ICS 29.200
K 81

T/CEC

中国电力企业联合会标准

T / CEC 208—2019

电动汽车充电设施信息安全技术规范

Technical specification for information security of electric vehicle charging facilities

2019–04–24发布　　2019–07–01实施

中国电力企业联合会　发布

中国电力企业联合会标准

电动汽车充电设施信息安全技术规范

T / CEC 208—2019

*

中国电力出版社出版、发行

（北京市东城区北京站西街 19 号　100005　http://www.cepp.sgcc.com.cn）

印刷

*

2019 年　月第一版　　2019 年　月北京第一次印刷

880 毫米×1230 毫米　16 开本　　印张　　千字

*

统一书号 155198・1564　定价 **0.00** 元

目　　次

前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》规定起草。

本标准由中国电力企业联合会提出。

本标准由中国电力企业联合会标准化管理中心归口。

本标准主要起草单位：工业和信息化部计算机与微电子发展研究中心、国网电力科学研究院有限公司、上海电器科学研究院、普天新能源有限责任公司、国网网安（北京）科技有限公司、浙江安科网络技术有限公司、中国电力企业联合会科技开发服务中心、中国电力技术市场协会。

本标准主要起草人：薛晓卿、傅晶、张小飞、鞠晨、方洪波、王洪奎。

本标准参与起草单位：许昌开普检测技术有限公司、青岛特来电新能源有限公司、华为技术有限公司、深圳市科陆电子科技股份有限公司、积成电子股份有限公司、全球能源互联网研究院有限公司、北京智充科技有限公司、江苏万帮德和新能源科技股份有限公司、浙江万马股份有限公司、国网北京市电力公司电力科学研究院、国网电动汽车服务有限公司、广东省电力设计研究院。

本标准的发布机构不承担识别这些专利的责任。

本标准为首次发布。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

电动汽车充电设施信息安全技术规范

1 范围

本规范规定了电动汽车充电设施信息安全的技术要求。

本规范适用于与电动汽车充电设施相关的运营平台、充电设备、移动智能终端软件的信息安全防护设计、运行维护、研发和测试评估环节等。

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 9387.1 信息技术 开放系统互连 基本参考模型 第 1 部分：基本模型

GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件

GB/T 19596 电动汽车术语

GB/T 29317—2012 电动汽车充换电设施术语

GB/T 34975—2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

T/CEC 102.4 电动汽车充换电服务信息交换 第 4 部分：数据传输及安全

3 术语和定义

GB/T 19596、GB/T 29317—2012 界定的以及下列术语和定义适用于本文件。

3.1

充电设施 charging facilities

充电运营网络中能够提供对外充电服务的充电桩、充电桩群和充电站，包括充电设备、运营平台和移动智能终端等。

3.2

基础软件 basic software

运行于基础资源之上的底层软件，一般包括主机操作系统、系统数据库、网络安全防护软件、审计应用、中间件等。

3.3

业务系统 operation system

为平台的终端用户和业务操作人员提供服务的系统。

3.4

移动智能终端 mobile intelligent terminal

能够接入移动通信网络，具有能够提供应用程序开发接口的开放操作系统，并能由用户自行安装、运行和卸载应用软件的移动通信终端产品。

3.5

移动智能终端应用软件 mobile intelligent terminal software

针对移动智能终端开发的应用软件，包括充电设施厂家的应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装和升级的适用于充电设施相关的应用软件。

3.6

信息服务系统 information service system

以处理电动汽车充电服务信息为核心的应用系统。由充电运行网络中的主要服务单元组成，包括

平台、设施和终端。

3.7

运营平台　operation system

充电运行网络中承担后台充电服务功能的运行和提供的信息服务系统。由 IT 基础设施和应用软件系统组成。

3.8

充电设备　charging equipment

承担充电服务功能的交直流充电设备以及配套设备。

3.9

终端　terminal

电动汽车用户使用的智能应用程序（App），通过终端用户能够获得充电服务，完成充电服务交易与缴费。

3.10

充电服务凭证　charging service certificate

充电服务发生或完成情况的信息证明。实物如智能卡等。

4　充电设施信息安全总体要求

4.1　信息安全防护对象与目标

4.1.1　防护对象

电动汽车充电设施的信息安全防护对象主要分以下两种类型：

a） 实体类型，即图 1 的 R_{ref}。此类型主要指充电设施中的充电设备、运营平台以及移动智能终端。

b） 接口类型，即图 1 的 I_{ref}。此类型主要指充电设施中涉及的各个实体之间的信息交换接口，即充电设备和运营平台之间的接口，运营平台与移动智能终端之间的接口，充电设备与移动智能终端之间的接口，以及充电设备和电动汽车之间的接口和运营平台与其他平台之间的接口。

