国　际　电　信　联　盟

ITU-T X.1403

(09/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务 (2) – 分布式账簿技术安全

将分布式账本用于去中心化身份管理的安全指南

ITU-T X.1403 建议书

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
网页安全	X.1140–X.1149
安全协议（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.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	**X.1400 – X.1429**
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
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
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
5G 安全	X.1800–X.1819

ITU-T X.1403 建议书

将分布式账本用于去中心化身份管理的安全指南

摘要

分布式账本技术（DLT）及其特定的实施方案（如区块链）为利用信任基础设施和平台提供了独特的机遇，这对于启用可信联盟/联邦以交换身份属性和身份信息可能很有用。ITU-T X.1403建议书提供了有关在身份管理中使用DLT数据的、电信特定的隐私和安全注意事项。

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.1403	2020-09-03	17	11.1002/1000/14264

关键词

分布式账本技术、身份管理。

* 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ID，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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1403 建议书

将分布式账本技术用于去中心化身份管理的安全指南

1 范围

分布式账本技术（DLT）提供了一个可信的基础设施，它对于启用去中心化身份管理系统进行身份属性和身份信息的交换很有用。

本建议书概述了将DLT用于去中心化身份管理的情况。工作范围包括：

– 关于将分布式账本用于身份和身份数据管理的简要概述，

– 关于去中心化身份之安全效益的讨论，

– 关于实施必要控制以减轻身份数据面临之威胁的导则。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；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考文献的可能性。ITUT-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.1252] ITU-T X.1252 (2010)建议书，基线的身份管理的术语和定义。

[ITU-T X.1254] ITU-T X.1254 (2012)建议书，实体认证保证框架。

[ITU-T X.1277] ITU-T X.1277 (2018)建议书，通用认证框架。

[ITU-T X.1278] ITU-T X.1278 (2018)建议书，客户端到认证者协议/通用2 – 因子框架。

3 定义

3.1 其他地方定义的术语

本建议书使用了其他地方定义的以下术语：

3.1.1 声称[ITU-T X.1252]：声明情况如此，无法提供证明。

3.1.2 证书[ITU-T X.1252]：指的是作为所声称身份和/或权利的证据的一组数据。

3.1.3 DID文档[b-W3C-2]：指的是用于描述DID主体的一组数据，包括诸如公钥和化名生物特征识别等机制，DID主体可用来认证自己并证明其与DID的关联。

3.1.4 实体[ITU-T X.1252]：指的是可在语境中识别的、单独和独立存在的任何事物。

3.1.5 联盟/联邦[ITU-T X.1252]：指的是用户、服务提供方和身份服务提供方的关联。

3.1.6 身份服务提供方（IdSP）[ITU-T X.1252]：指的是认证、维护、管理并可能创建和指配其他实体身份信息的实体。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 去中心化标识符（DID）：指的是一种全球唯一的标识符，由于它已通过分布式账本技术（DLT）或其他形式的去中心化系统进行注册，因此不需要一个集中/中心化的注册机构。

注 – 基于[b-W3C-2]中的定义。

3.2.2 DID主体：指的是DID文档所涉及的实体，即由DID标识并由DID文档描述的实体。

注 – 基于 [b-W3C-2]中的定义。

3.2.3 密钥链：指的是保护设备中可信硬件单元上私钥或数据存储安全的任务。

3.2.4 服务端点：指的是一项服务代表一个DID主体在其上进行操作的一个分布式账本地址。特定服务的示例包括发现服务、社交网络、文件存储服务和可验证的声明存储服务。服务端点也可以由通用数据交换协议（如可扩展的数据交换）来提供。

注 – 基于[b-W3C-2]中的定义。

3.2.5 信任框架：指的是一系列可合法执行的规范、规则和协议，用于管理一个身份系统。

3.2.6 钱包（身份钱包）：指的是一个应用程序，它主要允许用户通过在用户设备上存储相应私钥来持有标识符和证书。

3.2.7 零知识证明：指的是一个证明，它使用特殊的密码学和一个主密钥来允许有选择地透露一组声明中的信息。一个零知识证明可证明一组声明中的某些或全部数据是真实的，而无需透露任何其他信息，包括证明者的身份。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

