身份管理的局限与方法概述

Daniela Pöhn Wolfgang Hommel
daniela.poehn@unibw.de
wolfgang.hommel@unibw.de 慕尼黑联邦国防军大学，
CODE研究所，慕尼黑，德国

arXiv:2301.00442v1 [cs.CR] 1 Jan 2023

摘要
身份与访问管理（I&AM）是对用户及其权限进行管理的统称。用户需要通过它访问不同的服务。这些服务既可以由用户的所属组织（如公司或大学）提供，也可以由外部服务提供商（如合作伙伴）提供。I&AM负责管理标识符及其相关属性、凭据、用户所拥有的角色和权限。如今，需求已从仅访问互联网或公司内的单个网络服务，发展到访问由不同服务提供商提供、使用各种账户的大多数信息技术服务。人们已提出多种采用不同方法的身份管理模型。

为适应异构环境、用例以及身份管理的发展，本文扩展了已有的身份管理需求，并将现有的身份管理模型和方法映射到推导出的需求。基于该映射，本文识别出其优势、劣势和差距。例如，当前方法面临可信度和责任问题。互操作性问题则更为根深蒂固，因为这些方法的发展在一定程度上彼此分离，形成了异构环境。本分析结果强调了构建统一、全面的身份管理框架的必要性。

CCS 概念
• **安全与隐私 → 安全服务**；**访问控制**；身份验证；授权。

关键词
安全、身份、身份管理、联邦式身份管理、区块链

ACM 参考格式：
Daniela Pöhn 和 Wolfgang Hommel。2020年。身份管理中的局限与方法概述。载于第*15*届国际可用性、可靠性与安全会议（*ARES 2020*），*2020*年*8*月*25*日至*28*日，线上活动，爱尔兰。ACM，纽约，纽约州，美国，共9页。https://doi.org/10.1 145/3 407023.3407026.

ARES 2020，*2020*年*8*月*25*日至*28*日，线上活动，爱尔兰© 2020年 版权所有者/作者保留版权。出版权已授权给 ACM。此为作者版本，仅供个人使用。禁止再分发。最终记录版本发表于第*15*届国际可用性、可靠性与安全会议（*ARES2020 28, 2020, 25*.10.1145 3407023.3407026），*8*月 – 线上活动，爱尔兰，https://doi org/ / 。

1 引言
中大型组织，例如大学和公司，通常会向成员提供多种信息与通信技术服务。通常，每位成员都会获得一个用户名作为标识符。之后，用户只需使用用户名和某种凭据的组合，即可使用所有服务，例如电子邮件、文件和网络协作。用户名、加盐哈希密码以及称为属性的其他信息，都会集中存储在后端。组织会使用轻型目录访问协议（LDAP）或其他数据库管理系统来实现这一点。尽管本地身份与访问管理（I&AM）看起来很简单，但一旦需要与其他实体建立接口（例如开展合作或成立合资企业），就会变得复杂。

当组织成员想要访问外部服务（例如协作平台）时，要么需要重复创建用户账户，要么使用联合身份管理（FIM）。FIM 是多个实体之间的一种安排，旨在让用户使用与其所属组织相同的身份识别数据，访问这些实体所提供、且位于信任边界内的服务。FIM 主要基于安全断言标记语言（SAML）协议 [59], ，该协议在研究与教育领域以及国家级联盟中都很常见；也可以基于开放式身份连接（OIDC） [64]。OIDC 是构建在授权协议 OAuth [29], 之上的身份验证层，而 SAML 则同时涵盖这两个方面。OAuth 和 OIDC 广泛应用于当今的网络服务中，例如 Google 应用程序接口（API）。每个用户至少都隶属于某种所属组织；在 SAML 中，这类组织称为身份提供方（IdP），在 OIDC 中则称为依赖方（RP）。用户希望访问服务提供商（SP）（或开放式身份提供方（OP））提供的服务。因特定目的而开展协作的一组 IdP 和 SP 通常称为联邦。联邦在 SAML 中尤为常见 [59], ，不过目前也正在制定 OIDC 规范 [30]。虽然业界的联邦规模相对较小，但许多国家研究与教育网络（NREN）运营着大型身份验证与授权基础设施（AAI），其中包含数百个组织。技术信任通过预先共享元数据来建立，即以可扩展标记语言（XML）文件形式保存的实体相关信息。信任也可以通过合同确立，例如联盟运营方与参与实体之间签订的合同。

由于相对静态的 SAML 联邦存在局限，因此建立了诸如 eduGAIN [26], 之类的联合身份系统互联，并开发了联邦间元数据交换 [84] 和 TrustBroker [57], 等动态方案。随着业界倾向于使用 OIDC，各组织纷纷并行部署 OIDC，甚至彻底改用 OIDC。与此同时，

也建立了采用 SAML 的电子身份联邦 [34]。SAML 联邦通过带外机制建立信任，而采用 OIDC 则需要另行设置其他机制。这促使各种保障框架和注册表不断涌现 [39],；与此同时，还开发了类似域名系统（DNS）的结构，用于发现服务提供商并验证其是否属于信任体系，即 LIGHTest [62], 。

I&AM 和联邦身份管理（FIM）都关注组织。由于至少有一些用户关心自己的身份和隐私，因此人们开发了以用户为中心的解决方案。服务提供商的隐私政策概述了收集到的个人用户数据的使用方式，而现在可以通过欧盟《通用数据保护条例》（GDPR）获取这些信息。当时，大多数网站都以不太易懂的方式描述用户信息。以用户为中心的身份管理（UCIM）通过清晰的呈现方式和直观的隐私政策评估，针对这些不足进行了改进。Microsoft Passport 是最早的应用之一，它是 Microsoft 环境中的身份提供商，可作为互联网上的通用身份提供商使用。由于 Microsoft 融入了每一次通信，信任和隐私便成了其短板 [54]。随后开发了 Windows Cardspace，它可以通过 SAML 使用其他身份提供方。用户拥有多张信息卡，这些信息卡可以由用户自行创建，也可以由身份提供方管理。不过，该应用存在若干安全漏洞 [5]。用户管理的访问（UMA） [41], 是一种基于 OAuth 的标准，更进一步地使用户能够控制数据共享及其他受保护资源的授权。Sovrin [75] 将自主主权身份视为演进的下一步。用户必须是自主主权身份的最终所有者。因此，自主主权身份在管理和治理方面完全自主，而用户是唯一的事实来源。这一范式通过去中心化域名实现；从本质上说，这意味着使用分布式账本技术（DLT），即区块链 [21]。

因此，目前正在开发和应用彼此正交的方法。与 OIDC 相比，SAML 相对静态，具有稳固的信任边界。基于域名系统的结构则借助证书和电子身份增强信任。UMA 可应用于 OIDC，而自我主权身份（SSI）则可用于不同的用例。各种身份管理方法带来了不同的问题。组织中的管理员需要处理不同的解决方案，因此，要全面了解这些方案并应用一致的政策会变得十分繁琐。此外，如果不同公司相互合作或开展项目，其身份管理解决方案可能彼此不兼容，这就需要再引入一个系统进行管理。此外，组织的需求可能无法全部由这些系统满足，从而需要更多工具。除了管理员之外，终端用户和其他利益相关者也有许多解决方案可供选择。终端用户最终可能需要使用多个不同的系统来管理自己的身份。因此，全面了解各种方案的优势、劣势及其差距十分重要。这样的概述有助于利益相关者选择最合适的方法，并确定所需的工具。

为提供这一概述，我们在第2节扩展了已知的身份管理需求。相关工作分为第3至5节介绍的成熟模型：[85] 集中式身份管理、FIM和UCIM。我们根据这些需求分析现有方法，并指出其中的差距。本文最后对分析进行总结，并展望未来。

