**电动汽车充电设施信息安全防范技术规范**

# 总则

* 1. 为保障电动汽车充电基础设施信息安全，减少信息安全危害，保护用户隐私、人身和财产安全、公共安全，制定本规范。
  2. 本规范适用于与充电基础设施相关的各类企业；
  3. 充电基础设施的信息安全防护，必须遵循国家有关方针、政策，针对不同类型的信息安全威胁，立足自防自查，采取可靠有效的防护措施，做到安全可靠、经济合理、方便适用；
  4. 对于充电基础设施的信息安全防护，除应符合本规范的规定外，尚应符合国家现行有关标准的规定。

# 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。凡是注日期的文件，仅注日期的版本适用于本文件。凡是不住日期的版本，其最新版本（包括所有修改版本）适用于本文件。

GB/T 9387.1 信息技术 开发系统互联 基本参考模型 第1部分：基本模型

GB/T 19596-2004 电动汽车术语

GB/T 29371-2012 电动汽车充换电设施术语

T/CEC 102.4 电动汽车充换电服务信息交换 第四部分：数据传输及安全

GB/T 25070 信息安全技术 信息系统等级保护安全设计技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GA-T 708-2007 信息安全技术 信息系统安全等级保护体系框架

GB/T 5271.8 信息技术词汇第8部分：安全

GB17859-1999 计算机信息系统安全保护等级划分准则

GB/T AAAA-AAAA 信息安全技术信息系统安全等级保护定级指南

GB/T 11457-2006 信息技术 软件工程术语

GB/T 15532-2008 计算机软件测试规范

GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

GB/T 16260.2-2006 软件工程 产品质量 第2部分:外部度量

GB/T 16260.3-2006 软件工程 产品质量 第3部分:内部度量

GB/T 16260.4-2006 软件工程 产品质量 第4部分:使用质量的度量

GB/T 18336.1-2015 信息技术 安全评估准则 信息技术安全性评估准则

GB/T 18336.2-2015 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

GB/T 18336.3-2015 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求

YD/T 2407-2013 移动智能终端安全能力技术要求

YD/T 2439-2012 移动互联网恶意程序描述格式

YD/T 3082-2016 移动智能终端上的个人信息保护技术要求

YD/T 3039-2016 移动智能终端应用软件安全技术要求

中华人民共和国国务院令（292号令）《互联网信息服务管理办法》

# 术语

* 1. **充电基础设施**

充电运营网络中能够提供对外充电服务的充电桩，充电桩群和充电站均属于充电基础设施。

* 1. **运营平台**
  2. **充电设备**
  3. **支付方式**
  4. **移动终端**
  5. **通信协议**
  6. **网络边界**
  7. **授权 Authorization**

在用户身份经过认证后，根据预先设置的安全策略，授予用户相应权限的过程。

* 1. **Root权限 Root permission**

系统权限的一种，是Linux和Unix系统中超级管理员账号。Root权限是系统最高权限，可以对系统中任何文件（包括系统文件）执行操作。

* 1. **符合性评价 Conformity Evaluation**

对产品、过程或服务达到规定要求的程度所进行的系统性考核。

* 1. **数据安全 Data Security**

适用于数据的智能终端安全。

* 1. **数字签名 Digital Signature**

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者验证数据的来源和完整性，保护数据不被篡改、伪造，并保证数据的不可否认性。

* 1. **恶意代码 Malcious Code**

编写者以破坏计算机系统的安全性、可用性、完整性和正常使用为目的的程序指令，并可以在未经授权的情况下，在信息系统中安装、执行以达到不正当目的。

* 1. **恶意软件 Malware**

含有恶意代码的应用软件。

* 1. **恶意收费 Malicious Charge**

在用户不知情或未授权的情况下由终端上应用软件造成的用户经济损失。

* 1. **敏感信息 Sensitive Information**

需要保护的信息，该信息的泄漏、修改、破坏或丢失都会对人或事缠身可预知的损害。

* 1. **智能终端 Smart 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，并能够安装和运行第三方应用软件的移动终端。

* 1. **测试 Test**

在规定的条件下执行系统或组件、对结果进行观察或记录，并就该系统或该组件的某些方面作出评价的活动。

* 1. **测评环境 Test environment**

对被测对象进行合格性测试和评价时所需要的设施、硬件、软件、固件、规程和文档集等。

* 1. **测评报告 Evaluation Report**

说明对被测对象实施评价的行为和结果的文档。

* 1. **用户 User**

使用智能终端资源的对象，包括人或第三方应用程序。

* 1. **用户数据 User Data**

智能终端上存储的用户个人信息，包括由用户在本地生成的数据、为用户在本地生成的数据、在用户许可后由外部进入用户数据区的数据等。

* 1. **个人信息 Personal Information**

可为信息系统所处理，与特定自然人相关、能够单独或通过其他信息结合识别该特定自然人的计算机数据。

* 1. **支付网关 Payment Gateway**

银行或指派的第三方金融网络系统与Internet网络之间的接口，用于将Internet上传输的数据转换为金融机构内部数据的一组服务器设备。

* 1. **测评资源 Test resource**

测评活动中各种要素的总称。“要素”包括测评场地、软硬件设备、文档、测评人员、资金等。

* 1. **AES（Advanced Encryption Standard）**

高级加密标准，NIST于 2001年11月开始采用的块加密标准。

* 1. **MD5（Message-Digest Algorithm 5）**

单向散列算法，用以提供消息的完整性保护，具有唯一性与不可逆性。

* 1. **SSL （Secure Sockets Layer）**

位于TCP/IP协议与各种应用层协议之间的一种安全协议，提供用户和服务器认证服务，为数据通讯提供安全及数据完整性的支持。

* 1. **缩略语**

下列缩略语适用于本标准。

APP：应用程序(Application)

SQL：结构化查询语言（Structured Query Language）

URL：统一资源定位地址（Uniform/Universal Resource Lacator）

WLAN：无线局域网（Wireless Local Area Network）

XSS：跨站脚本（Cross Site Scripting）

# 充电设施信息安全防护框架

* 1. **信息安全防护框架**

电动汽车充电设施网络是一个基于信息基础架构的信息网络拓扑，信息网络拓扑由若干信息参考点和参考连接组成。

组成信息网络拓扑的信息参考模型有两种类型：

一种是实体，即信息参考点R。对于实体，采用系统安全要求进行安全防护规范。

一种是接口，即信息参考连接I。对于接口，采用接口安全要求进行安全防护规范。

参考信息参考模型，电动汽车充电设施网络信息安全防护框架整体上由技术安全要求和管理安全要求组成。信息安全技术要求包括系统安全要求和接口安全要求。

充电设施网络信息安全防护框架如图4-1所示。

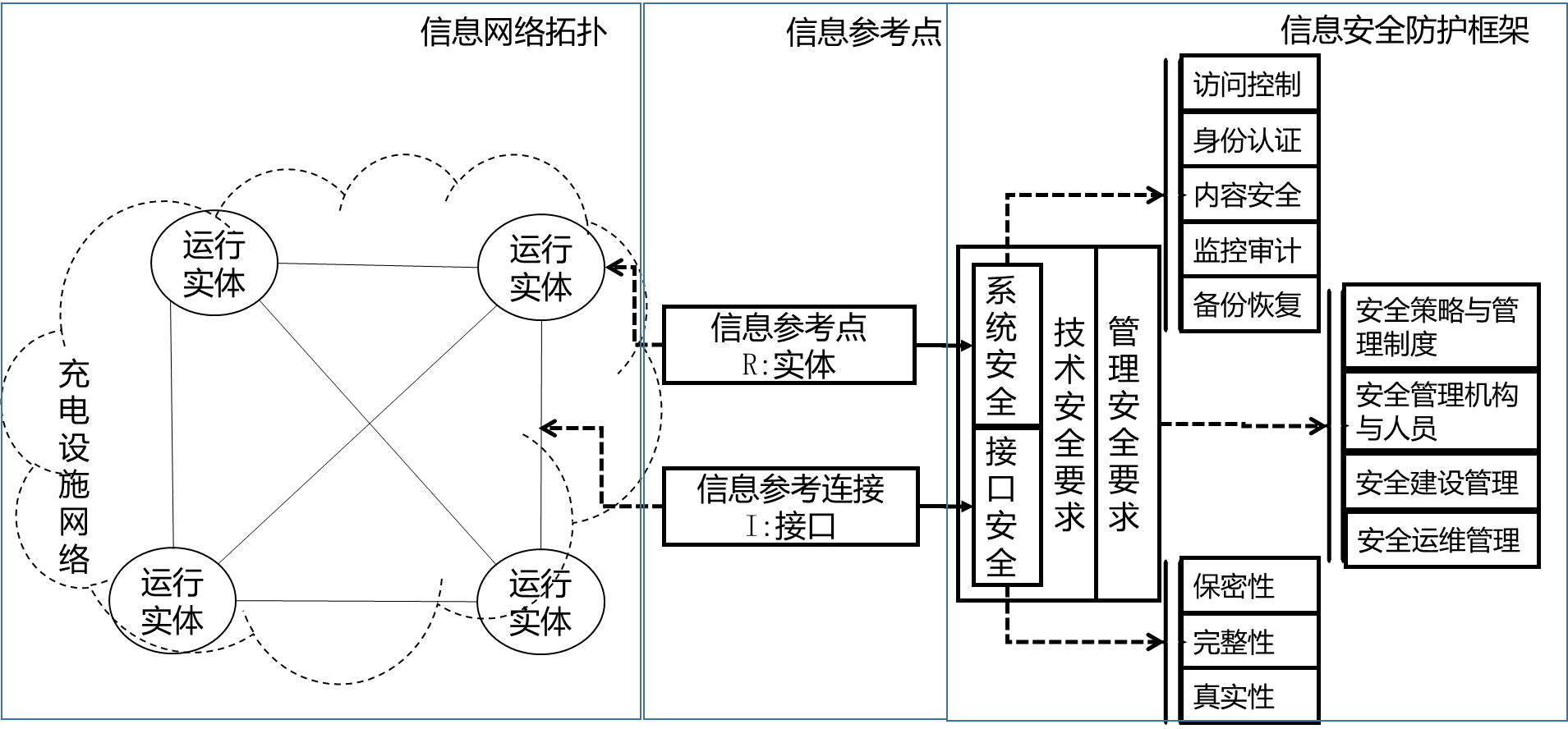


图4-1 充电设施网络信息安全防护框架

* 1. **信息安全基础架构**
     1. **信息架构**

结合信息参考模型，电动汽车充电设施服务网络是由若干信息服务运行实体以及运行实体之间的信息交换接口组成。基于电动汽车充电设施服务的信息基础架构如下图4-2所示。

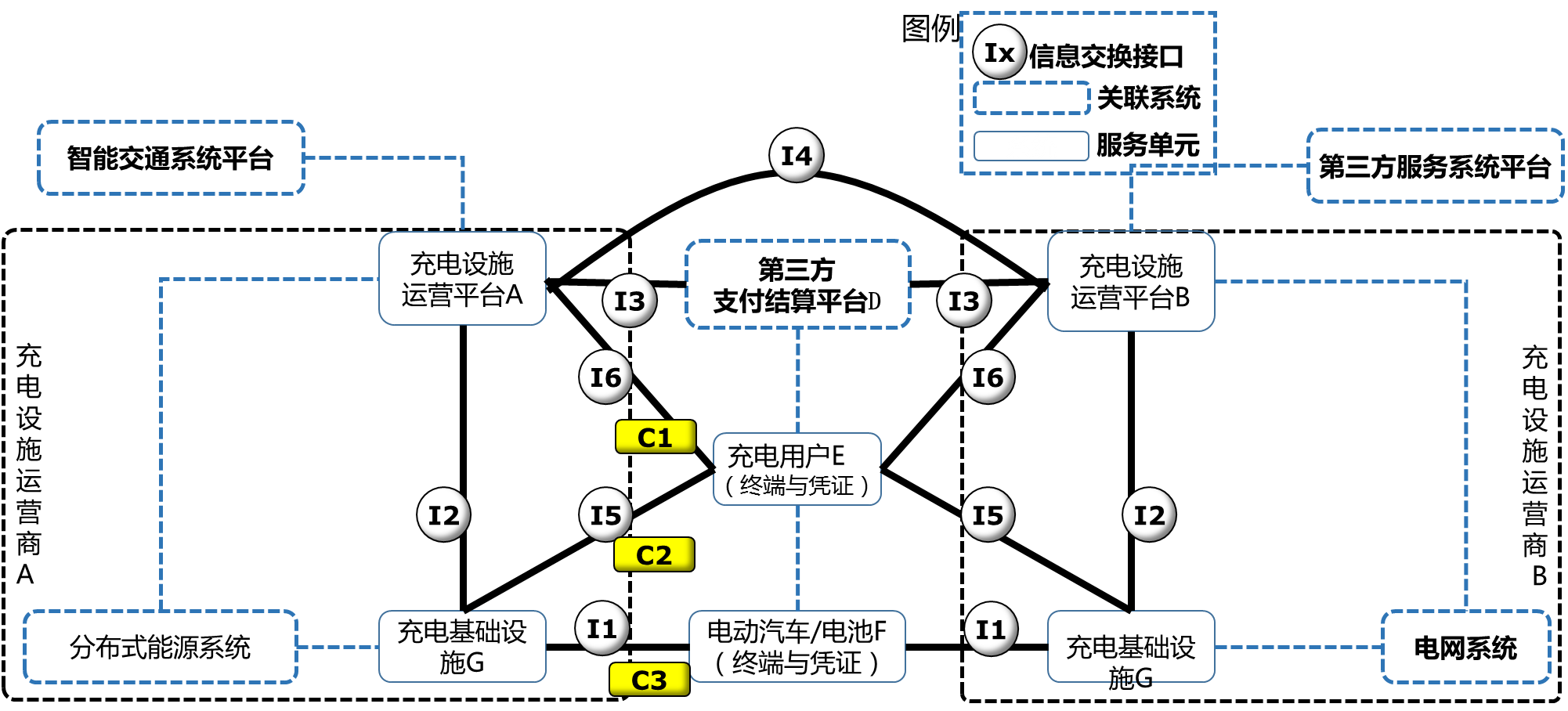


图4-2 充电设施网络信息交换基础架构

根据充电设施网络信息交换基础架构，充电设施网络信息安全的安全防护对象主要包括信息服务运行实体和信息交换接口。

* + 1. **信息服务运行实体**

信息服务运行实体由充电运行网络中的主要服务单元组成，包括平台和设施、终端和凭证。

（1）平台

平台主要承担充电服务功能的运行和提供，由服务系统和关联系统组成。

（a）服务系统是支持充电运营服务提供的基础系统平台。对于服务系统在信息系统安全角度提出明确的技术要求和管理要求，由本技术规范进行规范约束。参与信息安全防范的运行实体包括服务系统软件平台。

