ICS 33.060
M 36

团　　体　　标　　准

T/TAF　XXXX—XXXX

移动智能终端补充设备标识规范

Specifications for supplementary device identification of smart mobile terminal

点击此处添加与国际标准一致性程度的标识

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

电信终端产业协会　　发 布

目　　次

前　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由移动安全联盟提出并归口。

本标准起草单位：中国信息通信研究院、北京小米移动软件有限公司、维沃移动通信有限公司、广东欧珀移动通信有限公司、华为技术有限公司

本标准主要起草人：翟世俊、杨正军、陈婉莹、赵驰、焦四辈、梅敬青、宫建涛、周圣炎

引　言

随着大数据时代的到来，数据的价值也逐渐增加。同时各国对用户隐私保护的要求越来越高，传统的移动智能终端设备标识如国际移动设备识别码（IMEI）等已被部分国家认定为用户隐私的一部分。另外，在很多与隐私无关的场景中，如生产、售后、报关、政府抽检等场景，传统设备标识（如IMEI）被篡改或冒用的情况时有发生，给设备生产企业的经济利益带来损失，同时对设备追溯带来较大影响。因此,有必要制定符合各国隐私保护要求,同时能够满足不同行业需求的移动智能终端补充设备标识体系。

本规范旨在规范移动智能终端补充设备标识体系的体系架构、功能要求、接口要求以及安全要求。规范设备生产企业遵循标准要求开发统一接口调用方式，方便移动应用接入、减小维护成本。移动应用可通过软件开发工具包访问移动智能终端补充设备标识符。

移动智能终端补充设备标识规范

1 范围

本标准规定了移动智能终端补充设备标识体系的体系架构、功能要求、接口要求以及安全要求。

本标准适用于各种制式的移动智能终端，个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

移动智能终端 Smart Mobile Terminal

能够接入移动通信网，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用软件的移动终端。

3.1.2

移动智能终端操作系统 Operator System of Smart Mobile Terminal

移动智能终端最基本的系统软件，它控制和管理移动智能终端各种硬件和软件资源，并提供应用程序开发接口。

3.1.3

移动智能终端应用软件 Mobile Application

移动智能终端应用软件包括移动智能终端预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.1.4

用户 User

使用移动智能终端资源的对象，包括人或第三方应用程序。

3.2 缩略语

下列缩略语适用于本文件。

IMEI	International Mobile Equipment Identity	国际移动设备识别码
UDID	Unique Device Identifier	设备唯一标识符
OAID	Open Anonymous Device Identifier	匿名设备标识符
VAID	Vender Anonymous Device Identifier	开发者匿名设备标识符
AAID	Application Anonymous Device Identifier	应用匿名设备标识符

4 补充设备标识体系架构概述

补充设备标识体系的总体架构如下图所示。

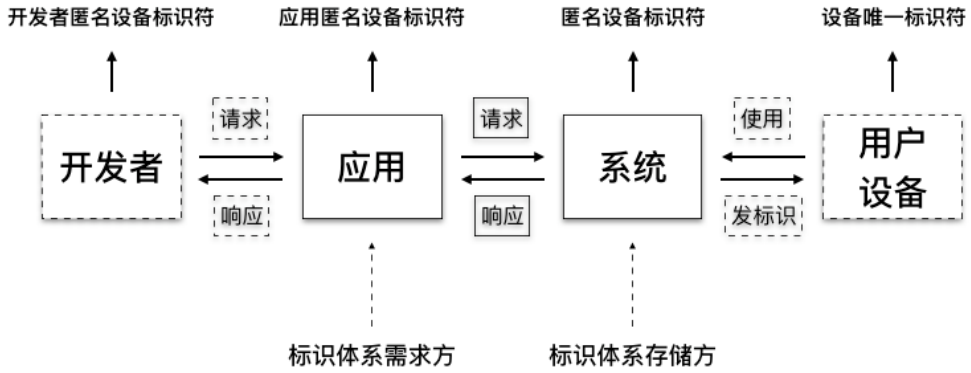

图1 补充设备标识体系的总体架构

移动智能终端补充设备标识体系架构共涉及四类实体，包括开发者、开发者开发的应用软件、移动智能终端设备的操作系统、用户及用户使用的设备。为保护用户用户的隐私和标识设备的唯一性，根据不同使用对象和不同用途，基于移动智能终端设备，分别生成设备唯一标识符、匿名设备标识符、开发者匿名设备标识符和应用匿名设备标识符，将这四个设备标识符构成补充设备标识体系。

