GD

中华人民共和国广播电视和网络视听行业技术文件

GD/J 120—2020

PGC 移动终端安全技术要求

Technical requirements for security capability of PGC system mobile terminal

2020－09－28 发布　　2020－09－28 实施

国家广播电视总局科技司　　发 布

目　　次

前　言

本技术文件按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别这些专利的责任。

本技术文件由国家广播电视总局科技司归口。

本技术文件起草单位：国家广播电视总局广播电视规划院、中央广播电视总台、北京电视台、上海文化广播影视集团有限公司、腾讯科技（北京）有限公司、北京奇安信科技有限公司、北京奇虎科技有限公司、北京华云安信息技术有限公司、北京时代远景信息技术研究院有限公司、北京汇智云科技有限公司。

本技术文件主要起草人：肖辉、琚宏伟、邓晖、朱剑、王立冬、李程、王燕青、邵勇、杨君蔚、蒋晓峰、胡恺、常树磊、董升来、赵占永、陈奇、王祥刚、王彦磊、沈传宝、张屹、石毅、万会来、张海峰、路琨、李安颖、吕大垒。

PGC移动终端安全技术要求

1 范围

本技术文件规定了PGC移动终端硬件安全要求、操作系统安全要求、应用安全要求、网络准入安全要求、数据交换安全要求和用户信息数据安全要求。

本技术文件适用于PGC移动终端的安全设计、开发、运行和维护。

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。

YD/T 1699—2007 移动终端信息安全技术要求

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

PGC系统 professionally generated content system

通过通讯传输网络实现媒体内容采集、制作、交互的专业系统。

3.1.2

PGC移动终端 professionally generated content terminal

用于PGC系统的移动终端。

3.1.3

PGC应用 professionally generated content software

安装在PGC移动终端上，实现PGC拍摄、编辑、直播连线和文件回传等功能的应用软件。

3.1.4

用户信息数据 user information data

PGC系统内，用于管理用户使用权限的相关数据。

3.2 缩略语

下列缩略语适用于本文件。

PGC 专业生产内容（Professionally Generated Content）

4 概述

PGC移动终端主要实现拍摄、编辑、直播连线和文件回传等功能。PGC移动终端安全主要由硬件安全、操作系统安全、应用安全、网络准入安全、数据交换安全和用户信息数据安全六部分构成。

5 安全技术要求

5.1 硬件安全要求

PGC移动终端硬件应符合YD/T 1699—2007中第6章的要求。

5.2 操作系统安全要求

5.2.1 标识与鉴别

PGC移动终端应满足如下标识与鉴别要求：

a) 应具备唯一用户标识，并能鉴别执行指令的来源；
b) 应对用户进行身份鉴权，如使用口令登录，登录策略应支持设置口令长度不小于8位字符，口令中应包含数字、英文字母和符号；
c) 登录PGC移动终端需至少采用两种身份鉴别技术，包括采用口令、密码技术、生物技术（包括指纹识别、面部识别、虹膜识别等生物识别技术），且其中一种鉴别技术至少应使用密码技术来实现。

5.2.2 访问控制

PGC移动终端应满足如下访问控制要求：

a) 系统应具有权限管理功能，不同用户应仅被授予完成任务所需的最小权限；
b) 系统访问控制能力范围应覆盖相关所有主体、客体以及它们之间的操作；
c) 可对客户端远程控制，实现客户端的远程管理和应急处理。

5.2.3 安全审计

PGC移动终端应满足如下安全审计要求：

a) 应能为操作系统事件生成审计记录，审计记录应包括日期、时间、操作类型等信息；
b) 应保护已存储的操作系统审计记录，以避免未授权的修改、删除、覆盖等；
c) 应能实现对PGC移动终端安全审计，审计所有PGC移动终端设备登录日志、安装日志、运行日志、错误日志、终端设备连接中断、删除日志等；
d) 应能保证审计日志保存6个月及以上，并能下载到本地或回传到统一审计系统。

5.2.4 系统更新

系统更新应在固件与应用软件兼容性测试通过后方可进行，PGC移动终端提供的固件远程更新功能，应满足如下要求：

a) 在固件远程更新时，应对固件采用签名的方式进行来源和完整性验证；
b) 在固件远程更新失败时，应具备报警功能，应可以回退至原来版本。

5.2.5 系统漏洞

系统不应具有高、中危漏洞；应定期进行补丁更新和系统版本升级，定期对PGC移动终端进行漏洞检测，及时发现系统漏洞并及时进行修补。

5.2.6 失效保护

应能自检出已定义的设备故障并进行告警，确保设备未受故障影响部分的功能正常。

5.3 应用安全要求

5.3.1 认证签名

应用软件应包含签名信息，且签名信息真实可信。

5.3.2 身份鉴别

PGC移动终端应用软件身份鉴别，应满足如下要求：

a) PGC 移动终端应用软件应对用户身份进行鉴别，并提供鉴别失败或登录超时的处理措施；
b) PGC 移动终端应用软件中的用户账号口令在使用过程中不应以明文形式显示和存储，并具备口令复杂度检查机制和修改或找回口令的验证机制；
c) 不得使用第三方账户授权，如微信、微博、QQ 等；
d) 登录 PGC 应用需至少采用两种身份鉴别技术，包括采用口令、密码技术、生物技术（包括指纹识别、面部识别、虹膜识别等生物识别技术），且其中一种鉴别技术至少应使用密码技术来实现。

