ICS 35.240.01 （注：此处请按照文本内容分类号对应填写准确）
CCS L 16（注：此处请按照文本内容分类号对应填写准确）

团 体 标 准

T /OIDAA XX—XXXX

基于分布式数字身份的个人数据授权使用流程和技术规范

Personal Data Authorization Process And Technical Specifications Based on Distributed Digital Identity

（工作组讨论稿）

（本稿完成日期：2024-11-30）

XXXX-XX-XX 发布 XXXX-XX-XX 实施

中关村安信网络身份认证产业联盟 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》给出的规则起草。

本文件由中关村安信网络身份认证产业联盟提出。

本文件起草单位：厦门中盾安信科技有限公司、北京中盾安信科技发展有限公司、中国建设银行研修中心（研究院）、中移信息技术有限公司、蚂蚁科技集团股份有限公司、华科云曜（北京）科技有限公司。

本文件主要起草人：王剑冰、郝久月、彭钢、吴晶、昌文婷、郭志明、蔡国城、李頔、李振裕、庄江龙、吴瑶、宋效军、边鹏、张晓蒙、叶可可、仲梓源、孟文博。

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。

引 言

本文件是根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数 据安全法》《中华人民共和国个人信息保护法》《中共中央、国务院关于构建数据基础制度更好发挥数 据要素作用的意见》《促进和规范数据跨境流动规定》《数据出境安全评估办法》等法律及政策意见中明确落实构建数据基础制度的相关规定，以维护国家数据安全、保护个人信息和商业秘密为前提，促进数据合规流通使用，推动个人数据授权机制，保障数据要素各参与方合法权益，所提出的基于分布式数字身份的个人数据授权的流程与技术规范，包括个人数据授权总体模型、个人数据授权流程、个人数据授权技术规范等方面内容。

基于分布式数字身份的个人数据授权使用流程和技术规范

1 范围

本文件规定了个人数据自主授权的场景、流程和相关技术要求。

本文件仅适用于数据流动中涉及个人数据的自主授权活动。

本文件不适用于涉及国家秘密的数据和军事数据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 35295	信息技术 大数据 术语
GB/T 36343-2018	信息技术 数据交易服务平台 交易数据描述
GB/T 5271.4-2000	信息技术 词汇 第 4 部分：数据的组织
GA/T 1721-2020	居民身份网络认证 通用术语
GB/T 31504-2015	信息安全技术 鉴别与授权 数字身份信息服务框架规范
GB/T 35273	信息安全技术 个人信息安全规范
GA/T 1721-xxxx	网络身份认证公共服务 通用术语
ITU-T X.1252	身份管理基准术语和定义
YD/T xxxx-xxxx	数字身份 分布式服务总体框架

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据（data）

对事实、概念或指令的一种形式化表示，适用于以人工或自动方式进行通信、解释或处理。 [来源：GB/T 5271.4-2000]

3.2

个人数据（personal data）

指个人的具体行为数据，但个人数据在一定程度上会包含个人信息，如个人购买记录、个人健康记录等。[来源：GB／T 35273]

3.3

数据主体（data subject）

指个人数据的主体角色，即个人数据中包含的一个已识别或可识别的自然人。[来源：GB／T 35273]

3.4

数据目录（data catalog）

指一组描述个人数据的元数据，为数据主体的个人数据创建一个信息完备且可搜索的清单。

3.5

数据提供方（data provider）

指通过个人数据确权取得个人数据持有权的机构或自然人，负责确保个人数据的采集、生成、存储和管理过程都具备合法性、公平性和透明性。

3.6

数据使用方（data user）

指有需求使用个人数据进行分析、处理、存储或传播的机构或自然人，负责确保个人数据处理的安全性和合规性，并在个人数据处理过程中尊重数据主体的隐私权和个人信息保护的权利。

3.7

数字身份（digital identity）

指一个主体对象的数字化描述，由赋予实体唯一对应的数字标识及与之关联的属性声明构成。[来源：GB/T 31504-2015，3.6，有修改]

3.8

分布式数字身份（distributed digital identity）

指参照 W3C 分布式数字身份标准实现的可支持分布式认证的数字身份。

3.9

个人数据授权平台（personal data authorization platform）

指为个人数据的授权流通提供一个全面的数据管理和授权、授权核验的技术平台。

3.10

分布式数字身份基础设施（distributed digital identity infrastructure）

指为参与个人数据流通的机构或自然人提供分布式数字身份签发和可信存证、取证服务能力的基础平台。

3.11

个人数据授权申请（personal data authorization request）

指数据使用方就特定用途需获取对应个人数据时，向数据主体提出明确的授权请求，详细说明对个人数据的使用目的、范围和期限的过程。

3.12

个人数据授权协议（personal data authorization agreement）

指由个人数据授权平台依据数据使用方就特定个人数据使用场景生成的各项内容约定。其中约定内容包括但不限于数据提供方信息、数据使用方信息、数据接口、个人数据内容说明、个人数据授权内容、授权时效性与免责条款等。本文本特指签署的电子化协议。

