ICS 35.240
A 01
备案号

MZ

中华人民共和国民政行业标准

MZ/T 080-2017

中国福利彩票系统软件安全性测试规范

Specification for welfare-lottery-system-software security-testing

2017-01-06 发布　　2017-01-06 实施

中华人民共和国民政部　发布

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国福利彩票发行管理中心提出。

本标准由民政部社会福利和慈善事业促进司归口管理。

本标准起草单位：中国福利彩票发行管理中心。

本标准主要起草人：栗演兵、张彤、朱志新、何天琼、张积涛、韩毅、闫峰、蔡荣生、黄晓辉、付小兵、李英华、杜莉婷。

中国福利彩票系统软件安全性测试规范

1 范围

本标准规定了彩票系统软件安全性测试的对象、管理、方法和工具、内容和评级。

本标准适用于中国福利彩票发行机构、销售机构、企业和第三方检测机构对彩票系统软件的安全性进行测试。

2 规范性引用文件

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GA/T 390-2002 计算机信息系统安全等级保护通用技术要求

GB/T 11457 软件工程术语

GB/T 15532-2008 计算机软件测试规范

3 术语和定义

下述术语及GB/T 11457中确立的术语和定义适用于本文件。

3.1

彩票系统软件 lottery-system-software

彩票系统软件是指实现一个或多个彩票玩法，能够完成彩票购买，彩票销售，彩票开奖，奖金兑付，业务管理这一系列彩票业务流程、并具备一定的安全性、可靠性的系统及软件。可包括以下子系统或模块：彩票交易、资金管理、参数管理、摇奖开奖、用户管理、代销者管理或渠道管理、投注终端管理、账户管理、彩票业务报表、运行监控、数据存储、网络系统、投注终端或客户端、关联软件或系统。

3.2

可用性 usability

确保授权用户对彩票系统的信息和资源的正常使用不会被异常拒绝，允许其可靠即时地访问信息和资源。

3.3

保密性 confidentiality

确保彩票相关的信息在存储、使用、传输过程中不会泄露给非授权用户。

3.4

完整性 completeness

确保彩票相关的信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。

3.5

抗抵赖性 non-repudiation
确保彩票交易参与者对交易信息和过程的不可否认。

3.6

可追溯性 traceability
确保彩票系统用户的操作记录能够被可靠地追踪。

3.7

安全性 security
彩票系统软件安全性是指彩票系统信息的完整性、保密性、可用性、抗抵赖性和可追溯性。

4 测试目的和对象

4.1 测试目的

a) 在模拟真实或真实的工作环境下，检验彩票系统软件安全性能否满足合同、软件需求规格说明、系统或子系统设计说明、软件设计说明、用户手册、彩票系统风险分析报告所规定的彩票系统软件安全性要求，应包括彩票系统信息的保密性、完整性、可用性、抗抵赖性和可追溯性要求；
b) 通过测试，发现彩票系统软件安全性缺陷；
c) 为彩票系统软件产品的质量和评价提供依据。

4.2 测试对象

安全性测试的对象是完整的彩票系统或者是其中一部分相对独立的子系统。

5 测试管理

5.1 测试人员

彩票系统安全性测试应由相对独立的人员进行。安全性测试人员角色职责见表1。

表1 安全性测试人员角色职责表

工作角色	具体职责
测试项目负责人	管理监督测试项目，提供技术指导，获取适当的资源，制定基线，技术协调，负责项目的安全保密和质量管理。
测试分析员	确定测试计划、测试内容、测试方法、测试数据生成方法、测试（软、硬件）环境、测试工具，评价测试工作的有效性。
测试设计员	设计测试用例，确定测试用例的优先级，建立测试环境。
测试程序员	编写测试辅助软件。
测试员	执行测试、记录测试结果。
测试系统管理员	对测试环境和资产进行管理和维护。

配置管理员	设置、管理和维护测试配置管理数据库。

5.2 测试的准入和准出条件

测试的准入准出条件如下：

a） 准入条件

开始安全性测试工作应具备下列条件：

1） 具有测试任务书（合同或项目计划）；
2） 具有安全性测试所需的文档；
3） 所提交的被测软件受控。

b） 准出条件

结束安全性测试工作应具备下列条件：

1） 已按要求完成了合同所规定的测试任务；
2） 实际测试过程遵循了原定的测试计划和测试说明；
3） 客观、详细地记录了测试过程和软件测试中发现的所有问题；
4） 测试文档齐全、符合规范；
5） 测试的全过程自始至终在控制下进行；
6） 测试中的问题或异常有合理解释或正确有效的处理；
7） 测试工作通过了测试评审；
8） 全部测试软件、被测软件、测试支持软件和评审结果已纳入配置管理。

