



中华人民共和国国家标准

GB/T 32414—2015

网 络 游 戏 安 全

Online game security

2015-12-31 发布

2016-07-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言	Ⅲ
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 密钥要求	1
5 资料保存安全	2
6 账号安全	2
7 虚拟财产	4

前 言

本标准按照 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。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:中国电子技术标准化研究院、中国信息产业商会网络游戏产业分会、上海盛大游戏公司、北京动感时空技术服务有限公司。

本标准主要起草人:赵菁华、陈胜喜、杜江杰、樊星、张展新。

网 络 游 戏 安 全

1 范围

本标准规定了网络游戏软件的安全要求。

本标准适用于网络游戏软件的开发和测试及网络游戏的运营。

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。

GB/T 1988 信息技术 信息交换用七位编码字符集

GB/T 17901.1 信息技术 安全技术 密钥管理 第1部分:框架

GM/T 0002 SM4 分组密码算法

GM/T 0003(所有部分) SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

风险控制判断 risk control judgement

针对账号和应用的限制和保护,设置风险判定条件。

4 密钥要求

4.1 密码算法要求

密码算法应符合以下要求:

- a) 对称加密算法应符合 GM/T 0002 的要求;
- b) 非对称加密算法应符合 GM/T 0003、GM/T 0009 和 GM/T 0010 的要求;
- c) 杂凑算法应符合 GM/T 0004 的要求。

4.2 密钥管理要求

密钥管理应符合以下要求:

- a) 密钥管理应符合 GB/T 17901.1 的要求;
- b) 设立加密密钥双重控制规则,分开保管和建立;
- c) 密钥在除加密设备以外不应以明文形式出现;
- d) 生成的密钥应以密文形式传输,不应将密钥与外部供应商共享;

- e) 密钥应至少每年进行一次密钥更改；
- f) 对于疑似泄露的加密的密钥应及时弃用或更改；
- g) 应要求密钥保管人签署文件，声明清楚并接受密钥保管责任。

5 资料保存安全

5.1 管理员密码要求

管理员密码应符合以下要求：

- a) 至少应选择对称加密，密码长度应超过 32 个字符，每个密码应至少包含 GB/T 1988 中的大小写字母、0~9 数字和其他可输入输出字符；
- b) 使用磁盘加密时，加密工具的管理账号应独立于操作系统的账号。

5.2 实名资料保存策略

网络游戏产品运营企业应根据业务、法律或法规要求制定用于证明个人身份有效性的实名资料的保留和处理策略。

5.3 用户支付账户信息保存

用户支付账户信息应符合以下要求：

- a) 显示支付账号时对其进行掩盖，至少掩盖 4 位；
- b) 如使用了磁盘加密而不是文件级或列级数据库加密，则对逻辑访问的管理应独立于本地操作系统的访问控制机制；
- c) 解密密钥不应与用户账户绑定。

6 账号安全

6.1 账号资料信息

6.1.1 账号资料管理

账号资料管理包括：

- a) 账号基本信息内容
在注册账号时至少应填写的信息包括：账号、密码，针对年满 18 周岁或取消沉迷措施限制的用户，还应提供用户姓名和公民身份证号码。
- b) 账号保护信息
在注册账号时至少应填写的账号保护信息包括：姓名、公民身份证号码、联系电话、电子邮箱和提示问题。
- c) 账号信息的补填与修改
账号注册应可以补填相应的账号资料信息，修改账号资料信息通过安全审核。
- d) 安全风险控制
账号资料在数据库中应加密保存，所在物理服务器应设置 IP 地址安全策略，禁止不相关应用服务器访问。应用服务器使用该数据库账户应仅对业务数据具有操作权限。

6.1.2 账号日志

账号日志至少应记录账号的注册、登录、管理及变更信息。