3.13

个人数据授权（personal data authorization）

指作为数据主体的自然人，在通过个人数据授权协议明确知晓数据使用方对其个人数据的使用需求和目的之后，依其意愿对个人数据授权协议使用分布式数字身份进行签署的过程。

3.14

个人数据请求（personal data request）

指数据使用方在获得数据主体授权的前提下，依照授权约定，向数据提供方获取数据主体授权的个人数据的过程。

3.15

个人数据授权验证（personal data authorization verification）

指数据提供方或数据使用方对个人数据授权进行真实性、有效性验证的过程，确保数据处理活动获得对应数据主体的个人授权。

4 缩略语

下列缩略语适用于本文件。

APP：智能手机的第三方应用程序（Application）

H5：超文本语言第五版本（Hypertext Markup Language，HTML5 的简称）

5 个人数据授权总体模型

5.1 概述

个人数据授权总体模型见图1。

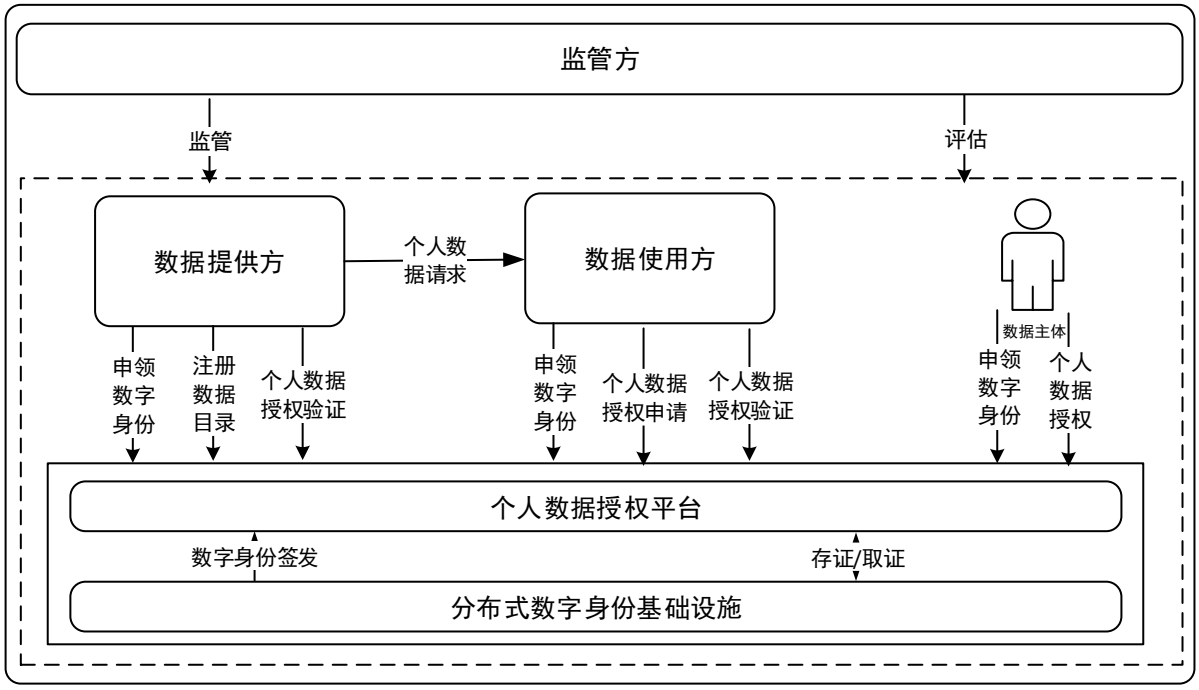

图 1：个人数据授权总体模型

个人数据授权总体模型包括监管方、数据提供方、数据使用方、数据主体、个人数据授权平台与分布式数字身份基础设施 6 个角色主体。

5.2 监管方

在个人数据授权流通中具有法定权利或主管部门授予监管职责的监管机构。包括但不限于以下活动：

a) 应通过申领分布式数字身份，完成身份的可信锚定；

b) 应负责制定和执行个人数据授权流通的相关政策、法律和标准，对个人数据授权流通的各项活动进行监管和指导；

c) 应负责对数据提供方、数据使用方、数据主体、个人数据授权平台、分布式数字身份基础设施的服务能力和安全运营能力进行评测，并出具客观、公平的测评结果。可通过授权认可的第三方独立测评机构完成相应测评，以确保各参与方在个人数据授权系统中的合规性和安全性。