充电设施信息安全防护对象之间的具体关系如图 1 所示。

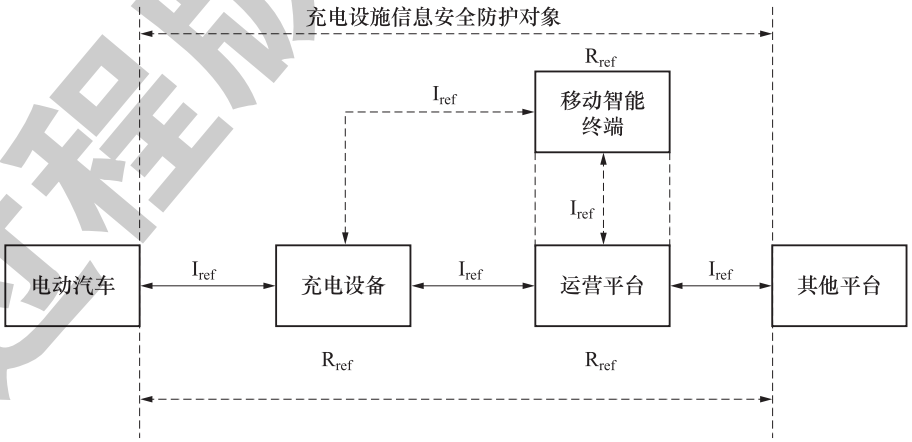


图 1　充电设施信息安全防护对象关系图

4.1.2　目标要求

根据充电设施信息安全防护对象不同，安全防护的主要目标要求划分为两类：

a） 系统安全目标要求：保护实体系统安全可靠运行，免受恶意攻击，确保系统服务可用。系统安

全目标要求分为访问控制、身份认证、内容安全、监控审计和备份恢复五个重点部分。

b） 接口安全目标要求：接口进行信息交换过程中，保护数据在存储、传输、处理过程中不被泄漏、破坏和未授权的使用等。接口安全目标要求分为保密性、完整性和可用性三个重点。