2 身份管理的需求

为了解不同身份管理方法的使用情况并发现可能存在的差距，我们确定了各项需求。根据Torres等人 [76], 的说法，主要需求包括可用性、互操作性、功能性、可信度、安全、移动性、隐私、执法和可负担性。Boujezza等人 [16] 将这些需求视为物联网的基础。Ferdous和Poet未将移动性列入其中 [22], , 而Gao等人 [25] 则专注于核心功能。文献 [27] 的作者认为，自我主权身份的需求包括用户控制与同意、受限用途下的最少披露、可证明其正当性的各方、定向身份、面向多元运营者和技术的设计、人类集成，以及跨情境的一致体验。

关于自我主权身份（SSI），用户管理也必须成为一项需求。除了身份管理之外，要实现当今身份管理模型、方法和协议之间的互操作性，可能还需要其他功能。因此，需求“功能性”被细分为“管理”和“功能性”。用户数据的位置更名为“可移植性”。随着欧洲出台《通用数据保护条例》（GDPR），用户可以要求导出自己的账户数据，然后将其导入另一个平台。因此，用户数据需要能够在不同系统之间移植。此外，用户还应能够使用不同的设备，参见“面向运营方与技术多元化的设计”这一需求。“可负担性”则拆分为“与现有系统集成”和“可扩展性”。随着设备及其对应身份不断增多，可扩展性也变得日益重要。

因此，后续章节将采用以下需求来评估不同的方法。这些需求扩展了Torres等人 [76]汇总的需求。它们已经过归纳，并涵盖不同的子需求，如表1所示。

3 集中式身份管理

随着身份管理朝着不同方向发展，以下将介绍相关领域中选定的研究成果。为了对这些研究进行分类，我们采用不同的身份管理模型：

- 集中式 / 以网络为中心，
- 联邦式 / 以应用为中心，• 去中心化 / 以用户为中心。

这些模型还有其他特征，并应用于使用不同协议的不同用例。尽管集中式身份管理是在单个实例之后演进出的第一个阶段，但至今仍在使用。通常，公司会控制其所有身份，并在服务之间使用单点登录。如果将身份管理外包，采用的很可能是联邦身份管理。此外，拥有不同办公地点的公司也可能建立一个联合。在集中式身份管理中，公司掌控执法 [REQ10] ，因此无需进一步实现互操作性 [REQ3]。如果建立了合作关系，情况则会有所不同。

3.1 基于域名系统的集中式身份管理

域名系统是一种分层且去中心化的命名系统，用于为连接到网络的计算机、服务及其他资源命名。

表1：身份管理要求

No.	Name	描述
REQ1	管理	身份管理、自动化
REQ2	可用性	用户界面、降低复杂性、一致的体验
REQ3	互操作性	互操作性 在协议之间 列、模型、信息孤岛
REQ4	可扩展性	环境迁移性
REQ5	功能性	翻译 服务， 代理，桥接、群组管理
REQ6	可信度	信任管理、权力分离 电力管理中的局限与方法概述，政策
REQ7	安全	基础与多边
REQ8	可移植性	的账户与系统
REQ9	隐私	匿名性， 假名性，透明性， 可控性，同意，数据最小化
REQ10	责任	执法， 数字 Evi-证，数据保留
REQ11	集成	可负担性、集成 into 流程与现有基础设-ture

域名系统最常见的用途是将易于记忆的域名转换为数字形式的互联网协议（IP）地址，以便通过底层网络协议定位和识别计算机服务与设备。在身份联邦中，所属组织通过特定协议发现，有时也借助服务发现，即由持有可能实体元数据列表的可信第三方协助发现。此外，为了让某个实体使用不同的协议，至少需要建立桥接。使用域名系统或可改善这一状况。欧盟项目 LIGHTest [63] [62] 基于域名系统和 DNS安全扩展（DNSSEC），将其作为发现与信任的方法。因此，需要设立信任方案发布机构（TSPA） [81] 。该方法可以采用基于角色的访问控制（RBAC）作为委托形式，同时统一委派数据格式 [80]。其缺点是需要 eIDAS 或某种形式的证书，这也意味着保障等级（LoA）固定，因此 [REQ6]仅部分满足；此外，它还采用了类似 SAML 的集中式结构。尽管该方法可用于物联网（IoT） [38], [REQ3] 仍未满足。

3.2 使用域名系统实现物联网集中式身份管理

Wang 和 Wen [83] 提出了一种用于物联网的隐私增强型 DNS 方案。域名系统的设计并未考虑当今世界中各种复杂的安全问题。因此，作者引入了新功能。然而，该方案未考虑缓存，这与 [REQ7] 和 [REQ9]相矛盾。此外，经过若干步骤后需要使用新的域名 [REQ1]。Lee等人 [48] 介绍了在 IPv6环境中，利用邻居发现，依据设备类别和型号对物联网设备进行自动配置的方法。相比之下，由于需要手动配置物联网设备的 DNS名称，该方法效率较低 [REQ1]。尽管通过域名系统进行发现广为人知，相关攻击也并非未知，但并未提供

表 2：集中式身份管理方法概览

Ref	Name	未满足的需求
	集中式身份管理	[REQ3]
[63] [62]	LIGHTest	[REQ6] [REQ3]
[81]	TSPA	[REQ6] [REQ3]
[80]	委托	[请求6] [请求3]
[38]	面向物联网的 LIGHTest	[REQ6] [REQ3]
[83]	隐私增强型 域名系统方案	[REQ1] [REQ7] [REQ9]
[48]	自动配置 物联网设备	[REQ1]
[69]	ACE	[REQ3]
[87]	自然环境	[REQ11]
[51]	博士论文	[需求1] [需求11]
[33]	基于云的物联网	[REQ11]

授权。如果向域名系统添加过多功能，消息大小也可能成为问题，并影响可扩展性 [REQ4], 。因此，进行更改变得困难 [REQ11]。根据所介绍的方法，基于域名系统的身份管理可用于无需匿名性的用例，但这些用例需要具备 eIDAS、固定的信任值，以及集中式的证书管理结构。

3.3 物联网集中式身份管理

不仅人类需要身份识别，计算机和物联网设备等事物也需要身份识别。物联网设备往往存在带宽或中央处理器（CPU）等方面的限制。因此，如 [23]所示，会采用不同的协议。Belran 和 Skarmeta [9] 概述了互联网工程任务组（IETF）的受限环境认证与授权（ACE）协议 [69], ，该协议由多份互联网草案（I-D）扩展 [REQ3]。 [87] 的作者使用带有时间属性、名称和位置解析功能的域名系统（DNS），在自然环境中识别并验证物联网对象。这样可以避免效率下降，但未考虑生命周期 [REQ11]。P. N. Mahalle 的博士论文 [51] 探讨了物联网设备的身份管理。尽管其中明确了标识符的上下文，但没有提及用户及其与对象之间的关系 [REQ1] [REQ11]。[33] 关注基于云的物联网。虽然考虑了物联网事物的生命周期，但未考虑所有者 [REQ11]。

3.4 集中式身份管理的结论

结果总结于表 2 中满足互操作性 [REQ3]这一要求。这并不难理解，因为它们完全采用集中式架构。此外，集中式身份管理方法在若干情况下似乎缺乏可信度 [REQ6], 、管理 [REQ1], 和集成 [REQ11]方面的能力。尤其是可信度和集成，是这种模型固有的特性。由于这些方法大多针对计算机用例进行描述，因此很难评估其可移植性 [REQ8] 。

