国家信息中心
State Information Center

国家电子政务外网管理中心
National E-Gov Network Administration Center

政务信息共享数据安全技术要求标准与应用实践

国家信息中心（国家电子政务外网管理中心）外网办 安全管理处

2021年5月

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 传真：010-68533919

目录/CONTENT

- 标准基本情况介绍
- 标准主要内容介绍
- 标准应用与技术实践

01 | 标准基本情况介绍

政策要求

整合异构信息资源，消除“信息孤岛”

各单位信息化建设相对独立、异构、分散，缺乏有效的总体规划和统一的设计标准，重复建设；信息交互共享困难，存在大量的信息孤岛和流程孤岛，需要通过构建信息资源共享交换平台，有效整合分散异构的信息资源，解决跨层级、跨地域、跨系统、跨部门、跨业务的数据共享交换问题。

开展大数据应用，发挥信息资源效能

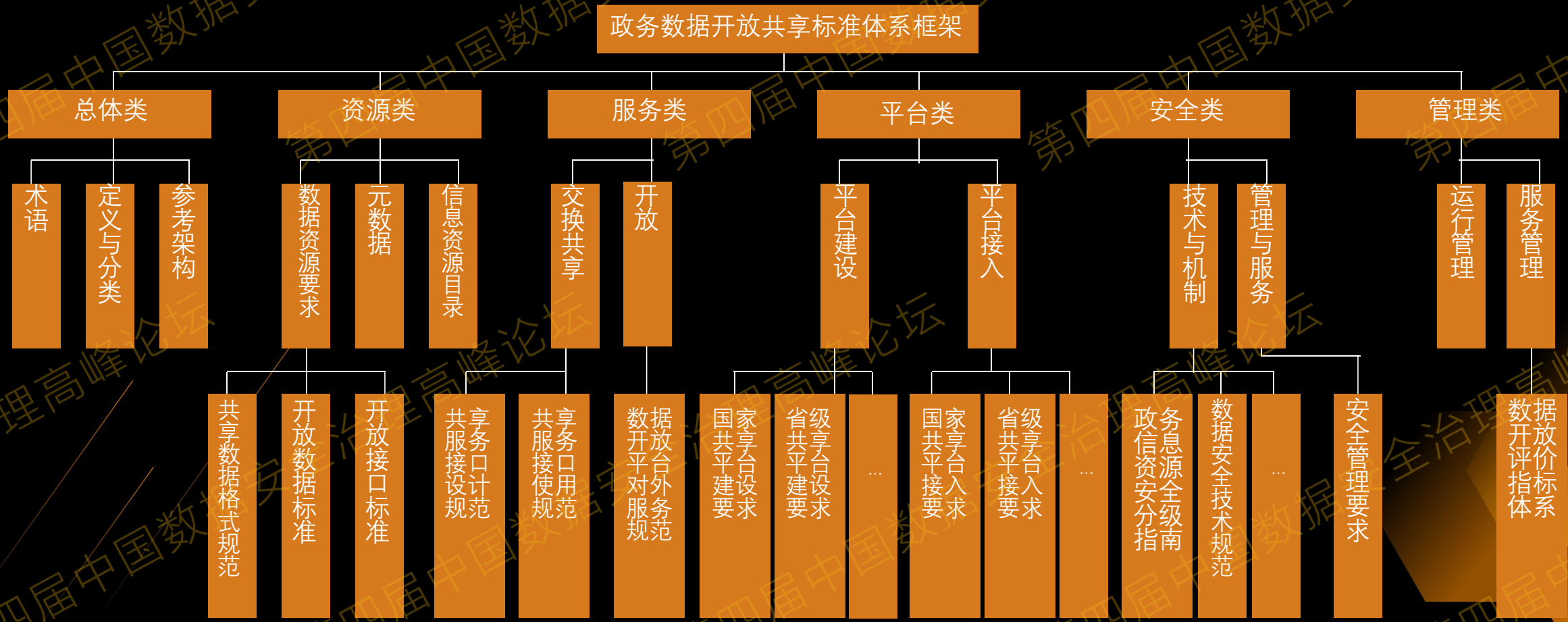
通过信息资源共享开放，可加强信息资源管理，汇集海量共享数据，灵活实现不同系统间的信息交换、信息共享与业务协同，同时通过大数据分析和挖掘，进一步发挥数据效能，提升政府精准治理能力，实现数据惠民。

- 加强政务信息资源采集、共享、使用的安全保障工作，**切实保障政务信息资源共享交换的数据安全**。
- 建立完善政务信息资源的网络安全保障等方面标准，各政务部门和共享平台管理单位应加强对共享信息采集、共享、使用全过程的身份鉴别、授权管理和安全保障，**确保共享信息安全。**

