Evaluation Warning: The document was created with Spire.Doc for .NET.

# 海东市大数据共享交换平台应用单位

# 接入规范（试行）

一、范围

1. 本要求是根据国家《大数据标准化白皮书(2018版)》建设要求系列之应用单位接入要求编制。

2. 本部分给出了应用单位接入所涉及的技术要求及技术管理要求。内容包括：前置环境配置要求、前置环境设置要求、安全技术要求、前置环境技术管理要求等。

3. 本部分适用于公共信息平台的建立和管理工作。

二、规范性引用文件

下列文件中的条款通过本要求的引用而成为本要求的条款。凡是注有日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB21062.1Y2007\_政务信息资源交换体系第1部分：总体框架； GB21062.2Y2007\_政务信息资源交换体系第2部分：分布式系统间信息交换技术要求；

GB21062.4Y2007\_政务信息资源交换体系第4部分：技术管理要求；

GB/T 7408-1994(EQV ISO 8601:1988)数据元和交换格式信息交换日期和时间表示法；

GB/T 19488.1-2004 电子政务数据元素第1部分：设计和管理规范；

RFC2616-1999 超文本传输协议标准；

本文<技术架构>章节内容引用《GB21062政务信息资源交换体系》第一部分总体框架第四章技术总体架构章节内容。

本文<系统管理架构>章节内容引用《GB21062政务信息资源交换体系》第四部分技术要求第四章技术管理架构章节、第五章职责章节内容。

本文<前置交换模块>章节内容引用《GB21062政务信息资源交换体系》 第二部分技术要求第四章前置交换子系统章节内容。

本文<交换桥接模块>章节内容引用《GB21062政务信息资源交换体系》 第二部分技术要求第四章交换桥接子系统章节内容。

本文<交换传输模块>章节内容引用《GB21062政务信息资源交换体系》 第二部分技术要求第四章交换传输子系统章节内容。

本文<交换管理模块>章节内容引用《GB21062政务信息资源交换体系》 第二部分技术要求第四章交换管理子系统章节内容。

三、术语与定义

GB/T 19710-2005 中规定的与以下术语和定义适用于本部分。

1. 数据交换管理者：管理信息资源结点的机构。

2. 交换内容提供者：提供信息资源交换内容的机构。

3. 交换内容使用者：使用信息资源交换内容的机构。

4. 前置环境：应用单位接入端系统软硬件及相关网络环境组成的应用单位前置系统的单元环境。

5. 目录交换：按订阅模式进行目录资源数据的交换。

6. 桥接系统：业务数据库与共享数据库的桥接器，保持交换数据库与共享数据库的同步。

7. 变更捕捉：捕捉数据资源变更情况。

8. 数据转入：以固定间隔时间轮询变更登记表，读取其中的记录，并将这些记录以约定的格式组成XML报文，存储到共享库的换出表中。

非结构化数据文件直接通过文件服务传输至交换中心文件服务器，并由中心分发非结构化数据文件。

9. 数据交换路由：以固定时间间隔轮询应用单位换入表，拆解XML报文，根据目标库自动分拣；

非结构化数据文件直接通过文件服务传输至交换中心文件服务器，并有中心分发非结构化数据文件。

10. 数据转出：独立运行的进程以固定间隔时间轮询交换库中的换入表，读取其中的XML报文，并将数据按定制的格式同步到共享库中；

非结构化数据文件描述信息存储在信息队列中，由各服务器根据队列信息分别从中心文件服务器获取所需数据文件。

11. 交换管理程序：完成数据交换审批流程、交换监控、交换调度、系统管理等功能一套程序，部署于中心。

12. Web 服务：基于web service的服务接口，采用约定的XML作为交易数据接口，分为服务端服务接口和客户端调用。

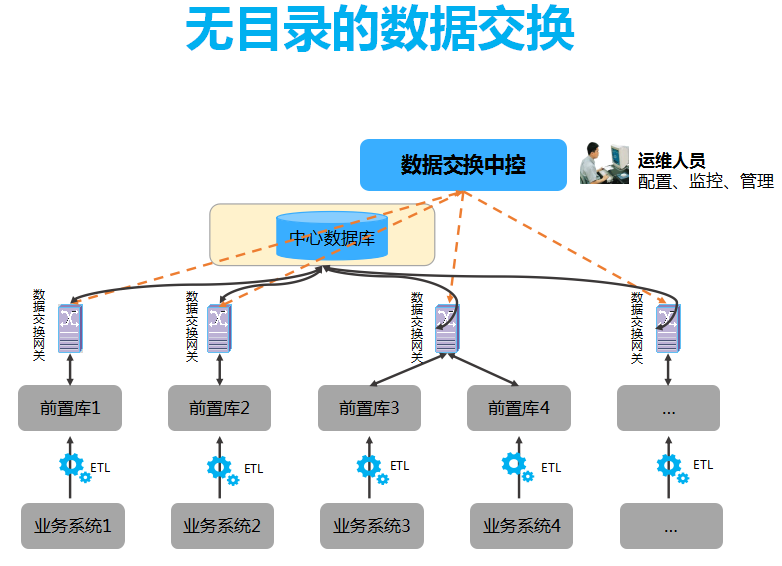
13. 访问认证：公共信息平台提供用户认证服务，由托管应用系统的客户端调用，用于验证用户是否合法。

