国际电联出版物
建议书

国际电信联盟
电信标准化部门

建议书
ITU-T X.1410 (03/2023)

X系列：数据网、开放系统通信和安全性

安全应用和服务（2） – 分布式账本技术（DLT）安全

基于分布式账本技术的数据共享管理的安全架构

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账本技术（DLT）安全	**X.1400–X.1429**
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X. 1410建议书

基于分布式账本技术的数据共享管理的安全架构

摘要

ITU-T X.1410建议书规定了基于分布式账本技术（DLT）的数据共享管理的安全架构。基于该架构，本建议书规定了基于DLT的数据共享管理的功能实体和程序之间的接口。分布式账本技术正在以创新的解决方案改变行业，并改变政府、机构和企业的运作方式。其去中心化和防篡改特性提供了一种在分布式计算机网络上安全复制、共享和同步数据的解决方案。当前用于与公司和数字平台共享商业数据和个人可识别信息（PII）数据的方法存在着漏洞，容易受到黑客攻击或糟糕数据管理泄露隐私数据。在数据共享管理中采用DLT或区块链允许个人或公司对其机密信息保持更直接的控制。在基于DLT的解决方案中，只有非PII数据（例如散列数据值）被存储在链上，而关于数据所有者的PII数据存储在链外。基于DLT的解决方案为改善数据状态的可追溯性、可验证性和可更改性提供了一种方法。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1410	2023-03-03	17	11.1002/1000/15109

关键词

数据共享、DLT、安全架构。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联没有收到实施本建议书可能需要的受专利/软件版权保护的知识产权通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询可通过ITU-T网站获得的适当的ITU-T数据库，网址为：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X. 1410号建议书

基于分布式账本技术的数据共享管理的安全架构

1 范围

本建议书阐述了基于DLT的数据共享安全架构。本建议书包括：

– 基于分布式账本技术（DLT）的数据共享安全架构设计；

– 数据共享安全架构的逻辑功能规范；

– 安全架构的逻辑功能之间的接口规范；

– 基于DLT的数据共享程序规范。

2 参引

下列ITU-T建议书及其它参引含有通过本文的引用构成本建议书条款的条款。所注明版本在出版时有效。所有建议书及其它参引均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参引的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1408] ITU-T X.1408 (2021)建议书，基于分布式账本技术的数据访问和共享的安全威胁和要求。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 地址（address）[b-ITU-T FG DLT D1.1]：在区块链或分布式账本网络中执行交易处理或其它活动的实体标识符。

3.1.2 区块链（blockchain）[b-ITU-T X.1400]：一种分布式账本，由数字记录的数据组成，这些数据按连续增长的数据块链排列，每个数据块都以密码方式链接在一起，并经过加固以防止篡改和修改。

3.1.3 认证机构（certification authority）（CA）[b-ITU-T X.509]：被一个或多个实体所信任的机构，用于创建并以数字方式签署公开密钥证书。可选地，认证机构还可以选择创建用户密钥。

3.1.4 数据提供者（data provider）[b-ISO/IEC/IEEE 15939]：作为数据来源的个人或组织。

3.1.5 身份（识别）（identity）[b-ISO/IEC 29100]：可用以识别个人可识别信息主体的一组属性。

3.1.6 链下（off-chain）[b-ISO 22739]：与区块链系统有关、但在区块链系统外定位、执行或运行。

3.1.7 链上（on-chain）[b-ISO 22739]：在区块链系统内定位、执行或运行。

3.1.8 个人可识别信息（personally identifiable information）（PII）[b-ISO/IEC 29100]：(a) 可用于识别相关信息与之关联的PII主体的任何信息；或者 (b) 直接或间接或者可能直接或间接与PII主体联系起来的任何信息。

注 – 为确定一个PII主体是否可识别，应考虑持有该数据的私密性利益攸关方或任何其他方可合理使用的所有手段，以确定该自然人。

3.1.9 公开密钥基础设施（public-key infrastructure）（PKI）[b-ITU-T X.509]：能够支持公开密钥管理的、能够支持鉴权、加密、完整性或不可否认服务的基础设施。

3.1.10 智能合约（smart contract）[b-ITU-T X.1400]：在分布式账本系统上编写的程序，该程序以一种可验证的方式为特定类型的分布式账本系统交易编码规则，并由特定条件触发。

3.1.11 对称加密系统（symmetric encryption system）[b-ISO/IEC 18033-1]：用于保护数据机密性的加密技术，由三个组成流程：加密算法、解密算法和密钥生成方法，其中加密算法和解密算法使用相同的密钥。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 数据消费者（data consumer）：读取数据，然后在发现词法或编码边界的范围内处理数据的用户。

注 – 改编自[b-ISO/IEC 20944-1]。

4 缩写词和首字母缩略语

本建议书使用了以下缩写词和首字母缩略语：

API 应用程序编程接口

CA 认证机构

DLT 分布式账单技术

PII 个人可识别信息

PKI 公共密钥基础设施

5 惯例

在本建议书中：

关键词**“建议”**（**is recommended**）指的是一项建议性的、并非绝对需遵守的要求，因此，宣称遵循本建议书时无需提及该项要求。

关键词**“可”**（**can**）和**“选”**（**optionally**）指的是一项允许的可选要求，不隐含任何建议的意味。本术语无意暗示供应商的实施方案必须提供选项，以及网络运营商/服务提供商可以选择启用该功能。相反地，本术语意味着供应商可以选择提供该功能，并仍宣称遵循规范。

本建议书使用*楷体*表示功能。

6 基于DLT的数据共享架构

分布式账单技术的去中心化和防篡改特性为在分布式计算机网络上安全地复制、共享和同步数据提供了解决方案。当前用于与公司和数字平台共享商业数据和个人可识别信息（PII）数据的方法已造成来自黑客攻击或糟糕数据管理的隐私漏洞。在数据共享管理中采用DLT或区块链允许个人或公司对其机密信息保持更直接的控制。在基于DLT的解决方案中，只有非PII数据（如散列数据值）被存储在链上。数据所有者的PII数据存储在链外。基于DLT的解决方案提供了一种提高数据状态的可追溯性、可验证性和可更改性的方法。在此背景下，本建议书规定了基于DLTs的数据共享管理的安全架构。数据共享管理利用对称加密系统，其中加密和解密算法使用相同的密钥。在[ITU-T X.1408]中描述了安全威胁。

本建议书是基于[ITU-T X.1408]制定的。虽然[ITU-T X.1408]是从概念的角度设计的，但本建议书是从实施的角度制定的。本建议书和[ITU-T X.1408]之间的术语对照如表1所示。

表1 – 本建议书和[ITU-T X.1408]之间的术语对照

本建议书	[ITU-T X.1408]
数据提供者	数据共享代理（数据所有者）
数据消费者	数据消费者客户端（数据处理器）
密钥存储服务器	密钥管理服务器
数据存储服务器	数据存储服务器（数据存储服务提供商）
基于DLT的数据共享管理	数据代理

6.1 功能架构概述

图1从实施的角度说明了基于DLT的数据共享管理的功能架构。这与[ITU-T X.1408]图B.1所示的基于DLT的数据访问和共享架构是一致的。后者是从概念角度设计的，是一种高级架构。图1中的功能架构由五个蓝色功能组件和三个灰色功能组件组成。