5.3.3 访问控制

PGC移动终端应用软件应满足如下访问控制要求：

a) 授权用户访问的内容不能超出授权的范围；
b) 限制应用用户账号的多重并发会话；
c) 应提供安全措施，能够对其远程配置加以控制。

5.3.4 密钥安全

PGC移动终端存储的应用根密钥，应满足如下要求：

a) 根密钥应随机生成，随机数熵值应不低于128bit；
b) 根密钥应存储并运行于安全区域，无法被外部获取。

5.3.5 加密安全

PGC移动终端应用在整个加密周期中，应满足如下要求：

a) 密码模块符合国家密码管理机构批准的密码模块；
b) 本地加密密钥应置于安全区域；
c) 非本地加密密钥应在业务结束时从本地销毁；
d) 加密运算过程中应防止密钥信息的泄露，通过密钥存取访问控制、密钥管理操作审计等方法确保密钥信息的安全。

5.3.6 运行安全

PGC移动终端应用运行过程中，应满足如下要求：

a) 具备硬件独立的安全运行区域，通过物理隔离防止篡改、非法获取等；

b) 可通过加密的方式实现应用数据安全存储。

5.3.7 升级更新

应用软件更新，应在用户授权的情况下进行，应用软件应明示软件更新内容，以及可能给用户带来的安全风险。

当应用软件升级失败时，应可以回退至原来版本。

5.3.8 漏洞修复

应检测应用软件可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞;如无法及时进行修复，需制定应急安全方案进行应对。

5.4 网络准入安全要求

5.4.1 网络接入认证

接入网络时，PGC移动终端应满足如下要求：

a) 应在接入网络中具有唯一PGC移动终端标识；

b) 应能向在PGC系统的服务器端证明其网络身份，支持基于加密协议的身份鉴别机制。

5.4.2 网络接入控制

PGC移动终端应满足如下网络接入控制要求：

a) 应设置网络接入控制策略，限制对PGC移动终端的网络访问；

b) PGC移动终端多次连接网络失败，应设置延迟或中断连接尝试，避免反复尝试对网络造成影响；

c) 应具有随机接入机制，即各PGC移动终端初始部署或重启之后延迟接入，使同一区域PGC移动终端错峰接入避免对网络造成冲击；

d) 可限制PGC移动终端数据包发送频率。

5.5 数据交换安全要求

5.5.1 传输完整性

PGC移动终端应满足如下传输完整性要求：

a) 应启用通信完整性校验机制，保护鉴别信息、隐私数据和重要业务数据等数据传输的完整性；

b) 应具有通信延时和中断恢复后继续处理业务的处理机制。

5.5.2 传输保密性

鉴别信息应进行加密传输。

5.6 用户信息数据安全要求

5.6.1 数据收集

收集用户信息数据前应明示收集的目的和范围，并且只有在用户同意的情况下方可进行。

5.6.2 数据存储访问

PGC移动终端应满足如下用户数据的存储要求：

a) 对存储在PGC移动终端上的用户信息数据应提供加密和访问控制机制，防止未授权访问；

b） 应控制PGC移动终端对外接存储设备的使用，如移动硬盘、U盘、TF（microSD）卡等。

5.6.3 数据迁移

PGC移动终端进行用户数据迁移应按照约定目的和用途进行，迁移数据之前应对双方进行身份认证和授权，并采用数字签名等技术手段保证数据的完整性和抗抵赖性，同时应采用密文方式传输。

5.6.4 数据删除

对存储在PGC移动终端的用户信息数据应具备彻底删除功能，被删除的用户信息数据不可恢复。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] YD/T 2407—2013 移动智能终端安全能力技术要求
[3] YD/T 3082—2016 移动智能终端上的个人信息保护技术要求
[4] YD/T 3228—2017 移动应用软件安全评估方法
[5] TAF-WG4-AS0027-V1.0.0:2018 面向低功耗广域网的物联网终端安全能力技术要求
[6] 陈卫平.一种面向融合媒体的PGC移动终端安全防护方法[J].网络空间安全，2018，3