身份管理立方体：身份管理方法分类

Daniela P¨ohn[1] and Wolfgang Hommel[1]

德国慕尼黑联邦国防军大学、CODE研究所，慕尼黑，德国{
daniela.poehn,wolfgang.hommel}@unibw.de

摘要。 本文全面介绍了身份管理方法的分类。该分类采用三个维度：拓扑、用户类型和环境类型。利用由此构建的身份管理立方体（IMC）分析现有方法，揭示了用户控制与对属性的信任之间的权衡。通过比较IMC与既有模型，本文找出了这些方法之间的缺失关联。本文进一步扩展IMC，提出身份管理形态学，用以描述协作特征。随后，进一步将这种形态学映射到用户和身份管理的生命周期。本文还结合当前方法，阐明了这些分类的实际意义。两种方法结合起来，能够全面刻画身份管理方法，并有助于选择合适的方法和实施所需工具。

关键词： 安全 · 身份管理 · 模型 · 分类法

arXiv:2301.00444v1 [cs.CR] 1 Jan 2023

1 引言

世界各地成千上万的 Web 应用程序通过互联网提供不同的服务。用户需要出示身份以进行身份验证，否则便无法访问这些服务。二十多年前，人们引入了身份管理（IdM）这一范式，用于管理具有不同身份的用户。它侧重于管理用户名（作为分配给用户的标识符）、某种凭证（通常是密码），以及电子邮件地址和邮政地址等其他信息，这些信息称为用户属性。

不同且不断演变的需求催生了身份管理系统（IdMS）的不同模型和协议。独立组织运行集中式身份与访问管理（I&AM）系统，而许多开展协作的组织，尤其是学术界的组织，则引入了联邦身份管理（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机构相同的身份识别数据。通过 FIM，用户可以在称为联合体的组织信任边界内，访问合作伙伴（称为服务提供商（SP））所提供的服务。常用的安全断言标记语言（SAML） [11]相当静态，而 OAuth 和 OpenID Connect（OIDC） [14] 则提供了一种动态方法，例如 Google 就采用了这种方法。FIM 的限制催生了不同的解决方案，

例如联合会间合作（如 eduGAIN [5]）、利用域名系统（DNS）进行发现和信任（如 LIGHTest [13], ），以及不同的保证框架和组件。与此同时，也开发了以用户为中心的解决方案。用户管理访问（UMA） [8], 是一种基于 OAuth 的标准，使用户能够控制数据共享及其他受保护资源的授权。自主主权身份（SSIs）的用户是该身份的最终所有者。SSIs 通常通过去中心化网络来实现，例如分布式账本技术（DLTs） [2]。去中心化标识符（DIDs） [12] 通常会使用 DLTs。

身份管理是安全框架的一项关键支柱。目前已有多种不同的模型和方法正在开发和运行。并非所有方法都能归入同一个模型，因此难以进行分类。本文作出以下改进：所开发的身份管理立方体（IMC）对不同的身份管理方法进行分类。该立方体通过一种形态学加以扩展，用以描述生命周期内协作的各个方面。我们将这两种分类方法应用于不同的协议和应用程序。这有助于识别合适的方法以及互操作性所缺少的工具，也为利益相关者梳理了生命周期中的重要方面。

本文结构如下：第 2 节讨论相关工作。第 3 节介绍一种新的身份管理分类方法，并简要归类当前的方法。此外，第 4 节提出一种形态学，并将其映射到身份和身份管理的生命周期。第 5 节将新开发的身份管理立方体和形态学应用于当前方法，并对此进行讨论。第 6 节总结迄今取得的成果，并展望正在进行的工作，以此作为全文结论。

2 相关工作

Yuan Cao 和 Lin Yang [16] 指出了身份管理的三个核心组成部分：用户、服务提供商（SP）和身份提供商（IdP）。作者进一步介绍了孤立式、集中式和联合式三种模型。据他们所述，身份管理范式可分为以网络为中心的范式、以服务为中心的范式和以用户为中心的范式。Sovrin [15] 认为，自我主权身份（SSI）是继孤立式、集中式、联合式和以用户为中心的身份管理模型之后的下一步。其他论文则采用孤立式、集中式、联合式和以用户为中心的模型，或集中式、联合式和去中心化模型。

Boujezza 等人 [1] 通过调整范式和需求，描述了一种物联网（IoT）分类法。作者将身份管理模型分为用户模型、服务提供商模型，以及结合用户和服务提供商的混合模型，并进一步划分出子模型。相比之下，Pal 等人 [10] 将物联网身份与以物为中心的身份联系起来。Gao 等人 [3]描述了一种面向大数据的身份管理模型，该模型基于授权、身份验证、身份识别和审计模块。Habiba 等人 [7] 使用身份管理需求分类法对云身份管理系统进行分类。此后还出现了其他方法，发展方向各异；我们将这些方法整合到自己的模型中。

3 身份管理模型

身份管理的主要功能是身份识别、身份验证和授权。在大多数情况下，身份验证需要提供密码，且密码需达到规定的复杂度或熵值。也可以采用第二因素、多因素验证和匿名方式。授权基于策略，这些策略用于说明用户是否有权访问特定功能或数据。在协作场景中，用户信息存储在身份提供商处。用户希望访问实体服务提供商提供的服务。次要实体包括可信第三方（TTP）、持有用户其他信息的属性权威机构（AA），以及在身份提供商和服务提供商形成信任边界时的联合运营方。随着新需求不断涌现，身份管理领域已经发展出不同的方法，未来也将继续出现新的方法。现有的身份管理模型无法适用于若干用例。因此，以下将开发并应用新的模型。