4 联合身份管理

联合身份管理是处于特定信任边界内的多个实体之间的一种安排。它使用户能够使用其所属组织中的同一身份标识，访问参与实体所提供的服务。在许多情形下，需要可信第三方。尤其是 SAML 联邦往往存在可扩展性问题 [REQ4]。不同的联邦身份管理方法之间存在互操作性问题 [REQ3]。责任 [REQ10]取决于所有实体；可信第三方或可提供额外功能，但以下方法并非如此 [REQ5]。Bargh 等人 [8] 指出，IdP 和 SP 数量不断增长是学术界公认的 SAML 问题。因此，不同方法都试图改善联邦身份管理中的信任与元数据交换的可扩展性，以及信任协商。Arias Cabarcos 等人提出的 IdMRep [6] 引入了动态信任值。该方法无法与新成员协同工作 [REQ6]。此外，信任引擎中累积的数据量可能导致大规模基础设施中的单点故障 [REQ4]。Md. Sadek Ferdous 和 Ron Poet 提出的动态身份联邦 [20] 着重于全自动建立联邦和信任。尽管技术层面的建立过程完全自动化，但用户仍须输入身份提供商的实体 ID 并生成代码，因此不够便于使用 [REQ2]。此外，将信任划分为可信、半可信和不可信，粒度相当粗 [REQ6],，而且每个实体都需要额外的数据库 [REQ11]。Pöhn 等人提出的另一种方法称为 TrustBroker [58],，它基于 SAML，但其通用概念也可应用于联邦身份管理 [REQ3]。此外还有其他联邦方法。Moreno 等人提出的 OLYMPUS [53] 能够保护隐私，同时支持分布式身份提供商。然而，它缺少 [REQ3]。Kang 和 Khashnobish [40] 提出的点对点（P2P）联邦方法采用去中心化架构，但在包含大量实体和联邦服务器的大规模基础设施中存在可扩展性问题 [REQ4]。Dhungana 等人 [19]提出了一个基于 UMA 和 OIDC、面向云网络的身份管理框架。因此，它无需采用 OIDC 联邦标准，即可实现联合身份管理 [30] [REQ11]。Isaakidis 等人提出的 UnlimitID [36] 采用基于代数消息认证码（MAC）的基于属性的匿名凭证。该方法可与 OAuth 配合使用，并会使假名过期。不过，在这段有限时间内，用户仍可能被关联起来 [REQ9]。此外，在某些用例中可能不允许使用假名 [REQ11]。采用 MAC 似乎是一种倒退。这些方法表明，联邦身份管理能够解决人们关注的某些方面，但并非全部。此外，尤其是基于 SAML 的联邦身份管理，很难移植到移动应用和物联网设备上 [REQ8]。

4.1 基于域名系统的联合身份管理

ID4me [71] 将 DNS 与 OIDC 相结合。它采用自动证书管理环境（ACME）协议，该协议会自动验证域名所有权，并简化证书的颁发。DNS 挑战用作发现方法，并由域名系统安全扩展提供保护。通信则通过基于 DNS 的命名实体认证（DANE）进行保护，但该机制在实践中很少使用。ID4me 设有身份代理这一角色，该角色负责管理属性，并通过 DNS 进行识别；另一个角色是身份权威机构，用于身份验证。因此，用户必须信任身份代理 [REQ6]。使用 DNS 的想法并不新鲜。Hulsebosch 等人 [35] 提出了在网格环境中结合这些机制，以实现有效且可信的用户控制光路建立。为此，DNS 树用于在虚拟组织（VO）这一联合形式中，动态建立身份提供商与光网络服务提供商（ONSP）之间的技术信任 [REQ3]。

4.2 基于电子身份的联合身份管理

欧盟第 910/2014 号法规，也称为 eIDAS，自 2018 年 9 月起生效。[37] 的作者展示了基于电子身份的联合身份架构。Berbecaru 等人 [13] 提出的方法描述了 eIDAS 与 STORK 之间的连接。STORK [51] [60] 是基于电子身份的电子身份联合体系。它采用欧洲电子身份互操作平台，该平台基于 SAML，每个国家设有一个节点。因此，这是一种异构的大规模基础设施。有几种方法描述了如何将学术属性集成到 eIDAS基础设施中，但未考虑跨联合体系的 eduGAIN；eduGAIN 是学术界事实上的标准联合体系 [14] [15] [REQ11]。Alonso 等人 [4] 提出了一种身份模型，用于将通过 OAuth 2.0 进行身份验证的 FIWARE 服务连接到 eIDAS 节点，从而满足相关法规要求。不过，这一方案仅适用于一种特定用例 [REQ3]。

4.3 联合身份管理即服务

其他方法将联合视为一项服务，并利用云基础设施。Zouari 和 Hamdi 提出的框架 AIDF [88] 采用了信任代理，这与 [58], 云中的做法类似。身份提供商和服务提供商在中央机构注册。服务提供商可以指定所需的身份标识和属性，同时还可以订阅声明转换和属性映射服务。如果属性采用了不同的语义和/或语法，就有必要进行属性映射。日期格式就是一个简单的例子。获得同意后，中央服务会自动在身份提供商和服务提供商之间建立联系。美国国家标准与技术研究院（NIST）的保证级别（LoA）提供了某种信任保证，目前发布于 2017 年《特别出版物 800-63》的第三版中。随着保证级别修订，该框架也需要相应更新。此外，除了 NIST 保证级别之外，也可以采用其他标准 [REQ6]。另外，针对身份提供商尚无信任保证，只有针对服务提供商的信任保证。Zefferer 等人 [86], 提出的方法也存在与 NIST 保证级别相同的缺陷，该方法将身份与电子身份关联起来。尽管电子身份的使用使这些联邦具有坚实的法律基础，但该方法高度定制化，仅适用于这一种用例 [REQ3]。

4.4 联邦身份管理总结

联邦身份管理方法的摘要见表3。联邦身份管理本身缺乏互操作性 [REQ3], 功能性 [REQ5], 和责任 [REQ10] 责任往往伴随着政策和其他协议。可以借助额外的工具实现互操作性，但现有协议本身却像信息孤岛。以 SAML 协议为例，它也缺乏可扩展性 [REQ4] 和可移植性 [REQ8] 。这些方法

表3：联邦式身份管理方法概述

Ref	Name	未满足的需求
	FIM	[REQ3] [REQ5] [REQ10]
[6]	IdMRep	[REQ4] [REQ6]
[20]	动态身份联邦	[REQ2] [REQ6] [REQ11]
[58]	TrustBroker	[REQ3]
[53]	OLYMPUS	[REQ3]
[40]	点对点联邦	[REQ4]
[19]	身份管理框架	[REQ11]
[36]	UnlimitID	[REQ9] [REQ11]
[71]	ID4me	[REQ6]
[35]	VO	[REQ3]
[14] [15]	学术 eIDAS	[REQ11]
[4]	FIWARE eIDAS	[REQ3]
[88]	AIDF	[REQ6]
[86]	电子身份联邦	[需求3] [需求6]

通常存在互操作性 [REQ3] 和可信度 [REQ6]方面的缺陷。此外，虽然常常提及集成 [REQ11]，但责任 [REQ10] 在一定程度上难以评估，因为这取决于具体实现和既定流程。当用户访问其他组织提供的服务时，所属组织与服务提供商、用户与服务提供商，以及用户与所属组织之间都需要建立信任。如果还涉及其他实体，也需要将其纳入信任建立过程。

5 以用户为中心的身份管理

以用户为中心的身份管理让用户能够掌控自己的身份。它从个人电脑上的简单客户端发展到 UMA 和自我主权身份，下文将对此进行介绍。尽管这种方式赋予用户更多权力，从而增加了价值，但 [REQ9], 与其他方法的互操作性较低 [REQ3], ，因为缺少 [REQ5] 。 [REQ10]取决于客户端和提供商。

5.1 面向物联网的以用户为中心的身份管理

Do van Thuan 等人 [78] 提出了一种以用户为中心的物联网身份管理方案，包含四种标识符，即 idpID、domIDPart、devIDPart 和 userIDPart。它们还描述了不同的关系，例如服务于一般人群、永久服务于某一个人、依次服务于多个人，以及同时服务于多个人。尽管所有变体都描述了设备与人员之间的关系，且该方案采用了多种标识符，但并未考虑生命周期本身 [REQ11]。此外，该方案应如何与其他方案和协议交互也尚不明确 [REQ3]。

5.2 采用 UMA 的以用户为中心的身份管理

Kumar 等人 [47] 和 Slomovic [70] 发表的研究表明，假名性和匿名性在某些用例中可能很重要。来自不同社交网络的身份可以汇总起来，并关联到同一个人。UMA 能够将身份解析与身份信息的维护解耦 [44] [50] [52] [17] ；