（b）关联系统是与服务系统之间进行业务协同和信息交换的外围系统平台。对于关联系统在信息系统安全角度由外围系统按照IT信息系统安全规范自行约束，不在本技术范围重复约束。关联系统包括分布式能源系统、电网系统、第三方支付结算平台、第三方服务平台和智能交通平台。

（2）设施

设施主要承担充电服务功能的交直流充电设备，以及周边配套设备以及基础设施。参与信息安全防范的运行实体包括设施硬件、以及设施内置的功能软件。

（3）终端

终端主要是指电动汽车用户使用的智能终端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。参与信息安全防范的运行实体包括智能终端APP系统与软件应用。

（4）凭证

凭证主要是指电动汽车用户提供用于完成充电身份认证，标识充电服务计费依据的信息结构。

* + 1. **信息交换接口**

各个信息服务运行实体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4-2所示。接口功能说明如表4-1所描述：

表4-1 信息交换接口

|  |  |  |  |
| --- | --- | --- | --- |
| 接口 | 接口定义 | 接口主要功能 | 信息安全目标 |
| I1 | 电动汽车与充电设施之间的信息接口 | 车与充电站设备之间的通信 | 包括物理接口与现场电缆通信和无线局域网络，相关充电控制信息容易受到攻击，安全相关标准有待研究增强； |
| I2 | 充电设施与后台系统之间的信息接口 | 充电站设备与服务系统平台通信，实现设备远程监控和管理服务 | 涉及互联网链路，数据通信网络的安全，技术相对成熟，但控制信息安全性目前缺乏约束性要求 |
| I3 | 服务系统平台与支付系统之间的信息接口 | 服务系统平台与支付平台的通信，完成支付结算有关功能。 | 通信采用网络专线服务等级，应达到支付认证信息安全要求(第三方支付平台安全保证)，目前较普遍采用的后台账户认证模式需要进一步增强安全措施； |
| I4 | 服务系统平台之间的信息接口 | 服务系统平台之间的通信，完成平台之间数据共享和互联互通，实现漫游服务。 | 信息共享及漫游服务：需做好数据隐私保护，采取数据加密、数据清洗技术，并统一建立安全技术标准 |
| I5 | 用户应用终端和凭证与设备系统之间信息接口 | 用户应用终端与凭证与设备之间的通信，实现服务接入和身份认证 | 与身份认证和业务认证有关：本地链路，重点在规范数据通信网络安全范畴及身份认证技术 |
| I6 | 终端和凭证与服务系统平台之间信息接口 | 用户应用终端与凭证与服务系统平台之间的通信，实现服务接入和身份认证 | 与身份认证和业务认证有关：互联网链路，重点在规范数据通信网络安全范畴及身份认证技术 |

* 1. **信息安全总体要求**
     1. **通用目标要求**

根据充电基础设施网络信息交换基础架构,充电设施信息安全防范的总体要求包括两方面内容，即面向充电设施服务网络中安全防护对象进行安全防范的技术安全要求和管理安全要求。

（1）技术安全要求

技术要求包括系统安全要求和接口安全要求

（a）系统安全要求：保护系统安全可靠运行，免受恶意攻击，确保系统服务可用的信息安全要求。系统安全要求分为五个重点部分：身份认证、访问控制、内容安全、监控审计和备份恢复。

（b）接口安全要求：保护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、破环和免受未授权的信息安全要求。接口安全要求分为三个重点部分：保密性、完整性和真实性。

（2）管理安全要求

管理安全要求：保护系统安全可靠运行，免受恶意攻击，确保系统服务可用的信息安全要求。管理安全要求分为四个重点：安全管理策略与制度，安全管理机构与人员，安全建设管理，安全运维管理。

* + 1. **系统安全目标分类**

系统的技术要求按照安全防护对象获得的安全防护效果划分为五个目标要求类型：

（a） CIS-A类要求，即访问控制，达到访问控制要求，即明确限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。

（b） CIS-B类要求，即身份认证，达到权限控制要求，即明确系统设置的安全规则或者安全策略，用户可以访问而且只能访问自己被授权的资源。

（c） CIS-C类要求，即内容安全，达到权限控制要求，即明确系统设置的安全规则或者安全策略，用户可以访问而且只能访问自己被授权的资源。

（d） CIS-D类要求，即监控审计，达到权限控制要求，即明确系统设置的安全规则或者安全策略，用户可以访问而且只能访问自己被授权的资源。

（e） CIS-E类要求，即备份恢复，达到权限控制要求，即明确系统设置的安全规则或者安全策略，用户可以访问而且只能访问自己被授权的资源。

* + 1. **接口安全目标分类**

（a） CXS-A类要求，即保密性，达到加密控制要求，即明确采用加密计划，改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。

（b） CXS-B类要求 即完整性, 应避免或至少检测到发送信息的未经授权的修改

（c） CXS-C类要求 即真实性，任何一方无法否认已发生的数据

* + 1. **管理安全目标分类**

管理要求按照安全防护对象实施过程划分为4个类型：

（a） CIM-A制度要求，达到制度管理规范要求，即明确策略、制度、机构、人员以及建设管理过程的安全管理要求。

（b） CIM-B机构要求，达到组织机构构建和人员管理要求，即安全组织机构、人员岗位， 职责分工等安全管理要求。

（c） CIM-C建设要求，达到信息系统建设管理要求，即系统设计、部署等建设过程的安全管理要求。

（d） CIM-D安全运维要求，达到运维管理规范要求，即明确日常运行管理过程中通用和应急处理过程的安全管理要求。

* 1. **信息安全分类要求**
     1. **技术安全要求**

信息服务运行实体的安全防护的技术要求在于系统安全。信息交换接口的安全防护的技术要求在于接口安全。

1. 信息服务运行实体的系统安全

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 安全防护对象 | | 对应具体要求所在章节描述 | 典型用例 | 系统安全 | | | | |
| 技术要求 | | | | |
| CIS-A | CIS-B | CIS-C | CIS-D | CIS-E |
| 信息服务运行实体 | 设施 | 5.2 | 交/直流充电桩(群)  充电场站 | √ | √ | NA | NA | NA |
| 终端 | 5.3 | 智能手机 | √ | √ | √ | √ | √ |
| 凭证 | 5.4 | 卡，二维码，PnC | NA | NA | √ | √ | √ |
| 服务系统 | 5.1 | 充电设施运营平台 | √ | √ | NA | NA | NA |
| 关联系统 | NA | 第三方服务平台等 | NA | NA | NA | NA | NA |

1. 信息交换接口的接口安全

信息服务运行实体之间通过信息交换接口实现信息交换，完成业务协同。由充电运行网络中的主要业务单元信息交换接口组成，包括图中I1-I6表示信息接口,其中:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 安全防护对象 | | 对应具体要求所在章节描述 | 对应要求 | 接口安全 | | |
| 技术要求 | | |
| CXS-A | CXS-B | CXS-C |
| 信息交换接口 | I1接口 | 5.5.2 | 车与桩的充电接口 | NA | √ | √ |
| I2接口 | 5.5.1 | 设备远程监控接口 | √ | √ | √ |
| I3接口 | 5.5.4 | 支付结算接口 | √ | NA | √ |
| I4接口 | 5.5.4 | 共享接口 | √ | √ | √ |
| I5接口 | 5.5.5 | 终端/凭证到平台的接口 | √ | √ | √ |
| I6接口 | 5.5.3 | 终端App /凭证到设备的接口 | √ | √ | √ |

* + 1. **管理安全要求**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 安全防护对象 | | 对应具体要求所在章节描述 | 对应要求 | 管理安全 | | | |
| 管理要求 | | | |
| 制度 | 机构 | 建设 | 运维 |
| 运行实体 | 设施 | 7.3/7.4 | 交/直流充电桩(群)  充电场站 | NA | NA | √ | √ |
| 服务系统 | 7.1/ 7.2/7.3/7.4 | 充电设施运营平台 | √ | √ | √ | √ |

# 信息安全技术要求

* 1. **运营平台技术要求**

运营企业按运营能力及业务发展需要，可选择自建数据中心或租用云服务的方式来建设运营服务平台；

自建数据中心时需要规划以下安全防护内容：包括运营平台数据中心机房的选址要求、建设场地规模、出入口访问控制制度、防盗窃和防破坏、防雷击、防火、防水、防潮、防静电要求以及温湿度控制等，同时需要进行电力供应保障，并做到电力电磁防护。

本部分安全防护等级的具体要求及内容须遵循《信息系统等级保护第三级基本要求》中“1.1技术要求-1.1.1物理安全”章节的内容。

租用云服务的方式进行建设运营平台时，同样需要考量云服务提供商的数据中心机房安全保护等级，其必须符合《信息系统等级保护第三级基本要求》（及以上）的标准进行搭建。

（1）基础资源安全防护

运营商在自建数据中心时，需配置的物理硬件包括网络设备、服务器主机、存储设备、安全防护设备等；运营商选择租用云服务的方式时，则需配置虚拟资源，主要包括计算资源、网络资源、存储资源以及安全防护组件等。

基础资源的配置均需具备至少双节点的冗余配置，网络接入需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。

服务器主机需采用双机配置以冷热备的方式进行冗余防护，租用云服务的方式则需考虑增加计算资源节点的冗余数量。

网络及安全设备在配置时需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，网络及安全设备需配置为双节点的方式。

应配置安全设备或同等功能的组件。

存储资源在配置时需根据运营平台的业务数据规模进行核算具体容量，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，还需配置独立的存储设备，并需双机配置或采用异地数据中心备份的方式；租用云服务时需提供冗余配置的存储资源或异地备份。

基础资源的设计架构应需具备在业务规模扩展时可及时灵活扩容调整的机制，不可因为业务功能或规模的调整影响整体系统运营。

（2）网络安全防护

运营平台系统应根据不同的业务划分为不同的子网网段。

重要服务器主机及核心业务区需部署在内网区域，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。

网络接入的出入口访问需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。

需保证主要网络设备的业务处理能力具备冗余空间、网络各部分带宽均可满足业务高峰期需要；并可按业务优先级灵活配置网络访问出入口流量。

对于网络的访问权限进行控制，平台需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。

此部分内容须遵循《信息系统等级保护第三级基本要求》中“1.1技术要求-1.1.2网络安全”章节的内容。

（3）业务区域隔离

根据运营平台业务功能需配置不同的业务区域，各区域需相对独立、互相隔离。

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。

对于重要的运营平台生产系统至少要具备热备双活可自主切换业务的系统配置，或具备主备的双活运营生产系统数据中心。

（4）基础软件安全防护

基础软件主要指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。

基础软件的选用必须使用正版或开源的软件及组件。

操作系统及相关组件需定期更新官网升级补丁，确保系统软件的稳定可靠。

应定期及时的对系统应用进行漏洞扫描，实时进行监测入侵防范及恶意代码防范。

实时对系统进行安全监控，保证对于系统应用的各操作合法并有操作审计记录。

各主机基础软件均需具有严格的身份鉴别配置，密码需复杂化，并定期进行更换。

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）业务系统安全防护

业务系统是为平台的终端用户和业务操作人员提供服务的系统。

所有业务软件均需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；

所有业务软件应为运营平台公司自主研发的知识产权，避免公版的应用造成数据信息泄露。

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泄露数据信息；

业务软件在交互过程中需具备自有的数据校验机制，对其数据传输的完整性进行安全保障。

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。

业务系统功能的操作安全防护应配置审计系统，记录各业务操作详细记录，并可隔离非法操作。

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；

业务数据需配置数据备份机制，根据运营需求确定历史数据的缓存时间及备份数量。

* 1. **充电设备技术要求**
     1. **概述**

本标准提出了充电设备的安全技术要求，重点内容为充电设备本体系统安全、充电设备数据安全、充电设备访问控制安全等共三项内容。

**充电设备本体系统安全**提出了充电设备生产商的本体系统安全技术规范，规范本体系统所提供的服务、功能、防护手段等，以及本体系统为保障安全而进行的持续性改进。

**充电设备数据安全**提出了充电设备本身数据储存以及与其他系统进行数据传输的规范要求，包括设备数据存储安全、数据传输安全等。

**充电设备访问控制安全**提出了对充电设备的使用、管理、应用系统接口调用等访问行为的安全控制，包括身份鉴别、访问控制、日志审计等。

* + 1. **防护原则**

（1）业务保障原则

充电设备防护策略的实施应确保本体系统以及上层应用软件可以正常运行，将对系统运行的影响最小化。

（2）技术可行性原则

防护策略应优先采纳技术成熟、可落地的安全技术手段，在全面推广之前应至少经过试点验证或者小范围推广证实其可行、有效。

（3）通用性原则

安全防护手段应具有一定通用性，可以解决普遍性问题，避免堆砌式的防护手段集成，为不成熟不稳定的临时技术进行补丁式防护。

* + 1. **充电设备本体系统安全**

（1）本体系统安全防护

充电设备应具备的防盗能力如下，如果充电设备的门板被打开,充电设备应告警并禁止充电。：

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。
2. 如必要，用户与制造商协商后可在设备上在设置挂锁，与原有的锁构成两重保护。
3. 设备内部的通讯部件应有明显的无法去除的标记，以防被更换。
4. 充电设备检测到门板被打开，应主动告警并禁止充电。

