ICS 33.050
CCS M 30

团　体　标　准

T/TAF XXX-XXXX

智能终端侧业务风险防控安全指南

Guidelines for business risk prevention and control security on smart terminal side

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

电信终端产业协会　发布

目　　次

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提出并归口。

本标准起草单位：蚂蚁科技集团股份有限公司、华为技术有限公司、小米通讯技术有限公司、荣耀终端有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、中国信息通信研究院、阿里巴巴（中国）有限公司、北京快手科技有限公司、百度在线网络技术（北京）有限公司、北京奇虎科技有限公司、北京字节跳动科技有限公司、联想（北京）有限公司、国民认证科技（北京）有限公司。

本文件主要起草人：朱丙营、文军、林冠辰、辛知、万小飞、彭晋、王思善、潘双全、王乐、王宝林、任冠一、赵晓娜、罗广文、李根、杨明慧、赵盈洁、宁华、杜云、黄天宁、落红卫、吴月升、唐家伟、郭建领、张屹、姚一楠、王宇晓、李汝鑫、林巍巍、李俊。

智能终端侧业务风险防控安全指南

1 范围

本文件提出智能终端侧的业务风险防控安全框架、模型输入和策略、业务风险定级及安全指南。
本文件适用于智能终端侧的业务风险防控安全能力的设计、集成、应用、检测等活动。

2 规范性引用文件

本文件无规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能终端 smart terminal

具备蜂窝网和互联网（网络）接入功能，可对人或物进行信息采集和处理，支撑业务应用的终端设备。

4 缩略语

下列缩略语适用于本文件。
API：应用程序接口（Application Interface）
APP：应用程序（Application）
ROM：只读存储器（Read Only Memory）
TEE：可信执行环境（Trusted Execution Environment）
IMEI：国际移动设备识别码（International Mobile Equipment Identity）
IMSI：国际移动用户识别码（International Mobile Subscriber Identity）
MAC：媒体访问控制（Media Access Control）
SIM：客户识别模块（Subscriber Identity Module）

5 业务风险防控安全框架

图1给出智能终端侧业务风险防控通用架构，包括业务风险防控能力组件、风控能力接口以及风控策略组件三个部分。风控组件基于安全环境（如TEE等）实现，包括系统风控、应用风控、身份风控模型组件以及风控策略组件，一般集成到智能终端操作系统中或者作为可信的系统服务供智能终端业务应用APP调用。智能终端平台负责给业务风控模型提供输入，风控策略组件根据智输入判断得出当前的风险状况，业务应用APP调用风控接口获得风控判断结果并进行相应处理，从而保障业务安全开展或运行。通过智能终端侧的业务风险防控机制，可实现用户个人、设备相关数据在操作系统层面进行处理，数据不出智能终端即可实现业务风险防控。

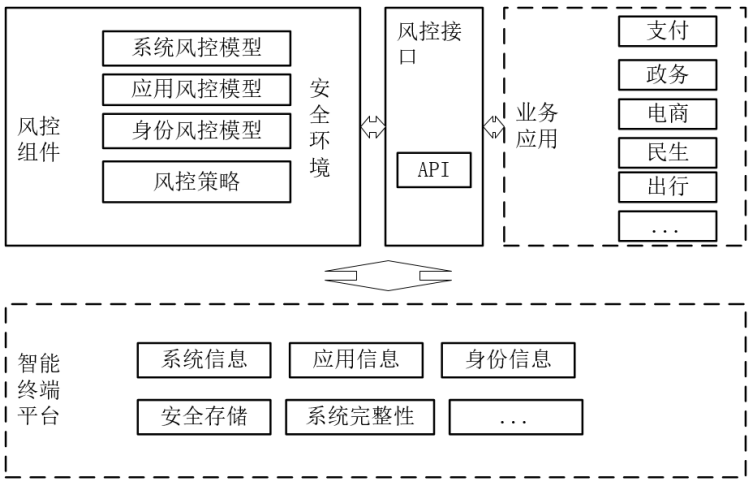

图1　智能终端侧业务风险防控安全框架

注：图中实线框部分为本标准的范围。

6　业务风险防控模型输入和策略

6.1　概述

本章给出了业务风险防控模型考虑的输入和策略。从设备系统角度的输入考虑、安装应用的角度以及用户进行业务三个角度进行划分，分为系统风控模型输入、应用风控模型输入和身份风控模型。本章的模型输入作为模型设计时的参考，基础需求一般需要满足，其它输入依据实际业务需求可能会不一样。

6.2　系统风控模型输入

系统风控模型提供识别系统是否处于风险状态的能力，系统风控模型的输入包括但不限于如下：

a）　是否真实物理智能终端，防止模拟器、云手机等手段（基础需求）；
b）　设备是否被 UNLOCK 及 ROOT（基础需求）；
c）　设备 ROM 是否官方原生，设备是否被刷机（基础需求）；
d）　设备参数是否被篡改，包括 IMEI、MAC、IMSI 篡改（硬件层面的修改）；
e）　系统进程是否被篡改，包括但不限于 system server，com.android.phone 等；
f）　是否被远程控制的能力（针对支付等高安全需求）；
g）　是否对当前屏幕录制（针对支付等高安全需求）；
h）　是否共享当前屏幕（针对支付等高安全需求）；
i）　提供持久化终端存储及针对该存储的增、删、改、查能力，用于标识设备风险。