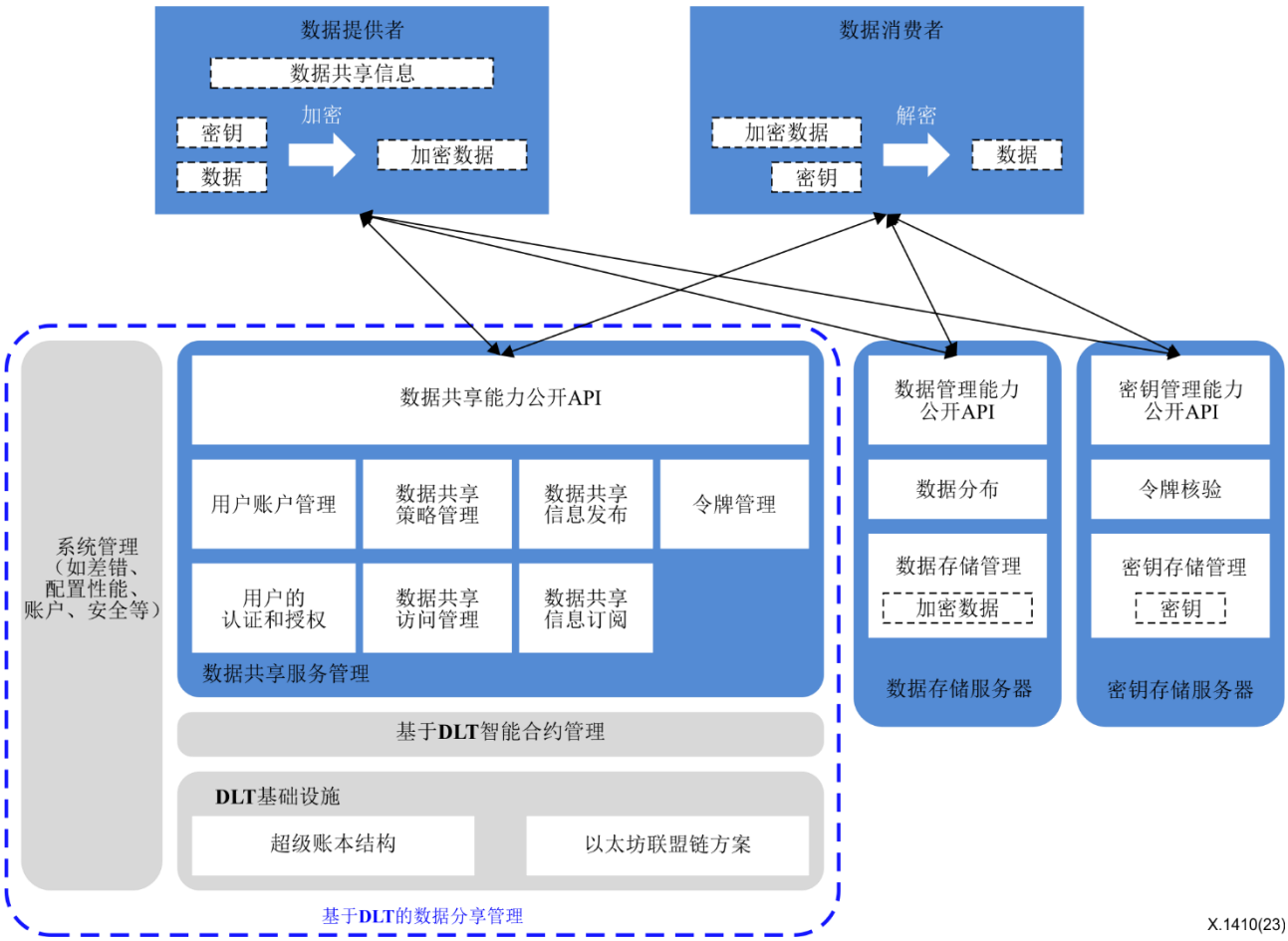


图1 – 基于DLT的数据共享管理的功能架构

这些组件描述如下：

– 五个蓝色功能组件是*数据提供者*、*数据消费者*、*数据共享服务管理*、*密钥存储服务器*和*数据存储服务器*，在6.2条中有详细定义和描述。

– 三个灰色功能组件是DLT*基础设施*、*基于*DLT*的智能合约管理*和*系统管理*（如故障、配置、性能、账户、安全），它们重用现有的开源DLT平台（如超级账本架构），不在本建议的范围内。

DLT的数据共享管理程序参见附件A。

6.2 功能组件

6.2.1 数据提供者和数据消费者

本建议书引入了两种类型的用户：数据提供者（即共享其数据的用户）和数据消费者（即消费其他用户共享数据的用户）。两种类型具有同样的功能：

1) 从认证机构（CA）取得数码证书（包括公开密钥）及相应的私钥；

2) 安全地存储获得的数字证书和相应的私钥；

3) 与基于DLT的数据共享管理服务器通信；

4) 获取并存储DLT网络节点的数字证书、网络参数和网络配置；

5) 接收来自基于DLT的数据共享管理的通知；

6) 利用对称加密系统。

数据提供者和数据使用者有自己的特定功能，如下所示：

– *数据提供者*具有以下功能：

1) 收集原始数据并降低其敏感性（例如，使数据匿名，删除姓名、手机号码、信用卡数据等敏感信息），而不会对要共享的数据质量产生负面影响；
2) 生成对称加密系统的密钥；
3) 使用对称加密系统用密钥加密数据；
4) 将密文和相应的加密密钥安全地存储在本地或远程服务器上；
5) 确保与基于DLT的数据共享管理的相互认证；
6) 向基于DLT的数据共享管理提供数据共享信息，包括数据提供者标识符、数据提供者公钥、密文标识符及其存储地址、加密密钥标识符及其存储地址、允许访问的行业、允许访问的用户以及其他数据属性（例如，数据类别、数据介绍、用途和价格）；
7) 将数据共享信息和其他信息结合形成数据共享策略，然后用私钥签署数据共享策略；
8) 将带有相应数字签名的数据共享策略发送到基于DLT的数据共享管理；
9) 接收来自基于DLT的数据共享管理的通知，该通知示意数据共享的智能合约已经被创建；
10) 管理数据共享策略，如查询和更新。

– *数据消费者*具有以下功能：

1) 订阅发布的数据共享消息；
2) 确保与基于DLT的数据共享管理的相互认证；
3) 获取数据共享信息；
4) 将数据消费者信息（例如，数据消费者身份、数据消费者公钥）和共享数据信息（例如，数据提供者身份、数据提供者公钥、密文标识符和加密密钥标识符）连同数字签名（由数据消费者私钥完成）一起发送到基于DLT的数据共享管理；
5) 从基于DLT的数据共享管理接收包括共享数据信息、密钥存储地址、密文存储地址和访问令牌的通知；
6) 向密钥存储服务器发送访问令牌，以便根据密钥存储地址获得数据加密密钥；
7) 根据数据存储地址得到密文；
8) 用获得的对称加密系统的密钥解密密文，得到明文数据；
9) 管理访问共享数据的记录。

6.2.2 数据共享服务管理

数据共享服务管理的每个组件的功能介绍如下。

– ***用户帐户管理***能够管理用户账户，如创建、更新、查询和删除。

– ***用户的身份验证与授权***具有以下功能：

1) 执行与用户（即，数据提供者、数据消费者）的相互认证；
2) 授权用户共享数据和访问共享数据。

– **数据共享策略管理**具有以下功能：

1) 从数据提供者接收数据共享信息和数据共享策略以及相应的数字签名；
2) 根据从数据提供者接收的信息创建DLT交易；
3) 将DLT交易提交给底层组件（即，DLT基础设施和智能合约管理）以创建数据共享智能合约，该合同将被分发到DLT网络节点；
4) 通知数据提供者和数据共享信息发布已经创建了数据共享智能合约；
5) 使数据提供者能够管理他们的共享数据。