操作系统应保证代码可控或采用必要安全加固措施，包括但不限于设定系统文件目录权限、建立进程访问保护机制、建立文件完整性保护机制、关闭不需要的端口和服务等。

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。

（可信计算）指标：充电设备本体二进制代码识别率≥90%；非本体二进制代码100%阻断运行；充电设备本体二进制代码被识别保护后理论上100%无法篡改，如被以特殊手段破坏可以100%执行自动恢复。

具有计量功能的充电设备，在计量计费时，应考虑具有电量校验功能。充电设备应对采集的电压、电流、电量等数据进行合理性校验，如果发现电量超范围、跳变等不在合理区间，则认为电表数据不可信，应进行告警。

专用型充电设备宜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。常见的备用方案如下：

1. 本地卡启动。
2. 本地VIN等车辆识别验证启动。
3. 本地蓝牙等物联启动方式；。
4. 其他可信离线启动方式。

（2）本体系统软件安全

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。（备注：结合平台侧相关要求）

应建立对充电设备业务应用的来源可信性验证和版本管理认证机制，只有经过认证的软件才能在本体系统上运行。验证级别分为A、B、C三级，A级验证来源厂商的信息；B级验证来源厂商信息和版本一致性；C级验证来源厂商、检测机构的信息和版本一致性；

方法一：充电设备业务应用来源可信性验证和版本管理认证机制建议采用国产商用密码算法SM2的签名验签机制。

方法二：采用软件固件本身携带信息完整性的校验码（如HMAC， CRC等校验码）的机制。具有多个处理器的充电设备，软件固件携带和本处理器匹配的唯一性信息标识码。

充电设备应具备软件容错机制，容错的一般方法包括：

1. 结构冗余。静态冗余常用的有：三模冗余TMR（Triple Moduler Redundancy）和多模冗余；动态冗余的主要方式是多重模块待机储备，当系统检测到某工作模块出现错误时，就用一个备用的模块来顶替它并重新运行；混合冗余兼有静态冗余和动态冗余的长处。
2. 信息冗余。为检测或纠正信息在运算或传输中的错误须外加一部分信息，这种现象称为信息冗余。
3. 时间冗余是指以重复执行指令（指令复执）或程序（程序复算）来消除瞬时错误带来的影响。
4. 其他冗余附加技术。
   * 1. **充电设备数据安全**

充电设备数据安全共分为以下三个内容：个人信息安全、数据有效性安全、数据传输及存储要求。

（1）个人信息安全

1. 对用户个人信息保护应满足GB/Z 28828-2012 《信息安全技术公共及商用服务信息系统个人信息保护指南》中第5章的要求。
2. 公用型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，建议采用屏蔽、替换、变换等方法进行脱敏处理。
3. 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。

（2）数据有效性安全

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。验证方法包括但不限于以下内容：

1. 非空数据验证；
2. 数据比较验证；
3. 数据类型验证；
4. 数据格式验证；
5. 数据范围验证；
6. 自定义验证。

（3）数据传输及存储要求

针对充电设备在数据的传输及存储方面提出以下要求：

1. 未经授权的任何实体（如公用型充电设备）应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，应采用屏蔽、变形、替换等技术对显示的用户敏感信息进行脱敏处理保护；
2. 不应未经授权，擅自修改和展示用户信息，用户信息包括但不限于用户姓名、账号、密码、手机号、充电记录的充电时间、充电电量、充电金额、账户余额。
3. 不允许除了管理员用户之外的其他用户改变非本人的口令；
4. 充电设备应保证存储和传输过程中数据的完整性，建议采用校验码技术或密码技术保证数据存储的完整性，完整性密码保护技术应采用国家密码管理局认可的密码技术，如采用SM3杂凑算法的消息鉴别码（MAC）生成技术、采用SM1对称算法或SM4对称算法的MAC生成技术等。
5. 充电设备应保证存储和传输过程中敏感数据的保密性，敏感数据包括但不限于用户姓名、账号、密码、手机号、余额等；建议采用SM1、SM4等国产商用密码算法进行数据加密。
   * 1. **充电设备访问控制安全**

（1）身份鉴别

充电设备在用户身份鉴别方面的安全要求如下：

1. 充电设备维护、升级、调试等过程中，如有登录需要，应使用身份认证管理技术，常见方法包括：用户名口令认证、短信认证、动态口令认证、数字证书认证等。
2. 具有账号管理功能的充电设备，其用户身份标识应具有不易被冒用的特点。可采用口令实现身份鉴别，口令长度应至少为8位，并至少采用数字、字母组合的方式。
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（建议登录失败次数不超过5次），当超出限制值时，采取特定的动作（如锁定账户10分钟或解锁才能登陆）。
4. 具有账号管理功能的充电设备，在用户身份鉴别信息丢失或失效时，可提供鉴别信息恢复机制。

（2）访问控制

1. 充电设备外部访问接口应采取安全预防措施。在应用系统中，访问控制的手段可包括用户识别代码、口令、登录控制、资源授权(例如用户配置文件、资源配置文件和控制列表)、授权核查、日志和审计。
2. 充电设备外部USB等物理访问接口不应直接暴露在设备体之外，应采用具有一定防冲压功能的外壳等安全措施进行保护。
3. 充电设备应具备控制无线接入的开关，可开启、关闭蜂窝网络、WLAN、蓝牙、红外、NFC等无线接入方式。当无线外围接口建立数据连接时，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。
4. 支持有线外围接口的充电设备，当有线外围接口建立数据连接时，充电设备应给用户相应的提示，仅当授权用户确认本次连接时，连接才可以建立。
5. 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。并基于用户的权能表，规定用户是否可对客体进行访问，充电设备访问权限权能表参见附表一。
6. 充电设备未经运营平台授权，不应从软件界面直接提供修改费率信息的功能。
7. 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。
8. 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。
9. 充电设备应尽量避免面向互联网开通高风险通用网络服务。
10. 确需远程维护的，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、可信通信通道确保远程接入安全。

（3）日志审计

充电设备应具备记录日志的能力，以实现设备行为的记录、留存和导出。要求充电设备审计日志的功能如下：

1. 未授权用户不得读取审计信息；
2. 审计数据应与用户身份关联，并覆盖到每个用户；
3. 审计日志中包括但不限于以下信息：事件发生的具体日期、时间、事件类型、用户身份、事件结果（成功/失败）。事件类型包括但不限于系统事件、业务事件、成功事件、失败事件以及对审计功能的操作；
4. 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. 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。
6. 充电设备应确保审计纪录保持一定的记录数和维持时间，审计日志留存时间应不少于6个月。

附表一

充电设备访问权限权能表

|  |  |  |  |
| --- | --- | --- | --- |
| 充电设备功能 | 充电用户权限 | 运营权限 | 维护权限 |
| 基本充电功能 | √ | √ | √ |
| 电池数据读取 | √ | √ | √ |
| 通信参数设置 | —— | √ | △ |
| 运营参数设置 | —— | √ | —— |
| 安全性能参数设置 | —— | —— | √ |
| 用户充电记录读取 | √ | √ | √ |
| 本机充电记录读取 | —— | √ | √ |
| 日志读取 | —— | √ | √ |
| 充电记录及日志删除 | —— | √ | √ |
| 充电记录及日志修改 | —— | —— | —— |
| 调试功能 | —— | —— | √ |

√ 有访问权限

—— 无访问权限

* 限制访问权限（是否可修改通信参数由设备拥有者确定）
  1. **智能终端APP应用软件**
     1. **测评目标**

（1）智能终端APP安全目标是要保证应用程序对敏感行为的可控性，确保应用程序无损害用户利益和危害网络安全的行为。

（2）测评智能终端APP是否符合国家相关法律、法规、标准和安全管理相关文件要求，为智能终端APP的安全规范提供技术和法律依据，主要包括：

——智能终端APP在使用过程中向用户展示的互联网信息必须合理合法，应付何国家和行业发布的互联网信息内容相关规定，不危害社会公共安全；

——智能终端APP的开发方应提供合法的身份信息，作为安全问题追溯的依据；

——检测智能终端APP不应存在超越其功能范围收集手机用户隐私数据、故意偷跑流量、恶意消耗手机资源等安全隐患；

* + 1. **运行机制要求**

（1）安装与卸载

电动汽车智能终端APP在安装和卸载过程中的安全要求如下：

a）支持预装在苹果iOS系统、微软Windows phone7系统、安卓Android 系统和塞班symbian系统等主流系统；

b）未经用户许可，不得安装；

c）检查应用程序的下载渠道是否正规合法，来自于官网下载或者是各个渠道；

d）下载和安装过程被意外中断情况下，系统程序应能够继续或重新进行下载和安装。

e）在安装和卸载过程中，不得捆绑下载其他应用软件；

f）不得安装本应用程序功能说明文档中未加说明的额外功能，不得安装用户未知和未允许的第三方应用；

g）应以用户可见的方式进行安装，应有安装界面，并能提示安装进度；

h）在安装过程中，应可以随时取消安装；

i）安装好后不得强制用户重启设备；

j）应提供卸载应用程序的方式，用户可以随时卸载应用程序；

k）卸载不应影响其他应用程序的功能、性能和信息安全性。

l）卸载应用程序必须卸载彻底，不能在系统中留下应用程序的临时文件和活动程序或模块。

（2）启动与退出

电动汽车智能终端APP在启动与退出的安全要求如下：

a）未经用户许可，不得预先设定自动启动；

b）开机自动运行功能可以设置开启和关闭；

c）应用程序运行时，不应故意破坏其他应用程序的正常运行；

d）除一些必须的应用（如即时消息类），应用程序不应常驻通知栏；

e）应用程序的运行不应强制用户下载其他应用，或在运行过程中未经用户许可在后台下载其他应用；

f）应用程序在发送联网请求时，应具备防止频繁联网的机制，如应用程序客户端在连续数次（3次）无法连接服务器后，不应继续频繁自动联网，造成终端资源消耗。应在较长时间（如10分钟）后再尝试连接服务器。

（3）升级检测

电动汽车智能终端APP在升级检测的安全要求如下：

a）应用程序如有更新版本，应提示用户更新，但不能未经用户允许自动更新；

b）应对升级包的完整性、合法性进行了校验，避免升级包被劫持；

c）2G/3G/4G wifi等网络环境下系统程序应该都能正常升级

d）如更新失败。不应反复联网更新；更新失败应能回到更新前的版本。

e）应有内存处理和保护机制，避免内存被修改和破坏；

f）在断电和内存不足的情况下，系统程序应能够继续进行相关升级，对于内存不足等情况系统程序应有友好的提示。

* + 1. **恶意行为防范要求**

恶意行为指未经用户许可或未明示用户的情况下，电动汽车智能终端APP所进行损害用户合法权益的行为。根据YD/T 2439-2012的规定，移动互联网恶意代码的恶意行为可以总结归纳为8类，即恶意扣费、隐私窃取、恶意传播、资费消耗、系统破坏、欺骗欺诈、流氓行为。

电动汽车智能终端APP不应具有本章规定的恶意行为。

（1）恶意扣费

在用户不知情或未授权的情况下，应用程序不应通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或支付费用，导致用户经济损失。

（2）信息窃取

在用户不知情或未授权的情况下，应用程序不应获取涉及用户个人信息、工作信息或其它非公开信息，包括短信、彩信、邮件、通讯录、通话记录、通话内容、地理位置、用户各类账号信息、用户各类密码信息、用户下载信息、用户文件内容等。

（3）远程控制

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。

（4）恶意传播

应用程序不应具有自动通过复制、传染、投递、下载等方式将自身、自身的衍生物或其它恶意程序进行扩散的行为。如自动发送包含恶意程序链接的短信、彩信、邮件信息；自动利用蓝牙通讯技术向其它设备发送恶意程序；自动利用无线网络技术向其它设备发送恶意程序；自动向存储卡等移动存储设备上复制恶意程序等。

（5）资费消耗

在用户不知情或未授权的情况下，应用程序不应通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等方式，导致用户资费损失。

（6）系统破坏

应用程序不应通过感染、劫持、篡改、删除、终止进程等手段导致电动汽车智能终端或其它非恶意软件部分或全部功能、用户文件等无法正常使用。不应干扰、破坏、阻断移动通信网络、网络服务或其它合法业务正常运行。

（7）诱骗欺诈

应用程序不应通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹等方式，诱导用户达到不正当目的（如退出、关闭、卸载、禁用或限制使用其它合法产品或退订服务）。