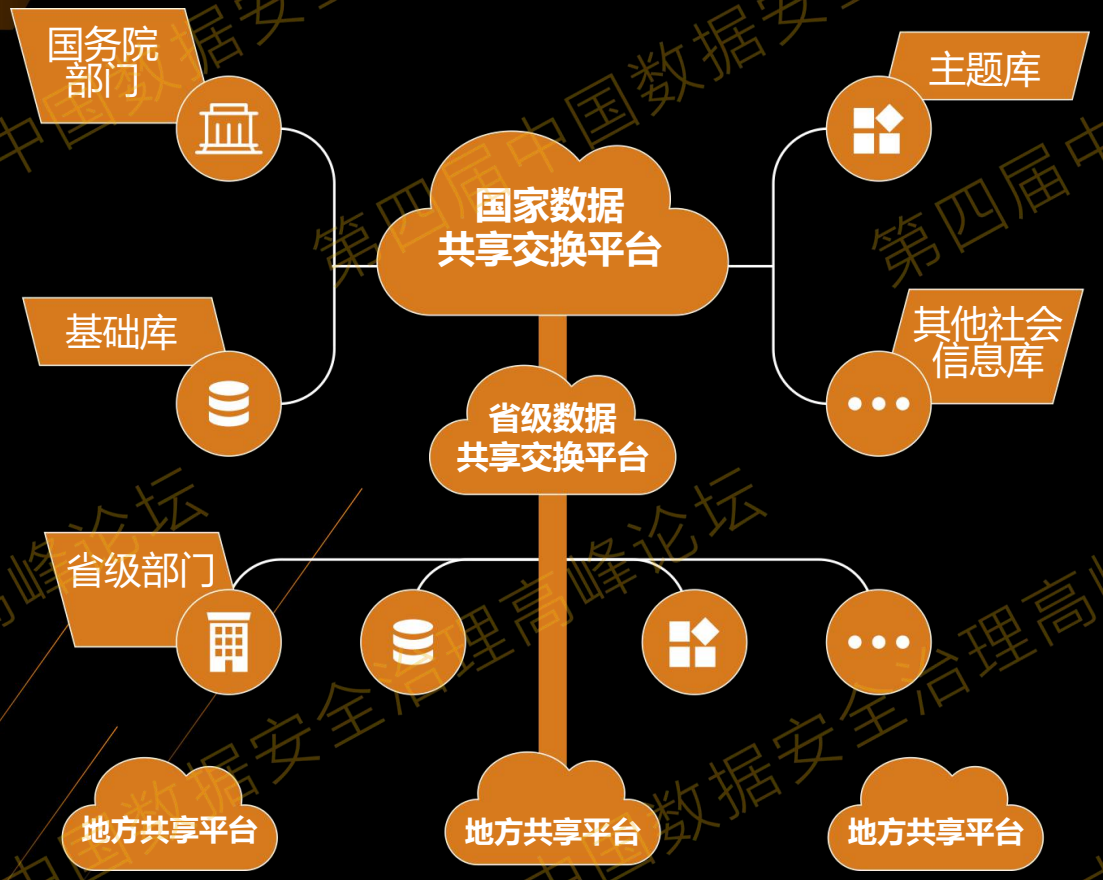
- 国发〔2016〕51号《政务信息资源共享管理暂行办法》
- 国办发〔2017〕39号《政务信息系统整合共享实施方案》
- 国办发〔2018〕45号进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案》
- 国发〔2018〕27号《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》

政务信息共享标准体系

在国家标准委直接指导下，信标委、信安标委联合国家电子政务外网管理中心等成立**政务信息共享标准工作组**，负责组织政务信息共享和开放标准制定。



工作基础



- 国家数据共享平台建设现状
- 截止目前，前置区覆盖76 个中央有关单位，31 个省（区、市）和新疆兵团。注册发布实时数据共享接口1206个，发布交换任务14726个，采用数据不落地方式，提供查询/核验服务 15.12亿次，订阅推送数据1011.01亿条，文件200.1TB。
- 已有相关规范基础：《国家数据共享交换平台体系（政务外网）总体框架》、《国家数据共享交换平台（政务外网）部门接入指南》、《国家数据共享交换平台（政务外网）省级平台接入指南》。

项目立项

2018年4月

1 在武汉召开的2018年全国信息安全标准化技术委员会SWG-BDS工作组第一次会议，就《信息安全技术 政务信息共享交换 数据安全规范》立项汇报

2018年7月

2 中国电子技术标准化研究院同意《信息安全技术 政务信息共享 数据安全技术要求》标准正式立项：《网络安全国家标准项目任务书》（项目编号：2018BZZD-SWG-003）

标准目标与范围

- 对政务信息共享数据流转的过程提出数据安全技术要求，包括政务信息共享数据准备、共享数据交换、共享数据使用等环节安全技术要求
- 适用于指导各级政务信息数据共享交换平台数据安全体系建设，规范各级政务部门使用政务信息数据共享交换平台交换非涉及国家秘密数据时的数据安全保障工作

标准编制组成员单位

- 国家信息中心
- 深圳奥联信息安全技术有限公司
- 中国电子技术标准化研究院信息安全中心
- 公安部信息安全等级保护评估中心
- 国家保密科技测评中心
- 中国信息安全测评中心
- 国家信息安全技术研究中心
- 清华大学
- 四川大学
- 中国电子科技网络信息安全有限公司
- 中国电子科技集团公司科学研究院
- 成都卫士通信息产业股份有限公司
- 全知科技（杭州）有限责任公司
- 亚信科技（成都）有限公司
- 北京安华金和科技有限公司
- 杭州数梦工场科技有限公司
- 陕西省信息化工程研究院
- 广东京信软件科技有限公司
- 北京信息安全测评中心
- 杭州美创科技有限公司