5.3 数据提供方

向数据使用方提供个人数据的角色。包括但不限于以下活动：（注：数据目录注册见附录 A、个人数据授权核验见附录 B、个人数据授权核验见附录 C）

a) 应通过申领分布式数字身份，完成身份的可信锚定；

b) 应负责确保个人数据的合法采集、生成、存储和管理，并按要求向国家有关部门进行登记备案；

c) 应负责积极促进个人数据流通，并主动对其持有的个人数据的数据目录进行登记和发布；

d) 应对其持有个人数据的安全性负责，对已获得数据主体授权的数据使用方提供个人数据，并采取必要的技术措施来保护数据不被未授权访问；

e) 应配合监管方的审计和合规性检查，以证明数据处理活动的合法性和合规性。

5.4 数据使用方

有特定个人数据使用需求的角色。包括但不限于以下活动：（注：个人数据授权见附录 B、个人数据授权核验见附录 C）

a) 应通过申领分布式数字身份，完成身份的可信锚定；

b) 应依据自身业务需求，在确保其用数需求符合相关数据保护法规和标准的同时，明确提出对个人数据使用目的和需求；

c) 应在对个人数据处理完成后，需根据个人数据授权协议和法律要求，妥善处理或销毁个人数据，确保数据主体的权益不受侵害；

d) 应配合监管方的审计和合规性检查，以证明数据处理活动的合法性和合规性。

5.5 数据主体

个人数据的主体角色。包括但不限于以下活动：（注：个人数据授权见附录 B）。

a) 应通过申领分布式数字身份，完成身份的可信锚定；

b) 应在个人数据流通中，具备对个人数据进行安全、自主授权和管理的权利，确保数据主体操作的真实性和不可抵赖性。可通过安全持有的分布式数字身份私钥进行自主签名来实现；

c) 应在个人数据流通中，具备对其个人数据享有授权和撤回授权的权利，即对个人数据授权协议可以根据自己的意愿进行授权签署，也可以在任何无条件下撤回已授权的个人数据授权协议；

d) 宜具备查看和审核其个人数据被使用情况的能力；

e) 宜具备通过个人数据授权获取相应的经济利益。

5.6 个人数据授权平台

为个人数据流通提供个人数据管理和授权管理的角色。包括但不限于以下活动：（注：数据目录注册见附录 A、个人数据授权见附录 B、个人数据授权核验见附录 C）

a) 应通过申领分布式数字身份，完成身份的可信锚定；

b) 应支持个人数据的接入管理，为数据提供方提供便捷的数据目录注册与发布的服务；

c) 应对用数场景的合规性进行审核，提供生成透明、规范的个人数据授权协议的服务；

d) 应建立个人数据授权流通全生命周期的管控体系，确保个人数据流通全流程操作可审计，数据可溯源；

e) 应配合监管方的审计和合规性检查，以证明数据处理活动的合法性和合规性。

5.7 分布式数字身份基础设施

负责为参与个人数据授权流通的数据提供方、数据使用方、数据主体、个人数据授权平台签发分布式数字身份，为个人数据授权流通的全生命周期提供可信存证、可信取证的服务能力。包括但不限于以下活动：