（8）流氓行为

a）应用程序不应在用户不知情或未授权情况下，长期驻留在系统内存中；

b）应用程序不应在用户不知情或未授权情况下，自动捆绑安装的；

c）应用程序不应在用户不知情或未授权情况下，自动添加、删除、修改收藏夹、快捷方式的；

d）在用户未授权的情况下，弹出广告窗口；

e）导致用户无法正常退出程序；

f）导致用户无法正常卸载、删除程序。

（9）侵犯用户隐私

对用户隐私保护要求应满足YD/T 3082-2016《移动智能终端上的个人信息保护技术要求》中第8章的要求。

（10）修改系统配置

在用户不知情或未授权的情况下，应用程序不应获取系统boot权限，未经允许修改系统配置。

（11）功能调用

a）在用户不知情或未授权的情况下，应用程序不应调用智能终端功能；

b）应用程序声明功能应予实际功能相符，不应申请本程序不需要的功能，如应用所申明的功能不需要获取用户通信录，但实际却读取了用户通信录信息；

c）应用程序应谨慎申请权限，不应过度申请终端权限。即申请了某些权限，但应用在整个代码中并未调用该权限；

d）应用程序在调用终端功能时，必须要给用户提示，只有经过用户许可才可以进行调用。

* + 1. **身份鉴别要求**

电动汽车智能终端APP在用户身份鉴别方面的安全要求如下：

a）应用程序应提供专用的登录控制模块对登录用户进行身份标识和鉴别，标识范围应该涵盖应用系统的所有使用者；

b）应用程序不应内置匿名账户，也不允许匿名用户的登录；

c）APP用户是否采取实名注册；

d）应用程序应具备用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识、身份鉴别信息不易被冒用；

e）应用程序应确保使用者在被授予敏感权限之前已经被鉴别；

f）应用程序应该对同一用户采用公司数字证书体系、硬件令牌、生物特征、一次性动态口令等两种或两种以上组合技术实现用户身份鉴别；

g）应用程序应该能识别非法鉴别请求，并可根据安全策略启动对失败标识和鉴别尝试进行锁定；

h）应用程序应该能够允许系统管理员用户随时更改失败次数和锁定时间；

i）应用程序对客户端用户每一次初始的会话连接请求，都应当要求其完成鉴别过程，对鉴别成功的每个会话都要维持其连接和中断的状态，在会话超时后，应使会话进入休眠状态或中断连接；

j）应用程序应该能够自动处理会话的异常状态，如连接超时、不完整连接等，并且应该提供给系统管理员适当的管理工具对会话进行实时控制，包括设置会话超时时间、最大允许会话数；

k）应用程序应该能够限制一个客户端只能有一个用户同时登录到系统中，一个用户只允许同时在一个客户端上登录到系统中。

l）应用程序应该可以让系统管理员用户去分发用户的初始口令，同时需要强制用户在初始登录时去改变管理员分发的口令；

m）应用程序应该不允许除了系统管理员用户之外的其它用户去改变非他们本人的口令；

n）应用程序在鉴别身份之前，应该能够检验用户口令是否过期，并强制性的要求口令过期的用户去更新口令；

o）应用程序在用户更新口令时应该能够检测用户的新口令是否已经被使用过，并阻止其选择使用过的最近几次的口令；

p）应用程序应该将系统的管理权限（包括用户管理、权限管理、配置定制）单独赋予系统管理员，这类用户仅负责进行系统级的管理，不具备任何业务操作的权限；

q）应用程序应该通过设置特殊的安全管理员，对系统中所有的安全功能进行管理或监视，例如具有操作审计、数据备份等权限，从而限制和监督系统管理员、业务员行使正常权限；

r）应用程序应该将业务操作权限赋予非管理员，这类用不能具备任何系统级的管理权限，并且其具有的权限转移和委托机制不能违背系统的授权原则。

* + 1. **业务权限要求**

电动汽车智能终端APP在业务权限方面的安全要求如下：

a）应用程序提供文件类用户数据的授权访问能力，当第三方应用访问被保护的用户数据时，应在用户确认的情况下才能访问。文件类用户数据包括图片、视频、音频和文档等；

b）禁止App内部组件被任意第三方程序调用；

c）应用程序应该具有访问控制功能，依据安全策略控制用户对资源的访问；

d）应用程序应该由授权主体配置访问控制策略，并严格限制默认用户的访问权限；

e）应用程序应该授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；

f）应用程序应该能够根据业务特性，设置权限互斥的原则，保证用户、权限合理对应关系，避免任何可能产生安全问题的权限分配方式或结果；

g）应用程序应该提供给系统管理员用户一个产生和修改用户授权的管理工具，并且保证在每次产生或修改权限后不需要重启系统就能立即生效；

h）若需要供外部调用的组件，应检查对调用者是否做了访问控制，如数字签名限制、Permission检查等；

i）避免程序中不规范使用导致的组件漏洞，如Activity安全、Broadcast Receiver安全、Service安全、Content Provider安全、Intent安全和WebView等；

j）检查自定义权限的保护级别，是否设置为signature或者signatureOrSystem。

* + 1. **网络通讯要求**

电动汽车智能终端APP在网络通讯方面的安全要求如下：

a）不应有未向用户明示且未经用户同意，擅自调用网络通讯功能，造成用户流量消耗的行为，包括在用户无确认情况下通过移动通信网络数据连接、WLAN网络连接、无线外围接口传送数据的行为；

b）不应有未向用户明示且未经用户同意，擅自调用网络通讯功能，造成用户费用损失的行为，包括在用户无确认情况下开启移动通信网络连接并收发数据的行为；

c）不应有未向用户明示且未经用户同意，擅自调用网络通讯功能，造成用户数据泄露的行为，包括在用户无确认情况下读取并传送用户电话本数据、通话记录、短信数据、彩信数据、通话录音、本地录音、图片、视频、音频和定位信息的行为；

d）应用程序中的互联网信息必须合理合法，不危害社会公共安全。

* + 1. **审计日志**

电动汽车智能终端APP在审计日志方面的安全要求如下：

a）未授权用户不得读取审计信息；

b）应覆盖到每个用户，审计数据应于用户身份关联；

c）应对重要安全事件进行审计，审计事件的类型至少应包括系统事件、业务事件、成功事件、失败事件以及对审计功能的操作；

d）审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

e）应该能够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；

f）应该保证无法删除、修改或覆盖审计记录；

g）审计记录应以易于理解的方式呈现；

h）审计日志留存事件应不少于6个月。

* + 1. **数据传输及存储要求**

电动汽车智能终端APP在数据传输及存储方面的安全要求如下：

a）未经授权的任何实体应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；

b）不应有未向用户明示且未经用户同意，擅自修改用户数据的行为，包括在用户无确认情况下删除或修改用户电话本数据、通话记录、短信数据和彩信数据的行为；

c）不应有未向用户明示且未经用户同意，擅自收集用户数据的行为，包括在用户无确认情况下开启通话录音、本地录音、拍照/摄像和定位行为；

d）不应存在数据传输过程中的非法调用和窃取漏洞，数据传输过程如数据输入、数据输出、数据传输、远程数据通信、本地数据通讯等；

e）不应存在数据存储和处理过程中的非法调用和窃取漏洞，数据存储和处理过程如数据存储、数据访问控制、敏感数据加密、内存数据安全等；

f）在证书验证、会话安全、调试信息、敏感信息显示等过程不应存在非法调用和窃取漏洞；

g）不应在本地明文保存用户密码；

h）不允许除了系统管理员用户之外的其他用户改变非本人的口令；

i）敏感的隐私信息应加密存储，如聊天记录、关系链、银行账号等；

j）系统文件、配置文件不应明文保存在外部设备上；

k）部分需要存储到外部设备的信息，每次使用前应判断信息是否被篡改

* + 1. **运行时解释要求**

电动汽车智能终端APP在运行时解释方面的安全要求如下：

a）对于嵌有解释器的软件，不应存在XSS跨站、SQL注入等高风险漏洞；

b）使用WebView的APP，不应存在URL欺骗等高风险漏洞。

* + 1. **代码安全**

电动汽车智能终端APP在代码方面的安全要求如下：

a）应用软件代码应防止被反编译和破解，如防止代码混淆、Dex保护、SO保护、资源文件保护以及第三方加载库的代码的安全等；

b）检查源代码中是否包含明文字符串、标准输出日志是否关闭等。

* + 1. **备份和恢复**

电动汽车智能终端APP在备份和恢复方面的安全要求如下：

a）应用程序应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；

b）应用程序应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；

c）应用程序在主界面或业务流程中任何环节非正常退出运行，智能终端APP再次启动，功能应正常使用；

d）智能终端设备其它应用程序出现异常情况导致关机或者重启，智能终端APP再次启动，功能应正常使用。

* 1. **充电服务凭证和认证要求**
     1. **充电服务凭证的分类**

在电动汽车和充电服务网络中，充电服务凭证是指充电服务发生或完成情况的信息证明，包括充电服务提供者、充电服务使用者标记和服务事物性标记，是获得充电服务认证的基础依据。充电服务凭证用于分为三种类型：充电服务凭证产生的位置如图5-1所示：

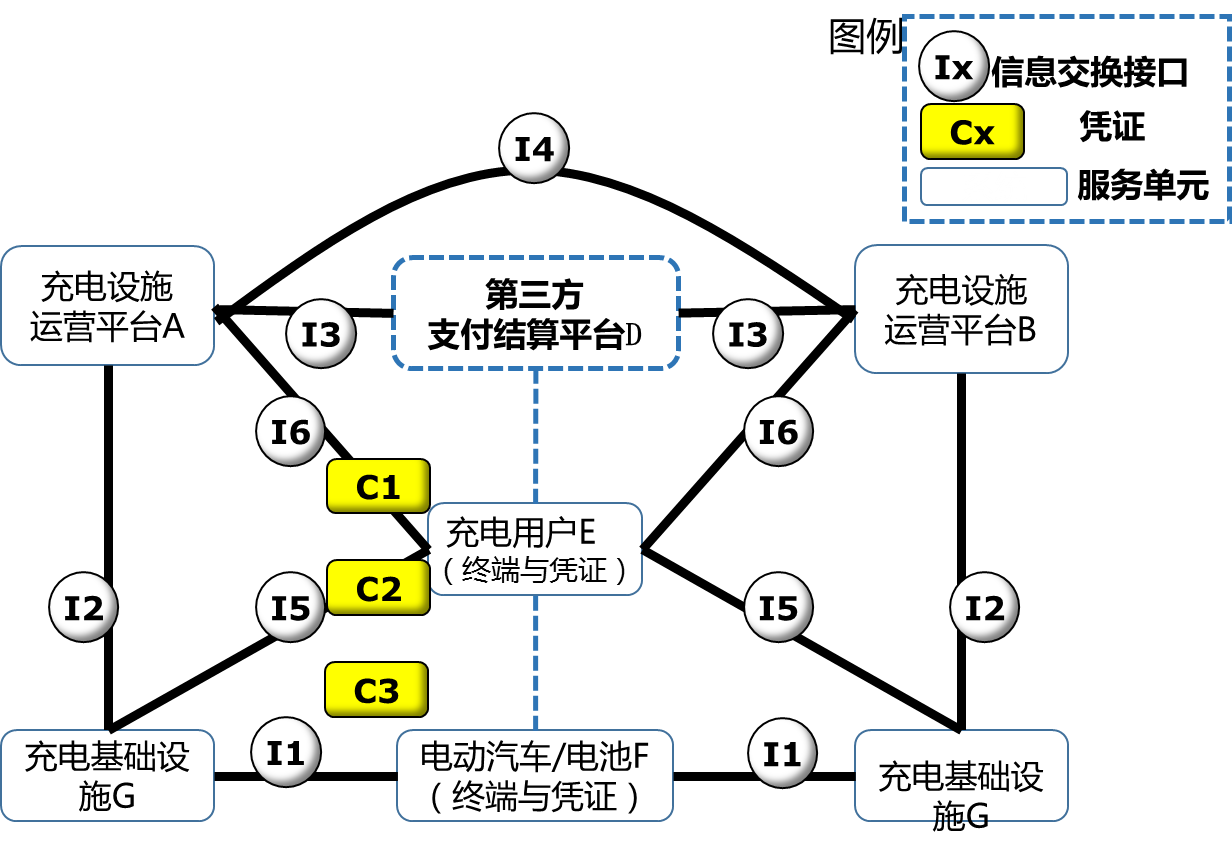


图5-1 充电服务凭证产生位置示意图

C1类型: 电动汽车用户通过智能 APP扫描设备二维码产生的充电服务凭证。

C2类型: 电动汽车用户通过RFID智能芯片卡，由通过设备持卡或智能终端刷卡后产生的充电服务凭证。

C3类型: 通过插枪后车辆与设备的交互，由车辆电动汽车智能终端产生的 充电服务凭证，此类型凭证基于参考ISO/IEC 15118-1参考规范.。

* + 1. **认证过程的接口安全要求**

充电服务的认证过程是识别电动汽车服务身份，获得服务授权的重要过程。充电服务的认证过程的安全防护主要在于接口安全要求。

（1）C1类型安全防护

（a）设备上所附属的二维码宜考虑适当的加密机制，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。

（b）二维码中涉及关键、敏感数据需要进行安全保护。

（c）通过App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。

（d）传输数据安全，App智能终端与后台进行的认证服务过程，应采用Https传输方式。二维码涉及各系统之间进行信息传输，各系统之间应建立安全通信信道，应对交易数据采用数字签名和加密等安全方式进行传输，确保数据不对监听和篡改。

（e） 传输数据的保密性，应对传输的数据进行保密性保护，不应引起信息泄露。

（f） 传输数据的完整性，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的校验。

（2）C2类型安全防护

（a）应用管理数据在卡片的个人化期间建立，以定义初始的安全域。

（b）以完整性和认证为目的的安全报文的MAC生成的第一步包括从IC卡的唯一的16字节安全报文认证（MAC）子密钥和2字节ATC分散得到一个唯一的16字节安全报文鉴别（MAC）过程密钥。