Cruz-Piris 等人甚至发表了一种用于物联网的应用。尽管 UMA 基于 OAuth，但这一原则也可以应用于 SAML [68]。然而，UMA 的原则或许无法应用于所有用例 [REQ3]。

5.3 基于自我主权身份（SSI）的用户中心型身份管理

Toth 和 Anderson- Priddy [77] 描述了自我主权身份管理的原则。Ferdous 等人 [21] 将身份法则从存在、自主、所有权、访问、单一来源、保护、可用性和持久性，扩展为自我主权身份所具备的用户控制与同意、受限用途下的最少披露、可证明正当的主体、定向身份、运营者和技术的多元化、人类集成，以及跨情境的一致体验。Sovrin [75] 将这一进展视为身份管理的一种演进。

自我主权身份通常通过区块链实现。万维网联盟（W3C）提出的去中心化标识符（DID）是一种新型标识符，用于可验证的去中心化数字身份。Stokkink 和 Pouwelse [73] 提出的 Claim Chain 是一种纯粹基于声明模型构建的自我主权身份方案，已得到实际应用，但限制也相当多。未经同意不会发送任何数据，但与此同时，也只能使用经认证的属性 [REQ3]。Friebe 等人 [24] 和 Steichen 等人 [72] 提出的 DecentID 基于以太坊智能合约，旨在保护属性隐私。出于可扩展性考虑，该方案利用分布式哈希表（DHT）等外部存储来存储属性。节点无法高效处理大型文件 [REQ4]。此外，还需要将身份关联到中心化注册合约 [REQ9]。Sora Identity [74] 将用户的手机作为主要参与方之一。尽管这种方案能够保护隐私，但设备的生命周期以及使用不同设备可能会带来问题 [REQ8]。另一种基于区块链的方案将其与公钥基础设施（PKI）结合 [82] [7] [REQ3]。这些方案支持撤销证书，但存在可扩展性问题 [REQ4]。Horcux Protocol [55][56] 是一种使用自我主权身份和生物特征开放协议标准（BOPS）的去中心化生物特征凭证存储方案。尽管生物特征识别容易出现假阳性和假阴性，且其实现往往存在缺陷，该方案仍采用了生物特征识别 [REQ7]。在 [65], Schanzen

bach 和 Banse 描述了一种采用 NameID [46]、改编自 UMA 的方法。由于他们使用安全的名称系统——GNU 名称系统（GNS）——来存储数据，因此不需要全球性的公共账本，也不会损害用户的隐私。Ahadipour 和 Schanzenbach [1] 介绍了一项关于分布式系统中授权的综述。在 [66], 中，作者介绍了去中心化基于属性的委托（ABD）。Schanzenbach 等人的 reclaimID [67] 基于此前发表的研究。属性通过基于属性的加密（ABE）进行加密，这意味着属性使用与用户身份关联的私钥进行自签名。该方法允许使用一个或多个

具有不同属性的身份。不过，隐私以及对属性的信任可能也是缺点之一 [REQ6] [REQ9]。

5.4 面向云环境的自我主权身份用户中心身份管理

身份钱包平台 CREDENTIAL [79] [45] [42] [32] 旨在开发一个安全且保护隐私的数据共享平台，让用户拥有完全控制权。 [32] 展示了如何将代理重加密和可编辑签名技术整合到其工作流程中，本质上相当于一个中间人。该平台有三类主要参与者：钱包平台、用户和数据接收方；数据接收方可以是用户，也可以是服务提供商，如 [42]所述。文中提出了一种保留元数据的高层架构，但由于日志文件可能泄露信息 [REQ7]，在实践中或许难以实现。Kostopoulos 等人 [45] 介绍了 CREDENTIAL 的架构。该架构缺少与现有协议的接口[REQ3] [REQ11]。最后，Veseli 等人 [79] 着重探讨隐私保护设计。LINDDUN（可链接性、可识别性、不可否认性、可检测性、信息泄露、内容不知情以及政策与同意不合规）方法 [18], 是一种隐私威胁分析框架，用于实现隐私保护设计。因此
，
尽管该方法基于云，数据仍经过加密。用户必须信任钱包提供商 [REQ3] [REQ6] [REQ11]。

5.5 以自我主权身份为联合的以用户为中心的身份管理

Halpin 等人提出的 NEXTLEAP [28] 是一种联邦身份管理方法，它基于消息认证码使用盲签名，以改进 OIDC。身份本身是一种注重隐私的区块链身份，并采用去中心化公钥基础设施。因此，访问控制以去中心化的方式进行。尽管其目的是实现安全消息传递，但在大规模基础设施中，可扩展性可能成为一项缺点 [REQ4]。 [49] 的设计考虑了跨组织身份验证系统。单向哈希可实现一次性密码本密码的概念，从而提供不可链接性。遗憾的是，该方法并未清楚说明性能表现 [REQ4]。

5.6 以自我主权身份为云联合的以用户为中心的身份管理

欧盟 SUNFISH 项目的目标是建立云联合，参见 Alansari 等人 [2] [3]。云联合是一种组织间的协作，各组织共享托管在各自私有云基础设施上的数据，以创造商业机会。尽管该方法以保护隐私的方式引入了分布式访问，但必须事先识别并验证用户身份。eIDAS 可作为信任来源，但云联合中的信任关系并未得到清楚说明 [REQ6]。通过使用令牌而非属性来实现用户匿名性的做法听起来颇有前景，但令牌并非在所有场景下都适用。此外，该方法完全基于英特尔软件防护扩展（SGX） [REQ11]。Bendiab 提出的动态云联合方法从动态云联合发展到结合模糊认知图动态信任模型的区块链 [43] [11] [10] [12]。在 [43], 中，作者介绍了包含用户、云服务提供商等实体的基本方法
r
（云服务提供商）、身份提供商、联合提供商（FP）和证书颁发机构。该令牌会从一个联合提供商（FP）发送到另一个联合提供商（FP），以进行验证和转换。云服务提供商会验证令牌的合法性，之后用户才能访问云服务。也可以通过一个简单的代理，在两个协议（如 eduGAIN 中的 SAML 和 OIDC）之间完成此操作 [REQ4]。 [11]中介绍了信任。每个用户都从受信任的身份提供商处获得自己的身份。如果云服务提供商不信任该身份提供商，双方可以实时计算彼此之间的信任。根据计算结果建立连接。作者描述了一种复杂的信任评估方法，该方法依据多种特征进行评估，例如安全和隐私，但这些因素难以衡量和获取 [REQ6]。随后，信任被存入区块链 [10]。云服务提供商无需依赖身份提供商等集中式机构，即可动态、分布式地管理信任关系。不过，这需要一个信任管理平台（TMP），并且云服务提供方负责验证其注册用户的身份。 [12]是下一步，使用模糊认知图对信任关系进行建模和评估。它采用一种信任计算模型，与前文介绍的特征类似。如果有更多信息可用，该模型就能计算未知实体的信任度。遗憾的是，该方法未考虑保证级别方法，例如信任向量（VoT） [61] [REQ6] [REQ11]。该方法有助于构建安全的基础设施即服务（IaaS）云联合。尽管该方法采用了匿名方法，但仍会将个人信息存储在外部数据库中 [REQ9]。此外，该方法仅关注一个用例 [REQ3]。

5.7 以用户为中心的身份管理总结

表4总结了以用户为中心的身份管理方法。UCIM 在互操作性 [REQ3],功能性 [REQ5], 和责任 [REQ10],方面存在不足，不过较早的方法、UMA 和自我主权身份之间也有差异。在自我主权身份中，这在一定程度上取决于用例、集中式／去中心化管理等因素。文中介绍的 UMA 方法缺少互操作性 [REQ3]。UMA 的原则应该适用于许多用例，但据作者所知，这一点尚未得到进一步探讨。面向物联网的 UCIM 在集成 [REQ11] 方面存在问题，想必在互操作性 [REQ3]方面也有问题。考察文中介绍的自我主权身份方法时，常会提及可扩展性 [REQ4]和隐私 [REQ9] 。许多方法只在较小规模的环境中经过测试，因此会产生可扩展性问题。隐私似乎与这些方法以用户为中心的特点相矛盾。并非所有方法都注重隐私，其他一些方法似乎也存在相关问题。对于云和联合用例，可扩展性 [REQ4],、可信度 [REQ6], 和集成 [REQ11] 往往有所欠缺。可信度问题较为棘手，因为用户对自己的数据拥有更多控制权，而服务提供商则需要信任用户的属性。