a) 应为监管方、数据提供方、数据使用方、数据主体提供分布式数字身份的签发、认证和管理服务；

b) 应为个人数据流通提供全生命周期的存证、取证服务；

c) 应配合监管方的审计和合规性检查，以证明数据处理活动的合法性和合规性。

6 个人数据授权流程

6.1 概述

个人数据授权流程见图 2。

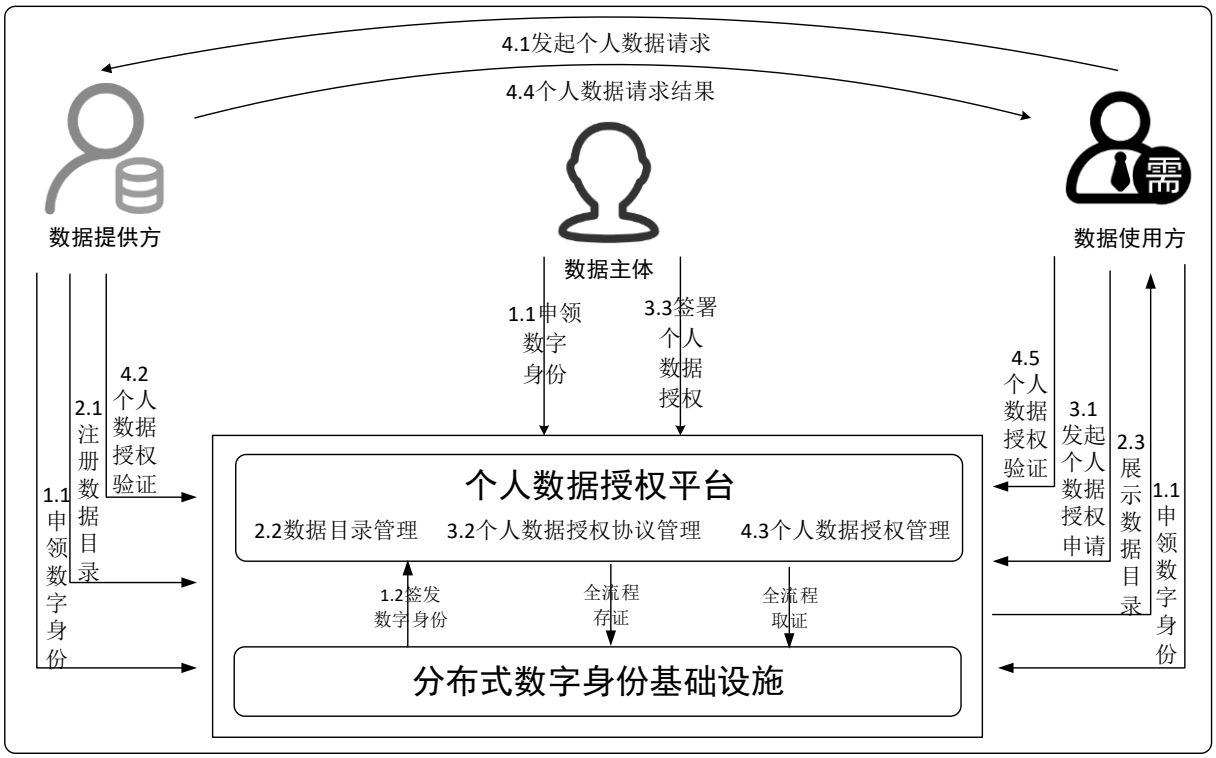

图 2：个人数据授权流程图

个人数据授权总体模型步骤说明如下：

一、 数据提供方、数据使用方、数据主体申领分布式数字身份

（1） 数据提供方遵循个人数据授权平台与分布式数字身份基础设施的准入机制，通过提交申请与审核流程申领分布式数字身份；

（2） 数据使用方遵循个人数据授权平台与分布式数字身份基础设施的准入机制，通过提交申请与审核流程申领分布式数字身份；

（3） 数据主体通过自然人法定基础身份证件信息向个人数据授权平台与分布式数字身份基础设施申领分布式数字身份。

二、 数据提供方注册数据目录（注：详细流程见附录 A）

（1） 数据提供方根据其持有的个人数据元数据信息，包括数据来源、类型、用途和使用限制等信息，向个人数据授权平台创建数据目录；

（2） 个人数据授权平台通过数据目录管理对已注册的数据目录进行上架发布；

（3） 数据使用方通过查询和检索功能来访问已发布的数据目录。

三、 数据主体个人数据授权（注：个人数据授权协议范本、详细流程见附录 B）

（1） 数据使用方依据业务需求，明确使用个人数据的目的、方式、使用规范和使用期限等，向个人数据授权平台发起个人数据授权申请；

（2） 个人数据授权平台依据数据使用方的授权申请，通过个人数据授权协议管理审核数据使用方的用数场景，并生成个人数据授权协议，同时向对应数据主体发起个人数据授权申请；

（3） 数据主体通过电子化方式如 APP、H5 等便捷方式知悉其个人数据的使用需求后，通过分布式数字身份对个人数据授权协议进行签署，完成个人数据授权；

四、 数据提供方、数据使用方个人数据授权验证（注：详细流程见附录 C）

（1） 数据使用方获得数据主体的个人数据授权后，向数据提供方发起个人数据请求；

（2） 数据提供方接收到数据使用方的个人数据请求后，向个人数据授权平台进行个人数据授权验证；
（3） 个人数据授权平台通过个人数据授权管理验证个人数据授权的真实性、有效性；
（4） 数据提供方接收到个人数据授权验证结果后，向数据使用方提供授权内的个人数据信息；
（5） 数据使用方接收到个人数据结果后，向个人数据授权平台进行个人数据授权验证，并进行后续业务操作。

6.2 限定条件

个人数据授权应当遵循一系列限定条件，以确保数据处理活动的合法性和合规性。具体来说，个人数据授权应当面向特定个人数据、特定用途进行展开，这意味着授权必须是具体和明确的，不能是模糊或笼统的。总体而言，个人数据授权场景应当在监管方的合规监管下构建，这包括事前约束、事后规制的法律关系，以确保数据处理活动的合法性。明确在特定空间和时间范围内，由特定数据使用方发起个人数据授权申请，经数据主体独立个人数据授权，从特定数据提供方处取得特定个人数据并进行加工和处理，用于特定之目的。这样的授权流程有助于保护个人隐私，同时促进个人数据的合理利用和流通。

7 个人数据授权技术规范

7.1 概述

个人数据授权技术规范是一套全面且系统化的框架，它涵盖了个人数据在授权、使用、传输和存储过程中的所有关键环节，确保这些流程的安全性、合规性、真实性和透明性。这些规范旨在完善个人数据流通安全治理标准，以保护数据主体的隐私权益，同时促进个人数据的合法流通和使用。通过遵循这些技术规范，可以确保个人数据授权过程中的每一步都符合法律法规，明确各方主体的责任和义务，规范个人数据流通行为，防止个人数据滥用，为个人数据流通提供制度保障。

7.2 个人数据识别与分类技术要求

个人数据识别与分类技术要求确保在保护个人隐私的同时，促进个人数据的便捷流通和合理利用。包含但不限于以下方面：

a) 应要求各参与方准确识别和分类个人数据，区分敏感数据和非敏感、判定风险等级。包括但不限于个人身份信息、个人生物识别信息、个人健康生理信息、个人财产信息、个人通信信息等；
b) 应要求实施差异化的数据保护措施，对不同类型、不同级别的个人数据采取相应的加密、访问控制等保护措施。