3.1 身份管理模型分析

为区分不同的身份管理方法，人们建立了相应的模型。这些模型后来针对以用户为中心的模型进行了更新，部分也针对自我主权身份进行了更新。如第 2 节所述，以下身份管理模型最为常用。

孤立式： 每项服务分别进行身份与访问管理。**集中式：** 以网络为中心。每个实体分别进行身份与访问管理，例如通过单点登录（SSO）。**联合式：** 以应用为中心。每个联合分别进行身份与访问管理，联合由一组身份提供商和服务提供商构成。可用协议包括 OIDC 和 SAML。**去中心化：** 以用户为中心。用户掌控身份与访问管理。在许多情况下用于联邦身份管理。可采用 UMA 和自我主权身份等方法。去中心化有时会进一步分为以用户为中心和自我主权身份两类。

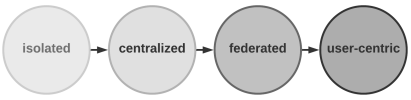
这些模型被视为几乎互不重叠的演进阶段，如图 1a 所示。模型描述了拓扑和真实数据源，即用户或其他实体。某些方法可以同时符合两种模型，见图 1b。例如，身份管理以用户为中心，但服务提供商组成一个联合。在这种情况下，自我主权身份和 UMA 分别属于两种模型。

3.2 身份管理立方体（身份管理立方体）

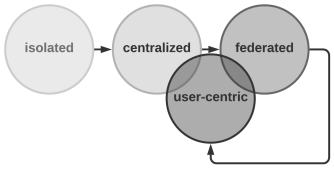
为了区分这些方法，我们使用以下维度。

拓扑： 身份管理方法的拓扑。**用户类型：** 采用该方法的用户类型。**服务类型：** 该方法所体现的服务类型。

这种拓扑 与以用户为中心的方式正交，因此可以作为一个类别。根据现有方法，拓扑可描述如下。由于管理开销，孤立式已不再采用，因此不纳入该类别。



（a）身份管理的演变模型



（b）身份管理-模型的正交性

图 1：身份管理模型

集中式： 每个实体对应一套身份与访问管理。

有 TTP： 涉及多个实体的身份与访问管理，其中至少有一个 TTP 参与其中。这适用于许多联邦身份管理的情况，因此与联合式类似。**无 TTP：** 涉及多个实体的身份与访问管理，其中不涉及任何 TTP。由于它描述的是一种分布式、完全去中心化的结构，因此涵盖了不同的方法。自我主权身份的大多数情况都属于此类别。

以用户为中心描述了两件事：作为真实数据源的人类用户，以及用户本身。其他用户类型包括计算机（如服务器）和物联网设备。因此，第二个类别是用户类型。人类用户又分为以用户为中心和以提供方为中心，描述的是属性处理方式。

用户： 分为以用户为中心和以提供方为中心。此类别包括 UMA、自我主权身份，也包括 SAML 和 OIDC。**计算机：** 例如机器对机器（M2M）通信。**物联网设备：** 物联网设备的计算能力通常较弱，因此会限制其执行计算密集型密码运算的能力。

尽管越来越多的网络服务（如 Office 365）得到使用，但仍有一些服务并非基于网络。为了区分服务类型，我们设定了以下特征。

非网络服务： 机器对机器通信，以及本地服务。**后台网络服务：** 交互式网络服务所需的服务，例如定位用户所属的组织。**交互式网络服务：** 终端用户使用的服务。

因此，新模型由三个类别构成，并以维度的形式呈现：拓扑、用户类型和服务类型。参照生命周期、方面、层（LAL）砖块 [4], ，这些类别构成一个立方体。图 2 展示了构建的身份管理立方体，其中标注了不同的维度。为清晰起见，图中省略了以用户为中心和以提供方为中心这两项。

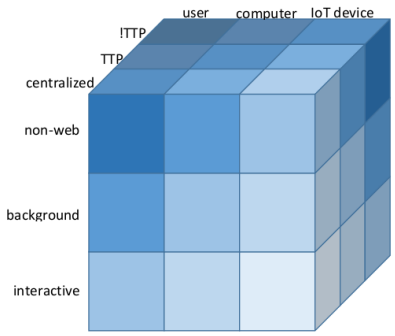


图 2：身份管理立方体

3.3 身份管理立方体应用于当前方法

为了展示身份管理立方体，我们按照上述类别对不同的身份管理方法进行分类。作为示例，我们选择了研究与教育（R&E）领域采用 SAML 联合会的集中式身份管理、Web 中的 OIDC、面向私人用户的 UMA，以及作为一种新方法的自我主权身份。此外，还介绍了面向服务器、物联网以及采用 Active Directory（AD）的身份管理。

SAML 用于研究与教育领域，使用户能够访问研究合作伙伴提供的网络服务。它基于轻型目录访问协议 (LDAP)、数据库，甚至是附加了联合功能的活动目录。各实体组成一个联合体，该联合体依赖于与联合体运营方签订的合同。因此，它具有以下特征，如图 3a 所示。

拓扑： 使用联合工具作为可信第三方。**用户类型：** 用户是人类，但此处的类型以提供方为中心。**服务类型：** 面向最终用户的交互式网络服务。

OIDC 也用于网络，但它是一种更动态的协议，不涉及可信第三方，并基于 OAuth。UMA 同样基于 OAuth 开发，但更以用户为中心。这一点可以从图 3b 所示的特征中看出。

