ICS 35.240.01
CCS L 67

DB36

江 西 省 地 方 标 准

DB36/T 1476—2021

碳普惠平台建设技术规范

Technical specification for construction of carbon generalized system of preferences platform

地方标准信息服务平台

2021 - 08 - 30 发布　　2021 - 10 - 01 实施

江西省市场监督管理局　　发 布

地方标准信息服务平台

目　　次

地方标准信息服务平台

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由抚州市市场监督管理局提出并归口。

本文件起草单位：抚州市发展和改革委员会、抚州市数字街区运营管理有限公司、江西思极智云数字科技有限公司、江西省质量和标准化研究院、江西省政府投资项目评审中心、江西省生态文明研究院。

本文件主要起草人：杨瑞春、冯哲、周吉、周悦梅、郑斌华、黄文浪、程国松、雷文锋、钟达、潘兴棋、龚跃林、吴玉环、毛炜翔、王锐、刘熙、许自豪、龚茗、吕雪、冯欣。

地方标准信息服务平台

碳普惠平台建设技术规范

1 范围

本文件确立了碳普惠平台建设的术语和定义、建设要求、总体技术架构、功能要求、数据接口要求、安全性要求、运行维护要求等内容。

本文件适用于碳普惠平台建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

低碳行为 low-carbon behavior

日常生产、生活中能够明显减少二氧化碳等温室气体排放的活动。

注：本文件低碳行为主要是指个人低碳行为，主要包括绿色出行、绿色生活、绿色消费、绿色公益等四大类。

3.2

减碳量 carbon emission reduction

低碳行为致使二氧化碳等温室气体排放减少的量。

3.3

碳积分 carbon credits

低碳行为致使减碳量而赋予一定价值的量化指标，作为低碳行为产生社会价值的衡量标准。

地方标准信息服务平台

3.4

碳普惠制 carbon generalized system of preferences

对公众自愿践行的低碳行为进行具体量化和赋予一定价值，通过与商业激励、政策激励、公益激励和交易激励相结合的正向引导机制。

3.5

碳普惠平台 carbon generalized system of preferences platform

基于碳普惠制，依托信息化技术，通过数据采集、记录并量化低碳行为的减碳量，并将减碳量换算成一定量的碳积分发放到相应账户中，可用碳积分兑换优惠及服务的公共服务平台。

3.6

第三方应用平台 third-party application platform

与碳普惠平台达成合作，通过接口等方式对接数据，共同为用户提供服务的其它应用或软件。

3.7

入驻商户 settled merchants

向碳普惠平台运营方提出入驻申请且提供相应证明材料后,通过资质审核可以入驻碳普惠商城平台的商户。

4 建设要求

4.1 平台设计应统筹规划，考虑各级平台实现各类数据资源共享、互联互通性，且保障数据交换过程的安全性。

4.2 应采用模块化设计，便于碳账户管理、商城运营、低碳应用等功能的扩展升级。

4.3 应提供统一数据交换平台功能，实现各级平台之间数据安全传输和共享。

4.4 应具备安全的信息化基础设施及环境，能够支撑碳普惠平台运行。

4.5 应具有完备访问控制及安全机制，系统具备灵活的访问权限配置机制及多层次的安全控制机制。

4.6 应优先采用主流成熟技术，系统应标准设计，可提供与第三方应用平台无缝对接能力。

4.7 应具备良好的响应速度、容错纠错能力、可维护性、可扩展性和稳定性。

4.8 应建立完善的运维保障机制，保障平台的稳定运行。

5 总体技术架构

5.1 总体架构

5.1.1 平台总体架构应保证实现所有业务及数据的有效、统一管理。

5.1.2 平台总体架构应分为五大层次，从下往上依次包括基础设施层、数据资源层、支撑层、应用层、交互层，采用微服务技术架构，保障平台可根据业务量自动伸缩扩展，总体技术架构见图 1。