7.3 分布式数字身份技术要求

分布式数字身份技术要求为各参与方提供安全、可信、可验证的分布式数字身份标识，通过确保参与机构与自然人身份的真实性，有助于构建个人、组织、数据之间的数字信任关系，并通过这种信任关系为确保个人数据授权流通过程中的安全性和可信性。包含但不限于以下方面：

a) 应要求参与机构以企业注册信息或法人信息通过准入方式申领分布式数字身份；
b) 应要求数据主体以国家法定身份证件信息通过实人认证方式申领分布式数字身份；
c) 应要求各参与方安全存储分布式数字身份私钥。

7.4 个人数据授权技术要求

个人数据授权技术要求明确用数场景，避免“一揽子授权”现象，确保个人数据授权过程中的透明度和合规性。包含但不限于以下方面：

a) 应严格审查用数场景，并根据用数场景生成清晰的个人数据授权协议，协议内容应包括协议签署主体、协议必要性约定和非必要性约定，明确告知协议授权内容，防止概括性授权；

b) 应遵循“一次一授权、一事一授权”的原则，确保数据主体可以对其个人数据的使用进行精确控制；

c) 在个人数据授权协议展示中，应采取适合的交互设计确保数据主体能够充分理解授权内容。如独立的弹窗、下滑查看详情的嵌套网页等方式。

7.5 个人授权可信技术要求

个人授权可信技术要求确保授权操作的安全性和不可抵赖性。包含但不限于以下方面

a) 在个人数据授权中，应采用‘opt-in’选择加入模式，意味着数据主体必须明确同意个人数据授权协议，而不是通过通知或隐式同意的方式；

b) 应采用符合国家要求的数字签名技术，确保个人授权行为的不可否认和可追溯到真实身份；

c) 宜配合其他认证方式加强个人授权行为的不可否认性，如通过生物识别技术、短信验证码认证、签署口令等。

7.6 个人数据安全与隐私保护技术要求

个人数据安全与隐私保护技术要求确保在个人数据的整个生命周期中，包括收集、存储、授权访问、传输和使用等环节中，个人数据的安全性和隐私性能得到妥善保护。包含但不限于以下方面：

