CSA GCR cloud security alliance
GREATER CHINA REGION ®

IAM白皮书

（试读本）

致谢

云安全联盟大中华区（简称：CSA GCR）IAM 工作组在 2020 年 5 月成立。由戴立伟担任工作组组长，工作组专家来自微软、华为、中国移动、奇安信、启明星辰、天融信、碧桂园、Okta、龙湖集团、竹云、万物安全、联软科技、易安联、星展银行、oyo 酒店、德勤等二十多个单位。

本白皮书由 CSA 大中华区 IAM 工作组专家撰写，感谢以下专家的贡献：

组长：戴立伟

贡献者名单：于继万，朱璐，江澎，张帆，董明富，于乐 ，谷雨，常官清，张彬，谢琴，李慧，杨清公，赵呈东，程伟强，郭晓锋，Jason Huang，伏明明，郑彬，黄超，徐阳，周潮洋，丁元东，史晓婧，张智，黄恒华，滕伟，孟茹

贡献单位：竹云，华为，中国移动，奇安信，绿盟，天融信，格尔软件，启明星辰，易安联，安讯奔，美云智数

研究助理：朱晓璐

（以上排名不分先后）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research/）上查看。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

序言

IAM（Identity and Access Management，身份与访问管理）致力于确保组织中的人、设备等在日益复杂的技术环境中合理访问资源，是保障信息系统高效连接，人员、设备访问安全，以及实现组织数字化转型目标的核心基础设施，并用于满足日益严苛的合规性要求。对于企业、政府等组织而言，IAM 都是一项非常关键的职能。它与业务紧密保持协同，使能组织在支持新业务计划方面变得更敏捷，因此对 IAM 技术开展研究非常必要。

随着数字化技术的深入应用以及国内外政策法规的不断完善，IAM 技术历经从单一功能模块到全面数字身份治理体系的发展历程，业务场景不断延伸，在智慧城市、数字政府以及各行业数字化转型中均具备丰富的应用场景。

云安全联盟大中华区依据 IAM 技术的发展和应用编制了此白皮书，此白皮书结合各行业与国内外 IAM 发展状况，对 IAM 发展历程、核心能力包含身份管理、访问控制与权限管理、合规审计、风险管控等以及现代增强型 IAM 技术的演进路线进行了详细介绍。同时针对 IAM 在云计算、物联网、零信任等技术领域的落地场景以及 IAM 在相关行业的应用场景和实践案例进行了重点解读和分析。

借此白皮书抛砖引玉，我们与行业专家共同探讨 IAM 的发展趋势，为相关从业者提供指导。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