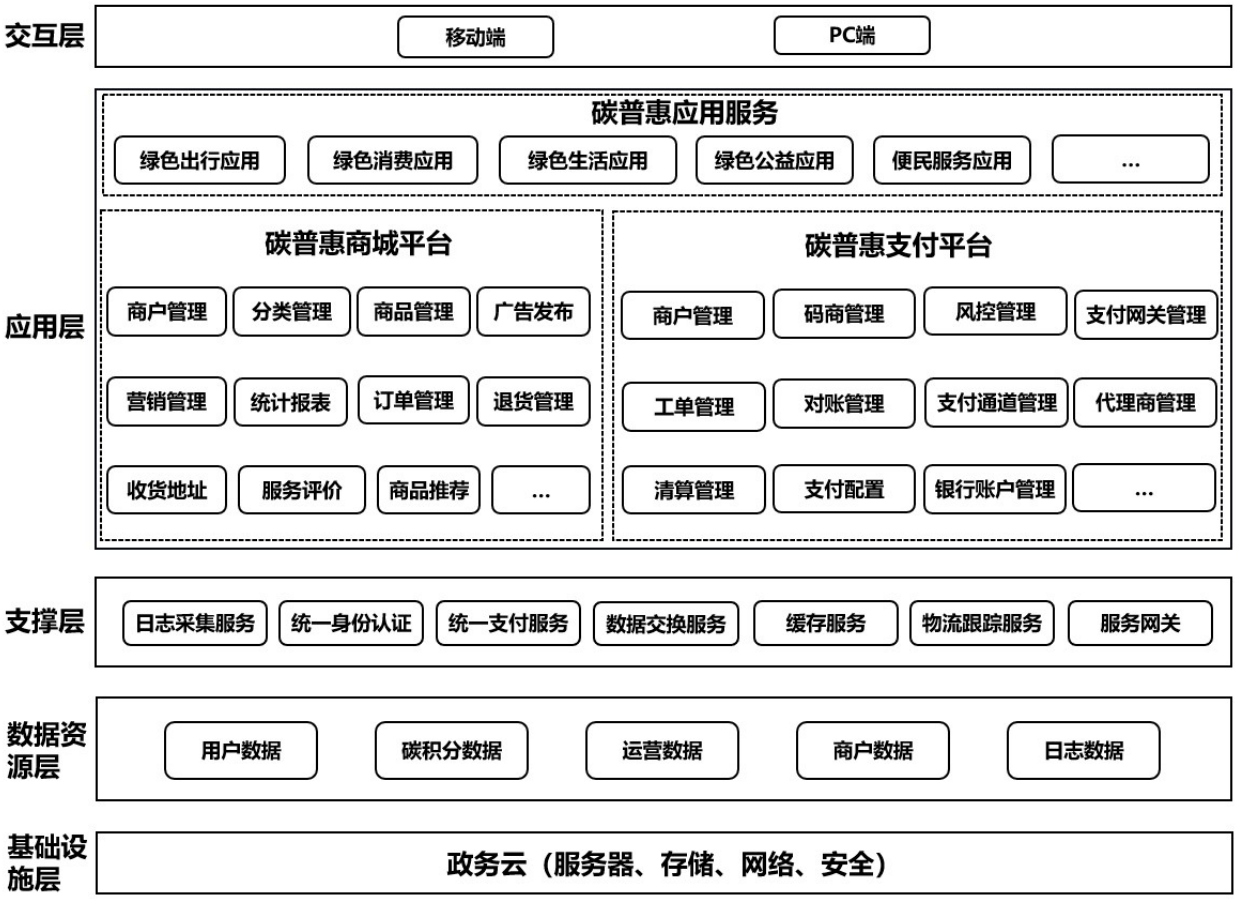

图1　碳普惠平台总体技术架构图

5.2　基础设施层

应依托政务云平台进行集约化部署建设，为平台提供安全、稳定的基础运行环境，包括主机硬件、交换机、路由器、防火墙、网络及安全防御设备，主机操作系统，第三方应用中间件等。

5.3　数据资源层

应包括碳普惠平台注册用户数据、低碳行为数据、运营数据、日志数据的采集、存储、分析和管理，为碳普惠公共服务提供统一的数据存储服务。

5.4　支撑层

应为平台的运行提供基础服务支撑，包括日志采集服务、统一身份认证、统一支付服务、缓存服务、数据交换服务、物流跟踪服务及服务网关等。

5.5　应用层

应为平台用户、平台运营方、平台入驻商户提供应用服务，由商城平台、支付平台、应用服务三部分组成。

5.6　交互层

应为平台用户、平台运营方、平台入驻商户提供包括 PC 端和移动端多种访问方式，支持各种类型移动终端设备。

地方标准信息服务平台

6 功能要求

6.1 基本要求

6.1.1 应包括 PC 端后台管理功能和移动端 APP 应用程序、小程序功能，PC 端应采用 B/S 访问方式，移动端应同时支持 Android、苹果 IOS 和华为鸿蒙系统。
6.1.2 应包括应用服务功能，可包括但不限于低碳应用、便民服务应用及营销工具应用。
6.1.3 应包括碳普惠商城平台相关功能，包括移动商城、商城商户管理系统、商城运营管理系统。
6.1.4 应包括碳普惠支付平台相关功能，包括电子钱包、支付平台商户管理系统、支付平台运营管理系统，可支持多家银行电子钱包，电子钱包应支持通用账户和专款专用账户。