（C）安全报文机制要求发卡机构管理唯一的IC卡安全报文认证（MAC）和安全报文加密主密钥。各类密钥具体功能如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 密钥名称 | 用途 | 密钥形式 | 存在条件 | 说明 |
| 应用密文密钥 | 用于交易中产生应用密文和发卡机构认证 | 对称密钥 | 必须存在 | 由发卡机构应用密文主密钥，按规定的分散方法获得，在交易过程中，按规定定义的方法派生过程密钥，用于应用密文产生和发卡机构认证 |
| 安全报文认证（MAC）密钥 | 用于安全报文中计算MAC | 对称密钥 | 必须存在 | 由发卡机构安全报文认证主密钥，按规定定义的分散方法获得，在交易过程中，按规定定义的的方法派生过程密钥，用于MAC计算和验证 |
| 安全报文加密密钥 | 用于脚本中数据的加密 | 对称密钥 | 必须存在 | 由发卡机构安全报文加密主密钥，按规定定义的分散方法获得，在交易过程中，按规定定义的方法派生过程密钥，用于报文加密 |
| 卡片公私钥对 | 用于脱机数据认证 | 非对称密钥 | 卡片支持DDA或CDA | 由发卡机构私钥对卡片公钥及相关信息签名产生IC卡公钥证书 |
| 应用开通密钥 | 用于开通扩展应用时指定文件记录的增加 | 对称密钥 | 卡片支持相关的扩展应用信息的记录 | 由发卡机构应用开通主密钥，按规定定义的分散方法获得，在开通应用的过程中，按规定定义的方法派生过程密钥，用于报文加密 |
| 扩展应用管理密钥 | 用于在读取或更新扩展应用中指定记录时进行保护 | 对称密钥 | 卡片支持相关的扩展应用信息的记录且指定的应用已经开通 | 由发卡机构扩展应用管理主密钥，按规定定义的分散方法获得，在交易的过程中，按规定定义的方法派生过程密钥，用于报文加密 |

（3）C3类型安全防护

（a）参考ISO15118安全？。

* + 1. **认证过程的系统安全要求**

（a）应用软件与后台系统应具备合法性检查，通过签名验签等密码技术与后台系统进行双向认证，确保后台系统和应用软件的合法性，并设置超时时间。

（b）后台需要对于设备、用户身份、用户信用等级等关联信息进行全面验证。

* 1. **安全通信技术要求**
     1. **桩到平台之间的通讯协议**

电动汽车充电站后台监控系统和充电机采用 TCP／IP 作为消息传输层协议 时，应使用TLS 协议实现数字证书认证、加密算法协商、密钥交换、消息鉴别码等安全功能，保证数据传输的安全性。

（1）TLS 协议

TLS 协议在整个网络协议栈中的位置如下图所示：

|  |
| --- |
| 应用层数据 |
| TLS协议 |
| 传输层（TCP） |
| 网络层（IP） |
| 数据链路层 |

TLS/SSL 协议应用于应用层协议和传输层协议（TCP）之间。TLS 协议为上层的应用层协议提供类似于 TCP 协议的数据流传输协议，同时通过 TCP 协议来传输加密后的应用层数据。对于上层的应用程序来说，TLS 协议取代了 TCP 协议，同时增加了加密认证等功能；对于下层的 TCP 协议来说，TLS 协议就相当于应用层协议。

TLS/SSL 为其承载的应用层数据提供传输层加密和校验机制。

TLS 协议是一种应用于传输层的安全协议，用于构建客户端和服务端之间的安全通道。TLS 协议本身基于 TCP 传输层协议，通过实现证书认证、密钥协商、 数据加解密等功能，对上层应用程序提供类似于 TCP 的流传输协议。

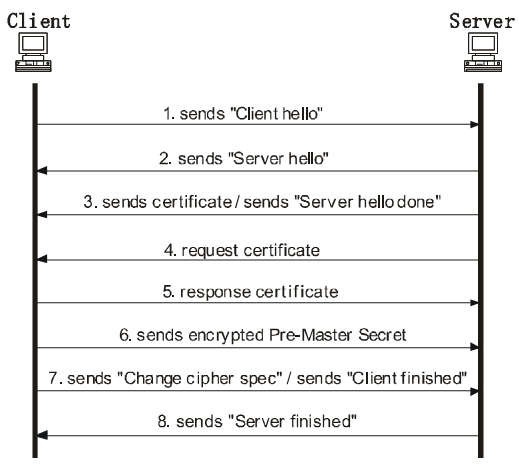
TLS 协议本身是分层结构，分为两层：下层的记录层协议提供对 TCP 数据流 的分段、压缩与解压、加密与解密、完整性校验等；上层协议包括握手协议（用 于身份鉴别和安全参数协商），密码规格变更协议（用于通知安全参数的变更）， 报警协议（用于关闭连接的通知和对错误进行报警）这三种协议。下面是 TLS 协 议的分层结构图。更详细的 TLS 协议内容请参见 RFC2246。

TLS协议栈

|  |  |
| --- | --- |
| 应用层数据 | 握手协议、密码规格变更协议、 告警协议 |
| 记录层协议 | |
| 传输层（TCP） | |
| 网络层（IP） | |
| 数据链路层 | |

标准TCP/IP协议栈

（2）安全连接建立流程



在 TCP 握手成功后，客户端发送客户端 hello 消息给服务端，服务端应回应服务端hello 消息，否则产生一个致命错误并且断开连接。客户端hello和服务端hello用于在客户端和服务端进行基于RSA或SM2的密码算法协商，以及确定安全传输能力，包括协议版本，会话标识，密码套件等属性，并且产生和交换随机数。

在客户端 hello 和服务端 hello 消息之后是身份验证和密钥交换过程。包括服务端证书、服务端密钥交换，客户端证书、客户端密钥交换。

在服务端发送完 hello 消息之后，接着发送自己的证书消息，服务端密钥交 换消息（可选）。如果服务端需要验证客户端的身份，则向客户端发送证书请求 消息。然后发送服务端hello完成消息，表示hello消息阶段已经结束，服务端等 待客户端的返回消息。如果服务端发送了一个证书请求消息，客户端必须返回一 个证书消息。然后客户端发送密钥交换消息，消息内容取决于客户端hello消息 和服务端hello消息协商出的密钥交换算法。如果客户端发送了证书消息，那么 也应发送一个带数字签名的证书验证消息供服务端验证客户端的身份。

接着客户端发送密码规格变更消息，然后客户端立即使用刚协商的算法和密 钥，加密并发送握手结束消息。服务端则回应密码规格变更消息，使用刚协商的 算法和密钥，加密并发送握手结束消息。至此安全连接建立过程结束，服务端和 客户端可以开始数据安全传输。

（3）使用要求

a）严禁使用不加密的套件

不应使用任何协商加密为NULL 的密码套件，不应使用已知为不安全的密码套件，推荐使用国产 SM4 算法进行加密。

禁用的密码套件列表如下，但不限于此： TLS\_NULL\_WITH\_NULL\_NULL； TLS\_RSA\_WITH\_NULL\_NULL-MD5；

TLS-RSA\_NULL\_WITH\_NULL SHA

b）版本协商

应使用 TLS1.0 以上版本协议进行连接。

c）密钥再协商密钥再协商周期应为可配置值，宜配置为 15min。

d）消息鉴别码

应使用消息鉴别码，推荐使用国产 SM3 算法。

注：TLS 使用消息鉴别码的能为可选项。本标准要求使用消息鉴别码，以应 对和检测中间人攻击。

（4）证书要求

a）应支持一个以上的证书颁发机构（CA）。

b）证书的应采用双向交换确认，通信中任一方未提供证书则应终止连接。

c）连接建立成功后证书到期不应中断连接，连接建立时过期证书视为无效证书。

d）当采用RSA算法时，密钥长度至少为2048位，不应使用已知为不安全的密钥长度。

e）应支持通过证书进行密钥交换和签名，宜采用国产SM2证书。

（5）证书管理

电动汽车充电站行业主管单位负责证书中心的建设和管理。

电动汽车充电站运营企业向行业主管单位提交证书申请，主管单位审核通过后制作数字证书，由运营企业完成数字证书的导入。

* + 1. **桩到车充电协议**

（1）介绍

电动汽车直流快速充电过程中伴随有高电压、大电流的能量传输，且电能量的输出与停止与充电通信协议密切相关，因此电动汽车充电过程中信息安全至关重要。电动汽车直流快速充电通信协议是基于控制器局域网（CAN总线）的通信协议。CAN总线本身具有通信实时性强、传输距离较远、抗电磁干扰能力强、成本低等特点，且具有优先权和仲裁功能、可靠的错误处理和检错机制，但CAN通信协议并不支持节点的安全认证和信息加密功能，节点的自由接入和数据明文传输使得CAN总线通信暴露在安全攻击下。本文提出一种针对电动汽车充电通信协议的信息安全机制，保证电动汽车充电过程中的通信信息安全。

（2）CAN通信安全脆弱性

CAN总线自身的特点使其具有安全脆弱性而极容易遭受安全威胁，

a）CAN数据帧没有安全认证域；

b）CAN数据帧数据域最多只能容纳8个字节，使得很难实现强安全机制；

c）CAN节点的处理器不具备强大的加解密处理能力；

d）没有对发送帧和接收帧进行身份验证。

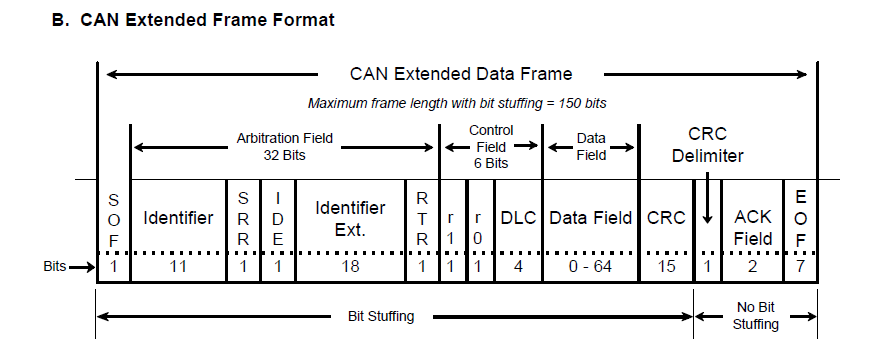
信息安全重在保护通信信息的机密性、完整性和可用性，考虑到CAN总线自身的特点以及与充电应用协议的兼容性，在不给总线节点增加过多处理负担和增加额外加密固件的前提下，本方案对GB/T 27930充电应用协议做出扩展，实现对CAN总线明文的加密和签名，保证CAN通信信息的私密性和完整性。

（3）CAN通信安全传输协议

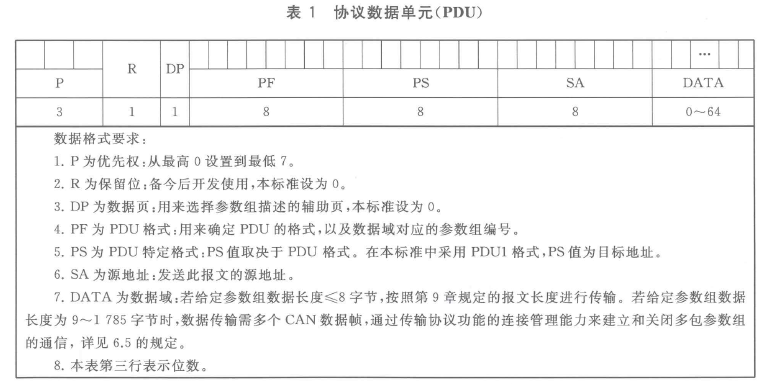
a）安全传输协议帧格式

为了与CB/T 2730定义的物理称和数据链路层保持一致，本方案定义的CAN通信安全传输协议仍采用CAN2.0B定义的帧格式。

GB/T 27930电动汽车直流充电协议采用的是CAN2.0B扩展帧格式，帧格式定义如下：



该协议继承了CAN2.0B和SAEJ1939:21对帧起始、仲裁域、控制域和CRC校验位的定义，其中帧起始，仲裁域SRR、IDE、RTR位定义，控制域位定义与CAN2.0B和SAEJ1939:21保持一致，CRC由CAN控制器计算。因此，与应用相关的只有仲裁域（29位ID）和数据域两部分，即GB/T 27930-2015 第6.2节规定的协议数据单元PDU格式：



b）安全传输协议加密机制

根据加密密钥和解密密钥的关系，密码安全机制分为对称加密机制和非对称加密机制。对称加密机制的加密密钥和解密密钥相同，或实质上相同，即从一个易于推导出另一个。非对称加密机制又称为公钥密码机制，其加密密钥和解密密钥不同，从一个很难推出另一个，其中，一个可以公开的密钥是公钥，另一个必须保密的密钥成为私钥。本方案为CAN通信安全传输协议设计了对称加密机制和非对称加密机制2种加密机制，供选择使用。

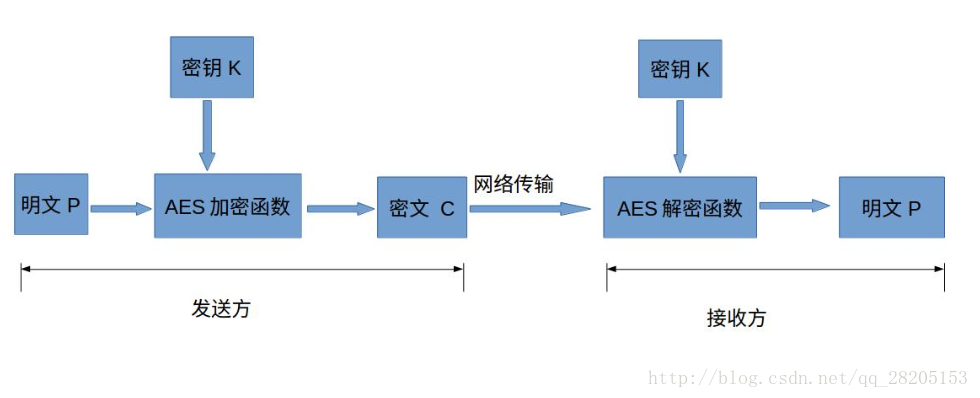
（4）对称加密机制

a）AES安全加密算法

对称加密机制的优点是算法简单、计算量小、加密速度快、加密效率高，适合加密大量数据，明文长度与密文长度相等。对称加密机制采用的密码算法常分为分组密码算法和流密码算法，本方案采用分组密码算法。分组密码算法将明文消息编码后的数字序列划分成长度为N的组，每组分别在密钥的控制下变换成等长的密文数字序列。典型的分组密码算法有DES、3DES、AES、IDEA、RC5、MARS等。

