# 国家法人单位信息资源库（一期）及社会

# 信用信息共享交换试点工程项目中央编办

# 数据综合服务系统技术需求

**一、总体要求**

1. 本部分内容是根据本项目实际情况制定的。
2. 投标人必须仔细阅读本部分的全部条款。对本部分中存在的任何疑问、遗漏或相互矛盾之处，或是对于相关要求不清楚，认为存在歧视、限制的情况，投标人可以向采购中心寻求书面澄清。
3. 本部分所列明的工艺、材料和设备的标准以及参照的品牌或分类号仅起说明作用，并没有任何限制性，投标人在投标中可以选用替代标准，品牌或分类号，但这些替代应当等于或优于文件技术要求。
4. 付款方式：

（1）合同签订后7个工作日内，甲方向乙方支付合同金额的40%。

（2）硬件设备到货并安装、调试合格试运行后7个工作日内，甲方向乙方支付合同金额的40%。

（3）项目完成且最终验收合格后7个工作日内，甲方向乙方支付合同金额的20%。

**二、技术要求**

1. 项目概述

1.1 建设背景

国家法人单位信息资源库（一期）及社会信用信息共享交换试点工程项目（以下简称法人库项目）是由国家发改委批准的中央预算内投资建设项目。项目由市场监督管理总局（原工商总局）牵头组织，中央编办、民政部、原质检总局、人力资源和社会保障部、税务总局、统计局、国家信息中心等部门共同建设。

1.2 建设目标

根据“十二五”国家政务信息化工程建设规划和“十三五”国家政务信息化工程建设规划，以国家统一的电子政务外网为依托，以中央编办提供的机关法人、事业单位法人信息为基础，融合人力资源和社会保障部、税务总局、统计局等部门的相关法人信息，采用统一社会信用代码为索引，能确定法人单位实有性和唯一性的机关法人、事业单位法人国家信息资源库，支撑包括全部法人的9项（含统一社会信用代码）信息的国家法人基础信息物理集中库；建设国家法人单位信息资源库（中央编办），包括全国机关法人（连带下设机构）、事业单位法人的全项数据，采用国家法人单位信息资源库（中央编办）与物理集中库共同对外提供信息服务；建立机关法人、事业单位法人信息共享与服务技术系统，为相关政府部门提供基于机关法人、事业单位法人9项（含统一社会信用代码）基础信息的查询、校核、分析、叠加、下载（有条件批量下载）等服务功能；建立信息安全体系和管理监控体系，为机关法人、事业单位法人的业务开展和信息共享提供保障。

通过本项目的实施，将切实提升中央编办“互联网+政务服务”能力，支持机关和事业单位统一社会信用代码赋码和登记管理全流程网上流转和不见面审批，方便机关和事业单位法人利用法人基础信息和电子证照信息办理相关业务，服务不收费、无介质，符合国家安全和密码相关要求。

2. 总体需求

一是完善建设机关与事业单位法人国家信息资源库（包含机关与事业法人业务信息和电子证照信息），为国家法人基础信息库提供全国机关法人、事业单位法人9项基础信息；

二是完善建设数据综合服务系统，具备查询分析、校核叠加、反馈管理等功能；

三是完善建设相关的安全保障环境和运维体系。

以上内容，由中央编办信息化基础运行环境以及建立在信息化基础运行环境之上的软硬件及相关系统用户所组成。信息化基础运行环境是指网络环境（与电子政务外网和互联网连接的部分）、服务器主机、存储环境、机房设施、数据库、机构编制围绕机关和事业单位登记管理的若干应用管理软件环境、终端等软硬件设施以及在此之上的应用开发、安全保障及运维等内容。

2.1 技术需求

1.100%中央单位、99%的省级单位（机关法人、事业单位法人）信息纳入法人库（不包括涉密单位）。

2.面向社会提供事业单位法人信息查询服务，年度报告专栏服务、信用信息通报服务、事业单位登记公告服务，不少于90%中央级单位对外公示，不良信息可实时公示。

3.数据更新频率方面，当事业单位法人信息（位于互联网）库在录入发生变化的数据后，24小时内将变量数据更新至国家法人单位信息资源库（中央编办、位于电子政务外网）。国家法人单位信息资源库（中央编办）录入/获取变量数据时，24小时内将变量数据更新至到国家法人库物理集中库。

4.性能指标方面：一般性的数据增加、修改、删除等操作，平均响应时间≤3秒，最长响应时间不超过5秒；一般业务操作的简单查询和统计，平均响应时间≤5秒，最长响应时间≤10秒；大数据量的查询、统计与复杂的统计汇总，平均响应时间≤30秒，最长响应时间不超过60秒。

2.2 系统需求

建设数据综合服务系统。包括查询服务、校核服务、分析服务、叠加服务、管理应用5个部分。提供机关法人、事业单位法人查询服务、校核服务、分析服务、叠加服务及管理服务，确保机关法人、事业单位法人基础信息及业务信息的鲜活、完整、准确、全面。

建设国家法人单位信息资源库（中央编办），囊括全国机关法人（连带下设机构）和事业单位法人的全项信息，并建立全国统一的机关和事业法人电子证照库。

完成相应应用支撑平台建设、网络系统建设（接入电子政务外网和互联网）、安全系统建设。

3. 技术要求

以下所有指标均为本项目所需设备的最低要求指标，投标商提供的产品应至少大于或等于所提出的指标。重要性是指该指标项的重要程度，与评分细则的扣分项应相对应。★代表最关键指标，一项不满足将导致扣5分；#代表重要指标，不满足将导致扣3分；无标识则表示一般指标项，不满足扣1分。

3.1 采购产品一览表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **货物名称** | **单位** | **数量** |
|
|  | 查询服务模块 | 套 | 1 |
|  | 校核服务模块 | 套 | 1 |
|  | 分析服务模块 | 套 | 1 |
|  | 叠加服务模块 | 套 | 1 |
|  | 管理应用模块 | 套 | 1 |
|  | 机关与事业单位法人基础信息库-电子证照管理模块 | 套 | 1 |
|  | 机关与事业单位法人基础信息库-电子证照应用模块 | 套 | 1 |
|  | 机关与事业单位法人基础信息库-业务信息存储模块 | 套 | 1 |
|  | 机关与事业单位法人基础信息库-电子证照信息存储模块 | 套 | 1 |
|  | 关系型数据库软件 | 套 | 3 |
|  | 前置库软件 | 套 | 1 |
|  | 数据服务平台 | 套 | 1 |
|  | 共享交换代理 | 套 | 1 |
|  | 应用服务代理 | 套 | 1 |
|  | 桥接服务 | 套 | 1 |
|  | 消息中间件 | 套 | 2 |
|  | 应用服务器中间件 | 套 | 3 |
|  | 核心交换机 | 套 | 2 |
|  | 汇聚交换机 | 套 | 8 |
|  | 接入交换机 | 套 | 8 |
|  | IDS | 套 | 2 |
|  | 漏洞扫描系统 | 套 | 1 |
|  | 网络安全审计系统 | 套 | 1 |
|  | 数据库审计系统 | 套 | 1 |
|  | 防火墙 | 套 | 10 |
|  | 网络病毒防火墙 | 套 | 2 |
|  | 堡垒主机 | 套 | 2 |
|  | 防病毒软件系统 | 套 | 1 |
|  | 数据库加密系统 | 套 | 1 |
|  | 主机安全审计系统 | 套 | 1 |
|  | 统一安全管理平台 | 套 | 1 |
|  | WEB应用防火墙 | 套 | 1 |
|  | 安全单向导入设备 | 套 | 1 |
|  | 安全密码模块 | 套 | 1 |
|  | 服务器 | 台 | 1 |

#### 3.2 产品清单及技术参数要求

以下所有技术参数均为本项目所需设备的最低要求技术参数，投标人提供的产品应至少大于或等于所提出的技术参数。重要性是指该技术参数项的重要程度，与评分细则的扣分项应相对应。★代表最关键技术参数，一项不满足将导致扣5分；#代表重要技术参数，不满足将导致扣3分；无标识则表示一般技术参数项，不满足扣1分。投标人须提供合适真实的产品方案进行应标，招标方或用户方可要求投标人在限定时间内提供投标型号产品进行综合测试。

1. 查询服务模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 当党政机关用户和党政机关应用提出查询需求时，快速高效的返回查询结果。用户登录门户后通过查询子系统输入特定的查询条件，该查询请求被分派到相应的资源区进行检索。用户通过调用查询服务，提取查询作业的返回结果，门户将结果进行汇聚后以用户期望的、预设的方式进行展现。  在调用各分库执行查询服务的同时，也同步调用机关事业法人库国家信息资源集中库的查询服务，待查询结果返回后，执行“查询结果比对”服务，并根据比对结果对集中库数据进行更新，以提高法人单位信息资源库数据的鲜活性。 |
|  |  | 一般查询 | 查询请求发起后，法人库按照一定的业务规则要求，反馈出相应的查询结果。同时保证查询数据的鲜活、准确、权威，查询方式的方便和快捷，查询范围经过严格授权，覆盖所有政务部门，并提供良好的查询体验。包括精确查询、模糊查询和定制查询三个模块。 |
|  |  | 批量查询 | 实现根据查询需求和查询条件规则，事先准备出批量查询条件，并将批量查询条件批量导入，执行相应查询的要求。通过执行查询过程，反馈出正确的查询结果。查询结果反馈形式可以支持图、表多种示意形式。包括批量查询模板定制、批量查询策略定制、批量查询三个模块。 |
|  |  | 扩展查询 | 提供直观图形化展示，结构化展示法人之间的隶属和变更等关系，展示机关法人、事业单位法人的轨迹信息，向用户提供开源的舆情关联信息，体现法人在社会上的活动；提供日志信息和档案信息的方便查询，以便进行数据质量的统计和流程服务的监控。包括法人叠加查询服务接口模块、法人关系查询模块、法人轨迹查询模块、日志查询模块、档案查询模块。 |
|  |  | 查询权限设置 | 实现法人信息的查询用户权限申请和权限配置的自动化和标准化，实现法人信息的查询申请得到及时响应，系统化管理数据的授权范围。包括查询权限申请、查询权限配置模块。 |
|  |  | 批量下载 | 提供机关法人、事业单位法人数据有条件下载功能，支持多种浏览器、多种下载工具，并提供重新下载、断点续传、完成消息推送等功能。包括批量下载策略定制、批量下载作业模块。 |
|  |  | 数据接口 | 与国家信息中心统一门户实现衔接，转发查询请求并将查询结果反馈。 |

1. 校核服务模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 通过对数据的校对、核查实现数据质量的持续改善。校核是用户使用查询和叠加服务时，对数据正确性的再一次验证的过程，如果查询和叠加结果数据与用户的实际情况相符则验证了法人信息库中的数据正确，如果查询结果与用户的实际情况不符，则发起反馈请求。 |
|  |  | 初始化校核 | 实现机关法人、事业单位法人基础数据、业务数据及信用信息入库时的比对和校验，提高数据校核的质量和时效性。由合规性比对模块、一致性检查模块、基准比对模块、多源比对模块、更新入库模块、规则模板制定模块、单条规则制定模块组成。 |
|  |  | 查询入口校核 | 政务用户在查询法人信息时，能够对其产生质疑，并反馈系统进行校核和更正。由判断信息校核方式模块、基准比对模块、多源比对模块、校核结果统计模块组成。 |
|  |  | 叠加入口校核 | 实现相关注册和业务办理系统在采集法人信息叠加时，将质疑的数据批量反馈给系统，通过基准比对和多元比对，校核法人库的相关信息。由基准比对作业模块、多源比对模块组成。 |
|  |  | 同步更新管理 | 实现中央编办业务系统的信息变更情况准确从前置库推送到法人库，进行级联修改，并通知相关前置库和业务系统进行修改更新。由更新策略制定模块、同步更新、更新反馈模块组成。 |
|  |  | 注册登记数据流管理 | 实现多个部委对机关和事业单位法人单项注册信息的统一管理与维护。由机关法人登记注册数据流管理模块、事业单位法人登记注册数据流管理模块组成。 |
|  |  | 数据接口 | 与国家信息中心统一门户实现衔接，转发校核请求并将校核结果反馈。 |

1. 分析服务模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 通过同比、环比分析，在线数据分析，关系网络分析等多种方式，多方位、多角度的实现对机关法人、事业单位法人数据的深层次应用，生成趋势分析、预测报表。 |
|  |  | 基础统计 | 实现法人单位基础信息库的类型、地域分布、状态等信息，分时间、地域、法人单位类型三个维度及其组合维度进行统计，并支持饼图、直方图、地图等多种信息展现方式。由法人类型统计服务模块、法人地域分布统计模块、法人单位状态统计模块组成。 |
|  |  | 数据质量统计分析 | 根据数据接收反馈系统的数据维护日志、数据反馈日志，统计分析法人基础信息资源来源、反馈统计、共享服务、准确性、实时性、完备性等数据质量等相关的指标。提供校核反馈的公示机制，通过社会监督与评价构建校核驱动力。 |
|  |  | 趋势分析 | 实现对法人单位稳定性、法人单位规模与增速趋势、财政供养人员规模趋势、法人信用状况趋势等的研究和分析。由法人单位稳定性趋势分析模块、法人单位规模与增速趋势分析模块、财政供养人员规模趋势分析模块、法人信用状况趋势分析指标模块组成。 |
|  |  | 事业单位编制管理工具 | 实现公共服务事项、法人权力清单、责任清单、机构设置、机构性质、人员编制关联情况的综合展示；并通过将事业单位业务信息与质检、工商、民政、统计、人社等部门法人信息的综合比对，实现事业单位事中事后监管。由事业单位编制信息展示模块、事业单位机构编制信息比对模块、信息反馈模块组成。 |
|  |  | 法人履职信息服务 | 实现对机关和事业单位法人履职信息的采集，实现履职信息面向社会公众、公务员、信息化支撑人员等用户不同程度的开放，提供智能关联查询功能，提供政策自助学习工具。由机关和事业单位法人履职信息采集模块、法人履职信息智能关联查询模块、政策自助学习模块组成。 |
|  |  | 机关事业单位协同工作服务 | 面向跨部门、跨行业、跨地域的机关和事业单位协同工作，提供文件资源汇集与共享、工作进展推送发布、评估反馈等功能。由机关和事业单位协同工作信息汇集模块、机关和事业单位协同工作进展展示模块、机关和事业单位协同工作评估模块组成。 |

