	支持需要使用多因素认证服务的用户信息管理功能，用户信息至少包括用户名称、用户唯一标识、证件类型、证件号、手机号等基本信息配置管理。
2	支持证书用户管理包括：证书用户注册、证书用户审核。
3	CA 证书管理：证书的新增、延期、注销、下载功能；多级证书链维护功能；证书配置项管理功能；
4	CA 证书模板管理功能
5	证书管理包括：双证书（签名证书与加密证书）签发、证书维护（延期、恢复、冻结、吊销）
6	对应的设备证书序列号、证书状态、证书起始时间、证书结束时间、证书操作（申请、更新、注销等）信息
7	系统管理功能包括用户管理（新增、编辑、锁定、解锁、删除）、角色管理
8	详细的认证日志记录，用于事后审计，至少包括认证记录、数字证书申请记录、服务器配置操作记录和异常认证记录等基本日志记录要求。
9	日志管理包括可根据用户和 IP 地址对登录日志进行查询功能；可根据 IP 地址对服务日志进行查询功能；
10	数字证书日志至少需要记录证书申请类型、数字证书序列号、数字证书申请时间、申请结果、如果失败，失败原因描述
11	操作日志和审计功能主要是针对登录访问多因素认证系统的管理用户，进行平台配置管理日志信息记录和审计功能，至少包括管理账户、操作类型（增加、删除、修改）、操作功能、操作资产对象的 IP 地址、操作状态、操作时间等进行查询管理，支持针对每条记录进行单独审计操作和审计管理。
12	证书 CRL 管理：CRL 生成与下载。
13	支持将用户登录访问 windows 操作系统、linux 操作系统的认证请求推送或者扫码方式通过手机数字证书进行统一证书认证后实现合法登录访问。
14	▲具备国家密码管理局商用密码检测中心颁发的身份认证系统商用密码产品认证证书，满足安全等级第二级或 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》标准。

采购文件中涉及上述修改内容的，一并更正。