ICS 35.240.30
L 72

T/HBSIA

湖北省软件行业协会团体标准

T/HBSIA 001.2-2024

标准数字化应用
第 2 部分：数据交换规范

Standard digital applications
Part 2: Data exchange specification

2024-08-23 发布　　2024-08-26 实施

湖北省软件行业协会 发布

目　　次

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。

本文件是T/HBSIA 001-2024的第2部分。T/HBSIA 001-2024已经发布了以下部分：

——第 1 部分：元数据

——第 2 部分：数据交换规范

——第 3 部分：数据质量规范

本文件由湖北省标准化与质量研究院提出。

本文件由湖北省软件行业协会归口。

本文件起草单位：湖北省标准化与质量研究院、武汉市道玄科技有限公司、武汉盛锦汇科技有限公司、武汉爱迪科技股份有限公司、湖北华中电力科技开发有限责任公司、武汉金档科技有限公司、武汉达梦数据库股份有限公司、武汉百智诚远科技有限公司。

本文件主要起草人：徐术坤、韩阳昱、华振楠、余梅、舒成、赵亮清、邵璇、莫颜君、康维、彭涛、王豪、周志强、马哲贵、刘红玲、周金良、吴颖波、吴锴、张永强、胡智慧。

引　言

为了更加有效地利用标准数字资源，促进标准数字资源的共享开放，编制可信、易于理解的标准数字化应用标准已成为使用标准数字资源的首要任务。《标准数字化应用》由以下部分构成。

——第 1 部分：元数据。目的在于确定元数据描述方法、模型、不同种类元数据的描述及拓展要求。

——第 2 部分：数据交换规范。目的在于确定标准数据交换体系、交换流程及交换方式。

——第 3 部分：数据质量规范。目的在于确定标准数据质量的总体要求、技术要求及质量评价。

标准数字化应用
第 2 部分：数据交换规范

1 范围

本文件规定了标准数字化应用中标准要素数据交换的基本要求、系统要求、交换流程、交换方式和安全技术要求。

本文件适用于标准数字化应用中的数据交换管理。

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 17859 计算机信息系统 安全保护等级划分准则

GB/T 28448 信息安全技术网络 安全等级保护测评要求

GB/T 28452 信息安全技术 应用软件系统通用安全技术要求

T/HBSIA 001.1-2024 标准数字化应用 第 1 部分：元数据

3 术语和定义

下列术语和定义适用于本文件。

3.1

标准要素数据 standard element data

利用信息技术对标准进行结构化和语义化处理，转换为计算机可理解和可处理的形式，能够通过数字设备进行读取、传输和使用的数据。

3.2

服务接口 service interface

数据服务系统提供给应用系统访问数据的应用编程接口。

4 缩略语

下列缩略语适用于本文件。

API:应用程序接口(Application Programming Interface)

CA:证书颁发机构(Certificate Authority)

DMZ:隔离区(Demilitarized Zone)

EMAIL:电子邮件(Electronic Mail)

HTTP:超文本传输协议(HyperText Transfer Protocol)

HTTPS:安全超文本传输协议(Secure HyperText Transfer Protocol)

IP:互联网协议(Internet Protocol)

JSON:脚本语言对象符号，一种轻最级的数据交换格式(JavaScript Object Notation)

XML:可扩展标记语言(eXtensible Markup Language)

MQ:消息队列(Message Queue)
UTF:Unicode 转换格式(Unicode Transformation Format)
WEB:全球广域网(World Wide Web)

5 标准要素数据交换基本要求

5.1 兼容性

5.1.1 应兼容多种文件格式,包括 XML、JSON 等文件格式,支持用户自定义的文件格式。
5.1.2 应支持 HTTP、HTTPS 等协议,支持 EMAIL、WEB、API、MQ 等多种交换方式。

5.2 稳定性和可靠性

5.2.1 应按照交换节点所承载的应用系统运行保障的具体要求，提供相应的服务。
5.2.2 对于交换失败的数据应有重发机制和确认校验机制，还应提供消息队列存储、事务控制、容错容灾、错误处理、消息回执、异常监控告警等处理机制，以保障稳定性和可靠性。
5.2.3 应保证数据的唯一性。
5.2.4 应支持异步通信。
5.2.5 应支持多链路、数据堆积突发传输要求，提供负载均衡控制、限流与并发数据处理机制。

5.3 有效性

5.3.1 应保证数据在存储、传输、处理过程中不被篡改,宜采用加密和加签等技术。
5.3.2 应保障报文在传输、存储、处理等过程中数不丢失。
5.3.3 应保证业务数据在传输过程及时送达。

5.4 安全性

应符合GB 17859规定的计算机信息系统第三级及以上安全要求，符合GB/T 28448、GB/T 28452安全保护相关要求和定级方法,并符合下列要求:

a) 应采用统一的身份认证，宜用数字证书技术标识用户身份；
b) 应具备防火墙、入侵检测、安全评估、防病毒等系统网络安全防护措施；
c) 应对敏感的业务数据进行加密存储、传输数据存储、传输，宜支持各种标准的加密算法；
d) 应对敏感业务数据操作、接收及发送采用日志管理，日志数据永久保留。

5.5 数据格式

5.5.1 交换数据的字符编码应采用 UTF-8。
5.5.2 交换数据如需压缩,应采用 ZIP 算法压缩后传输，压缩文件的文件名前缀命名与原报文一致。
5.5.3 交换数据名称命名应包含报文类型、发送方、接收方及日期时间等信息。

