ICS 35.100.05
L 79

DB3502/T

福 建 省 厦 门 市 地 方 标 准

DB 3502/T XXXX—XXXX

国际贸易"单一窗口"数据开放服务 第1部分：总体技术要求

Open data services of international trade Single Window—
Part 1:General technical requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2023－XX－XX 发布　　2023－XX－XX 实施

厦门市市场监督管理局　　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DB3502/T XXX《国际贸易“单一窗口”数据开放服务》的第1部分。DB3502/T XXX已经发布了以下部分：

——第 1 部分：总体技术要求；

——第 2 部分：报关业务数据元规范；

——第 3 部分：报关业务服务接口规范。

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××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

引　言

国际贸易“单一窗口”数据开放服务平台的建设，可以充分发掘数据资产价值，提升厦门“单一窗口”创新服务效率，优化厦门市营商环境，积极服务“单一窗口”相关企业。DB3502/T XXX旨在确立数据开放服务平台总体架构、技术架构、开放过程等的技术标准，为数据开放服务平台的建设提供基础规范，拟由十七个部分组成。

——第 1 部分：总体技术要求；
——第 2 部分：报关业务元数据标准规范；
——第 3 部分：报关业务服务接口规范；
——第 4 部分：运输工具元数据标准规范；
——第 5 部分：运输工具服务接口规范；
——第 6 部分：舱单业务元数据标准规范；
——第 7 部分：舱单业务服务接口规范；
——第 8 部分：跨境电商元数据标准规范；
——第 9 部分：跨境电商服务接口规范；
——第 10 部分：快递件业务元数据标准规范；
——第 11 部分：快递件业务服务接口规范；
——第 12 部分：保税业务元数据标准规范；
——第 13 部分：保税业务服务接口规范；
——第 14 部分：服务目录标准规范；
——第 15 部分：安全管理标准规范；
——第 16 部分：数据服务流程标准规范；
——第 17 部分：运维服务标准规范。

国际贸易"单一窗口"数据开放服务 第1部分：总体技术要求

1 范围

本文件规定了国际贸易“单一窗口”数据开放服务平台的总体架构、技术架构、外部连接关系、数据开放、安全要求以及运维要求等。

本文件适用于国际贸易“单一窗口”数据开放服务平台的设计、建设及运维工作，数据共享交互、服务对接工作可参照使用。

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 5271.17－2010 信息技术词汇 第17部分：数据库

GB/T 9361 计算机场地安全要求

GB/T 22239－2019 信息安全技术网络安全等级保护基本要求

GB/T 22240－2020 信息安全技术 网络安全等级保护定级指南

GB/T 28827.1－2022 信息技术服务 运行维护 第1部分：通用要求

GB/T 28827.3－2012 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 28827.4－2019 信息技术服务 运行维护 第4部分：数据中心服务要求

GB/T 28827.6－2019 信息技术服务 运行维护 第6部分：应用系统服务要求

GB/T 29262－2012 信息技术 面向服务的体系结构（SOA） 术语

GB/T 29263－2012 信息技术 面向服务的体系结构（SOA）应用的总体技术要求

GB/T 35273－2020 信息安全技术 个人信息安全规范

GB/T 35295－2017 信息技术 大数据 术语

GB/T 36597－2018 建立国际贸易单一窗口指南

GB/T 37973－2019 信息安全技术 大数据安全管理指南

GB/T 37988－2019 信息安全技术 数据安全能力成熟度模型

GB/T 39477－2020 信息安全技术 政务信息共享 数据安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

单一窗口 single window

贸易和运输相关各方在单一登记点提交满足全部进口、出口和转口相关监管规定的标准信息和单证的一项措施。

[来源：GB/T 36597－2018，2.1]

3.2

数据开放服务平台 open data service platform

提供数据服务访问、监控、服务注册的平台。

3.3

数据服务 data service

提供数据采集、数据传输、数据存储、数据处理（包括计算、分析、可视化等）、数据交换、数据销毁等数据各种生存形态演变的一种信息技术驱动的服务。

3.4

数据集 dataset

数据记录汇聚的数据形式。

[来源：GB/T 35295－2017，2.1.45]

3.5

元数据 metadata

关于数据或数据元素的数据（可能包括其数据描述），以及关于数据拥有权、存储路径、访问权和数据易变性的数据。

[来源：GB/T 5271.17－2010，17.06.05]

3.6

开放数据 open data

可为其他数据使用的数据。

[来源：GB/T 35295－2017，2.1.44]

3.7

角色 role

与用户的访问控制权限有关的安全属性。一个角色可能有一种或几种服务有关，一个角色可能对应着一个或多个用户，一个用户可能承担着一种或多种角色。本文件中指参与数据开放管理过程的相关主体。

3.8

服务目录 service catalog；SC

记录服务提供者所提供服务的全部种类以及服务目标情况，为选择服务、检索服务提供支撑的列表。

[来源：GB/T 29262－2012，2.12]

