政企移动软件安全平台简介

一、平台构成

“政企移动软件安全平台”(简称GEAP平台)由公安部网络安全保卫局批准，北京市科委项目支持，以国产密码技术为核心的互联网平台。

平台根据国家网络安全等级保护2.0建立，为企事业单位提供APP开发者审核、APP安全开发、数字签名、安全检测、运行管理APP全生命期管控服务，保证政企APP合规、安全、绿色、高品质、责任可追溯。

平台由四个部分组成：政企软件开发管理、政企软件市场、政企软件仓库、GEAP安全终端。

二、平台功能及作用

(一) 政企软件开发管理

功能：

APP开发者注册、APP签名、安全辅助开发、APP提交和管理等。

作用：

1、确保APP实名开发，保证APP供应链安全，满足等保2.0第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、平台颁发国密签名证书，提供国密SM2算法的APP签名工具，对APP进行国密实名签名，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。)。

3、平台提供 APP 加固，有效抵御被破解、被逆向分析，保护应用内存数据不被访问，截取及修改，保护应用数据不被窃取等。

（二） 政企软件市场

功能：

1、GEAP 平台管理员对开发者提供的 APP 进行安全审核、检测，对 APP 进行二次签名，APP 上架，以及 APP 运营等管理；

2、政企机构注册购买 APP,员工下载 APP 使用。

作用：

1、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、平台 APP 进行安全检测审核，从渠道检测、安全检测、资源内容检测、安全态势分析等多方面对 APP 进行测评，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。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 APP 进行开发者和 GEAP 平台的“双签名”，可防止恶意 APP 传播，进一步降低 APP 安全风险。

（三） 政企软件仓库

功能：

1、政企单位员工通过 GEAP 客户端下载本单位 APP；

2、政企机构对本单位 APP 及员工进行管理。

作用：

政企机构管理员对入库软件实行安全策略设置，对政企软件进行运行监控，保证软件安全运行。

（四） **GEAP 安全终端**

功能：国产密码模块、安全域隔离、APP 国密签名/验证、APP 签名证书白名单、防截屏、防刷机等功能。

作用：

平台安全终端对 APP 实名签名验证，只有 GEAP APP 市场里的软件可以下载安装，从其它渠道下载的软件无法安装。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。满足了等保 2.0 第三级安全计算环境相关要求（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;）。