主要工作过程

立项
- 2018/4
- 2018/7

草案准备
- 2018/8
- 2018/9
- 2018/10

征求意见稿准备
- 2018/11
- 2018/12

征求意见第二稿
- 2018/12
- 2019/02
- 2019/03-04

送审稿
- 2019/07

正式发布
- 2020/11/19

7次会议
- 标准组内三次会议
- 外部专家三次会议
- TC260大数据组会议

5稿草案
- 标准组内部修订三稿
- 响应外部意见修订两稿

114条意见
- 外部专家97条
- 大数据组全会17条

版本1
- 响应TC260大数据组全会意见17条

版本2
- 响应新成员单位意见

第一稿
- 响应责任编辑意见

征求意见
- 收集到50条意见

第二稿
- 响应征求意见

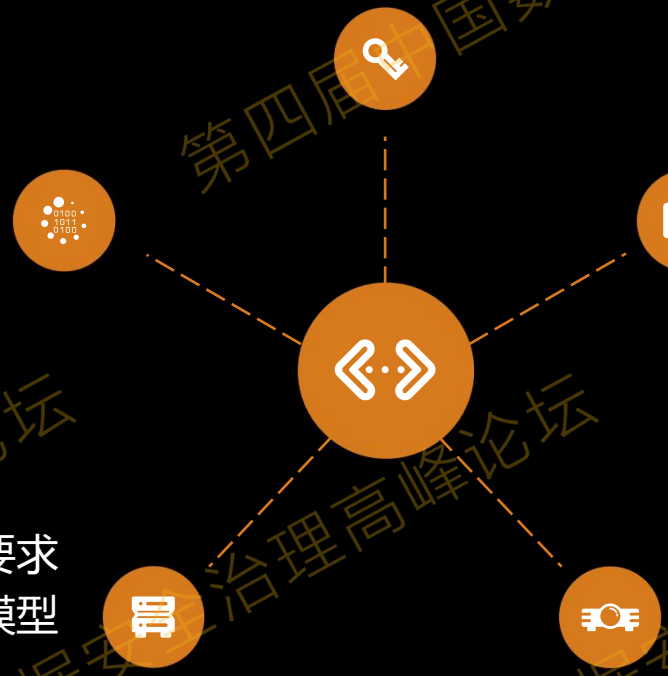
送审稿
- 责任编辑意见

02 | 标准主要内容

标准制定方法

深入调研、分析现有政务信息共享交换平台业务和相关安全风险点

抽象政务信息共享交换涉及主体、权责、对象、模式、流程、功能集合



形成政务信息共享交换业务模型与政务信息共享数据安全技术框架

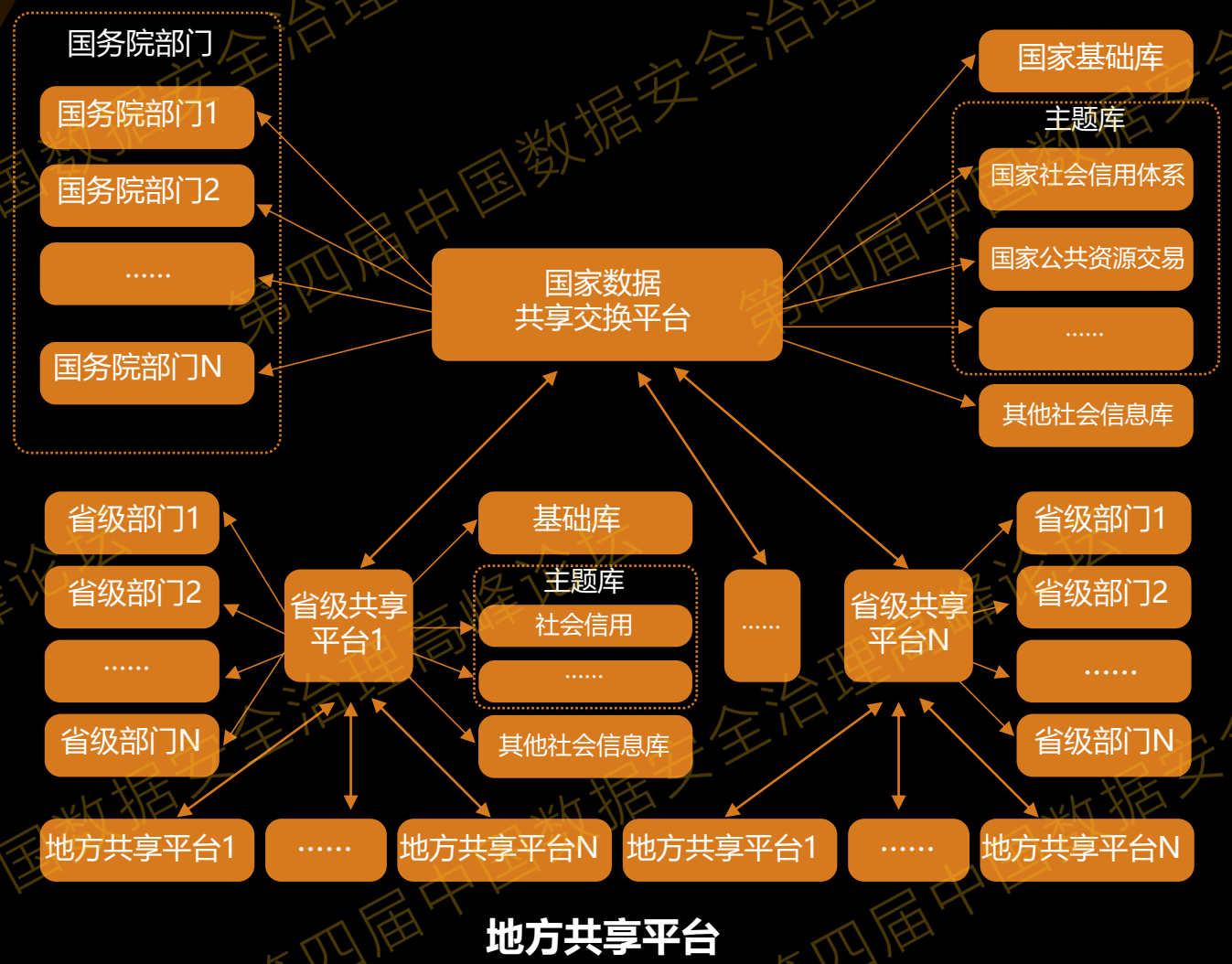
参考重要相关标准

- 信息安全技术 大数据交易服务安全要求
- 信息安全技术 数据安全能力成熟度模型
- 信息安全技术 大数据服务安全能力
- NIST Big Data Interoperability Framework: Volume 4, Security and Privacy