致谢 **4**

序言 **5**

1 介绍 **8**

1.1 目标读者 8

2 系统概述 **9**

2.1 身份管理和访问控制发展行业背景 9

2.2 什么是 IAM 14

2.3 Identity、Authentication、Authorization、Audit 的定义和关系及与 IAM 的联系 14

2.4 IAM 的核心能力 17

2.5 IAM 发展历程及趋势 19

3 身份管理 **21**

3.2 身份识别服务 25

3.3 用户分类管理 26

3.4 用户全生命周期管理 29

3.5 用户信息存储 32

3.6 用户的同步和回收能力 42

3.7 密码管理 45

3.8 特权账号管理说明 46

3.9 身份管理的其他业务特征 50

4 登录认证 **51**

4.1 身份信任的概念及模型 51

4.2 认证类型及 MFA 53

5 访问控制与权限管理 **94**

5.1 访问控制模型说明 94

5.2 权限管理要素和系统设计 112

5.3 常见云原生权限策略说明 118

5.4 数据权限管理方式（如通过 API 网关完成鉴权） 124

5.5 权限定编定岗 126

5.6 权限合规与互斥.....128
5.7 权限定期审阅.....131
5.8 权限挖掘.....133
6 审计与风控.....134
6.1 常见身份审计项说明.....134
6.2 事后审计方式说明.....135
6.3 风险发现以及可持续检测.....137
6.4 UEBA.....139
7 CIAM 体系说明.....142
7.2 用户隐私许可.....143
7.3 用户授权同意.....145
8 IDaaS 体系说明（Identity As A Service）.....147
8.1 IDaas 的定义.....147
8.2 IDaaS 的技术特征.....148
8.3 IDaaS 的使用场景.....150
9 IoT 身份管理体系说明.....154
9.1 物体身份唯一标识说明.....154
9.2 IoT 身份互联方式（人物互联、物物互联）（说明互联方式即可采用的认证手段）
.....157
9.3 常见 IoT 身份互联场景说明.....162
10 IAM 与零信任的关系.....175
10.1 IAM 在零信任中的作用.....175
10.2 零信任发展对 IAM 带来的挑战.....181
11 IAM 实践案例分享.....185
11.1 IAM 体系案例研究.....185
11.2 中通 IAM 一帐通平台.....189
11.3 碧桂园权限中台实践探索之路.....195
12 总结 （组长）.....206

1 介绍

各领域加速向数字化、移动化、智能化发展，信息化建设与数字化转型的大力投入已成为企业以及政府单位的共识，组织信息环境变得庞大复杂，业务场景发生明显变化，从而给身份管理与信息安全管理带来挑战：

1. 信息化系统数量逐渐增多，部分企业存在成百上千套信息化系统，每套信息化系统的身份管理、认证、权限等部分均各自独立建设，不仅重复建设、成本较高，而且易形成信息孤岛，从而为管理以及运维带来很大难度，影响企业运行效率，存在安全漏洞与隐患。
2. 身份安全问题越来越严重，很多企业与单位内部存在大量孤儿账号、僵尸账号，成为被黑客掌握和攻击的短板；个人信息大规模泄露事件频繁出现；物联网设备存在弱密码和默认密码，进而被攻破与控制等等。尤其是零信任体系的快速发展且得到普遍认可，IAM 作为零信任中的核心组件，成为越来越多单位开展信息化建设的核心基础设施。
3. 随着数字化建设的深入推进，各单位期望将原先多种渠道下的用户做统筹管理，从而形成用户中心、认证中心、权限中心、审计中心等通用共享功能模块，通过敏捷地方式快速响应外部未知业务需求，提升用户体验，促进业务发展。
4. 当前大数据、人工智能、区块链、物联网等技术的快速发展，逐渐与 IAM 体系融合，形成新一代的增强型现代 IAM 体系。现代 IAM 具备了 UEBA 等主动防御的事前检测能力、权限动态管控与事中控制能力、事后全面审计与追溯的能力。
5. 随着网络安全法、欧盟 GDPR 以及中国个人信息保护法等法律法规的逐步出台，个人信息保护、管理合规、隐私控制等成为各国企业与政府单位的强制要求。IAM 是实现其同意权、拒绝权、数据可移植性、范围受限访问等要求的必然基础。
6. 此白皮书结合业内与国内外 IAM 发展状况，对 IAM 发展概述、身份管理、登录认证、访问控制与权限管理、合规审计以及新型 IAM 发展情况进行了详细介绍。由于编写时间仓促，有不足之处，望读者谅解并协助指正。

1.1 目标读者

- IAM 行业从业者

- 信息安全行业从业者
- 企业信息总监

2 系统概述

2.1 身份管理和访问控制发展行业背景

在企业信息化水平快速提升的背景下，随着 IT 应用的不断深化与拓展，应用系统逐渐增多，涉及的业务范围不断扩大，用户对应用系统的依赖程度越来越高，用户因业务需要而使用多个应用系统的情况也越来越多。用户管理是应用系统建设、管理和运维工作的一个重要方面。随着应用系统的增多，传统的烟囱式建设、单独管理的用户管理模式不仅使各应用系统运行的总成本不断上升，同时也提高了管理的难度，带来了安全风险。

2.1.1 业务需求背景

身份管理和访问控制平台的建设应实现企业内部员工、供应商、合作伙伴和外部客户身份信息统一供应、统一存储、统一认证、统一权限及审计管理等功能，并根据统一身份和认证业务的特点进行相应的制度和规范的建设，以形成保障业务用户身份和账号安全的完整体系，因此平台的建设需满足以下需求。

- 身份管理需求

通过身份管理和访问控制平台的搭建，以数字身份为连接点，打通信息孤岛，建立用户全生命周期的数字身份与账号权限的自动化管控机制，实现从统一身份源将用户的信息自动同步至其它应用系统中。建立组织的统一用户信息全景图。实现组织范围内的组织结构及人员分布的实时查询和展现。