6 结论与未来工作

如今，安全是网络环境中的一项关键需求。身份无处不在，随着身份盗窃日益猖獗，安全的身份管理比以往更加重要。本文扩展了已知需求。基于新的方法、异构环境以及可能的用例，我们新增了一些需求。同时，其他一些需求也被重新

表4：以用户为中心的身份管理方法概述

Ref	Name	未满足的需求
	UCIM	[REQ3] [REQ5] [REQ10]
[78]	面向物联网的UCIM	[REQ3] [REQ11]
[44]	UMA	[REQ3]
[17]	物联网的 UMA	[REQ3]
[73]	Claim Chain	[REQ3]
[24]	DecentID	[REQ4] [REQ9]
[72]	IPFS 的自我主权身份	[REQ4] [REQ9]
[74]	Sora Identity	[REQ8]
[82] [7]	基于区块链的 PKI 管理框架	[REQ3] [REQ4]
[55] [56]	Horcux 协议	[REQ7]
[67]	reclaimID	[REQ6] [REQ9]
[79]	CREDENTIAL	[REQ3] [REQ6] [REQ7] [REQ11]
[28]	NEXTLEAP	[REQ4]
[49]	基于区块链的 AAA 系统	[REQ4]
[2] [3]	SUNFISH	[REQ6] [REQ11]
[43]	动态云联邦联	[REQ3] [REQ4] [REQ6] [REQ9] [REQ11]

定义。身份管理 [REQ1]是一项新的需求，而功能性 [REQ5] 对于这些方法之间的互操作性仍然不可或缺。《通用数据保护条例》促使需求从移动性转向可移植性 [REQ8],，因为用户可以要求迁移其账户，而且人们使用的不同设备也越来越多。这也使原本的可负担性被拆分为可扩展性 [REQ4] 和集成 [REQ11],。

接下来，我们将概述不同的身份管理方法，并按身份管理模型和用例进行分类。这些方法涵盖特定用例的集中式身份管理、联合身份管理，以及以用户为中心的方法，例如用户管理访问和自主主权身份。我们将这些方法与推导出的需求进行比较，从而概述其优势与不足。

集中式方法缺乏互操作性 [REQ3], 可信度 [REQ6], 管理 [REQ1], 和集成 [REQ11]。无法评估可移植性 [REQ8] 。这些缺陷是该模型固有的。联合身份管理普遍存在互操作性 [REQ3], 功能性 [REQ5], 和责任 [REQ10]方面的问题。SAML 同样缺乏可扩展性 [REQ4] 和可移植性 [REQ8] 。所述联邦身份管理方法还存在可信度 [REQ6] 和集成 [REQ11] 方面的缺陷。以用户为中心的身份管理在互操作性 [REQ3], 功能性 [REQ5], 和责任 [REQ10]方面存在不足。此外，可信度 [REQ6] 也是一个问题。视具体方法而定，可扩展性 [REQ4] 和集成 [REQ11] 也可能无法实现。没有任何一种方法能够满足所有需求。所述方法未涵盖两项需求：责任 [REQ10] 和功能性 [REQ5]。责任主要由所属组织承担，而其他方法则试图满足功能性 [REQ5]。互操作性 [REQ3] 和可信度 [REQ6] 或许能在某种方法或模型内部实现，但无法跨方法或模型实现。因此，集成 [REQ11]也很困难。简单地将不同方法结合起来，并不能满足既定需求。并行运行多种方法会耗费更多人力和时间。此外，这还可能导致政策各异，数据库进一步变得不一致。因此，至少需要提供概览并建立各方法之间的连接器，以便它们相互交互并提供整体概览。要满足所有需求，还需要进一步开展工作。

因此，利益相关者将受益于一个涵盖不同模型及相应方法的框架。该框架需要足够灵活，以支持未来的工作。为满足尚未满足的需求，该框架需要包含其他工具和推荐流程，包括不同方法之间的连接器以及一份概述。未来，我们计划在整体框架的设计中开发缺失的组件。下一步将针对不同用例调整该框架。此外，还将对身份管理模型进行分类。

参考文献

[1]Ava Ahadipour 和 Martin Schanzenbach。2017 年。分布式系统中的授权综述：信息存储、数据检索与信任评估。载于第 *16* 届 *IEEE* 国际可信、安全与隐私计算和通信会议，。IEEE，1016–1023。http://dx . . 10.1109 .2017.346 [2] doi org/ /Trustcom/BigDataSE/ICESS Shorouq Alansari、Federica Paci、Andrea Margheri 和 Vladimiro Sassone。2017 年。云联合体中的隐私保护访问控制。载于*2017* 年 *IEEE* 第 *10* 届云计算国际会议（*CLOUD*）。757–760。https://doi . 10.1109 .2017.108 org/ /CLOUD Shorouq Alansari、Federica Paci [3] 和 Vladimiro Sassone。2017 年。云联合体分布式访问控制系统。载于*2017* 年 *IEEE* 第 *37* 届分布式计算系统国际会议（*ICDCS*）。2131–2136。https://doi . 10.1109 .2017.241 org/ /ICDCS Alvaro Alonso、Alejandro Pozo、[4] Johnny Choque、Gloria Bueno、Joaquin Salvachúa、Luis Diez、Jorge Marìn 和 Pedro Luis Chas Alonso。2019 年。依据 eIDAS 欧洲法规为 FIWARE OAuth 2.0 服务提供访问的身份框架。*IEEE Access*（2019 年），88435–88449。https://doi . 10.1109 .2019.2926556 org/ /ACCESS W. A. Alrodhan 和 C. J. [5] 2007 Mitchell。年。解决 CardSpace 中的隐私问题。载于第三届信息保障与安全国际研讨会。285–291。https://doi。org/10。1109/IAS。2007。12[6] Patricia Arias Cabarcos、Florina Almenárez、Félix Gómez Mármol 和 Andrés Marín。2013 年。是否进行联合：一种用于推动身份管理中合作的基于声誉的机制。《无线个人通信》（2013 年），1–18。https://doi。org/10。1007/s11277-013-1338-y [7] Louise Axon 和 Michael Goldsmith。2017 年。PB-PKI：一种注重隐私的基于区块链的公钥基础设施。载于第 *14* 届电子商务与电信国际联合会议论文集——第 *6* 卷：*SECRYPT*（*ICETE 2017*）。INSTICC、SciTePress，311 318 0006419203110318 –。https://doi。org/10。[8] 2011 5220/ Mortaza S. Bargh、Bob Hulsebosch 和 Hans Zandbelt。年。跨联邦的信任与元数据交换的可扩展性。*TNC*（2011 年）。[9] V. Beltran 和 A. F. Skarmeta。2016 年。CoAP 委托授权概述：受限环境认证与授权（ACE）。载于*2016* 年 *IEEE* 第三届物联网世界论坛（*WF-IoT*）。706–710。https://doi。org/10。1109/WF-IoT。2016。7845482[10] Gueltoum Bendiab、Nicholas Kolokotronis、Stavros Shiaeles 和 Samia Boucherkha。2018 年。WiP：一种新颖的云身份管理基于区块链的信任模型。载于*2018* 年 *IEEE* 第 *16* 届可靠、自主与安全计算国际会议、第 *16* 届普适智能与计算国际会议、第 *4* 届大数据智能与计算及网络科学与技术大会（*DASC/PiCom/DataCom/CyberSciTech*）。724–729。https://doi . 10.1109 .2018.00126 org/ / [11] 2018 DASC/PiCom/DataCom/CyberSciTec Gueltoum Bendiab、Stavros Shiaeles 和 Samia Boucherkha。年。面向“云端”联合身份管理的新型动态信任模型。载于*2018* 年第 *9* 届 *IFIP* 新技术、移动性与安全国际会议（*NTMS*）。1–5。https://doi。org/10。1109/NTMS。2018。8328673