14. 应用单位：接入公共信息平台的机构单位。

15. 主管单位：公共信息平台的管理单位。

16. 数据中心：公共信息平台的组成部分，用于信息资源的存储。

四、前置环境



五、系统组成

前置系统由目录服务系统、交换服务系统、系统软件（数

据库、交换中间件、安全软件、操作系统）、系统硬件及相关网络环境构成。

系统硬件及相关网络环境主要为构建整个前置环境总集的基础，支撑软件系统正常、可靠运行。

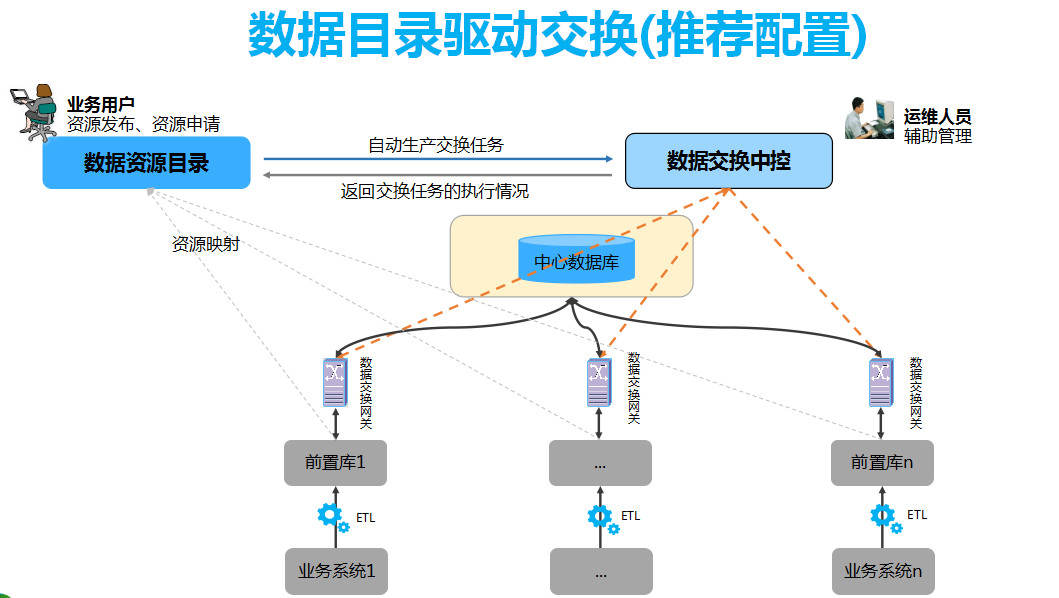
系统软件中操作系统是基础，数据库主要是支撑组织和存储数据的工具，安全软件是数据和系统软件的安全保障。

交换服务系统中桥接系统是将应用单位内部数据传输至前置环境内的“桥梁”。通过桥接系统传输数据可将前置机与应用单位业务系统之间隔离，保证应用单位业务系统与公共信息平台各自的独立性。

目录服务系统则将各项资源整理后进行编目，通过一系列审批流程后，该部分目录可通过中心数据服务向外部提供目录和数据资源访问服务。

**1. 前置目录服务**

前置系统目录管理功能示意图如下：



（1）承担共享信息生成、发布及访问功能

共享信息资源生成：将各应用单位业务信息资源生成本单位用于共享的信息资源，将其放在前置系统中；

共享信息资源发布：发布基于统一的网络为主的共享信息资源；

共享信息资源访问：提供共享信息资源访问服务，用户可以浏览、查询、下载共享信息，并且基于统一的网络进行共享信息资源共享。

（2）承担公共信息目录管理功能

公共信息资源目录管理实现对汇聚到公共资源交易中心的目录内容进行自动审核和其它相关的管理工作。目录管理功能包括：

审核功能：按照国家相关标准（或建议标准），对目录信息内容进行自动形式审核，符合标准的目录信息内容自动进入目录信息内容服务信息库，并按照标准要求自动发布。未通过形式审核的目录信息内容，自动回退到相关应用单位，经形式修正后重新进入审核流程；