- 身份认证及单点登录需求

随着业务的发展，应用越来越多，种类越来越复杂，因此统一身份安全管理平台需在提供多种集成方式的基础上支持对多种强认证方式的灵活扩展，包括证书、动态口令、生物识别等，以保证用户的登录安全。

- 应用集成需求
  - 能支持 JAVA/.Net/PHP 等不同应用的 SSO 集成；

- 统一身份安全管理平台集成的方式应包括多种，针对不同类型的应用提供 最合适的集成方式，对于不能改造的应用也能提供解决方案；

- 集中审计需求

根据法规政策监管要求，身份管理和访问控制平台需要具备相关的审计功能，对用户管理和访问控制中的关键流程、操作进行审计。

2.1.2 技术背景

身份管理和访问控制平台在建设过程中需要考虑以下技术需求：

- 应用服务器及存储资源需求
  - 支持主流的应用和应用开发平台的集成
  - 支持主流 LDAP 的集成
  - 支持主流的商业和开源数据库集成
  - 支持单机，集群，分布式，云端，混合等多种模式部署
- 用户认证支持
  - 传统的用户名/口令
  - 可扩展认证接口
  - 多因子认证
  - 防止篡改，重放攻击等
  - 手机 OTP 令牌认证
- 网络需求
  - 支持分布式部署和管理
  - 通过不同入口进入网络的设备，能访问的效果不同
- 扩展性要求

  平台的设计应采用分层的模块化结构，以达到设置修改灵活，扩充方便，适应业务的发展变化。
- 容灾备份要求

  同城、异地容灾系统的设计
- 性能要求

  需要高可靠性、稳定性的网络交换系统、服务器存储系统、数据库管理系统、

应用中间件等软硬件支撑系统作为支撑。

2.1.3 安全背景

随着企业积极开展数字化转型以提高企业的信息化水平，提升企业整体运作效率的同时，带来则是因为未重视信息安全所带来的隐患，比如分散在各业务单元的系统孤岛、数据孤岛。一些航空、金融行业，即使是在同等行业里面相对算是规模较小，但每年新建的系统多达几十套。

而它们会随着企业的成长，愈发严重，最终成为企业的致命弱点。那么这些弱点体现在哪些地方，我们可以看以下三个案例。

案例一：2015 年 3 月，由互联网白帽子用渗透工具扫出来的弱口令，经 CNVD 验证，并上报至 CNCERT 的安全漏洞，国内某大型运营商某后台存在弱口令导致泄露 16 个数据库帐号密码等信息事件。

案例二：2014 年 12 月国内大型汽车集团某内部关键站点弱口令泄露大量内部信息（姓名、职位、手机号码、开户行、内部邮箱）

案例三：2011 年 12 月 CSDN 的明文密码和用户帐号泄露事件。

- 有近 45 万的用户使用 123456789 和 12345678 做口令。
- 有近 40 万的用户使用自己的生日做口令。
- 有近 15 万的用户使用自己的手机号做口令。
- 有近 25 万的用户使用自己的 QQ 号做口令。
- 设置成弱口令的用户占了 590 万，也就是那种就算你用 MD5 或是 SHA 散列的也能很快就被暴力破解出来的口令。
- 只有 8000 多个用户的口令里在 8 个长度以上，并有大写字母，小写字母，数字，并不在字典表里。

从上面三个历史案例我们可以了解到，不管是互联网系统、还是企业内部系统，对用户身份凭证的保护水平受限于对安全的认知、重视。而其后果则是因为数据泄露、系统受破坏等，致使企业受到经济损失、政府的处罚等。

因此，在当前安全事件频发的形势下，组织亟需建设统一身份安全管理平台，构建以身份为核心的新安全边界。在整体信息安全框架内，统一身份安全管理平台遵循统一的信息安全管理相关策略、制度，在物理安全、应用安全、数据安全、网络安全和主机

安全等基础性安全建设内容基础上，在应用系统身份鉴别、访问控制、关键操作抗抵赖、通信安全、个人信息保护和资源控制等方面加强安全保护，最终实现业务安全的目标。具体安全需求如下：