英文缩写	中文名称	英文全称	长度
UDID	设备唯一标识符	Unique Device Identifier	最长 64 位
OAID	匿名设备标识符	Open Anonymous Device Identifier	最长 64 位
VAID	开发者匿名设备标识符	Vender Anonymous Device Identifier	最长 64 位
AAID	应用匿名设备标识符	Application Anonymous Device Identifier	最长 64 位

设备唯一标识符是指设备唯一硬件标识，设备生产时根据特定的硬件信息生成，可用于设备的生产环境及合法性校验。

匿名设备标识符是可以连接所有应用数据的标识符，移动智能终端系统首次启动后立即生成，可用于广告业务。

开发者匿名设备标识符是指用于开放给开发者的设备标识符，可在应用安装时产生，可用于同一开发者不同应用之间的推荐。

应用匿名设备标识符是指第三方应用获取的匿名设备标识，可在应用安装时产生，可用于用户统计等。

应用向系统发送获取设备标识的请求时，系统需要对应用采取合适的手段进行身份验证，并验证其请求符合策略规定，才可将结果返回给应用。

UDID 、OAID、VAID和AAID这四个设备标识符之间不存在映射关系。

5 补充设备标识体系的功能要求

5.1 设备唯一标识符功能要求

5.1.1 设备唯一标识符的生成

设备唯一标识符可在移动智能终端生产时生成，并内置于移动智能终端中，也可在调用设备唯一标识符时生成。

设备唯一标识符的可利用硬件参数、随机参数等生成参数通过加密算法生成。

5.1.2 设备唯一标识符特性

设备唯一标识符具有以下特性：

(1) 不可逆：通过加密算法生成的设备唯一标识符不能够被反向追踪。

(2) 唯一性：生成参数中包括硬件参数，确保生成的设备唯一标识符的唯一性。

(3) 封闭性：设备唯一标识符仅可被授权的应用访问。

(4) 一致性：设备唯一标识符不因恢复出厂设置、用户操作而改变。

(5) 不可篡改性：设备唯一标识符的生成参数中包含硬件参数，且不能被未授权方修改。

5.1.3 设备唯一标识符的重置

设备唯一标识符在移动智能终端出厂后无法重置。

5.1.4 设备唯一标识符的开启\关闭受控机制

移动智能终端应不提供设备唯一标识符的开启\关闭受控机制，设备唯一标识符无法关闭。

5.2 匿名设备标识符功能要求

5.2.1 匿名设备标识符的生成

匿名设备标识符在移动智能设备系统首次启动后生成。

匿名设备标识符生成参数中可包含设备唯一标识符等参数。

5.2.2 匿名设备标识符的特性

匿名设备标识符具有以下特性：

(1) 可关闭性：匿名设备标识符可以被用户关闭。

(2) 连接性：匿名设备标识符可以链接所有应用数据。

5.2.3 匿名设备标识符的重置

发生下述事件时，匿名设备标识符重置：

(1) 用户在系统设置中手动重置，匿名设备标识符将重置；

(2) 移动智能终端恢复出厂设置时，匿名设备标识符将重置；
(3) 匿名设备标识符自身可定期重置。
重置后生成新的匿名设备标识符，且应用只能获取新的匿名设备标识符。

5.2.4 匿名设备标识符的开启\关闭受控机制

移动智能终端应提供匿名设备标识符的开启\关闭受控机制，用户可以选择在系统设置中关闭匿名设备标识符；关闭后，应用获取到的匿名设备标识符的返回值为NO。

5.3 开发者匿名设备标识符功能要求

5.3.1 开发者匿名设备标识符的生成

开发者匿名设备标识符可在应用安装时生成，首先通过开发者账号判断该设备中是否已存在该账号对应的开发者匿名设备标识符，如果不存在或目前没有安装该开发者的其他应用，则生成新的开发者匿名设备标识符，否则返回已有开发者匿名设备标识符。
开发者匿名设备标识符生成参数中可包含设备唯一标识符等参数。

5.3.2 开发者匿名设备标识符的特性

开发者匿名设备标识符的具有以下特性：
(1) 同一个设备上，同一个开发者开发的多个应用，开发者匿名设备标识符取值相同；
(2) 同一个设备上，不同开发者开发的的应用，开发者匿名设备标识符取值不同；
(3) 不同设备上，同一个开发者的应用，开发者匿名设备标识符取值不同；
(4) 不同设备上，不同开发者的应用程序，开发者匿名设备标识符取值不同。