1. 叠加服务模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 基准叠加 | 实现机构编制部门法人单位相关的业务信息与全国法人单位信息资源库的法人信息进行关联映射，并进行基准性叠加。由单次叠加模块、批量叠加模块组成。 |
|  |  | 叠加扩展 | 实现法人基础信息叠加的服务配置，日志管理和异常情况的及时预警。由服务配置模块、叠加日志管理模块、叠加预警权利模块组成。 |
|  |  | 用户管理 | 实现对各级用户的身份管理、权限管理、信息维护，通过用户申请、身份验证、身份审核等实现新用户的注册；通过用户信息维护管理实现老用户信息的维护、用户信息统计，通过权限赋予、权限设置、角色分配等实现不同级别用户权限的设定。由用户注册模块、用户权限管理、用户信息统计模块组成。 |
|  |  | 信息管理 | 实现对全国基础法人库信息的多类别综合管理，涉及数据源、数据质量、元数据三个方面，同时提供数据审计与数据监控功能。 |
|  |  | 数据接口 | 与国家信息中心基础数据交换平台实现衔接。 |

1. 管理应用模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 为管理用户提供数据加载、反馈管理、数据更新、数据维护监管和数据协同等服务功能，实现数据从加载入口到维护监管全流程综合管理应用。 |
|  |  | 数据加载 | 实现法人信息的采集、清理、比对、入库、反馈等工作，形成较为完整的法人信息资源。由信息采集配置模块、信息整合入库模块组成。 |
|  |  | 反馈管理 | 数据反馈包括数据处理反馈和校核反馈，将数据校核结果和数据处理结果通过反馈管理子系统反馈编办对接系统。由数据清洗模块、数据比对模块、数据入库模块、数据反馈模块组成。 |
|  |  | 数据更新 | 调用本部委的数据更新服务，完成数据更新的过程，数据更新子系统提供数据更新服务的入口。由增量更新模块、增量追加模块、全面覆盖模块组成。 |
|  |  | 数据维护监管 | 实现对各共建单位校核反馈结果的处理情况进行监管，并提供统计报告。由数据维护监管模块、校核反馈模块组成。 |
|  |  | 数据接口 | 提供统一的协同服务入口，通过协同子系统调用各部委的协同服务，实现共享信息的交换。 |

1. 机关与事业单位法人基础信息库——电子证照管理模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 受理机关和事业单位电子证照相关业务申请，提供电子执照的生成、变更、注销等的全生命周期管理。本模块在中央编办以全国集中方式运行，各级事业单位登记管理局用户登录本模块完成相关业务。 |
|  | # | 与第7项（电子证照应用模块）、第9项（电子证照存储模块）、第34项（安全密码模块）为同一品牌 |
|  |  | 证照签发 | 签发管理。根据业务系统发起的申请请求，签发电子证照。 |
|  |  | 注销管理。根据业务系统发起的注销请求，注销电子证照。 |
|  |  | 异常状态列表签发。根据接收的事业单位注销信息等，签发并发布异常状态列表。 |
|  |  | 发布管理。提供异常状态列表的发布服务，以及发布策略的配置。 |
|  |  | 模板配置。配置电子证照外观模板。 |
|  |  | 状态管理。提供系统版本、系统配置、运行环境、机构信息等。 |
|  |  | 统计模块。提供单项或综合的电子证照的查询、统计功能，并提供导出功能。 |
|  |  | 安全通信。采用双向身份鉴别机制，保证通信双方身份的真实性。通信双方通过密码技术保障所传输信息的机密性。对传输的信息进行电子签名，保证数据完整性。 |
|  |  | 业务同步 | 数据同步。通过系统接口，实现与事业单位登记管理系统间的数据交互，包括事业单位登记信息、变更信息，状态信息等。 |
|  |  | 业务受理。将事业单位登记管理系统提交的事业单位登记信息安全提交到证照签发模块，完成电子证照业务受理。 |
|  |  | 数据管理。提供数据备份、恢复、备份策略管理功能。 |
|  |  | 业务统计管理。提供电子证照业务量、发放量统计。 |
|  |  | 系统管理 | 系统运行监控。提供各应用系统运行情况的监控。 |
|  |  | 电子证照发放查询。提供机关和事业单位电子证照发放情况的查询。 |
|  |  | 统计分析。提供电子证照业务情况和发放情况的统计分析功能，支持按登记机关、电子证照状态、时间等维度的统计查询分析。 |
|  |  | 权限管理。设置控制操作人员访问系统功能的权限。 |
|  |  | 数据接口 | 与事业单位登记管理系统统一用户身份认证管理。  实现与事业单位登记管理系统的信息同步 |
|  | # | 标准符合性 | 符合国家电子文件管理部际联席会议《电子证照基础国家标准》相关要求 |

1. 机关与事业单位法人基础信息库——电子证照应用模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 为机关和事业单位提供帐户设置与授权、电子证照管理功能，电子证照使用功能。机关和事业单位可使用电子证照完成电子签名、出示电子证照、验证电子证照、留档电子证照等功能。  本模块由移动客户端和服务端组成。其中服务端在中央编办以全国集中方式运行，支持各级事业单位登记管理局用户登录本模块完成相关业务，受理使用电子证照的机关法人和事业单位法人、合规的电子证照应用方相关业务请求。  移动客户端支持使用电子证照的机关法人和事业单位法人、合规的电子证照应用方完成相关业务，支持二维码等使用方式，支持通过窗口或第三方APP等扫描使用。 |
|  | # | 与第6项（电子证照管理模块）、第9项（电子证照存储模块）、第34项（安全密码模块）为同一品牌 |
|  |  | 帐户设置与授权 | 机关和事业单位帐户管理。对机关实施赋码和对事业单位实施登记后，系统自动为该机关和事业单位创建一个初始用户和一级用户。 |
|  |  | 多级用户管理。包括初始用户、一级用户、二级用户等。初始用户为机关和事业单位法定代表人；一级用户为电子证照实际管理人，每个机关和事业单位仅有一人；二级用户为办事人员，可以有多个，由一级用户负责管理。 |
|  |  | 授权管理。根据机关和事业单位内部管理实际情况，对电子证照的使用进行授权。 |
|  |  | 接口服务。提供电子证照使用授权管理接口，供机关和事业单位内部办公系统等调用。 |
|  |  | 证照领取 | 电子证照下载。对机关实施赋码和对事业单位实施登记后，即可自动生成电子证照，机关和事业单位可通过移动APP下载。初始用户和一级用户必须来自事业单位登记管理系统。 |
|  |  | 电子证照查询。查询结果与纸质证照的展示效果一致。 |
|  |  | 验证服务 | 电子证照真实有效性验证。包括验证电子证照是否由登记管理部门签发，该电子证照的状态是否有效。 |
|  |  | 机关和事业单位身份认证。提供基于电子证照的身份认证功能，验证机关和事业单位身份的真实性。 |
|  |  | 电子签名验证。对机关和事业单位使用电子证照对业务数据进行电子签名提供验证服务，验证签名数据是否是该机关和事业单位提交的，且未经篡改。 |
|  |  | 照面信息获取。可对电子证照实施解析，获取照面信息。 |
|  |  | 验证管理 | 服务授权。对使用电子证照各类验证服务的应用方进行统一管理，只有获得授权的应用系统才能调用电子证照验证服务。 |
|  |  | 服务监控。对验证服务提供情况实时监控，及时掌握各项服务访问情况。 |
|  |  | 服务统计。对各应用系统调用电子证照服务情况进行统计。 |
|  |  | 数据接口 | 向使用电子证照验证服务的应用方提供验证服务接口。包括但不限于电子证照验证接口、机关和事业单位身份识别认证接口、电子证照签名数据验证接口、信息获取接口等。 |
|  |  | 与事业单位登记管理系统统一用户身份认证管理。  实现与事业单位登记管理系统的信息同步。 |
|  |  | 与国家电子政务外网身份认证管理系统衔接，支持同步给机关和事业单位法人发放国家电子政务外网法人身份证书 |
|  | # | 标准符合性 | 符合国家电子文件管理部际联席会议《电子证照基础国家标准》相关要求 |

1. 机关与事业单位法人基础信息库——业务信息存储模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 以全国集中方式，存储和检索机关法人、事业单位法人基础数据、业务数据、信用信息及全部的过程及演变信息。 |
|  | ★ | 性能要求 | 能够在通用服务器上运行，支持服务器集群部署，能够在高并发量下进行查询响应并优化，支持1000个用户同时在线使用 |
|  | ★ | 加密防护 | 支持核心业务数据存储的加密防护，对使用的商用密码密钥具备密钥管理功能。所有密码运算和处理操作要使用经国家密码管理委员会批准的标准密码算法。密码算法、密码协议的使用符合国密局要求。 |

1. 机关与事业单位法人基础信息库——电子证照存储模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 与第6项（电子证照管理模块）、第7项（电子证照应用模块）、第34项（安全密码模块）为同一品牌 |
|  | # | 数据接口 | 电子证照签发成功后，由电子证照管理系统将电子证照保存到电子证照库。 |
|  |  | 支持电子证照应用系统对外提供电子证照查询服务、下载服务，服务于应用过程中对电子证照电子归档需求。 |
|  |  | 数据存储 | 实现机关和事业单位所有电子证照全国集中存储。包括最新状态的电子证照，以及历史存在的电子证照。支持当前电子证照和历史电子证照的分区存储。 |
|  |  | 电子证照可以以PDF文件和OFD两种格式存储 |
|  |  | 数据管理 | 数据采集。接收电子证照管理系统发送的电子证照，采集全国集中电子证照库所需的信息资源。 |
|  |  | 数据入库。按照入库规则加载电子证照到在用库，并将历史电子证照信息保存至历史库以供备查。 |
|  |  | 系统管理 | 应用系统管理。确保只有经授权的应用系统才能访问电子证照库。 |
|  |  | 数据备份。提供数据备份及备份策略管理功能。 |
|  |  | 统计分析。提供电子证照相关信息及应用服务情况的统计分析功能。支持多种统计条件查询，并提供统计结果的表格导出功能。 |
|  |  | 数据接口 | 与事业单位登记管理系统的电子文件（电子档案）模块实现数据衔接 |
|  | # | 标准符合性 | 符合国家电子文件管理部际联席会议《电子证照基础国家标准》相关要求 |

1. 关系型数据库软件

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ |  | 提供的数据库应是大型关系型数据库管理系统，支持ANSI/ISO SQL 99标准； |
|  |  |  | 数据库应是一个支持多平台、开放式系统，应支持各主流厂商的硬件及支持64位UNIX、 Linux、Windows 2003/2008 Server以上等多种主流操作系统平台； |
|  | ★ |  | 数据库需要支持UNICODE、GBK和GB18030字符集； |
|  |  |  | 支持主流程序设计语言对数据库开发，具备开放式的客户编程接口，提供ODBC、JDBC、OLEDB、.Net Data Provider(NDP)、PHP、Perl等开发接口，以及嵌入式SQL编程接口ESQL，提供与Oracle OCI、Pro\*C、C++、PL/SQL兼容的开发接口；针对ODBC接口和JDBC语言标准;支持通用的数据库开发平台 |
|  |  |  | 具备完善的数据库管理功能和强大的检索功能；支持大数据量的加载；提供存储过程和触发器功能； |
|  |  |  | 数据库应有海量数据处理能力，系统容量管理能支持128TB以上 |
|  |  |  | 支持水平范围分区和水平列表分区技术，支持组合分区技术，支持两种以上的垂直分区技术。单表容量能支持32TB以上 |
|  |  |  | 数据库具有完备的安全技术，如用户管理，角色管理，以及强认证等安全技术； |
|  | ★ |  | 产品安全级别达到《GB/T 20273-2006信息安全技术数据库管理系统安全技术要求》 |
|  |  |  | 支持数据库自动实时跟踪、监控，可自动性能调优，并能为管理员提供调优建议；支持自动化的内存、空间管理等；具有完备的管理工具来管理各类数据库对象，对系统进行诊断并性能优化； |
|  |  |  | 数据库具有离线备份、联机备份机制和数据库恢复机制，具有自动备份和日志管理功能，支持数据块级的增量备份； |
|  | # |  | 支持并行应用集群技术，支持多节点共享存储集群部署，共享存储集群应是可伸缩的，可通过增加节点扩展处理能力 |
|  |  |  | 应支持7×24小时全天候运行，容错及无断点的错误恢复机制。 |