4.1.3 总体目标

充电设施信息安全防护对象须规定并满足安全防护总体目标要求，具体见表 1。

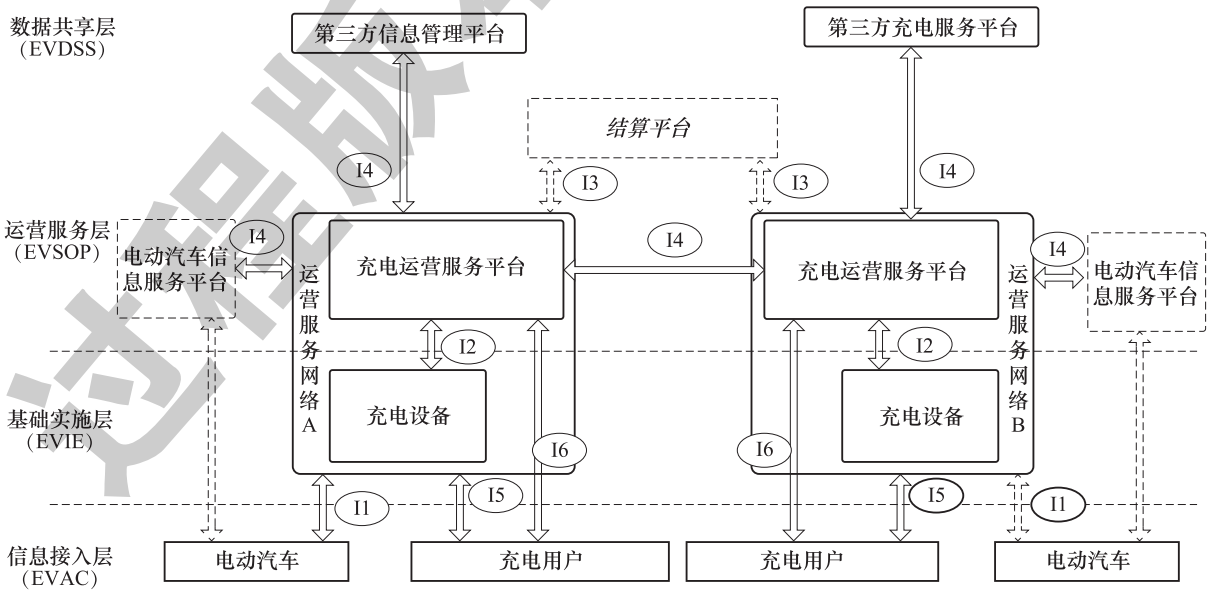
表 1 充电设施信息安全防护对象总体目标要求

防护对象		防护目标要求	
		系统安全目标要求	接口安全目标要求
R_{ref}	运营平台	√	√
R_{ref}	充电设备	√	√
R_{ref}	移动智能终端	√	√
I_{ref}	设备与运营平台之间接口	√	√
I_{ref}	设备与移动智能终端之间接口	√	√
I_{ref}	设备与电动汽车之间接口	—	√
I_{ref}	运营平台与其他平台之间接口	—	√
注：“—”指本标准不涉及，“√”指本标准涉及。			

4.2 基础架构与接口

4.2.1 信息基础架构

电动汽车充电设施信息交换基础架构如图 2 所示。从信息基础架构上看，信息安全防护对象包括信息服务系统和信息交换接口。



⟺ 已经定义的信息交换接口
⟷ 待定义的信息交换接口

注：本标准涉及*I*接口的约定，具体约定参照具体相关协议约定。

图 2 电动汽车充电设施信息交换基础架构

4.2.2 信息服务系统

信息服务系统指以处理电动汽车充电服务信息为核心的应用系统，是充电运行网络中的主要服务单元。信息服务系统包括平台系统、设施系统和终端系统。主要功能及要求见表 2。

表 2 信息服务系统主要功能及要求

系统	平台主要功能	信息安全防护重点要求
平台系统	实现联网监测、运行管理、客户服务和计费账务等功能	重点防护基础系统平台、网络、基础软件和业务系统的安全可靠运行，免受恶意攻击，确保系统服务可用
设施系统	实现身份认证、充电、联网、监测功能	重点防护充电设备的设备安全可靠运行，数据安全管理，控制安全可信执行
终端系统	实现用户能够获得充电服务，完成充电服务交易与缴费功能	重点防护 App 终端运行机制安全，应用管理安全、防止恶意行为等

4.2.3 信息交换接口

信息服务系统之间通过信息交换接口实现信息交换，完成业务协同。充电运行网络中的主要信息交换接口有 6 种类型，接口类型与连接关系如图 2 所示，接口功能及要求见表 3。

表 3 信息交换接口功能及要求

接口	接口定义	接口主要功能	信息安全防护重点要求
I1	电动汽车与充电设备之间的信息接口	电动汽车与充电设备之间的通信功能，实现设备充电认证和充电中安全管理与监测	重点防护避免仿冒获取和控制充电控制信息，须对物理接口、现场电缆和无线网络通信等有明确的监测和管理要求
I2	充电设备与运营平台之间的信息接口	充电设备与运营平台之间的通信功能，实现设备远程监控和管理服务	重点防护基于互联网链路下的数据通信网络和控制信息安全，须对充电设备远程通信协议格式、交互机制、异常监测和处理流程等有明确的监测和管理要求
I3	运营平台与支付系统之间的信息接口	运营平台与支付平台之间的通信功能，完成支付结算功能	重点防护账户信息安全，应达到支付认证信息安全要求（第三方支付平台安全保证）
I4	运营平台之间的信息接口	运营平台之间的通信功能，完成平台之间数据共享和互联互通，实现漫游服务	重点防护平台间的数据通信网络和控制信息安全，须对平台之间通信协议格式、交互机制、异常监测和处理流程等有明确的监测和管理要求
I5	移动智能终端和充电服务凭证与充电设备之间的信息接口	移动智能终端或充电服务凭证与设备之间的通信功能，实现服务接入、身份认证与充电授权	重点防护在充电设施现场环境下，不同终端或凭证在身份认证和业务认证过程信息的保密性、完整性和可用性，须对通信协议格式和数据规范等有明确的监测和管理要求
I6	移动智能终端和充电服务凭证与运营平台之间的信息接口	移动智能终端或凭证与运营平台之间的通信功能，实现充电服务接入、身份认证与充电授权	重点防护在互联网环境下，不同终端或凭证在身份认证和业务认证过程信息的保密性、完整性和可用性，须对通信协议格式和数据规范等有明确的监测和管理要求