在安全框架下提出具体的安全技术要求

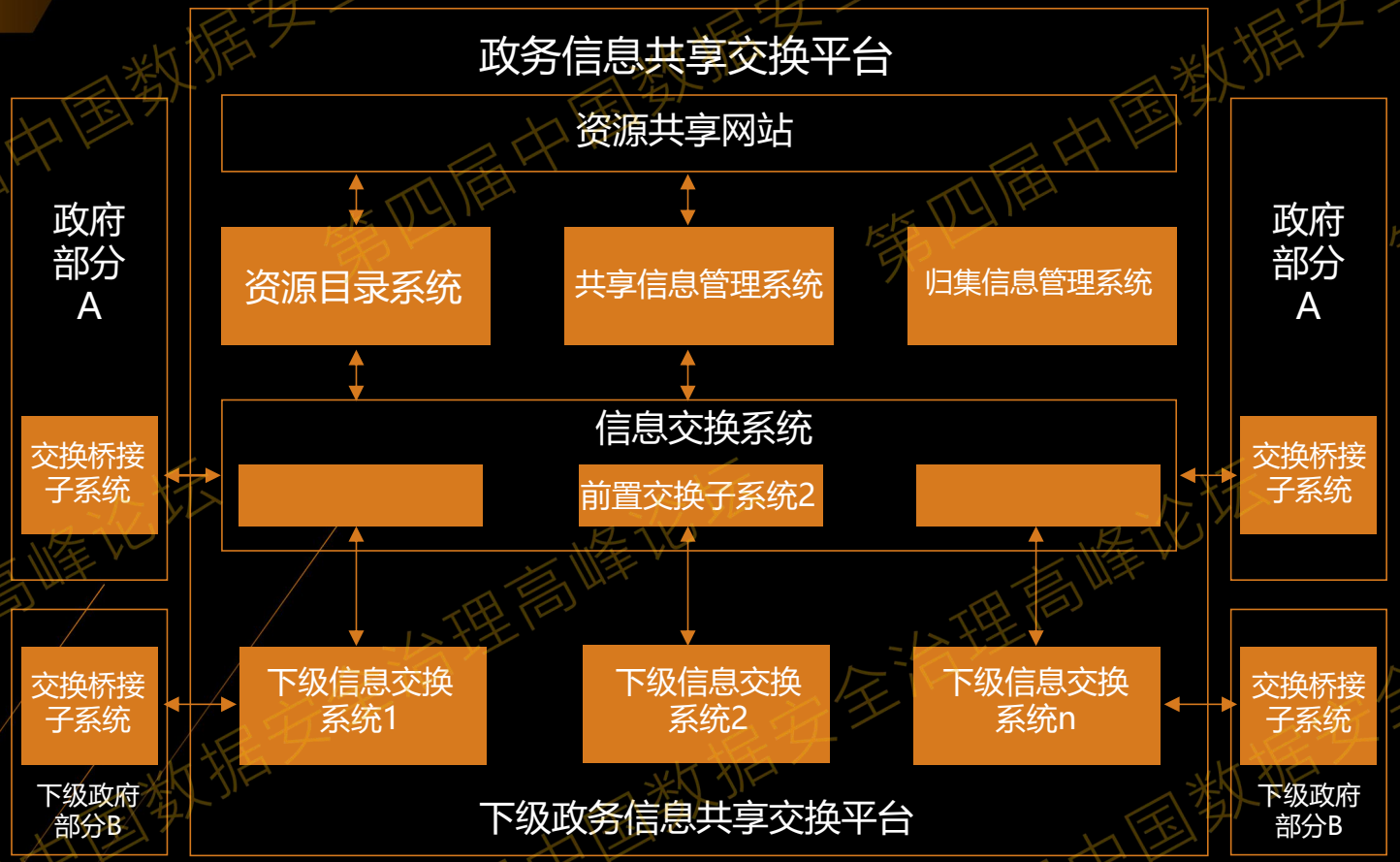
- 按角色
- 分阶段
- 结合关键功能和共享数据的生命周期
- 形成安全控制点和技术要求

政务信息共享交换平台数据共享交换体系



- 国家数据共享交换平台作为政务信息资源共享交换的枢纽部署在国家电子政务外网公共区，为中央部门及地方单位提供信息资源目录汇集管理、信息资源共享交换、业务协同应用支撑等服务。
- 政务信息共享交换平台由国家、省级、地市级等多级数据共享交换平台组成。各级共享交换平台横向对接所辖区域政务部门信息资源，纵向多级连通，形成横向联通、纵向贯通的数据共享交换体系。

政务信息共享交换平台一般框架



政务信息共享交换平台与资源共享业务相关的业务核心系统包括：

- 资源共享网站
- 资源目录系统
- 共享信息管理系统
- 信息交换系统
- 归集信息管理系统

政务信息共享模式与数据交换方式

共享交换模式

- 直通模式
- 代理模式
- 服务模式

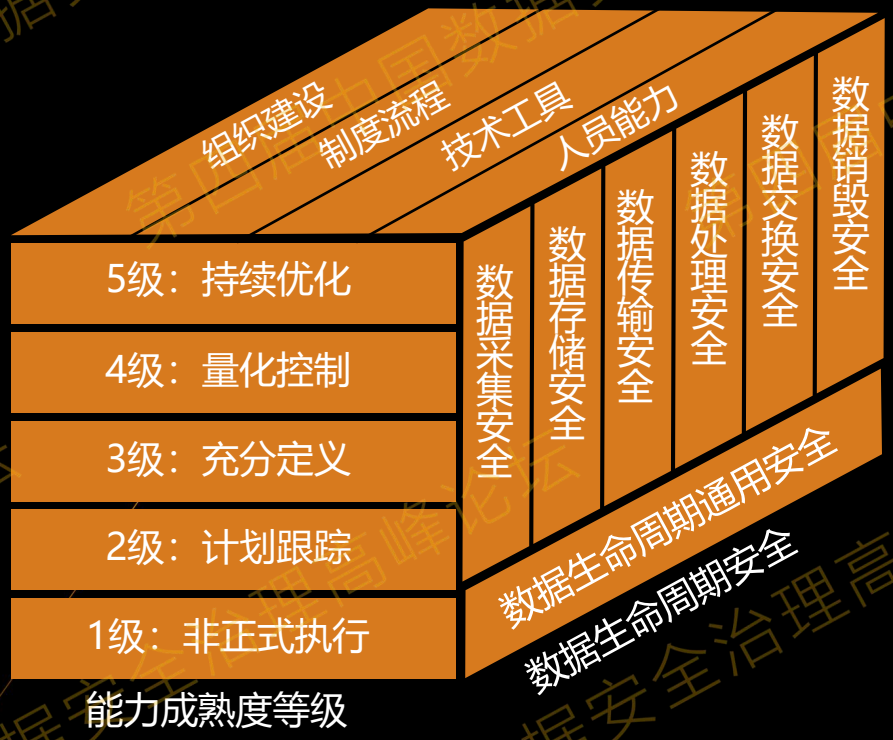
数据交换方式

- 库表交换
- 资源文件交换
- 服务接口
- 综合服务

（基础数据）查询
（基础数据）核验

（按需）统计分析

以数据生命周期构建安全能力--数据安全成熟度模型



在标准制定方法论上，充分借鉴了《信息安全技术 数据安全成熟度模型》（GB/T 37988-2019）相关思路，按照数据生命周期，分为数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全六个阶段，并进一步细化过程域。