1. 前置库软件

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 基本要求 | 提供的数据库应是大型关系型数据库管理系统，支持ANSI/ISO SQL 99标准； |
|  |  |  | 数据库应是一个支持多平台、开放式系统，应支持各主流厂商的硬件及支持64位UNIX、 Linux、Windows 2003/2008 Server以上等多种主流操作系统平台； |
|  | ★ |  | 数据库需要支持UNICODE、GBK和GB18030字符集 |
|  |  |  | 支持主流程序设计语言对数据库开发，具备开放式的客户编程接口，提供ODBC、JDBC、OLEDB、.Net Data Provider(NDP)、PHP、Perl等开发接口，以及嵌入式SQL编程接口ESQL，提供与Oracle OCI、Pro\*C、C++、PL/SQL兼容的开发接口；针对ODBC接口和JDBC语言标准;支持通用的数据库开发平台； |
|  |  |  | 具备完善的数据库管理功能和强大的检索功能；支持大数据量的加载；提供存储过程和触发器功能； |
|  |  |  | 数据库应有海量数据处理能力，系统容量管理能支持128TB以上。 |
|  | # |  | 支持水平范围分区和水平列表分区技术，支持组合分区技术，支持两种以上的垂直分区技术。单表容量能支持32TB以上 |
|  |  |  | 数据库具有完备的安全技术，如用户管理，角色管理，以及强认证等安全技术； |
|  |  |  | 支持数据库自动实时跟踪、监控，可自动性能调优，并能为管理员提供调优建议；支持自动化的内存、空间管理等；具有完备的管理工具来管理各类数据库对象，对系统进行诊断并性能优化； |
|  |  |  | 数据库具有离线备份、联机备份机制和数据库恢复机制，具有自动备份和日志管理功能，支持数据块级的增量备份； |
|  | # |  | 支持并行应用集群技术，支持多节点共享存储集群部署，共享存储集群应是可伸缩的，可通过增加节点扩展处理能力 |
|  |  |  | 应支持7×24小时全天候运行，容错及无断点的错误恢复机制； |

1. 数据服务平台

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 数据处理服务 | 提供对机关法人、事业单位法人基础信息的清洗和比对校核服务。通过数据处理，形成部门真实、鲜活、完备和权威的机关法人、事业单位法人基本信息。对于经过清洗和比对的结果数据通过部门的数据共享交换代理反馈给部门的前置数据库，供部门进行核查。 |
|  |  | 数据处理服务主要功能包括：数据清洗、数据比对、数据入库和数据反馈。 |
|  |  | 数据管理服务 | 提供数据源管理功能。对数据源的维护及接入过程管理。 |
|  |  | 提供数据质量分析功能。对机关法人、事业单位法人数据的质量进行统计分析、抽检评定，生成数据维护情况分析、抽检情况分析报告，主要包括数据质量问题类指标和数据质量处理情况指标，并定期发布数据质量分析报告，由共建单位对数据质量进行联合管理。 |
|  |  | 提供元数据管理功能。元数据管理实现元数据维护、元数据审核、元数据注册、元数据变更和元数据注销功能。通过元数据编目模块生成核心元数据目录存放在各部门的元数据库；可提供服务的元数据分别生成公共资源目录和交换服务目录，经审核后发布到门户，各政务部门可登录网站进行目录查询并浏览核心元数据内容。 |
|  |  | 提供数据审计功能。针对数据的提取、传输、预处理、加载、维护校核、入库等过程，系统需提供过程日志、应用日志等审计管理功能，对数据维护情况、数据校核情况和数据质量进行统计分析。 |
|  |  | 提供数据监控功能。系统需提供数据维护的监控功能，进行全程监控，并生成统计分析报表。对数据数量、质量、频度、构成等信息进行分析挖掘，发现异常及时报警，及时发现并处理系统异常。对日志进行分析挖掘，对效率、范围、异常率等信息进行分析挖掘，辅助系统管理人员对数据采集与整合策略进行调整。 |
|  | # | 统一架构、统一管理 | 提供统一的运行环境，基于微服务体系架构，内置服务管理、流程引擎、数据管理、传输引擎、元数据管理等核心组件，数据加工服务、数据质量服务、数据共享服务既能运行在同一个引擎中，也可以根据需要部署在不同的引擎中运行。 |
|  | # | 实现数据质量、元数据、数据血缘关系、数据资产管理、数据加工处理、数据共享服务等的统一管理，基于统一管理引擎和统一的规则库实现统一管理和存储。 |
|  | # | 基于统一工具内实现数据质量检查、数据加工规则等的可视化配置、部署、管理。支持数据结构变化和服务模型一致性检查及报警。 |
|  | ★ | 统一任务调度 | 提供菜单生成器生成菜单，方便基于菜单交互调度。 |
|  | ★ | 提供定时调度（多样定时组合，时间间隔可到秒），并能可视化配置。 |
|  | ★ | 提供跨节点调度，方便位于不同机器上运行节点之间的调度，并能可视化配置。 |
|  | ★ | 提供流程调度，配置好的服务经过拖拉生成流程，支持子流程，可嵌套调用定制的任务或流程。 |
|  | ★ | 支持平行处理、顺序执行、条件处理、意外处理；可根据CPU、I/O、网络等情况调整并行处理的并发数。 |
|  | ★ | 当流程运行出意外时，可选择补偿运行、断点续运行、间隔检查运行等处理方式。 |
|  |  | 集群及高可靠性 | 能可视化设定集群主从关系等，方便通过增加机器实现负载的扩展。 |
|  |  | 支持软负载分配方式，将服务调用自动分配到负载比较小的机器上运行, 当一个节点出现故障时，不影响其他节点运行，接入的服务调用会被自动分配到没有故障的节点上运行。 |
|  |  | 数据检查 | 为减轻对信息系统数据库影响，数据质量检查采用数据流检查技术，数据质量检查方法及计算运行在引擎中而不是依赖数据库的SQL。 |
|  |  | 不仅具备库和表的初步探测检查、数据加工过程中的数据质量检查，还要具备事后的精度数据质量检查，并能对问题数据筛选、排查、问题跟踪，提供数据质量报告和问题数据分析，异常数据处理、数据比对验证检查等功能。 |
|  |  | 库和表的初步探测 | 提供全库初步探测，对库中全部或者部分表做初步探测获得库基本信息，每个表初步探测包括表名、主键字段数、外键字段数、字段数、必填字段数、记录数、空值率、空值比等。并以报表的方式提供。 |
|  |  | 提供数据库表基本信息分析，可以查看表数据、查看元数据、查看统计信息、查看键关系、查看填充信息。 |
|  |  | 表基本信息分析的统计信息包括字段名称、记录数、独特值数、模式值数、空值数、缺省值数等 |
|  |  | 精度数据质量检查 | 提供数据质量检查服务对数据库表做指定规则检查，包括格式检查、范围检查、缺失记录检查、相似重复记录检查、精度检查、逻辑表达式检查、复合规则检查等。 |
|  |  | 并分别根据不同规则特点提供不同的录入界面。 |
|  |  | 逻辑表达式检查包括逻辑检查、字符串逻辑检查。提供可视化定义界面。 |
|  |  | 相似重复记录检查，包括完全重复记录检查、相似记录检查。提供可视化定义界面。 |
|  |  | 复合检查是指多种数据质量检查规则的and、or的组合，并能可视化配置。提供可视化定义界面。 |
|  |  | 提供数据质量检查方法接口、相似度检查方法接口，方便采用java增加数据质量检查方法。 |
|  |  | 检查结果处理 | 数据质量检查结果存储到指定数据库中，存储表结构根据选择的检查字段、定义的检查规则自动生成，并提供可视化界面，方便修改信息配置。 |
|  |  | 针对每个数据质量检查服务提供数据质量检查结果报告，包括异常数据、异常数据检查的规则描述，并能做问题数据统计、修改情况统计、检查规则统计。 |
|  |  | 对与检查出的存在数据质量问题的数据，提供能在线修改的界面，方便将异常数据修改到数据质量存储表中，提供选项方便将确认的修改数据发送到数据源方。 |
|  | ★ | 比对和验证检查 | 对源库表和目标库表做一致性比对检查，包括表结构比对、数据一致性比对，能发现并展示不一样的结构、不一致的数据（包括增加、修改、减少的数据） |
|  | ★ | 对源和目标文件夹下的文件做比对和验证检查，能发现并展示不一致的文件，包括增加、修改的文件。 |
|  |  | 数据加工能力 | 采用数据流加工技术，提供统一加工服务实现数据库、NoSQL（hive、hbase、mogodb）、搜素引擎（ElasticSearch）、文件、XML、Web Service、传输队列、适配器、内存表、JSON等之间的相互交换。 |
|  |  | 通过工具可视化配置，通过拖拉等操作，可视化实现异构数据之间的转换、加工、映射。 |
|  |  | 支持对数据源实时、增量、批量、全量的交换策略，抽取条件可以是静态语句、动态SQL规则、来自变量、来自变量组等。支持变化数据捕捉增量抽取策略。 |
|  |  | 支持数据分块、分组并行处理。可视化定义分组并发数。 |
|  |  | 保证过程中事务完整性。支持按行提交、按块提交、完成后提交方式，并能可视化配置。 |
|  |  | 提供多种数据转换方法，包括字符串转换、字段赋值、时间类转换、数据比对与翻译、数学运算、身份证格式转换等。 |
|  |  | 多种逻辑处理，包括：格式匹配检查、字符串逻辑检查、重复记录检查、范围内检查、逻辑检查、复合逻辑检查、自定义逻辑检查等。并能可视化配置。 |
|  |  | 提供加工过程中的数据质量检查，根据数据逻辑判断规则，将干净的数据装载到目标中，将判断有问题的数据路由到数据库表或者数据文件中。 |
|  |  | 可视化选择数据路由策略，根据路由条件将数据加载到不同的目标上，数据加载目标可以是数据库表、文件、XML、消息队列、数据处理器方式等 |
|  |  | 易用性 | 提供统一的工具实现ETL服务、ETL调度、ETL流程、ETL转换及逻辑规则的可视化定义等。 |
|  |  | 节点管理，可视化创建节点运行环境、可视化查看部署在的节点上的资源，包括服务、流程、变量等。 |
|  |  | 提供详细的数据加工运行日志，便于用户跟踪数据加工过程、加工的数据记录数和插入、修改、删除的数据记录数等。 |
|  |  | 记录由于技术原因出现的废弃数据能方便检查。 |
|  |  | 对于运行过程中的异常情况报警，并记录原因。 |
|  |  | 元数据管理 | 提供元数据注册管理，包括分类管理、注册、审核、发布。 |
|  |  | 提供元数据变更管理，包括变更注册、变更审核、变更发布、版本管理。 |
|  | ★ | 数据建模 | 提供模型分类管理，包括目录的创建、编辑、删除等。 |
|  | ★ | 提供正向数据建模功能，可视化定义数据模型，定义模型之间的关系。 |
|  | ★ | 提供反向数据建模功能，可视化导入已存在数据库表的模型相互关系，并能修改完善其元数据。 |
|  |  | 模型实体化 | 对于已创建的数据模型可以根据选择的数据库类型，实体化为相应的表结构。 |
|  |  | 支持主流的数据库，如Oracle、SqlServer、Mysql、GBase等。 |
|  |  | 元数据授权及使用 | 对实体化的库表、字段等元数据授权给不同用户使用。 |
|  |  | 用户在数据加工配置过程中，只能配置经过授权表和字段的加工服务。 |
|  |  | 加工配置规则使用数据建模定义的元数据属性描述相应的表、字段及相关关系。 |

1. 共享交换代理

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 功能性要求 | 实现编办对接系统和共享交换平台之间的双向数据交换，提供从前置库中采集数据代理及从共享交换平台反馈数据并存储于前置库。 |
|  |  | 提供从前置库中自动识别并采集法人数据，进行封装及传输，支持多种传输模式，支持多线程、支持多表采集等代理所需要的运行环境，并提供代理监控与管理。 |
|  |  | 易用性 | 在同一个工具内，可视化实现数据节点的管理、数据服务的配置、服务目录管理、项目目录管理、运行及监控管理等。  节点管理，可视化创建节点运行环境、可视化查看部署在的节点上的资源，包括服务、流程、变量等。  提供详细的数据服务运行日志，便于用户跟踪数据加工过程、加工的数据记录数和插入、修改、删除的数据记录数等。  提供统一数据交换及整合服务，实现数据库、文件、XML、传输队列、适配器等之间的相互交换。该服务是可视化配置实现的，通过拖拉建立和异构系统的映射关系。 |
|  |  | 数据交换能力 | 支持数据库：Oracle、SQL Server、DB2、Sybase ASE、Sybase IQ、Informix、My SQL、FoxPro、Access等；国产数据库：达梦、人大金仓、神州通用数据库等。也支持SQL语句作为数据源。  支持文件：文本文件（分隔符、定长等）、Excel文件、DBF文件、MDB文件等。分隔符文件要支持组合分隔符。能可视化配置文件与异构系统的交换。  支持XML， XML可以是文件，也可以是来源消息队列、API、 Web URL等。能可视化配置XML与异构系统的交换。  提供内存对象映射满足API、传输队列数据抽取。  可视化定义内存表与异构系统的交换；可视化配置数据采集结果可输出到通道中，实现数据传输服务的绑定。  跨网段的数据交换能力。跨网段是指数据源和数据目标位于不同的网段，每个网段不能访问跨网段的数据库。能配置跨网段的数据交换服务；能实现跨网段的实时联动的数据交换；支持CLob字段、blob字段等；每个网段的工具都能监控数据交换情况。  支持对数据源实时、增量、批量、全量的交换策略，抽取条件可以是静态语句、动态SQL规则、来自变量、来自变量组等。支持变化数据捕捉增量抽取策略。 |
|  |  | 数据加工能力 | 提供多种数据转换方法，包括字符串转换、字段赋值、时间类转换、数据比对与翻译、数学运算、身份证格式转换等。  提供交换过程中的数据质量检查，根据数据逻辑判断规则，将干净的数据装载到目标中，将判断有问题的数据路由到数据库表或者数据文件中。 |
|  |  | 数据传输能力 | 实现异构、异地数据内容输出到通道、通道传输、接收方数据内容入库的一体化处理。通道支持加密、压缩、优先级、通道绑定处理、支持通道落地传输。整个过程可视化配置。  提供文件传输服务，用于保障数据文件传输的可靠性、可管理性、安全性。文件传输支持变化文件传输、文件夹传输、可定义传输数据块大小、传输线程并发数、可选择文件传输加密方法、压缩传输，支持同步、异步传输方式。整个文件传输配置在一个界面内可视化完成。  提供通用文件作为异构数据库的表（含有blob、clob、日期等字段格式）的传输存储。实现异构数据库表的数据经过加工等处理后生成通用数据文件，经过文件传输服务将文件传输到异地，接受方收到数据文件立即调用服务将数据文件内容交付到到异构数据库表中，整个过程是一体化联动处理的。通过可视化配置。  提供和外部FTP、SFTP的传输服务，满足和外部系统的文件传输需要。  FTP文件传输服务，包括文件的上传和下载，支持文件和文件夹传输，支持变化文件传输、删除已传输文件等处理。FTP的文件传输是可视化配置的  SFTP文件传输服务，包括文件的上传和下载，支持文件和文件夹传输。SFTP的文件传输是可视化配置的。 |
|  |  | 调度能力 | 提供跨网段的实时数据交换，提供跨节点、跨网段的服务联动调度策略满足同步、异步业务联动需要，至少服务代理、发送方及接收方前后处理、流程等服务联动调度策略是经过可视化配置完成的。  提供文件分类调用，对文件夹下的不同类型的文件设定不同的处理规则，调用不同类型的交换及加工服务，处理的文件名以变量方式传递给相应的交换及加工服务，便于变量的重用。  提供菜单生成器，方便用户通过菜单运行数据服务；提供定时调度（多样定时组合，时间间隔可以到秒），并能可视化配置；提供文件触发调度，监控给定文件夹，当满足监控条件的文件出现时触发。并能可视化配置。 |
|  |  | 集群及高可靠性 | 能可视化设定集群主从关系等，方便通过增加机器实现负载的扩展。  运行节点能调用位于不同机器上的交换及加工服务，并通过流程实现服务之间联动调度，支持并行调度。  支持软负载分配方式，将服务调用自动分配到负载比较小的机器上运行, 当一个节点出现故障时，不影响其他节点运行，接入的服务调用会被自动分配到没有故障的节点上运行。  能可视化部署服务，并能保证服务模型和规则自动同步。  ，能通过节点管理查看集群中每个节点部署的服务。  能可视化管理集群中每个节点的运行的服务，查看服务运行池，修改池大小、查看服务实例运行情况。 |