5.3.3 开发者匿名设备标识符的重置

发生下述事件时，开发者匿名设备标识符重置：
(1) 同一设备上，同一开发者的全部应用被卸载后，重新安装该开发者开发的应用时，该开发者在此台设备上的开发者匿名设备标识符将重置；
(2) 移动智能终端恢复出厂设置，所有应用的开发者匿名设备标识符将重置；
(3) 开发者匿名设备标识符自身可定期重置。
重置后生成新的开发者匿名设备标识符，且应用只能获取新的开发者匿名设备标识符。

5.3.4 开发者匿名设备标识符的开启\关闭受控机制

移动智能终端应不提供开发者匿名设备标识符的开启\关闭受控机制，开发者匿名设备标识符不可关闭。

5.4 应用匿名设备标识符功能要求

5.4.1 应用匿名设备标识符的生成

应用匿名设备标识符可在应用安装时生成，生成参数中可包含设备唯一标识符等参数。

5.4.2 应用匿名设备标识符的特性

应用匿名设备标识符具有以下特性：
(1) 匿名化、无隐私风险：应用匿名设备标识符和已有的任何标识符都不关联，并且每个应用只能访问自己的匿名设备标识符。

(2) 同一个设备上，同一个开发者的多个应用，应用匿名设备标识符取值不同；
(3) 同一个设备上，不同开发者的应用，应用匿名设备标识符取值不同；
(4) 不同设备上，同一个开发者的应用，应用匿名设备标识符取值不同；
(5) 不同设备上，不同开发者的应用程序，应用匿名设备标识符取值不同。

5.4.3 应用匿名设备标识符的重置

发生下述事件时，应用匿名设备标识符重置：
(1) 同一设备上，应用被卸载后，重新安装该应用时，该应用在此台设备上的应用匿名设备标识符将重置；
(2) 移动智能终端恢复出厂设置，应用匿名设备标识符将重置；
(3) 应用匿名设备标识符自身可定期重置；
(4) 点击系统设置内的清除数据，应用匿名设备标识符将重置。
重置后生成新的应用匿名设备标识符，且应用只能获取新的应用匿名设备标识符。

5.4.4 应用匿名设备标识符的开启\关闭受控机制

移动智能终端应不提供应用匿名设备标识符的开启\关闭受控机制,应用匿名设备标识符不可关闭。

6 补充设备标识获取接口要求

补充设备标识获取接口包括补充设备标识状态获取接口、匿名设备标识符获取接口、开发者匿名设备标识符获取接口和应用匿名设备标识符获取接口。

设备唯一标识符仅可被授权的应用访问。

6.1 补充设备标识状态获取接口

该接口用于获取移动智能终端是否支持补充设备标识体系，确认支持后，可以继续获取所需设备标识符。

```
public static boolean isSupported()
```

参数	返回	说明
无	boolean：是否支持补充设备标识符获取	true为支持，false为不支持

6.2 匿名设备标识符获取接口

```
public static String getOAID(Context context)
```

参数	返回	说明
Context：应用的Application Context	String：返回匿名设备标识符或异常状态	匿名设备标识符最长64位，返回null表示不支持，异常状态包括网络异常、appid异常、应用异常等

6.3 开发者匿名设备标识符获取接口

public static String getVAID(Context context)

参数	返回	说明
Context：应用的Application Context	String：返回开发者匿名设备标识符或异常状态	开发者匿名设备标识符最长64位，返回null表示不支持，异常状态包括网络异常、appid异常、应用异常等

6.4 应用匿名设备标识符获取接口

public static String getAAID(Context context)

参数	返回	说明
Context：应用的Application Context	String：返回应用匿名设备标识符或异常状态	应用匿名设备标识符最长64位，返回null表示不支持，异常状态包括网络异常、appid异常、应用异常等

7 补充设备标识安全要求

7.1 访问控制

对于来自应用的请求进行验证，访问过程应是安全可信的，应只接受通过认证的对象的访问。同时应对敏感数据进行访问权限控制。

7.2 存储安全

设备标识体系的存储应确保完整性和隐私性，不可被其它非法实体访问或篡改。证书、密钥等安全数据需要加密存储。

7.3 防篡改攻击

应对程序的完整性、参数内容的完整性和有效性进行检查，以防御篡改攻击。

附 录 A
（规范性附录）

参 考 文 献