5 信息安全技术要求

5.1 运营平台技术要求

5.1.1 系统安全防护

5.1.1.1 系统配置应具备至少双节点的冗余配置，网络接入应具备至少双链路的接入方式，以避免硬件

单节点故障或单网络链路的中断而导致业务系统瘫痪。

5.1.1.2 服务器主机应采用双机配置以冷备用或热备用的方式进行冗余防护，若采用租用云服务的方式则应考虑增加计算资源节点的冗余数量。

5.1.1.3 网络及安全设备在配置时应与接入的网络链路相匹配，在采用双链路接入配置的方式时，网络及安全设备应配置为双节点的方式。

5.1.1.4 应配置安全设备或同等功能的组件。

5.1.1.5 存储资源在配置时应根据运营平台的业务数据规模核算具体容量。自建数据中心时，在保证服务器设备自身的存储空间充足时，还应配置独立的存储设备，并应双机配置或采用异地数据中心备份的方式。租用云服务时应提供冗余配置的存储资源或异地备份。

5.1.2 网络安全防护

5.1.2.1 运营平台系统应根据不同的业务进行分区分域，将系统划分为不同的子网网段。

5.1.2.2 重要服务器主机及核心业务区应部署在内网区域，通过路由设备建立安全的访问路径，避免其直接与外网进行连接；核心业务区与其他日常业务网段划分不同子网，并采取可靠的技术隔离手段。

5.1.2.3 网络接入的出入口访问应通过安全防护设备进行控制与隔离，建立完善的过滤策略及入侵防范策略。

5.1.2.4 对网络的访问权限进行控制，平台应具备安全审计的防护标准；对运营业务中产生的数据和操作进行日志记录，并可进行备份。

5.1.2.5 各业务系统区域应具备独立且完整的硬件及网络规划，以避免各业务阶段使用的硬件或基础资源混乱而造成对正式运营系统的影响。

5.1.2.6 重要的运营平台生产系统宜具备双活热备的系统配置，可自主切换业务。

5.1.2.7 提供对充电设备的网络访问行为能力，对异常行为进行阻断。

5.1.3 基础软件安全防护

5.1.3.1 操作系统及相关组件应定期更新升级补丁，确保系统软件的稳定可靠。

5.1.3.2 应定期对系统应用进行漏洞扫描，进行监测入侵防范及恶意代码防范。

5.1.3.3 应实时对系统进行安全监控，保证对系统应用的各操作合法并有操作审计记录。

5.1.3.4 各主机基础软件均应具有严格的身份认证配置，口令应具有一定的复杂度，并定期进行更换。

5.1.3.5 应实时监控各服务器硬盘存储资源，并具备实时提醒告警等功能。

5.1.4 业务系统安全防护

5.1.4.1 业务软件应配置至少双冗余的结构，避免因业务软件的崩溃造成应用单节点故障，导致业务功能无法使用，影响业务运营系统。

5.1.4.2 业务软件在对外进行数据交互时，应有本运营公司的数据交互协议或加密方式，避免在交互过程中造成数据混乱无法识别或被非法解析导致数据信息泄露。

5.1.4.3 业务软件在交互过程中应具备自有的数据校验机制，对其数据传输的完整性、安全性进行保障。

5.1.4.4 业务信息中具有重点需要防护的数据敏感信息时，应有数据脱敏的机制。

5.1.4.5 业务系统功能的操作安全防护应配置审计系统，各业务操作应详细记录。

5.1.4.6 业务系统应按实际运营情况中发现的问题漏洞实施业务系统的更新升级，并明确备案各阶段版本及更新说明。

5.1.4.7 业务数据应配置数据备份机制，根据运营需求确定历史数据的缓存时间及备份数量。

5.1.4.8 应对实时访问行为进行监测，及时告警异常行为。

5.2 充电设备技术要求

5.2.1 设备安全

5.2.1.1 设备的进、出线孔应使用合适的装置或适当的措施密闭，防止外部仪器工具的进入。
5.2.1.2 设备内部的通信部件应有明显的难以去除的标记，以防被更换。
5.2.1.3 充电设备检测到异常应主动告警并禁止充电。
5.2.1.4 操作系统应保证代码可控或采用必要安全加固措施。
5.2.1.5 应建立能够识别充电设备本体代码、主动阻断未知代码执行的安全免疫机制，通过对充电设备本体代码的完整性校验，防止其被篡改并可以在异常状态下执行自动恢复。
5.2.1.6 以最小化安装方式配置软件，对非必要功能的使用进行禁止或限制。
5.2.1.7 应对系统软件升级且充电设备业务应用的加载软件应具备认证机制，只有经过认证的软件才能在本体系统上运行。