1. 应用服务代理

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | # | 总体要求 | 提供对外的数据接口代理服务，为上层应用提供相应的法人信息服务，为各部门的用户（或应用系统）与国家法人信息资源库之间建立统一的共享数据访问通道 |
|  |  | 支持规范和技术 | 产品支持JavaEE标准规范，包括JSP 2.1，JSF 1.2，JMS 1.1,JTA 1.0,JavaMail 1.3,JCA 1.5,Web Services for Java EE 1.2,JAX-WS 2.1,JAX-RPC 1.1,SAAJ 1.3,JMX 1.4,JACC 1.0 JDBC 3.0,JNDI 1.2,JAAS 1.0,JACC 1.0,WS-I Basic Profile 1.2,SAAJ 1.3,SOAP 1.1 and 1.2,JAXB 2.0等基本规范。 |
|  |  | 开发性要求 | 支持各种主流平台，如HP-UX、AIX、SOLARIS、WINDOWS （包括2003/XP/WIN7等）、Linux、UNIX等。 |
|  |  | 提供图形化的集成开发环境，支持交换集成组件和服务的图形化开发，支持可视化、可拖拽的流程编排方式，通过拖曳方式实现集成组件的连接。每个流程以适配器开始，然后采用过程化的流程编排方式进行流程编排，提供集成组件参数图形化配置。 |
|  | ★ | 支持与各种数据库的集成。包括：SQL Server 2000/2005/2008，Oracle 9i/10g/11g，MySql，Sybase DB2,Informix,金仓,达梦 7等； |
|  |  | 通过可视化开发环境直接生成XML Schema元数据信息，可自动从选定的数据库表、SQL语句、JSON消息、Class对象转换生成XSD数据模型。 |
|  | ★ | 提供Keytool安全证书GUI管理工具，Keytool类型支持JKS、JCEKS、UBER、PKCS#12、BKS等，可视化环境下生成密钥证书文件。 |
|  |  | 服务组件和各适配器均可进行可视化流程编排，根据实际集成业务需求快速调整并进行热部署生效。 |
|  |  | 支持流程调试debug，可开启调试模式，在流程图中某一节点设置多个断点进行调试，跟踪变量数据，分析问题。 |
|  |  | 支持多人协作开发，流程资源支持版本管理，可根据需要回退到历史版本，根据需要可锁定保留多个tag的历史版本 |
|  |  | 支持将服务器所有集成资源进行导入和导出的功能，可自定选择部分或者所有资源，方便在多个节点之间进行资源迁移，备份 |
|  | ★ | 功能性要求 | 支持多种文件的数据提取和装载，文本文件可以是定长文件，或以自定义的分隔符分割的文件；二进制文件；XML格式文件，支持标准的XML文件格式，Excel文件，EDI文件，H2010平文件。 |
|  |  | 提供可视化映射工具，可在多个变量之间进行拖拽完成变量的转换和映射，支持一对一、一对多、多对多、以及常量赋值等映射功能，也可以直接在连线逻辑中进行更复杂代码级转换处理。 |
|  | ★ | 提供对数据库轮询、查询、删除、更新等操作，数据库操作组件可以调用数据库的存储过程和函数的功能，提供数据库存储过程调用组件。 |
|  | ★ | 支持动态捕获数据库变化数据，可支持触发器、同步CDC、异步CDC、闪回等多种变化数据捕获技术满足增量数据获取的需求。 |
|  |  | 支持基于WebService实现信息共享、交换和流程处理、业务流转等功能和服务。提供服务发布向导快速发布服务；可直接将SQL语句以及数据库表操作发布为WEB服务；提供服务消费调用组件，动态调用已注册的服务或提供WSDL的外部服务。 |
|  |  | 提供HTTPS和HTT-Basic安全功能；提供基于WS-Security安全规范的服务鉴权功能，支持UserToken、时间戳、证书、签名等多种消息安全机制。 |
|  |  | 提供标准协议适配接入组件，快速集成三方应用系统。提供HTTP(S)、Socket(S)、SMTP、POP3、Web Service、JMS、AMQ、FTP、定时器、IBM MQ原生接口、MSMQ、AS2 等应用协议接入组件。 |
|  |  | 提供基于界面配置的可视化的路由表规则配置，提供路由规则组件，提供外部路由表适配组件。 |
|  |  | 产品内置应用服务器和消息中间件，可在ESB引擎服务端部署JavaWeb企业应用，也可以将其作为MQ消息代理进行P2P&Pub-Sub模式的消息传输 |
|  |  | 支持多个节点组网分布式部署，跨网络节点之间通过内置的消息中间件建立稳定可靠的传输链路，即使通信节点不在线，以及网络连接不稳定的情况下，也可保证消息不漏，不丢，不重。 |
|  |  | 基于EDA事件驱动架构，产品引擎支持事件扩展，用户可针对引擎内部产生的相关事件进行截取和识别，并进行相应的逻辑处理，以满足特定情况下的业务集成及监控管理需求。 |
|  |  | 流程支持多种启动方式，支持事件驱动启动以及调度任务启动；也可以将流程设置为随ESB服务器自动启动执行 |
|  |  | 管理性要求 | 统一监控平台提供完善的日志监控功能，对流程数据的传输进行统计分析；服务调用日志进行统计分析；文件传输日志统计；调度任务日志；平台用户操作日志；流程处理跟踪日志。 |
|  |  | 提供基于web的统一监控管理平台，对服务器所有资源进行监控管理。支持集中的流程监控和管理，包括节点监控、流程监控、日志管理等。其中流程管理，可以进行流程的部署、反部署，可以启动、停止流程，可以查询和统计流程的运行信息等。 |
|  |  | 支持在分布式环境内通过节点管理中心对多个服务器、用户信息进行统一管理，包括：远程状态监控；远程启动，停止，重启；远程配置修改、保存等。 |

1. 桥接服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  |  | 功能要求 | 实现数据加工处理逻辑从设计、开发、调试、部署，到运行、管理、监控各个生命周期不同阶段的集成开发平台,提供简单易用的开发部署工具，并能够对整个处理过程进行管理。 |
|  |  | 支持主流的操作系统平台，包括Sun Solaris，HP-UX, IBM AIX, Linux, Windows等，包括32位和64位，并且保证当操作系统扩展和升级时，原有应用能够平滑移植。 |
|  |  | 提供基于标准的JDBC、ODBC接口，实现对各种主流数据库系统的支持，如Oracle、DB2、SQL Server、MySQL、KingBase、HBase、DM等 |
|  |  | 提供丰富的数据抽取和加载组件，支持包括数据库、普通文本、CSV、XML、Excel等多种格式的文件。 |
|  |  | ETL工具需提供资源库，用于持久化存储流程配置信息、数据库信息、基础资源信息等，并可辅助团队协作开发。 |
|  |  | 提供可视化图形操作界面，支持中文界面，支持零编码配置，以实现处理流程的快速开发。 |
|  | ★ | 支持多种同步方式，如：全量同步、增量同步、数据比对同步、双向同步。 |
|  |  | 支持多种数据抽取模式，如闪回表、镜像表、时间戳、标志位、触发器、日志抽取等。 |
|  |  | 基于日志方式提供两种或两种以上抽取方式。 |
|  |  | 提供数据校验的功能，如空值检测、长度检查、数值范围检查、正则表达式校验等。 |
|  |  | 提供对消息传输协议的支持，支持JMS协议，支持主流消息中间件如：Apusic MQ、IBM MQ、MSMQ。 |
|  |  | 提供了调试预览功能，可进行数据行级别的调试和预览，跟踪和观察每一行数据经过流程中每一个转化组件进行加工处理的结果 |
|  | ★ | 支持ETL集群，提供动态集群和静态集群模式 |
|  |  | 在ETL处理过程中支持数据等待、数据阻塞，并可根据阻塞情况执行后续的异常处理。 |
|  | ★ | 管理要求 | 提供异常处理机制，提供监控管理机制，保证异常信息、运行日志、交换统计和资源库无缝衔接，无需单独管理，并持久在数据库中。 |
|  |  | 提供C/S监控管理功能，能够对数据处理状态进行实时监控，粒度至每个组件处理的记录数和异常数，并且可以评估单个组件处理数据的性能指标和整个处理流程的性能指标。 |
|  | ★ | 提供B/S管理控制台，可对资源库、服务器进行统一管理。提供部署、监控、统计等功能。 |
|  | ★ | B/S管理控制台具备完整的日志管理功能、完善的数据审计功能。并且有相关的监控预警机制，保证ETL正常进行，不影响数据源系统的正常工作。 |

1. 消息中间件

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  |  | 开发能力与技术规范 | 符合JMS 1.1及JNDI规范 |
|  |  | 底层核心模块采用JAVA语言开发，具备良好的跨平台性 |
|  |  | 支持多种消息协议，提供灵活的底层通讯方式，包括AMQP、MQTT（物联网传输）、OpenWire、REST、Stomp |
|  |  | 支持TCP、UDP网络协议。 |
|  |  | 支持多种开发工具和编程接口，特别是流行的开发工具。如C。C/C++、.NET、Perl、php、python、Ruby等。实现对这些工具的灵活接口 |
|  |  | 支持多种类型消息，字节消息、文本消息、流消息、Map消息、文件消息、对象消息等。 |
|  |  | 支持事务管理，提供本地事务支持和分布式事务支持。 |
|  |  | 支持消息传输时的断点续传。 |
|  | ★ | 通过JCA 1.5 resourceadaptors的配置 |
|  |  | 支持多种类型的消息持久模式：如文件、日志文件、KV数据库、内存数据库、关系数据库等。 |
|  | ★ | 提供对Spring的支持,可以很容易内嵌到使用Spring的系统里面去,同时支持Spring2.0特性。 |
|  |  | 支持集群技术 | 支持集群，能够承受大并发，避免单点故障，提供7\*24小时不间断服务。 |
|  |  | 支持集群环境中的消息智能分发技术（抗抢夺算法）。 |
|  |  | 支持工作负载均衡和通信故障切换功能。 |
|  |  | 支持集群的监控管理，提供集群派发策略配置。 |
|  |  | 提供集群与队列数据复制技术，并说明实现机制 |
|  |  | 支持大消息 | 提供对大消息及大文件（大于4G）的可靠传输。 |
|  |  | 支持上传和下载过程中的断点续传。 |
|  |  | 提供独立的文件传输通道，提升文件传输效率，并阐述实现机制。 |
|  |  | 支持实时监控平均速率， 最大速率，进度， 并且可以设置最大传输速率。 |
|  |  | 安全性 | 支持消息队列和主题的权限控制，可设定用户或组对队列或主题进行的各种操作权限。 |
|  |  | 支持客户端与服务器间、服务器与服务器间的SSL安全通道加密，支持额外的口令短语安全保护。 |
|  |  | 支持消息传输过程中消息体加密，并支持通过用户的加密库或算法进行加密。 |
|  |  | 管理和监控 | 提供图形化的节点网络监控工具，监控节点的运行情况 |
|  |  | 支持可分级，可配置的日志功能 |
|  |  | 支持远程图形化的参数配置功能，支持第三方工具接入。 |
|  |  | 支持用户设置消息优先级，并支持消费者独占，保障队列级优先传输，同时严格保障消息顺序。 |
|  |  | 支持与其他消息中间件桥接工具包。 |