3.9

微服务 microservices

面向服务的体系结构架构样式的一种软件开发技术。

3.10

数据服务提供方 data provider

基于数据开放服务平台，采用服务接口方式提供数据服务的部门。

3.11

数据服务接收方 data receiver

基于数据开放服务平台，采用服务接口使用数据的企业或服务单位。

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）

BaaS：区块链即服务（Blockchain as a Service）
CA：证书认证机构（Certification Authority）
DaaS：数据即服务(Data as a Service)
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
SOA：面向服务架构（Service Oriented Architecture）

5 总体架构

在 “单一窗口”平台框架下，数据开放服务平台支持企业和第三方平台、政府部门、服务单位等外部系统依据相关接口标准通过相关服务接口接入数据开放服务平台，实现与 “单一窗口”平台对接。数据开放服务平台总体架构见图1所示，具体说明如下：

——基础设施层：提供数据开放服务相关的基础设施，包括软件、硬件、操作系统、网络等设施，并提供软件部署所需的数据库服务器、应用服务器、中间件等基础环境；

——技术支撑层：大数据基础平台对数据进行基础管理整合后，在数据开放平台注册服务接口，通过数据交换平台与数据开放服务平台进行数据交换；

——应用层：注册的数据服务经过审核后，由数据开放服务平台进行发布，提供给数据服务接收方使用，主要应用包括报关业务、运输工具、舱单业务、跨境电商、快递件业务、保税业务等；

——门户层：提供对门户的管理，包括服务门户及管理门户，服务门户是提供对外服务的门户，管理门户是对所有对外提供的服务进行管理；

——用户接入层：用户通过 PC 端、移动端（APP/小程序）、第三方接入等方式，遵循 CA 形式，访问数据开放服务平台调用服务获取数据；

——法律法规及标准规范体系：以国际贸易、信息化、单一窗口相关法律法规和标准规范构成数据开放服务平台的建设依据；

——运维管理及安全保障体系：由数据开放服务平台相关的运行服务、服务流程、运维服务及安全管理等构成。

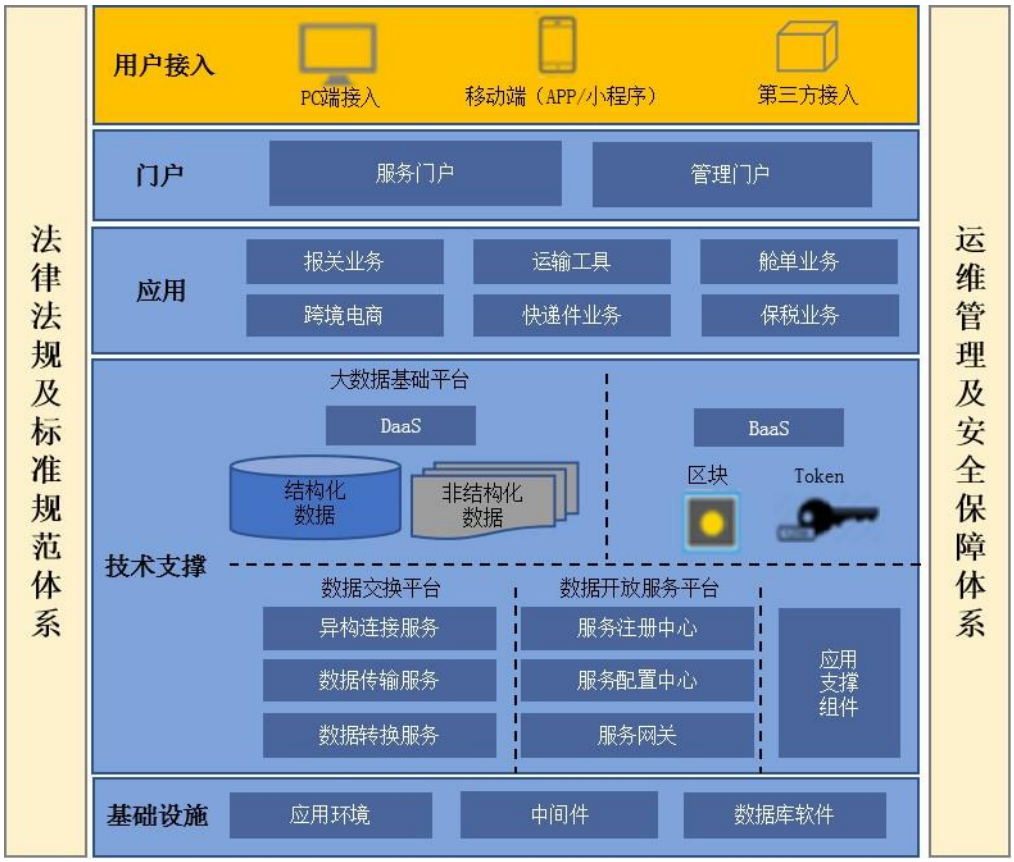

图1　数据开放服务平台总体架构

6　技术架构

数据开放服务平台以GB/T 29263－2012的架构要求为基础，采用微服务技术架构，提供数据开放服务集成框架，提供微服务运行依赖的服务组件如注册中心、配置中心、API网关等，实现服务鉴权、数据缓存、流量控制、日志记录、熔断控制、协议转换、认证授权、定时任务等功能。数据开放服务平台微服务架构见图2。