DDO 文档

DID 去中心化标识符

DIdAm 去中心化身份和访问管理

DLT 分布式账本技术

IdAM 身份访问和管理

IdSP 身份服务提供方

IT 信息技术

PKI 公钥基础设施

PII 个人可识别信息

RP 依赖方

SAML 安全断言标记语言

SP 服务提供商

SSI 自我主权身份

SSO 单点登录

URL 统一资源定位符

5 惯例

本建议书适用于以下描述方式表达的规定：

a) 须（shall）表示要求；

b) 应/应该（should）表示建议；

c) 可/可以（may）表示允许；

d) 能/可以（can）表示可能性和能力。

6 迈向去中心化数字身份

分布式账本技术在推进去中心化身份系统的演进和成熟方面发挥着至关重要的作用。

移动设备和物联网的增长增大了传统身份和访问管理系统（IdAM）向可支持基于移动和云的系统的敏捷和智能平台演进的压力。

传统身份管理系统建立在集中/中心化机构（例如，公司目录服务、证书机构或域名注册机构）基础之上。这些组织上集中/中心化机构中的每一个都充当其自己的信任域。在传统的IdAM系统中，集中/中心化机构可代表单点故障。身份联盟/联邦[ITU-T X.1252]作为权宜之计而出现，它使IdAM系统能够跨系统与不同的组织（负责控制自己的域）一起工作。

DLT的出现为开发去中心化身份和接入管理（DIdAm）解决方案提供了机会。DLT提供了一种不需要一个集中/中心化机构即可管理信任的方法，从而可避免任何单点故障。此外，DLT使任何实体都可以在任意数量的分布式账本上创建和管理自己的标识符。

为了满足不断变化的业务需求，数字身份模型一直在不断演进。第6节描述了三种基本的身份模型。

6.1 集中/中心化身份模型

这是最古老的数字身份模型，也是目前用得最多的[ITU-T X.1252]。在集中/中心化身份模型中，组织充当身份服务提供方（IdSP）。在该模型中，一个组织与其每个用户建立一种点对点的可信关系。该模型是传统的筒仓式模型，利用该模型，组织向用户颁发证书，允许用户访问该组织的服务。

在该模型中，每个组织充当一个IdSP。组织负责管理用户的数字身份并决定接受的信任关系。通常，通过使用诸如用户名和密码之类的共享机密来建立用户与IdSP之间的信任。在某些情况下，共享机密会通过多因素认证（例如，硬件令牌、生物特征识别技术或FIDO [ITU-T X.1277]和[ITU-T X.1278]）解决方案得到增强。

在集中/中心化模型中，IdSP可以存储和收集有关用户的数据。可以根据身份服务提供方（IdSP）的业务模型，将数据货币化、共享或出售给其他方。用户必须信任IdSP在管理其数据方面能恰当行事。尽管最终用户可以从组织的服务中受益，但在大多数情况下，它们无法控制对自己身份、个人数据或个人身份属性的管理。在该模型中，IdSP是用户身份的所有者。用户无法将其数据发送给其他提供方。

集中/中心化身份模型要求用户为与每个IdSP的每个业务关系创建和管理单独的证书。在允许用户访问其资源之前，组织要求创建这些证书。该模型中的多个在线身份使用户不知所措。登录时缺乏相互认证使该模型容易遭受网络钓鱼和证书收割攻击。该模型鼓励用户重用密码，这会带来进一步的安全风险和漏洞。

当涉及身份的生命周期管理时，集中/中心化模型会给IdSP带来负担。特别是，该模型要求每个IdSP进行身份审核[ITU-T X.1254]，作为身份生命周期管理中身份注册阶段的一部分。为对所声称身份建立一定的信任，需要进行身份审核。在给定身份的整个生命周期中，可能会重复此过程。从用户的角度来看，此步骤是有问题的，原因是集中/中心化模型要求用户与每个身份提供方分别进行身份审核步骤。此外，由于组织依赖于成为黑客定期攻击目标的集中/中心化数据存储，因此数据泄露威胁增加了帐户接管的风险。

6.2 联盟/联邦化身份模型

组织已经意识到第6.1节中讨论的集中/中心化身份模型的局限性，并已采取行动来开发联盟/联邦化身份模型以应对这些挑战。联盟/联邦化身份模型旨在通过使用户能够使用另一个域中的身份来减轻用户的负担。安全断言标记语言（SAML）[ITU-T X.1242]为具有单点登录（SSO）功能的个人提供了更多便利。

联盟/联邦化身份管理系统可以提供跨组织和系统边界的认证和授权功能。它要求建立业务和信任协议，以便一个提供方处的用户身份能被其他提供方（联盟/联邦成员）认可。通常，信任协议还包括有关数据所有权、个人身份信息（PII）使用和合规性的合约性的协议[ITU-T X.1242]。

联盟/联邦模型使用户受益，原因是身份服务提供方通常会向用户提供单点登录体验。它减少了用户需要维护和获取的单独证书的数量。在该模型中，参与联盟/联邦的依赖方（包括其用户）取决于给定IdSP服务的可用性以及其留在联盟/联邦中的意愿。