注：基础需求为模型正常运行需具备的需求，下同。

6.3　应用风控模型输入

应用风控模型主要提供识别应用是否处于风险状态的能力，该模型通过可靠的安全机制或者能力识别应用，应用风控模型的输入包括但不限于如下：

a）　应用的数字证书是否合法（基础需求）；
b）　应用执行流程在运行时是否被篡改；
c）　是否安装恶意应用及恶意应用的活动；

d) 是否被多开应用启动；
e) 应用是否在当前设备首次安装。

6.4 身份风控模型输入

身份风控模型提供识别身份是否处于风险状态的能力，该能力通过可靠的安全机制识别用户真实身份，如识别正常用户，初级黑灰产，高级黑灰产，黑客等，身份风控模型的输入包括但不限于如下：

a) 按键行为是否真实（基础需求）；
b) 最近特定天数重置/刷机的次数，用于识别黑灰产常用的设备归零操作（基础需求）；
c) 设备的调试状态（基础需求）；
d) 是否是网络代理；
e) 是否安装 SIM 卡；
f) 是否是本人或者真实人操作；
g) 是否无位移，位置固定或悬空状态。

6.5 业务风险防控策略

风控策略动态调整不同维度风控能力项的权重，输入不同的风控模型构建相应的安全能力。风控策略一般预置在安全环境中，根据业务需求快速匹配并构建相应的安全能力。根据业务需要，可动态下发、更新风控策略。

7 业务风险定级

7.1 业务风险定级原则和方法

智能终端侧的业务风险可分为高级、中级、低级、无风险四个等级。智能终端侧的业务风险定级原则包括：

a) 就高不就低；
b) 风险累积则级别提升。

智能终端侧的业务风险定级可以从系统风控、应用风控以及身份风控三个维度判断，只要有一个维度风险为高级（或中级）风险，则智能终端侧的业务风险定为高级（中级）。如果多个低级（或中级）风险出现，则风险定级可以分别上升为中级（或高级）。

7.2 通用风险评估方法示例

6.1、6.2、6.3中的各单项风险分值为10分，总风险分值为各单项分值之和。总风险分值反馈给业务应用，供业务应用决策参考；或者通过分级原则确定风险等级，反馈给业务应用。

8 业务风险防控安全要求

系统风控模型、应用风控模型、身份风控模型以及风控策略应部署在安全环境中，防止模型、策略以及相关数据被篡改，风控策略文件应储存在安全环境中。

应建立安全通道并进行加密和加签，以保障模型的下发、风控策略的更新以及风险等级数据传输的安全，保障数据的保密性和可靠性。

附 录 A
（资料性）
业务风险防控接口

A.1 接口描述

业务风险防控接口描述如下所示：

```
/*
 * java Risk Monitor 统一接口定义
 * @param1: app_name 标识app调用者名称，用于辅助风控模块进行访问控制
 * @param2: command ID 执行命令，用于功能
 *@param3: in_param 输入数据，部分命令需要辅助参数，也可为空
 *@return ： 返回命令执行结果，统一为byte数组类型，
*/
byte[] riskMonitorInvoke (String app_name, int commandID, byte[] in_param) throws RiskMonitorException;
```

A.2 commandID 定义

commandID 定义如下所示：

```
    enum {
        GET_VERSION,  /*获取RiskMonitor相关模块版本信息，包括系统模块、安全应用、风控策略配置版本信息 */
        GET_RISK_SCORE, /* 获取风险评估分数，可以通过in_param 指定风险域*/
        GET_RISK_MAX_VALUE,/* 获取各风险域下风险值的最大值 */
        SPECIFIED_RISK_OPT,/*APP定制策略命令执行，根据in_param 指定定制参数 */
        UPDATE_RISK_CONFIG, /*更新风控策略配置，包括系统通用策略和APP定制策略*/
        RESERVED /* 预留，暂不实现 */
}
```

A.3 风险域定义

风险域定义如下所示：

```
enum{
        SYSTEM, /* 系统风险 */
        APPLICATION,/* 应用风险 */
        IDENTITY, /* 身份风险 */
        SPECIFIED, /* APP自定义风险策略 */
        RESERVED /* 预留，暂不实现 */
}
```

A.4 定制策略命令说明

定制策略用于厂商特殊类型应用如安全应用、金融应用定制的风控能力扩展。扩展功能通过in_param参数区分。

电信终端产业协会团体标准

智能终端侧业务风险防控安全指南

T/TAF XXX—XXXX

*

电信终端产业协会印发
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