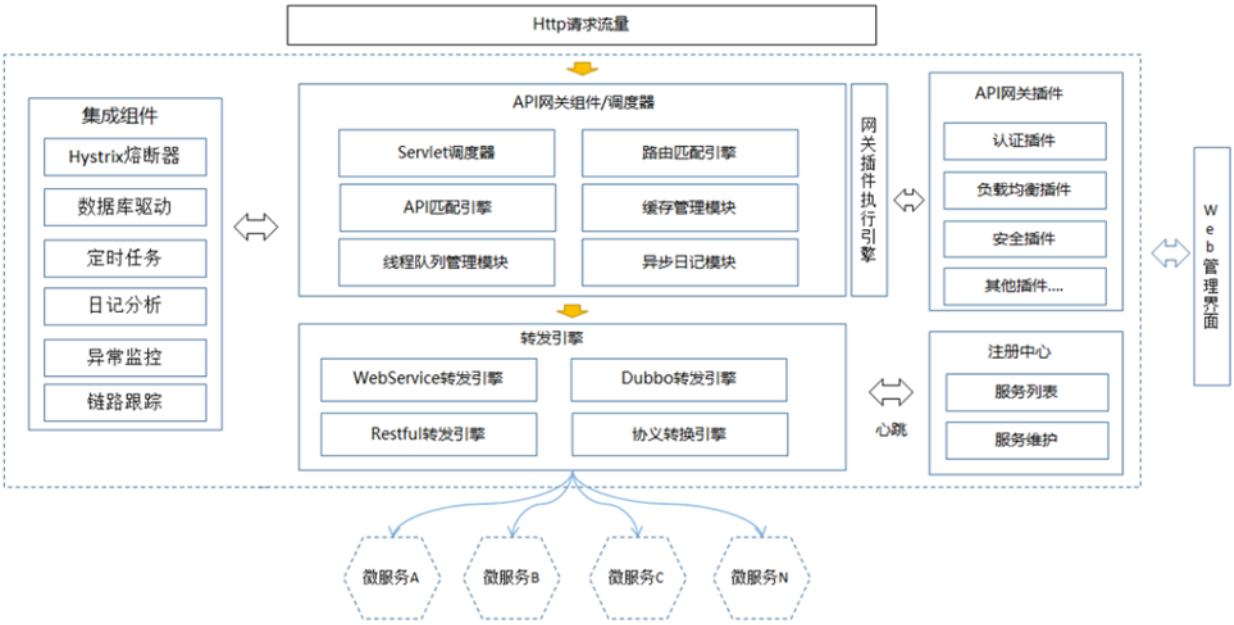

图2　数据开放服务平台微服务架构

7　外部连接关系

数据开放服务平台与大数据基础平台、数字口岸平台、外围系统连接关系见图3，具体说明如下：

——外围系统向大数据基础平台和数字口岸平台提供规范数据；

——大数据基础平台具备数据量管理、数据存储管理、数据资源目录以及数据分级分类等功能，为“单一窗口”数据开放服务平台提供数据支撑；

——“单一窗口”数据开放服务平台通过数据服务接口以数据交换的形式获取大数据基础平台和数字口岸平台的数据服务；

——数字口岸平台和大数据基础平台作为“单一窗口”数据开放服务平台数据服务提供方，相关数据服务接口注册到“单一窗口”数据开放服务平台，“单一窗口”数据开放服务平台对注册的服务进行审核、评估和测试，数据服务应满足相关业务需求以及数据服务安全、性能需求；