维护功能：对目录内容管理信息库、目录内容服务信息库中的目录内容提供维护功能；

标识符前段码管理：按照国家相关标准（或建议标准），提供前段码分配管理功能，为各应用单位分配并维护固定的前段码；

目录服务地址管理：存储公共资源交易中心的目录服务地址，用于公共资源交易中心之间的互连互通；

监控功能：监控系统的运行状态。

（3）数据目录交换服务

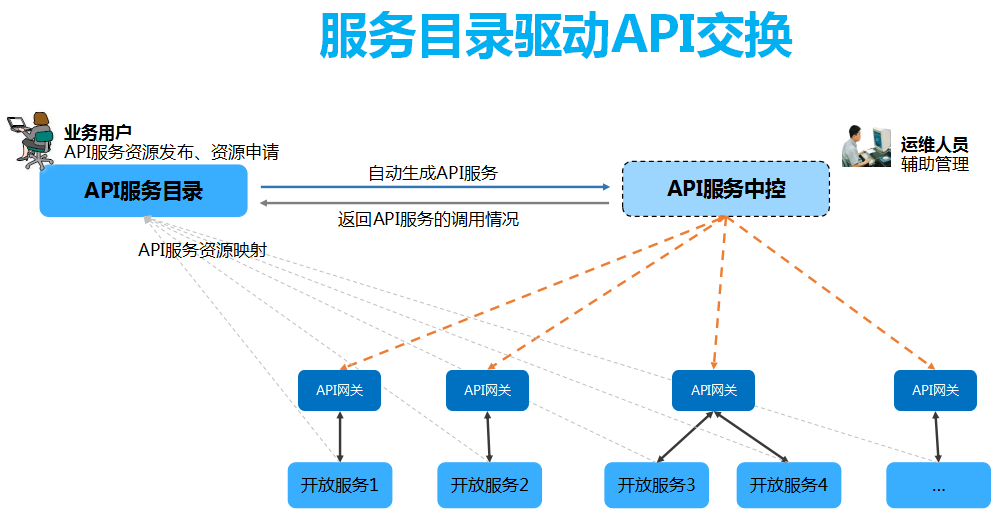
基于云上海东实现对共享交换目录内容的发布，并向用户提供公共信息目录内容的查询服务。公共信息目录服务功能包括：

目录内容发布：提供目录服务接口，实现以下功能:查询请求解析；向目录内容信息库发出目录检索查询请求；按相关标准规范要求，封装返回的查询结果，并返回给查询请求者。

目录内容查询：为了便于人机交互，需要提供基于网络的目录内容查询功能：分类导航；单个检索词的检索；多个检索词的组合检索。

**2. API服务目录交换服务**

前置系统中交换服务分为两部分：桥接系统和交换系统。

前置系统中的桥接系统用来实现应用单位业务信息库与交换信息库、共享信息库与交换信息库之间的信息同步。桥接系统可采用服务目录驱动API交换，服务目录驱动API交换示意如图所示：

桥接系统可由桥接服务运行环境、桥接配置工具、桥接管理、应用适配器等部分组成。桥接服务是利用桥接服务配置工具，组装应用适配器组件，以完成一个应用单位数据采集并存储至交换共享库的服务程序。桥接服务运行环境须提供日志管理、安全管理、适配器管理等基本功能。主要功能包括：

（1）支持两个桥接对象之间的信息同步，即支持应用单位业务信息库或共享信息库与交换信息库之间的信息同步；

（2）支持各种主流操作系统；

（3）支持国内外主流数据库；

（4）支持结构化文件、非结构化文件；

（5）采用适配器组件访问桥接对象，实现数据的获取与存储；

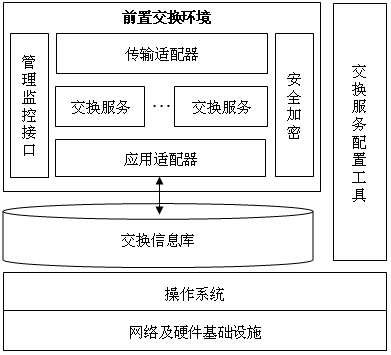
（6）提供增量数据自动识别的功能，在不修改业务信息库结构的情况下，系统能够自动识别出需要交换的信息，包括新增、被修改或被删除的信息；