拓扑： 使用 WebFinger 技术时不涉及可信第三方，但在某些用例中可以集中化。**用户类型：** 大多数情况下是人类最终用户，可以是以提供方为中心（OIDC），也可以是以用户为中心（UMA）。**服务类型：** 通常是面向最终用户的交互式网络服务，但也可能是其他类型。

自我主权身份 被视为身份管理演进的新阶段，因为用户可以掌控一切。这一概念不依赖可信第三方，但出于可扩展性和性能方面的考虑，正逐渐演变为带有可信第三方的拓扑。大多数方案专注于交互式网络服务，不过这一概念也可应用于其他服务。因此，自我主权身份具有图 3c 所示的以下特征。

拓扑： 最初，自我主权身份不依赖可信第三方，但正逐渐演变为集中式服务。

用户类型： 自我主权身份以用户为中心，因此属于以用户为中心的模式。**服务类型：** 面向最终用户的交互式网络服务。

除了网络应用程序外，后端还运行着服务器，通常通过密钥访问。公钥存储在服务器上，而管理员持有私钥。因此，该服务不是基于网络的，通常采用集中式架构或由可信第三方提供。由此，服务器的身份管理可描述如下，如图 3d 所示。

拓扑： 采用集中式架构，由集中式身份管理或可信第三方提供。**用户类型：** 既可以是机器对机器中的计算机，也可以是人类用户。**服务类型：** 这些服务通常不是基于网络的。

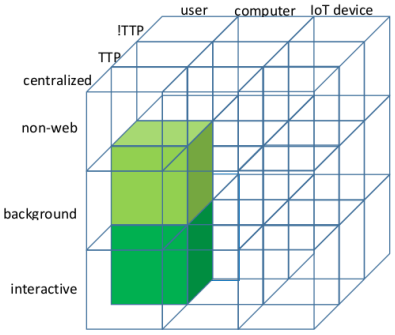
基于活动目录的集中式身份管理 用于公司，使员工能够登录自己的计算机、配置文件夹和共享资源，还能通过单点登录 (SSO) 访问网络服务。它具有以下特征，如图 3e 所示。

拓扑： 活动目录本身是集中式的。
用户类型： 重点关注人类用户，但身份管理以提供方为中心。此外，Windows 计算机也可以是用户。
服务类型： 由于依赖 Windows，因此可以支持所有类型的服务。

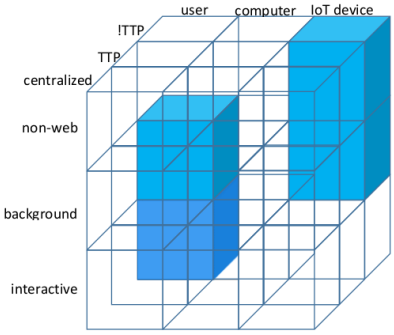
物联网设备 通常使用受限应用协议（CoAP）而非超文本传输协议（HTTP）进行通信。缺少浏览器来执行基于用户代理的授权，或输入能力受限的设备无法使用 OAuth 或 SAML 等典型网络协议。一种选择是使用共享密钥，另一种选择是使用 ACE-OAuth。ACE-OAuth 将 OAuth 方法映射到受限环境的认证与授权（ACE）。其特征如图 3f 所示。

拓扑： 物联网网络通常采用集中式管理，可以有可信第三方，也可以没有。**用户类型：** 用户类型为物联网设备。**服务类型：** 物联网设备主要提供后台服务。

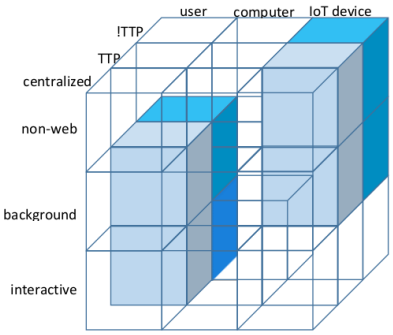
所选方法可以合并到一个身份管理立方体中。颜色沿用上图中的设定：活动目录为深绿色，SAML 为黄色，OIDC 为深蓝色，SSI 为浅蓝色，服务器为橙色，物联网为浅绿色。该立方体表明，许多方法用于交互式网络和人类用户，而这些协议本身也可用于其他用例。该图还展示了这些方法之间的差异。活动目录侧重于集中式拓扑，SAML 通常使用可信第三方，而 OIDC、UMA 和 SSI 往往无需可信第三方。图 4a 展示了最常见的服务类型，图 4b 则还加入了特殊用例。两幅图都表明，所选方法未涵盖身份管理立方体的所有方面。若 SSI 采用集中式参与方，则可在一定程度上满足 SAML 的应用场景，因为它会像后图所示那样，通过可信第三方实现双重功能。



