国家税务总局
新型全国涉税APP生命期一体化服务平台
总体方案

（根据有关文件拟制）

北京三博安科技有限公司

2020年12月18日

国家税务总局
新型全国涉税 APP 生命期一体化服务平台

一、背景

(一) 政策要求

2016 年 11 月，全国人大常委会通过《网络安全法》明确：国家关键信息基础设施、公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，需要建立纵深安全防护体系——风险评估+安全监测+安全态势感知等多方面的安全防护。

2019 年 12 月 1 日，国家网络安全等级保护 2.0 标准 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》正式实施，对移动安全提出明确防护要求。

2019 年 1 月 25 日，中央网信办、工业和信息化部、公安部、市场监管总局发布“关于开展 APP 违法违规收集使用个人信息专项治理的公告”，开展 APP 专项治理。

国家税务总局提出“坚持‘战建互促’‘攻防并举’，坚持‘安全即服务’‘以实战为导向’，着力构建一体化的网络安全保障体系，不断提高税务系统网络安全防护能力”的指导思想。

二、现状及问题

(一) 现状

国家税务总局于 2016 年 11 月起，构建了税务移动应用 APP 全生命周期安全的防护系统。对全国各级税务机关在互联网移动应用市场、门户网站所发布的涉税 APP 提供安全编码、安全 SDK 保护、源码审计、安全加固、渗透测试、安全检测、个人信息保护、盗版检测等功能支持，通过第三方应用市场渠道监测，对发布后的 APP 进行监测，努力实现全国涉税 APP 能够安全下载和使用。

（二） 存在问题及分析

一是，涉税APP防盗版能力需进一步增强。目前，税务采用两种方式防止APP盗版：APP加固、对分发渠道上的APP进行分析。由于这两种方式无法确定APP开发者真实身份，APP完整性难以保证，因此，APP的真实性、合法性无法辨别，给监测APP篡改、假冒带来困难。要解决涉税APP开发者真实性问题。

二是，涉税APP在第三方移动应用市场发布、下载仍存在严重安全风险。目前，涉税APP发布的主要渠道是互联网移动应用市场，这些市场对APP开发者和APP安全审核不严格，软件恶意行为不被约束，仿冒软件泛滥，涉税APP在这种环境里受到攻击、假冒的风险非常大，监管难度和成本高。据国际专业组织报告《2019移动应用威胁态势报告》将国内多家APP商店，包括华为、小米、手机助手等，列为“最可能下载恶意APP的商店”。要解决涉税APP可靠分发渠道问题。

三是，涉税APP在手机上安装运行尚未满足等级保护2.0新要求。涉税APP在移动终端安装、运行时没有实行实名签名验证和管

控，不满足网络安全等级保护2.0对APP签名验证要求，一旦安装了被二次打包的恶意软件，移动终端则会遭遇广告骚扰、吸资扣费、窃取用户隐私，严重的可通过APP攻击税务信息系统。要解决APP计算环境安全问题。

三、目标

为进一步提升涉税移动应用APP系统安全性，降低纳税人数据泄漏的风险，保护纳税人合法权益，满足国家网络安全政策法规新要求，新型全国涉税APP生命期一体化服务平台的目标是：

1.整合涉税APP开发、检测、发布流程，构建全国涉税APP一体化集中管控平台。

对税务APP开发商进行统一资质审核、备案和管理，保证APP开发商是正规的税务总局认可的机构，满足等级保护2.0对APP开发者的要求，保证APP供应链安全；对涉税APP进行统一安全合规检测；对通过安全检测的APP实行备案、集中发布，彻底规避涉税APP在第三方移动应用市场发布安全风险，满足等保2.0对APP发布渠道的要求，提高总局对全国涉税APP上线后监管力度和效率，降低监管成本。

2. 提高涉税APP监管实战化能力和水平，建立APP生命期实时信息分析、研判大数据监测平台。

整合涉税APP开发商注册、APP上架、下载、安全及合规检测、盗版分析等数据，将全国涉税APP生命周期一体化管理平台数据输

送到态势感知平台等其他系统，对全国涉税APP全网、全时段实施安全监测，有效地支撑税务系统的安全运营；对重点涉税APP的安全监测提供数据支撑，为安全管理工作提供执法依据。