– **数据共享访问管理**具有以下功能：

1) 接收来自数据消费者的数据访问请求（包括数据消费者信息、共享数据信息和相应的数字签名），并检查根据数据共享策略是否允许数据消费者访问数据（例如，只有来自指定行业或国家的数据消费者可以访问共享数据）；
2) 根据从数据消费者接收的信息创建DLT交易；
3) 将DLT交易提交给底层组件（例如，DLT基础设施）以记录数据访问，该数据访问将被分发到DLT网络节点；
4) 通知令牌管理已经创建了数据访问交易，并且将创建访问令牌；
5) 从令牌管理接收接入令牌；
6) 向数据消费者发送数据共享访问信息（例如，访问令牌、密钥存储地址、数据存储地址）；
7) 使数据消费者能够管理他们的数据共享访问记录。

– **数据共享信息发布**具有以下功能：

1) 接收来自数据共享策略管理的通知，其包含新的数据共享信息；
2) 发布新的数据共享信息；
3) 通知数据共享信息订阅发布了新的数据共享信息。

– **数据共享信息订阅**具有以下功能：

1) 接收来自数据共享信息管理的通知，其包含新的数据共享信息；
2) 向订户发送新的数据共享信息。

– **令牌管理**具有以下功能：

1) 从数据共享访问管理接收通知以创建访问令牌；
2) 创建访问令牌；
3) 将创建的访问令牌发送给数据共享访问管理。

– **数据共享功能公开应用程序编程接口（API）**使用户能够如上所述管理和访问数据共享服务。

6.2.3 密钥存储服务器

密钥存储服务器中每个组件的功能描述如下。

– **密钥存储管理**具有以下功能：

1) 从数据提供者接收存储密钥的请求；

2) 对*数据提供者*进行认证；

3) 安全地存储密钥，例如，将密钥存储在密文和/或隔离存储中；

4) 通知*数据提供者*密钥已经被存储；

5) 接收来自*令牌验证*的通知，该通知指示接入令牌的验证结果；

6) 将密钥发送给*数据消费者*。

– ***令牌验证***具有以下功能：

1) 从数据消费者接收访问令牌；

2) 验证接收到的访问令牌；

3) 将验证结果发送给*密钥存储管理*。

– ***密钥管理功能公开API***使用户能够管理和访问数据加密密钥。

6.2.4 数据存储服务器

数据存储服务器中每个组件的功能描述如下。

– ***数据存储管理***具有以下功能：

1) 接收来自*数据提供者*的存储密文的请求；

2) 对*数据提供者*进行认证；

3) 存储密文；

4) 通知*数据提供者*密文已经被存储。

– ***数据分布***具有以下功能：

1) 接收来自*数据消费者*的请求；

2) 对*数据消费者*进行认证；

3) 密文发送给*数据消费者*。

– ***数据管理功能公开API***使用户能够管理和访问共享数据。

7 基于DLT的数据共享管理的安全架构

根据图1中的功能架构，数据消费者请求并接收一个数据加密密钥，然后用它解密密文数据，最后获得明文共享数据。之后，明文共享数据就不能被基于DLT的数据共享管理控制了。数据消费者可能会以明文形式将共享数据转发给没有权限访问它的其他用户。