5.2.2 数据安全

5.2.2.1 充电设备具备本机充电记录读取功能，不应显示用户完整的敏感信息。
5.2.2.2 未经使用者授权，充电设备不应主动获取或向第三方提供充电权限认证以外的信息。
5.2.2.3 充电设备应具备数据有效性校验功能，保证数据符合系统设定要求。
5.2.2.4 未经授权的任何实体不能从加密存储区域的数据中还原出用户隐私数据的真实内容。
5.2.2.5 不应未经授权擅自修改和展示用户信息。
5.2.2.6 充电设备应保证存储和传输过程中数据的完整性。
5.2.2.7 充电设备应保证存储和传输过程中敏感数据的保密性。

5.2.3 控制安全

5.2.3.1 充电设备维护、升级、调试等过程中，应使用身份认证管理技术。
5.2.3.2 具有账号管理功能的充电设备，其用户身份鉴别信息应具有复杂度要求。
5.2.3.3 具有账号管理功能的充电设备，应提供并启用登录失败处理功能；多次登录失败后应采取必要的保护措施，当超出限制值时，采取特定的动作。
5.2.3.4 具有账号管理功能的充电设备，在用户身份认证信息丢失或失效时，可提供鉴别信息恢复机制。
5.2.3.5 具有账号管理功能的充电设备应对登录的用户分配账号和权限。
5.2.3.6 具有账号管理功能的充电设备应及时删除或停用多余的、过期的账号，避免共享账号的存在。
5.2.3.7 充电设备外部访问接口应采取安全保护措施。
5.2.3.8 充电设备应具备控制接入的开关。当建立数据连接时，充电设备能够发现该连接并给用户相应的状态提示，仅当用户确认建立本次连接时，连接才可建立。
5.2.3.9 充电设备应为不同访问主体类别提供不同的访问权限。访问权限划分应遵循最小特权原则。
5.2.3.10 关闭非系统运行和维护所必需的网络通信端口。
5.2.3.11 未授权用户不得读取审计信息。
5.2.3.12 应能按照频次将所有的审计记录备份至本地，或者将事件数据安全地发送到外部。
5.2.3.13 充电设备应保护已存储的审计记录，以避免未授权的删除、修改或覆盖，并检测对审计记录的修改。
5.2.3.14 充电设备应确保审计记录保持一定的记录数和维持时间，审计日志留存能力不少于 10000 条。
5.2.3.15 审计日志要覆盖对设备有较大影响的操作。

5.3 移动智能终端软件技术要求

5.3.1 运行机制要求

5.3.1.1 在安装和卸载过程中，不得捆绑下载其他应用软件；不得安装功能说明文档中未说明的额外功能，不得安装用户未知和未允许的第三方应用。
5.3.1.2 卸载应彻底，卸载后不应残留相关临时文件、活动程序或模块。
5.3.1.3 包含可有效表征供应者或开发者身份的签名信息、软件属性信息。
5.3.1.4 应对安装包或升级包的完整性、合法性进行校验。

5.3.2 应用安全要求

5.3.2.1 应具备身份鉴别功能，能够对登录用户进行身份标识和鉴别。
5.3.2.2 不应内置匿名账户，禁止匿名用户的登录。
5.3.2.3 具备口令强度和口令时效性检查机制。
5.3.2.4 授权用户访问的内容不能超出授权的范围。
5.3.2.5 未得到许可前不应访问终端数据和终端资源。
5.3.2.6 未得到允许前不应修改和删除终端数据。
5.3.2.7 未授权用户不得读取审计信息。
5.3.2.8 应能按照频次将所有的审计记录备份至本地，或将事件数据安全地发送到外部。
5.3.2.9 审计日志留存时间应不少于 6 个月。
5.3.2.10 未经授权的任何实体不能从加密存储区域的数据中还原出用户私密数据的真实内容。
5.3.2.11 不应存在数据存储和处理过程中的非法调用和窃取漏洞。
5.3.2.12 不应以明文形式存储或通过网络传输用户敏感数据，以防止数据被未授权获取。
5.3.2.13 备份机制应完整有效，且应对备份数据进行保护。