- 系统安全要求

由于统一身份安全管理平台处于用户数据管理的核心位置，必须保证其自身系统的安全性。

  - 统一身份安全管理平台在设计过程中的内部流程、开发规范、接口规范必须符合企业相关的安全规范和安全要求；
  - 统一身份安全管理平台必须采用安全的操作系统和应用软件，根据需要对主机操作系统进行定期安全加固；
  - 统一身份安全管理平台在设计中，应避免不必要的信任关系，尽量使高安全级别的系统访问低安全级别系统，避免存在一定安全隐患的系统将风险转移到高优先级的系统。

- 数据安全要求
  - 统一身份安全管理平台的数据生成、存储、使用必须是符合企业相关的安全规范，有明确的数据安全访问、存储、备份机制；
  - 统一身份安全管理平台中的敏感性数据，如用户信息、密码信息、审计信息等支持加密方式存储。加密算法的类型必须考虑与其他身份管理模块之间的配合通信。
  - 通讯安全要求
  - 统一身份安全管理平台产品内部组件之间通讯连接能够支持加密方式；
  - 统一身份安全管理平台同其他系统间互通在性能允许情况下支持安全的加密通讯连接。

2.1.4 政策背景

2.1.4.1 国际相关法规政策要求

国际上许多政府要求企业关注身份管理。 Sarbanes-Oxley，Gramm-Leach-Bliley 和 HIPAA 等法规要求组织负责控制客户和员工对信息的访问。 身份管理系统可以帮助组

织遵守这些规定。

欧盟的《通用数据保护条例》“GDPR”要求所有组织对个人数据的使用，必须征得个人的同意，而且个人可随时收回使用权；要求企业必须梳理其当前个人信息资产分布，确保用户有唯一地方可以修正这些信息；在用户的要求下，用户数据可以从一个组织转移到其他组织。

2.1.4.2 中国相关法规政策要求

《中国网络安全法》明确提出，国家实施网络可信身份战略，网络可信身份认证体系是网络安全的核心。支持研究、开发安全、便捷的电子身份认证技术，推动不同电子身份认证体系的互认。推动已有的网络身份认证体系的互联互通，建立跨平台的网络可信身份体系。例如在第四章“网络信息安全”第四十二条规定：“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。”

2019 年 5 月 10 日，《网络安全等级保护制度 2.0》标准正式发布，实施时间为 2019 年 12 月 1 日。“等保 2.0”在二级和三级中对身份安全标准都有明确规定，主要分三部分：身份鉴别、访问控制、安全审计。

例如在等保 2.0 三级中对“身份鉴别”的要求是：1、系统用户采用用户名和用户标识符标识用户身份，并确保在系统整个生命周期内用户标识的唯一性；2、应支持用户身份标识和用户鉴别；3、在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

在等保 2.0 三级中对“访问控制”的要求是 1、应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并将这些权限的部分或全部授予其他用户；2、自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级和（或）记录或字段级； 3、自主访问操作包括对客体的创建、读、写、修改和删除等。

在等保 2.0 三级中对“安全审计”的要求是：1. 安全审计应记录应用系统的相关安全事件（重要和非重要的都要记录）；2. 安全审计记录应包括安全事件的主体、客体、时间、类型和结果等内容 ；3. 安全审计应提供审计记录查询、分类、分析和存储保护；

4. 安全审计应确保对特定安全事件进行报警；5. 安全审计应确保审计记录不被破坏或非授权访问；6. 系统应为安全管理中心提供接口，对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

2.2 什么是 IAM

IAM 在 Gartner 中的定义为：Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reason。即 IAM 是一个可有效控制人或物等不同类型用户访问行为和权限的管理系统，能够有效控制什么人或物体在什么时间有权限访问哪些资源。

IAM 致力于解决至关重要的需求，即确保在日益复杂的技术环境中合理访问资源，并满足日益严格的合规性要求。对于任何企业而言，IAM 都是一项非常关键的任务。它与业务紧密保持协同，并且需要业务技能，而不仅是技术专长。企业通过成熟的 IAM 产品可以降低其身份管理成本，同时更重要的是，在支持新业务计划方面变得更敏捷。