为了支持数据提供者安全地与他人共享数据，并防止数据消费者将共享的数据以明文形式转发给其他用户，图1中的功能架构需要增强的安全特性，如图2所示。

7.1 安全架构概述

图2描述了基于DLT的数据共享管理的安全架构，它确保：

– 图1中功能组件之间的通信是安全的；

– 数据提供者对数据进行加密，并在与他人共享之前设置访问权限；

– 数据消费者在访问之前根据访问权限对密文形式的共享数据进行解密；

– 数据消费者在完成数据访问后，按照与数据提供者相同的方式对共享数据进行加密，这样数据消费者以密文形式存储共享数据；

– 数据消费者只将密文形式的共享数据转发给其他人。

这样，即使用户收到了其他人转发的共享数据，他们也必须向位于DLT的数据共享管理机构请求访问权限。

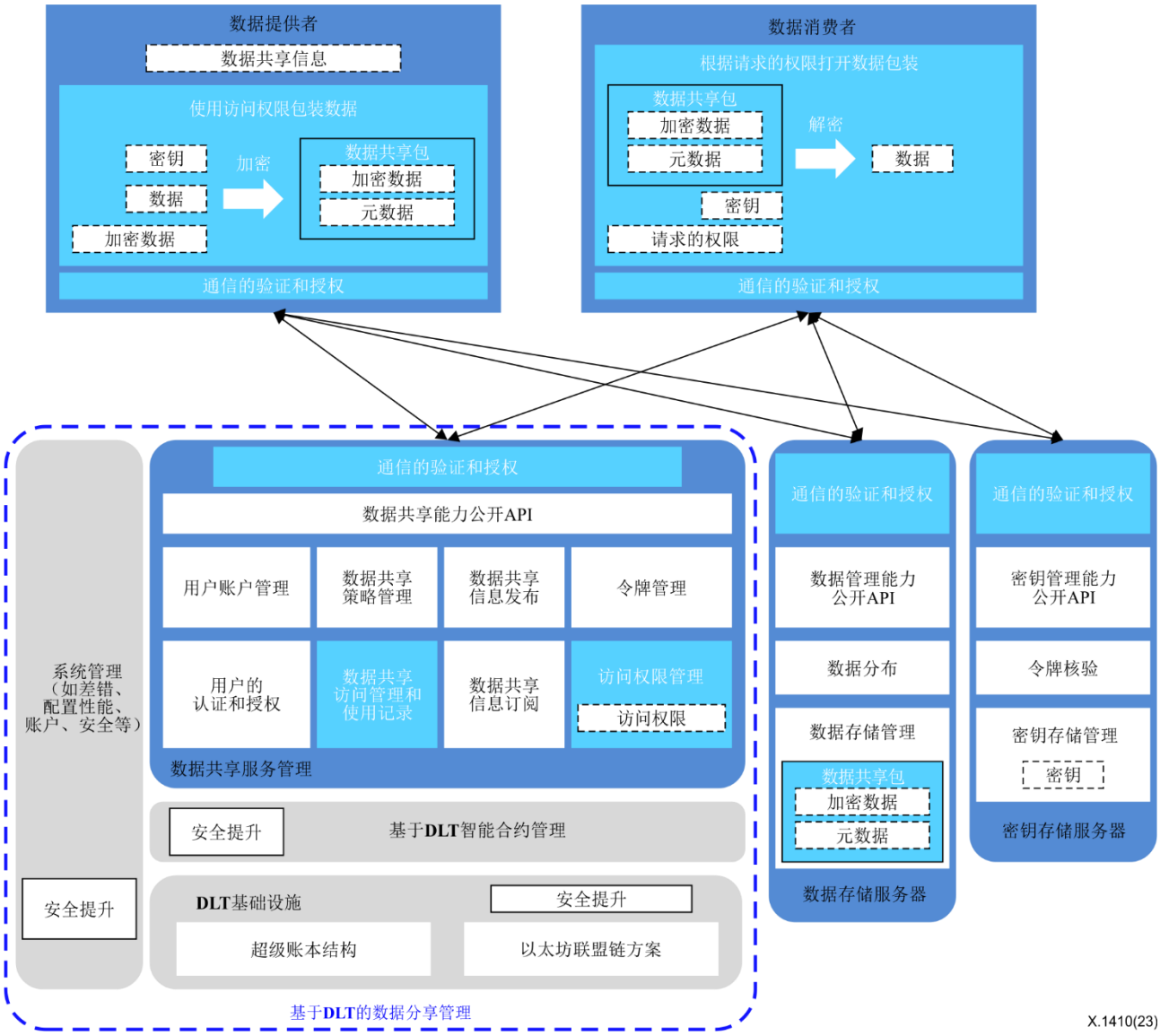


图2 – 基于DLT的数据共享管理的安全架构

与图1不同，图2包含淡蓝色背景的功能组件，它们是逻辑安全功能，在第7.2条中有详细描述。

本建议书没有介绍图2中三个灰色功能组件的安全性增强；参见[b-ITU-T X.1402]。

7.2 安全功能组件

7.2.1 用访问权限包装数据

为支持用户为要共享的数据设置访问权限，需要通过引入新的逻辑安全功能来增强图1中的*数据提供者*，该功能将数据与*访问权限*包装在一起，具有以下功能：

– 生成对称加密系统的密钥，用于加密要共享的数据；

– 与*密钥存储服务器*通信以注册密钥标识符和获取它的地址；

– 与数据存储服务器通信以注册数据共享包标识符和获取它的地址；
– 设置共享数据的访问权限，包括访问次数、到期时间、只读、密钥标识符及其存储地址、数据共享包标识符及其存储地址；
– 生成元数据，包括数据共享包标识符、数据提供者标识符、数据提供者的公共密钥和前述信息的签名；
– 生成包括加密数据和元数据的数据共享包；
– 通过安全传输通道将密钥上传到密钥存储服务器；
– 通过安全传输通道将数据共享包上传到数据存储服务器；
– 通过安全传输通道将访问权限上传至数据共享服务管理。

7.2.2 根据要求的权限展开数据

为支持用户根据请求的权限访问共享数据，需要通过引入新的逻辑安全功能来增强图1中的数据消费者，根据请求的权限展开数据，该功能具有以下功能：

– 获取执行数据共享智能合约的地址；
– 与数据共享服务管理通信，执行数据共享智能合约并获得所请求的许可，包括访问次数、到期时间、只读、密钥标识符及其存储地址、数据共享包标识符及其存储地址；
– 与密钥存储服务器通信以获得加密密钥；
– 与数据存储服务器通信以获得包括加密数据和元数据的数据共享包；
– 基于元数据中的签名验证收到的数据共享包；
– 基于加密密钥解密加密的数据；
– 根据所请求的许可，以明文形式向用户呈现共享数据；
– 在完成数据访问后，以与数据提供者相同的方式加密共享数据。

7.2.3 访问权限管理

为支持用户设置对共享数据的访问权限，或者支持用户根据所请求的权限访问共享数据，需要通过引入新的逻辑安全功能（访问权限管理）来增强图1中的数据共享服务管理，该功能具有以下能力：

– 支持用户设置共享数据的访问权限：
  • 从数据共享策略管理收到由数据提供者设置的访问权限；
  • 存储访问权限；
  • 发送对数据共享策略管理的响应；
– 支持用户根据请求的权限访问共享数据：
  • 从数据共享访问管理和使用记录中接收数据消费者请求的许可；
  • 生成所要求的权限；
  • 向数据共享访问管理和使用记录发送所请求的许可。

7.2.4 数据共享访问管理和使用记录

为支持用户跟踪其共享数据的使用情况，图2中的数据共享访问管理和使用记录需要通过以下功能进行增强：

– 与访问权限管理进行通信，以便获得所请求的权限；

– 根据所请求的许可记录共享数据的使用情况。

7.2.5 通信的验证与授权

为了确保通信安全，图1中的五个功能组件（即数据提供者、数据消费者、数据共享服务管理、密钥存储服务器和数据存储服务器）需要通过引入新的逻辑安全功能，通信的验证与授权来增强。

当数据提供者或数据消费者向数据共享服务管理、密钥存储服务器或数据存储服务器发送请求消息时，通信的验证与授权可以支持：

– 数据共享服务管理/密钥存储服务器/数据存储服务器基于证书[b-IETF RFC 4306]、[b-IETF RFC 5246]或预共享密钥[b-IETF RFC 4279]、[b-IETF RFC 4306]验证数据提供者/数据消费者；

– 数据提供者/数据消费者基于证书[b-IETF RFC 4306]、[b-IETF RFC 5246]验证数据共享服务管理/密钥存储服务器/数据存储服务器；

– 数据共享服务管理/密钥存储服务器/数据存储服务器基于白名单/黑名单[b-IETF RFC 5782]、[b-IETF RFC 5851]或访问控制列表[b-IETF RFC 4314]、[b-IETF RFC 4949]授权数据提供者/数据消费者；