与集中/中心化身份模型一样，联盟/联邦化模型中的认证不是相互的，并受到相同的限制。

6.3 去中心化身份模型

可以使用DLT或其他基于新兴标准的技术（例如，可验证的声称[b-W3C-1]和去中心化标识符（DID）[b-Sovrin]、[b-W3C-1]和[b-W3C-2]）来实现去中心化身份。去中心化身份模型可以建立在分布式账本（DLT）以及用户与组织之间的关系基础之上[b-Sovrin]和[b-W3C-17]。在该模型中，用户和组织是对等的。

去中心化身份允许用户承担对其身份的控制和所有权。所有权程度可以根据去中心化模型而有所不同。特别是，在自我主权身份（SSI）模型中，它假定实体将能够控制自己的数字身份。

如今，大多数身份解决方案对身份、透明性和可移植性的控制的支持都是有限的，原因是具有专有系统的身份提供方可以简化此类解决方案。完全符合SSI模型的身份系统可能会在不久的将来出现，但这并不排除需要定义其创建原则，参见第6.3.1和6.3.2节的讨论。第7节对将DLT用于去中心化身份管理的问题做了进一步讨论。

6.3.1 去中心化标识符

DID [b-W3C-2]是可验证、去中心化身份系统的一种标识符类型。DID的格式允许其处于DID主体的控制下，这使之独立于任何集中/中心化注册表、身份提供方或证书机构。DID是统一资源定位符（URL），它将DID主体与用于和该主体进行可信交互的方式相关联。DID文档（DDO）[b-W3C-2]的标准元素包括：

1) DID（用于自我描述）
2) 公钥集（用于验证）
3) 认证协议集（用于认证）
4) 服务端点集（用于交互）
5) 时间戳（用于审计历史记录）
6) 签名（用于完整性检查）

解析DID [b-W3C-2]的任务是使用DDO进行的，该文档是一个描述如何使用该特定DID的简单文档。每个DID文档至少包含三个元素：加密材料、认证套件和服务端点。与认证套件结合使用的加密材料提供了一组机制来对DID主体（与DDO相关的用户）进行认证。认证选项的示例是公钥和化名生物特征识别协议。服务端点启用与DID主体的可信通信。

为将DID [bW3C-2]与特定的分布式账本一起使用，需要定义一种DID方法。DID方法规范可以基于[b-RFC 8141]。一种DID方法规定一组规则，这些规则用于控制在一个特定的DLT上如何注册、解析、更新和撤销一个DID。所有DID都在一个分布式账本中进行规定和解析。

使用基于DLT的DID [b-W3C-2]减少了对有关标识符的集中/中心化注册表以及有关密钥管理的集中/中心化认证机构的依赖。由于DID驻留在分布式账本上，因此每个实体都可以充当自己的信任域，从而形成去中心化信任基础设施。这在集中/中心化标识符、联盟/联邦化标识符和去中心化标识符之间建立了一座互操作性的桥梁。

DID有一个公共和私有加密密钥对[b-W3C-2]。DID的所有权由依赖于私钥的加密算法来证明，只有DID的所有者才应拥有之。因此，可以发布、更改、查询或删除DID。由于每个DLT都可能有自己的DID方法实施方案，因此在实践中，DID的“创建、读取、更新和删除（CRUD）”操作将有不同的实施方案。

6.3.2 可验证的证书

可验证的证书[b-W3C-1]解决了通过通信网络、以可验证并保护个人PII的方式交换证书（如驾照、年龄证明、学历和医疗数据）的问题。在这种方法中，证书由称为可验证的声称的声明组成。可验证的声称[b-W3C-1]在实体需要证明自己的某种资质或情况的时候是很有用的，例如：

- 超过一定年龄，
- 能够驾驶某种特定的汽车，
- 要某种特定的药物，

- 经培训并获电工认证，
- 有专业的行医许可，
- 获准国际旅行。

可验证的证书生态系统由四个主要角色组成：

1) 发布者，发布有关特定主体的、可验证的证书，
2) 持有者，持有代表某个主体的证书。持有者通常也是证书的主体，
3) 验证者，请求一个有关主体的配置文件。配置文件包含一组特定的证书。验证者确认配置文件中提供的证书适合于目的，
4) 标识符注册，一种用于发布主体标识符的机制。

声称[b-W3C-1]是关于某个主体的一个声明，表示为主体 – 特性 – 值之间的一个关系。声称可以合并在一起，以表示有关特定主体之信息的一个图。

当发布者将数据发送给持有者时，它将一组声称绑定到一个称为证书的数据结构中，并对该数据结构进行数字签名[b-W3C-1]。当验证者向持有者请求数据时，持有者通常将一组证书捆绑到一个称为配置文件的数据结构中，并对该数据结构进行数字签名[b-W3C-1]。