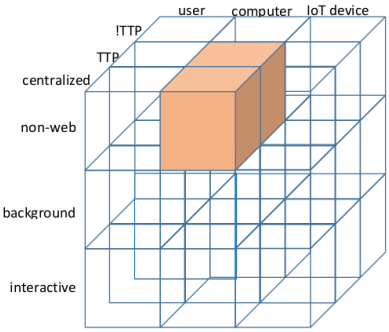
(a) 用于 SAML 的身份管理立方体



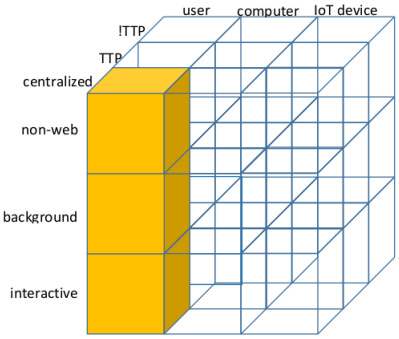
(b) 用于 OIDC 的身份管理立方体



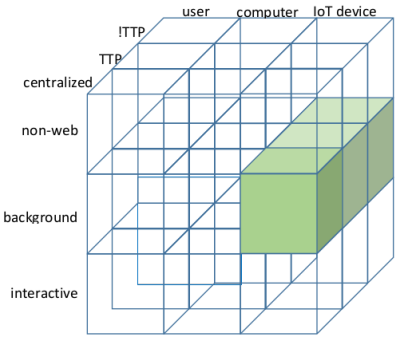
(c) 用于自我主权身份的身份管理立方体



(d) 用于服务器的身份管理立方体



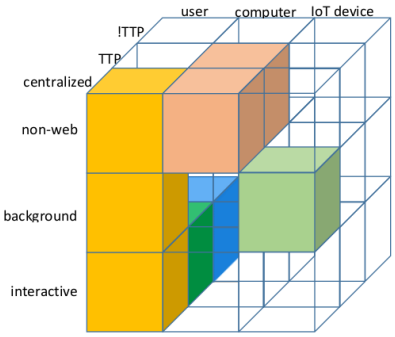
(e) 用于活动目录的身份管理立方体



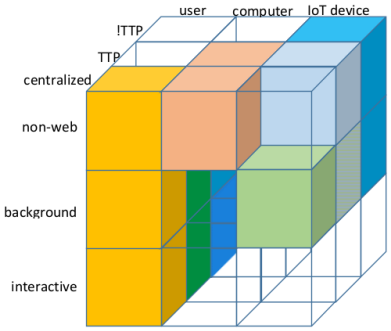
(f) 用于物联网的身份管理立方体

图 3：应用于不同用例的身份管理立方体

尤其是这些共享单一立方体表明，不同方法之间应能轻松实现互操作性；而将不同方法组合到不同立方体中，可能需要投入更多精力并使用更多工具。此外，可以采用以用户为中心或以服务为中心的方式。由于缺乏对属性的信任，大多数方法无法兼顾两者。



（a）合并的身份管理立方体



（b）包含特殊用例的合并身份管理立方体用例

图 4：合并的身份管理立方体

4 身份管理的形态学

为了确定满足程度，需要采用统一的格式，对这些方法进行更详细的描述。因此，我们建立了一种类似形态学的特征体系。形态学侧重于组织方面，而身份管理立方体则对技术进行分类。 [6] 的作者根据形态学描述了 Inter-FIM 的特征。由于这些特征需要涵盖所有身份管理方法，因此也与身份管理立方体相关；为此，我们针对通用身份管理的需求扩展了形态学。接下来，我们将形态学映射到生命周期，以明确在何时作出何种决策。最后，我们通过形态学对各种方法进行表征。

4.1 形态学的设计

形态学描述了合作的特征。 [6] 采用合作结构、成员、群体结构、联合维度、组织维度、持续时间、协作类型、协调、建立、信任圈、承诺程度和信任关系。由于这种方法聚焦于 Inter-FIM，以下特征可以省略或需要调整。

合作结构：该结构描述了联合体的拓扑和定制化合作。拓扑由立方体描述，而合作的不同方面则属于形态学的一部分。**合作：**不再使用联邦身份管理、项目和社区，而是通过“加入原因”和“秩序”来描述这一特征。**形式化** 区分“有限合同”和“合作协议”，以描述合同之间的差异。**加入动态：**范围更广，涵盖“稳定”和“不稳定”。

为描述不同的组织方面，还需添加其他特征。若干特征与身份管理架构相关。

加入原因： 为区分私人用途与商业原因，纳入了这一特征。**连接性：** 描述相关方之间的互动，这可能会对架构产生影响。**合作方向：** 扩展了考察范围。**管理：**自动化程度，与架构相关。**合作结构：** 分为 “ 层级式 ” 或 “ 异层级式 ”。**信任级别：** 相关方之间的信任。**身份：** 由于其会对架构产生影响，因此将其纳入。

4.2 身份管理形态学

由此形成了一种形态学，其中包含更多且范围更广的特征。如表1所示，该形态学包含以下类别。

发起： 合作的发起。**合作：** 合作的设置。**协调：** 协调的设置。**信任：** 参与实体之间的信任。**身份：** 身份的设置。

发起 包括加入原因和加入动态。原因可以是“个人”“社会”（如社交媒体中的情形）、“法律规定”或“经济”。经济原因还可进一步细分为“时间”“风险”“收益”“能力”“成本”“压力”和“保护”。另一种区分方式是“计划性的”（如有必要）和“自发事件驱动”。动态 分为“稳定”或“不稳定”，也就是说，它是可预测的，或不可预测的。

合作本身由整合程度、连接性、专业限制、事实限制、合作方向、秩序、地方性、组织性和形式化来描述。整合程度和合作伙伴之间的连接性都属于合作伙伴之间的网络化。整合程度可以是“自主”“协调”或“集成”。这意味着合作伙伴可以自主工作，也可以协调一致地朝着某个目标努力。集成则可能意味着组织的合并。连接性分为两个等级：“低”和“高”。它在一定程度上与整合有关。接下来的类别是两种限制，