– 生成会话密钥，该密钥将用于保护数据提供者/数据消费者与数据共享服务管理/密钥存储服务器/数据存储服务器之间的通信。

7.3 安全共享数据的程序

7.3.1 数据提供者共享数据并设置访问权限的程序

数据提供者通过设置访问权限来共享数据的程序如图3所示。

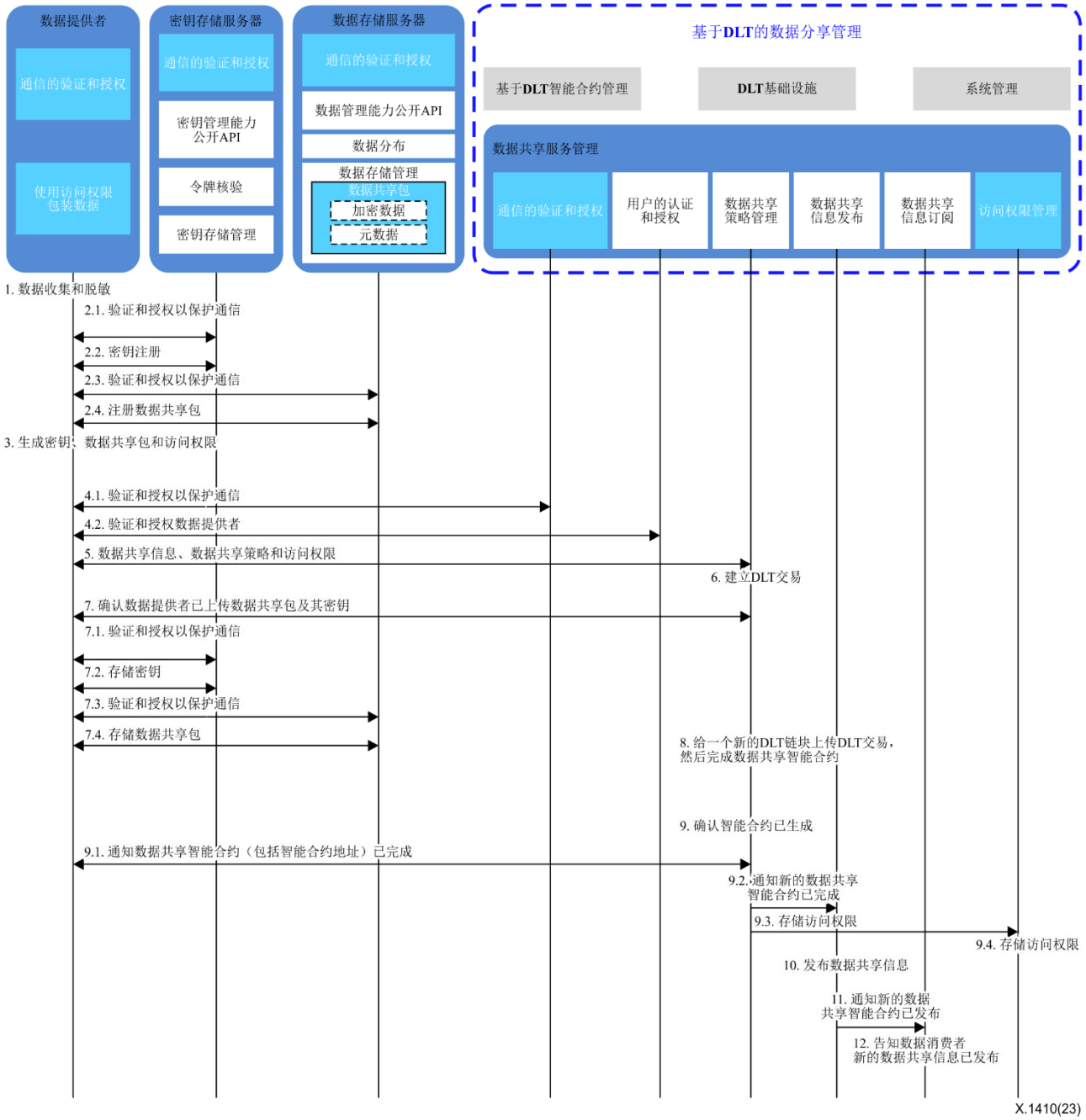


图3 – 数据提供者通过设置访问权限来共享数据的程序

如图3所示，程序描述如下。

1) 数据提供者收集原始数据并降低其敏感度，而不会对共享数据的质量产生负面影响。

2) 数据提供者在本地或远程密钥存储服务器和数据存储服务器上注册数据共享包及其密钥，如下所示：

2.1) 数据提供者和密钥存储服务器的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥；

2.2) 数据提供者连接到密钥存储服务器，注册密钥标识符并从中获取它的地址；

2.3) 数据提供者和数据存储服务器的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥；

2.4) 数据提供者连接到数据存储服务器，注册数据共享包标识符并获取它的地址。

3) 数据提供者创建数据共享信息，该信息包括数据提供者标识符、数据提供者公钥、数据共享包标识符及其存储地址、密钥标识符及其存储地址、允许访问的行业、允许访问的用户以及其他数据属性（例如，数据类别、数据介绍、用途和价格）。

数据提供者生成一个密钥，用于加密要共享的数据。

数据提供者设置数据的访问权限，包括访问次数、到期时间、只读、密钥标识符及其存储地址、要共享的数据共享包标识符及其存储地址；

数据提供者生成元数据，该元数据包括数据共享包标识符、数据提供者标识符、数据提供者公钥和前述信息的签名；

数据提供者生成包括加密数据和元数据的数据共享包。

4) 在发布要共享的数据之前，需要：

4.1) 数据提供者和数据共享服务管理的通信验证与授权，以进行相互验证并获得用于保护它们之间后续通信的会话密钥。

4.2) 数据提供者和数据共享服务管理的用户进行相互验证和授权。相互验证成功后，用户验证与授权组件检查数据提供者是否有权发布要共享的数据。

5) 数据提供者根据数据共享服务管理的数据共享策略管理的要求提供数据共享信息。数据提供者创建包含数据共享和其他信息的数据共享策略。数据提供者将数据共享信息、数据共享策略、访问权限及其数字签名发送给数据共享策略管理。

6) 在从数据提供者接收到数据共享信息、数据共享策略、访问许可和相应的数字签名之后，数据共享策略管理验证数字签名，然后创建DLT交易。

7) 数据共享策略管理向数据提供者确认密钥和数据共享包已经分别存储在密钥存储服务器和数据存储服务器上。如果没有，需要采取以下步骤：

7.1) 数据提供者和密钥存储服务器的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥；

7.2) 数据提供者连接到密钥存储服务器并将密钥存储在其上；

7.3) 数据提供者和数据存储服务器的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥；

7.4) 数据提供者连接到数据存储服务器，并将数据共享包存储在其上。

8) 数据共享策略管理将一个或多个DLT交易连同它们的数字签名一起发送到底层组件DLT基础设施和基于DLT的智能合约管理，以形成包含用于数据共享的一个或多个智能合约的新块。新生成的块被分发到相关联的DLT节点。将DLT交易加载到DLT链取决于底层的具体实施技术（如超级账本架构、Ethereum Quorum），此内容超出了本建议书的范围。