7 使用DLT的去中心化身份

去中心化身份可以被视为由DLT来锚定的身份。在这种方法中，零知识证明[b-W3C-1]可以用一种普遍可发现的方式来链接身份。去中心化身份允许用户一次向可信第三方证明其身份，并将有关其标识符的证明存储在DLT中。DLT作为身份信任支撑。DLT提供身份基础设施服务，以支持对等通信、基于DLT的公钥基础设施（PKI）服务以及可验证的声称交换协议等。

去中心化身份允许用户通过一个简单明了的过程来访问服务。例如，用户与IdSP进行交互，而IdSP则使用DLT来创建用户DID，它指向该用户可以使用的一个DLT位置。此步骤对最终用户是透明的。此步骤等效于为用户创建一对私钥和公钥。私钥以某种形式的数字钱包与用户一起存储。相应的公钥存储在DLT中。公钥充当钱包标识符（DLT上又称为用户身份），经过哈希处理，安全地存储在账本中。作为DLT提供之服务的一部分，可以由DLT发布者来为特定的用户发布和签署声称，并提供给用户。这些声称可以存储在用户的钱包中。

在该模型中，用户可以通过以令牌形式向服务提供方提供其标识符来访问服务。服务提供方通过对标识符的哈希值与其存储在DLT中的相应哈希记录进行比较来验证身份。服务提供方根据验证结果同意或拒绝访问。

7.1 钱包初始化

[b-Sovrin]和[b-W3C-1]中的工作提供了一个有关交互的示例，它支持基于身份的服务。用户决定使用基于DLT的身份信任系统的去中心化身份服务进行交互。在这方面，DLT提供的服务使最终用户能够建立一个DID以及与账本的一个关系。通过为用户保存一个账本地址并创建用于与用户交互的公共私钥对，来达成为该用户建立一个DID的任务。账本还可以提供可用于创建DID文档并建立用户规定之所需文档链接的服务。账本提供核心身份服务，使服务能够发现如何与用户钱包进行交互，以便在用户控制下查询可用的声称。

在账本上创建一个DID的行为将创建一个钱包，供用户用来向信赖方（RP）提供经过验证的声称。钱包持有由DID方法确定的用户的私钥、公钥和其他身份配置文件。零知识技术的使用[b-Sovrin]确保可以以保护PII的方式来验证声称，并与传统的纸质证书和文档的当前用法相符。例如，在一个创建过程中，用户可以使用驾驶证来证明其年龄，而无需驾驶证签发机构参与交易。钱包可以是虚拟钱包，其中钱包的一部分在用户的移动设备上，而钱包的另一部分可以在云上。这种配置使得能够通过创建代理来代表用户采取行动并提供服务，而无需用户的直接参与。

以下步骤与该过程有关：

1) DID注册：用户下载与DLT服务提供方关联的钱包，并在账本上注册其DID。DLT生成与身份钱包关联的私钥和公钥对。作为注册过程的一部分，将创建一个地址并将其存储在DLT中。

2) 身份初始化：对于要在去中心化身份系统中使用的DLT，假定存在一个信任框架，该信任框架为参与者规定一个可用的身份服务列表。在这方面，用户可以依赖可验证用户身份之发布者（可信方）的可用性。最初，用户可以以自我断言的声称开始。然后，用户可以在其钱包初始声称的基础上收集来自多个提供方的其他声称，以纳入其钱包中，并增强其在系统内的身份有效性。每种关系都受到发布者、持有者（用户）和验证者之间相互DID的保护。

3) 验证：如果持有者（用户）想访问依赖方提供的某项服务，则RP（验证者）将请求用户提供其钱包中可用声称的访问权限。验证者而后咨询DLT，以便通过使用与交易中所述之DID相对应的公钥来验证经签名的声称。依据有关持有者私钥的知识，系统假定钱包是真相的来源。系统假定进行了适当的认证，以确保合法的钱包所有者是执行交易的实体。

4) 声称验证：RP使用钱包提供的声称，以使用基于DLT PKI的签名和哈希验证技术来验证用户的身份和属性。

5) 授权：RP根据身份认证的结果来确定可以访问哪些服务。

7.2 DID解析和认证

DID概念[b-W3C-2]有助于为任何DID创建一个通用解析器[b-DIF]。该通用解析器可以参与可互操作的DID认证层。DID认证使身份所有者可以在与RP交互期间控制DID。这要求依赖方执行以下步骤：