综合权威分析机构的解释，IAM 是保障信息系统高效连接，人员访问安全，以及实现组织数字化转型目标的核心基础设施。IAM 核心价值是连接、安全和效率。IAM 是数字化转型的必要条件，是组织信息化的顶层设计以及信息化管理的重要支撑部分。

2.3 Identity、Authentication、Authorization、Audit 的定义和关系及与 IAM 的联系

身份管理包括数字身份的创建，管理和删除。 访问管理包括仅对实体需要访问的数据进行授权。

IAM 核心模块包含身份，认证和授权（注意：此三个模块为 IAM 体系最为关注的三个模块，并非 IAM 全部内涵）。

2.3.1 身份 Identity

身份（Identity）是一个自然人在传统 IT 系统或者云端的唯一标识。身份管理旨在构建企业或组织中的各类用户在其信息化体系中统一规范的身份识别和管理体系。

供应和取消供应是访问管理的关键方面。供应是创建帐户以允许用户访问正确的系

统和资源的过程。用户供应的目的是简化帐户创建并提供一致的框架以提供对最终用户的访问。

取消供应是当用户不再需要访问权限时禁用用户帐户的过程。这可能是由于用户离开组织，在组织内转移，角色更改等导致的。在云计算环境中，取消供应是指终止或禁用云平台或基于云的用户帐户中的 IAM 服务。

身份管理的核心是基于工作流的账号全生命周期管理。

2.3.2 认证 Authentication

认证是验证尝试访问受保护资源的实体的凭据的过程。

身份验证必须以安全，可靠和可管理的方式进行。对于要求更高安全级别的受访资源，可能需要多因素身份验证。

单一登录（SSO）是访问管理的功能，其中用户经过一次身份验证，并且会话的凭据在安全域内的不同应用程序之间被判定为可信。这通常在一个安全或风险域内完成。在运营特定云基础架构中所有应用程序的组织中，SSO 是一项关键要求。

2.3.3 授权 Authorization

授权是访问控制的重要机制。用户和应用程序或系统都必须授权以访问资源或其他服务。授权要求包括建立可信身份配置文件并创建（或重用现有的）访问控制策略。

授权和访问控制对于信息安全管理至关重要。安全性应包括粗粒度和细粒度授权，并且应支持对人类用户和机器对机器交互的授权。授权功能必须与其他安全功能配合使用，尤其是身份验证，消息保护和事件监控。

授权管理应确保用户也具有合理的访问权限。策略定义和执行功能都必须可用。针对现有的授权策略，用户访问需要实时批准或拒绝。

访问控制是根据“托管策略”分配的，“托管策略”是一组规则，用于确定哪些用户，组和角色有权访问哪些资源。许多组织遵守“最小权限原则”（PoLP），该原则规定，应向用户授予他们充分发挥作用所需的最小权限。

通过限制内部或外部威胁行为者可以执行的操作，PoLP 可以大大降低发生严重数据泄露的风险。

授权正在经历从 RBAC 到 ABAC 再到 PBAC 的演进过程。

PBAC(基于策略的访问控制)可以实现访问控制的简化和权限设置智能化：

- 授权不依赖于任何特定实现（XACML）并且可以用自然语言实现设置；
- PBAC 可以实现环境设置；
- 策略可以基于事件快速调整；
- PBAC 可以通过控制数据访问，控制访问蔓延，组织授权用户以正确的方式访问数据；

2.3.4 IAM 架构

身份和访问管理（IAM）包括人员，流程和系统，这些人员，流程和系统用于通过确保对实体的身份进行验证，然后基于受保护的资源（此保证的身份）授予正确的访问级别来管理对企业资源的访问以及其他上下文信息。