表1：身份管理的详细形态学发起

加入原因	个人	社会	经济	law
加入动态	稳定		不稳定	
合作				
整合程度	自主	协调	集成	
tion				
连接性	low		high	
专业限制 用户		R&D	部门	价值链
事实限制	短期	中期	long	永久
合作方向	垂直	水平	对角	
合作方向				
秩序	战略	项目	R&E	区域
地方性	本地	区域	国家级	国际
组织	微观	meso	宏观	
形式化	安排	有限 con-	合作	资本 跨
		论述	协议	交织
协调				
管理	手动	辅助	自动化	
参与者数量	双边	简单	复杂	
裤子				
群体结构	open	with 限	封闭	
		制		
合作结构	层级式		异层级式	
ture				
Sort 协调的	隐式		显式	
tion				
信任				
直接性	直接		传递	
信任圈	静态	动态	虚拟	
信任级别	zero	low	中期	high
身份				
透明度	low	中期	high	
可控性	low	中期	high	
身份识别	内部	外部	组合	
身份验证	匿名	简单	2FA	MFA
方法				
身份验证组	内部	外部	组合	
织				
授权	内部	外部	组合	

专业性和事实性。专业限制 描述参与合作的组织部分。它可以是“研究”、“部门”、完整的“价值链”，或仅仅是一个或多个“用户”。事实限制 分为“永久”或“受限”。受限还可进一步分为“短期”、“中期”和“长期”。合作方向 描述两个经济层级之间的关联紧密程度。“横向合作”是指同一行业或价值链同一层级的公司的合作；而“纵向合作”是指不同经济层级的组织之间的合作，例如零售公司与生产公司之间的合作。如果参与的公司既不处于同一经济层级，也不属于同一行业，则这种合作属于“对角合作”，例如旅行公司与食品公司之间的合作。秩序 描述合作的缘由，可以是“战略”、“项目”、“研究与教育”，或基于“区域”。地方性和组织性都是合作的维度。合作的地方性可以是“本地”、“区域”、“国家级”或“国际”。国家级联合会包括研究与教育联合会，例如瑞士的 SWITCHaai。eduGAIN 是国家级对应组织的国际伞状联合会。

组织 维度描述了合作的观察层面。这里使用了经济学术语。“微观”层面由单个实体构成，而“中观”层面则包含多个组织，例如联合中的组织。“宏观”层面展示了合作中的合作，例如联合会间合作。形式化 对实体间的正式程度进行分类。“安排”可以是口头的，也可以以某种方式书面记录；而“合同”则分为有限期限的合同和合作合同。最后一步是相关实体之间的“资本”交织。面向最终用户使用社交媒体就是安排的一个例子，而合同通常用于项目。形式化还描述了约束强度，即相关实体放弃自主权的程度。

这种协调说明了合作的管理方式，包括管理、参与者数量、群体结构、秩序和协调类型。参与者数量与群体结构相关。开放式合作没有固定的参与者数量。封闭式合作允许采用简单结构，也允许采用双边结构。协调还与信任有关。管理可以是“手动”“辅助”或“自动化”。参与者数量与合作密切相关。参与的实体之间可以达成“双边”协议，合作可以采用“简单”结构，也可以是“复杂”结构。双边合作仍可使用重复的用户库，但涉及更多实体时则无法如此。简单网络可以通过安全断言标记语言（SAML）联合体实现，而复杂结构在技术实现上也更加复杂。OpenID Connect（OIDC）可用于实现此类结构。群体结构可以是“开放”“有限制”或“封闭”。OIDC通常是开放的，而SAML联合体在研究与教育领域存在限制，或在行业中是封闭的。合作结构可以是“层级式”，也可以是“异层级式”，后者表示所有合作伙伴的层级大致相同。协调类型有两个可能的值：“隐式”或“显式”。

采用显式协调时，可以辅助整合一个机构协调实例。隐式协调则需要本地协调。

信任实体之间的信任源于多种不同因素，例如推荐或过往经验。在形态学中，仅描述合作的基本要素，包括直接性、动态性和平均信任级别。信任圈（CoT）与合作类型有关。如果群体结构有限，则信任圈可以是静态的。如果参与者数量复杂，那么信任圈就是虚拟的，因为不可能完全了解所有参与者的全部信息。直接信任意味着静态或动态信任圈。直接性描述两个实体之间的信任是如何产生的。信任可以是“直接的”，也可以通过另一个实体成为“传递／间接的”。动态性描述信任随时间的变化，其类型可以是“静态”或“动态”。最后，信任级别可以是“零”“低”“中期”或“高”。

作为最后一个类别，对身份进行分类。身份尤其描述信任因素以及以用户为中心的特征。这包括透明度、可控性、身份识别、身份验证（由身份验证方法和组织因素构成），以及授权。透明度可以是“低”“中期”或“高”。同样的特征也适用于可控性。身份识别、身份验证和授权可以由不同实体“内部”或“外部”执行，也可以通过不同实体的“组合”执行。身份验证方法描述所使用的凭据类型，可以是“匿名”、“简单”（例如密码）、“双因素身份验证（2FA）”或“多因素身份验证（MFA）”。为了降低形态学的复杂度，可以省略适用的特征。下一步可以添加用例的特殊特征，例如联合拓扑。这取决于具体的用例。