1) 依赖方将DLT上身份所有者的DID解析为一个DID文档，

2) 依赖方尝试使用在DLT上DID文档中找到的认证对象来对身份所有者进行认证，

3) 在身份所有者的证明被建立为一个加密签名的情况下，认证对象可以包括或参考一个公钥对象。

7.3 将DLT用于去中心化身份和访问管理系统（DIdAm）的益处

将DLT用作去中心化身份系统的信任框架，为提供方设计框架奠定了基础，该框架允许提供方充当用户与各种账本之间的中间件抽象层。这些交互需要传统的身份和访问管理系统来建立适当的框架以支持去中心化系统。本质上，集中/中心化系统和去中心化系统的合并可以称为去中心化身份管理系统（DIdAm）[b-Angelov等]。从这个角度看，DIdAm [b-Angelov等]是一个由若干系统组成的大系统，它可与支持基于DID的去中心化身份模型的许多DLT进行交互。如图1所示。

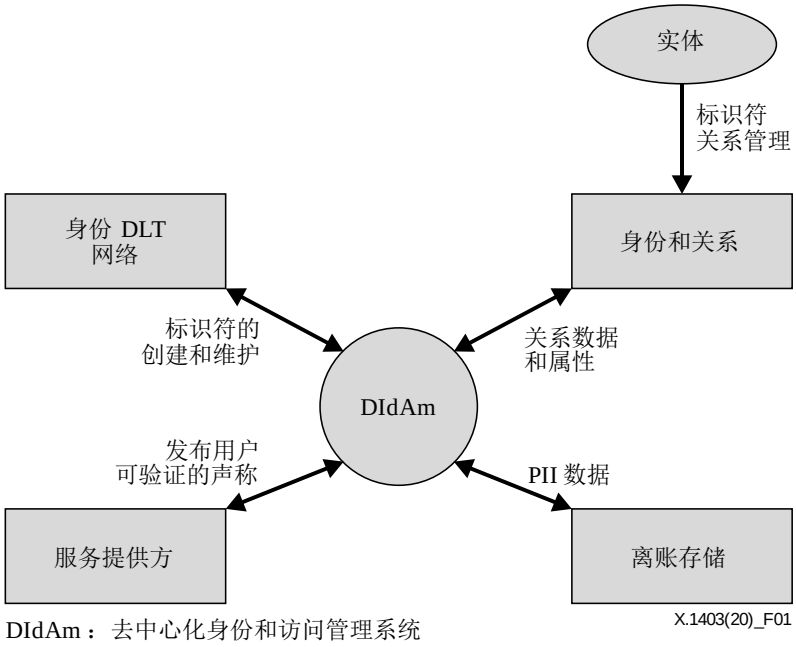

图1：DIdAm框架

使用DLT的DIdAm的组件为：

1) 去中心化身份所有者：这是一个实体，它使用DIdAm在多个账本中提供的服务来管理其去中心化身份。

2) 服务提供方（SP）：向身份所有者（引导身份）提供服务的发布者。例如，诸如汽车部门之类的政府机构或者诸如金融机构之类的私营公司。

3) 离账身份仓库：这是一个数据库，当中存储用户身份属性、声称和一般信息。用户可以控制数据的存储位置。这通常是对PII敏感的数据，应离账存储。用户自行决定仓库应提供数据读写能力。

4) 可以将基于DLT的身份系统视为具有不同信任边界和加密密钥的独立身份系统。因此，DIdAm必须代表用户推动账本之间的交互。

DIdAm的服务可以由企业内部执行，或者可以由某第三方来扮演此类提供方的角色。

7.3.1 在多个DLT账本中支持去中心化身份

有许多接口要求[b-Angelov等]，需要使用跨多个DLT的DID来支持去中心化身份。因信任框架的各种不同要求（例如，DLT的类型是公共的还是私有的）而产生困难。DIdAm应该能够支持用户，而不管用户对其正在使用之通信访问网络类型的偏好。图1显示了面向身份所有者的、统一接口能力下的DIdAm，它能工作于多个账本。

DIdAm [b-Angelov等]充当最终用户的抽象层。它使用户能够在使用单个虚拟接口的同时与多个DLT进行交互。DIdm还将充当企业的抽象层，基于传统的IdM系统可以与企业交互，以支持集中/中心化IdM的内部功能。这种抽象的益处是用户能够管理任意数量账本上的身份。这将使用户能够与提供方建立关系，并能够更好地控制其身份。

7.3.2 支持身份服务

在传统的IdAm系统中，身份服务提供方可以向依赖方证明用户的身份。DIdAm [b-Angelov等]应该能够支持此角色，尤其是要与旧系统向后兼容。以下行动可以支持证明要求：