IAM 的构建模块可以分为三类：

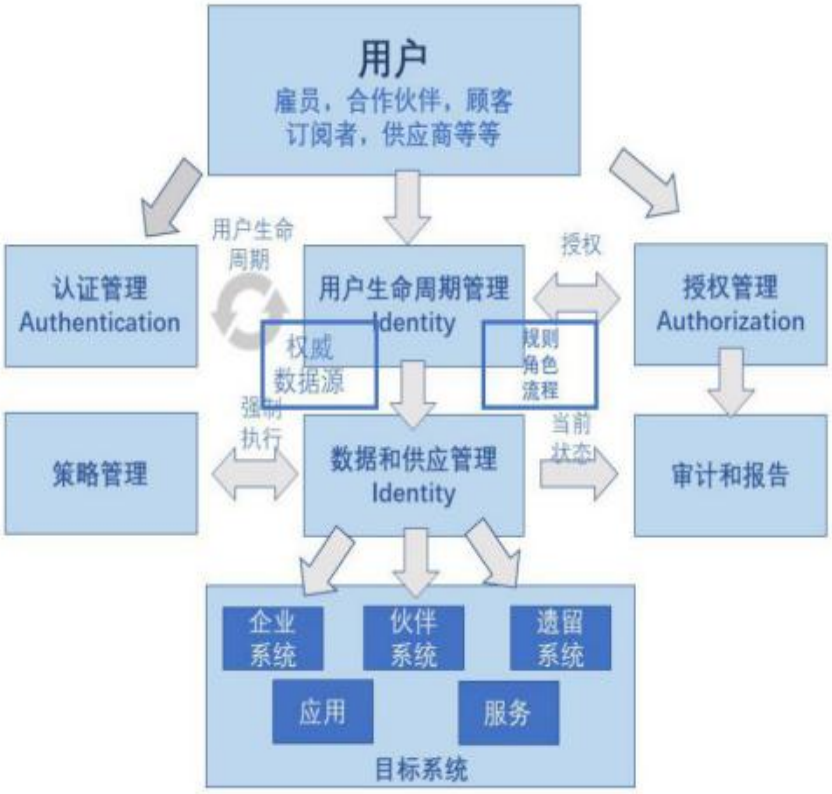
身份：如何定义和管理在线体验？

认证：如何证明身份？

授权：身份可以做什么？

IAM 概念体系结构涉及将各种传统 IAM 功能组合到整体的逻辑层中。

- 访问和策略服务：身份验证，授权和访问策略管理的各个级别和深度
- 用户服务：供应，自助密码重置，委托管理和集中式用户管理服务
- 身份服务：来自权威源的身份数据同步，用户数据同步和关联，密码策略实施和同步，身份虚拟化，模拟和转换（从人员级别到企业/组/企业级别）
- 合规服务：合规和政策，维护审核跟踪，监视安全事件和报告功能
- 数据服务：集中的身份和权利存储库，提供有关用户身份的商业情报，并提供操作和合规性的访问报告数据。



图：IAM 架构

2.4 IAM 的核心能力

IAM 应包含数字身份自动化管理、身份数据同步、统一认证及访问控制策略管理、授权管理、自适应智能融合认证、访问行为审计、权限互斥审阅、合规管理以及确保实时预警和有效防范的风险管理机制等核心能力。

2.4.1 身份管理

身份管理包含用户管理、机构管理、应用管理、数据同步、密码策略管理、生物特征管理以及用户自服务等能力，覆盖了用户全生命周期管理、用户属性自定义、用户电子身份唯一化、用户电子身份自动化等多方面，建立统一用户身份库，集中管理组织内部员工、外部用户、访客、供应商等各类型人员的电子身份/账号，从开通、授权、变更、禁用、删除进行全生命周期统一管理，实现身份同步与聚合。

2.4.2 权限管理

IAM 平台建立权限统一管理的入口，集中管理包含角色、机构、用户组、菜单、按钮等权限。根据身份权限流程实现业务权限、系统权限的自动化赋予与回收，提供用户自助开通、变更、撤销权限等服务，确保可信的人在合理的时间访问适当的系统和数据；通过权限自动化规则引擎管理，实现权限半自动授权和按规则自动授权，支持按账号、组织、岗位等不同维度进行授权。同时提供权限合规和权限互斥的能力。

2.4.3 统一认证及访问管理

提供各类应用的统一登录入口和集中导航，实现一套账号体系登录、全网通行；融合多种认证方式，构建统一认证服务能力，支持包括密码、证书、短信等传统认证方式，指纹、声纹、人脸等生物识别方式，AD、钉钉、企业微信等第三方认证服务，QQ、微信等社交认证服务等，同时支持快速扩展其他认证方式；平台能根据不同应用的安全等级设置、访问人群、风险指数，灵活配置认证方式和访问策略。