——数据服务接收方通过“单一窗口”数据开放服务平台检索和调用服务，并获取数据。

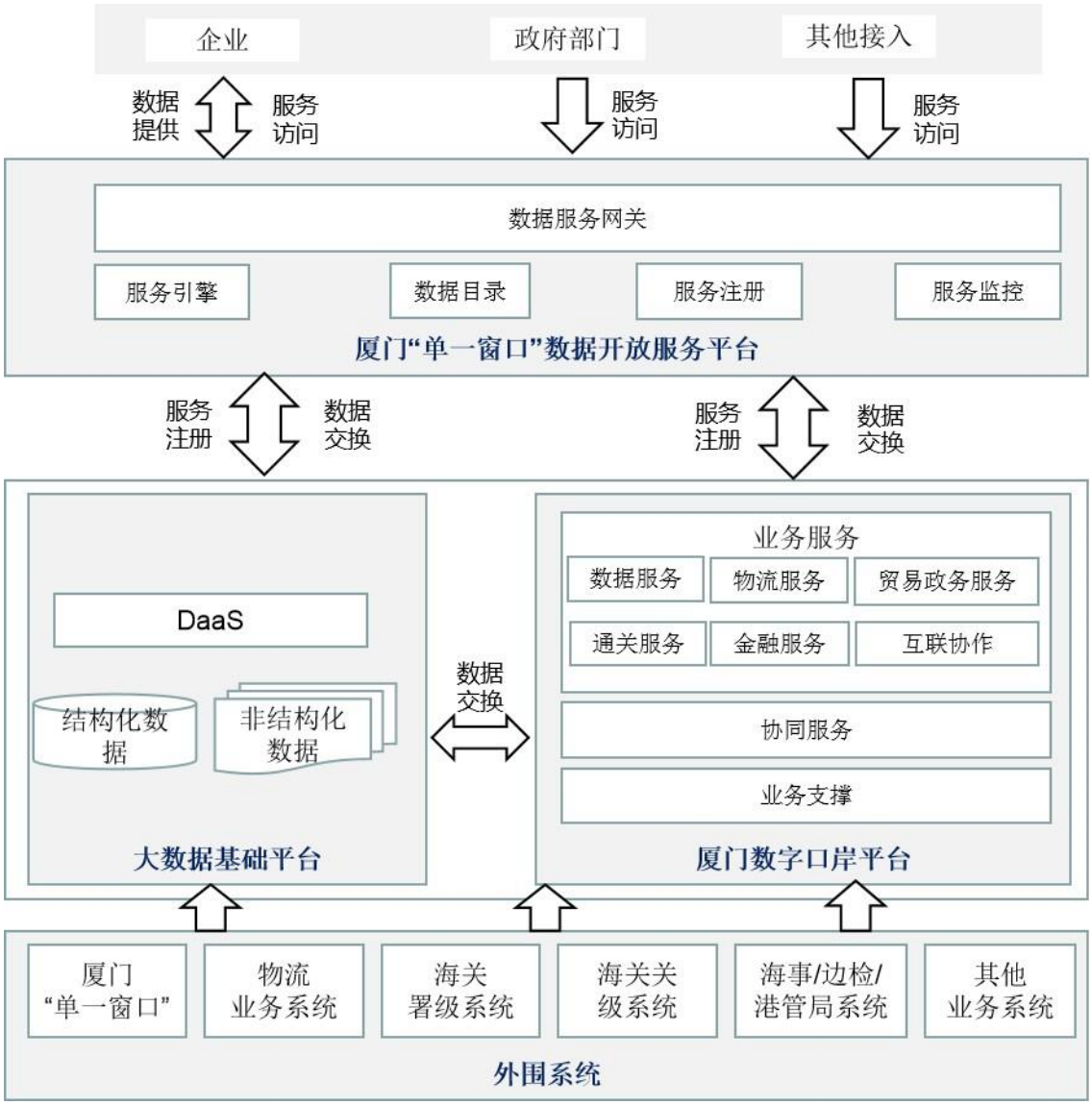

图3　外部连接关系

8　数据开放

8.1　角色与职责

“单一窗口”数据开放服务化流程中，“单一窗口”平台作为数据服务提供方，数据开放服务平台作为数据开放服务的管理者，企业、政府部门、第三方作为数据服务接收方。数据开放服务角色与职责见图4，具体说明如下：

——数据服务提供方：对数据资源目录进行整理，对接数据源并按需采集，形成元数据信息，遵循安全规范，根据需要进行数据脱敏配置元数据，遵照数据服务分类，将元数据信息映射、发布为业务数据实体；