6 标准要素数据交换系统要求

6.1 服务端

6.1.1 应具备数据接收、发送、格式转换、代码转换等数据处理功能。
6.1.2 应具备数据呼叫、应答、自动转发、地址转换、差错校验、出错报警、审核和确认、命名和寻址、合法性和完整性的检查及报文传输等功能。
6.1.3 应支持 EMAIL、WEB、API、MQ 等多种传输方式接收、发送数据。

6.1.4 可主动选择发送模式，自主选择并发线程数量与定义，支持选择文件正常发送与异常情况下的处理方式及备份方式。

6.1.5 应对接收的数据依照约定格式形成回执，对所有数据处理过程中出现的错误进行记录，并生成出错回执通知。

6.1.6 应具备数据传输状态、数据接/发方传输量、数据传输路径，数据类型等统计分析功能。

6.1.7 应具备数据交换实时监控，包括对数据传输状态监控，针对不同时段、不同客户,不同数据类型、不同传输路径等各种条件下的数据传输量的监控，并可通过日志管理详细、准确、及时记录每一个数据交换过程的属性信息及状态信息，并支持自定义查询、统计及报表功能。

6.1.8 应基于 IP、DMZ 安全中继和基于角色的用户访问的鉴别、授权,保证数据安全性。

6.1.9 应支持链路加密(如 HTTPS 等),数据加密、数据认证(如 CA 认证)。

6.1.10 应实现用户及用户传输协议、数据类型、基础代码等管理。

6.1.11 应设计备份模块,自定义文件备份时长。应配置备份服务器，按承载、保存数据文件。

6.2 客户端

6.2.1 应支持数据手工或自动发送方式。

6.2.2 应具备数据自动解析并存储至数据库功能。

6.2.3 应只备自动纠错、监控及故障告警等功能。

6.2.4 应具备数据校验、流量控制、查询、统计等功能。

6.3 接口

6.3.1 应支持 Web Service、RESTful 等不同接口接人方式，并支持不同的接口返回方式。

6.3.2 单次请求响应时间应不大于 80ms,支持并发数应不小于 50 个,事务最长处理时间应不大于 200 ms。

6.3.3 接口应保持开放性。在确保安全性的前提下，可通过互联网访问。

7 标准要素数据交换流程

数据交换流程应包括数据准备、数据处理、数据管理及数据共享4个步骤，具体要求如下：

a) 标准数据准备：应对交换所需要的标准收集、整理，按照 T/HBSIA XX 要求的数据结构、数据集等元素描述数据交换内容，按照分类编码规范将数据分类，存储在对应目录；

b) 标准数据处理：应根据交换需求对交换数据进行数据格式的处理，数据格式处理包括标准基础信息和标准指标信息；

c) 标准数据管理：对元数据进行管理；

d) 标准数据交换：应根据数据交换双方约定的方式，采取手动或自动方式进行数据交换。

8 标准要素数据交换方式

8.1 概述

数据交换方式包括：数据库对接、API对接、文件对接等方式。数据库对接适用于结构化数据的共享交换， API对接适用于所有类型数据的共享交换，文件对接适用于非结构化数据和半结构化数据的共交换。

8.2 数据库对接

数据库对接应主要满足以下技术要求：

a) 数字化数据交换原则上应统一采用数据库对接的方式；

b) 数据库对接应支持主流数据库管理系统；

c) 数据提供方应定期更新数据内容，确保共享数据和业务数据的一致性；

d) 数据使用方应通过仅具备读数据权限的业务数据库链接地址、只读用户名/密码获取数据。

8.3 API 对接

API对接方式适用于交换数据的实时调用，应由数据提供方根据数据内容进行API应用程序编程接口封装并提供共享，数据使用方通过访问API取业务系统数据。

宜采用REST形式的服务接口方式，也可采用Web Service或基于消息中间件的服务接口方式。

采用REST形式的服务接口方式时，应支持通过HTTP/HTTPS协议调用服务；服务调用参数和返回数据应采用JSON格式。

采用Web Service或基于消息中间件的服务接口方式时，应有完整、准确、清晰的服务接口调用描 述。

8.4 文件对接

文件格式应遵循以下要求：结构化数据的交换宜采用XML、JSON、CSV或TXT格式，也可使用约定的电子表格文件格式；具体数据字段按照T/HBSIA XX要求。

9 安全技术要求

9.1 系统安全

9.1.1 应支持监测系统态势，实时监控系统访问异常情况、分析系统受攻击的变化趋势。

9.1.2 应具备双活中心或灾备中心，确保系统的安全性和可恢复性。

9.1.3 应基于国家商用密码算法采取加密传输、认证和数据签名校验等安全机制，防止数据在传输过程中被窃取和篡改。

9.2 数据安全

9.2.1 数据管理应采取访问控制、数据隔离、传输安全，存储安全等必要的技术手段，保证数据未向非授权的实体提供或泄露、未被非授权的实体修改或篡改，并保证被授权的实体按要求能够访问和使用数据或资源。

9.2.2 数据应实行分级管理，不同级别的数据采取不同的保护措施。对重要和敏感的数据，应定义为较高的安全管理级别，实行加密存储，边界防护和数据用户鉴权。

9.2.3 在数据交换节点建立连接之前，应对接入用户进行身份认证。

9.2.4 数据交换过程中，应根据数据安全保护级别，利用 CA、加密和加签等技术，保证数据存储、传输处理过程中的安全性和完整性。