政务信息共享交换模型构建方法分析

- 共享交换角色与权责

共享数据提供方

保障共享资源数据的来源真实、数据准确、完整

可用共享交换服务方

保障共享交换过程交换实体可信、数据传输安全、交换行为可查

共享数据使用方

保障获取共享资源数据的使用安全

- 对象

资源目录

目录数据、服务接口等

资源数据

普通数据，敏感数据

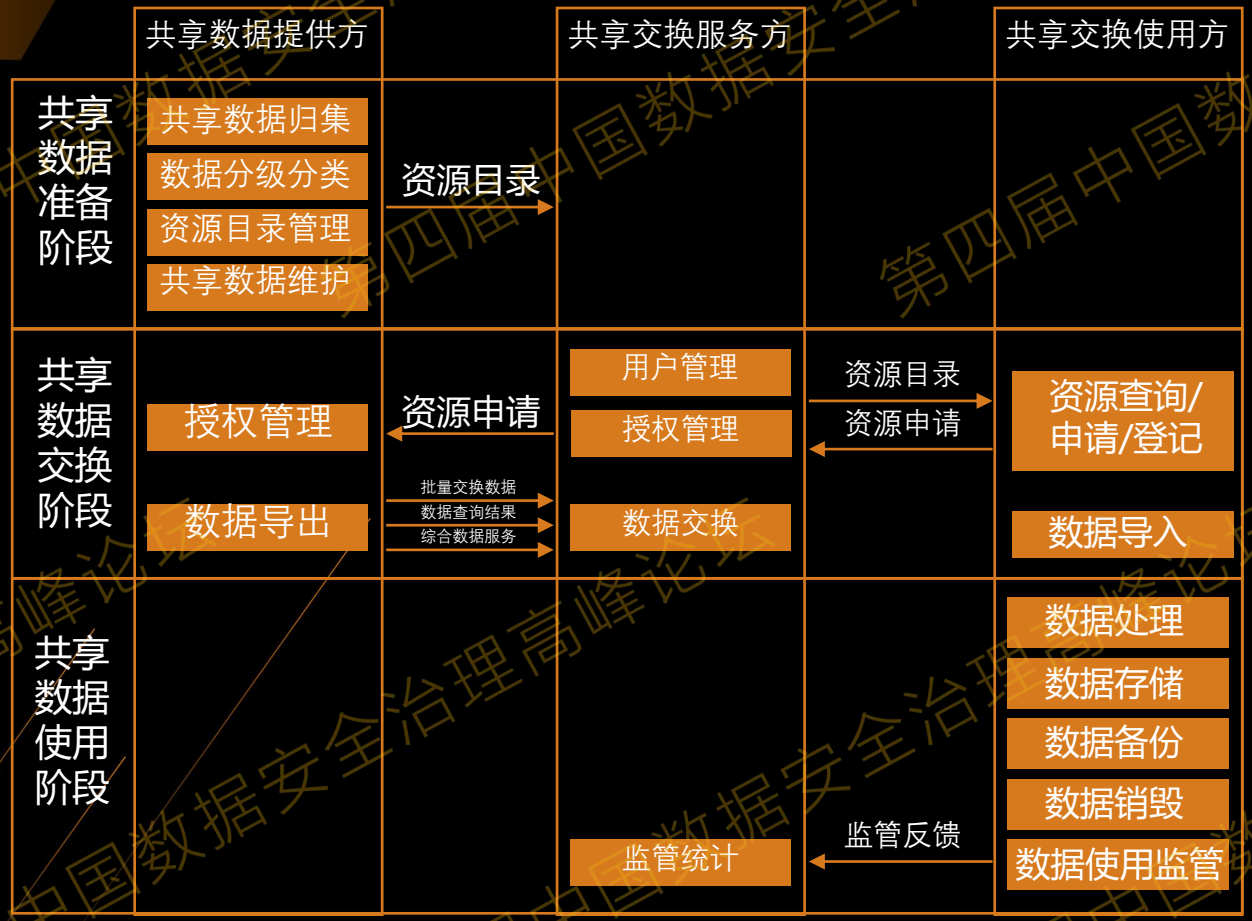
- 参照数据安全能力成熟度模型，结合数据生命周期阶段与政务信息共享的特点构建安全过程域

