**长沙农村商业银行股份有限公司**

**零信任网络安全平台项目**

**业务需求**

**信息技术部**

**2021年08月**

## 零信任网络安全平台业务需求书

* 1. **项目背景**

随着银行的信息化程度、移动化程度不断提高，银行内部业务系统逐步成为组织的核心资产，随时随地处理内部业务系统的信息变得越来越普遍和重要。企业员工有职场内（公司场所）、职场外（远程）灵活办公的需求。职场内，以防止企业内部威胁为主；职场外，当员工因疫情或其他等原因需在家临时办公，或者长期出差在外，以及外部伙伴因业务合作需要访问企业内部系统，需要确保远程办公访问过程的安全，以减少企业内部系统被从职场外部入侵的风险。

目前我行员工主要是通过手机端访问行内的OA系统、即时通讯及其他应用系统，随着近几年互联网系统的发展，我行在互联网上的信息资产也越来越多，暴露面扩大，安全风险也相应变大，风险主要表现如下：

1. 远程办公接入终端的可信问题使得访问业务系统的风险增高；
2. 互联网终端自身带入木马、蠕虫、病毒等恶意程序感染业务系统；
3. 数据在互联网链路传输，面临劫持和监听的风险；
4. 业务直接暴露，且弱口令无法杜绝。

零信任网络安全平台作为长沙农村商业银行数字化转型方案中基础平台，能有效防止弱身份及密码与访问管理、账号劫持、内部恶意人员威胁、高持续威胁等网络威胁，提供认证、授权、隐身、风险检测等能力。

随着移动业务的快速发展，改进银行服务效率和服务质量，更为精准地定位客户的金融需求，实现各种高附加值的增值服务，发掘更多的潜在客户，零信任网络安全平台的建设为更广泛的客户群体提供安全可靠的银行服务，做实做深普惠金融，切实履行地方银行责任担当。

* 1. **需求分析**

对于金融行业而言，随着数字化转型发展卓有成效，各种基于新技术的创新应层出不穷，使金融服务的覆盖范围和质效均实现了显著提升，但金融机构的网络安全边界也随之不断扩大，传统架构很难应对边界模糊带来的更广泛的内外部威胁，也无法解决复杂网络架构和多样化接入方式带来的成本增多。对此，零信任基于产品化、组件化、场景化等技术特点，可以提供一种轻量级、动态发展的安全策略，且随着数字化转型的逐步深入，零信任本身也将会愈加完善。

总体来看，零信任主要表现为以下三点：

一是信任最小化。所有设备、用户和网络流量都应该被认证、授权和加密。

二是网络无特权化。应当始终假设外部和内部威胁每时每刻都充斥着网络，并且不能仅仅依靠网络位置来建立信任关系。

三是权限动态化。访问控制策略应该动态的基于尽量多的数据源进行计算和评估。

综上，不难看出，零信任的本质是引导安全架构从网络中心化走向身份中心化，进而以身份为中心进行细粒度的自适应访问控制。这里有一个非常重要的前提是身份的识别和认证，落实在技术层面是要构建一个统一的身份认证系统，需要采集包括人、设备、系统和应用等在内的各方面信息。

* 1. **功能需求**

**3.1零信任网络安全平台组件-控制中心**

1.用户管理：可对用户执行创建、删除、停用、编辑、导入、导出、同步等操作，本地用户具有唯一标识ID。

2.组织管理：支持创建、导入、编辑、同步组织机构关系，并关联用户，组织机构具有唯一标识ID。

3.角色管理：内置多级管理员角色，系统管理员可新建、编辑、删除用户组（角色）并关联用户，管理员角色及用户组具有唯一标识ID。

4.认证管理：支持对接第三方统一认证平台；支持针对不同的访问主体定制用户登录认证策略；支持调用标准认证源（如短信、钉钉、企业微信、指纹、人脸、LDAP等）认证。

5.授权策略管理：支持基于角色的授权策略配置，配置主体、客体角色授权；支持基于属性的授权策略配置，可为角色授权提供属性条件过滤规则与控制；提供可信环境风险、用户行为分析、用户环境属性多维度的授权策略统一管理功能。