其中AES算法自美国国家标准技术研究所（NIST）于2001年11月26日发布以来，AES已经成为对称密钥加密算法中最流行的算法之一。因为AES的基本要求是比三重DES快而且至少和三重DES一样安全，综合考虑的算法的安全性和执行的效率，本方案选择AES算法做为CAN通信安全传输协议的加密算法。

发送方将明文经过密钥采用AES加密函数进行加密后，将密文传送至接收方，接收方使用相同的密钥经过解密函数计算后得出明文（AES加密算法可参见《高级加密标准（AES）算法》）。



通过该图可以看出，安全协议的实现需要的两个关键要素：算法和密钥。现代密码学的一个显著的特点是算法的安全是基于密钥的安全，因为算法的细节是可以公开的，所以只有保证密钥的安全才能保证实际通信或加密数据的安全，如果密钥采用明文在网络中分发，或恶意第三方在获悉通信双方协商密钥过程后能很容易地计算得到密钥，那么即使采用安全强度很高的密码算法也不能保障数据传输的机密性。问题是如何才能在不安全的环境中为用户分发密钥信息，使得密钥能够安全、正确并有效地使用呢？这就需要密码协议，在现代密码学中，除了算法研究外，密码协议研究是密码学的另外一个重要方向。

b）密钥交换协议

密码协议，是使用密码学完成某项特定的任务并满足安全需求的协议，其目的是在网络环境中提供各种安全服务，在实体之间安全地分配密钥或其他各种秘密，确认发送和接收的消息具有抗抵赖性。在本方案中使用的密码协议是一种密钥协商协议，是通信系统中的成员在公开的信道上建立秘密密钥的过程，在密钥协商协议中，通信各方预先都不知道密钥是什么，而是在协商的过程中通过各方交互信息得到。密钥协商协议又称为密钥协定协议，其中两个成员之间的密钥写上协议也称为密钥交换协议。

迪菲－赫尔曼（Diffie–Hellmankey exchange，简称“D–H”）密钥交换协议是一种经典的密钥交换协议。它可以让双方在完全没有对方任何预先信息的条件下通过不安全信道建立起一个密钥。这个密钥可以在后续的通讯中作为对称密钥来加密通讯内容。

该协议利用了有限域中计算离散对数的困难性问题，通过使用两个全局公开的参数-一个素数P和一个整数g，其中g是p的一个原根

Diffie-Hellman密钥交换协议

|  |  |  |
| --- | --- | --- |
| **步骤** | **用户A** | **用户B** |
| 步骤一 | 从[0，1，……，p-1]中随机选取r | 从[0，1，……，p-1]中随机选取s |
| 计算g1=gr (mod p) | 计算g2=gs(mod p) |
| 将g1发送给用户B | 将g2发送给用户B |
| 步骤二 | 计算会话密钥  K=g2r(mod p)=(gs)r(mod p) | 计算会话密钥  K=g1s(mod p)=(gr)s(mod p) |

为了安全起见，必须使用非常大的r, s以及p，否则暴力破解密钥将成为可能。如果 p 是一个至少 300 位的质数，并且XA和XB至少有100位长，那么即使使用全人类所有的计算资源和当今最好的算法也不可能从g, p和g(r\*s) mod p 中计算出 r\*s。

（5）非对称加密机制

对称密码机制虽然有算法简单、计算量小、加密快的有点，它也存在诸如密钥分配、密钥管理和没有签名功能等局限性。那么能不能在不直接传递密钥的情况下，完成解密呢？非对称加密机制就解决了这样的难题。

非对称密码机制也叫公钥密码机制，与对称加密机制不同，非对称加密体制的加密密钥和解密密钥不同，加密和解密使用存在某种对应关系不同的规则，这样就可以避免直接传递密钥。非对称机制的加密算法和加密密钥可以公开，其中加密密钥成为但由加密密钥推导出相应的解密密钥在计算上却是不可行的，因此只要每个通信方保管好自己的解密密钥，通信就是安全的。迄今为止，人们已经设计除了许多非对称加密机制，其中RSA算法是目前应用最广泛的非对称加密算法之一，RSA算法的过程可以简要描述如下：

a）生成公私钥对。A方首先选取两个大素数p和q，计算其乘积n=p\*q以及欧拉函数φ(n)=(p-1)(q-1)；然后随机选取加密密钥e，1<e<φ(n)，满足e和φ(n)互质。接着使用欧几里得扩展算法计算解密密钥d，以满足ed≡1modφ(n)，其中，e和n是公钥（可以让所有人知道），d是私钥（只有自己知道）。

b）RSA加密。B要向A发送消息M，须对先对明文M按位分组，每组的位长度为k，满足2k≤n，使用mi来表示分组后的消息，利用从A处获得到公钥(e，n)计算密文ci，加密算法为：ci=Ee(mi)=mie(modn)，B方将每个分组消息依次加密后的密文ci组合得到密文C输出。

c）RSA解密。A方接收到密文C后先进行分组，等到分组后的密文ci，利用自己的私钥（d，n）进行解密，解密算法如下：mi=Dd(c)=cid(mod)n。A将按组解密后的明文mi组合得到明文M。

RSA算法的安全性很大程度上取决于“密钥长度”（一般只是指模值的位长度），目前主流密钥长度至少都是1024bits以上，低于1024bit的密钥已经不建议使用（安全问题）。加密后的分组密文位长跟密钥的位长度是相同的，若密钥长度位为1024bits，那么密文最短长度将达到128字节。本方案规定，对于加密后数据域长度超过8个字节的密文，采用SAEJ1939定义的报文传输协议，传送加密后的密文。

（6）安全传输协议消息鉴别

电动汽车与充电桩之间通信采用CAN总线协议，总线上可接入多个节点，且多个节点均可向总线发送报文，那么如何区分总线上的报文是期望接收的报文呢？这就需要对消息鉴别以确定消息来源。

在网络通信中，存在一些针对消息内容的攻击方法，如伪造信息、篡改消息内容、改变消息顺序、消息重放或者延迟等。为了防止上述攻击，可采用消息鉴别技术，消息鉴别主要是确保消息的完整性、真实性和不可否认性。

本方案规定，消息鉴别码为GB/T 27930标准规定的应用层PDU的签名值，PDU包括报文的ID和数据域两个部分，将签名值使用密钥加密后填充在密文传输帧的数据域中。接收方接收密文后进行解密，将解出来的明文按照相同的签名算法计算，如果得出的值与明文签名部分的签名值相同，则可认为是正确的发送方发来的消息（因为只有正确的发送方和接收方知道密钥和明文，所以任何伪造的第三方不可能生成正确的签名值）。

（7）安全传输协议实现

本方案对GB/T 27930规定的PGN参数组进行扩展，定义密钥约定PGN和密文传输PGN以实现密钥的交换和密文的传输。

a）对称加密机制下的传输协议实现

素数和原根约定。充电机上电后使用请求PGN（00EA00），请求BMS是否支持素数约定PGN（002000），若BMS回复否定确认NACK，则表明BMS不支持通信安全传输协议。否则BMS使用素数随机生成器生成一个大素数p(为了保证密钥的长度，素数值的二进制表示应至少是128bits)。充电机使用素数约定PGN（002000）将大素数p发送给BMS（大素数长度超过8个字节，素数约定报文应使用传输协议进行传送）；BMS接收分组报文后对报文进行重组获得大素数P，使用原根约定PGN（002100）将素数P的一个原根g发送个充电机，则双方对全局参数p和g约定成功。

公钥交换。充电机收到原根g后，从{0，1，……，p-1}中随机选取一个r（私密，只有自己知道），计算充电机的公钥g1=gr (mod p)，使用公钥发送PGN（002200），将g1发送给BMS；BMS收到g1后，从{0，1，……，p-1}中随机选取一个s（私密，只有自己知道），计算BMS的公钥g2=gs (mod p)，使用公钥发送PGN（002200），将g2发送给充电机。

明文加密。充电机和BMS交换公钥后，分别使用自己的私钥计算密钥K= g2r(mod p)= g1s(mod p)= (gs)r(mod p)。充电机和BMS获得对称密钥后，采用AES128对称加密算法对后续满足GB/T 27930规定充电应用过程的明文以及明文PDU产生的MD5哈希值进行加密。

密文传输。充电机和BMS分别使用密文传输PGN（003000）将加密后的密文填充在数据域中进行传送，密文传送报文ID的PS、SA定义与GB/T 27930保持一致。

密文解密。充电机和BMS接收到报文后，根据参数组编号判断是否为密文传输协议，然后根据密钥解析报文的数据域，获得PDU明文值和明文签名值，并根据重新计算明文PDU的签名值。若计算签名值与接收报文中签名值一致则使用明文信息，否则丢弃该明文信息。明文信息的使用与GB/T 27930对充电流程、参数组定义和参数定义保持一致。



图对称加密机制

（8）非对称加密机制下的传输协议实现

公钥n交换。充电机上电后使用请求PGN（00EA00），请求BMS是否支持公钥n交换PGN（002000），若BMS回复否定确认NACK，则表明BMS不支持通信安全传输协议。否则充电机使用素数随机生成器寻找2个长度为512bits附近的素数p1和q1，保证p1\*q1的乘积值n1的长度达到1024bits(为了保证密钥的长度，模数长应至少是1024bits)，充电机使用公钥n发送PGN（002000）将公钥n1发送给BMS；BMS接收到充电机的公钥n1后，使用素数随机生成器寻找2个长度为512bits附近的素数p2和q2，保证p2\*q2的乘积值n2的长度达到1024bits(为了保证密钥的长度，模数长应至少是1024bits)，BMS使用公钥n发送PGN（002000）将公钥n2发送给充电机。自此公钥n交换完成。

公钥e交换。充电机收到BMS公钥n2后，随机选取加密密钥e1，1<e1<φ(n1)=(p1-1)(q1-1)，且e1与φ(n1)互质，计算解密密钥d1，满足e1d1≡1modφ(n1)。充电机使用公钥e交换PGN（002100）将公钥e1发送给BMS；BMS接收到充电机公钥e1后，随机选取加密密钥e2，1<e2<φ(n2)=(p2-1)(q2-1)，且e2与φ(n2)互质，计算解密密钥d2，满足e2d2≡1modφ(n2)，BMS使用公钥e交换PGN（002100）将公钥e2发送给充电机。自此公钥e交换完成。

明文加密。充电机和BMS获得对方的公钥后，充电机使用BMS的公钥(e2，n2)、BMS使用充电机的公钥(e1，n1)，对后续满足GB/T 27930规定的充电应用过程明文以及明文PDU产生的MD5哈希值进行加密，加密前先对消息进行分组，分组值的bit长度k取满足k≤log2n的最大值。充电机每一个分组明文mi的密文c1=mie2 mod n2；BMS每一个分组明文mi的密文c2=mie1 mod n1；

密文传输。充电机和BMS分别使用密文传输PGN（003000）将加密后的密文填充在数据域中进行传送，密文传送报文ID的PS、SA定义与GB/T 27930保持一致。

密文解密。充电机和BMS接收到报文后，根据参数组编号判断是否为密文传输协议，然后根据各自的私钥解析报文的数据域，充电机解密过程为mi=c2d1modn1；BMS的解密过程为mi=c1d2modn2，获得PDU明文值和明文签名值，并根据PDU名文职重新计算明文PDU的签名值。若计算签名值与接收报文中签名值一致则使用明文信息，否则丢弃该明文信息。明文信息的使用与GB/T 27930对充电流程、参数组定义和参数定义保持一致。

（9）AES加密机制和RSA加密机制的对比

安全性：AES和RSA都很安全，至少在目前的计算机体系结构下，没有任何有效的攻击方式。量子计算机时代，RSA有一定的破绽，量子计算机穷举计算质因子速度可以提高N个数量级，能够在有限的时间内破解RSA密钥。AES256至少目前并没有什么明显的漏洞。但是AES作为对称加密技术，如何安全的分发密钥是一个难题。通过任何方式传递密钥都有泄密的风险；RSA作为非对称加密技术的代表，其非对称的特点，满足公钥可以随处分发，只有私钥能解密公钥加密的数据，可以用于密钥分发（D-H密钥交换协议的对称加密密钥的交换也可以使用RSA算法来替换）。

效率：AES作为对称加密技术，加密速度很快；RSA加解密的速度其实相当慢，只能对小块的数据进行加解密。RSA算法的速度总是比AES慢。因为RSA的计算量远大于AES，在加密密和解密时需要做大量的模数乘法运算，耗用资源大，并且会导致密文变长。同样的硬件实现，AES比RES快大约1000倍，因此在实际使用中，RSA算法很少用于加密大块的数据。

考虑到安全的同时要兼顾效率，因此本方案建议采用AES加密算法和DH密钥交换协议。

（10）总结

本方案提出的CAN通信安全传输协议实现，能够有效的解决CAN总线任意两个节点间的信息安全性传输问题，但CAN总线并没有限制第三个节点的接入，如果总线上有伪造的第三个节点存在，该节点在信道的中央进行两次D-H密钥交换，一次和充电机另一次和BMS，就能够成功的向充电机假装自己是BMS，反之亦然。而攻击者可以解密（读取和存储）充电机或BMS的信息并重新加密信息，然后传递给另一端。由于没有公钥基础设施，总线节点间不能进行身份认证，也就无法防范此类攻击，因此本方案中提出的方法，仅用于解决双节点CAN总线的通信信息安全传输问题。

* + 1. **支付方式与桩之间的通讯协议**

（1） 支付方式分类

在充电服务网络中，充电服务 分为两种：线上支付和线下支付。

（a） 线上支付

参与电动汽车充换电设施运营及服务的线上支付，即远程支付。电动汽车用户通过在网银或者app手机客户端支付。该支付方式，通过平台与设备建立信息交换，主要的通讯协议涉及桩设备到平台以及平台与支付平台之间 。