9) 数据共享策略管理通知相关组件已经创建了用于数据共享的智能合约。

9.1) 数据共享策略管理通知数据提供者数据共享智能合约已经完成。该通知包括用于执行智能合约的地址。

9.2) 数据共享策略管理通知数据共享信息发布，数据共享智能合约已经完成。该通知包括用于执行智能合约的地址和数据共享信息。

9.3) 数据共享策略管理通知访问权限管理，数据共享智能合约已经完成。该通知包括用于执行智能合约的地址和访问许可。

9.4) 访问权限管理存储访问权限。

10) 在接收到数据共享策略管理的通知后，数据共享信息发布发布接收到的新数据共享信息。

11) 数据共享信息发布通知数据共享信息订阅，用于数据共享的智能合约已经完成。该通知包括用于执行智能合约的地址和新的数据共享信息。

12) 数据共享信息订阅方收到数据共享信息发布的通知后，将执行智能合约的地址和新的数据共享信息发送给订阅方。

7.3.2 数据消费者根据请求的权限访问共享数据的程序

数据消费者根据请求的权限访问共享数据的程序如图4所示。

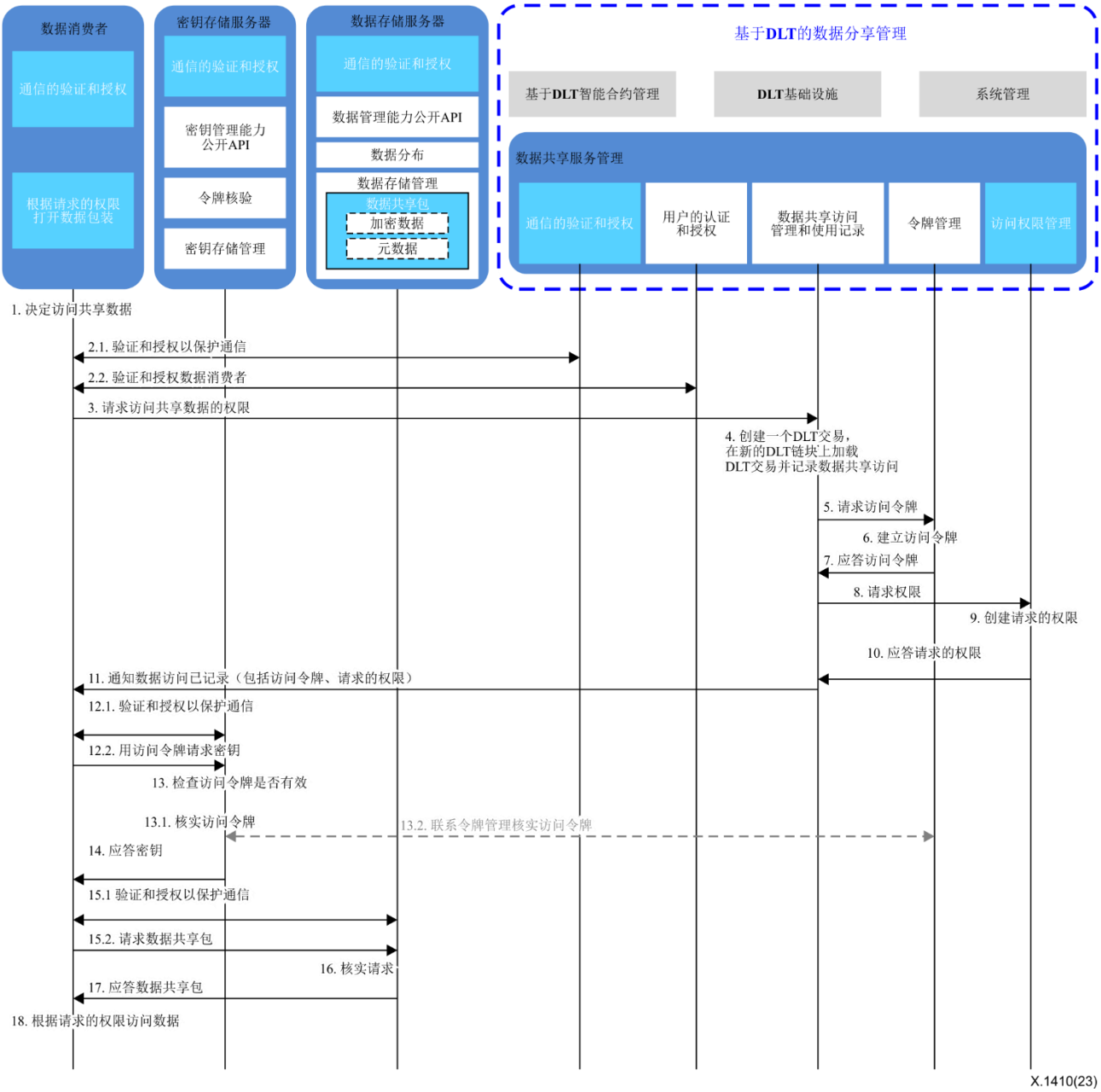


图4 – 数据消费者根据请求的权限访问共享数据的程序

如图4所示，数据消费者根据请求的权限访问共享数据的程序描述如下：

1) 数据消费者通过搜索数据共享信息发布订阅发布信息或他人转发获取数据共享信息。数据消费者决定访问共享数据，并执行数据共享智能合约。数据消费者决定访问共享数据，并执行数据共享智能合约。

2) 在执行数据共享智能合约以访问共享数据之前，执行以下操作。

   2.1) 数据消费者和数据共享服务管理的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥。

   2.2) 数据消费者确保与数据共享服务管理的用户验证与授权组件的相互认证。相互验证成功后，用户验证与授权组件检查数据消费者是否有权访问共享数据。

3) 数据消费者将其身份信息（例如，标识符、公钥）和数据共享信息连同其数字签名一起发送到数据共享访问管理和使用记录。

4) 在接收到数据消费者身份信息、数据共享信息及其数字签名之后，数据共享访问管理和使用记录验证数字签名，然后根据数据共享策略检查是否允许数据消费者访问数据（例如，只有来自指定行业或国家的数据消费者可以访问共享数据）。如果访问共享数据的所有要求都得到满足，则数据共享访问管理和使用记录根据从数据消费者接收的信息创建一个DLT交易。数据共享访问管理和使用记录将一个或多个DLT交易及其数字签名发送到底层组件DLT基础架构和基于DLT的智能合约管理，以形成包含一个或多个数据访问记录的新块。新生成的块被分发到相关联的DLT网络节点。将DLT交易加载到DLT链取决于底层的具体实施技术（如超级账本架构、Ethereum Quorum），此内容超出了本建议书的范围。

5) 数据共享访问管理和使用记录通知令牌管理创建访问令牌。

6) 在接收到来自数据共享访问管理和使用记录的通知后，令牌管理创建访问令牌。

7) 令牌管理将创建的访问令牌发送到数据共享访问管理和使用记录。

8) 数据共享访问管理和使用记录通知访问权限管理创建所请求的权限。

9) 在接收到来自数据共享访问管理和使用记录的通知后，访问权限管理创建所请求的权限。

10) 访问权限管理将请求的权限发送给数据共享访问管理和使用记录。

11) 在接收到访问令牌和所请求的许可之后，数据共享访问管理和使用记录记录共享数据的使用，并将访问令牌、所请求的许可、密钥信息（例如，标识符及其存储地址）、数据共享包信息（例如，标识符及其存储地址）、其他信息（例如，密钥存储服务器和数据存储服务器的数字证书）发送给数据消费者。

