ICS 33.050
CCS M 30

团　体　标　准

T/TAF 129—2022

移动互联网应用超文本传输协议状态（Cookie）技术隐私保护指南

Privacy protection guide of hypertext transfer protocol status (Cookie) technology in mobile applications

2022-09-15 发布　　2022-09-15 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。

本文件中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。

本文件起草单位：中国信息通信研究院、北京抖音信息服务有限公司、泰尔认证中心有限公司、阿里巴巴(中国)有限公司、北京快手科技有限公司、华为技术有限公司、OPPO广东移动通信有限公司、北京奇虎科技有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：王宇晓、李昳婧、武林娜、李梦月、杨骁涵、谭德芳、安潇羽、黄若、田申、刘凯红、赵云、常琳、陈思宇、宁华、黄天宁、落红卫、衣强、李腾、姚一楠、刘献伦。

引　　言

随着移动互联网的迅速发展和日益成熟，Cookie技术作为实现网络服务功能的基础功能，在自动登录、购物车、视频续放、广告等方面都得到了广泛的应用。但随着《个人信息保护法》、《数据安全法》等相关法律法规的发布，用户个人信息保护及其相关问题被国家和社会普遍关注，而Cookie技术的滥用可能造成用户个人信息泄漏，侵犯用户的知情权和选择权。

根据《网络安全法》、《个人信息保护法》、《数据安全法》等相关法律要求，给出移动互联网应用Cookie技术隐私保护实践指导，旨在避免因不合理使用Cookie技术处理用户个人信息而造成用户权益损害，进一步促进移动互联网行业的健康稳定发展。

移动互联网应用超文本传输协议（Cookie）技术隐私保护指南

1 范围

本文件提供了移动互联网应用使用Cookie技术处理用户个人信息时的典型应用场景、安全风险、处理原则以及相应保护措施。

本文件适用于指导和建议移动互联网应用对Cookie技术的应用，也适用于第三方评估机构等组织对移动互联网应用进行监督、管理和评估。

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 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 35273界定的以及下列术语和定义适用于本文件。

3.1

移动智能终端 smart mobile terminal

能够接入移动通信网，具有能够提供应用软件开发接口的操作系统，具有安装、加载和运行应用软件能力的终端。

3.2

移动应用软件 mobile application

针对移动智能终端所开发的应用程序，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智能终端下载、安装、升级、卸载的应用软件。

3.3

个人信息 personal information

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.4

敏感个人信息 personal sensitive information

一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

4 Cookie 技术及业务场景

4.1 Cookie 简介

Cookie 是一段不超过 4KB 的小型文本数据，由键值对及其控制属性组成，服务器将其存储在用户本地终端，主要用于在 HTTP 无状态的情况下实现用户会话状态维持，每次向服务器发送请求时都会同时将该信息发送给服务器，服务器收到请求后，可以根据该信息处理请求。

根据移动互联网常见应用处理关系可将Cookie分类为第一方和第三方。

移动互联网应用程序开发过程中原生网络服务或WebView网络请求均可涉及Cookie技术的使用。移动互联网应用场景WebView组件的业务场景多见于第三方服务，如广告、电商、网页客服等。

4.2 Cookie 业务场景分类

移动互联网应用的业务功能中，根据其使用目的和业务功能场景，可将Cookie分为功能型、安全型、分析型、广告营销型等四种常见类别，业务场景分类可见表1。

a) 功能型Cookie主要用于为用户提供网络功能服务，维护会话状态如登录、页面偏好设置、功能状态记录等；
b) 安全型Cookie主要用于风控服务下验证用户身份，避免恶意攻击以保证用户安全以及打击作弊行为维护网络服务的安全性；
c) 分析型Cookie主要用于记录用户与特定服务的互动情况，如记录网页点击情况，用于产品内容改进和提高用户体验，移动互联网应用通常不直接使用Cookie方式进行广告统计、分析，常见于WebView形式的第三方服务；
d) 营销型Cookie主要用于广告投放、个性化以及衡量广告效果，移动互联网应用通常不直接使用Cookie用于广告统计、分析，常见于WebView形式的第三方服务。