——数据开放管理者：提供统一的数据开放服务管理中心，支持各种数据开放服务的注册、发布、关联、配置等管理，支持对数据服务权限的配置与管理；

——数据服务接收方：数据服务接收方根据数据服务需求向数据服务提供方进行服务申请，数据服务提供方应进行服务授权并提供权限范围内的数据浏览、查看和使用。

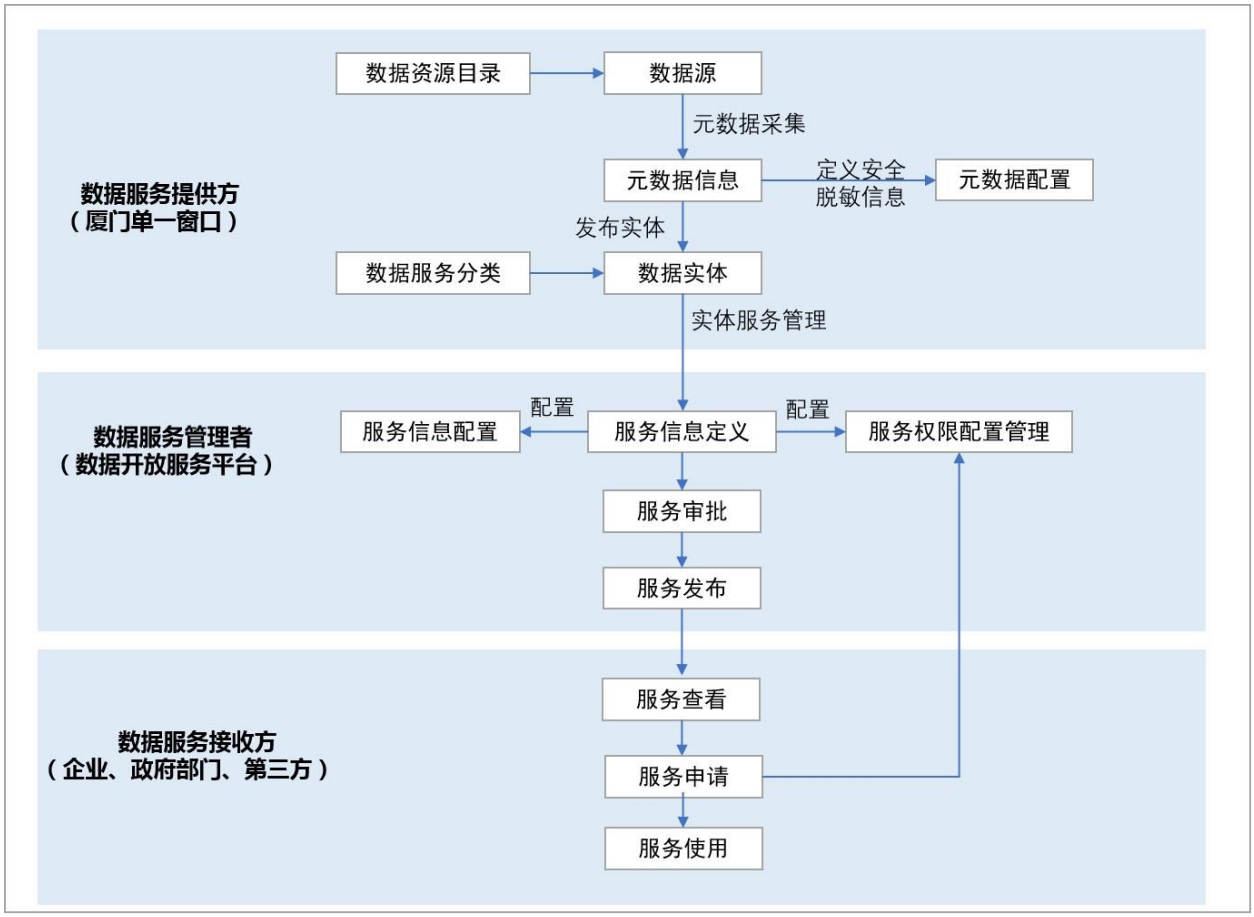

图4　角色与职责

8.2　开放过程

建立标准的、实时数据开放服务平台，对“单一窗口”数据资源实现数据资源目录化，通过数据开放服务平台协助企业进行自助式开发，同时提供数据服务的运营和监控。数据开放核心流程见图5，具体要求如下：

a)　数据目录化：

1)　确定数据开放范围和制定数据开放计划。对开放数据进行标准化处理，包括进行开放数据资源的汇聚、整合、清洗、格式化、安全及隐私保护、质量控制等工作，并按相关规定进行数据脱敏；

2)　根据相关规定编制开放数据目录，实现数据资源目录化，形成“单一窗口”开放数据资源目录，梳理“单一窗口”相关业务源数据、并将要开放的数据资源推送到数据交换区、数据开放区，形成数据目录。

b)　目录服务化：注册开放数据服务，将数据服务接口注册到数据开放服务平台，进行数据服务开发，将数据开放区的数据资源通过数据服务装配和开发，形成具体的数据服务，如实时数据服务、批量数据服务等；

c)　数据开放化：

1） 形成服务 API，企业根据应用需求通过数据开放服务平台向“单一窗口”平台提出数据开放申请；
2） 数据开放服务平台受理申请开展评估并进行结果反馈，同意开放的给企业进行授权，与企业签署数据使用授权协议；
3） 企业获取开放数据、反馈开放数据应用成果，通过数据服务申请审批及数据服务运维监控等形成数据服务开放化。