（b）线下支付

参与电动汽车充换电设施运营及服务的线下支付，即近场支付。电动汽车用户通过在刷卡或者现场连接，完成支付。该支付方式，通过现场通信技术与设备建立信息交换，主要的通讯协议涉及卡、App和车载终端到设备以及设备到平台，平台到支付平台之间。

（2） 线上支付与与桩设备之间的通讯协议的安全要求

a) 支付过程涉及各系统之间进行信息传输，各系统之间应建立安全通信信道，应对交易数据采用数字签名和加密等安全方式进行传输，确保数据不对监听和篡改。

b) 公网环境下，支付信息不应以明文形式传输。

c) 应对传输的数据进行保密性保护，不应引起信息泄露。

d) 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的校验。

（3） 线下支付与桩设备之间的通讯协议的安全要求

a) 通用数据：包括时间、终端识别号、终端交易记录等。外界可以对这些数据进行访问，但不允许进行无授权修改；

b) 敏感数据：包括认证中心公钥、用于PIN加密的对称密钥及终端内部的参数。在未授权的情况下，外界不允许对这类数据进行访问和修改。

* + 1. **平台之间的通讯协议**

1. 平台间数据传输一般流程

平台间的信息交换应符合GB/T 9387.1中关于会话连接的要求，一般需要经过平台认证、数据请求和数据返回3个步骤。



图1充换电服务信息平台间的交换流程

1. 平台间数据信息安全保护基本要求概述

参与电动汽车充换电设施运营及服务的各角色和实体之间应在正常、安全、有效的原则下通过规范的接口进行信息交换，相互协同地向电动汽车用户及监管部门提供数据服务。

平台所属方须提供严格的系统安全保密机制，保障信息交换接口安全、稳定、可靠地运行，保障传输和接收数据的安全和完整。基本要求：

1）采用身份认证、访问控制、数据加密、数字签名等安全措施；

2）采用安全可靠并且普遍使用的加密算法；

3）密钥的存贮和交易信息的加密／解密需要在安全的环境中；

4）遵循数据安全保密的国家和行业标准；

5）定期更换密钥；

1. 具备对报文做来源正确性鉴别的机制（HMAC）。
2. 安全通讯的技术要求

平台运营商必须满足数据安全传输控制方面的要求，提供严格的系统安全保密机制，保障信息交换接口安全、稳定、可靠地运行。

A．接口安全的技术要求

a平台认证

应采用用户名/口令认证、密钥认证或数字证书认证等方式进行。

· 基于平台标识和平台密钥进行平台身份认证

· 平台身份认证成功后数据接口提供方向数据接口调用方授予Token，并将其作为全局唯一凭证，每次调用各接口时均需验证Token的有效性，Token的有效期由服务端确定，最长不应超过7天。

· 使用SSL数字证书认证时，宜采用组织验证型(OV)及以上等级的证书。

b访问控制

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。

B 数据安全的技术要求

a数据保密性要求

消息发送方应对消息字段中涉及交易及隐私等数据利用消息密钥进行加密，加密算法宜使用AES 128位加密，加密模式采用CBC，填充模式采用PKCS5Padding方式。消息接收方收到消息之后，根据消息密钥对消息体中的消息数据进行解密，校验参数合法性后方可进行后续业务处理。

b数据完整性要求

· 消息报文应使用数字签名：参数签名采用HMAC-MD5算法，采用MD5作为散列函数，通过签名密钥对整个消息主体进行加密，并采用MD5信息摘要的方式形成新的密文，按照消息体顺序拼接。参数签名要求大写。

· 数据传输过程中应设置重发机制：重发次数应大于等于3次，重发周期宜为1min。

（4）通信密钥的使用及管理要求

A 密钥体系

每个运营商平台、政府平台、第三方平台之间交互前需要分配平台标识（OperatorID）、平台密钥（OperatorSecret）、消息密钥（DataSecret）、消息密钥初始化向量（DataSecretIV）和签名密钥（SigSecret）。

1）平台标识（OperatorID）: 固定9位，平台所属方的组织机构代码，作为平台的唯一标示。

2）平台密钥（OperatorSecret）:可采用32H、48H和64H，由 0-F字符组成，为申请认证使用。

3）消息密钥（DataSecret）:用于对所有接口中Data信息进行加密。

4）消息密钥初始化向量（DataSecretIV）：固定16位，用户AES加密过程的混合加密。

5）签名密钥（SigSecret）: 可采用32H、48H和64H，由 0-F字符组成，为签名的加密密钥。

B 密钥的安全管理要求

密码算法用于密钥的产生、分发、HMAC以及加密等安全功能，相关的算法模块在其生命周期内不能被修改、导出至安全环境外部。

指定功能的密钥仅能做指定功能使用，不能被其他任何功能使用。

a 密钥的产生

数据密钥应具备随机产生特性，密钥产生后要检查密钥的有效性，弱密钥和半弱密钥需被剔除。

运营商加入信息交换时，必须申请独立的密钥文件，密钥可由运营商协商产生。

b 密钥的分发

密钥的分发应该由安全方式进行，可通过线下分发、联机报文或数字信封的方式加密传输。

c密钥的存储

密钥宜保存在硬件加密机内。如果出现在硬件加密机外，则必须密文方式出现。

密钥注入、密钥管理和密钥档案的保管应由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。

c 密钥的销毁

当新密钥产生后，生命期结束的旧密钥必须从数据库和内存中清除，防止被替换使用；同时所有可能重新构造此密钥的信息也必须清除。新密钥成功启用和旧密钥自动销毁的记录将被更新。

* + 1. **APP到服务器的通讯协议**

（1）移动应用架构

移动应用的架构由移动应用的APP和移动应用的服务端组成，如图1所示。

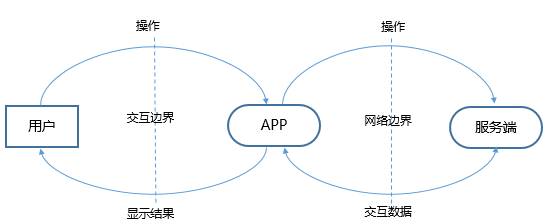


图1移动应用的基本架构

用户：具有对移动应用进行操作行为的主体。

APP：指移动应用的客户端，为用户提供本地服务的程序。

服务端：指移动应用的服务端，本标准规定的服务端仅包含为客户端提供针对性的服务程序。

边界：指主体之间互联互通的界限，包括交互边界、网络边界、运行环境边界、系统边界等。

其中，移动应用的客户端架构如图2所示。



图2移动应用的客户端架构

移动应用的客户端主要由业务逻辑模块和安全模块构成：

业务逻辑模块：完成移动应用每项业务特征过程的描述集合。

安全模块：为移动应用涉及用户的账号、口令、个人信息等敏感数据提供加解密、为移动应用网络链接提供安全保障、存储用户个人密钥以及用户身份验证鉴权等功能的集合。

移动应用的客户端涉及到的外部实体包括用户、系统、服务端和其他移动应用，包含以下功能：

交互功能：实现用户与移动应用进行交互操作的集合，包括数据显示、数据输入等。

接口功能：提供给移动应用开发人员基于移动应用访问的一组程序的能力集合，其无需访问源代码，或理解内部工作机制的细节。

通信功能：移动应用与服务端进行通信和服务所必须遵循的规则和约定的集合。

移动应用的服务端架构如图3所示。



图3移动应用的服务端架构

移动应用的服务端主要由认证鉴权和业务逻辑构成：

认证鉴权：对移动应用与服务端的通信请求、答复进行鉴权行为的集合。

业务逻辑：完成服务端每项业务特征过程的描述集合。

移动应用的服务端涉及到的外部实体包括移动应用和其他服务器，包含以下功能：

通信功能：移动应用服务端与客户端、与其他服务器进行通信和服务所必须遵循的规则和约定的集合。

（2）移动应用数据

移动应用的数据是移动应用在客户端、服务端以及通信过程中产生并存储的数据。包含但不限于用户敏感数据、业务逻辑数据和系统运行数据等。

（3）APP接入认证

当APP请求远程接入系统时，应采用双向认证机制，并采用安全机制保障身份凭证传输的保密性、完整性。

服务端对APP的认证至少包括APP载体的设备硬件指纹信息。

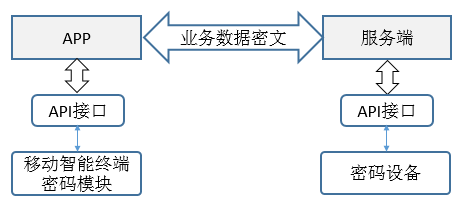
（4）远程传输安全

应采用认证、加密、数据完整性保护等安全机制，保障APP到服务器之间数据传输的保密性、完整性和数据原发/接收行为的抗抵赖；

应采用会话超时检测机制，保障APP数据传输的可用性。

加密方式可根据业务需要选择应用主动加密或链路透明加密。

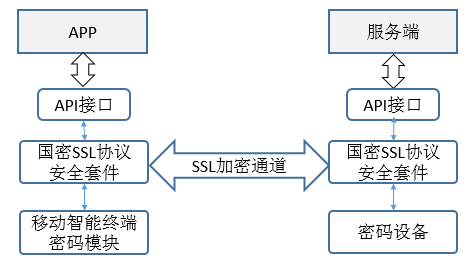
应用主动加密示意如下：



APP通过调用移动智能终端密码模块提供的API接口，调用数字签名/延签、数据加解密、完整性等密码运算服务，对所保护的关键业务数据进行主动加密和完整性保护。移动密智能终端码模块安全级别应不低于二级。

服务端通过调用密码设备提供的的API接口，调用数字签名/延签、数据加解密、完整性等密码运算服务，对所保护的关键业务数据进行主动加解密和完整性保护。密码设备包括硬件密码卡、服务器密码机等专用密码设备。

链路透明加密示意如下：



链路透明加密即APP和服务端程序只需要通过安全厂商提供的国密标准SSL协议安全套件的几个API接口，即可实现国密标准SSL加密通道的建立，对业务数据进行透明加密和完整性保护。

（5）数据安全存储

应对APP产生的敏感数据加密存储。

应采用基于角色的数据访问控制机制。

# 信息安全管理

* 1. **安全策略和管理制度**
     1. **安全策略**

应制定信息安全防范工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

* + 1. **管理制度**

应对安全管理活动中的各类管理内容建立安全管理制度；

应对要求管理人员或操作人员执行的日常管理操作建立操作规程；

应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系。

* + 1. **制定和发布**

应指定或授权专门的部门或人员负责安全管理制度的制定；

安全管理制度应通过正式、有效的方式发布，并进行版本控制。

* + 1. **评审和修订**

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

* 1. **安全管理机构和人员**
     1. **岗位设置**

应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；

应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

应设立系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

* + 1. **人员配备**

应配备一定数量的系统管理员、网络管理员、安全管理员等；

应配备专职安全管理员，不可兼任。

* + 1. **授权和审批**

应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

* + 1. **沟通和合作**

应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理信息安全问题；

应加强与各类供应商、业界专家及安全组织的合作与沟通；

* + 1. **审核和检查**

应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

* + 1. **人员录用**

应指定或授权专门的部门或人员负责人员录用；

对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；

应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

* + 1. **人员离岗**

应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

* + 1. **安全意识教育和培训**

应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

应针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；

应定期对不同岗位的人员进行技能考核。

* + 1. **外部人员访问管理**

应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

外部人员离场后应及时清除其所有的访问权限；

获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

* 1. **安全建设管理**
     1. **定级和备案**

应对电动汽车充电设施关键信息系统组织相关部门和有关安全技术专家进行论证定级，并将备案材料报主管部门和相应公安机关备案。

* + 1. **安全方案设计**

应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

应根据电动汽车充电设施关键信息系统的安全保护等级及与其他关键系统的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；