4.3 映射到生命周期的形态学

形态学可以映射到身份管理的生命周期，帮助开始合作的各方确定其框架。生命周期与戴明循环 [9],类似，包含计划、执行、检查、处理几个阶段。戴明循环是一种迭代式的四步管理方法，用于商业领域，旨在控制流程和产品的改进。它可应用于服务管理、安全管理以及许多其他领域，例如身份管理。身份管理的生命周期包含发起、协议、合作、重新评估和改进，以及终止几个阶段。重新评估可能促成改进，也可能导致终止。身份管理生命周期的各个阶段具有以下特征。

发起：某个目的促成合作的发起。
协议：经过讨论后，双方签署协议，说明合作框架。身份管理应当成为协议的一部分。否则，各方需要在协议之外就信息技术方面达成一致。

合作： 合作开始了。在许多情况下，合作开始得很慢，需要逐步将一切安排妥当。随后会出现合作热潮，一切都在运转，最初的目的也有望实现。在信息技术领域，开始阶段需要投入工作，建立基础设施。

重新评估： 这描述了合作是否继续进行，以及是否需要做出更改。身份管理也是如此。**改进：** 这些更改带来了改进，并得以实施。**终止：** 如果目的已经实现，或由于其他原因导致合作结束，该项目的身份管理也会终止。

上一节所述的形态学可以映射到生命周期。这有助于更全面地了解所需作出的决策，如图 5a 所示。发起 阶段包含发起形态学的两项特征，即“加入原因”和“加入动态”。合作 和协调具有“协议”和“合作”方面的特征。这是因为，有些特征是在达成协议时确定的，而另一些则对合作产生更大影响。因此，协议的特征包括：“形式化”、“限制”、“合作方向”、“合作结构”、“维度”、“参与者数量”和“群体结构”。合作则包括“信任”、“身份”、“整合程度”、“连接性”、“管理”和“合作类型”。在重新评估 期间，每个方面都会重新评估。改进过程中，某些方面会得到增强。如果合作结束，生命周期也随之终止。

身份管理生命周期包括用户生命周期，因为用户会在项目或生命周期中不断变化。在项目期间，一些用户会离开，另一些用户则会加入。组织中的身份管理也是如此。最终，每个用户账户都需要关闭。用户的生命周期包括以下阶段。

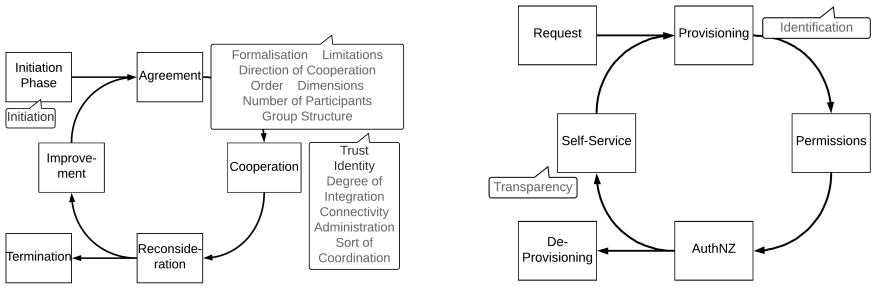
请求： 用户在身份管理系统中请求一个账户。**配置：** 系统为账户配置属性、角色和权限。**身份识别：** 用户进行身份识别。**身份验证和授权：** 先进行身份验证，然后进行授权。**自助服务：** 用户可以访问自助服务。**取消配置：** 最终，用户账户被取消配置。

用户生命周期与形态学的交互很少：在请求阶段信任服务提供商，随后进行身份识别、身份验证和授权，并在自助服务阶段体现透明度。这也在图 5b 中进行了可视化。

因此，身份管理模型总体上描述各种方法，而形态学则详细说明合作的各个方面。形态学与生命周期的映射解释了需要采取的行动顺序。这可以为项目和组织提供身份管理流程方面的指导。然而，尽管立方体提供了初步提示，但目前仍缺少用于选择最合适方法的决策矩阵。此外，还需要与已经建立的流程（例如服务管理和安全管理）之间的接口。

4.4 形态学在当前方法中的应用

接下来，将该形态学应用于基于 AD 的集中式身份管理，并介绍其与 SAML、OIDC、自我主权身份、服务器和物联网设备的差异。集中式



(a) 形态学 映射至身份管理系统生命周期 (b) 映射至用户生命周期的形态学-cle

图 5：映射至生命周期的形态学

基于 *AD* 的身份管理 通常用于公司。根据公司是否存在合作、是否设有多个分支机构，其复杂度会有所不同。此外，根据观察角度的不同，例如用户或公司的视角，可以用不同颜色标示不同属性。假设本例中的公司仅使用 AD 管理其用户，而通过其他方式开展合作。因此，可以构建如下形态，见表2。加入原因是经济因素，而动态性稳定。AD 是在某个时间点引入的。考察合作时，考虑的是公司内部的合作。因此，集成程度为集成。由于所有参与者共同工作，连接性为高。AD 是为公司的整个价值链引入的。这应当是一种永久性解决方案，尽管技术和决策会发生变化。合作方向无法通过该分类来描述。秩序基于一项战略，而该公司是本地的。组织因素属于微观层面。公司内部的合作取决于与员工签订的合同。管理工作有望得到辅助，而参与者数量可描述为双边。群体结构至少目前是封闭的，协调方式则是层级式且显式的。信任是直接的，且较为静态，信任程度为中期，因为所有员工都需要提交文件。身份由公司内部管理，并采用简单因素和第二因素。