a) 应使用符合国家要求的密码技术来进行个人数据安全保护；

b) 应要求在个人数据收集中，需确保其采集的个人数据来源合法合规；

c) 应要求在个人数据存储中，需采用安全隔离、容灾备份等方式对个人数据进行安全保护，以防止个人数据的丢失和损坏；

d) 应要求在个人数据授权访问中，需防止个人数据遭受未授权访问、泄露和其他安全风险，确保只有经过数据主体授权的数据使用才能访问获取；

e) 应要求在个人数据传输中，需采用安全协议和加密技术来保护个人数据的传输安全性；

f) 应要求在个人数据使用中，需遵守相关法律法规、尊重数据主体的权益，确保个人数据处理活动的合法性和合规性。

7.7 全流程监管与审计技术要求

全流程监管和审计技术要求在个人数据授权流通中建立安全审计和溯源机制，保障个人数据流通过程中的安全性和合规性。包含但不限于以下方面：

a) 应要求在个人数据流通过程中的安全性、合规性进行全面审查和评估，达到及时发现并纠正个人数据流通中的安全问题，确保个人数据在流通中的安全可控；

b) 应要求在个人数据在流通过程中的来源、流向、授权、使用等行为操作进行记录和追踪。

附 录 A
（规范性）
数据目录注册机制

A.1 数据提供方注册数据目录流程

数据目录注册流程见图C.1。

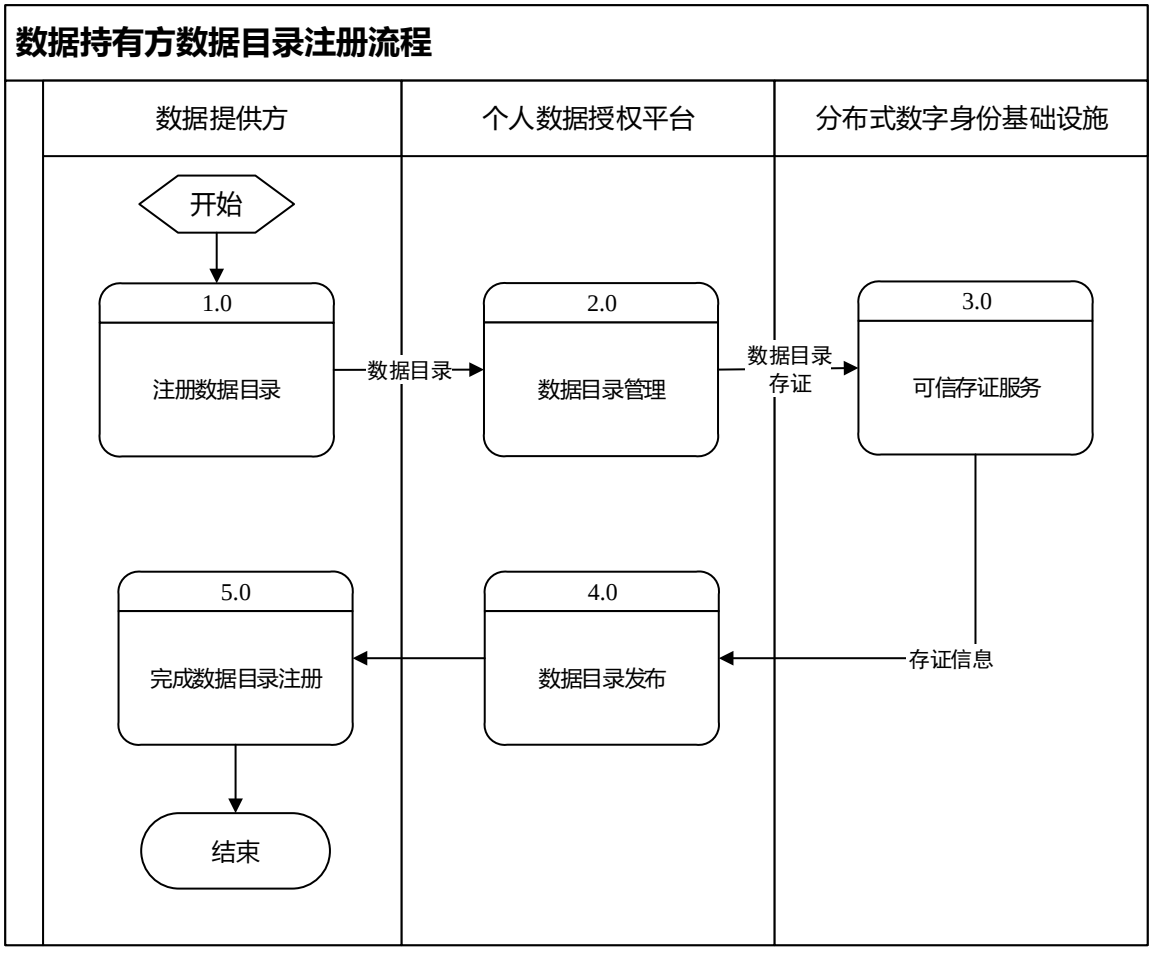

图 C1：数据目录注册流程

流程说明如下：

a) 【数据提供方】依据其持有的个人数据元数据信息，向【个人数据授权平台】注册数据目录；

b) 【个人数据授权平台】创建数据目录，并向【分布式数字身份基础设施】进行数据存证后，上架发布数据目录；

c) 【数据使用方】通过检索、查询已发布数据目录，流程结束。

附 录 B
（规范性）
个人数据授权机制

B.1 个人数据授权协议范本

个人数据授权协议范本参考宜包括以下部分内容：

（一）协议签署主体

个人数据授权协议须由数据主体进行签署，如授权场景需要协议中提供数据来源及授权合规性声明、数据使用方承诺等内容的，数据提供方或数据使用方应一并进行协议签署。

（二）协议必要性约定

个人数据授权协议必要性条款应当包含以下内容：

（1）直接授权、间接授权：数据主体授权数据提供方为直接授权，数据主体授权数据使用方为间接授权。

（2）授权信息[字段]