2.4.4 风险管控

基于 IAM 平台中事先预设好的风险管理规则，同时根据用户访问元数据（时间、地点、习惯、账号、关系、行为、权限等）实时计算用户访问行为的风险评分，当系统检测到反欺诈风险时，平台主动阻断风险以保证用户访问的安全性。

2.4.5 合规审计

通过平台的可视化报表记录用户访问行为，提供事后追溯能力，同时定期对审计日志进行归档，持久化保存日志数据。

2.5 IAM 发展历程及趋势

2.5.1 IAM 发展历程

1853 年的第一份出生证明–早在 1853 年，英国政府就对婴儿进行了强制性出生登记。整个美国在 1902 年被标准化。有关出生的数据最早在 1500 年代记录在英格兰的教堂里。

1903 年第一个驾照–密苏里州和马萨诸塞州成为第一个颁发并要求人们拥有驾照才能操作汽车的州。

1920 年首次护照–第一次世界大战后，国际联盟提出了全球护照标准，并受到国际联盟的支持。

1935 年第一个社会安全号码– 1935 年签署了《美国社会安全法》。1936 年 11 月，纽约的约翰·戴维·斯威尼（John David Sweeney，Jr.）发行了第一个社会安全号码。由于税收原因，许多其他国家/地区也部署了类似的国民身份证号，或者作为一般的身份证号码。

1960 年，第一个数字身份和密码– FernandoCorbató引入了使用密码来使单个文件保密的功能。身份管理系统随着网络计算的发展而发展。身份管理包括手动电子表格和用于跟踪帐户的定制应用程序。安全的重点是在网络防火墙内保护敏感信息。

1990 年商业互联网的诞生– 1989 年开始了第一个商业拨号服务。1991 年广播了第一个实时在线视频。1993 年，第一个消费者网络浏览器问世。传统的身份管理系统适用于在线应用程序。成本高，维护复杂，不安全且难以更改。

2000 年身份管理堆栈诞生了–互联网在全球范围内增长到 4 亿用户。身份盗用和数据泄露呈指数增长。由于遵守法规，美国 2002 年《萨班斯法案》增加了对身份管理的需求。身份和访问管理公司激增并合并。安全性得到改善，但是成本和复杂性仍然很高。供应商竞争成为“端到端”身份和访问管理提供商。

2006 年首个身份管理托管服务–在线人数增长到 1,114,274,426。成本和复杂性的增加导致了 IAM 的第一个托管服务。单点登录需求增加，但是解决方案有限且难以部署。云服务开始在所有行业中激增。

2010 年身份即服务（IDAAS）云–对可用 IAM 技术的需求和不满导致一系列 IDAAS 云服务专注于简化，自动化和降低成本。区块链技术导致快速采用比特币和去中心化系

统的新模型。IAM 行业仍然专注于集中式身份堆栈平台。

2014 年，集中式身份破坏–集中式身份平台因快速采用云应用程序而增加了数据公开度，从而被打乱。应用程序集成和安全协调变得更加困难且管理昂贵。数据泄露迅速增加。

2016 分散的“自带身份”身份管理诞生了– IdRamp 分散的身份结构的诞生是为了简化应用程序集成，扩展业务功能和自动化安全流程。“自带”去中心化身份成为一种实用的方法，可以在不影响现有投资的情况下提高安全性和扩大业务价值。

2020 年基于分账的 IAM 和自我主权身份–基于分账的 IAM 和自我主权身份解决方案激增，以改善安全性和法规遵从性。采用“自带”去中心化身份服务将传统 IAM 与自我主权身份模型联系起来。

2.5.2 IAM 发展趋势

Gartner 在最新发布的《2020 年规划指南：身份和访问管理》中提出关键论点：IT 必须推进 IAM（身份和访问管理）计划。IAM 安全技术专家应关注无口令认证、价值驱动的 IGA（身份治理和管理）、增强的消费者隐私要求、混合/多云环境的趋势。