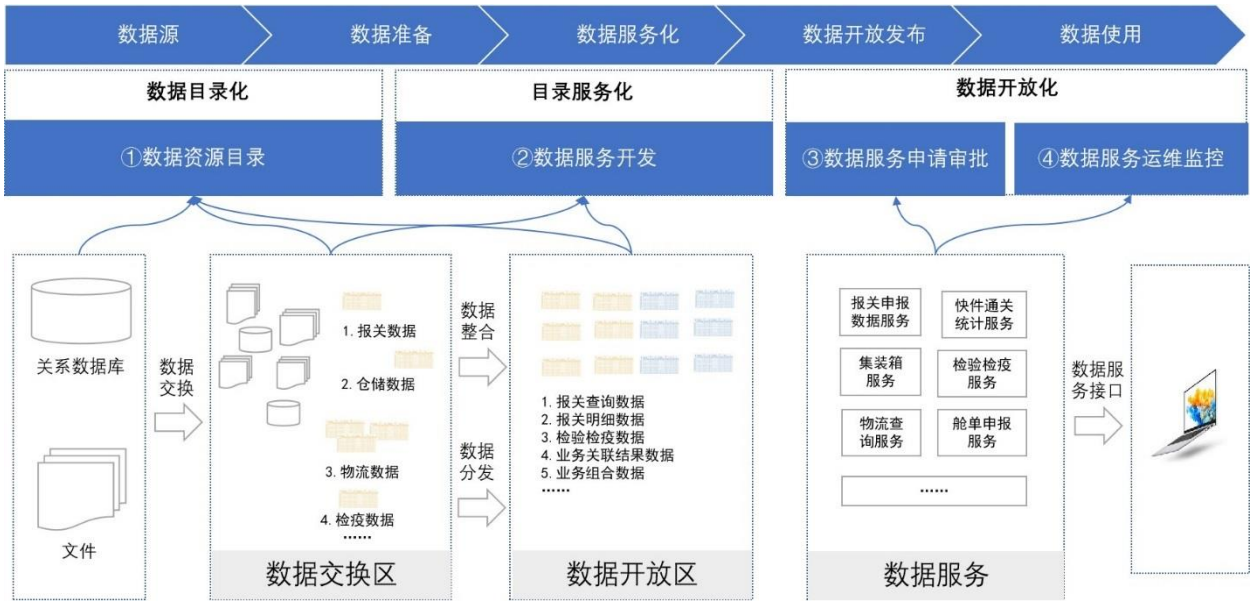

图5 数据开放核心流程

8.3 核心功能

8.3.1 数据资源中心

“单一窗口”依据相关的对接标准规范及数据开放标准规范采集数据资源元数据信息，数据开放服务平台基于元数据驱动实现数据库资源采集、预览，将数据资源按照分类、主题、应用等多个层次对数据进行分类管理、识别、定位和共享，通过数据资源中心串联企业和“单一窗口”数据开放服务平台。数据资源中心系统全局数据视图见图6，应具备以下能力：

——通过数据目录名称、标签、关键字、部门、主题等要素设置快速检索通道；
——提供开放数据资源的来源部门、数据量、所属主题、更新频率、发布时间、最后更新时间、条件开放、标签、数据简介，数据集的数据字段名称、数据字段长度、类型格式等元数据信息，企业用户能够了解开放的数据资源信息。

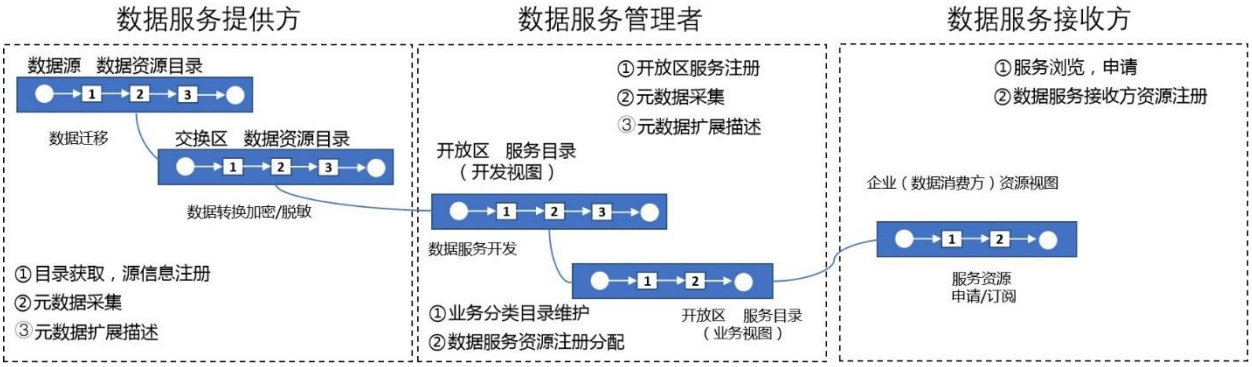

图6 数据资源中心全局数据视图

8.3.2 服务目录中心

数据开放服务中服务项目及服务级别应从用户角度进行描述，数据服务管理者在开放区以开发视图形式进行开发形成服务目录，数据服务接收方在开放区通过业务视图形式，在服务目录中选取所需的服务接口。数据服务提供方将数据服务接口发布在数据开放服务平台。服务目录中心为数据服务接收方提供相关开放数据资源访问的服务接口，数据服务接收方需要获取某一具体数据值时，通过数据开放服务平台获取相应的数据权限后，访问数据开放服务平台进行接口调用。

服务目录中心应具备以下服务能力：

——支持将数据一键/便携化发布为 API 服务；

——支持结构化数据、非结构化数据、半结构化数据的开放发布；

——支持结果集等形式的实时接口服务发布；

——支持批量数据发布；

——支持发布订阅等多种服务提供模式。

8.3.3 开发者中心

开发者中心为开发者在数据开放服务平台提供接口开发、服务接入、服务管理、数据管理、实施推广等全流程服务。开发者中心通过建立业务部门、企业、“单一窗口”平台联动机制，提供数据开放应用的互动社区，开展数据开放前的咨询服务、开放中的技术服务、开放后的跟踪服务。

8.3.4 数据网关

通过数据开放服务平台的数据网关对单一窗口中所有开放的接口进行统一管理与监控，数据网关提供基础组件、统一API接入、统一API可视监控、统一API安全管控、统一服务管控编排功能，提供认证、鉴权、缓存、流量管控、超时处理、协议转换、服务编排等多种管控能力，构建企业与厦门“单一窗口”数据开放共享链路。