3.增强涉税APP防盗版能力，构建以国产密码技术为核心的涉税APP实名签名/验证机制。

落实中华人民共和国《密码法》，采用国产密码算法技术，构建以国产密码技术为核心的涉税APP实名签名/验证机制，对涉税APP进行实名签名保护，APP运行时对进行签名验证，满足等保2.0关于APP指定签名证书的要求，彻底防止假冒、二次打包涉税APP安装、运行。

4.增强APP安全检测、加固技术手段，保证纳税人个人信息及涉税数据安全。

遵照国家法律法规，加强涉税APP个人信息安全检测，保证不存在超范围采集个人敏感信息，在APP发布前进行漏洞、恶意代码扫描等安全检测和加固，保证APP代码合规性、安全性，防止涉税APP被病毒，木马，蠕虫侵入造成涉税数据和个人数据被窃取。

四、解决方案

（一）平台总体结构

利用第三方服务机构建立“新型全国涉税 APP 生命期一体化服务平台”(简称“平台”)，以密码技术为核心，面向全国涉税 APP 开发商、涉税 APP 使用者提供：涉税 APP 开发商审核、备案、APP

合规检测、数字签名/验证、集中下载等服务，并为国家税务总局提供监测数据支撑。见下图。

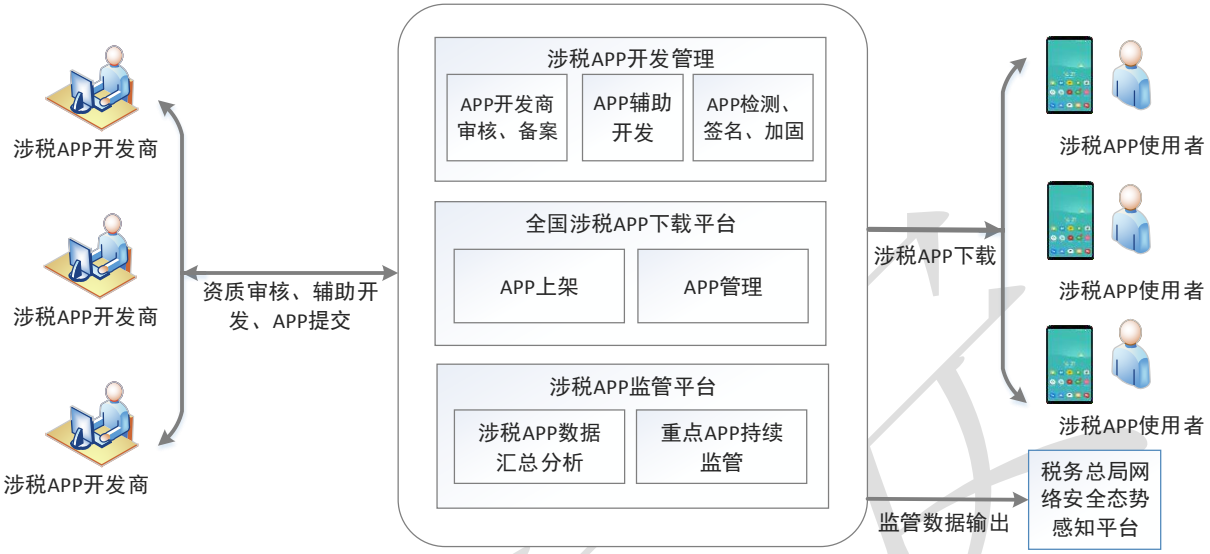

图 新型全国涉税APP生命期一体化服务平台

平台由三个子系统组成：涉税 APP 开发管理、涉税 APP 下载平台、涉税 APP 监管平台。

1．涉税 APP 开发管理系统

为涉税 APP 开发商提供注册、审核、备案，APP 签名证书，安全辅助开发，APP 提交、检测、加固等服务。平台管理员审核开发商资质，APP 开发商国密证书管理，APP 开发商资料管理等。

2．全国涉税 APP 下载平台

对开发商提交的 APP 进行安全审核、检测，对合格的 APP 进行二次签名，涉税 APP 进行上架、下架、版本等管理。全国涉税 APP 用户通过“涉税 APP 手机客户端”下载使用涉税 APP。

3．涉税 APP 监管平台

对全国涉税 APP 开发商、APP 基本信息、APP 下载量、APP 日活量、APP 崩溃信息、安全及合规检测、盗版等数据进行全生命期

大数据监测据、统计分析，以可视化图表动态呈现全国涉税移动应用的实时安全态势，对重点 APP 进行持续监管，并将数据输送到税务总局网络态势感知平台等其他系统。

（二）目标保障

1.整合涉税APP开发、检测、发布流程，构建全国涉税APP一体化集中管控平台。

(1)平台对税务 APP 开发商进行统一资质审核、备案和管理，审核企业法人信息、企业营业执照、地址等资质信息，审核通过后为开发者提供开发者证书，保证 APP 开发商是正规的税务总局认可的机构，保证 APP 供应链安全，满足等保 2.0 三级安全建设管理相关条款要求：