1. 应用服务器中间件

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  |  | 开发与管理 | 符合JAVAEE 5.0规范，通过JAVAEE 5.0认证，在SUN公司的官方网站的认证通过列表上能够查询到。全面支持JAVAEE 6.0规范。 |
|  |  | 支持主流硬件平台，列出所支持的硬件平台。 |
|  |  | 支持多种数据库，如Oracle、MS SQL Server、DB2、Informix、Sybase、达梦、金仓等 |
|  |  | 支持Linux、UNIX、Windows等平台的最新发行版本,并对国产操作系统如中标、红旗等有良好的支持。 |
|  | ★ | 提供基于B/S结构的管理控制台，同时管理控制台需包含面向集群节点、应用、数据源等集群环境的统一配置与管理功能。 |
|  | # | 内置原生的负载均衡器（非Apache等第三方WebServer）。 |
|  | # | 支持客户端缓存（CSC）技术。详细说明如何实现。 |
|  | ★ | 支持部署Web Service；支持WS-Security、SOAP 1.2、WSDL 1.1、JAX-RPC 1.0、UDDI 2.0等技术标准。支持Java EE7.0 web Socket功能。 |
|  |  | 支持热部署、远程部署等多种部署方式。 |
|  | ★ | 支持多种安全加密算法，支持SM2国密算法。同时实现用户的密码满足规定的质量量度（如长度、复杂度、有效期、重复次数等参数）。 |
|  | # | 可提供密级功能，密级标识应不得篡改。 |
|  | # | 提供审计功能，实现对用户在系统的事件进行记录和存储，能够进行查询，能够对审计进行响应。审计记录内容包括：事件发生的时间、地点、类型、主体、客体和结果。 |

1. 核心交换机

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 性能要求 | 背板带宽≥19Tbps，包转发速率≥2880Mpps； |
|  | ★ | 硬件指标 | 整机主控引擎插槽≥2个，业务插槽≥6个； |
|  | ★ | 实际配置 | 配置双引擎、双电源、配置借口：≥48个万兆以太网光端口，实配同品牌万兆多模模块≥24个； |
|  | ★ | IPv4路由功能 | 支持静态路由/支持RIPv1/v2/支持OSPFv2/支持IS-IS/支持BGPv4/支持OSPF/IS-IS/BGP GR/支持等价路由/支持策略路由/支持路由策略 |
|  | ★ | IPv6路由功能 | 支持OSPFv3/支持RIPng/支持BGP4+/支持IS-ISv6/支持手工隧道/支持ISATAP/支持6to4隧道/支持IPv6和IPv4双栈 |
|  | # | ERPS | 链路收敛时间≤50ms |
|  |  | 链路聚合 | 最多可支持8个端口聚合；最多可支持64个聚合组；支持LACP； |
|  | # | QOS | 支持基于第二层、第三层和第四层的ACL；整机提供ACl条目数不小于1K条；支持基于端口和VLAN的 ACL；支持IPv6 ACL；支持出方向ACL，以便于灵活实现数据包过滤；支持802.1x认证，支持集中式MAC地址认证 |
|  | # | 镜像 | 支持本地端口镜像和远程端口镜像RSPAN； 支持流镜像，同时支持N：M的端口镜像（M大于1）； |
|  |  | MPLS | 支持L3 MPLS VPN/支持L2 VPN: VLL (Martini, Kompella)/支持MCE/支持MPLS OAM/支持VPLS,VLL/支持分层VPLS，以及QinQ+VPLS接入/支持P/PE功能/支持LDP协议 |
|  |  | 虚拟化 | 支持N:1多虚一虚拟化；支持跨设备链路聚合，单一IP管理，分布式弹性路由；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；支持远程堆叠； |
|  |  | 可靠性 | 支持热补丁功能，可在线进行补丁升级；支持快速环网保护协议，环网故障恢复时间不超过50ms；支持MSTP功能：收敛时间≤50ms；支持PVST功能：收敛时间≤50ms |
|  | # | SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换，支持多控制器（EQUAL模式、主备模式）, 支持VXLAN 二层交换,支持VXLAN 路由交换,支持VXLAN 网关； |
|  | ★ | 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2，支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准 |
|  | ★ | 资质 | 要求提供工信部电信设备进网许可证 |

1. 汇聚交换机

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 性能要求 | 背板带宽≥1Tbps，包转发速率≥960Mpps； |
|  | ★ | 实际配置 | 固化≥48个1G/10G SFP+接口，≥4个QSFP+接口；实配模块化1+1冗余风扇，双交流电源；≥24个10E SFP+万兆光模块； |
|  | ★ | 电源风扇 | 支持模块化电源冗余，模块化风扇冗余、前后风道、风道可调，支持热插拔； |
|  | ★ | 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP；支持IPv6静态路由、RIPng、OSPFv3、BGP4+；支持IPv4和IPv6环境下的策略路由；支持IPv6手动隧道、6to4隧道和ISATAP隧道； |
|  |  | 组播 | 支持IGMP v1/v2/v3，MLD v1/v2；支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；支持PIM Snooping；支持MLD Proxy；支持组播VLAN；支持PIM-DM，PIM-SM，PIM-SSM；支持MSDP，MSDP for IPv6；支持MBGP，MBGP for Ipv6； |
|  |  | 镜像 | 支持本地端口镜像和远程端口镜像RSPAN；支持流镜像；同时支持N：M的端口镜像（M大于1） |
|  |  | 虚拟化 | 支持N:1多虚一虚拟化；支持跨设备链路聚合，单一IP管理，分布式弹性路由；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；支持远程堆叠； |
|  | # | SDN | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换 |
|  |  | 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)；支持快速环网保护协议，环网故障恢复时间不超过200ms； |
|  |  | 管理维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准 |
|  | ★ | 资质 | 要求提供工信部电信设备进网许可证 |

1. 接入交换机

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 性能要求 | 交换容量≥590Gbps，包转发速率≥250Mpps； |
|  | ★ | 实际配置 | 固化≥48个10/100/1000Mbps电接口，≥4个SFP+光接口；支持万兆光口≥12个，实配2个万兆SFP+模块；支持扩展插槽≥1；实配模块化双风扇、双电源； |
|  | ★ | 电源风扇 | 支持模块化电源冗余，模块化风扇冗余、前后风道、风道可调； |
|  | # | 表项要求 | MAC地址表≥64K；路由表容量≥32K；ARP≥32K； |
|  | # | 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP；支持IPv6静态路由、RIPng、OSPFv3、BGP4+；支持IPv4和IPv6环境下的策略路由；支持IPv6手动隧道、6to4隧道和ISATAP隧道； |
|  | # | 组播 | 支持IGMP v1/v2/v3，MLD v1/v2；支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；支持PIM Snooping；支持MLD Proxy；支持组播VLAN；支持PIM-DM，PIM-SM，PIM-SSM；支持MSDP，MSDP for IPv6；支持MBGP，MBGP for Ipv6； |
|  |  | 镜像 | 支持本地端口镜像和远程端口镜像RSPAN；支持流镜像；同时支持N：M的端口镜像（M大于1）； |
|  | # | 业务扩展 | 支持多业务插卡，内置软AC功能 |
|  |  | 虚拟化 | 支持N:1多虚一虚拟化；支持跨设备链路聚合，单一IP管理，分布式弹性路由；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预；支持远程堆叠； |
|  |  | SDN | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换 |
|  |  | 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)；支持快速环网保护协议，环网故障恢复时间不超过200ms； |
|  |  | 管理维护 | 支持SNMP V1/V2/V3、RMON、SSHV2；支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准 |
|  | ★ | 资质 | 要求提供工信部电信设备进网许可证 |