研究与教育领域的*SAML* 实体组成联合体，这些联合体分布于各个地区、国家乃至全球。实体与联合体运营方签订合同，而联合体运营方则与联合体间运营方签订合同。实体之间的协调程度相当低。由于身份由所属机构管理，信任程度较低。因此，可以看到以下形态学。

发起： 个人因研究与教育而加入，而公司则出于经济原因加入。这种动态相当稳定，因为实体必须签署合同。
合作： 这种合作是自主的，仅由联合体及联合体间运营方进行少量协调。实体之间的连接性较低，因为联合体内有许多不同的服务，而且只有

表2：基于活动目录的集中式身份管理形态学发起

加入原因 个人	社会		经济	law
加入动态	稳定		不稳定	
合作				
集成程度	自主	协调	集成	
tion				
连接性		low	high	
专业限制 用户		R&D	部门	价值链
事实限制	短期	中期	long	永久
合作方向	垂直	水平	对角	
关系				
秩序	战略	项目	R&E	区域
地方性	本地	区域	国家级	国际
组织	微观	meso	宏观	
形式化	安排	有限 con-	合作	资本 交互-
		地带	协议	编织
协调				
管理	手动	辅助	自动化	
参与者人数	双边	简单	复杂	
参与者				
群体结构	open	with 局限-	封闭	
		性		
合作结构-	层级式		异层级式	
ture				
Sort 协调-	隐式		显式	
tion				
信任				
直接性	直接		传递	
信任圈	静态	动态	虚拟	
信任级别	zero	low	中期	high
身份				
透明度	low	中期	high	
可控性	low	中期	high	
身份识别	内部	外部	组合	
身份验证	匿名	简单	2FA	MFA
方法				
身份验证或-	内部	外部	组合	
组织				
授权	内部	外部	组合	

一小部分用户会使用某个服务提供商提供的特定服务。实体通常会与联合体运营方联系。合作仅限于研究，而所需时间取决于多种因素。合作可以是垂直的，也可以是水平的。多数情况下，地方性范围为国家级或国际级。此外，还建立了区域联合体。组织形式可以是中观或宏观，具体取决于联合

。联合体通过与联合体运营方签订的合同予以正式确立，实体之间也会通过部分安排进行协调。

协调： 管理需要通过手动步骤提供辅助。由于需要签订合同，参与者数量较少，群体结构也存在限制。秩序更偏向异层级式而非层级式，协调也更偏向隐式而非显式。

信任： 信任通过联合体运营方或联合体间运营方传递。参与者数量固定，信任圈也相应保持静态，动态性较低。信任级别较低或中等，具体取决于是否采用单独的手段。**身份：** 由于形成了包含额外属性权威机构的社区，并且使用了其他身份识别手段，因此授权和身份识别可以是内部的，也可以是组合式的；身份验证则是内部的。由此产生的结构使透明度和可控性都比较低。

采用 *OIDC* 的身份管理与 SAML 的区别在于，其协议是动态的，且广为人知的用例是网络身份验证。对于 OIDC，发起可能有多种原因，因此其动态性不稳定。合作较为松散，协调也是如此。信任级别较低，但可以通过第二因素提高。不同的组合也会影响身份。自我主权身份 则有所不同：用户可以控制属性，进而影响信任和身份。如果公司在内部托管其服务器，那么合作就在公司内部进行，也可能涉及其他办公室。物联网设备既可用于家庭，也可用于组织。人们通常对这些设备的信任度较低，因为他人可能在不被察觉的情况下篡改设备。

5 讨论

我们从两个方面对身份管理方法进行了描述：身份管理立方体（IMC）阐明技术方面，形态学则用于描述组织方面。为了汇总身份管理方法，我们注意到现有身份管理模型之间存在交集。这些交集帮助我们确定了区分身份管理方法所需的类别。拓扑、用户类型和服务类型这三个类别被排列在一个立方体中，即身份管理立方体。身份管理立方体明确了用户类型和拓扑这两个特征，同时也明确了视角，即以用户为中心还是以提供方为中心。某种方法或许可以归入此前使用的两个模型，但身份管理立方体能够对其进行明确分类。考虑到这三个类别具有灵活性，未来的方法也应能够据此进行描述。接下来，我们将不同的身份管理方法应用到立方体中。这些方法既包括面向最终用户的典型网络服务，也包括服务器和物联网相关方法，由此构成了一个丰富多彩的身份管理立方体。有些用例比其他用例更为典型。除此之外，应用过程简单直接，并展现了各种方法之间的相似之处和差异。这些发现或许表明，不同方法可以进行组合。值得注意的是，所展示的示例中，信任与以用户为中心的特征并未同时出现。因此，身份管理立方体有助于组合不同的身份管理方法，并探索尚缺少哪些工具。

接下来，我们开发了身份管理形态学。形态学描述了合作的不同方面。在本例中，需要考虑发起、合作、协调、信任和身份这些类别及其分类。随后，我们展示了形态学与不同生命周期之间的关系。作为指导，形态学可用于加快后续阶段的实施和评估。之后，我们将形态学映射到不同的方法上。结果呈现出一定的差异，这取决于实际实施情况。尽管如此，组织环境得以明确。这并未涵盖内部流程，相关内容将在未来的工作中探讨。