6.2 应用服务功能

6.2.1 低碳行为应用

将平台用户低碳行为转化为减碳量及碳积分，主要包括绿色出行、绿色消费、绿色生活、绿色公益等可记录用户低碳行为数据的应用。

6.2.2 便民服务应用

可为平台用户提供涉及日常出行、信息查询、网上缴费、无感停车缴费、智慧物业、家政等便民服务。

6.2.3 营销工具应用

可包括但不限于朋友圈分享等多种营销功能。

6.3 商城平台功能

6.3.1 移动商城

6.3.1.1 应为平台用户提供便捷的网上购物服务，支持商品浏览、在线购买、线上支付、商品退货、订单物流查询、服务评价等。
6.3.1.2 应提供碳积分优惠兑换专区和绿色消费积分专区服务。
6.3.1.3 应包括但不限于商品搜索、购物车、在线支付、订单管理、收货地址管理、退货管理、碳积分优惠专区、普惠商品专区、物流查询、碳积分查询、服务评价等。

6.3.2 商户后台管理

6.3.2.1 应为平台入驻商户提供日常门店运营管理功能，商家可上架本店经营许可范围内的各类商品，了解每日商品销售情况，并为平台用户提供商品咨询、商品退换货等服务。
6.3.2.2 应包括但不限于商品管理、订单管理、用户统计、服务评价管理、订单统计、结算统计、优惠券管理、退货管理、物流跟踪、会员管理等。

6.3.3 平台运营后台管理

应为平台入驻商户提供日常运营管理功能，包括商户入驻审核、商品分类管理、营销活动策划管理、广告发布管理及各类运营数据统计分析等。

6.4 支付平台功能

6.4.1 电子钱包

应与具备相关资质的金融机构合作，电子钱包应包括用户开户、钱包充值、绑定银行卡、交易记录查询、密码修改、免密设置、销户功能，方便用户在移动商城购物和日常出行、线下消费的快捷支付。

6.4.2 支付平台商户管理

6.4.2.1 应为入驻支付平台的商户提供日常运营管理，商户可查询本店收款情况、资金流水情况、支付订单情况等。

6.4.2.2 包括但不限于资金流水查询、二维码管理、支付通道管理、支付订单管理、对账管理、银行账户管理等。

6.4.3 支付平台运营管理

6.4.3.1 应为支付平台运营方提供日常运营管理，包括支付平台商户入驻审核、代理商资格审核管理、平台资金风控管理、平台资金清算，为入驻商户提供售后及统计报表服务。

6.4.3.2 包括但不限于商户管理、代理商管理、风控管理、清算管理、工单管理、客服管理、码商管理、订单统计、支付配置、报表分析、对账统计管理、支付网关管理、系统管理、支付管理等。

7 数据接口要求

7.1 碳普惠平台和第三方应用平台接口数据交互方式应采用 HTTPS 协议，并以 POST 请求方式提交，请求数据与返回数据均使用 JSON 格式，参见附录 A。

7.2 敏感数据的传输应进行加密处理，依据 GB/T 35276、GB/T 32905、GB/T 32907 的要求采用 SM2、SM3、SM4 国密算法加密。

8 安全性要求

8.1 基本要求

应满足 GB/T 22239 安全等级保护基本要求并根据 GB/T 22240 安全防护等级三级标准设计，需通过第三方检测机构的安全性评测。

8.2 应用系统

8.2.1 访问控制

8.2.1.1 应控制不同用户在不同数据、不同业务环节上的查询、添加、修改、删除的权限，提供面向 URL 地址、Service 接口、IP 地址的控制能力，提供 Session 的超时控制。

8.2.1.2 应限制登录失败次数，避免客户密码遭到窃取。

8.2.2 数据库系统

8.2.2.1 应通过系统权限、数据权限、角色权限管理，建立数据库系统的权限控制机制，任何业务终端不应直接访问数据库服务器，应通过 Web 服务器或接口服务器访问数据库服务器，并设置严格的数据库访问权限。