[12] Gueltoum Bendiab、Stavros Shiaeles、Samia Boucherkha 和 B.V. Ghita。2019 年。FCMDT：一种用于云联邦身份管理的新型模糊认知图动态信任模型。《计算机与安全》（2019 年 6 月）。https://doi . 10.1016 . .2019.06.011 org/ /j cose Diana Berbercaru、[13] Andrea Atzeni、Marco de Benedictis 和 Paolo Smiraglia。2017 年。迈向更强的数据安全：电子身份管理基础设施。载于2017 年第 25 届 Euromicro 并行、分布式和网络处理国际会议（PDP）。 391 395 . 10.1109 .2017.90 –。https://doi org/ /[14] 2018 PDP Diana Berbercaru 和 Antonio Lioy。年。将学术属性集成到 eIDAS 基础设施中以支持跨境服务。载于2018 年第 22 届系统理论、控制与计算国际会议（ICSTCC）。691–696。https://doi . 10.1109 .2018.8540674 org/ /ICSTCC Diana Berbercaru、Antonio Lioy [15] 和 Cesare Cameroni。2019 年。大学电子身份：基于 eIDAS 基础设施构建跨境服务。《信息》 10, 6 2019 10060210 （）。[16] 2015 https://doi.org/10.3390/info H. Boujezza、M. AL-Mufti、H. K. B. Ayed 和 L. Saidane。年。物联网身份管理系统分类。载于2015 年 IEEE/ACS 第 12 届计算机系统与应用国际会议（AICCSA）。1–8。https://doi . 10.1109 .2015.7507266 org/ /AICCSA Luis Cruz-Piris、[17] Diego Rivera、Ivan Marsa-Maestre、Enrique De la Hoz 和 Juan R. Velasco。2018 年。基于将通信过程建模为资源的物联网环境访问控制机制。《传感器》18 卷第 3 期（2018 年 3 月）， 917 18030917 。https://doi.org/10.3390/s Mina Deng、Kim Wuyts、[18] Riccardo Scandariato、Bart Preneel 和 Wouter Joosen。2011 年。隐私威胁分析框架：支持隐私需求的 elicitation 与满足。《需求工程》16 卷第 1 期（2011 年 3 月），3–32。https://doi.org/10.1007/s 00766 010 0115 7 - - - R. D. Dhungana、A. [19] Mohammad、A. Sharma 和 I. Schoen。2013 年。云网络基础设施身份管理框架。载于2013 年第 9 届信息技术创新国际会议（IIT）。13–17。https://doi . 10.1109 .2013.6544386 org/ /Innovations Md.Sadek Ferdous 和 [20] 2013 Ron Poet。年。使用安全断言标记语言（SAML）的动态身份联合。载于《身份管理政策与研究》，Simone Fischer-Hübner、Elisabeth de Leeuw 和 Chris Mitchell（编）。IFIP 信息与通信技术进展，第 396 卷。Springer Berlin Heidelberg，131–146。https://doi.org/10.1007/ 978 3 642 37282 7_13 - - - - Md Sadek Ferdous、Farida Chowdhury 和 [21] Madini O. Alassafi。2019 年。探索利用区块链技术实现自主主权身份。《 IEEE Access 》 7 （2019 年）， 103059 103079 . 10.1109 .2019.2931173 –。https://doi org/ /[22] 2012 ACCESS M. S. Ferdous 和 R. Poet。年。身份管理系统比较分析。载于2012 年高性能计算与仿真国际会议（HPCS）。 454 461 . 10.1109 .2012.6266958 –。[23] 2017 https://doi org/ /HPCSim I. Florea、R. Rughinis、L. Ruse 和 D. Dragomir。年。物联网标准化协议综述。载于2017 年第 21 届控制系统与计算机科学国际会议（CSCS）。190–196。https://doi . 10.1109 .2017.33 org/ /CSCS Sebastian Friebe、Ingo Sobik 和 [24] Martina Zitterbart。2018 年。DecentID：利用智能合约实现去中心化且保护隐私的身份存储系统。载于2018 年第 17 届 IEEE 国际可信、安全与隐私计算和通信会议暨第 12 届 IEEE 大数据科学与工程国际会议（TrustCom/BigDataSE）。37–42。https://doi . 10.1109 .2018.00016 org/ /TrustCom/BigDataSE F. Gao、F. [25] 2016 Zhang、J. Xia 和 Z. Ma。年。大数据分析通用身份管理模型。载于2016 年第 18 届先进通信技术国际会议（ICACT）。 1 1 . 10.1109 .2016.7423325 –。https://doi [26] 2016 . . . org/ /ICACT GÉANT。年。eduGAIN 技术网站。https://technical edugain org/status php。[在线，1 月 3, 2023]。[27] Samia El Haddouti 和 M. Dafir Ech-Cherif El Kettani。2019 年。使用区块链技术分析身份管理系统。载于2019 年先进通信技术与网络国际会议（CommNet）。 1 7 . 10.1109 .2019.8742375 –。https://doi org/ /COMMNET Harry [28] 2017 Halpin。年。NEXTLEAP：以隐私保护方式实现身份去中心化，保障安全消息传递。载于第 12 届可用性、可靠性与安全国际会议论文集（意大利雷焦卡拉布里亚）（ARES '17）。ACM，纽约，美国， 92 1 92 10 . 10.1145 3098954.3104056 : – : 。https://doi org/ / D. [29] 2012 *2 0* Hardt。年。OAuth . 授权框架。RFC 6749。RFC编辑部。http://www.rfc-editor.org/rfc/rfc6749.txt http://www.rfc-editor.org/rfc/rfc6749.txt。[30] Roland Hedberg、Michael B. Jones、Andreas Solberg、Samuel Gulliksson 和 John Bradley。2019 年。OpenID Connect联邦1.0——草案 10。OpenID 规范。OpenID 基金会。[31] Jorge Lopez Hernandez-Ardieta、John Heppe 和 Jose Fernando Carvajal-Vion。2010 年。STORK：欧洲电子身份互操作平台。《IEEE拉丁美洲汇刊》8 卷第 2 期（2010 年 4 月），190–193。https://doi.org/10.1109/TLA.2010.5514447