身份管理立方体和形态学都无法从所有方面描述身份管理，但有助于对不同方法、用例及其实施进行分类。这种分类有助于在身份管理生命周期中组合不同方法、发现缺失的工具，并考量所有相关方面。

6 结论与未来工作

如今，身份无处不在。随着互联网用户和账户数量不断增长，使用的服务器也越来越多。新的机遇也带来了新的用例。身份管理模型是在区块链热潮兴起之前开发的。此后，新的方法应运而生。

本文介绍了一种广泛的身份管理分类方法。我们将现有的身份管理模式扩展为包含三个维度的身份管理立方体。拓扑、用户类型和环境类型能够更详细地描述身份管理方法，但对于实际协议仍未作出明确说明。我们将身份管理立方体应用于不同方法，展示了信息孤岛，以及一些借助额外工具便较易实现互操作的方法。这表明，许多方面取决于组织内部的实际实施。此外，它还揭示了用户控制与对属性的信任之间存在权衡。我们进一步将身份管理立方体扩展为身份管理形态学，用以描述合作的特征。随后，我们将这种形态学映射到用户和身份管理的生命周期中。映射结果有助于在合作过程中辨别相关问题。身份管理立方体与身份管理形态学这两种方法相结合，能够全面刻画身份管理方法。这有助于为组织或合作选择合适的方法。此外，还可以探索实现互操作性所需的工具。将其整合进流程并制定指南以选择最合适的身份管理方法，本文未作探讨，将留待后续工作。这些方法也表明，整体身份管理所需的一些有趣特性尚未设计出来。

为了构建一个整合不同身份管理方法的整体身份管理框架，现正开发一种架构。该架构通过服务模型加以扩展，以可视化所需流程。下一步，将研究与现有管理流程交互的流程。为确定最合适的身份管理方法，我们创建了一个决策矩阵；这一切都有助于简化身份管理的使用并提升其质量。

参考文献

1. Boujezza, H., AL-Mufti, M., Ayed, H.K.B., Saidane, L.: 《物联网身份管理系统分类法》。载于：2015年IEEE/ACS第12届计算机系统与应用国际会议（AICCSA），第1–8页（2015年11月）。https://doi.org/10 7507266 2 1109 2015 . /AICCSA. . . Ferdous, M.S., Chowdhury, F., Alassafi, M.O.: 《利用区块链技术探索自我主权身份》。IEEE Access **7**，103059–103079（2019）。https://doi.org/10 2931173 3 1109 2019 . / ACCESS. . . Gao, F., Zhang, F., Xia, J., Ma, Z.: 《面向大数据分析的通用身份管理模型》。载于：2016年第18届国际先进通信技术会议（ICACT），第1–1页（2016年1月）。https://doi.org/10 7423325 4 1109 2016 . /ICACT. . . Garschhammer, M., Roelle, H.: 《服务导向对质量规范的要求》。载于：Sahai, A., Wu, F.（编），《效用计算》，第1–14页。Springer Berlin Heidelberg，柏林、海德堡（2004） 5. G´EANT：eduGAIN技术网站。https://technical.edugain.org/status.php (2020 [4, 2023])，在线，1月。Grabatin, M., Hommel, W., 6 Metzger, S., P¨ohn, D.: 《DAME：按需互联网规模的SAML元数据交换》。《系统与测量进展国际期刊》**8**，156–167（2015） 7. Habiba, U., Masood, R., Shibli, M.A., Niazi, M.A.: 《云身份管理的安全问题与解决方案：分类法》。《复杂自适应系统建模》**29** 8 1 2194 3206 2014 10 1186 40294 014 0005 ( )，–（11月）。https://doi.org/ . /s - - - . Kantara Initiative：主页 – 工作组 – 用户管理访问。https:// kantarainitiative.org/confluence/display/uma/Home (2020)， [在线，1月 4, 2023] 9 。Milgram, L., Spector, A., Treger, M.：第21章——计划、执行、检查、处理：戴明循环或休哈特循环，第……卷，《智能管理》。Gulf Professional Publishing（1999）10. Pal, S., Hitchens, M., Varadharajan, V.: 《物联网身份建模：综述、分类与趋势》。载于：2018年第12届传感技术国际会议（ICST），第45–51页（2018年12月）。https://doi.org/10 8603595 11 1109 2018 . /ICSensT. . . Ragouzis, N., Hughes, J., Philpott, R., Maler, E.: 《安全断言标记语言（SAML）V2.0技术概述》。技术报告，OASIS（2008）12. Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., Holt, J.: 《去中心化标识符（DID）v1.0——核心架构、数据模型与表示》。技术报告，万维网联盟（2020）13. Roßnagel, H.: 《信任体系成员资格的发现与验证机制：LIGHTest参考架构》。载于：Fritsch, L., Roßnagel, H., H¨uhnlein, D.（编），《开放身份峰会2017》，第81–92页。德国信息学会，波恩（2017）14. Sakimura, N., Bradley, J., Jones, M.B., de Medeiros, B., Mortimore, C.: 《OpenID Connect核心1.0》。技术报告，OpenID基金会（2014）15. Tobin, A., Reed, D.: 《自我主权身份的必然崛起》（2017）， [在线，1月16 4, 2023] 。Yuan Cao, Lin Yang: 《身份管理技术综述》。载于：2010年IEEE信息论与信息安全国际会议，第287–293页（2010年12月）。https://doi.org/10.1109/ICITIS.2010.5689468