1) DIdAm应该充当可信的合作伙伴。它应确保身份所有者通过针对发布者的正确的、可验证的声称程序来获得准确、有效的断言。

2) 减少用户的身份审核摩擦。通常，用户将需要与每个发布者一起完成身份审核阶段。适当设计的DIdAm通过成为交互中积极的可信参与者，可以帮助用户克服此限制。

3) 实时数据验证。数据不准确是旧系统中的问题。DIdAm可以通过提供服务来缓解此问题，这些服务有助于依赖方确定用户属性是否陈旧。

4) 同意意见的管理。同意意见是合规性的一个有机组成部分。DIdm可以向用户和依赖方提供服务，以确保考虑到同意意见的合规性。

7.3.3 管理密钥链

术语“密钥链”指的是保护与用户设备上钱包关联之私钥存储安全的任务。DID、可验证的证书和服务提供方之间存在直接的一对一关系。该设备可以是一个移动的设备或一个基于浏览器的设备。由于在此当前安全模型中，对私钥的访问用于验证用户的身份，因此保护密钥对的任务对防止身份欺诈攻击而言至关重要。在处理多个DLT上的多个DID时，用户面临保护私钥集的任务，这些私钥用于在整个身份空间中解锁其身份。

密钥链是安全存储与用户DID对应之私钥的结构。它是身份所有者拥有的结构，并控制转换为拥有DID的私钥。DIdAm应该能够代表用户来管理密钥链。尤其是：

1) 用户在DIdAm域内操作时应该能够使用密钥链的功能和存储空间。

2) 密钥管理应在用户的控制之下。

3) 对密钥链的访问应予管理并应是可审计的。

4) DIdAm可以提供使用户能够保存和恢复钱包的服务。

8 将DLT用于DIdAm的安全指南

去中心化身份解决了与集中/中心化和联盟/联邦化身份模型相关的一些关键问题。分布式账本技术容易受到网络安全风险的影响。安全风险包括因人为错误（如软件编码错误）而导致的风险。

通常，即使在某些情况下可能需要为所有用户提供一个唯一的ID，也不应将用户DID发布在无许可的账本上。不过，可以将有助于用户信任账本的数据（例如，IdSP公钥、撤销列表）和有助于增强互操作性的数据（例如，可变的证书模式）作为账本上的公共信息。

本节论述去中心化身份模型的安全优势、面临的挑战和安全风险。

8.1 分布式账本安全注意事项

分布式账本有两种主要类型，分类为无许可型和许可制型。无许可型账本允许任何实体访问、查看、提议新的数据或者验证账本上的现有数据，只要它们遵循账本建立的协议即可。账本通过共识协议来确保数据的机密性、完整性、可用性和一致性，以在可能互不信任的参与者之间建立信任。在无许可型账本的操作中通常没有任何中央机构。

许可制型账本是一个系统，它由可信方组成，这些可信方根据其在信任框架中的角色需要而被授予使用权限。在该模型中，选定的参与者可以更改账本数据。根据信任协议，某些账本可以允许对账本进行开放性读取访问。

无许可型账本可通过共识协议来确保信任，共识协议在计算上是一种开支，并确实会对运行在其上的身份系统的吞吐量和性能产生直接影响。另一方面，许可制型账本以来账本创建者之间的信任来确保账本数据（包括身份数据）的安全。许可制型账本通常比无许可型账本更快、更经济。

8.2 将DID用于DLT的益处

去中心化身份提供以下益处：

1) 身份可移植性：去中心化DID可确保个人对其数字身份的控制。它消除了对集中/中心化IdSP的依赖。从理论上讲，个人可以拥有、控制和管理自己的身份及其关系。

2) 鼓励基于关系的身份服务：DID使实体能够为几乎所有关系建立数字标识符。用成对的化名DID来保护PII。

3) 最小化安全风险：DID要求标识符的所有者通过展示与对应公钥关联的私钥的知识来证明所有权。实时地在DLT上对声称验证进行动态校验。无需集中/中心化服务器即可完成验证，从而减少攻击面。

4) 成本分配：DLT上的身份验证可受益于使用DID在DLT参与者之间重用身份证明的能力。这样可以降低成本并增强安全。

5) PII的设计：去中心化主权DID服务分散了因使用集中数据存储来存储用户信息而带来的风险，并因此提高了攻击者的攻击难度。

6) 同意的和保持跟踪的个人数据共享：DID提供了基于约定策略的、在用户与提供方之间共享数据的能力，这提高了用户保护其数据的能力。

7) 动态的和经改进的联盟/联邦：在DLT中使用DID可将信任扩展到所有参与该生态系统的组织。参与者可以专注于提供服务，而不是专注于联盟/联邦的细节以及如何建立联盟/联邦。