（3）数据来源合规性声明

（4）授权信息用途

（5）授权时效性

（6）授权撤销条款

（7）数据修改权限及用途

（8）数据复制权限及用途

（9）数据删除

（三）协议非必要性约定

（1）数据存储条款

（2）数据计算说明

（3）数据第三方输出条款（未约定则不得输出）

（4）数据安全措施

（5）数据加工产品的知识产权说明

（6）隐私及商业秘密的额外约定

B.2 个人数据授权流程

个人数据授权流程见图D.2。

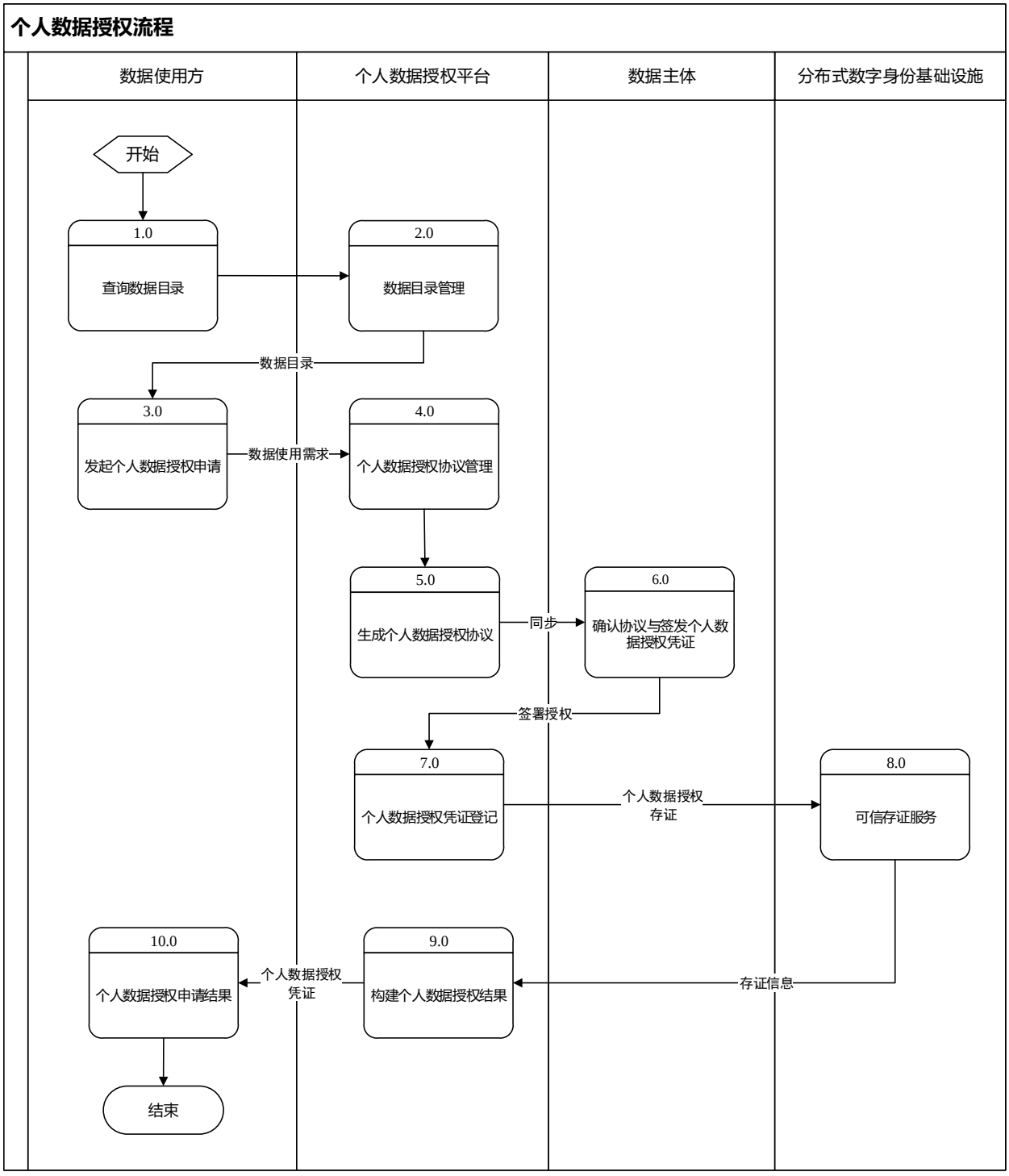

图 D2：个人数据授权流程

流程说明如下：

a）【数据使用方】向【个人数据授权平台】检索、查询数据目录信息，【个人数据授权平台】返回已上架的数据目录数据；

b）【数据使用方】依据自身业务需求，向【个人数据授权平台】发起所需数据目录对应的个人数据授权申请；

c）【个人数据授权平台】依据个人数据授权申请，对【数据使用方】进行用数审核，生成个人数据授权协议，并向【数据主体】同步个人数据授权协议发起个人数据授权申请；

d) 【数据主体】通过 APP、H5 等方式知悉个人数据授权协议内容，使用分布式数字身份签发个人数据授权凭证；

e) 【个人数据授权平台】接收【数据主体】个人数据授权凭证后，向【分布式数字身份基础设施】进行授权存证登记，并返回个人数据授权凭证给【数据使用方】，流程结束。

附 录 C
（规范性）
个人数据授权验证机制

C.1 个人数据授权验证流程

个人数据授权验证流程见图E.1。

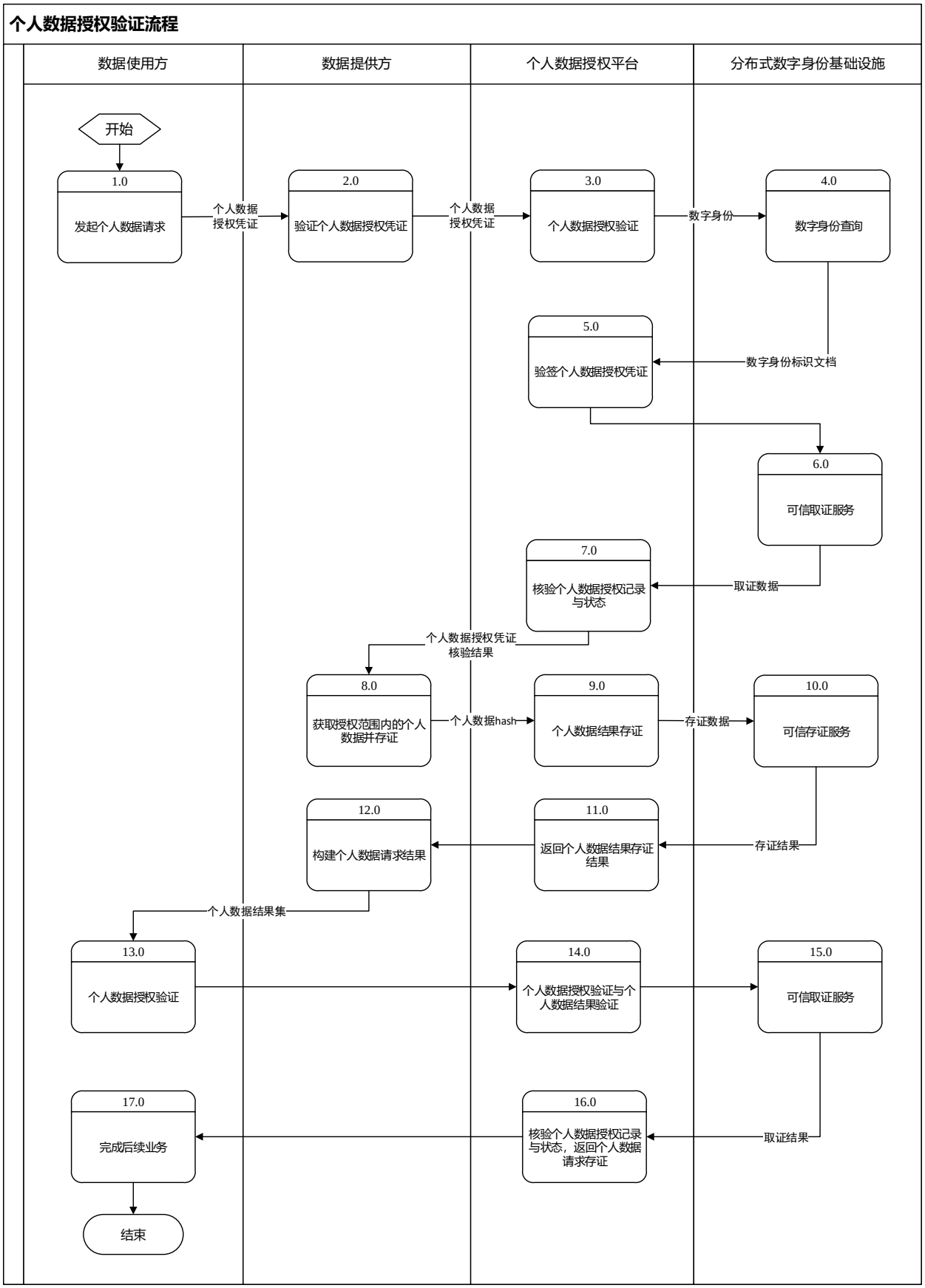

图 E1：个人数据授权验证流程

流程说明如下：

a)【数据使用方】获取到个人数据授权凭证后，向【数据提供方】发起个人数据请求，获取已授权的个人数据；

a)【数据提供方】接收到个人数据请求，向【个人数据授权平台】进行个人数据授权凭证验证；

b)【个人数据授权平台】向【分布式数字身份基础设施】获取【数据主体】分布式数字身份信息，通过公钥信息验证个人数据授权凭证的真实性，向【分布式数字身份基础设施】获取个人数据授权记录状态信息，验证个人数据授权凭证的有效性；