9 安全要求

9.1 安全总则

系统安全应满足下列要求：

——应建立完善的安全管理制度；

——应建立安全管理保障体系，实现物理安全、网络安全、数据安全、运行安全等；

——系统建设完成后应进行系统安全评估，包括但不限于硬件安全评估、软件安全评估和数据安全评估等，宜委托专业评估公司进行系统安全评估并出具系统安全评估报告；
——建立对数据开放的处理机制，数据在“单一窗口”平台统一管理，作为企业开放上报、使用数据的专属交换空间，该开放区为企业提供数据出口通道，管理端通过安全管控措施审计企业用户使用情况；
——应建立开放数据访问分级分类的机制，对企业访问及使用自身数据、访问“单一窗口”平台数据、访问其他企业数据时，针对数据的不同级别采用相应的访问策略，对敏感、非敏感数据进行分类处理；
——应建立数据全生命周期的数据安全保障体系，从数据采集、数据存储、数据传输、数据交换、数据授权使用、数据销毁安全等过程提供相应技术和管理措施；
——应保证隐私信息不发生泄露，个人信息安全应遵循 GB/T 35273 中的相关规定；
——数据开放服务平台按 GB/T 22240 的规定确定安全保护等级，安全等级保护要求不低于 GB/T 22239 规定的二级要求；
——依据数据开发服务平台安全需求并根据 GB/T 22239 要求，对开发及部署的产品健全安全制度，提升系统和数据抗风险的能力，提高数据安全性和保障应用系统的连续性。

9.2 物理安全

物理安全应满足下列要求：
——计算机房的安全应符合 GB/T 9361 的规定；
——系统使用的硬件设备应采取防盗、防毁、电源保护等安全保护措施，包括但不限于应用服务器、数据库服务器、网络设备、存储设备等，并控制机房的访问权限；
——确保数据中心安全性，包括物理访问控制、监控和报警系统、灾难恢复计划等，防止数据丢失、损坏或被盗。

9.3 网络安全

网络安全应满足下列要求：
——根据数据开放服务平台的安全设置配置方案，设计及实现过程应满足 GB/T 22239 中二级安全等级的相应要求；
——网络应采用有效的安全保障手段进行安全保护，包括但不限于数据加密、防火墙、安全网关、安全路由器、远程访问控制、入侵检测、病毒防护、网络监测、漏洞扫描、恶意代码检测与防范等；
——采用 SM2/SM4 等国密的加解密技术对数据进行相应的处理；
——网络工作人员应通过数据、软件、硬件等网络安全考核并定期进行相关培训。

9.4 数据安全

数据安全应满足下列要求：
——采用 SM2/SM4 等国密的加密解密方案；
——应对数据采取脱敏等安全保护措施；
——应制定系统设计、实现、使用及管理等各个阶段的数据安全策略；
——公共数据开放前应依照相关法律法规进行数据安全审查，未经数据安全审查的数据不应对外开放；
——宜采用具有安全功能的国产化操作系统和数据库系统。

9.5 应用安全

应用安全应满足下列要求：

——应构建统一身份认证管理系统提供用户身份鉴别功能，对系统使用人员进行统一身份认证，使用用户名、密码等身份认证方式，附加随机验证码校验；

——应对用户权限进行访问控制；

——应具备应用级别权限控制，提供基于个人、单位、部门、群组、角色、岗位、级别等多维度权限控制；

——应实现权限分散管理，按照功能和数据分别进行授权管理。

9.6 分级分类机制

9.6.1 数据分级

将数据提供方提供的数据分为无条件开放类、有条件开放类、非开放类，应采用分级的安全防护措施，企业访问及使用自身数据、“单一窗口”数据、其他企业数据时，应针对数据的级别、类别采用相应访问策略，具体要求如下：

——企业访问自身数据：企业查询访问本企业在厦门“单一窗口”平台自身报关、货物、运输工具等数据，对本企业完全开放，属于无条件开放类；

——企业访问厦门“单一窗口”数据：企业访问厦门“单一窗口”公共开放数据，如通关参数、商品目录数据资源等需要授权才能开放的数据，企业应发起访问申请，经数据开放服务平台进行审核并发放授权后进行访问，属于有条件开放类；

——企业访问其他企业或服务单位数据：企业访问其他企业数据，应通过第三方企业进行数据授权后，并在数据开放服务平台提供的隐私数据计算服务下，实现第三方企业原始数据不出域，数据输入、运算、结果输出全流程密态保护，同时数据经授权后方可进行安全计算，最小化利用，数据调用可追溯审计。

9.6.2 数据分类

将数据分为敏感数据和非敏感数据，采用相应的技术对敏感数据进行加密、脱敏、脱密、访问控制等处理，具体要求如下：

——对敏感数据进行加密，经过授权才能访问和解密数据；

——采用访问控制技术，经过授权才能访问敏感数据；

——采用数据脱敏技术，将数据中的敏感信息脱去或替换为伪造数据；

——在进行大数据分析前，应与数据所有者签署隐私保护协议，确定数据使用范围和限制。

9.7 数据开放处理机制

数据开放服务平台采用安全机制和管控措施，为企业使用数据和上报数据开辟专属的数据交换空间，存储厦门“单一窗口”开放的非敏感数据；同时统一数据开放管理，为企业提供数据开放区，具体要求如下：