共享数据准备阶段（主要是共享数据提供方）

共享数据交换阶段（三方）

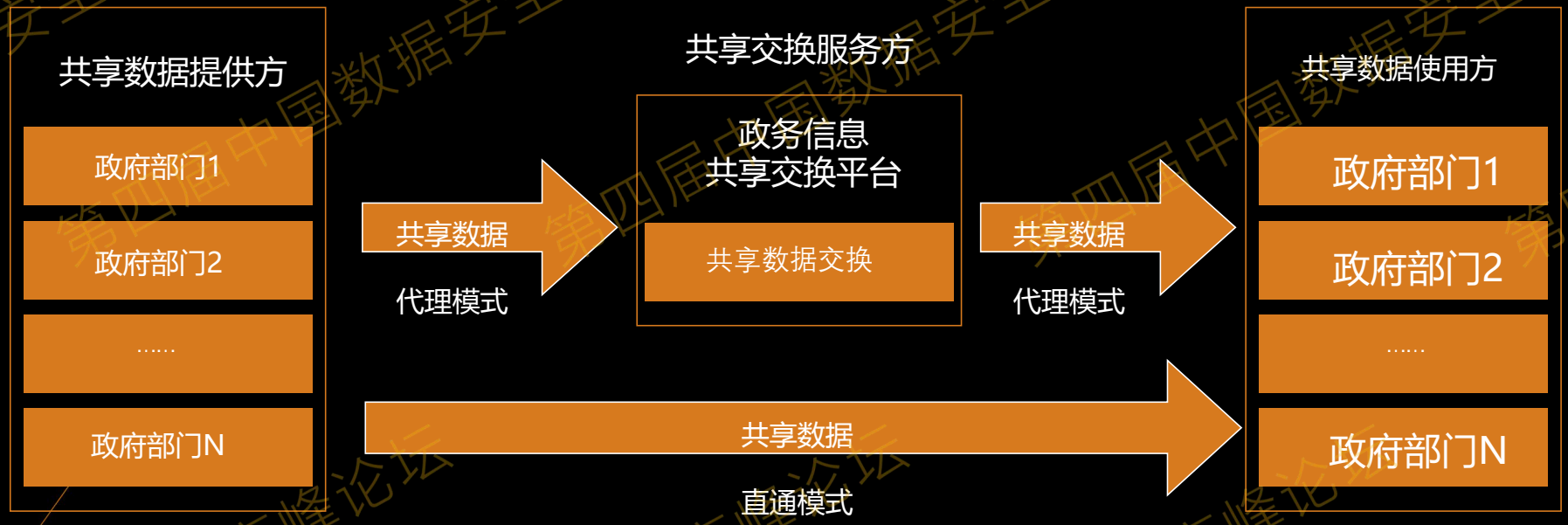
共享数据使用阶段（主要是共享数据使用方）

政务信息共享交换业务模型



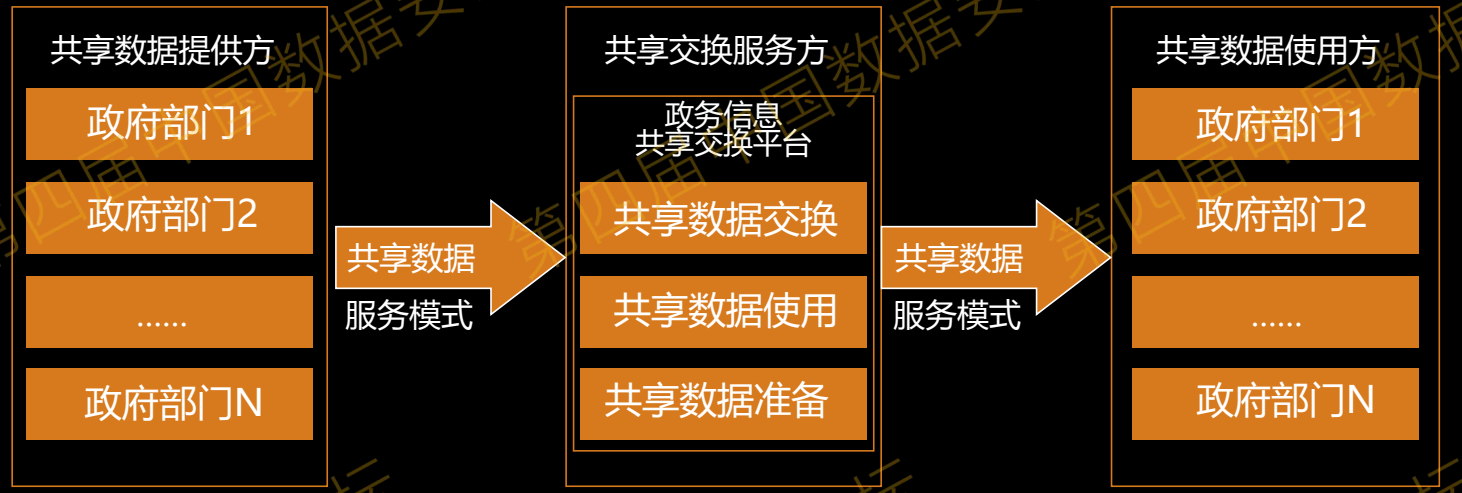
政务信息共享由共享数据提供方、共享交换服务方与共享数据使用方三方参与，由共享数据准备、共享交换和共享数据使用三个阶段组成。

共享交换平台代理模式与直通模式和业务模型对应关系



政务信息共享交换的直通模式和代理模式用于将政务部门已有政务资源数据在共享交换平台的支撑下提供给共享数据使用方，共享交换平台不参与共享数据的加工、处理等环节。在直通模式下，数据不经过共享交换平台。在代理模式下，数据仅在必要情况下在交换系统中临时缓存，交换完成后缓存数据即被清除。

共享交换平台服务模式和业务模型对应关系



服务模式

- **共享数据归集阶段:** 作为数据使用方采用本方的交换服务从数据提供方获取数据
- **共享数据加工阶段:** 作为数据使用方对归集的共享数据进行处理、加工
- **共享数据服务阶段:** 作为数据提供方采用本方的交换服务向新的数据使用方提供共享数据服务
- **各阶段根据不同角色确定需要满足的安全技术要求**

政务信息共享数据安全技术框架

政务共享数据安全技术要求框架由数据安全技术要求和基础设施安全技术要求两部分组成。

- 数据安全技术要求体系涵盖共享数据准备、共享数据交换和共享数据使用三个阶段中各功能集合所需的安全技术要求。
- 基础设施安全技术要求明确了政务信息共享交换业务的基础网络、云平台、前置交换子系统和资源共享网站等方面的安全防护要求。

