ICS 33.030
CCS M 21

团 体 标 准

T/TAF 319—2025

移动应用程序（APP）热更新框架安全服务规范

Security service specification for mobile application hot update framework

2025-11-17 发布 2025-11-17 实施

电信终端产业协会 发布

版权声明

本文件的版权属于电信终端产业协会，任何单位和个人未经许可，不得进行技术文件的纸质和电子等任何形式的复制、印刷、出版、翻译、传播、发行、合订和宣贯等，也不得未经允许采用其具体内容编制本团体以外各类标准和技术文件。如有以上需要请与本团体联系。

邮箱：tafrb@taf.org.cn

电话：010-82052809

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　安全要求 2
6　服务规范 2
6.1　企业内部使用 3
6.2　对外能力提供 3

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、OPPO广东移动通信有限公司、小米通讯技术有限公司、荣耀终端股份有限公司、北京快手科技有限公司、北京三星通信技术研究有限公司、阿里巴巴（北京）软件服务有限公司、北京微梦创科网络技术有限公司、北京三快在线科技有限公司。

本文件主要起草人：王淞鹤、宋恺、王艳红、武林娜、杜云、陈鑫爱、李可心、邓佑军、桑明臣、李腾、吴崇武、吴越、张倞诚、赵晓娜、肖振威、落红卫、王昕、王彬、刘艾婧、任资政、康宇、吴斌。

引　言

热更新作为移动应用开发中普遍使用的一种技术方案，常用于实现代码热修复、灰度测试等业务场景，提高了开发效率，丰富了应用场景。然而，热更新技术被恶意开发者利用，成为侵害用户权益、规避合规监管、对抗技术检测的手段。为解决热更新技术滥用问题，需进一步明确热更新框架开发者、热更新能力提供者的主体责任，确保热更新框架自身安全性以及服务提供过程中的规范性。

移动应用程序（APP）热更新框架安全服务规范

1 范围

本文件主要规范移动应用程序热更新框架的安全服务规范，主要分为安全要求和服务规范两方面。安全要求主要对热更新能力实现过程中的技术安全性和可靠性提出相关技术要求，服务规范部分主要面向企业内部使用和向第三方提供服务两个具体场景下提出规范性要求。

本文件适用于指导热框架型开发者和服务提供者的安全能力建设，适用于监管机构、第三方测评机构对热更新框架进行监督、评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 43435-2023 信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

热更新 hot update

通过动态下发并加载代码、资源、Web页面，在App或SDK不重新下载和安装的情况下，实现代码逻辑及资源文件实时更新的技术。

3.2

热更新框架 hot update framework

实现热更新能力的软件组件集合，包括提供热更新能力的开发框架、软件工具链、软件开发工具包等。

3.3

热更新服务提供者 hot update service provider

向第三方应用软件开发者提供热更新能力的企业、组织或个人。

3.4

热更新框架开发者 hot update framework developer

从事热更新框架设计、开发、维护等活动的主体（企业、组织或个人）。

4 缩略语

下列缩略语适用于本文件。

APP：移动应用程序（Application）
SDK：软件开发工具包（Software Development Kit）

5 热更新框架使用流程图

热更新框架使用场景可分为企业自有APP或产品使用和对外提供，企业自有APP或产品使用指企业为满足自身产品热更新需求，自行研发或并仅限用于自身产品热更新的场景，具体如图1所示；对外提供是指研发并通过服务或工具等形式对外提供热更新能力的场景，该场景涉及参与方包括热更新服务提供者以及使用者，具体如图2所示。