1. **IDS**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | ≤2U机箱，冗余电源，液晶屏，6个10/100/1000M自适应电口（其中1个管理口、5个业务接口）；，1个空扩展槽 |
|  | ★ | 性能要求 | 吞吐量≥4Gbps |
|  |  | 部署方式 | 支持旁路监听的工作模式，具备IPv4与IPv6双协议栈入侵检测能力 |
|  | ★ | 入侵检测能力 | 支持融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2至7层深度入侵检测 |
|  |  | 系统应提供覆盖广泛的攻击特征库，能够针对7000种以上的攻击行为、异常事件，以及网络资源滥用流量进行检测 |
|  | ★ | 支持入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测规则 |
|  |  | 支持基于网络、用户、应用的安全检查模式 |
|  |  | 支持对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解、非授权访问、缓冲区溢出、SQL注入、跨站脚本、网页挂马、DoS/DDoS攻击等恶意流量的检测 |
|  | # | 应用识别 | 采用关联分析技术实现准确的攻击及应用威胁识别 |
|  | # | 支持基于安卓开发的多种社交软件和应用，如，微信、飞信、新浪微博、网易新闻、百度新闻等 |
|  |  | 安全可视 | 设备自带液晶屏，不用登陆设备可实现对设备状态的查看 |
|  | **★** | 设备可以图形化展示应用风险指数、网络风险指数便于用户整体了解网络风险等级 |
|  | # | 产品可以图形化显示设备接口面板信息，直观查看接口是否联线 |
|  |  | 特征库 | 内置IDS、AV、应用特征库， |
|  |  | 安全审计 | 支持将攻击流量通过镜像口镜像出去，供第三方设备存储、分析、审计等 |
|  |  | 支持将日志存储在本地，标配大于500G日志存储硬盘。 |
|  |  | 系统管理 | 提供管理友好的中文Web图形界面配置，支持Telnet、SSH、串口登陆命令行模式配置。 |
|  |  | 支持通过web方式调用设备命令行窗口功能，无需登录串口就可对设备进行命令行操作。 |
|  | # | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **漏洞扫描系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  |  | 硬件要求 | 机架式硬件设备，系统硬件采用全内置封闭式结构，产品稳定可靠性高 |
|  | ★ | 至少具备6个10/100/1000自适应电口，支持1个扩展插槽；设备采用单电源，配置有USB、console接口；硬件为双存储结构，软件系统与日志采用独立存储，硬盘只用来存储日志，硬盘容量≥500GB |
|  | ★ | 支持液晶面板实时显示，包含IP地址、登陆用户、CPU、内存等详细信息 |
|  | ★ | 性能指标 | 系统扫描IP地址无限制，支持扫描A类、B类、C类地址，系统扫描支持100个IP地址并行扫描；Web扫描域名无限制，Web扫描任务并发数为15个域名 |
|  |  | 部署方式 | 产品支持旁路部署方式，具备IPv4与IPv6双协议栈漏洞扫描能力 |
|  |  | 产品应支持多路并行扫描机制，可以同时对多个隔离网络进行漏洞扫描 |
|  | # | 产品分布式部署需支持自定义管理中心端口号、策略端口号、远端扫描引擎名称等信息 |
|  | # | 管理员只支持本地和证书两种， AD/LDAP/Radius以及短信认证。 |
|  | # | 产品分布式部署提供远端扫描引擎列表，列表需对设备状态、策略同步、规则同步、引擎类型等状态提供最直观的展示效果 |
|  | **★** | 资产管理 | 产品具备以树形结构方式管理，针对树形结构的资产呈现资质风险 |
|  |  | 产品应支持对扫描耗时、起始时间、结束时间、扫描进度、发现漏洞数、检测网页数等多种在线扫描数据呈现 |
|  |  | 产品需支持监控系统，提供对系统、流量、主机、接口、连接、屏蔽等至少6种状态监控功能 |
|  | # | 产品应支持多种不同的方式自动发现网络资产。可以灵活配置资产发现所用技术手段，提供至少4种技术手段 |
|  |  | 产品应支持可按时、按日、按周、按月定制扫描计划，到时间自动进行扫描，支持后台自动运行 |
|  | ★ | 系统扫描 | 产品应具备操作系统、数据库、网络设备等主流系统的漏洞库列表，并提供至少15种以上的漏洞库分类 |
|  | # | 产品漏洞库列表数量须大于15000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准兼容 |
|  |  | 产品需至少提供3个威胁情报中心联动的接口配置功能，同时收集多家数据情报供设备使用 |
|  | # | 产品应支持主流虚拟机管理系统的漏洞检查，支持Vmware ESX\Vmware ESXi等相关漏洞 |
|  | # | 产品应支持DNS服务的安全漏洞检查，包括DNS缓存中毒、DNS拒绝服务漏洞、签名欺骗等至少100种以上的相关漏洞库 |
|  | # | 产品应支持通过WI-FI网关对移动设备系统进行漏洞检查，需支持对iOS、Android、Blackberry、windowsphone等操作系统，并提供至少50种以上的相关漏洞库 |
|  | # | 产品应支持后门检测的安全漏洞检查，包括对Microsoft IIS特洛伊木马检测、Mac OS X恶意程序等常见后门漏洞的安全检测，并提供至少100中以上的相关漏洞库 |
|  |  | 产品需支持屏蔽分析，提供IP地址、屏蔽时间、屏蔽原因等数据分析，并提供12种屏蔽原因独立分析查询功能 |
|  | # | 产品应支持对常见P2P软件的安全漏洞检测，包含对常见的电驴、iTunes、BitTorrent等软件的安全检测，并提供至少50种以上的相关漏洞库 |
|  | # | Web安全 | 产品应具备专用的Web漏洞库，具备SQL注入、跨站脚本、信息泄露等常见Web漏洞的漏洞库列表，并提供至少9种的漏洞库分类 |
|  | # | 产品应支持对Web网站漏洞扫描的同时，查看网站漏洞情况和Web目录结构，数据进行实时同步呈现 |
|  | # | 口令破解 | 产品应具备专用的口令破解字典，包括密码字典、用户名字典、组合字典等多种口令破解字典 |
|  | # | 口令破解利用SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测 |
|  |  | 配置核查 | 产品应具备专业配置核查的漏洞库，具备主流的操作系统、数据库、网络设备、安全设备的相关安全配置核查漏洞库 |
|  | # | 产品应具备操作系统的配置核查，能够对主流操作系统进行安全配置进行检查，支持windows、linux、unix等主流操作系统 |
|  | # | 产品应具备网络设备的配置核查，能够对主流网络设备进行安全配置进行检查，支持Cisco、华为、Juniper、F5等主流网络设备 |
|  | # | 产品应具备安全设备的配置核查，能够对主流安全设备进行安全配置进行检查，支持Cisco、华为、赛门铁克、Juniper、McAfee等主流安全设备 |
|  |  | 报表分析 | 产品应具备在线查询功能，可以根据漏洞严重级别进行区别展示，并以颜色对漏洞级别进行区分 |
|  |  | 可对日志的关键字段进行追加搜索，从上一次的搜索结果中重新按照新的规则搜索日志。 |
|  | ★ | 产品应具备以漏洞为中心为查询对象，查询存在漏洞的相关资产，并可以查询深入的详细漏洞明细 |
|  | # | 产品应具备漏洞对比机制，针对多次漏洞扫描情况进行对比，了解新增漏洞、减少漏洞的详细数据 |
|  |  | 产品应具备漏洞报表导出机制，支持word、html、execl等导出格式，并支持导出统计报表和详细报表 |
|  |  | 统计分析 | 产品需支持攻击主机统计分析，提供攻击源、被攻击主机、被攻击端口、起始时间、结束时间、持续时间、攻击类型、攻击状态、最大流量等至少9种攻击主机统计数据 |
|  |  | 升级与备份 | 产品应具备漏洞升级服务，支持手动、自动升级方式 |
|  | # | 产品需支持微软WSUS升级机制，提供微软WSUS账号、密码、地址、端口号的相关设置，并通过HTTPS进行链接 |
|  |  | 告警与验证 | 产品应具备告警支持，支持邮件、短信、SNMP、Syslog、FTP、日志存储阈值等多种告警机制 |
|  | # | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **网络安全审计系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | 机架式硬件设备，至少具备6个千兆电口，1个扩展槽，1T硬盘，单交流电源。 |
|  | ★ | 性能要求 | 适用700M带宽场景  并发连接数≥200万  新建连接速率≥5万/秒 |
|  | # | 部署方式 | 支持串接与旁路部署方式，具备IPv4与IPv6双协议栈安全审计能力 |
|  | ★ | IPv6支持 | 能够支持IPv6环境下的网址访问审计、生成分析报表等功能；能够在IPv6环境下，正确审计显示用户的IPv6地址 |
|  |  | 账号安全 | 支持管理员账号初始密码检测 |
|  |  | 角色管理 | 支持将设备管理权限分割为管理员、审计员与审核员共同管理设备：管理员能够设置策略，无法查看审计日志；审核员能够审核管理员配置的策略是否合法；审计员能够查看策略，无法设置策略； |
|  |  | 审计日志 | 日志中心支持选择企业级Oracle数据库，访问日志中心数据采用https加密方式访问，避免传输过程被窃取。 |
|  |  | 用户识别 | 支持对802.1X、Kerberos、LDAP、POP3、SMTP、Radius、PORTAL、PPPOE、城市热点等系统的单点登录。 |
|  |  | 安全监控 | 支持统计显示安全防护功能所保护的终端数量，支持统计显示病毒查杀数量，支持统计显示检测/拦截的恶意URL访问次数，支持统计显示检测到的失陷主机数量，支持显示最近10次安全事件记录。 |
|  | ★ | 失陷检测 | 支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志；支持拦截对外部威胁IP的访问请求和阻塞失陷主机IP两种控制策略。 |
|  | ★ | 审计管理 | 支持对微信PC版进行行为和聊天内容审计，支持记录发送/接受信息的微信账号，支持记录与单人/群聊/公众号的发送/接收内容 |
|  |  | 病毒云查 | 支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗；支持病毒查杀日志查询 |
|  | # | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **数据库审计系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | 采用独立的标准机架式硬件架构，软硬件一体化系统，全操作系统，内嵌数据库，用户无需另外安装操作系统及数据库管理系统。 |
|  | ★ | 接口配置6个千兆电口，总容量6T，配置RAID5方案，硬盘有效存储>=4TB，内存>=32GB ，双电源，可支持3个扩展插槽。 |
|  | ★ | 性能要求 | 性能指标：峰值事件处理能力不低于30000条语句/秒，日志存储最低25亿条。 |
|  | # | 部署方式 | 支持串接与旁路部署方式，具备IPv4与IPv6双协议栈的数据库审计能力 |
|  | # | 工作模式 | 支持分布式部署方式，并支持数据库审计集中管理功能，可快速查看所有审计系统的状态、风险状态等，方便区域性管理及防护策略的落实 |
|  |  | 支持AA，AP工作模式，IP地址可在设备间漂移，根据设备状态将流量牵引到主设备。支持包括半连接，全连接会话信息全状态同步；支持会话保持信息同步；以保障业务不间断切换。 |
|  | # | 数据库审计能力 | 全面支持后关系型数据库Cache的集成工具Terminal、Portal、Studio、Sqlmanager、MedTrak工具的审计，其中Portal能审计到Sql语句、查询Global、返回结果，Terminal能审计到M语句和返回结果 |
|  | # | 在无需重启被审计数据库的情况下，支持对MS SQLSserver 加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息 |
|  | # | 应用关联审计 | 支持B/S、C/S应用系统三层架构http应用审计，可提取包括应用系统的人员工号（账号）在内的“六元组”身份信息，精确定位到人，并可获取XML返回结果。 |
|  | # | 通过应用层代理，可解析客户端请求内容，并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。例如对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于Cookie、User-Agent、URL、HTTP头的分担模式 |
|  | ★ | 审计策略支持 | 审计策略支持18种以上分项响应条件，可支持数据库操作命令（包括select、create等14个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、进程名、会话ID、关键字、时间（含开始结束日期）等 |
|  | # | 支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警 |
|  | # | 支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警 |
|  |  | 支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 |
|  | ★ | 事件查询统计 | 告警检索效率高达亿条数据分钟级，搜索条件支持全范围搜索（特别要求在超过亿条数据量时），一次性完成搜索的响应时间在分钟级别 |
|  | # | 配置管理 | 翻译功能：实现对SQL语句转换成中文自然语言的描述功能，便于非技术人员理解报警内容 |
|  |  | 数据管理 | 提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式； |
|  | # | 支持管控逻辑内外隔离，通过内外网策略联动完成配置。不允许仅从内网端完全管理网闸，避免黑客从一端攻破网闸获取完整控制权限。 |
|  | ★ | 审计结果隐秘设置，通过\*号对审计结果中的重要信息进行隐秘处理，防止二次泄密 |
|  | # | 攻击检测能力 | 支持对SQL注入、跨站脚本攻击等web攻击的识别与告警 |
|  |  | 系统本身具备能发现未知仿冒进程工具、防范非法IP地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）、设置系统黑白名单等安全功能 |
|  | ★ | 数据库监控 | 支持对MySQL、Oracle、sqlserver、mongodb、redis数据库的状态监控，主动发现数据库潜在风险 |
|  | ★ | 提供基于环境动态，整体地洞悉安全风险，以数据为基础，从全局视角提升对安全威胁的发现识别、理解分析的数据库态势感知，及时发现各种异常和危险操作 |
|  |  | 第三方接口功能 | 支持Syslog和SNMP Trap方式向外发送审计日志 |
|  |  | 提供接口可实现与网络设备的联动 |
|  |  | 能够与终端管理软件联动，设备检测到未安装终端管理软件的PC，可将其Web访问自动重定向到特定页面并提示下载； |
|  |  | 支持与FTP服务器对接（备份与还原） |
|  | ★ | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **防火墙**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | 多核并行处理架构，≤2U机架式硬件设备，冗余电源，标准配置6个10/100/1000M自适应电口，4个SFP插槽，支持两个扩展槽，支持22个接口；1个Console口，支持液晶屏 |
|  | ★ | 性能要求 | 网络处理能力为40G，并发连接≥460万，每秒新建连接15万/秒 |
|  | # | 部署方式 | 支持路由、透明、混合等部署方式，具备IPv4与IPv6双协议栈转发能力 |
|  |  | 基础组网 | 可对源地址为IPv4地址、目的地址为IPv4地址的会话执行目的地址转换，将IPv4地址转换为服务器地址，并支持服务器地址探测 |
|  | ★ | 能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。 |
|  |  | 支持入站的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果 |
|  |  | 支持出站的DNS代理功能，支持在不更改内网终端设备DNS服务器地址设置的情况下，将DNS解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果 |
|  |  | 支持在IPv6环境下配置安全策略、SSL解密策略等规则，实现漏洞防护、间谍软件防护、URL过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理 |
|  | ★ | 可对文件传输协议进行还原和分析，可分析的协议至少包含如下：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB。 |
|  |  | 支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计； |
|  |  | 访问控制 | 支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制。要求设备可基于地理区域配置安全策略，并支持地理区域对象的导入。 |
|  |  | 流量日志记录至少包含以下字段：时间、IP、IP地理位置、端口、域名、HTTP头信息、SQL语句、邮件收件人和发件人、文件名、文件MD5、应用层payload前100字节。 |
|  | ★ | IP/MAC绑定 | 支持二层MAC地址IP地址绑定；支持跨三层MAC地址IP地址绑定 |
|  |  | 攻击防护 | 支持防御IP地址欺骗，可将IP与安全域关联，即指定IP或网段从特定安全域流量流入，否则视为IP地址欺骗 |
|  |  | 产品需支持TCP DDoS防护策略，应具备端口扫描、SYN flood、Conn Flood、ACK flood、序号攻击、慢攻击等常见TCP DDoS攻击防御能力 |
|  |  | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |
|  | # | 支持本地病毒查杀 |
|  | ★ | SSL 解密 | 支持IPv4和IPv6流量的HTTPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，并可同时基于安全域、IPv4和IPv6地址进行例外设置 |
|  | ★ | 安全管理 | 支持统计网络中确认失陷的主机及有风险但不能完全确认为失陷的主机数量及风险等级状态，并支持查看失陷时间、威胁类别、情报来源、威胁简介、失陷主机IP、用户名、资产等信息，并支持一键跳转处置。 |
|  | # | 基于情报检测的实时主机检测及告警 |
|  |  | 支持统计网络内威胁事件的数量及风险等级状态，并支持一键跳转查看威胁详情和处置详情。 |
|  | ★ | 所投设备需提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取 |
|  |  | 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
|  | ★ | 可提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示 |
|  |  | 可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤等安全功能选项 |
|  | # | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |
|  | # | 要求提供IPV6 Ready认证资质 |

1. **网络病毒防火墙**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | 多核AMP+架构，≤2U机架式硬件设备，冗余电源，至少配置6个10/100/1000M自适应电口，2个SFP插槽，支持1个扩展槽，1个Console口，支持液晶屏； |
|  | ★ | 性能要求 | 网络处理能力≥20G，并发连接数标配≥500万，每秒新建连接≥25万/秒， |
|  | # | 部署方式 | 支持路由、透明、混合等部署方式，具备IPv4与IPv6双协议栈转发能力 |
|  |  | 访问控制 | 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查 |
|  |  | 应用过滤 | 支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输方式等特征分类 |
|  |  | URL过滤 | 支持用户自定义重点URL分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为 |
|  |  | 邮件过滤 | 所投产品必须支持基于关键字的接收、发送或双向Email发件人、收件人过滤，并支持自定义RLB服务器地址配置，并可结合IP黑名单或白名单 |
|  | # | 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |
|  |  | 所投产品必须支持对最多6级的压缩文件进行解压查杀 |
|  | ★ | 支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
|  |  | 入侵防护 | 支持漏洞防护，特征库包含 “永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应攻击名称、CVEID、CNNVDID、严重性、影响平台、类型、描述等详细信息； |
|  | ★ | 异常感知 | 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断 |
|  |  | 支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看威胁详情和处置详情；支持基于受害主机、威胁情报一键跳转威胁活动统计分析 |
|  |  | 安全分析 | 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
|  |  | 支持关联威胁事件日志，自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块关联检查日志集中显示 |
|  | # | 策略处置 | 支持接收针对突发重大安全事件“应急响应消息”，显示安全事件名称、类型、防护状态、处置状态、相应操作等信息；根据设备安全配置变化动态显示应急响应处理结果 |
|  |  | 支持针对“应急响应消息”的手动或自动处置，处置方法包括基于漏洞的处置和基于威胁情报的处置 |
|  |  | 协同联动 | 支持与云端联动，实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能 |
|  | ★ | 产品资质 | 计算机信息系统安全专用产品销售许可证 |