c)【数据提供方】接收个人数据授权凭证的验证结果后，查询【数据主体】已授权的个人数据并计算数据 hash 值，向【个人数据授权平台】进行个人数据结果存证；

d)【个人数据授权平台】接收到个人数据结果存证请求后，向【分布式数字身份基础设施】进行可信存证，并返回存证结果；

e)【数据提供方】完成个人数据结果存证，向【数据使用方】返回个人数据请求结果；

f)【数据使用方】接收到个人数据请求结果后，向【个人数据授权平台】发起个人数据授权验证与个人数据结果验证请求；

g)【个人数据授权平台】接收到核验请求后，向【分布式数字身份基础设施】进行可信取证，核验个人数据授权记录状态，获取【数据提供方】完成个人数据结果存证结果，返回核验结果；

h)【数据使用方】接收到核验请求结果后，进行后续业务，流程结束。

参 考 文 献

[1]《中华人民共和国网络安全法》
[2]《中华人民共和国数据安全法》
[3]《中华人民共和国个人信息保护法》
[4]《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》(简称“数据二十条”)
[5]《网络数据安全管理条例》
[6] W3C Recommendation: Decentralized Identifiers (DIDs) v1.0
[7] GB/T 25069-2022 信息安全技术 术语
[8] GB/T 31504-2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范
[9] GB/T 35273 信息安全技术 个人信息安全规范
[10] GB/T 37964 信息安全技术 个人信息去标识化指南
[11] GA/T 1721-xxxx 网络身份认证公共服务 通用术语
[12] ITU-T X.1252 身份管理基准术语和定义
[13] YD/T xxxx-xxxx 数字身份 分布式服务总体框架