表1 Cookie常用业务场景分类

类别	业务场景	实际用途
功能型	登录	用于维持用户登录状态
	匿名标识	用于缓存功能，降低服务器压力
	偏好设置	用于偏好设置记录如语言、页面颜色等
	页面功能状态记录	用于记录页面功能状态，如是否自动播放下一个等
安全型	风控	用于常规账号安全风控策略，避免薅羊毛、刷单等安全风险
	防范CSRF攻击	用于保证安全服务，防止被恶意攻击
分析型	功能互动、性能及数据分析	--
营销型	广告投放、监测及个性化	--

5 Cookie 处理基本原则及处理措施

5.1 基本原则

5.1.1 合法正当原则

基于合法、正当目的利用Cookie技术开展个人信息处理活动。

5.1.2 最小必要原则

只处理为实现该功能所必需的最少个人信息，目的达成后及时删除个人信息。

5.1.3 目的明确原则

具有明确、清晰、具体的个人信息处理目的。

5.1.4 公开透明原则

以清晰、简洁、易懂、易于接受的方式公开处理个人信息的范围、目的、规则。

5.2 安全及隐私保护措施

移动互联网应用对Cookie的设计、处理需符合5.1基本原则。

5.2.1 安全措施

移动互联网应用在使用Cookie技术时，宜满足以下安全措施。不同类别和功能的Cookie应用根据需求，采取不同的安全措施，不可恶意窃取Cookie。

a) 使用适当的算法生成Cookie保证其自身的不可预测性，避免被暴力破解和伪造攻击；
b) 单独且正常配置Cookie的安全属性，如开启Cookie的HttpOnly参数、设置Secure属性等，避免跨站攻击等导致Cookie泄漏风险；
c) Cookie需要配合签名技术使用，避免其数据被篡改；
d) Cookie需要加密或安全传输协议等进行传输，避免数据被窃取；
e) Cookie本地存储时需要加密或采取访问控制等技术确保避免泄露。

5.2.2 隐私保护措施

5.2.2.1 告知同意

若因业务功能需要通过Cookie处理个人信息时，需基于用户同意或其他合法性基础进行个人信息处理活动。若基于用户同意处理个人信息的，在收集使用前对用户进行充分告知。告知同意方式可根据产品或服务的业务功能特点，可多种方式组合并行包括且不限于页面文案、链接、交互界面、浮窗等。

告知同意方式可见以下要求：

a) 若APP或其集成的第三方代码、插件等通过Cookie处理个人信息的，可采取个人信息保护政策等方式告知用户其处理的种类、目的、方式，并征得同意；
b) 若APP集成的第三方网页服务通过Cookie技术处理个人信息的，第三方网页服务单独告知用户其处理的个人信息种类、目的、方式，并征得同意。

若业务功能使用 Cookie 而不处理个人信息的，在使用 Cookie 前，宜告知用户其相应用途，不再征得用户同意。

5.2.2.2 Cookie 处理措施

Cookie处理措施包括以下内容：

a) 不以误导、欺诈等方式利用Cookie窃取用户的个人信息；
b) 通过Cookie进行个人信息处理活动的，需要获得用户授权或具备其他合法性基础；
c) 通过Cookie进行个人信息处理活动的，其处理个人信息的种类、目的和方式需要遵循最小必要原则，不超出实际需要的功能或业务场景处理个人信息，如静态图片资源访问不在Cookie中处理个人信息；
d) 若需通过Cookie处理个人信息时，其涉及的个人信息种类、频率需要满足最小必要原则；
e) APP访问其集成第三方网页服务时，不可将其Cookie内容传递给第三方网页；
f) 若需通过Cookie处理个人信息时，个人信息类别包括网络身份标识、上网浏览记录信息，不可包括其他类别的个人信息或敏感个人信息。不同业务场景下可处理的个人信息类别可见表2，若存在其他业务功能场景可根据5.1基本原则另行评估。