[32]Felix Hörandner、Stephan Krenn、Andrea Migliavacca、Florian Thiemer 和 Bernd Zwattendorfer。2016 年。《CREDENTIAL：一种保护隐私的云端数据共享框架》。载于《2016 年第 11 届可用性、可靠性与安全国际会议（ARES）》。742–749。https://doi . 10.1109 .2016.79 org/ /ARES Susmita Horrow 和 [33] Anjali Sardana。2012 年。云端物联网身份管理框架。载于《首届物联网安全国际会议论文集》（印度科拉姆）（Secu- rIT 12）。计算机协会，美国纽约州纽约市，200–203。https://doi . 10.1145 2490428.2490456 org/ / Bob Hulsebosch、[34] Gabriele Lenzini 和 Henk Eertink。2009 年。D2.3——质量认证方案。交付成果。STORK-eID联盟。[35] R. J. Hulsebosch、Mortaza Bargh、P. H. Fennema、J. F. Zandbelt、Martin Snijders 和 Henk Eertink。2006 年。利用身份管理与安全 DNS，实现有效且可信的用户控制型光路建立。载于《国际网络与服务会议》（ICNS'06）。79–79。https://doi . 10.1109 .2006.115 org/ /ICNS Marios [36] Isaakidis、Harry Halpin 和 George Danezis。2016 年。UnlimitID：使用代数消息认证码的隐私保护型联合身份管理。载于《2016 年 ACM 电子社会隐私研讨会论文集》（奥地利维也纳）（WPES '16）。ACM，美国纽约州纽约市，139–142。https://doi . 10.1145 2994620.2994637 org/ / Carretero Jesus、Guillermo [37] Izquierdo-Moreno、Mario Vasile-Cabezas 和 Javier Garcia-Blas。2018 年。欧洲电子身份系统的联合身份架构。《IEEE Access》6（2018），75302–75326。https://doi . 10.1109 .2018.2882870 org/ /ACCESS Isaac Henderson [38] Johnson Jeyakumar、Sven Wagner 和 Heiko Roßnagel。2019 年。为物联网传感器网络中的故障自动验证实现分布式轻量级信任基础设施。载于《2019年开放身份峰会》，Heiko Roßnagel、Sven Wagner 和 Detlef Hühnlein（编）。德国计算机学会，波恩，83–93。[39] Leif Johansson。2012 年。保障等级（LoA）配置文件的 IANA 注册表。RFC 6711。RFC编辑部。[40] Myong Kang 和 Amitabh Khashnobish。2009 年。一种点对点联合身份验证系统。载于《2009 年第六届信息技术：新一代国际会议》。 382 387 . 10.1109 .2009.159 – 。[41] 2015 https://doi org/ /ITNG Kantara Initiative。 。主页 – WG – 用户管理的访问。https://kantarainitiative.org/confluence/display/uma/Home。[在线，1 月 3, 2023]。[42] Farzaneh Karegar、Christoph Striecks、Stephan Krenn、Felix Hörandner、Thomas Lorünser 和 Simone Fischer-Hübner。2016 年。CREDENTIAL 的机遇与挑战。施普林格国际出版，尚，76–91。https://doi.org/10.1007/ 978 3 319 55783 0_7 - - - - Bendiab Keltoum 和 Boucherkha [43] Samia。2017 年。一种面向云环境的动态联合身份管理方法。载于《第二届物联网、数据与云计算国际会议论文集》（英国剑桥）（ICC '17 104, 5 . 10.1145 ）。ACM，美国纽约州纽约市，文章页码。https://doi org/ / 3018896.3025152 Fumiko Kobayashi 和 John R. [44] 2014 Talburt。 。将身份解析与身份信息维护分离。载于《2014 年第 11 届信息技术：新一代国际会议》。349–354。https://doi.org/10.1109/ITNG.2014.88[45]Alexandros Kostopoulos、Evangelos Sfakianakis、Ioannis Chochliouros、John Sören Pettersson、Stephan Krenn、Welderufael Tesfay、Andrea Migliavacca 和 Felix Hörandner。2017 年。迈向采用安全云身份服务。载于《第 12 届可用性、可靠性与安全国际会议论文集》（意大利雷焦卡拉布里亚）（ARES '17）。ACM，美国纽约州纽约市， 90 1 90 7 . 10.1145 3098954.3104061 : – : 。https://doi org/ / [46] 2016 + = Daniel Kraft。 。Namecoin OpenID NameID！https://nameid.org。 [在线，1 月 3, 2023]。[47] Deepesh Kumar Srivastava、Basav Roychoudhury 和 Harsh Vardhan Samalia。2018 年。用户配置文件属性在多个在线社交网站之间身份匹配中的重要性。载于《2018 年第 8 届云计算、数据科学与工程国际会议（Confluence）》。14–15。https://doi . 10.1109 .2018.8442455 org/ / [48] CONFLUENCE Sejun Lee、Jaehoon Paul Jeong 和 Jung-Soo Park。2016 年。DNSNA：物联网设备的 DNS 名称自动配置。载于《2016 年第 18 届先进通信技术国际会议（ICACT）》。1–1。https://doi . 10.1109 .2016.7423411 [49] org/ /ICACT Peggy Joy Lu、Lo-Yao Yeh 和 Jiun-Long Huang。2018 年。一种利用区块链技术的隐私保护型跨组织身份验证／授权／计费系统。载于《2018 年 IEEE 国际通信会议（ICC）》。 1 6 . 10.1109 .2018.8422733 – 。[50] https://doi org/ /ICC Maciej P. Machulak、Eve L. Maler、Domenico Catalano 和 Aad van Moorsel。2010 年。对网络资源的用户管理访问。载于《第 6 届 ACM 数字身份管理研讨会论文集》（美国伊利诺伊州芝加哥）（DIM 10）。计算机协会，美国纽约州纽约市，35–44。https://doi.org/10.1145/1866855.1866865

