

智能终端匿名标识符数据安全技术要求

一、项目信息			
中文名称	智能终端匿名标识符数据安全技术要求		
英文名称	Technical requirements for data security of anonymous identifiers in smart terminals		
标准类别	<input checked="" type="checkbox"/> 安全 <input type="checkbox"/> 卫生 <input type="checkbox"/> 环保 <input type="checkbox"/> 基础 <input type="checkbox"/> 方法 <input type="checkbox"/> 管理 <input type="checkbox"/> 产品 <input type="checkbox"/> 其他		
制定/修订	<input checked="" type="checkbox"/> 制定 <input type="checkbox"/> 修订	被修订标准号	
ICS	35.030	CCS	L70
技术归口单位 (或技术委员会)	工业和信息化部		
起草单位	中国信息通信研究院、OPPO 广东移动通信有限公司、维沃移动通信有限公司、北京抖音信息服务有限公司等		
项目周期	<input type="checkbox"/> 6 个月 <input type="checkbox"/> 12 个月 <input type="checkbox"/> 16 个月 <input checked="" type="checkbox"/> 18 个月 <input type="checkbox"/> 22 个月		
是否同步制定外文版	<input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否		
二、目的、意义			
目的、意义	<p>智能终端匿名标识符是指由终端操作系统或设备厂商提供的匿名字符串，可用于标识互联网中终端设备的数据信息，是移动互联网生态的基础，在数字经济的发展中具有不可或缺的重要作用。鉴于 IMEI 等传统设备标识与设备终身绑定，用户无法自行更改或重置，我国于 2018 年提出匿名标识符（OAID），在保障用户隐私安全的基础上，有效应用于广告转投放归因监测、个性化内容推荐、安全风险防控等商业场景，实现用户权益保护与产业商业价值的平衡。但在匿名标识符应用过程中，还存在开关及重置路径复杂、开关名称不清晰、关闭后返回机制不统一等问题；且在标识收集及使用过程中，部分收集使用方未遵循“最小必要”原则，存在超范围收集及使用的违规情形。</p> <p>为落实《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规要求，有必要对智能终端匿名标识符的技术实现及使用提出要求，明确其生成、</p>		

	开关、重置相关的功能及要求，进一步强化安全和收集使用要求。
三、范围和主要技术内容	
范围和主要技术内容	<p>本文件规定了智能终端匿名标识符的功能要求、安全要求及收集使用要求。本文件适用于移动智能终端、智能网联汽车、智能家居等终端设备匿名标识符及互联网应用程序收集使用匿名标识符的设计、开发、测试和评估，个别条款不适用于特殊行业终端、专业应用。技术内容包括：</p> <p>一、功能要求：</p> <ol style="list-style-type: none"> 1 匿名标识符的生成 2 匿名标识符的开关 3 匿名标识符的重置 <p>二、安全要求</p> <ol style="list-style-type: none"> 1 数据收集 2 数据存储 3 数据使用 4 数据传输 5 数据提供 <p>三、互联网应用程序收集使用匿名标识符安全要求</p> <p>四、软件开发工具包收集使用匿名标识符安全要求</p>
国内外情况简要说明	<p>鉴于 IMEI 等传统设备标识与设备终身绑定，用户无法自行更改或重置，随着全球数据安全与隐私保护要求的提升，苹果与谷歌两大主流操作系统厂商分别推出了非永久性且可重置的广告标识符 IDFA（Identifier For Advertising）、GAID（Google Advertising Identifier）。我国于 2018 年提出匿名标识符（OAID），在保障用户隐私安全的基础上，有效应用于广告转投放归因监测、个性化内容推荐、安全风险防控等商业场景，实现用户权益保护与产业商业价值的平衡。</p>
备注	