6 测试方法和工具

6.1 测试方法

彩票系统安全性测试可采用静态测试方法和动态测试方法。静态测试方法常采用静态分析、代码走查方法。动态测试方法常采用白盒测试方法和黑盒测试方法。

6.2 测试工具

可使用人工或者自动化测试工具，包含但不限于：自动化安全性功能测试工具和渗透测试工具。

注：渗透测试工具包括但不限于自动化漏洞扫描工具、风险评估工具、模拟攻击和侦听工具。

7 测试环境

彩票系统软件安全性测试环境包括测试的运行环境和测试工具环境。

运行环境应符合软件安全性测试任务书的要求，通常是模拟真实环境或真实环境。测试工具要求是经过认可的工具。

8 测试过程

彩票系统安全性测试过程包括：测试计划、测试设计、测试执行、测试总结。测试过程遵照GB/T 15532-2008 中第4章第3条的要求执行。

9 测试内容

9.1 平台安全

测试彩票系统采用的操作系统、数据库系统和通用基础服务的安全。

测试内容应包括：操作系统漏洞检测与修复、通用基础应用程序漏洞检测与修复、彩票系统防病毒措施。

9.2 通信安全

测试彩票系统的网络设计和实现以及传输链路的安全。

测试内容应包括：网络隔离、访问控制、硬件和软件加解密、身份鉴别机制、各项网络协议运行漏洞。

9.3 应用安全

测试彩票系统应用安全，包括认证和授权、审计跟踪、系统应急响应。

测试内容应包括：彩票系统软件的程序安全性、彩票业务的抗抵赖性、彩票业务的访问控制、彩票业务实体的身份认证、彩票业务的备份与恢复机制、彩票业务数据的惟一性、一致性、防冲突性、彩票业务系统的可用性、系统应急响应计划与实施方案。

9.4 数据安全

测试彩票系统数据的安全，包括但不限于彩票销售数据、开奖数据、计奖数据、兑奖数据、弃奖数据、彩票资金数据、彩民信息数据。

测试内容应包括：数据访问控制、标识与鉴别、数据完整性、数据可用性、数据监控和审计、数据存储与备份安全。

10 测试评级

10.1 安全等级

安全性测试完成后，应对测试对象进行测试评级。根据测试结果，安全性由低到高可分为一级、二级、三级、四级、五级。各级的技术要求见附录A。

10.2 一级

一级应符合的要求如下：

a) 通过简单的用户标识和鉴别来限制系统的功能配置和数据访问控制,使用户具备自主安全保护的能力，防止非法用户对数据的读写与破坏；
a) 采用 GA/T 390-2002 4.3.13 条密码支持第一级进行用户口令设计、存储和传输；
b) 具备防病毒措施；
c) 具备自我信息备份和增量备份、手动故障恢复功能。

10.3 二级

二级应符合的要求如下：

a) 彩票系统采用更细粒度的自主访问控制，划分安全管理角色，细化系统管理；
b) 通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责；
c) 增加系统审计功能，增强可追溯性；
d) 采用 GA/T 390-2002 4.3.13 条密码支持第二级进行用户口令设计、存储和传输；

e） 采用 GA/T 390-2002 4.3.13 条密码支持第二级提供的功能，进行数据完整性保护；
f） 具备网络防病毒措施，具备局部系统备份和热备份、手动故障恢复功能；
g） 具备应急计划和应急措施。

10.4 三级

三级应符合的要求如下：
a） 彩票系统具有系统审计保护级的所有功能；
b） 系统提供安全策略模型、数据标记和强制访问控制的非形式化描述，具有准确标记输出信息的能力，消除通过测试发现的所有错误；
c） 采用 GA/T 390-2002 4.3.13 条密码支持第三级进行用户口令设计、存储和传输；
d） 采用 GA/T 390-2002 4.3.13 条密码支持第三级提供的功能，进行数据完整性、保密性和真实性保护及完整性检验；
e） 采用“最小授权原则”设置系统管理员、安全管理员和审计员；
f） 具备整体防御网络防病毒措施，具备热备份、全系统备份、自动故障恢复功能；
g） 具备应急计划和应急措施。

10.5 四级

四级应符合的要求如下：
a） 彩票系统具有明确定义的形式化安全策略模型，采用完全控制策略，并将第三级系统中的自主和强制访问控制扩展到所有彩票信息与用户，同时采用隐蔽通道；
b） 增强用户鉴别机制，采用 GA/T 390-2002 4.3.13 条密码支持第四级进行用户口令设计、存储和传输；
c） 采用 GA/T 390-2002 4.3.13 条密码支持第四级提供的功能，进行数据完整性、保密性和真实性保护及完整性、真实性检验。提供可信设施管理；
d） 增强了配置管理控制。系统具有相当的抗渗透能力；
e） 具备多层防御网络防病毒措施，具备热备份、全系统备份、主机系统异地备份、自动故障恢复和灾难性恢复功能；
f） 具备应急计划和应急措施，明确处理流程图。

10.6 五级

五级应符合的要求如下：
a） 彩票系统安全性满足访问监控需求；
b） 进一步强化和细化访问控制，为每个用户指定用户名和用户组，并规定其访问方式；
c） 支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号,提供系统恢复机制；
d） 系统具有很高的抗渗透能力；
e） 采用 GA/T 390-2002 4.3.13 条密码支持第五级进行用户口令设计、存储和传输；
f） 采用 GA/T 390-2002 4.3.13 条密码支持第五级提供的功能，进行数据完整性、保密性和一致性保护及检验；
g） 具备多层防御网络防病毒措施，具备热备份、全系统备份、主机系统异地备份、自动故障恢复和灾难性恢复功能；
h） 具备应急计划和应急措施，明确处理流程图。

11 工作产品

彩票系统软件安全性测试完成后形成的文档有：

a) 安全性测试计划；
b) 安全性测试说明；
c) 安全性测试报告；
d) 安全性测试记录；
e) 安全性测试问题报告。

附 录 A
（规范性附录）
彩票系统安全级别技术要求

本附录给出了彩票系统安全各个级别的技术要求。
表中○表示该级别应符合的技术要求。

表A.1 平台安全技术要求

章节	技术要求				一级	二级	三级	四级	五级
9.1 平台安全	操作系统	操作系统漏洞	系统升级和更新			○	○	○	○
		本地访问控制	登录规程			○	○	○	○
			用户注册		○	○	○	○	○
			特权管理	用户鉴别				○	○
				用户指定用户名和用户组，并规定其访问方式					○
				安全管理员					○
			用户口令管理	设立	○	○	○	○	○
				使用		○	○	○	○
				保存		○	○	○	○
				变更	○	○	○	○	○
				其他口令				○	○
			用户访问权利的审查	划分安全管理角色		○	○	○	○
				采用“最小授权原则”设置系统管理员、安全管理员和审计员			○	○	○
			强制访问	部分用户			○	○	○
				全部用户				○	○
			可信路径	隐蔽通道				○	○
		远程登录控制					○	○	○
		日志			○	○	○	○	○

A.1（续）

章节	技术要求				一级	二级	三级	四级	五级
9.1 平台安全	数据库	访问控制	登录规程		○	○	○	○	○
			用户注册		○	○	○	○	○
			特权管理	用户鉴别				○	○
				用户指定用户名和用户组，并规定其访问方式					○
				安全管理员					○
			用户口令管理	设立	○	○	○	○	○
				使用		○	○	○	○
				保存		○	○	○	○
				变更	○	○	○	○	○
				其他口令				○	○
			用户访问权利的审查	划分安全管理角色		○	○	○	○
			数据标记				○	○	○
			强制访问	部分用户			○	○	○
				全部用户				○	○
		日志			○	○	○	○	○
		历史数据	保存		○	○	○	○	○
			销毁			○	○	○	○
	配置管理控制							○	○
	通用基础服务	通用基础应用程序漏洞					○	○	○
	危害防护	防病毒			○	○	○	○	○
		防入侵					○	○	○
		防恶意软件			○	○	○	○	○

表A.2　通信安全技术要求

章节	技术要求		一级	二级	三级	四级	五级
9.2 通信安全	网络设计和实现的安全性	使用网络服务的政策	○	○	○	○	○
		结构安全与网段划分 网络隔离	○	○	○	○	○
		强制路径			○	○	○
		外部连接的用户身份验证	○	○	○	○	○
		节点鉴别	○	○	○	○	○
		访问控制	○	○	○	○	○
		拨号访问控制	○	○	○	○	○
		远程诊断端口保护				○	○
		网络连接控制（边界完整性检查）		○	○	○	○
		网络路由控制			○	○	○
		网络防病毒措施		○	○	○	○
		整体防御网络防病毒措施			○	○	○
		具备多层防御网络防病毒措施				○	○
		入侵防范、恶意代码防范		○	○	○	○
		网络安全审计		○	○	○	○
	网络服务的安全	公共网络服务安全				○	○
	传输链路的安全性	硬件和软件加解密		○	○	○	○
		网络协议运行漏洞				○	○

表A.3　应用安全技术要求

章节	技术要求			一级	二级	三级	四级	五级
9.3 应用安全	认证和授权	彩票终端机的认证和授权	彩票终端机的识别	○	○	○	○	○
			终端登录程序	○	○	○	○	○
			用户标识和鉴别	○	○	○	○	○
			口令管理	○	○	○	○	○
			使用系统工具	○	○	○	○	○
			终端超时		○	○	○	○
			连接时间的限制		○	○	○	○
			登录规程		○	○	○	○
		彩票从业人员的认证和授权		○	○	○	○	○
		彩票应用访问控制	信息访问限制	○	○	○	○	○
			敏感信息隔离		○	○	○	○
		密码控制	使用密码控制的政策		○	○	○	○
			采用GA/T 390-2002 4.3.13条密码支持第一级进行用户口令设计、存储和传输	○				
			采用GA/T 390-2002 4.3.13条密码支持第二级进行用户口令设计、存储和传输		○			
			采用GA/T 390-2002 4.3.13条密码支持第三级进行用户口令设计、存储和传输			○		
			采用GA/T 390-2002 4.3.13条密码支持第四级进行用户口令设计、存储和传输				○	
			采用GA/T 390-2002 4.3.13条密码支持第五级进行用户口令设计、存储和传输					○
			数字签名		○	○	○	○
			认可服务		○	○	○	○
			密钥管理		○	○	○	○

A.3 （续）

章节	技术要求			一级	二级	三级	四级	五级
9.3 应用安全	彩票业务系统应用程序安全	正确性	检验、恢复	○	○	○	○	○
		完整性	检验、恢复	○	○	○	○	○
		可用性	检验、恢复	○	○	○	○	○
		时钟同步		○	○	○	○	○
		历史数据	保存、销毁	○	○	○	○	○
	审计跟踪	监视系统访问和使用	事件记录	○	○	○	○	○
			监视系统使用		○	○	○	○
			发生与安全相关的事件时发出信号					○
		彩票业务数据的惟一性/一致性/防冲突性		○	○	○	○	○
		业务的抗抵赖性		○	○	○	○	○
	彩票系统应急响应	备份与恢复机制	自我信息备份和增量备份、手动故障恢复功能	○	○	○	○	○
			具备局部系统备份和热备份、手动故障恢复功能		○	○	○	○
			具备热备份、全系统备份、自动故障恢复功能			○	○	○
			具备热备份、全系统备份、主机系统异地备份、自动故障恢复和灾难性恢复功能				○	○
		彩票应急响应计划与实施方案	具备应急计划和应急措施		○	○	○	○
			明确处理流程图				○	○

表A.4　数据安全技术要求

章节	技术要求		一级	二级	三级	四级	五级
9.4 数据安全	彩票数据访问控制		○	○	○	○	○
	彩票的标识与鉴别	彩票数据标记，具有准确标记输出信息的能力			○	○	○
	数据完整性	检测	○	○	○	○	○
		恢复	○	○	○	○	○
	数据可用性	检测、恢复	○	○	○	○	○
	数据监控和审计	日志	○	○	○	○	○
	数据存储与备份安全	备份 恢复	○	○	○	○	○
	彩票交易数据的加密	采用GA/T 390-2002 4.3.13条密码支持第二级提供的功能，进行数据完整性保护		○			
		采用GA/T 390-2002 4.3.13条密码支持第三级提供的功能，进行数据完整性、保密性和真实性保护及完整性检验。			○		
		采用GA/T 390-2002 4.3.13条密码支持第四级提供的功能，进行数据完整性、保密性和真实性保护及完整性、真实性检验				○	
		采用GA/T 390-2002 4.3.13条密码支持第五级提供的功能，进行数据完整性、保密性和一致性保护及检验					○

参 考 文 献

[1] GA/T 712-2007 信息安全技术 应用软件系统安全等级保护通用测试指南
[2] GB/T 9386 计算机软件测试文档编制规范
[3] GB 17859-1999 计算机信息系统安全保护等级划分准则
[4] GB/T 18336.1-2008 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型
[5] GB/T 18336.2-2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求
[6] GB/T 18492 信息技术 系统及软件完整性级别
[7] GB/T 20269-2006 信息安全技术 信息系统安全管理要求
[8] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
[9] GB/T 20272-2006 信息安全技术 操作系统安全技术要求
[10] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
[11] GB/T 20274.1-2006 信息安全技术 信息系统安全保障评估框架 第一部分 简介和一般模型
[12] GB/T 20274.2-2008 信息安全技术 信息系统安全保障评估框架 第二部分 技术保障
[13] GB/T 20274.3-2008 信息安全技术 信息系统安全保障评估框架 第三部分 管理保障
[14] GB/T 20274.4-2008 信息安全技术 信息系统安全保障评估框架 第四部分 工程保障
[15] GB/T 20945-2007 信息安全技术 信息系统安全审计产品技术要求和测试评价方法
[16] GB/T 22080-2008 信息技术 安全技术 信息安全管理体系 要求
[17] GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则