6.设备管理：支持设备信息注册、维护、删除、停用、导入、导出；支持收集CPU、内存、磁盘、IP、MAC、操作系统等信息。

7.事件管理：出现重要安全事件时，在首页进行提醒，管理员可以一键处理、忽略或者进行预警条件的编辑；事件告警支持邮件、短信方式通知。

8.可视化展示：支持展示全网安全分数、已部署终端数、待处理威胁数、待处理高危漏洞数，支持一键部署终端、处理威胁和漏洞，同时展示服务器状态，包括CPU使用率、磁盘空间、流量情况。

**3.2零信任网络安全平台组件-代理网关**

1.应用资源管理：提供对应用名称、应用地址、应用域名、应用协议等应用系统资源的统一管理功能；支持Web业务登录表单自定义填充；支持Web业务登出状态自动检测；支持Web业务URL参数自定义配置；支持token传递、消息透传等多种应用发布方式，保证应用系统安全对外发布；支持令牌传递模式，支持URL、Header、Cookie自定义传递；支持静态页面接管及定制功能。

2.传输安全：支持标准TLS1.0/TLS1.1加解密，可禁用SSLv3/v2协议；支持应用配置HTTP强制转换HTTPS，自动完成HTTP到HTTPS加密服务；管理TLS加解密算法的强度，支持自定义最新算法会话协商：AES128-SHA,AES256-SHA,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-SHA,ECDHE-RSA-AES256-SHA,DES-CBC3-SHA,RC4-SHA,RC4-MD5；支持国密算法：SM1、SM2、SM3、SM4算法；支持TLS会话自动重协商；支持用户登录次数锁定及锁定周期控制。

**3.3零信任网络安全平台组件-环境检测**

1.基础安全性感知：支持感知发现终端中恶意行为；支持感知终端上的高危漏洞，及时发现终端当前的已知风险。

2.管理能力：支持对感知内容进行管理和配置，能够允许管理员自定义感知策略、感知内容、风险等级、评分规则、执行频率等，并可同时配置并执行多个不同感知策略。

3.应用环境感知：支持针对移动终端（鸿蒙、Android、IOS）和PC终端（Window、Mac、Linux）是否安装违规的软件；运行违规的进程、存在违规的注册表和服务项行为进行感知；支持感知终端防火墙状态；支持感知终端高危服务；支持感知终端病毒查杀状态；支持感知终端上的高危漏洞，及时发现终端当前的已知风险；支持感知终端其他安全状态和信息，保证终端安全合规的运行。

4.设备识别：可采集硬件信息，包括CPU、内存、磁盘、IP、MAC操作系统等信息，并上报至控制中心。

5.应用监控：系统采用应用监控技术，可感知到应用的启动信息，并将启动信息上报至控制中心。

6.统一管理：统一控制中心，对全网终端的感知环境进行集中管理，基于终端感知模版/终端的感知结果管理/数据报表的管理等功能。

7.可信度度量：采用“可信加权”原则，将所有风险项产生的权值进行相加，以百分制提供给策略方，策略方再根据不同的权值制定相应的安全策略；可以对可信指标进行分级，可以支持三种等级划分的定义。

8.资产安全检查：可以支持安全防护、终端环境、用户行为、终端安全基线等检测项，指标不低于50个。

9.终端客户端安装：支持支持IOS系统、Android系统、鸿蒙系统、Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10及以上；Windows server系列操作系统；mac操作系统；Linux系列操作系统；支持管理员可以通知终端用户到指定网页下载；支持可自行下载为离线安装包，再拷贝到终端上进行安装；支持SDK集成，行内APP应用程序集成SDK；支持主流浏览器插件方式。