（7）提供图形化的信息交换桥接配置及管理工具，支持桥接指标定义、处理、桥接管理等功能；

（8）支持多个桥接任务或服务的同时运行，支持桥接服务的动态和远程部署；

（9）提供系统管理与监控、日志管理功能。

前置系统中的交换系统的逻辑结构由网络通信系统、操作系统、交换信息库、前置交换环境、提供交换服务配置工具等组成。交换系统的基本结构如图所示：



交换系统是交换域的边界，实现交换域与应用单位业务系统的隔离。前置交换环境由传输适配器、管理监控接口、安全加密模块等部分组成，是交换服务的运行容器。安全加密服务提供基本的数据加密功能，保证信息传输过程中的安全。交换前置环境提供管理监控接口，交换管理监控子系统通过管理监控接口对交换前置环境进行监控。前置交换功能包含：

（1）支持交换信息库与交换传输子系统间的信息交换。交换传输子系统能够从交换信息库中提取数据交给交换传输子系统传递，也能够从交换传输子系统中获取数据存储到交换信息库；

（2）支持各种主流操作系统；

（3）支持国内外主流数据库；

（4）采用传输适配器接入到交换传输子系统；

（5）采用适配器访问交换信息库，实现对交换信息库中数据的获取与存储；

（6）提供图形化的交换服务配置工具，配置、测试、部署交换服务，提供远程部署功能；

（7）支持多个交换服务并发运行；

（8）提供管理与监控接口，支持远程管理与监控的功能。

**3. 前置环境配置**

前置环境系统的硬件、软件、数据库系统、操作系统及相关系统软件的配置要求及性能要求。

本要求所指前置环境包括系统硬件、系统软件等。

（1）系统硬件

前置交换机、前置路由器、前置防火墙、前置服务器、前置存储。

（2）系统软件

操作系统、数据库、消息中间件（可选）、杀毒软件、桥接软件、目录系统软件。

### （3）迁云用户资源调查表

注：此表为参考模板，迁云部门可根据自己的业务类型及业务范围及平台规模提交资源需求表

|  |  |  |
| --- | --- | --- |
| **1、系统硬件** | 前置  交换机 | 快速以太网交换机 ；内存 16MB DRAM 和 8MB 闪存 ；传输速率 10Mbps/100Mbps ； 网络标准 IEEE 802.1x、IEEE 802.3x、IEEE 802.1D、IEEE 802.1p CoS、IEEE 802.1Q、IEEE 802.3ab、IEEE 802.3u、IEEE802.3 ；端口数量 24 ；接口介质 10/100Base-T ； 传输模式 支持全双工。 |
| 前置  路由器 | 模块化接入路由器；固定的广域网接口：2 个集成的 WIC 插槽；固定的局域网接口：2 个 10/100FE 端口；其他端口： 控制台端口（最高可达 115.2kbps）；辅助端口（最 高可达 115.2kbps）；1 个网络模块（NM）插槽；板载 AIM（内部）1 个插槽；处理器：40MHz CPU，性能 20Kpps；内存 16MB 闪存，最大 48MB；系统内存 32MB，最大128MB 。 |
| 前置  防火墙 | 体系结构：硬件、内核检测防火墙；管理方式：支持 GUI 或基于 SSL 的管理，可进行可信登录点管理；运行模式：支持路由、交换、混合、NAT、VlanTrunk 三种模式；吞吐量：不低于 400M bps；端口：至少 4 个 10/100Base-TX 自适应以太网口；并发连接数：不低于 80 万；VPN 支持：支持网关对网关，移动客户端对网关建立 VPN加密隧道；支持源目的地址过滤、源目的端口过滤，协议过滤（TCP/UDP/ICMP）、接口过滤、时间过滤、方向过滤，实现全状态包过滤；支持完整的 HTTP 代理、邮件代理、FTP 代理、Telnet 代理；支持静态、动态、端口映射、双向网络地址转换；支持 FTP、TFTP、DNS、ORACLE 访问、RTSP、H.323、RPC 等应用的动态端口按需打开；支持 IP/MAC 绑定，还可自动收集 IP/MAC 信息；策略机制：基于策略树的梯度过滤机制，将攻击检测、报文分拣、IP过滤、连接状态监控、用户认证、应用协议 报文分析、应用协议通信状态检查、内容安全检查等内容构建成一个力度递增的过滤体系；具有 B1 安全级别的安全操作系统；支持网关对网关，移动客户端对网关建立 VPN 加密隧道；支持 IPSec；支持 DES、3DES、硬件加密算法 SSF33；支持HMAC-MD5,HMAC-SHA1；支持 Okaley 群：默认1536bitMODP 群另支持768bit，1024bit的MODP群；支持NAT，IP压缩等技术。 |
| 前置  服务器 | 支持各种操作系统、主流数据库系统环境；1 个双核，1.6 GHz （含）以上处理器，支持 2 个 CPU；2GB内存DDRII；2 个146GB SAS 10K 热插拔硬盘, 最大可支持10块； 磁盘阵列卡嵌入式 SATA RAID 控制器；IDE 控制器 Ultra ATA 100；最大热插拔硬盘数支持热插拔。 |
| 前置存储（可选） |  |
| **2、系统软件** | 操作系统 | Windows2012server 或以上/Linux/Unix |
| 数据库 | 主流高版本数据库 |
| 消息中间件（可选） |  |
| 杀毒软件 | 利用现有的杀毒软件客户端 |
| **3、桥接软件** |  | 统一开发、安装桥接软件 |
| **4、目录系统软件** |  | 统一安装目录系统软件 |