5.3.3 恶意行为防范要求

5.3.3.1 在用户不知情或未授权的情况下，应用程序不应订购非法业务。
5.3.3.2 在用户不知情或未授权的情况下，应用程序不应非法获取信息。
5.3.3.3 在用户不知情或未授权的情况下，应用程序不应接受远程控制端指令并进行相关操作。
5.3.3.4 应用程序不应导致电动汽车智能终端无法正常使用。

5.3.4 其他安全要求

5.3.4.1 应用软件代码应防止被反编译和反调试。
5.3.4.2 源代码中不存在已公布的高危风险漏洞。
5.3.4.3 应用软件应做日志防泄漏措施。

5.4 接口安全技术要求

5.4.1 充电设备和运营平台之间的接口

5.4.1.1 充电设备与运营平台之间的通信应优先采用硬件加密认证设备进行认证加密，对来源于运营平台的控制命令和参数设置指令应采取安全鉴别和数据完整性验证措施。
5.4.1.2 充电设备与运营平台之间的业务数据应采取加密措施，实现数据的保密性，并且应该符合国家相关的管理规定。禁止使用已知为不安全的加密算法和安全措施。

5.4.1.3 充电设备应具备防网络干扰功能，在网络瘫痪等紧急情况下，可通过备用方案保证充电设备的正常使用。备用方案启动应有明确标识，在网络恢复后，充电设备应主动上传网络异常状态和备用方案充电记录。

5.4.1.4 需远程维护的，采用安全加密协议或虚拟专用网络等技术建立安全的访问路径、可信的通信通道确保远程接入安全。

5.4.2 充电设备和电动汽车之间的接口

5.4.2.1 充电设备和电动汽车之间的通信网络应通过安全网关与外部网络进行隔离，由网关进行可信消息的分发和处理。

5.4.2.2 协议应用数据不应使用明文传输，由应用协议负责安全加密机制的实现。

5.4.2.3 充电设备和电动汽车建立安全的传输通道后，通信双方应能验证消息的完整性。

5.4.3 运营平台之间的接口

5.4.3.1 应采用多因子认证方式进行平台认证，保障信息交换接口安全、稳定、可靠地运行。

5.4.3.2 应采用 IP 访问控制、时间访问控制等手段或结合使用，以限制同一终端在一定时间内对平台数据接口的高频访问。

5.4.3.3 消息发送方应对消息字段中涉及交易及隐私等数据采用安全可靠且普遍使用的加密算法，消息接收方在校验参数合法性后方可进行后续业务处理。

5.4.3.4 消息报文应使用数字签名、重发机制等方式保障传输和接收数据的完整性。

5.4.4 以移动智能终端作为认证接口

5.4.4.1 设备上附属的二维码应具备适当的加密机制。在二维码编码前进行加密，以保证只有通过解密识别的扫码设备才能正确识别出设备信息。

5.4.4.2 二维码中涉及的关键、敏感数据需要进行安全保护。

5.4.4.3 通过移动智能终端扫描二维码获得服务凭证，必须与后台进行信息交换，获得真实的服务认证结果。

5.4.4.4 移动智能终端与运营平台进行的认证服务过程，应采用安全传输方式。二维码涉及各系统之间信息传输，各系统之间应建立安全通信通道，应对交易数据采用安全方式进行传输，确保数据不被监听和篡改。

5.4.4.5 应对传输的数据进行保密性保护，不应引起信息泄露。

5.4.4.6 应具备对传输数据的鉴别机制，确保发出数据的完整性和接收数据完整性。

5.4.5 以智能卡作为认证接口

5.4.5.1 应用管理数据在卡片的初始化期间建立，应定义初始的安全域。

5.4.5.2 发卡机构应建立可靠、完善的密钥管理制度。

5.4.5.3 应采用合适的认证操作，包括持卡人认证、卡认证和终端认证。

5.4.5.4 应对被保护区域的访问建立存取权限控制。

5.4.5.5 应在数据传输过程建立加密机制。