8.2.2.2 应建立完备的数据修改日志，通过安全审计记录追踪用户对数据库的操作，明确对数据库的安全责任。

8.2.3 身份认证

应通过信息加密、数字签名、身份认证等措施综合解决信息的机密性、完整性、身份真实性和操作的不可否认性问题。

8.3 运行环境

8.3.1 网络与边界

应配备防火墙、入侵检测等安全设备，保证网络免受攻击和非法访问，防止外部入侵，确保网络正常运行和传输的安全。

8.3.2 主机系统

应选用 Linux 操作系统或国产操作系统，定期扫描操作系统安全漏洞并及时给系统打补丁，要求选用国产杀毒软件和攻击防御系统软件对主机系统进行安全防护。

8.4 数据安全性

8.4.1 应对所有数据进行定期备份，可采用定期全备份、差分备份、按需备份、异地备份和增量备份的策略，来保证数据的安全。

8.4.2 应对口令等敏感数据进行加密存储，对敏感数据做脱敏处理，参见附录 B。

8.4.3 应将加密密钥与加密数据分开进行存储，并对密钥进行严格的访问。

8.4.4 应保护用户隐私，用户信息安全管理应符合 GB/T 35273 的要求。

9 运行维护要求

9.1 网络基础

应定期评估网络基础平台的性能，制定故障维护预案，及时消除可能的故障隐患，保证路由设备、网络交换设备等网络基础设施的安全性、可靠性、可用性。

9.2 数据存储

9.2.1 应定期评估存储设施及软件平台的性能，确认数据存储的安全等级，保证数据存储设施如服务器设备、集群系统、存储阵列、存储网络等以及支撑数据存储设施运行的软件平台的安全性、可靠性和可用性，保证存储数据的安全。

9.2.2 应制定故障应急预案，及时消除故障隐患，保障信息系统的安全、稳定、持续运行。

9.3 主机系统

应定期评估系统平台，保证操作系统、数据库系统、中间件、其他支撑应用软件系统及网络协议等的安全性，及时处理安全漏洞。

9.4 风险评估

应对系统的安全威胁、脆弱性、漏洞以及安全管理进行评估，制定风险应对策略和风险处理机制，及时消除或弱化风险，将残余风险控制在可控范围内。

9.5 病毒防护

应制定病毒防护和恢复策略，定期评估病毒影响，采取相应的病毒防护措施，制定病毒事件处理预案。

9.6 数据维护

应定期评估数据的完整性、安全性、可靠性，保证数据存储、数据访问、数据通信、数据交换的安全，制定备份、冗灾策略和数据恢复策略，消除可能存在的安全隐患和威胁。

地方标准信息服务平台

附 录 A
（资料性）
JSON 规范

标准 JSON 的合法符号：{(左大括号) }(右大括号) "(双引号) :(冒号) ,(逗号) [(左中括号)](右中括号)

JSON 字符串：特殊字符可在字符前面加 \ 或使用 \u 加 4 位 16 进制数来处理，二进制需要进行 base64 转码。 如{"name":"jobs"}。

JSON 布尔：必须小写的 true 和 false 如 {"bool":true}。

JSON 空：必须小写的 null 如 {"object":null}。

JSON 数值：不能使用 8/16 进制

{"num":60}

{"num":-60}

{"num":6.6666}

{"num":1e+6}<!-- 1 乘 10 的 6 次方，e 不区分大小写 -->

{"num":1e-6}<!-- 1 乘 10 的负 6 次方，e 不区分大小写 -->

JSON 对象:

```
{
    "starcraft": {
        "INC": "Blizzard",
        "price": 60
    }
}
```

JSON 数组:

```
{
    "person": [
        "jobs",
        60
    ]
}
```

JSON 对象数组:

```
{
    "array": [
        {
            "name": "jobs"
        },
        {
            "name": "bill",
            "age": 60
        },
        {
            "product": "war3",
```

地方标准信息服务平台

```
            "type": "game",
            "popular": true,
            "price": 60
        }
    ]
}
```


地方标准信息服务平台

附 录 B
（资料性）
数据脱敏规则

B.1 具体数据脱敏规则见表 B.1。

表 B.1 数据脱敏规则

序号	脱敏内容	脱敏规则	示例
1	中文姓名	保留第一位，后面以*替换	李**
2	公民身份号码	保留前 1 位，后 1 位	3******************8
3	固定电话	保留后 4 位	****1234
4	手机号码	保留前 1 位，后 2 位	1********34
5	地址	保留前 6 位	抚州市临川区****
6	电子邮箱	保留电子邮件账户第 1 位和@后面的部分	g**@163.com
7	银行卡号	保留银行卡前 6 位，后 4 位	622260*********1234
8	公司开户银行联号	保留前 2 位	12**********

地方标准信息服务平台