[51] Parikshit N. Mahalle。2014 年。物联网身份管理框架。学位论文。[52] Eve Maler。2015 年。借助用户管理访问扩展同意的效力：一种支持异步、可集中管理且可扩展至互联网的同意标准架构。载于《2015 年 IEEE 安全与隐私研讨会》。175–179。https://doi.org/10.1109/SPW.2015.34[53] Rafael Torres Moreno、Jorge Bernal Bernabe、Antonio Skarmeta、Michael Stausholm、Tore Kasper Frederiksen、Noelia MartÃnez、Nuno Ponte、Evangelos Sakkopoulos 和 Anja Lehmann。2019 年。OLYMPUS：迈向面向隐私且用户友好的无感知身份管理服务。载于《2019 年全球物联网峰会（GIoTS）》。1 6 . 10.1109 .2019.8766357 –。https://doi org/ /[54] 2003 GIOTS R. Oppliger。。Microsoft .Net Passport：安全分析。《Computer》36，7（7 月 2003 29 35 . 10.1109 .2003.1212687），–。[55] 2018 https://doi org/ /MC Asem Othman 和 John Callahan。。魂器协议：一种去中心化生物特征自我主权身份方法。载于《2018 年国际神经网络联合会议（IJCNN）》。1–7。https://doi . 10.1109 .2018.8489316 org/ /IJCNN Asem Othman 和[56] 2019 John Callahan。。魂器协议：一种分布式移动生物特征自我主权身份协议。施普林格国际出版，尚， 355 377 978 3 030 26972 2_17 –。[57] 2014 https://doi.org/10.1007/ - - - - Daniela Pöhn、Stefan Metzger 和 Wolfgang Hommel。。面向动态联合和跨联合的 SAML 元数据代理。载于《INFOCOMP 2014 论文集，第四届先进通信与计算国际会议》（法国巴黎）。IARIA，132–137。ISBN：978-1-61208-365-0。[58] Daniela Pöhn、Stefan Metzger 和 Wolfgang Hommel。2014 年。Géant-TrustBroker：对基于 SAML 的跨联合身份验证与授权基础设施进行动态、可扩展的管理。载于《ICT 系统安全与隐私保护》，Nora Cuppens-Boulahia、Frédéric Cuppens、Sushil Jajodia、Anas Abou El Kalam 和 Thierry Sans（编）。IFIP 信息与通信技术进展，第 428 卷。Springer Berlin Heidelberg，307–320。https://doi.org/10.1007/ 978 3 642 55415 5_25 - - - - Nick[59] Ragouzis、John Hughes、Rob Philpott 和 Eve Maler。2008 年。《安全断言标记语言（SAML）V2.0 技术概述》。技术报告。OASIS。[60] Carlos Ribeiro、Herbert Leitold、Simon Esposito 和 David Mitzam。2018 年。STORK：一个真实、异构、大规模的电子身份管理系统。《Int. J. Inf. Secur.》17，5（2018 年 10 月），569–585。https://doi.org/10.1007/s10207-017-0385-x [61] J. Richer 和 L. Johansson。2018 年。信任向量。RFC 8485。RFC编辑部。http://www.rfc-editor.org/rfc/rfc8485.txt http://www.rfc-editor.org/rfc/rfc8485.txt。[62] Heiko Roßnagel。2017 年。一种发现和验证信任方案成员资格的机制：最轻量级参考架构。载于《2017 年开放身份峰会》，Lothar Fritsch、Heiko Roßnagel 和 Detlef Hühnlein（编）。德国计算机学会，波恩，81–92。[63] Heiko Roßnagel 和 Sven Wagner。2019 年。LIGHTest。《Datenschutz und Datensicherheit - DuD》43，4（2019 年 4 月），220–224。https://doi.org/10.1007/s 11623 019 1096 4 - - - Nat[64] Sakimura、John Bradley、Michael B. Jones、Breno de Medeiros 和 Chuck Mortimore。2014 年。OpenID Connect Core 1.0。技术报告。OpenID Foundation。[65] Martin Schanzenbach 和 Christian Banse。2016 年。通过去中心化安全命名系统管理和呈现用户属性。载于《数据隐私管理与安全保障》。第 11 届数据隐私管理国际研讨会（DPM 2016）和第 5 届安全保障国际研讨会（QASA 2016）。《欧洲计算机安全研究研讨会》，希腊克里特岛伊拉克利翁，213–220。http://dx.doi.org/10.1007/ 978 3 319 47072 6_14 - - - - Martin Schanzenbach、[66] Christian Banse 和 Julian Schütte。2018 年。利用安全命名系统实现实用的去中心化基于属性的委托。载于《计算与通信中的信任、安全与隐私国际会议（TrustCom）》。IEEE，244–251。http://dx . . 10.1109 .2018.00046 [67] doi org/ /TrustCom/BigDataSE Martin Schanzenbach、Georg Bramm 和 Julian Schütte。2018 年。reclaimID：利用命名系统和基于属性的加密实现安全的自主主权身份。载于《2018 年第 17 届 IEEE 可信、安全与隐私计算和通信国际会议暨第 12 届 IEEE 大数据科学与工程国际会议（TrustCom/BigDataSE）》。946–957。https://doi . 10.1109 .2018.00134 org/ /TrustCom/BigDataSE[68] 2013 Michael Schwartz。。使用 SAML 和 UMA 设置反向代理的示例。https://www.gluu.org/blog/recipe-for-a-reverse-proxy-using-saml-and-uma/。[在线，1 月 3, 2023]。[69] L. Seitz、S. Gerdes、G. Selander、M. Mani 和 S. Kumar。2016 年。受限环境中的身份验证与授权用例。RFC 7744。RFC编辑部。[70] Anna Slomovic。2014 年。身份验证中的隐私问题。《IEEE Security Privacy》12, 3 2014 71 73 . 10.1109 .2014.52（5 月），–。[71] 2019 https://doi org/ /MSP Katja Speck。。独立的联合数字身份管理解决方案 ID4me 宣布在 CloudFest 2019 上启动公开测试版。https://id4me.org/独立的联邦式数字身份管理解决方案 \-id4me-宣布在 C[线上，1月 3, 2023]。[72] Mathis Steichen、Beltran Fiz、Robert Norvill、Wazen Shbair 和 Radu State。2018 年。基于区块链的去中心化 IPFS 访问控制。载于*2018 IEEE* 国际物联网会议（*iThings*）、*IEEE* 绿色计算与通信会议（*GreenCom*）、*IEEE* 网络、物理与社会计算会议（*CPSCom*）和 *IEEE* 智能数据会议（*SmartData*）。1499–1506。https://doi . 10.1109 _2018.2018.00253 org/ /Cybermatics[73] 2018 Quinten Stokkink 和 Johan Pouwelse。。基于区块链的自主主权身份部署。载于*2018 IEEE* 国际物联网会议（*iThings*）、*IEEE* 绿色计算与通信会议（*GreenCom*）、*IEEE* 网络、物理与社会计算会议（*CPSCom*）和 *IEEE* 智能数据会议（*SmartData*）。1336 1342 . 10.1109 _2018.2018.00230 – 。[74] 2018 https://doi org/ /Cybermatics Makoto Takemiya 和 Bohdan Vanieiev。。Sora Identity：区块链上的安全数字身份。载于*2018 IEEE* 第 *42* 届年度计算机软件与应用会议（*COMPSAC*），第 02 卷。582–587。https://doi . 10.1109 .2018.10299 org/ /COMPSAC Andrew Tobin 和[75] Drummond Reed。2017 年。自主主权身份的必然崛起。https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sov ereign-Identity。pdf [在线，1月 3, 2023]。[76] J. Torres、M. Nogueira 和 G. Pujolle。2013 年。《未来网络身份管理综述》。*IEEE*通信调查与教程 15, 2（第二 2013 787 802 . 10.1109 .2012.072412.00129），–。https://doi org/ /[77] 2019 SURV Kalman Toth 和 Alan Anderson-Priddy。《自主数字身份：身份范式的转变》。*IEEE*安全与隐私 17, 3（2019 年 5 月），17–27。https://doi . 10.1109 .2018.2888782 org/ /MSEC Do van Thuan、Pranas Butkus[78] 和 Do van Thanh。2014 年。《物联网的用户中心身份管理》。载于*2014* 年 *IT* 融合与安全国际会议（*ICITCS*）。1–4。https://doi . 10.1109 .2014.7021724 org/ /[79] ICITCS Fatbardh Veseli、Jetzabel Serna Olvera、Tobias Pulls 和 Kai Rannenberg。2019 年。《通过设计实现隐私保护：身份钱包平台设计与实施的经验教训》。载于第 *34* 届 *ACM/SIGAPP*应用计算研讨会论文集 （塞浦路斯利马索尔）*(SAC'19)*。ACM，美国纽约州纽约， 1475 1483 . 10.1145 3297280.3297429 –。https://doi org/ / Georg[80] Wagner、Olamide Omolola 和 Stefan More。2017 年。《协调委托数据格式》。载于 *2017* 年开放身份峰会，Lothar Fritsch、Heiko Roßnagel 和 Detlef Hühnlein（编）。德国计算机学会，波恩，25–34。[81] Georg Wagner、Sven Wagner、Stefan More 和 Martin Hoffmann。2019 年。《基于域名系统的信任方案发布与发现》。载于*2019*年开放身份峰会，Heiko Roßnagel、Sven Wagner 和 Detlef Hühnlein（编）。德国计算机学会，波恩，49–58。[82] Alexander Yakubov、Wazen M. Shbair、Anders Wallbom、David Sanda 和 Radu State。2018 年。《基于区块链的 PKI 管理框架》。载于*NOMS 2018 - 2018* 年 *IEEE/IFIP*网络运行与管理研讨会。1–6。https://doi . 10.1109 .2018.8406325 org/ /NOMS Yanjiong Wang 和 Qiaoyan[83] 2011 Wen。《面向物联网的增强隐私域名系统方案》。载于*IET*国际通信技术与应用会议（*ICCTA 2011*）。699–702。https://doi . 10.1049 .2011.0758 org/ /cp Ian[84] 2009 A. Young 和 Chad La Joie。《联合身份系统互联与元数据交换：概念与方法》。http://iay。org。uk/blog/2009/05/concepts-v1。10。pdf。[在线，1月 3, 2023]。[85] Yuan Cao 和 Lin Yang。2010 年。《身份管理技术综述》。载于*2010* 年 *IEEE* 信息理论与信息安全国际会议。287 293 . 10.1109 .2010.5689468 –。https://doi org/ /ICITIS[86] Thomas Zefferer、Dominik Ziegler 和 Andreas Reiter。2017 年。《兼得两全：安全云联合体与 eIDAS》。载于*2017* 年第 *12* 届互联网技术与安全交易国际会议（*ICITST*）。396–401。https://doi . 10.23919 .2017.8356430 org/ /ICITST Zhi-Kai[87] Zhang、Michael Cheng Yi Cho、Zong-Yu Wu 和 Shiuhpyng Winston Shieh。2015 年。《在自然环境中识别和验证物联网对象》。*Computer* 48, 8 2015 81 83 . 10.1109 .2015.213 (8月)，–。[88] 2016 https://doi org/ /MC Jaweher Zouari 和 Mohamed Hamdi。《AIDF：云的身份即服务框架》。载于*2016* 年网络、计算机与通信国际研讨会（*ISNCC*）。1–5。https://doi。org/10。1109/ISNCC。2016。7746120