——8.3.4.1移动应用软件采购：b)应保证移动终端安装、运行的移动软件由指定的开发者开发。

——8.3.4.2移动应用软件开发：a）应对移动业务应用软件开发者进行资格审查。

(2)平台对涉税 APP 进行统一安全合规检测，包括漏洞扫描、安全检测、内容检测、个人隐私权限检测等，分析 APP 是否有恶意代码、安全漏洞、滥用权限、非法收集信息、违法内容等潜在风险，保证 APP 安全、绿色、合规。满足等保 2.0 第三级关于 APP“软件安全检测”要求：

——8.1.9.4自行软件开发：e)应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。

（3）平台对开发商提交的 APP 检测完毕后，对不合规的 APP 通知开发商进行整改，重新提交检测。将合规的 APP 统一发布到税务专用应用市场，并对所有应用进行上架、分类、更新、下架、安全策略设置等管理，提高总局对全国涉税 APP 集中管控力度和效率，降低监管成本。满足等保 2.0 关于 APP“可靠渠道”下载要求：

——8.3.4.1 移动应用软件采购：a)应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

2.提高涉税APP监管实战化能力和水平，建立APP生命期实时信息分析、研判大数据监测平台。

（1）汇总显示全国涉税 APP 生命周期一体化管理平台数据，并将其输送到态势感知平台等其他系统，对全国涉税 APP 全网、全时段实施安全监测，有效地支撑税务系统的安全运营。

（2）对重点 APP 进行持续监测，收集其漏洞数据、崩溃数据、权限使用、恶意行为等数据，为安全管理工作提供执法依据。并对发现的威胁主动预警，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁。

（3）为了加强监测力度，通过平台 APP 辅助开发功能指导 APP 开发商将监测程序加入涉税 APP 中，当 APP 运行时向全国涉税 APP 生命周期一体化管理平台上传 APP 运行状态信息。

3.增强涉税APP防盗版能力，构建以国产密码技术为核心的涉税APP实名签名/验证机制。

（1）采用国产密码算法，对涉税 APP 进行实名签名保护，将 APP 开发商和 APP 进行绑定，确保 APP 实名开发，保证 APP 的安全和责任可追溯，防止 APP 被篡改，重新打包等风险。满足等保 2.0 第三级安全通用要求和安全建设管理相关规定：

——8.1.10.9密码管理：a)应遵循密码相关国家标准和行业标准； b)应使用国家密码管理主管部门认证核准的密码技术和产品。

——8.3.4.1移动应用软件采购：a)应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名;

——8.3.4.2移动应用软件开发：b）应保证开发移动业务应用软件的签名证书合法性。

（2）涉税 APP 安装运行时进行签名验证，只有从税务专用应用市场里下载的有官方签名的 APP 可以安装，从其它渠道下载的 APP 无法安装，实现 APP 国密签名及验证的闭环，从而保证移动终端环境生态安全，彻底防止假冒、二次打包涉税 APP 安装、运行。满足等保 2.0 关于 APP 指定签名证书的要求：

——8.3.3.2移动应用管控：b)应只允许指定证书签名的应用软件安装和运行。

4.增强APP安全检测、加固技术手段，保证纳税人个人信息及涉税数据安全。

（1）依据《信息安全技术个人信息安全规范》（GB/T 35273-2017）、《APP 违法违规收集使用个人信息自评估指南》、《关于开展

APP 侵害用户权益专项整治工作的通知》（工信部 337 号令）等标准，采用动静结合的检测手段，针对 APP 使用全过程进行权限检测，确保 APP 中不存在权限滥用，敏感权限调用，超范围采集个人敏感数据等情况。

（2）在 APP 上架前，对 APP 进行全面的安全检测和加固。检测移动应用中存在的安全漏洞、编码缺陷、违法内容等问题，提前避免因安全漏洞导致的安全事故，及时预防安全风险。并对移动应用进行加固，防止移动程序被反编译、动态调试、窃取数据和二次打包。满足等保 2.0 第三级关于 APP 检测的要求：

——8.1.9.4自行软件开发：e)应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。