8) 容错：DLT的去中心化性质提供了一定程度的容错和基础设施适应性。

8.3 威胁和漏洞

分布式账本继承了可缓解信息通信技术系统网络安全风险的功能。经改进的安全功能示例包括：

1) 更好的系统适应性：DLT的分布式体系结构可防止其出现单点故障。

2) 更强的鲁棒性：共识机制提高了分布式账本的整体完整性，原因是在接受账本中的任何新数据之前，参与者之间需要达成共识。

3) 更高的透明性：由于系统在账本基础设施层面拥有许多单独的安全层，因此恶意软件将更难以在DLT内实施破坏。

使用DLT构建的去中心化身份系统将继承这些技术带来的安全风险。此外，使用DLT进行身份管理还存在其他风险。

8.3.1 身份数据管理

CRUD代表“创建 – 读取 – 更新 – 删除”。这些是传统存储数据库的基本操作。在DLT中，特别是在获得许可的区块链中，实施实体无法删除区块链上的已写入交易。甚至更新现有交易也无法完成，原因是它们是不可变的。因此，“CRUD”操作不能视为处理用户数据的常规操作。

相反地，对区块链的操作可以描述为CRAB：创建、检索、添加和刻录。“添加”代替“更新”意味着实施者只能将新的交易添加到区块链技术上，因此而更改“世界状态”（迄今为止所有的过去事件/交易之和）。CRAB中的“刻录”操作意味着你抛弃加密密钥，因此无法添加新的交易或者对资产的账本状态做任何进一步的更改。

因此，重要的是要注意在DLT或区块链上写入个人数据，原因是未来不会取出或遗忘数据。在这方面，最好利用DLT中指向外部数据的指针离链写数据。不过，离账存储数据也有缺点。尤其是：

- 透明性的益处减少了，原因是用户将不知道其是否无权访问离账数据。
- 区块链数据所有权的益处减少了，原因是一旦数据离账，则任何可以访问它的实体都可以拥有它。

8.3.2 密钥可链接性

DID有可能被关联。如果在多个关系中使用同一DID，则会发生这种情况。DLT账本可以通过使用有关关系的成对的唯一DID来缓解这种风险。这意味着对每个关系，每对使用的DID都不相同。在这种场景下，每个DID都充当一个化名[b-W3C-2]。仅当DID主体明确授权这些方之间的关联时，才需要与多个方共享一个化名DID。

注意：如果可以对相应DID文档中的数据进行关联，则甚至可以对化名DID进行关联[b-W3C-2]。例如，使用公共服务端点，可以使用多个DID文档中的名称来关联有关同一DID的信息。因此，用于化名DID的DID文档还需要使用成对的唯一公钥。

8.3.3 DID密钥保护

私钥的管理很重要。如果主密钥存储在非安全的位置上，即使是在单个设备上，也可能会发生身份被盗的现象。使用设备上的安全存储设施应作为一条要求。

8.3.4 PII保护技术

建议不要在账本上存储任何敏感信息。量子计算的出现将确保随着时间的流逝，每一种双向加密技术都可被破解，目标是永远别在账本上存储任何敏感信息。

尽管哈希是单向函数，但由于黑客有无限的时间来尝试对摘要进行暴力破解，因此哈希可能会很敏感。因此，账本中不应存储任何哈希。

除了可以将诸如出生日期之类的原始数据存储在账本上之外，还可以将对一些问题的答案（例如，表明一个21岁以上的人）存储在账本上的智能合约中。这可以被看作是一个符合要求的声称。

建议仅在DLT上存储私有或敏感数据的哈希。PII数据即使已经加密也不应存储在账本上。敏感数据应离帐存储，并应在需要使用数据的、已经批准的实体之间进行交换。这种方法降低了DLT违规将导致敏感数据丢失的风险。应将安全的点对点技术用于支持离账访问的数据交换。应使用适当的离账数据存储技术，包括有关数据归档和恢复的计划。例如，如果身份所有者声称其是经许可的保险提供方，则可以由在去中心化身份系统中扮演可信提供方角色的一个实体来验证该声称，并将证明以哈希形式存储在DLT中。证明可以是来自声称者的数字签名声称的哈希。应确保离账仓库的安全。