(4)其他要求

前置网络设备：统一按区域网络要求进行配置。

前置服务器：内部网卡配置成应用单位内网地址、外部网卡配置网络分配地址；系统盘与数据盘分开，硬盘采用镜像配置；

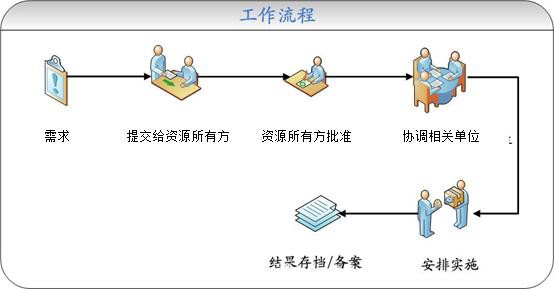
数据库：其库表应包括三大类：系统表、共享信息库表、数据交换表。其中系统表的命名根据系统要求，数据交换表由交换系统自动生成。

（5）注意事项

由应用单位自行安排安装防病毒软件，并建立相应的病毒库更新工作机制；

对前置服务器的各项操作进行严格管理，要求：不得随意修改操作系统或数据库系统的用户密码，不得随意增加操作系统或数据库用户；不得随意安装或卸载各类软件，不得随意删除任何文件，不得对文件进行更名或移动；不得随意对数据库系统进行表空间增删、数据文件增删等操作；不对随意修改数据库系统的数据结构，包括增删或修改表、字段、存储过程、触发器等；除了桥接程序、交换服务系统、共享服务系统、目录服务系统、服务应用接口程序外，其它任何程序都不得对数据库系统进行访问等操作；其它可能影响到前置服务器正常运行的任何操作。

确实出于各种需求，需要进行上述操作的，必须报主管单位批准，协调各方进行配合，由主管单位统一安排实施，流程如下：



六、前置环境管理

**1. 角色**

前置系统管理涉及的管理角色有提供者、使用者和管理者。提供者、使用者负责前置交换子系统的基本运行管理，管理者负责前置交换环境的日常监控与管理。

**2. 提供者管理要求**

提供者对前置系统环境的管理要点应包括：

（1）提供者应配合管理者建设前置系统环境；

（2）提供者应配合管理者确定共享信息指标，确定共享信息库信息表的结构；

（3）提供者应负责前置系统环境基本管理，负责网络与硬件环境、操作系统、共享信息库的数据库系统的稳定运行，前置系统能够不间断运行；

（4）提供者应负责共享信息库的运行维护，负责共享信息库数据表的数据备份与清理。

**3. 使用者管理要求**

使用者对前置系统的管理要点应包括：

（1）使用者应配合管理者建设前置系统环境；

（2）使用者应配合管理者确定共享信息指标，确定共享信息库信息表的结构；

（3）使用者应负责前置系统环境基本管理，负责网络与硬件环境、操作系统、交换信息库的数据库系统的稳定运行，前置系统能够不间断运行；

（4）使用者应负责共享信息库的运行维护，负责共享信息库数据表的数据备份与清理。

**4. 管理者管理要求**

管理者对前置系统的管理要点应包括：

（1）管理者应负责建设前置系统；

（2）管理者应负责协调并明确共享信息指标；

（3）管理者应根据共享信息指标规范与共享信息内容、共享信息流程的要求，配置与部署共享服务，实现共享信息库之间的信息交换；

（4）管理者应负责前置系统的前置运行环境监控与管理，保证前置系运行环境与共享服务的稳定运行。

七、数据安全

1. 各委办局的接入数据清洗工作由各单位自行负责，云提供商和大数据服务中心不负责接入数据的清洗工作。

2. 各委办局的信息维护工作需自行承担，数据冗余及灾备工作由云提供商负责，具体事项可用书面协议的形式进行规范约束。