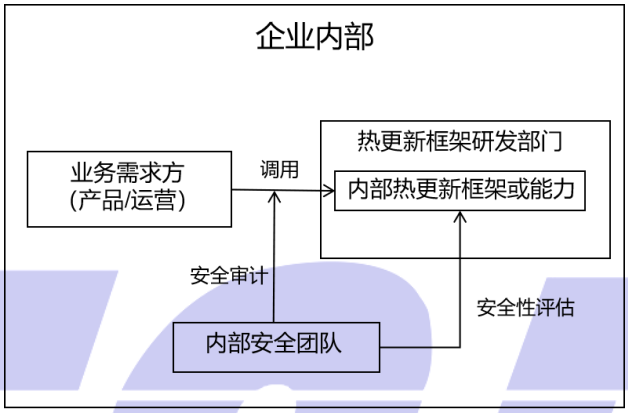

图1 自有APP或产品使用场景

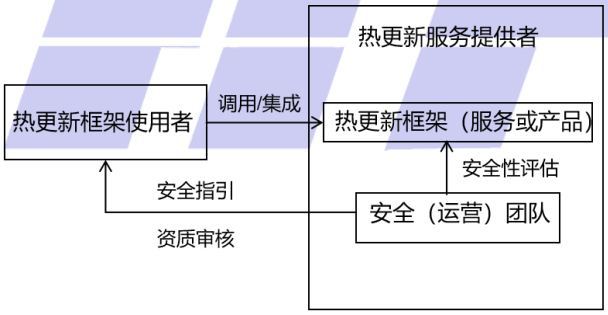

图2 外部提供场景

6 安全要求

热更新框架开发者在设计、研发热更新框架时应确保其安全性，具体应满足以下要求：

a） 不应利用系统漏洞等方式实现APP热更新能力；
b） 应通过数字签名等方式对热更新内容来源进行校验，确保热更新发起方身份的真实性；
c） 涉及通过SDK形式实现热更新能力的，其安全性应满足GB/T 43435-2023第5章的相关要求；
d） 宜通过安全传输协议（如TLS 1.3）实现热更新数据传输过程中的安全性。

7 服务规范

7.1 企业内部使用

涉及仅向企业自有APP或产品使用的热更新框架，应满足以下要求：

a） 应针对热更新框架使用建立权限管控机制和审批流程，仅授权人员或申请授权后可以使用热更新能力；

b） 应记录使用热更新框架的具体日志信息（包括更新内容、版本信息、执行时间、操作人员等），相关记录至少留存六个月；

c） 应对热更新内容应进行内部安全审核，确保更新包体不存在已知的安全漏洞；

d） 宜定期对热更新框架使用情况进行审查，包括使用人员、执行记录、审批流程等。

7.2 对外能力提供

涉及通过闭源产品向第三方提供热更新服务的，服务提供者应满足以下要求：

a） 在热更新服务提供前，应对热更新框架使用者（以下简称为使用者）开发者资质进行审查和评估；

b） 在热更新服务提供前，应通过提供开发指南、开发手册等方式引导使用者正确使用热更新框架，包括明确热更新的使用场景、技术使用红线、异常处理及安全事件说明等；

c） 在热更新服务提供前，应与使用者通过合同等方式，约定热更新能力使用范围，并明确双方在热更新过程中需履行安全职责和义务；

d） 宜向热更新框架使用者提供标准化的代码开发模版，引导使用者正确开展环境配置、初始化、功能调用和调试等操作；

e） 涉及提供代码或组件更新的，应提供内容签名校验能力，确保热更新内容的完整性、不可否认性；

f） 宜对异常热更新行为进行监控（如频繁热更新、后台静默更新等）；

g） 宜集成授权弹窗组件，在APP首次调用热更新框架前向用户申请授权；

h） 应定期开展漏洞发现活动，当发现自身存在漏洞时，应制定漏洞修补方案，并提醒使用者及时更新修复；

i） 应建立应急响应机制，对涉及利用热更新框架引发的安全事件，应配合监管机构进行技术溯源。

电信终端产业协会团体标准

移动应用程序（APP）热更新框架安全服务规范

T/TAF 319—2025

*

版权所有 侵权必究

电信终端产业协会发布
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn