ICS 35.240.60
L 67

DB11

北　京　市　地　方　标　准

DB 11/T 1165.8—2019

收费公路联网收费系统 第8部分：信息安全

Network toll collection system for toll highway

Part 8: Information safety

2019-03-27 发布　　2019-10-01 实施

北京市市场监督管理局　发布

目　　次

前　言

DB11/T 1165 《收费公路联网收费系统》分成以下几个部分：

——第1部分：系统构成及硬件技术要求；

——第2部分：基础数据元和编码规则；

——第3部分：收费系统介质技术要求与数据格式；

——第4部分：拆分与结算；

——第5部分：清分结算规则；

——第6部分：数据通信接口；

——第7部分：数据库设计；

——第8部分：信息安全；

——第9部分：应用软件技术要求。

本部分为DB11/T 1165的第8部分。

本部分按GB/T 1.1－2009 给出的规则起草。

本部分由北京市交通委员会提出并归口。

本部分由北京市交通委员会组织实施。

本部分的起草单位：北京市首都公路发展集团有限公司、北京云星宇交通科技股份有限公司。

本部分主要起草人：张明月、徐志斌、范文江、张恒利、刘绍民、孔祥杰、毕爽、陈日强、张卿、刘刚、李少丁、刘星宇、佟乐、王刚、杨勇、朱婷婷、纪海颖、赵永忠、俞宏熙。

收费公路联网收费系统
第8部分：信息安全

1 范围

DB11/T 1165的本部分规范了收费公路联网收费系统的信息安全保护等级和技术要求。

本部分适用于收费公路联网收费系统的新建、改建或扩建。

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，仅所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 17859 计算机信息系统安全保护等级保护划分准则

GB 50016 建筑设计防火规范标准

GB 50045 高层民用建筑设计防火规范

GB 50116 火灾自动报警系统设计规范

GB 50174 电子信息系统机房设计规范

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 24719 公路收费亭

GB/T 25069 信息安全技术术语

GB/T 5271.8 信息技术 词汇 第8部分:安全

GB/T 9361 计算机场地安全要求

DB11/T 1165.1 收费公路联网收费系统 第1部分：系统构成及硬件技术要求

3 术语和定义

GB 17859、GB/T 25069、GB/T 5271.8、DB11/T 1165.1界定的以及下列术语和定义适应于本文件。

3.1

骨干网络 backbone network

收费总中心网络、灾备中心网络、收费分中心网络以及他们之间构成的网络，包括核心层和汇聚层。

4 收费系统信息安全保护等级

收费公路联网收费系统应符合GB/T 22239中信息系统安全等级保护第三级要求，包括物理安全、网络安全、主机安全、应用安全、数据安全等方面技术要求的安全保护能力。

5 收费系统信息安全技术要求

5.1 物理安全

5.1.1 无人值守机房

无人值守机房包括收费所（站）机房、收费广场机房，应满足如下要求：

a) 具备对出入人员远程身份识别和认证能力；
b) 采用阻燃材料，具备相应安全防护、防盗、防火能力；
c) 配置 UPS 设备，供电时间应不小于 1 小时，宜配置柴油发电机作为备用电源；
d) 设置温、湿度自动检测和调节设备；
e) 具备火灾自动检测能力，配备消防灭火设施；
f) 采取防雷措施，防雷接地电阻应小于 10Ω；
g) 机房设备接地小于 4Ω，采用联合接地时应小于 1Ω。

5.1.2 有人值守机房

有人值守机房包括收费总中心机房、灾备中心机房、收费分中心机房，应满足5.1.1及以下要求：

a) 配置电子门禁系统；
b) 配置备用柴油发电机作为备用电源；
c) 配置自动消防系统；
d) 符合 GB 50174 中的防震、防风、防雨、防潮、防尘、防静电等技术要求，设置避雷、防雷装置；
e) 收费总中心的机房设独立操作间，操作间采用隔离墙与主机房进行区域隔离；
f) 设置视频监控系统，并具备人员闯入报警功能；
g) 采取联合接地，接地电阻应小于 1Ω。

5.1.3 收费车道

收费车道包括MTC车道和ETC车道，应满足如下要求：

a) 设置防盗设施；
b) 配备灭火装置；
c) 配备应急照明装置；
d) 供电线路应配置漏电压防护设备；
e) 供电装置和供电线路应设置接地；
f) 设置联动报警装置；
g) 符合 GB/T 24719 中防护性要求。

5.2 网络安全

5.2.1 网络安全结构

网络安全结构要求如下：

a) 联网收费系统网络与其他网络应采取隔离措施；
b) 骨干网络应具有自愈保护能力，宜采用环型网络结构；
c) 收费总中心、灾备中心、收费分中心、收费所（站）应划分子网或网段，以不同的广播域对内部网段进行隔离。

5.2.2 访问控制

访问控制应满足如下要求：

a) 在收费总中心、灾备中心和各收费分中心应设置独立的安全域，进行安全隔离和访问控制；
b) 本系统安全域之间及以外的边界防护应采取访问控制策略，控制数据传输，并且只允许特定授权的终端用户访问该安全域。

5.2.3 数据安全交换

数据安全交换应满足如下要求：

a) 联网收费系统各层级之间应使用专网连接，具有防监听、数据加密等安全防护能力；
b) 只允许收费总中心、灾备中心和收费分中心向收费系统外进行数据单向推送。

5.2.4 入侵防范

入侵防范应满足如下要求：

a) 收费总中心、灾备中心和收费分中心应配置入侵检测系统或入侵防护系统；
b) 入侵检测系统应配置多层次的扫描器。

5.2.5 网络设备防护

网络设备防护应满足如下要求：

a) 防止 IP 地址被盗用或仿冒，防止用户间的相互攻击；
b) 关闭网络设备不安全或不使用的服务；
c) 限制管理员登录网络设备的地址，只允许管理员指定终端进行登录；
d) 启用网络设备的登录失败处理功能。无人为操作时间应不超过 10min，登录失败超过 5 次，应锁定账户，并由指定管理员才能解锁账户；
e) 只允许指定的设备对网络设备进行访问与管理。

5.3 主机安全

5.3.1 用户安全管理

用户安全管理包括总\分中心主机、票证主机、应用服务器、数据库服务器、票据服务器、备份服务器，应满足如下要求：

a) 用户应设置成不同级别，并限制用户尝试登陆到系统的次数；
b) 数据库系统，宜将数据库访问权限分为登录权限、管理权限、管理员权限三种用户权限；
c) 按照操作权限最小化原则使用操作系统与数据库，口令应分级设置和动态管理，不应使用操作系统默认的用户、口令等；口令至少有 8 位包含字母数字的密码，有效期最长不超过三个月。

5.3.2 日志审计

日志审计满足如下要求：

a) 应对收费总中心、灾备中心和收费分中心的内网系统日志进行严格管理，实时监测和记录系统状态；
b) 数据库管理系统宜采用用户审计、系统审计、操作审计、对象审计等多种审计管理方法；
c) 应由系统管理员定期对系统日志进行安全审计和分析，当有入侵事件发生时，应立即进行审计。

5.3.3 剩余信息保护

收费系统服务器应开启操作系统剩余信息保护安全策略，在用户登录系统前，应完全清除前一用户残留的身份鉴别信息。

5.3.4 入侵防范

入侵防范应满足如下要求：

a) 操作系统和数据库系统应进行漏洞检测，并根据检测结果及时进行防护，漏洞扫描软件应不超过六个月进行一次系统升级；
b) 应卸载主机操作系统中无用的组件和应用程序，关闭无用端口，禁用远程修改注册表功能；
c) 应设置操作系统的屏幕密码保护，系统 10 分钟内无界面操作自动锁屏；
d) 远程登录的操作系统账号 20 分钟内无操作时自动断接；
e) 入侵检测系统应检测主机受入侵行为，记录入侵源 IP、攻击类型、攻击目的、攻击时间等，并提供实时报警。

5.3.5 恶意代码防范

恶意代码防范应满足如下要求：

a) 应统一部署恶意代码防范策略、软件,实时监测收费总中心、灾备中心、收费分中心的防范状态；
b) 应定期升级防病毒软件的恶意代码库,至少一周进行一次。

5.3.6 资源控制

应对主机进行监控，宜采用设定终端接入方式、设置主机安全策略、监视服务器、合理限制用户系统资源使用等措施对主机进行保护。

5.4 应用安全

5.4.1 身份鉴别

身份鉴别宜进行证书加口令等双因素认证。

5.4.2 访问控制

访问控制应满足如下安全要求：

a) 根据不同用户的权限，限制账户可访问的资源；
b) 通过规定的权限对账户管理系统进行访问控制策略配置；
c) 根据系统模块及功能，完成系统权限的划分；
d) 信息资源应设置敏感标记，规定的指定用户不能进行修改；
e) 根据不同级别账户权限，限制账户对具有相应级别敏感标记的数据进行操作；
f) 账户使用前先修改密码，并定期修改。

5.4.3 剩余信息保护

剩余信息保护应满足如下要求：

a) 剩余信息包括收费系统的鉴别信息、收费系统生成的临时文件和目录与数据库记录；
b) 收费系统的鉴别信息存储在内存中，当用户身份鉴别过程结束之后，立即对内存中存储鉴别信息的内存资源进行释放；
c) 主机应对临时文件、数据库记录、硬盘等剩余信息进行保护。

5.4.4 通信完整性和保密性

在收费系统的设计与开发中，通信完整性和保密性应满足如下要求：

a) 应采用校验机制保障通信的完整性；
b) 应采用密码技术实现通信过程中的保密性进行数据传输。

5.4.5 抗抵赖性

收费系统应结合数字证书认证系统，采用电子签名技术对重要文件和数据进行电子签名以及时间戳技术，实现对数据发送方的抗抵赖防护。

5.4.6 软件容错

软件容错满足如下安全要求：

a) 在收费系统开发过程中，对于所有人机接口输入或通过通信接口输入的数据格式或长度进行格式验证和非法参数过滤，减少系统错误的发生；
b) 对用户输入异常参数进行检查，当检测到系统出现异常时，应具备自动恢复功能；
c) 收费总中心、灾备中心、收费分中心等数据库服务器应采用双机热备的方式，切换时间小于60 秒。

5.4.7 资源控制

资源控制应满足如下安全要求：

a) 实时监控系统资源使用情况，当系统资源使用水平降低到一定程度时，系统自动报警，通知系统管理员进行处理；
b) 应对账户使用系统资源的最大值和最小值进行合理设置；
c) 应对同一账户的多重并发访问操作进行限制；
d) 通过应用中间件的相关配置，应限定最大并发会话连接数。

5.5 数据安全

5.5.1 数据完整性

数据完整性应满足如下安全要求：

a) 建立数字证书认证系统，并为收费系统的用户颁发数字证书；
b) 结合数字证书系统对应用系统传输过程中的数据进行数字签名，保证数据传输的完整性。

5.5.2 数据保密性

数据保密性应采用数据加密技术对数据进行加密传输。

5.5.3 备份和恢复

备份和恢复应满足如下安全要求：

a) 应建设本地数据备份及异地灾备系统；
b) 收费总中心全量备份一周两次，增量备份每天一次；
c) 收费分中心全量备份一周一次；
d) 收费所（站）全量备份每天一次。

参 考 文 献

[1] 交通运输部 2007年第35号公告 收费公路联网收费技术要求
[2] GB/T 20271—2006 信息安全技术信息系统安全通用技术要求
[3] GB/T 21052—2007 信息安全技术信息系统物理安全技术要求