12) 在从数据共享访问管理和使用记录接收到访问令牌、请求的许可、密钥信息和数据共享包信息之后，数据消费者执行以下操作：

12.1) 数据消费者和密钥存储服务器的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥；

12.2) 数据消费者根据密钥存储地址将访问令牌发送给密钥存储服务器的令牌验证，获得加密密钥。

13) 密钥存储服务器的令牌验证检查访问令牌是否有效。

13.1) 密钥存储服务器的令牌验证从数据消费者接收访问令牌，然后验证访问令牌。

13.2) 视需要，当验证访问令牌时，令牌验证可能必须与基于DLT的数据共享管理的令牌管理进行通信。

14) 令牌验证将验证结果发送给密钥存储服务器的密钥存储管理。在接收到来自令牌验证的验证结果后，密钥存储服务器的密钥存储管理将密钥发送给数据消费者。

15) 数据消费者从密钥存储服务器的密钥存储管理接收到密钥后，进行如下操作。

15.1) 数据消费者和用于数据存储服务器的通信验证与授权进行相互验证，并获得用于保护它们之间后续通信的会话密钥。

15.2) 数据消费者向数据存储服务器发送请求，以便获得数据共享包。

16) 数据存储服务器的数据分配收到数据消费者的请求后，对数据消费者进行验证。

17) 数据存储服务器的数据分配将数据共享包发送给数据消费者。

18) 数据消费者根据所请求的许可访问数据。数据消费者在完成数据访问后，以与数据提供者相同的方式加密共享数据。

附件A

DLT数据共享管理程序

（此附件是本建议书不可分割的组成部分）

本附录描述了两个主要步骤：1) 数据提供者基于DLT发布要共享的数据；以及2) 数据消费者基于DLT访问共享数据。

在描述基于DLT的数据共享管理程序之前，假设具备以下条件：

– 每个用户（如数据提供者、数据消费者）都获得了一个数字证书及其相应的私钥，该证书由用户自己或从一个CA生成；

– 每个用户都进行了相应的正确配置（如DLT节点的数字证书、DLT网络连接参数、网络配置）；

– 对称加密系统可供用户使用（例如，数据提供者、数据消费者）。它们为数据的保密性提供了足够的加密强度；

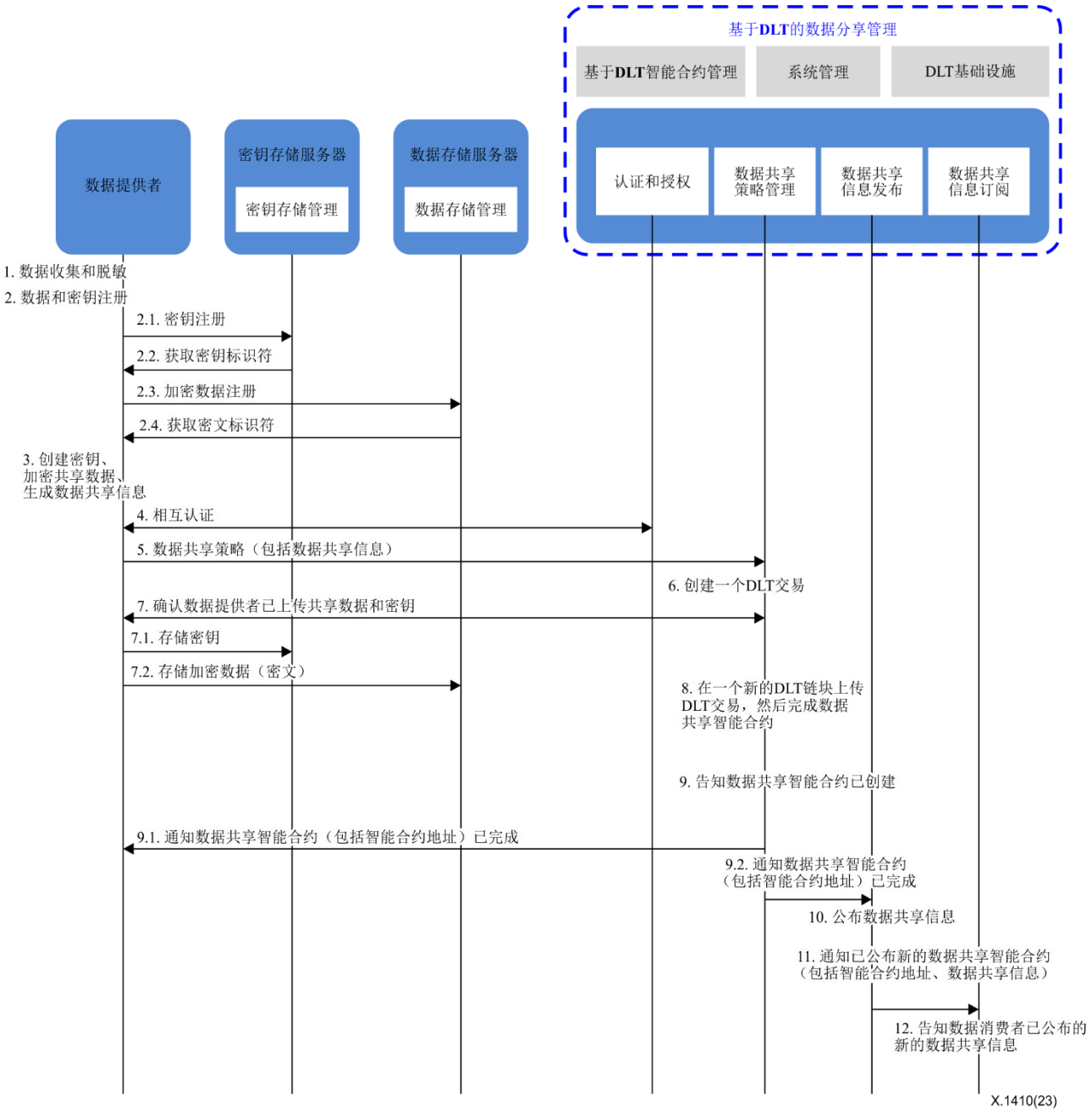
– DLT基础设施和基于DLT的智能合约管理正常工作；

– DLT网络工作正常；

– 密钥存储服务器和数据存储服务器正常工作。

A.1 DLT数据提供者发布基于DLT的共享数据的程序

数据提供者发布基于DLT的共享数据的程序如图A.1所示。



图A.1 – 数据提供者发布基于DLT的共享数据的程序

如图A.1所示，程序描述如下。

1) 数据提供者收集原始数据并降低其敏感度，而不会对要共享的数据质量产生负面影响。

2) 数据提供者在本地或远程密钥存储服务器和数据存储服务器上注册要共享的数据和对称加密系统的密钥，如下所示：

   2.1) 生成用于对称加密系统的数据加密密钥。

   2.2) 数据提供者从密钥存储服务器获得密钥标识符及其存储地址。

   2.3) 使用对称加密系统用密钥加密数据，并注册加密数据，如密文。

   2.4) 数据提供者从数据存储服务器获得密文标识符及其存储地址。

3) 数据提供者生成数据加密密钥，并用生成的加密密钥加密要共享的数据。加密数据就是密文。数据提供者创建数据共享信息，该信息包括数据提供者标识符、数据提供者公钥、密文标识符及其存储地址、数据加密密钥标识符及其存储地址、允许访问的行业、允许访问的用户以及其他数据属性（例如，数据类别、数据介绍、用途、价格）。

4) 在发布要共享的数据之前，数据提供者确保与基于DLT的数据共享管理的用户验证与授权组件的相互认证。凭证数字证书可用于相互验证。相互验证成功后，用户身份验证与授权组件检查数据提供者是否有权发布要共享的数据。

5) 验证和授权成功后，数据提供者根据基于DLT的数据共享管理的数据共享策略管理的要求提供数据共享信息。数据提供者创建包含数据共享和其他信息的数据共享策略。数据提供者将数据共享政策及其数字签名发送给数据共享政策管理。

6) 在从数据提供者接收到数据共享策略和相应的数字签名之后，数据共享策略管理验证数字签名，然后创建DLT交易。

7) 数据共享策略管理向数据提供者确认密钥和密文已经分别存储在密钥存储服务器和数据存储服务器上。如果没有，需要采取以下步骤：

   7.1) 数据提供者将密钥存储在密钥存储服务器上；

   7.2) 数据提供者将密文存储在数据存储服务器上。

8) 数据共享策略管理将一个或多个DLT交易与其数字签名一起发送到底层组件DLT基础设施和基于DLT的智能合约管理，以形成包含一个或多个用于数据共享的智能合约的新块。新生成的块被分发到相关联的DLT节点。将DLT交易加载到DLT链取决于底层的具体实施技术（如超级账本架构、Ethereum Quorum），此内容超出了本建议书的范围。

9) 数据共享策略管理通知相关组件已经创建了用于数据共享的智能合约。

   9.1) 数据共享策略管理通知数据提供者数据共享智能合约已经完成。该通知包括用于执行智能合约的地址。

   9.2) 数据共享策略管理通知数据共享信息发布，数据共享智能合约已经完成。该通知包括用于执行智能合约的地址和数据共享信息。

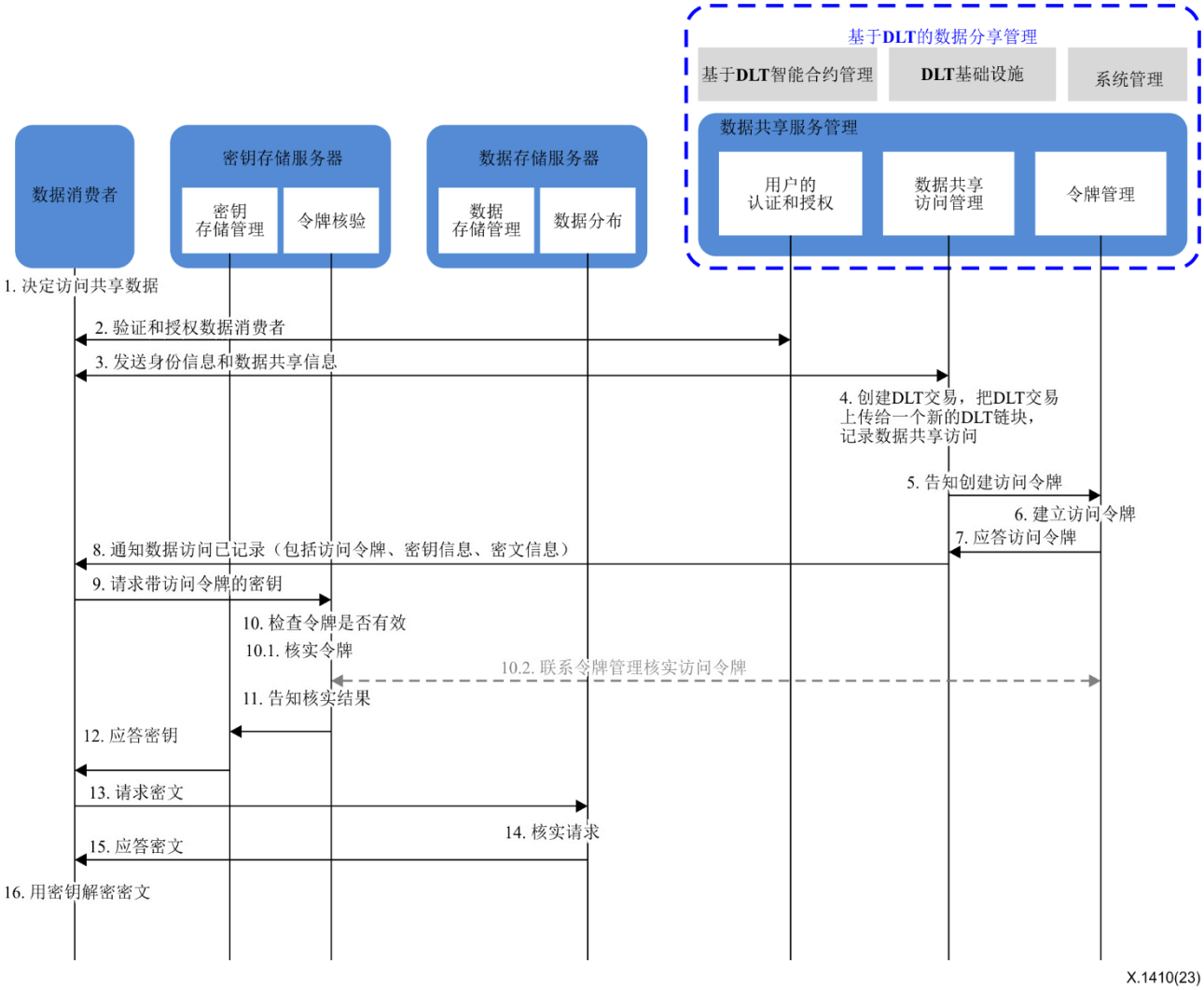
10) 在接收到来自数据共享策略管理的通知后，数据共享信息发布发布接收到的新数据共享信息。