标准主要内容

范围

规范性引用文件

术语定义与缩略语

政务信息共享安全框架

政务信息共享交换业务模型
政务信息共享数据安全技术要求框架

数据安全技术要求

共享数据准备安全技术要求
共享数据交换安全技术要求
共享数据使用安全技术要求

基础设施安全技术要求

通用要求
基础网络
政务信息共享交换云平台
前置交换子系统
资源共享网站

附录A：政务信息共享交换平台一般框架

附录B：政务信息共享交换模式

共享数据准备安全要求

- 共享数据归集
- 数据分级分类
- 资源目录管理
- 共享数据维护

目标：保障共享数据来源真实、数据准确、完整、可用

安全技术：数据源鉴别、分级分类、数据存储加密、数据存储隔离、数据召回等

共享数据维护过程安全技术要求

数据质量控制

建立并落实数据质量控制机制，保障所提供的共享数据与本部门原始数据的一致性

数据存储加密

敏感数据采用符合GM/T 0054等国家相关标准规定的数据加密方式与密码算法进行加密存储

数据存储隔离

数据存储环境进行分域分级设计，将数据分域分级存储

数据更新召回

支持共享数据更新和失效数据召回

共享数据交换安全要求

- 用户管理
- 授权管理
- 数据导出
- 数据交换
- 数据导入

目标：保障交换过程交换实体可信、数据传输安全、交换行为可查

安全技术：身份管理安全、授权管理安全、数据脱敏、数据加密、事务标记、身份鉴别、访问控制、安全传输、操作抗抵赖、过程追溯等

共享数据交换过程安全技术要求

事务标识

对每次数据交换指定具有唯一性的交换事务标识

身份鉴别

鉴别数据交换两方身份

访问控制

根据授权和身份进行数据访问控制

安全传输

保障传输过程数据安全性，包括数据加密、缓冲处理等

操作抗抵赖

对敏感数据交换过程实施数字签名，防止对操作行为的抵赖

过程追溯

通过三方详细日志实现交换过程可追溯

联接口安全

保障级联接口间数据交换的保密性、一致性和完整性

共享数据使用安全要求

- **数据处理**
- **数据存储**
- **数据备份**
- **数据销毁**
- **数据使用监管**

目标：保证共享数据使用安全

安全技术：身份鉴别、访问控制、数据脱敏、数据处理溯源、加密保护、安全存储、安全销毁等

共享数据处理过程安全技术要求

身份鉴别

对数据处理相关系统访问和数据操作进行身份鉴别

访问控制

对数据处理相关系统系统和数据访问根据授权和身份进行控制

授权管理安全

明确授权目的和范围，保留授权记录，敏感数据访问应经过二次授权

数据脱敏

数据处理过程中产生的敏感数据应进行数据脱敏，建立有效性的评价机制

数据加密

实现加密数据的处理，包括计算中间结果的加密保护

数据防泄露

设置传播策略和传播范围，防止数据在未授权条件下的下载、复制、截屏等

分布处理安全

分布式处理过程中计算节点安全策略的一致性和数据的一致性

数据处理溯源

支持溯源数据的采集和存储，保障溯源数据能重现数据处理过程

数据分析安全

安全审计

数据使用及处理全过程进行安全审计，提出审计日志要求等

基础设施安全技术要求

- 通用要求
- 基础网络
- 政务信息共享交换云平台
- 前置交换子系统
- 资源共享网站

与相关规范、标准的协调性

相关标准协调性

- 涉及的系统架构/部件遵循GB/T 21062-2007政务信息资源交换体系
- 涉及的密码算法和密钥管理应遵循国家商用密码的有关规定
- GM/T 0054-2018 信息系统密码应用基本要求
- 安全技术要求参考 GB/T 35274-2017大数据服务安全能力要求
- 基础设施安全符合
- GB/T 22239-2019 信息系统安全等级保护基本要求（三级）
- 云平台基础服务符合
- GB/T 31168-2014 云计算服务安全能力要求（增强级）