1. **堡垒主机**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | 采用专用千兆多核硬件平台和安全操作系统，≤2U机架式硬件设备，支持6个千兆电口和4个千兆光口，支持2个接口扩展槽位，内置4TB硬盘，冗余电源，支持液晶屏 |
|  | ★ | 性能参数 | 支持300路图形会话或800路字符会话并发。 |
|  | # | 部署方式 | 支持旁路部署方式，支持IPv4与IPv6双协议栈 |
|  |  | 支持协议类型 | 支持常用协议：SSH、Telnet、RDP、VNC、FTP、SFTP |
|  |  | 支持应用发布协议扩展，如支持web应用、Oracle/MSSQL/Mysql/DB2等数据库客户端、vSphere Client/用户等第三方C/S客户端 |
|  | ★ | 策略 | 访问控制策略基于用户、用户组、资源账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP剪切板控制、时间限制、IP限制进行设置 |
|  | ★ | 访问控制策略支持配置双人授权候选人，针对核心设备，需要管理员现场审批才能操作 |
|  | # | 运维安全分析 | 支持用户构成（饼图）分析，可按活动用户、锁定用户、30天未登录用户等进行展示，分析是否存在僵尸账号、闲置账号 |
|  |  | 对于重要的未知威胁告警，将告知客户攻击的相关背景信息（包括攻击行业，受害范围）。 |
|  | # | 支持用户、资源活跃度排行（Top10）及用户和资源的授权关系（网状图）分析，分析用户是否存在越权访问 |
|  | # | 支持资源使用状态（柱形图）分析，分析是否存在闲置、故障资源 |
|  | # | 支持资源访问趋势（折线图）分析，分析访问是否存在异常 |
|  |  | 资源管理功能 | 支持组织架构管理，对资源按科室、部门等进行独立管理、独立授权 |
|  |  | 支持自动学习功能，能自动收集资源IP、设备类型、运维协议、端口号等并自动保存至堡垒机 |
|  | # | 支持对云主机导入、管理、监控（CPU、内存等）和启停等操作，包括但不限于阿里云、腾讯云、华为云等 |
|  | **★** | 支持文件管理权限、RDP剪切板权限、上传、下载权限的申请 |
|  |  | 身份认证 | 支持本地认证、USBKey、短信认证、数据库认证、邮箱认证、证书认证、动态口令认证、LDAP认证、windows AD认证、RADIUS认证，并且支持支持本地用户名密码、证书认证、第三方证书、LDAP、短信验证码、邮箱验证码。可实现USBKey认证、LDAP认证、硬件特征码等多种因子绑定认证。 |
|  |  | 支持静态密码、RADIUS、LDAP、AD域等认证方式，支持AD/LDAP用户同步 |
|  | # | 内嵌Google令牌认证引擎，支持手机APP扫描二维码绑定用户 |
|  |  | 监控及回放 | 支持SSH、Telnet、RDP、VNC、FTP、SFTP、web应用、数据库等全协议的监控及回放，支持倍速播放、拖放、空闲过滤等播放设置 |
|  | # | 支持对用户运维会话实时统计功能，可实时监控运维屏幕、手动阻断会话、查看执行的命令及操作日志回放 |
|  | # | 支持对RDP屏幕文字内容、标题窗口、键盘输入、鼠标单/双击的记录检索和定位回放，定位回放无延迟 |
|  | # | 系统管理功能 | 支持第三方平台API接口，可对堡垒机用户、资产、策略及授权数据进行增删改查，允许第三方平台自动将用户、资产、策略及授权等数据同步至堡垒机 |
|  | # | 多级管理 | 支持多级管理，能对同一单位、分散在不同省市的堡垒机统上的用户、资产、授权、审计等数据分上下级集中管理，统一下发升级策略 |
|  |  | 支持android和ioS系统终端VPN接入 |
|  | # | 支持对下级设备日志集中管理和存储 |
|  |  | 数据库安全 | 支持一键查询威胁事件详情，威胁事件详情需要包括告警来源、威胁类型、威胁名称、威胁情报IOC、已经相关的会话记录。 |
|  | # | 支持基于用户、指令、数据库等组合设定访问控制策略 |
|  | # | 支持联动数据库审计设备，拦截指定用户的运维会话，防止对数据库的篡改、删除等危险操作 |
|  | ★ | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **防病毒软件系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 基本要求 | 提供客户端杀毒、补丁分发管理功能，与主机安全审计系统为统一的管理平台，客户端授权数50点 |
|  | ★ | 客户端支持要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012；中标麒麟/Deepin/SUSE Linux/Red Hat Linux |
|  | ★ | 病毒防护 | 支持文件与目录自定义黑白名单的方式来管理全网终端的文件；文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件； |
|  | # | 支持病毒查杀统计：通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件； |
|  |  | 要求产品具备本地多引擎查杀能力，且引擎可配置； |
|  | ★ | 支持linux、国产操作系统杀毒、云桌面（至少两家）产品 |
|  |  | 要求产品具备公有云检测能力，并且公有云特征储备超过100亿； |
|  |  | 支持私有云查杀，预置至少2亿黑名单及2000万全面的白名单，终端威胁统一到控制中心查询黑白并进行查杀。 |
|  | # | 要求产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力 |
|  | ★ | 要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽 |
|  | ★ | 补丁管理 | 终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁 |
|  | ★ | 产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能 |
|  |  | 产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源 |
|  |  | 资产管理 | 支持自动发现设备的IP-MAC地址的绑定 |
|  |  | 支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件 |
|  |  | 支持正版软件的正版序列号的读取功能，确保软件正版化。 |
|  |  | 日志报表 | 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表； 展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况 |
|  | ★ | 设备联动 | 支持与本项目中防火墙产品联动，达到网关终端边界联动防御效果 |
|  | ★ | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **数据库加密系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件要求 | 国产品牌，非OEM产品；≤2U标准机架式硬件设备、冗余交流电源、≥4个10/100/1000M自适应电口、1个HA接口、1个控制口，≥8G内存，≥1TB存储介质 |
|  |  | 性能要求 | 并发连接数≥500，吞吐量≥1000M |
|  | ★ | 数据库兼容性 | 能够支持对达梦等国产数据库、 Oracle等国外数据库系统的加解密 |
|  | # | 服务发现 | 支持服务扫描和发现功能，可自动发现cache、DB2、GBASE、postgresql、teradata等超过10种数据库 |
|  |  | 支持按服务类型进行统计，并以各类图表的形式展示，可生成报表并导出。 |
|  | # | 敏感数据数据发现 | 支持对数据扫描功能，实现对数据库的表、字段等敏感信息的自动识别，可支持姓名、邮箱、电话、身份证号、邮编、账号、银行识别码、药物名称、密码、银行卡号等数据。 |
|  |  | 支持对敏感数据分布的服务器进行统计，并以图表的形式展示，可导出为报表。 |
|  | # | 数据加密 | 支持对数据库表中的敏感字段指定加密算法及加密方式，至少支持AES、3DES加密算法 |
|  |  | 密文数据支持增删改查操作 |
|  | # | 支持对数据库表的中的指定行指定加密算法及加密方式 |
|  |  | 可通过配置界面详细的显示出加密的表、列的详细信息包括加密状态、加密进度等信息 |
|  | # | 可通过配置界面详细的显示出解密的操作及解密进度 |
|  |  | 加密遮蔽，支持对字段中部分内容进行遮蔽操作。 |
|  | # | 支持达梦数据库中int，integer，varchar，varchar2，date，datetime，char数据类型加密 |
|  |  | 数据库加解密策略 | 支持自定义数据库表、列加解密，不同行（列）、元数据可选择不同的加密算法和密钥长度 |
|  |  | 数据加解密权限控制 | 支持对数据库用户授权，授权用户能够访问明文，非授权用户只能够访问密文，通过安全策略能够限制DBA、开发人员、第三方外包服务人员等高权限用户访问敏感数据。 |
|  |  | 对加密数据的访问授权可基于表、程序名、IP、时间点、星期范围等进行授权，并能够进行访问审计 |
|  |  | 对加密数据的访问授权可精确到命令级，可对select、updata、delete操作进行授权 |
|  |  | 敏感数据审计 | 支持自定义敏感数据，并能够对敏感数据访问进行审计； |
|  | # | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **主机安全审计系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 基本要求 | 提供客户端安全审计功能，与防病毒软件系统为统一的管理平台，客户端授权数50点 |
|  | ★ | 客户端支持要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012 |
|  | # | 运维管控 | 支持远程协助终端（不依赖Windows远程桌面协议）、远程关机、重启终端；  支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用； |
|  | # | 可监控指定终端网络、应用程序的上传，下载速度与流量； |
|  | ★ | 支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；违规外联发生时可针对内外网连接状态分别设置违规处理措施 |
|  | # | 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。 |
|  |  | 支持网址白名单，通过信任网址白名单可以管理企业网络内信任的网址，加入信任后终端不再将此网址视为威胁 支持网址黑名单，可设置终端不能访问的网址URL，终端访问这些URL时会被拦截，并展示拦截记录 |
|  | ★ | 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限 |
|  |  | 支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查 |
|  |  | 终端支持在线、离线策略，可同时使用在线或离线两种状态，保证终端安全运行；  支持按照域名、操作系统、WIFI SSID等条件匹配预先设定好的场景策略；  支持LDAP账号的终端用户策略模式； |
|  | # | 终端审计 | 支持移动存储设备、网络共享服务器、本地硬盘特定扩展名或特定目录下的文件访问、修改、删除、移动等行为的审计 |
|  | ★ | 支持网络打印操作、本地打印操作、虚拟打印操作审计，记录包含终端ＩＰ，文件名称与类型，打印机名称，纸张类型等信息；支持自定义文档类型的打印审计； |
|  | # | 支持邮件发送审计，通过设置例外,忽略已知类型的可信邮箱,如本企业的内网或外网邮箱等,重点记录未知收件人的邮件日志； |
|  | # | 支持终端访问的互联网全日志的审计，支持自定义浏览器进程与主机地址的筛选； |
|  |  | 支持对应用程序的启动和停止进行记录,统计软件运行的活动状态 |
|  |  | 支持USB、蓝牙或红外等终端外设接口接入外设的使用情况审计 |
|  |  | 支持终端的启动、关闭、待机、休眠、等状态的记录与统计 |
|  |  | 支持本机账户或域账户登录日志统计 |
|  |  | 资产管理 | 支持自动发现设备的IP-MAC地址的绑定 |
|  |  | 支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件 |
|  |  | 支持正版软件的正版序列号的读取功能，确保软件正版化。 |
|  | # | 设备联动 | 支持与本项目中防火墙产品联动，达到网关终端边界联动防御效果 |
|  | ★ | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **统一安全管理平台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 产品形态 | 安全管理系统软件，支持系统的基础框架（平台核心服务、告警管理、报表管理、权限管理、系统配置），包括网络管理模块（网络拓扑发现模块、设备面板管理模块、机架物理视图管理模块）、网络设备监控模块、安全设备监控模块、服务器监控模块；以上模块可自选。平台内置数据库，包括100个监控节点许可。 |
|  |  | 管理范围 | 能够集中监控网络中的主机设备、网络设备、安全设备、应用系统。具体包括：交换机、路由器、防火墙、Windows服务器、AIX服务器、Linux服务器、HP-UX服务器、Solaris服务器、SQL Server、Oracle、DB2、Sybase、MySQL数据库系统、webshpere/ weblogic中间件、Mail/Web/FTP/DNS/DHCP/WINS和LDAP服务等。 |
|  |  | 资产管理 | 可对网络中的IP资产进行管理，支持以安全域的方式对资产进行分组，资产的属性包括安全CIA指标，支持自定义资产属性，可根据需要对资产属性进行任意扩展。 |
|  | # | 综合拓扑管理 | 支持网络拓扑发现，自动生成网络拓扑图，支持分层显示和全局显示两种展现方式。在全局显示模式下，能够在一个拓扑图上显示三层、二层网络设备和终端设备。拓扑图上能够显示节点之间的链路连接，并标示流量值。如果节点出现故障，拓扑图节点能够显示为红色，如果链路出现故障。支持对拓扑图的鸟瞰、缩放、导出、导入、更换底图、编辑。内置ping、tracerouter、telnet等常用工具，可直接调用。通过拓扑地图，用户可以调用设备的http接口、telnet接口、ssh/ssh2接口实现对设备的直接访问和控制。 |
|  | # | 机房物理视图管理 | 支持机房和机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态，出现问题就会闪烁告警。用户点击机架上的每个设备，可以进入这个设备的明细监控界面。支持拓扑图和机架视图中的设备的双向定位。支持机房3D图形显示 |
|  | # | 真实设备面板图 | 用户可以看到设备的真实面板图，并可以针对面板上的接口进行实时监控和设置，进行形象化管理 |
|  | # | 智能监控频道 | 智能监控频道为用户提供了一个从总体上把握网络中各种IT资源整体运行情况的界面。通过智能监控频道，用户可以快速导航到系统的各个功能界面，可以看到当前企业和组织的整体健康等级。 |
|  |  | 用户可以自定义频道，每个频道都能够自由组织视图，包括视图的布局和显示的内容。监控频道中的每个窗口都能够移动、放大、缩小，窗口中显示的统计和摘要信息都能够点击、下钻、查看明细。监控频道能够最大化显示，作为运维中心的主控界面，在大屏幕或者投影银幕上呈现 |
|  | # | 业务安全监控 | 能够描述出业务系统组成关系的业务拓扑图，针对图中的每个软硬件资产设定关键监控指标，并实时跟踪，计算出当前业务系统的整体健康状态。能够监控业务系统的整体连续性，可以查看到最近24小时、最近7天，最近30天的业务运行状态、健康状况、实时业务快照和告警信息。用户可以自由定义、编辑、修改业务拓扑图，业务拓扑的元素包括主机、网络设备、安全设备、数据库、中间件、各种类型的服务和应用，业务拓扑可以嵌套，并以树形结构展示 |
|  |  | 主机监控 | 能对包括服务器和HP、IBM小型机在内的各种主机操作系统进行监控。不仅能够检测主机性能，还能够检测主机安装的软件信息、在线用户信息、主机进程信息、主机网络连接信息、主机服务运行信息等 |
|  |  | 网络和安全设备监控 | 可以对网络设备属性，网络设备状态监控，网络性能监控，cpu利用率监控，内存利用率监控，接口监控，设备面板管理，端口通断控制。可以下发防火墙策略。 |
|  |  | 应用监控 | 监控过程无需安装任何探针或者代理，通过智能协议探测的方式对各类服务和应用系统进行监控。应用监控还能够对用户指定的URL地址进行web站点的基本网页防篡改监测。检测网页的时候，用户可以指定复杂的正则表达式。 |
|  |  | 报表管理 | 提供了针对全网络运行状态的分析报表。这是进行综合分析的数据报表，可以让管理员了解和评估整个网络系统的运行状态。能够根据用户的需求定制时间，例如生成日报表，周报表，月报表和年报表等；管理员可以根据自定义的时间段生成网络运行报表、性能分析报表和可用性报表。报表可以另存为HTML、EXCEL、文本、PDF、WORD等多种格式。 |
|  | # | 外部系统集成 | 可在事件层与网络、服务器、数据库系统方面的专业管理工具集成，可提供比较丰富的API接口，与业务系统进行集成，可提供多种格式的日志分析、读取功能。同时可以读取中心现有的的主机审计、网络行为审计系统的日志进行分析并展现在首页集中管理界面中。 |
|  | # | 自带数据库 | 无需另外安装数据库，系统自带数据维护功能，无需另外进行数据库维护。 |
|  |  | 事件处理性能 | 不低于10000条/秒 |
|  |  | 事件查询性能 | 数据库中数据量不小于50G时数据查询结果返回时间小于3秒。 |
|  |  | 功能扩展 | 提供SNMP Trap、Syslog事件转发功能，支持对第三方的Web Service接口调用 |
|  | ★ | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **WEB应用防火墙**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件规格 | ≤2U机架式硬件设备，1T硬盘，冗余电源，配置8个千兆SFP插槽，6个10/100/1000M自适应电口，2组bypass，1个Console口，2个USB口.Web安全保护128个站点。 |
|  | ★ | 性能要求 | 网络吞吐量≥12Gbps，应用层处理能力≥2Gbps，HTTP新建连接数≥30000/s，并发连接数≥240万，HTTP并发≥160万 |
|  | # | 部署模式 | 产品支持IPv4与IPv6双协议栈镜像分析数据并实现旁路阻断功能，产品具备专门的阻断接口设置 |
|  |  | Web安全 | 产品具备支持SQL注入、跨站脚本、防爬虫、扫描器、信息泄露、溢出、协议完整性等至少7种知识库展示说明 |
|  |  | 产品具备支持HTTP协议校验细粒度规则检测，至少提供20种HTTP协议校验策略参数，其中要包括Cookies、Response、Range等策略参数 |
|  |  | 产品具备对HTTP协议检验参数提供参数值设置、并提供3种严重级别分类和至少5种处理动作设置 |
|  | **★** | 自学习系统 | 具备自学习系统，无需人工干预，自动获取网站相关信息 |
|  | **★** | 具备根据网站流量自动生成网站文件和URL地址的树形结构展示拓扑图 |
|  |  | 威胁情报中心 | 产品具备支持威胁情报中心联动功能，具备FTP、API、key联动方式 |
|  | # | 产品具备至少提供3个威胁情报中心联动的接口配置功能，同时收集多家数据情报供设备使用 |
|  | # | 网站云防护 | 产品具备网站云防护攻击数据统计分析模型，提供CC攻击、Web漏洞攻击等数据分析 |
|  |  | 产品具备网站云防护通过域名解析方式实现Web防御功能 |
|  |  | DDoS清洗 | 产品具备TCP DDoS防护策略，应具备端口扫描、SYN flood、Conn Flood、ACK flood、序号攻击、慢攻击等常见TCP DDoS攻击防御能力、具备UDP DDoS防护策略，应具备UDP flood、DNS flood等常见UDP DDoS攻击防御能力、具备HTTP DDoS防护策略，应具备HTTP限速、CC攻击等常见HTTP DDoS攻击防御能力 |
|  | **★** | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. **安全单向导入设备**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 硬件规格 | 系统采用2+1模式，即系统由A网主机模块、B网主机模块和交换模块组成，其中交换模块由分别插在A网主机和B网主机PCI-E接口的交换卡组成。  ≤2U机架式硬件设备，冗余电源；具有液晶面板, 能够显示产品品牌、型号、CPU/内存占用率、网络接口状态等信息，  内网：6个10/100/1000Base-T端口，2个SFP接口，1个Console口，2个USB口；  外网：6个10/100/1000Base-T端口，2个SFP接口，1个Console口，2个USB口 |
|  | ★ | 性能要求 | 系统吞吐量≥4G |
|  | # | 部署方式 | 串接部署在不同的安全域之间，支持IPv4与IPv6双协议栈 |
|  |  | 主模块 | 内、外网分别具有独立的管理接口，而不是通过网络接口管理，也不是通过内网一个管理接口完成全部管理 |
|  | **★** | 支持带内管理，可通过业务口进行网闸管理工作；用户可自行选择是否启用带内管理功能 |
|  |  | 提供基于https的图形化安全管理，支持用户名/口令、数字证书、U-KEY等多种认证管理方式; |
|  |  | 文件交换模块 | 支持FTP、SMB方式的文件单向导入 |
|  |  | 支持多种同步模式，源端删除、源端移动 |
|  |  | 支持任务启动、停止 |
|  |  | 数据库同步模块 | 支持SQL Server、Oracle数据库同步，不需要更改数据库结构和添加数据表，不影响数据库服务器性能 |
|  | **★** | 同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件），支持windows、linux、unix等多种数据库操作系统类型。 |
|  | # | 支持周期复制、实时复制、增量更新等多种同步方式。 |
|  | **★** | 分发访问 | 支持两台两台单向设备实现标准TCP访问 |
|  |  |  | 网闸自身完成，不需要第三方软件或服务器支持 |
|  |  | 单向TCP | 支持单向TCP定制服务；支持源地址绑定、网络接口地址绑定功能； |
|  |  | 支持限定一次报读数据长度限制、连续摆渡的数据报文个数限制、微妙级延时时间配置 |
|  |  | 单向UDP | 支持单向UDP定制服务；支持源地址绑定、网络接口地址绑定功能； |
|  | **★** | 防护设置 | 支持双引擎病毒模块，可根据用户需求选择需要的病毒引擎； |
|  | ★ | 产品资质 | 要求提供计算机信息系统安全专用产品销售许可证 |