11) 数据共享信息发布通知数据共享信息订阅，数据共享智能合约已经完成。该通知包括用于执行智能合约的地址和新的数据共享信息。

12) 数据共享信息订阅方收到数据共享信息发布的通知后，将执行智能合约的地址和新的数据共享信息发送给订阅方。

A.2 数据消费者访问基于DLT的共享数据的程序

数据消费者访问基于DLT的共享数据的程序如图A.2所示。



图A.2 – 数据消费者访问基于DLT的共享数据的程序

如图A.2所示，程序描述如下：

1) 数据消费者通过搜索数据共享信息发布订阅发布信息或他人转发获取数据共享信息。数据消费者决定访问共享数据，并执行数据共享智能合约。

2) 在执行数据共享智能合约以访问共享数据之前，数据消费者确保与基于DLT的数据共享管理的用户验证与授权组件的相互认证。建议使用凭据数字证书进行相互验证。相互验证成功后，用户验证与授权组件检查数据使用者是否有权访问共享数据。

3) 在成功验证和授权之后，数据消费者将其身份信息（例如，标识符、公钥）和数据共享信息连同其数字签名一起发送给数据共享访问管理。

4) 在接收到数据消费者的身份信息、数据共享信息及其数字签名后，数据共享访问管理验证数字签名，然后根据数据共享策略检查是否允许数据消费者访问数据（例如，只有来自特定行业或国家的数据消费者才能访问共享数据）。如果访问共享数据的所有要求都得到满足，则数据共享访问管理将根据从数据消费者接收的信息创

建一个DLT交易。数据共享访问管理将一个或多个DLT交易及其数字签名发送到底层组件DLT基础架构和基于DLT的智能合约管理，以形成包含一个或多个数据访问记录的新块。新生成的块被分发到相关联的DLT网络节点。将DLT交易加载到DLT链取决于底层的具体实施技术（如超级账本架构、Ethereum Quorum），此内容超出了本建议书的范围。

5) 数据共享访问管理通知令牌管理创建访问令牌。

6) 在接收到数据共享访问管理的通知后，令牌管理创建访问令牌。

7) 令牌管理将创建的访问令牌发送给数据共享访问管理。

8) 数据共享访问管理收到访问令牌后，将访问令牌、密钥信息（如标识及其存储地址）、密文信息（如标识及其存储地址）、其他信息（如密钥存储服务器和数据存储服务器的数字证书）发送给数据消费者。

9) 数据消费者收到数据共享访问管理的访问令牌、密钥信息和密文信息后，根据密钥存储地址将访问令牌发送给密钥存储服务器的令牌验证，获得加密密钥，用于解密密文。

10) 令牌验证检查访问令牌是否有效。

    10.1) 密钥存储服务器的令牌验证从数据消费者接收访问令牌，然后验证访问令牌。

    10.2) 视需要，当验证访问令牌时，令牌验证可能必须与基于DLT的数据共享管理的令牌管理进行通信。

11) 令牌验证将验证结果发送给密钥存储管理。

12) 密钥存储管理收到令牌验证的验证结果后，将加密密钥发送给数据消费者。

13) 在从密钥存储管理接收到加密密钥之后，数据消费者向数据存储服务器发送请求以获得密文。

14) 数据存储服务器的数据分配收到数据消费者的请求后，对数据消费者进行验证。

15) 数据存储服务器的数据分配将密文发送给数据消费者。

16) 数据消费者用密钥解密密文，然后以明文访问共享数据。

参考文献

[b-ITU-T X.509] ITU-T X.509建议书（2019年），信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架。

[b-ITU-T X.1400] ITU-T X.1400建议书（2020年），分布式账本技术的术语和定义。

[b-ITU-T X.1402] ITU-T X.1402建议书（2020年），分布式账本技术的安全框架。

[b-ITU-T FG DLT D1.1] ITU-T FG DLT D1.1技术规范（2019年），分布式账本技术术语和定义。

[b-ISO/IEC 18033-1] ISO/IEC 18033-1:2021，信息安全 – 加密算法 – 第1部分：总则。

[b-ISO/IEC 20944-1] ISO/IEC 20944-1:2013，信息技术 – 元数据注册互操作性和绑定（MDR-IB）– 第1部分：框架、通用词汇和一致性的通用规定。

[b-ISO/IEC 29100] ISO/IEC 29100:2011，信息技术 – 安全技术 – 隐私框架。

[b-ISO/IEC/IEEE 15939] ISO/IEC/IEEE 15939:2017，系统和软件工程 – 测量流程。

[b-IETF RFC 4279] IETF RFC 4279（2005年），用于传输层安全性（TLS）的预共享密钥密码套件。

[b-IETF RFC 4306] IETF RFC 4306（2005年），互联网密钥交换（IKEv2）协议。

[b-IETF RFC 4314] IETF RFC 4314（2005年），IMAP4访问控制列表（ACL）扩展。

[b-IETF RFC 4949] IETF RFC 4949（2007年），互联网安全术语表，第2版。

[b-IETF RFC 5246] IETF RFC 5246（2008年），传输层安全性（TLS）协议，1.2版。

[b-IETF RFC 5782] IETF RFC 5782（2010年），DNS黑名单和白名单。

[b-IETF RFC 5851] IETF RFC 5851（2010年），宽带多业务网络中访问节点控制机制的框架和要求。

ITU-T 建议书系列

A 系列	ITU-T 工作的组织
D 系列	资费及结算原则和国际电信/ICT 的经济和政策问题
E 系列	综合网络运行、电话业务、业务运行和人为因素
F 系列	非话电信业务
G 系列	传输系统和媒介、数字系统和网络
H 系列	视听及多媒体系统
I 系列	综合业务数字网
J 系列	有线网络和电视、声音节目及其他多媒体信号的传输
K 系列	干扰的防护
L 系列	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M 系列	电信管理，包括 TMN 和网络维护
N 系列	维护：国际声音节目和电视传输电路
O 系列	测量设备的技术规范
P 系列	电话传输质量、电话设施及本地线路网络
Q 系列	交换和信令，以及相关联的测量和测试
R 系列	电报传输
S 系列	电报业务终端设备
T 系列	远程信息处理业务的终端设备
U 系列	电报交换
V 系列	电话网上的数据通信
X 系列	**数据网、开放系统通信和安全性**
Y 系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z 系列	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