03 | 标准应用与技术实践

应用与实践一：国家数据共享交换平台数据标识和分类分级

安全标签是敏感数据在共享交换前、共享交换中、共享交换后的安全“属性”，是一种数据安全保护技术措施！

国密算法：
保护数据完整性、不可篡改、防止监听

列式水印：
针对库表，嵌入列式水印标记

授权时间：
数据使用有效期，例如：2020-01-03至2020-12-31；

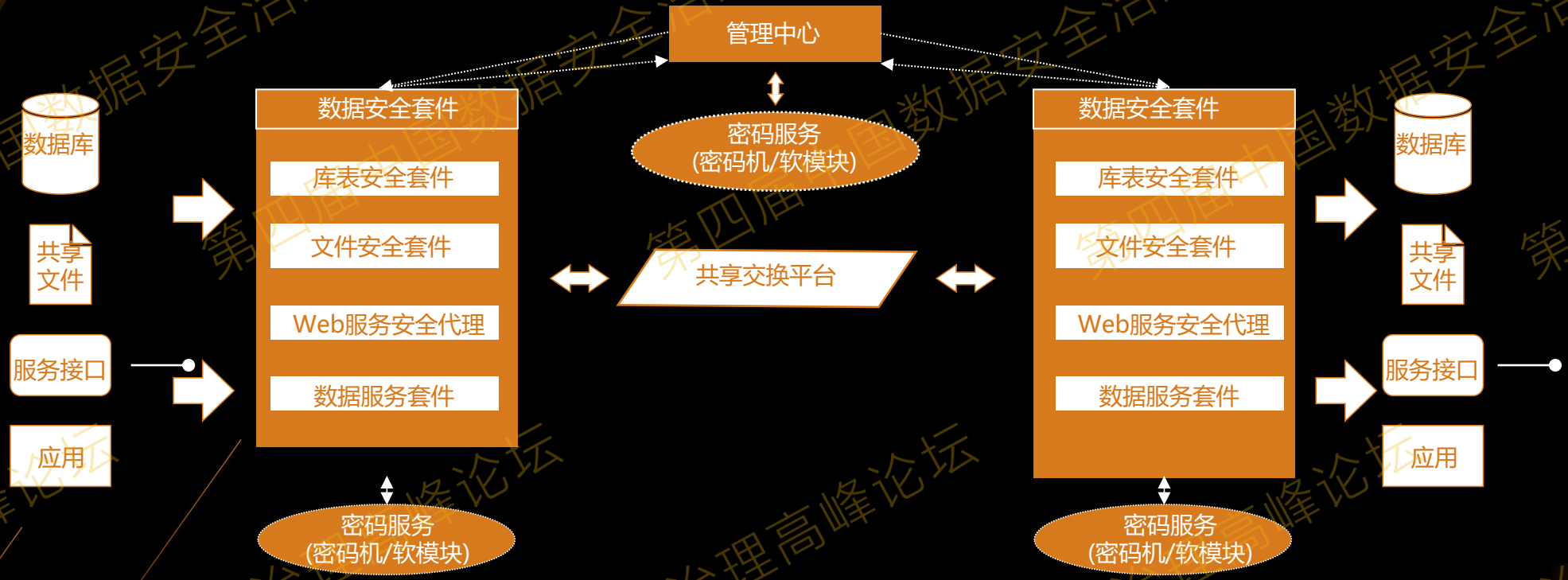
溯源标记：
数据打标过程中向数据插入溯源信息

授权范围：
数据使用范围，可以是机构、用户、应用等；

使用频率：
针对服务接口和数据服务，接口调用频次限定，如1000次/min；

交换共享数据的安全盾牌-数据安全标签

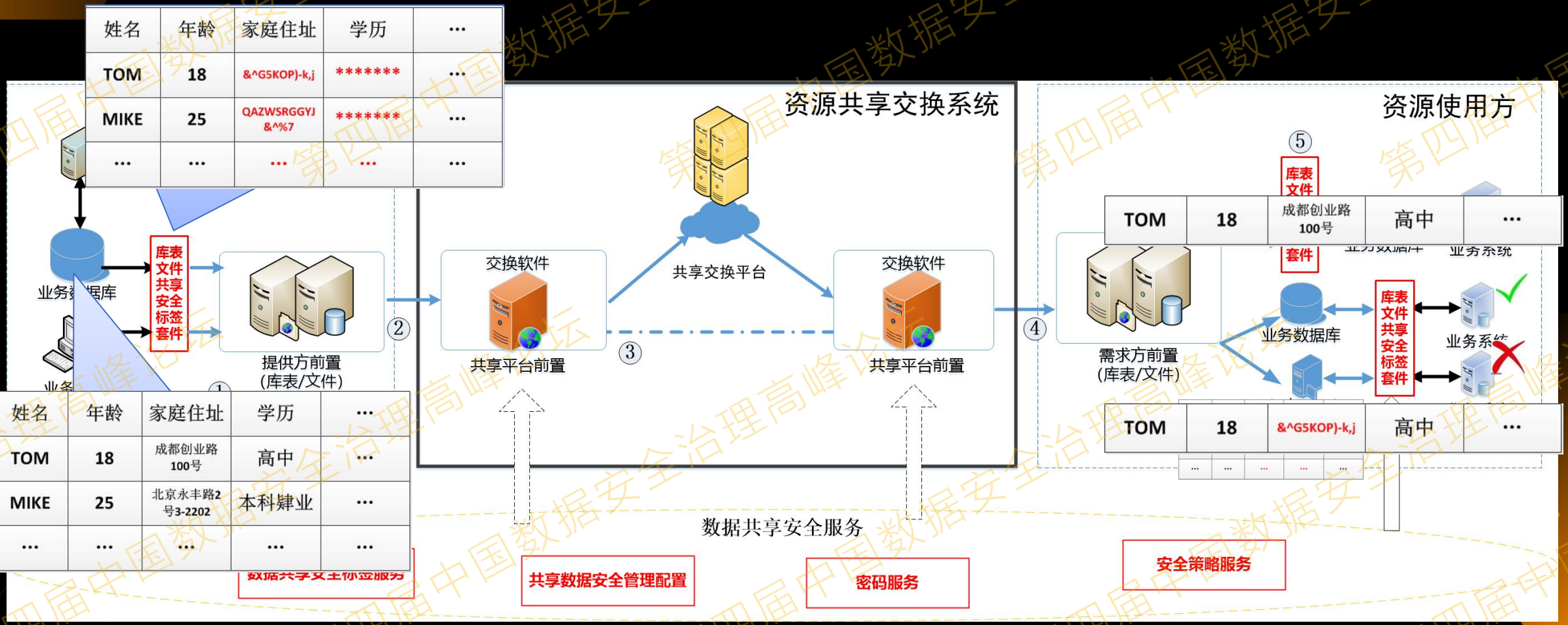
系统组成



- 管理中心：软件系统。提供共享数据对接、安全策略配置、数据保护任务创建等配置管理功能安全套件；
- 软件系统。实现前置库数据抽取、数据分级保护、安全标记、Web服务传输保护等功能。
- 密码模块：系统需要密码服务支持。可根据相关管理要求选择配用密码机或软模块

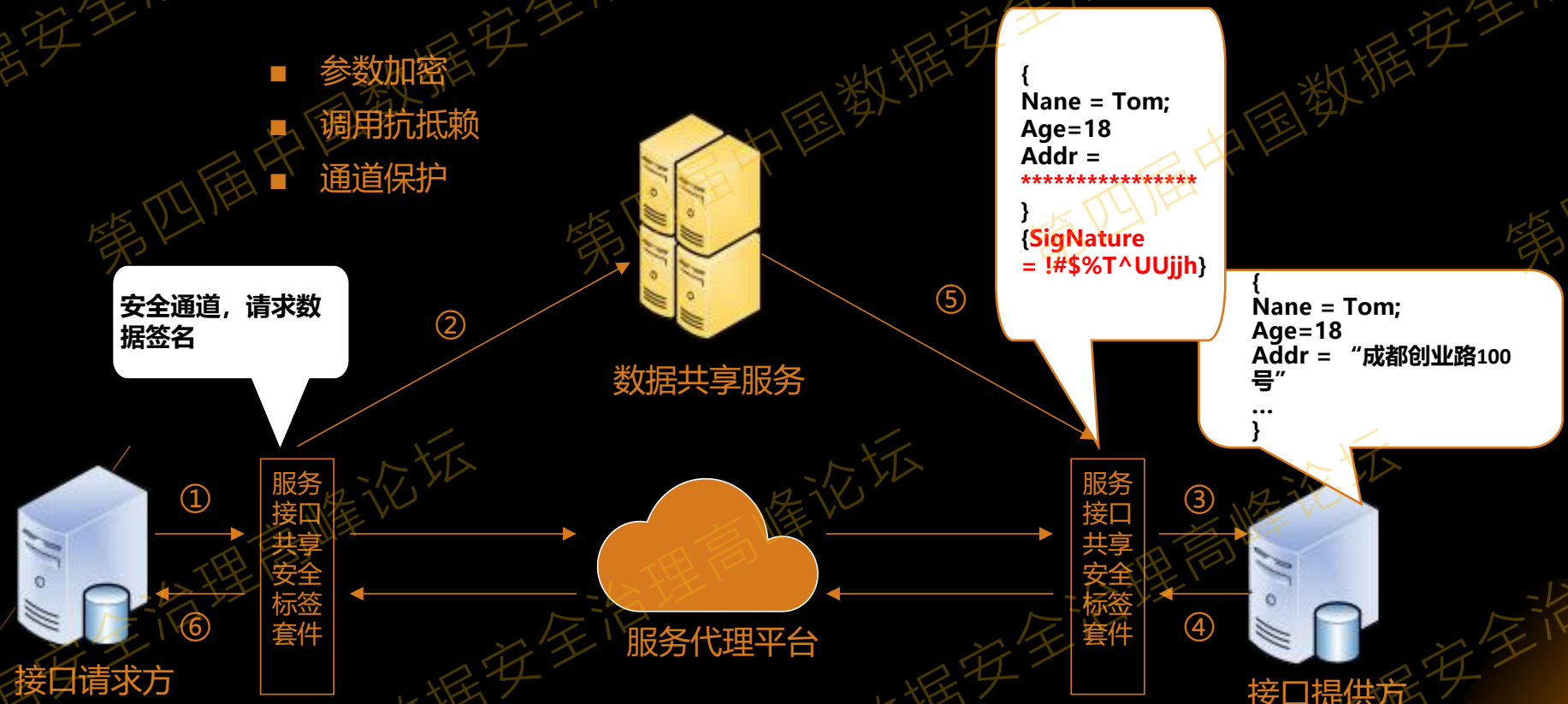
典型防护流程—库表文件

可实现数据分类分级、数据分级保护、多形式安全标记、全过程数据溯源、细粒度安全管控



典型防护流程—服务接口

- 参数加密
- 调用抗抵赖
- 通道保护



THANKS