表2　不同业务场景下可处理的个人信息类别参考

类别	业务场景	可处理的个人信息类别
功能型	登录	网络身份标识
	匿名标识	网络身份标识
	页面偏好设置	上网浏览记录信息
	功能状态记录	上网浏览记录信息
安全型	风控	网络身份标识
	防范CSRF攻击	网络身份标识
分析型	功能互动、性能及数据分析	网络身份标识、上网浏览记录信息
营销型	广告投放、监测及个性化	网络身份标识、上网浏览记录信息

5.2.2.3　Cookie 存储要求

Cookie存储在本地时，若包括个人信息，移动互联网应用将其存储在移动智能终端受控存储空间，避免非授权访问而导致泄露。

5.2.2.4　Cookie 保存时间

Cookie保存时间包括以下内容：

a) Cookie的保存时间需要遵循最小必要原则，设置为满足业务功能的最短时间。不同类别及业务场景下Cookie保存时间可见表3，APP可视实际情况降低相应保存时间，不宜超出。若存在其他业务功能场景可根据5.1基本原则另行评估。

注：保存时间的计算根据用户最后活跃时间开始进行统计，用户主动触发相关功能后保存时间可重新开始计数。

b) 宜为用户提供可选择的有效保存时间选项，并清晰说明不同保存时间下可能造成的用户使用体验影响。

表3　不同类别及业务场景保存时间参考

类别	业务场景	Cookie性质	保存时间
功能型	登录	持久性	30天
	匿名标识	持久性	7天

表3　不同类别及业务场景保存时间参考（续）

类别	业务场景	Cookie性质	保存时间
功能型	页面偏好设置	持久性	90天
	功能状态记录	会话性	会话结束
安全型	风控	持久性	7天
	防范CSRF攻击	持久性	30天
分析型	功能互动、性能及数据分析	--	--
营销型	广告投放、监测及个性化	--	--

5.2.2.5　删除要求

删除要求包括以下内容：

a）APP 需对超出保存时间的 Cookie 及时清除；

b）APP 宜为给用户提供清除缓存路径说明，便于用户删除 Cookie；

c）APP 提供的网页服务若使用 Cookie 并包含个人信息，可提供单独的清除 Cookie 功能。

附 录 A
（资料性）
Cookie 技术应用常见风险

Cookie技术在实际应用过程中，存在安全、个人信息安全等多种风险。表A.1给出详细的风险情况描述。

表A.1 Cookie技术应用常见风险举例

序号	类型	风险描述
1	Cookie 篡改	Cookie存储在移动智能终端本地，容易被获取。若在无其他防篡改机制如签名校验的情况下，容易被修改来获取不同级别的访问权限，存在较高的安全风险。
2	Cookie劫持	WebView组件通过JS脚本可轻易获取本地存储的Cookie。WebView组件没有默认严格限制安全策略，而是提供了多个API接口来定制化配置。若开发者若未设置安全的属性，易被劫持、被跨域访问攻击，存在较高的安全风险。特别是在记录登录状态等业务场景下，可通过Cookie替代原始身份访问服务器。
3	Cookie 作用域设置不当	Cookie可通过Domain和Path属性来设置其作用域，业务功能场景下，需要不同的域名共享Cookie。如果作用域范围设置过大，将会导致非预期的Cookie访问情况，如通过伪造更小作用域的Cookie覆盖原始内容，存在较高的安全风险。
4	违规收集个人信息	未经用户同意或未具备其他合法性基础，通过Cookie技术采集、处理或窃取个人信息。
5	超范围收集个人信息	超范围收集个人信息，非功能或服务所必须，利用Cookie技术处理超出最小必要范围的个人信息，如在Cookie中存储位置信息、账号密码等。
		超频次收集个人信息，非功能或服务所必须，利用Cookie技术超出最小必要频次传输个人信息。
6	Cookie 敏感数据泄露	若Cookie中包含敏感个人信息如身份证号、密码等，在非安全传输信道（TLS）传输传输时，容易被窃取造成个人信息泄漏。
		若Cookie中包含敏感个人信息如身份证号、密码，并将其明文存储在移动智能终端本地，容易被窃取造成个人信息泄露。

电信终端产业协会团体标准

移动互联网应用超文本传输协议状态（Cookie）技术隐私保护指南

T/TAF 129—2022

*

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