应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，系统应经过批准后才能正式实施。

* + 1. **产品采购和使用**

应确保相关信息安全产品采购和使用符合国家的有关规定；

应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；

应预先对产品进行选型测试，确定产品的候选范围。

工业控制系统重要设备及专用信息安全产品应通过国家及行业监管部门认可的专业机构的安全性及电磁兼容性检测后方可采购使用。

* + 1. **软件开发**

应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

应制定代码编写安全规范，要求开发人员参照规范编写代码；

应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；

应确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码、后门和隐蔽信道进行检测；

应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

* + 1. **工程实施**

应指定或授权专门的部门或人员负责工程实施过程的管理；

应制定工程实施方案控制安全工程实施过程；

应通过工程监理措施控制项目的实施过程，确保工程实施的质量。

* + 1. **测试验收**

应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

* + 1. **系统交付**

应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

应对负责运行维护的技术人员进行相应的技能培训；

应确保提供建设过程中的文档和指导用户进行运行维护的文档。

* + 1. **风险评估**

应根据系统的安全级别定期进行风险评估，发现不符合相应安全保护标准要求的及时整改；

应根据相关政策等要求合理选择风险评估方式，如自评估、第三方评估机构等。

* + 1. **服务供应商选择**

应确保服务供应商的选择符合国家的有关规定；

应与选定的服务供应商签订保密等相关协议，明确整个服务供应链各方需履行的信息安全相关义务；

应定期监视、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

购买云服务的，应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

* 1. **安全运维管理**
     1. **环境管理**

应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等。

系统部署在公有云平台的，应选择云计算基础设施位于中国境内的云服务商，且通过国家相关部门的安全性审查。

* + 1. **资产管理**

应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

* + 1. **设备维护管理**

应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

购买云服务的应要求云服务商制定相应措施。

* + 1. **漏洞和风险管理**

应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

应定期开展安全风险评估，形成安全风险评估报告，采取措施应对发现的安全问题。

* + 1. **网络和系统安全管理**

应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；

应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

* + 1. **恶意代码防范管理**

应提高所有用户的防恶意代码意识，告知对外来计算机或存储设备接入系统前进行恶意代码检查等；

应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

应定期验证防范恶意代码攻击的技术措施的有效性。

* + 1. **配置管理**

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

* + 1. **密码管理**

应采用国家密码管理主管部门批准使用的密码算法；

应使用国家密码管理主管部门认证核准的密码产品。

* + 1. **变更管理**

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

* + 1. **备份与恢复管理**

应识别需要定期备份的重要业务信息、系统数据及软件系统等；

应规定备份信息的备份方式、备份频度、存储介质、保存期等；

应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

* + 1. **安全事件处置**

应及时向安全管理部门报告所发现的安全弱点和可疑事件；

应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

* + 1. **应急预案管理**

应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

* + 1. **外包运维管理**

应确保外包运维服务商的选择符合国家的有关规定；

应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

应确保选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。

# 数据与隐私

* 1. 任何应用涉及收集或使用个人数据的，应明确提示用户，并得到用户授权，同时允许用户关闭相关功能；
  2. 涉及个人数据的产品或应用，接入互联网前应明确提示用户，并得到用户授权；
  3. 应用由于业务需要对个人数据进行收集或使用的，不应超出声明范围，且应循最小化原则；
  4. 应对存储的个人数据和重要数据提供访问控制、加密、日志记录等安全保护机制；
  5. 应提供机制或指导来删除或匿名化超过存留期的、或临时应用的个人数据；
  6. 应支持用户卸载涉及个人数据的应用；
  7. 修改或删除个人数据时，应明确提示用户，并得到用户授权；
  8. 个人数据和重要数据的删除应是安全删除；
  9. 应在资料中列出所收集或使用的个人数据列表，并说明收集或使用的目的和保护措施；
  10. 出于故障定位等目的收集个人数据和重要数据的，应对个人数据和重要数据进行过滤或匿名化处理；
  11. 将个人数据共享给第三方，或者个人数据在应用软件之间的共享应明确提示用户，并得到用户授权。

# 附录A 测评报告

A.1总则

测评实施方在测评完成后，应向委托测评方提交正式的的测评报告，测评报告应包括但不限于以下内容：

1. 测评对象概述；
2. 测评依据；
3. 测评概要；
4. 测评分析；
5. 测评结论；
6. 附件。

A.2测评对象概述

对委托测评的单位、被测评对象名称、测评内容、测评范围等进行简要说明。

A.3测评依据

测评机构进行测评时所依据的基础，如国家有关法律、法规，以及国家、税务行业和地方现行的软件项目相关标准和规范等。

A.4测评概要

A.4.1 测评人员

列出参与该测评人员的角色、姓名和具体职责。可以表格形式罗列重要角色人员。

A.4.2 测评环境

列出执行该测评时所搭建的软、硬件环境、网络环境配置信息，对于架构的环境，需要绘出网络拓扑图，根据网络拓扑图列出相关配置。

A.4.3 测评时间

列出测评主要活动或关键工作的时间跨度和工作量，如开始时间、结束时间，工作人时等。

A.4.4 测评的类型及范围

详细描述本次测评所测评的类型及范围，类型包括（但不限于）功能测评、性能测评、安全测评、数据标准符合性测评、交付物测评等。范围如功能包含全部功能点、性能测评含盖的业务流程、项目文档等。

A.5 测评分析

按照所发现缺陷的严重级别、功能模块分布和趋势进行图形或表单统计，并根据测评对象的特性对税务部门关注重点和经常出现的错误进行分析。

A.5.1 缺陷分析

对上述缺陷和其他收集数据进行综合分析，如：缺陷密度（缺陷总数/功能点总数），缺陷发现效率（缺陷总数/执行测评用时）等。通过缺陷密度可以得出系统各功能或需求的缺陷分布情况。

A.5.2 覆盖分析

A.5.2.1 测评覆盖分析

测评覆盖率＝执行用例数/用例总数×100％。

A.5.2.2 需求覆盖分析

需求覆盖率＝Y（P）项/需求项总数×100％。

A.5.2.3 统计

按需求编号给出每一需求测评的通过与否。Y表示通过、P表示部分通过，N/A表示不可测评或者用例不适用，统计各项总数计算需求的覆盖率。

A.6测评结论

依据测评结果及其分析给出测评结论，根据测评情况可给出适中的建议。

A.7附件

附件应包含安全风险严重等级定义，具体内容参照附录B。

# 附录B 安全风险严重等级

B.1 安全风险严重等级定义

表B.1 安全风险严重等级定义

|  |  |
| --- | --- |
| 严重等级 | 描 述 |
| 严重 | 缺陷对进度的影响可能是非常致命的，或者可能是一个停止器——即终止用户继续使用系统；或者影响测评工作继续进行的缺陷。 |
| 较严重 | 系统基本能正常工作但同一错误现象频繁出现或者问题不解决时会给后续工作带来较大风险（如需求描述不正确导致系统设计错误）。 |
| 一般 | 不属于“严重”、“较严重”、“微小”之外的缺陷。 |
| 微小 | 不影响系统功能，但影响系统的易用性（如界面美观问题、操作建议等）或产出物的一些非技术性质量问题（如文档版本、错别字等）。 |

# 附录C 数据加/解密方法

C.1 AES加密算法

数据传输的加密使用对称加密算法AES加密，AES算法的密钥长度、分组长度和轮数的关系如表1所示。

1. **Key-Block-Round关系**

|  |  |  |
| --- | --- | --- |
| **密钥长度**  **(Nk words)** | **分组长度**  **(Nb words)** | **轮数**  **(Nr)** |
| 4 | 4 | 10 |
| 6 | 4 | 12 |
| 8 | 4 | 14 |

对于AES加密和解密变换，AES算法使用的轮函数由4个不同的以字节为基本单位的变换复合而成，该过程由四个不同的阶段组成：

1)S盒变换，用一个S盒完成分组中的按字节代替；

2)行移位变换，一个简单的置换；

3)列混淆变换，一个利用在域GF(28)上的算术性的代替；

4)轮密钥加变换，一个利用当前分组和扩展密钥的一个部分进行按位异或。

AES对数据的加密过程是通过把输入的明文和密钥由轮函数经Nr轮迭代来实现的，结尾轮与前Nr-1轮不同。前Nr-1轮依次进行S盒变换、行移位变换、列混淆变换和轮密钥加变换；结尾轮与前Nr-1轮相比去掉了列混淆变换。

而解密过程与加密过程相反，通过把输入的密文和密钥由轮函数经Nr轮迭代来实现的，结尾轮与前Nr-1轮不同。前Nr-1轮依次进行逆行移位变换、逆S盒变换、轮密钥加变换和逆列混淆变换；结尾轮与前Nr-1轮相比去掉了逆列混淆变换。

AES算法的加密解密过程如图2所示。



**图2 AES加/解密过程图**

C.2 数据加/解密示例（密钥、向量不作为固定值）

密钥：1234567890abcdef

初始向量：1234567890abcdef

明文信息：

1. {"total":1,"stationStatusInfo":{"operationID":"123456789","stationID":"111111111111111","connectorStatusInfos":{"connectorID":1,"equipmentID":"10000000000000000000001","status":4,"currentA":0,"currentB":0,"currentC":0,"voltageA":0,"voltageB":0,"voltageC":0,"soc":10,}}}

秘文：

1. il7B0BSEjFdzpyKzfOFpvg/Se1CP802RItKYFPfSLRxJ3jf0bVl9hvYOEktPAYW2nd7S8MBcyHYyacHKbISq5iTmDzG+ivnR+SZJv3USNTYVMz9rCQVSxd0cLlqsJauko79NnwQJbzDTyLooYoIwz75qBOH2/xOMirpeEqRJrF/EQjWekJmGk9RtboXePu2rka+Xm51syBPhiXJAq0GfbfaFu9tNqs/e2Vjja/ltE1M0lqvxfXQ6da6HrThsm5id4ClZFIi0acRfrsPLRixS/IQYtksxghvJwbqOsbIsITail9Ayy4tKcogeEZiOO+4Ed264NSKmk7l3wKwJLAFjCFogBx8GE3OBz4pqcAn/ydA=

# 附录D 参数签名方法

D.1 HMAC-MD5算法

HMAC（K，M）=H（K⊕opad∣H（K⊕ipad∣M））

其中:K是密钥（OperatorSecret），长度可为64字节，若小于该长度，在密钥后面用“0”补齐。

M是消息内容；

H是散列函数；

opad和Ipad分别是由若干个0x5c和0x36组成的字符串；

⊕表示异或运算；

∣表示连接操作。

D.2 HMAC-MD5流程

1) 在签名密钥（SigSecret）后面添加0来创建一个长为64字节的字符串(str)；

2) 将上一步生成的字符串(str)与ipad(0x36)做异或运算，形成结果字符串(istr)；

3)将消息内容data附加到第二步的结果字符串(istr)的末尾；

4)做md5运算于第三步生成的数据流(istr)；

5) 将第一步生成的字符串(str)与opad(0x5c)做异或运算，形成结果字符串(ostr)；

6)再将第四步的结果(istr)附加到第五步的结果字符串(ostr)的末尾；

7)做md5运算于第六步生成的数据流(ostr)，输出最终结果(out)。

D.3 参数签名示例

**签名密钥**：1234567890abcdef

**运营商标识（OperatorID）：**123456789

**参数信息（Data）：** il7B0BSEjFdzpyKzfOFpvg/Se1CP802RItKYFPfSLRxJ3jf0bVl9hvYOEktPAYW2nd7S8MBcyHYyacHKbISq5iTmDzG+ivnR+SZJv3USNTYVMz9rCQVSxd0cLlqsJauko79NnwQJbzDTyLooYoIwz75qBOH2/xOMirpeEqRJrF/EQjWekJmGk9RtboXePu2rka+Xm51syBPhiXJAq0GfbfaFu9tNqs/e2Vjja/ltE1M0lqvxfXQ6da6HrThsm5id4ClZFIi0acRfrsPLRixS/IQYtksxghvJwbqOsbIsITail9Ayy4tKcogeEZiOO+4Ed264NSKmk7l3wKwJLAFjCFogBx8GE3OBz4pqcAn/ydA=

**时间戳（TimeStamp）：**20160729142400

**自增序列（Seq）**：0001

**签名（Sig）**：745166E8C43C84D37FFEC0F529C4136F

# 附录E（资料性附录）

应用于 IEC60870-5-104 规约的示例

通常情况下，安全通信过程的建立包括五个阶段。

E.1 建立 TCP 连接（TCP 三次握手）

客户端向服务器发出 TCP 连接请求，服务器响应请求并完成三次握手。 E.2 客户端安全连接请求（ClientHello）

客户端向服务器发出建立安全通信的请求，称为 ClientHello。在这一步， 客户端主要向服务器提供以下信息：

（1）支持的协议版本，比如 TLS 1.0 版。

（2）一个客户端生成的随机数，稍后用于生成"对话密钥"。

（3）支持的加密方法，比如 RSA 公钥加密。

（4）支持的压缩方法。

E.3 服务器安全连接回应（SeverHello） 服务器收到客户端请求后，向客户端发出回应，称为 SeverHello。服务器的

回应包含以下内容：

（1）确认使用的加密通信协议版本，比如 TLS 1.0 版本。如果浏览器与服 务器支持的版本不一致，服务器关闭加密通信。

（2）一个服务器生成的随机数，稍后用于生成"对话密钥"。

（3）确认使用的加密方法，比如 RSA 公钥加密。

（4）服务器证书。

（5）请求客户端证书。

E.4 客户端安全连接回应

客户端收到服务器回应以后，首先验证服务器证书。如果证书不是可信机构 颁布、或者证书中的域名与实际域名不一致、或者证书已经过期，就会向访问者 显示一个警告，由其选择是否还要继续通信。

如果证书没有问题，客户端就会从证书中取出服务器的公钥。然后向服务器 发送下面四项信息：

（1）客户端的证书。

（2）一个随机数。该随机数用服务器公钥加密，防止被窃听。

（3）编码改变通知，表示随后的信息都将用双方商定的加密方法和密钥发 送。

（4）客户端握手结束通知，表示客户端的握手阶段已经结束。这一项同时也 是前面发送的所有内容的 hash 值，用来供服务器校验。

上面第二项的随机数，是整个握手阶段出现的第三个随机数，又称"pre- master key"。有了它以后，客户端和服务器就同时有了三个随机数，接着双方 就用事先商定的加密方法，各自生成本次会话所用的同一把"会话密钥"。

E.5 服务器的响应

服务器收到客户端的第三个随机数 pre-master key 之后，计算生成本次会 话所用的"会话密钥"。然后，向客户端最后发送下面信息。

（1）编码改变通知，表示随后的信息都将用双方商定的加密方法和密钥发 送。

（2）服务器握手结束通知，表示服务器的握手阶段已经结束。这一项同时也 是前面发送的所有内容的 hash 值，用来供客户端校验。

至此，整个握手阶段全部结束。接下来，客户端与服务器进入安全通信，应 用层完全采用普通的 IEC60870-5-104 协议，只不过用"会话密钥"加密内容。 A.6 安全通信连接建立流程如下所示：

客户端 服务端

tcp(syn)=1 --------> tcp(syn, ack)=1 tcp(ack)=1 -------->

ClientHello -------->ClientCertificate

ClientKeyExchange

ServerHello ServerCertificate ServerKeyExchange\* CertificateRequest\*

<-------- ServerHelloDone

CertificateVerify

[ChangeCipherSpec]

Finished -------->

[ChangeCipherSpec]

<-------- Finished

104StartDT:ACT=1 -------->

<-------- 104StartDT:CON=1

104Data <-------> 104Data