1. 安全密码模块

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
|  | ★ | 总体要求 | 保障电子证照生成、入库、管理和应用等全生命周期的安全性，提供防伪、防篡改、防抵赖、防假冒等信息安全保障服务。  支持智能移动终端，移动终端上的密码模块是纯软件实现且不依赖于任何硬件密码设备。 |
|  | # | 与第6项（电子证照管理模块）、第7项（电子证照应用模块）、第9项（电子证照存储模块）为同一品牌 |
|  | ★ | 性能要求 | 支持300万移动终端 |
|  | ★ | 密码算法 | 支持国产密码算法SM2、SM3和SM4。 |
|  | ★ | 密钥管理 | 由移动客户端和服务端共同完成签名私钥的分割产生、分散存储等密钥管理功能。 |
|  | # | 密码服务 | 由移动客户端和服务端共同协作执行数字签名等密码服务 |
|  | ★ | 资质 | 要求提供国家密码管理局《商用密码产品型号证书》 |
|  | ★ | 符合GM/T0039-2015《密码模块安全检测要求》安全等级第二级及以上相关要求 |

1. 服务器

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **技术参数** | **参数值** |
| 服务器机箱 | | | |
|  | ★ | 外观高度 | 标准机柜安装，配置上架导轨 |
|  | ★ | 扩展能力 | 支持≥14片刀片服务器，支持不同型号Intel,AMD,x86和Unix小机刀片服务器混插，并支持存储刀片，磁带机刀片，工作站刀片的混插 |
|  | ★ | 互连模块插槽 | 配置≥8个互连模块插槽，支持以太网交换，SAN交换，SAS交换机及IB交换机 |
|  |  | 以太网络模块 | ≥2个以太网模块，支持冗余连接，单个以太网模块上联端口≥6个千兆RJ45接口 |
|  |  | Infinband交换模块 | 支持对内连接满配QDR接口，提供满配外接QDR接口 |
|  |  | 管理 | 提供本地LCD液晶屏图形化机箱管理，状态显示并能人机交互，配置管理模块，支持冗余配置，支持KVM |
|  |  | 电源 | 提供6个冗余热插拔电源，支持N+1、N+N电源冗余模式，N≥3，单个电源模块支持≥2500W，支持直流，交流，单相，三相电源接入 |
|  |  | 风扇 | 提供≥10个冗余热插拔主动式散热风扇 |
|  |  | 管理软件 | 基于Web的架构与应用管理架构，管理设备不需要安装任何插件，软件部署要求在20分钟内部署完成，实现管理软件单一入口登陆方式，管理相关数据中心设备 |
|  |  | 部署软件 | 支持系统快速部署软件，可同时分发安装Windows，Linux等主流操作系统 |
| 刀片服务器 | | | |
|  | ★ | 服务器外型和数量 | 实配八个刀片服务器 |
|  | ★ | CPU型号 | Intel Xeon SP 4110处理器或更好 |
|  | ★ | CPU核数 | ≥8核 |
|  | ★ | CPU颗数 | 2颗 |
|  | ★ | 内存类型 | DDR4 |
|  | ★ | 内存容量 | ≥256GB DDR4 2666内存 |
|  |  | 内存频率 | ≥2133Mhz |
|  | # | 内存插槽数 | 16个 |
|  | # | 内存保护 | Advanced ECC先进内存保护技术及联机备用模式 |
|  | # | 内存扩展数量 | 支持≥2TB内存 |
|  |  | 硬盘接口 | 支持2.5"热插拔 SAS/SATA/SSD/NVMe硬盘 |
|  |  | 硬盘容量 | ≥2块600GB SAS硬盘，热插拔 |
|  |  | 硬盘转速 | ≥10000RPM |
|  |  | 启动盘可选项 | 支持双M.2卡配置Raid1，作为操作系统安装盘 |
|  |  | 阵列控制器 | SAS磁盘阵列控制器, 配置1GB 非易失性高速缓存, 支持RAID 0/1; |
|  |  | 操作系统 | 实配LINUX 、WINDOWS SERVER等正版操作系统 |
|  |  | PCI-E插槽 | ≥2个PCI-e 3.0 \*16 插槽 |
|  |  | 网络接口 | ≥2端口10Gb Ethernet网卡 |
|  |  | 远程管理卡 | 配置独立的远程管理卡，实现服务器远程管理 |
|  |  | 管理软件 | 配置远程监控图形界面,可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱等操作，提供服务器健康日记、服务器控制台记录/回放功能 |

#### 3.3系统集成及项目实施方案

投标人应根据本项目的具体需要，提供合理的系统集成方案，在方案中要重点说明：

（1）结合甲方现有系统现状情况，提供开发软件、基础软件、硬件平台等的详细的安装、部署与规划方案。

（2）提供详细的项目实施方案。

（3）完成全部软硬件产品的安装与调试工作，包括设备安装、上架、加电等；

（4）项目实施完成后，中标人应将系统的全部有关技术文件、图表资料及测试、验收报告等文档汇集成册交付用户，并交付相应的电子版本，所提交的文档包括但不限于：实施方案、参数表、设备配置手册、日常操作及维护手册等，所有的技术文件必须是中文。

投标人应结合项目建设目标、建设内容，对项目工作任务分解，制定详细进度计划、组织保障、运行管理措施：

（1）建设目标要在明确项目总体目标的基础上，进一步确定项目的分阶段目标。目标的制定要求做到可衡量、可执行、可考核；

（2）工作任务按照分项目和时间进行结构化分解，任务分解最小到周；

（3）进度计划要求划分项目的实施阶段，确定项目的重大节点和里程碑，提出有效的节点控制办法，保证项目的整体时间进度要求；

（4）组织保障要求按照项目不同阶段和不同层级，规划项目的组织、沟通方式和职责，制定项目管理的制度和流程；

（5）风险控制要按照政策、业务、技术、管理、进度、资金等多个方面对项目进行定量和定性风险评估，划分风险等级，并提出有效的风险控制应对策略。

#### 三、服务要求

#### 1、售后以及开发运维服务要求

|  |  |  |
| --- | --- | --- |
| 序号 | 内容 | 服务要求标准 |
|  | 投标人服务要求 | （1）投标人承诺所有硬件三年免费保修、所有软件一年免费保修升级、电话报修后4小时上门服务、12小时内排除故障。  （2）投标人承诺所有硬件过三年免费保修期后按原价维修（按投标货物价格数量表所列价格，更换零部件的按合同签订时的零部件价格）、所有软件过一年免费保修升级期内按按原价的10%进行维修升级，响应速度同保修期响应速度。  （3）在保修期间，如故障产品的维修周期超过2个工作日，中标人为用户提供相同型号或性能相近的备用产品使用；同一产品出现两次故障，中标人必须更换为不低于该设备性能的新产品。  （4）在维保期间，提供24小时的免费技术咨询服务，每年不低于2次的定期巡查服务和技术升级服务等。 |
|  | 软件开发要求 | 投标人须承担法人库和电子证照系统的开发部署过程从计划到上线等各阶段内容。 |
|  | 运维要求 | 投标人应综合考虑本项目所有服务器产品虚拟化资源的统一池化管理，要求实现异构资源管理、组织与分配、自动化运维、智能监控、业务流程定制管理等，作为项目验收内容，提供详细的运维方案。 |

#### 2、培训要求

（1）培训目标

根据项目的实际情况，提供多种形式的培训服务，以到达良好培训效果。

确保建设单位的技术人员能够熟练地进行维护和管理。确保建设单位的相关人员对其使用的设备能熟练地操作和使用。

（2）培训教材

投标人必须负责提供培训所需计划和资料（包括纸质文档和电子文档），培训教材包括但不限于视频教材、WORD和HTML用户手册、培训PPT。培训所使用的语言和教材必须是中文。

（3）培训对象

培训建设单位的人员包括但不限于中央编办相关业务人员、系统运行维护人员等。

（4） 培训内容

培训内容包括设备及维护培训等。培训的时间、内容、人员、期次等具体内容在具体执行过程中需根据建设单位意见进行调整。应提供详细的培训方案。培训方案主要包括培训教师、培训内容、培训大纲、培训计划、培训对象等几个方面。

#### 3、其他要求

（1）知识产权要求

投标人应保证中央编办使用该货物及服务或其中的任何一部分时，免受第三方提出的侵犯其知识产权的索赔或诉讼。如有任何上述指控，投标人应独自承担可能发生的一切法律责任和费用。

（2） 保密要求

投标人必须对项目技术文件以及由投标人提供的所有内部资料、技术文档、数据和信息予以保密。投标人必须遵守与投标人签订的保密协议，未经投标人书面许可，投标人不得以任何形式向第三方透露本项目标书以及本项目的任何内容。投标人在应答时必须说明具体安全保密管理，确保安全保密承诺得以落实。