8.3.5 应商锁定

账本可以标准化，但软件组件特定于某个给定的解决方案，并可能是专有且不可互操作的。

8.3.6 基于身份的攻击

分布式账本容易遭受基于身份的攻击，类似于那些针对传统信息技术基础设施的攻击，例如，欺骗和女巫攻击。恶意的攻击者可以部署此类攻击来接管账本中的大多数节点。如果攻击成功，则攻击者可破坏账本的共识验证和分布式体系结构保护措施。对基于云的目录服务使用强大的认证解决方案可以缓解这种风险。

8.3.7 通信网络的影响

DLT的分布式结构在处理许多参与者各自拥有自己的通信基础设施保护解决方案时会产生操作问题。这种结构给身份管理、访问控制、安全配置、PKI密钥存储和管理带来了挑战。

DLT操作需要正在运行的节点，这些节点使用可能容易遭受安全威胁的不同的通信网络拓扑、软件代码和协议。这些威胁的影响因DLT性质（私有的或公共的）的不同而不同。这样，身份管理系统和身份数据就容易受到针对DLT的通信网络层面的攻击。身份管理系统的设计者应考虑到通信网络层面的问题，其中包括：

1) 在DLT共识算法出现故障的情况下，会对身份数据造成哪些影响？
2) 如何处理DLT或区块链冲突？
3) 身份数据的灾难恢复计划是什么？
4) 在一小部分参与者控制DLT共识机制的情况下，会对身份数据造成哪些威胁？

8.3.8 身份数据加密

离账存储的身份数据被视为是身份所有者机密的和私有的信息。用户应该能够从账本中获得帮助，以协助批量地或在传输过程中对数据进行加密，尤其是当在各个提供方之间共享数据时。

8.3.9 备份

就可验证的声称或者私钥和个人数据而言，在保护其设备和其内容时，用户面临风险。

需要对用户钱包进行适当的数据恢复和修复。

此外，用户将需要确保其数据受到保护并备份到账本上。确保没有数据损坏或丢失的技术应作为服务提供给最终用户。

8.3.10 智能合约

在实施去中心化身份系统时可能需要使用智能合约。智能合约是由开发人员使用计算机编程语言编写的。这些程序易受开发和编程错误的影响，尤其是随着智能合约复杂性的增加。智能合约准确性的不确定性要求开发治理框架，以确保去中心化身份系统具有适当的流程和程序，以应对因不正确的智能合约（无论是有意的还是无意的）而导致的任何限制。

8.3.11 DLT证书管理

身份管理系统包括管理身份生命周期的任务，其中包括身份审核任务。与身份管理相关的任务包括创建、发布、存储、撤销和替换证书以及欺诈检测。

在账本中使用证书给安全从业人员带来了一些独特的挑战。在去中心化身份系统中，与传统访问系统相比，丢失或错放私钥将付出更高的代价。例如，如果用户的钱包私钥丢失，则将永久禁止用户对其DLT的访问。如果密钥被盗，则会造成更大的损失，原因是证明私钥的“激情”等同于身份盗用。恢复机制的困难还取决于DLT的性质。与要求就交易达成共识的无许可账本相比，处理私有账本中的这些问题会显得容易一些。

这些问题应包括在DLT治理系统的设计中，原因是没有中央机构来处理欺诈或技术难题。这需要信任治理框架来确保从一开始就涵盖身份生命周期的所有状态，并且DLT参与者事先商定适当的程序，以支持身份恢复服务，例如：密钥生命周期管理、对块负载的哪些部分进行加密、如何撤销密钥、如何保护和恢复私钥，以及如果检测到欺诈将会发生什么。

参考书目

[b-RFC 8141] RFC 8141, *Uniform Resource Names (URNs)*, April 2017.

[b-Angelov et al.] Angel Angelov, Mihail Milkov, Markus Sørensen, *Decentralized Identity Management System for Self-Sovereign Identity*, https://projekter.aau.dk/projekter/files/281068659/Master_Thesis_ICTE4SER4.2.pdf.

[b-Baars] Djuri Baars, *Towards Self-Sovereign Identity using Blockchain Technology*, https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.

[b-Blog] Blockchain platforms, https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b.

[b-DIF] Decentralized Identity Foundation (DIF), https://identity.foundation/#wgs.

[b-Gartner] Gartner, Blockchain, *Evolving Decentralized Identity Design*, Published 1 December 2017 – ID G00324208, By Analysts Homan Farahmand.

[b-Sovrin] Sovrin Foundation, https://sovrin.org/.

[b-W3C-1] W3C, *Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web*, https://www.w3.org/TR/2019/CR-vc-data-model-20190725/.

[b-W3C-2] W3C, *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes*, August 2019, https://w3c-ccg.github.io/did-spec/.

ITU-T 系列建议书

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

瑞士印刷
2021年，日内瓦