——企业可利用在线数据服务和离线数据服务接收和交换开放的数据；

——数据开放区为企业提供数据出口通道，并提供安全管控措施审计企业用户使用开放数据情况；

——提供企业报关数据上报安全通道，对数据开放服务采取相应的安全措施，包括密钥管理和鉴权服务、访问控制和隔离、数据安全和个人信息保护、安全审计和血缘追踪等数据全生命周期管理措施。

9.8 数据全生命周期安全保障

数据全生命周期安全保障应提供包括数据采集、数据存储、数据传输、数据交换、数据授权使用、数据销毁安全等过程的安全技术和安全管理措施，具体要求如下：

——数据采集安全：支持数据采集工具的安全控制，并根据数据标准和特点对被采集数据进行分级分类，实现访问控制，数据采集未越权及数据来源可追溯；

——数据存储安全：通过访问控制、入侵防范、存储加密、防泄漏、防勒索、数据备份、数据容灾、数据审计等策略，保障数据在非安全的网络存储环境中的安全性；

——数据传输安全：通过压缩、重传、断点续传等技术实现高效传输，通过多种加密算法对数据进行加密传输；

——数据交换安全：自动发现敏感数据，通过脱敏规则进行数据变现，保障数据从高安全域流通到低安全域时敏感数据不泄露，并且脱敏后的新数据能保持源数据中的业务数据逻辑关系，不影响交换后的数据使用；

——数据授权使用安全：数据接收方应与数据提供方签订数据授权协议，包括共享数据内容、具体字段、数据授权策略、双方责任义务等。双方签订数据授权协议后，数据使用方即可通过相应接口获取数据，数据开放服务平台记录数据授权和数据应用过程；

——数据销毁安全：应建立数据清除、净化机制，通过授权使用的数据进行销毁时应遵循合规合法原则。

10 运维要求

10.1 一般规定

系统运行维护应遵循GB/T 28827.1运行维护的相关要求，并满足下列要求：

——应制定系统运行维护管理制度，配备专业系统管理员，定期监测系统运行环境、数据库状况、系统升级、数据备份情况等，系统管理员应对系统运行中出现的问题及时汇总、分析和解决，按照管理权限进行系统优化、完善；

——应对操作系统、数据库管理系统、应用软件和网络设备等设置权限；

——做好数据资源中心和数据服务目录的运维服务，做好数据备份，服务发生故障时，及时启动备用服务，保障数据开放服务平台核心功能的稳定运行及对外服务的可靠提供；

——应制定备份管理制度，及时备份基础数据、业务数据等各类相关数据；

——进行系统更新和维护时，应进行软件和数据的备份工作；

——系统管理员应定期分析系统运行日志，包括但不限于应用系统日志、业务操作日志及数据日志，及时发现系统异常情况。

10.2 运维服务实施

系统运维实施应满足下列要求：

——基础设施运维服务，对基础设施的日常运维巡检，当基础设施发生故障时，及时对故障进行处理；

——应用系统运维服务，应符合 GB/T 28827.6 中相关要求，对数据开放服务平台、应用生态各业务系统、开发者中心等相关系统及平台进行运维；

——数据运维服务，符合 GB/T 28827.4 中相关要求，主要包括对数据资源中心及数据服务目录中心的维护。

10.3 系统应急处置

系统应急处置应满足下列要求：

——应急响应规范应符合 GB/T 28827.3 中的要求，制定相应的应急响应制度及应急方案，应包括火灾预防、灭火设备、备份和恢复策略等；

——将应急事件按应急事件的可控性、严重程度和影响范围进行等级划分；

——应急事件处理，当系统异常、故障、崩溃时根据相应的具体问题第一时间排查处理；

——根据事件处置结果进行调查并形成安全事件处理报告；

——定期进行应急演练和培训，评估改进应急预案和应急管理制度。

参 考 文 献

[1] GB/T 18391.1－2009 信息技术数据元的规范与标准化 第1部分:数据元规范与标准化框 架[S].北京:中国标准出版社,2009.

[2] GB/T 19488.1 电子政务数据元 第 1 部分:设计和管理规范[S].北京:中国标准出版 社,2004.

[3] GB/T 25647－2010 电子政务术语

[4] GB/T 38664.1－2020 信息技术 大数据 政务数据开放共享 第1部分：总则

[5] GB/T 38664.2－2020 信息技术 大数据 政务数据开放共享 第2部分：基本要求

[6] GB/T 38664.3－2020 信息技术 大数据 政务数据开放共享 第3部分：开放程度评价

[7] GB/T 39477－2020 信息安全技术 政务信息共享 数据安全技术要求

[8] JGS/T 11－2014 海关业务基础数据元目录[S].北京:中国海关出版社有限公司,2016.

[9] JGS/T 12－2014 海关业务代码集[M].北京:中国海关出版社有限公司,2016.

[10] JGS/T 18－2014 海关关区代码[M].北京:中国海关出版社朋限公司,2016.

[11] 中华人民共和国交通部.中华人民共和国国际船舶保安规则.[2007-03-26].

[12]《中国海关报关实用手册》编写组.中国海关报关实用手册[M].北京:中国海关出版社有限公司,2021.

[13] DB52/T 1125－2016 政府数据资源目录 编制工作指南

[14] DB52/T 1126－2016 政府数据 数据脱敏工作指南