从 2020 年起，IAM 领域发展的几个趋势如下：

趋势一：IAMaaS （IAM 即服务）

随着企业越来越多地将 IT 环境迁移到云端，许多 IAM 功能被转移到云中并实现了自动化。远程用户可以轻松地访问其工具：他们只需使用一次登录（SSO）即可访问所需的所有资源。

趋势二：在微服务之间实现 IAM

IAM 解决方案开始与微服务集成。在一个这样的解决方案中，微服务之间的每个通信还包括一个唯一的令牌，该令牌在收到后便会得到验证。应用程序仅在收到有效令牌后才执行请求的功能。在微服务环境中使用 IAM 可以防止不良行为者假冒微服务或窃听应用程序。

趋势三：区块链上的数字身份

自我主权身份使用户在网上也能够以“亲自证明”相同的方式对自己进行身份验证。用户可以存储自己的个人识别数据，而不必将其提交到某个公司管理的集中化数据库

中。

趋势四：基于风险的身份验证

也称作自适应身份验证，这种验证方式可以被描述为变量矩阵，这些变量的结合会产生一个风险信息。基于这个风险信息，在某些功能执行前，可能需要添加额外的身份验证要求。基于风险的身份验证系统旨在识别升高的身份验证风险。

趋势五：IOT 扩大了身份的边界

随着物联网的大力发展，设备，机器人，IOT 等设备如今都需要访问网络和数据资源，所以这些设备也应该纳入身份管理的范围。

趋势六：IAM 与 UEBA 的整合

将 UEBA 与 IAM 集成可创建基于实时用户行为检测的主动修复方法。对于部署 IAM 的企业来说，已经收集的大量 IAM 数据为行为提供了必须的上下文，将这些数据投入使用可为潜在的安全事件提供强大的机制和预防性控制。

3 身份管理

身份管理对象

身份管理的对象是信息系统的所有实体，比如人员、组织、设备、应用等，它们作为数据在系统内被存储和处理。这些个体通常具有一些属性，信息系统的业务目标决定了与个体有关的哪些属性将用于其身份。

从不同视角出发，身份管理的对象可分为访问主体对象，访问客体对象和被管理的实体内容。

3.1.1 访问主体对象（2E、2B、2C、IoT 等）

访问主体是访问控制流程里的主动的实体，主体访问客体。访问主体可以是人员、终端、主机，或者应用程序等。传统的主体对象为企业员工，随着信息技术的不断发展，一些新的主体对象比如合作伙伴、消费者、IoT 身份等开始涌现。

3.1.1.1 企业员工 Employee

企业员工是传统的主体对象。企业由于自身的组织形式，决定了其身份管理具有以

下特点：

- 与企业的组织架构相吻合
- 结合组织架构构建身份管理，将员工纳入组织架构中并根据所处节点的不同为其授予不同的权限。
- 统一的管理策略
- 企业员工由 HR 或 IT 部门统一录入，对用户体验、性能有一定的容忍度，更追求一致的管理策略，比如统一的密码管理策略、全员 MFA 等。
- 最小权限原则
- 企业员工的权限分配应遵循最小权限原则，员工应只具有满足其工作需求的最小权限，从操作层面主动杜绝员工越权行为。
- 权限轻松随着人员的调动而更改
- 当员工加入或离开组织时，企业要能够轻松配置和取消其访问权限。

3.1.1.2 合作伙伴 Business Partner

随着企业规模的日渐扩大，企业与合作伙伴之间的合作较往常更加频繁，企企业间人员的互访问给身份管理带来了新的挑战：

- 联邦身份管理和认证
- 合作伙伴可能要求使用自己的用户来登录系统，这就要求企业的身份管理要支持联邦身份认证。联邦身份提供了企业间的单点登录功能，增加企业灵活性。
- 与供应商系统的集成
- 企业的身份管理要与供应商系统（比如 ERP、CRM、OA 等）无缝衔接。
- 数据合规与授权
- 企业间互访问与数据共享要重视与身份和授权相结合，遵从日益严格的数据和隐私法规。

3.1.1.3 消费者 Consumer

消费者身份管理需要更多的平衡用户体验与企业的安全要求，往往具有以下特点：

- 数量巨大

- 消费者数量往往巨大，常常达到百万千万甚至亿级。用户访问量可能突然爆发、消费者行为不可控等给系统设计带来巨大压力。
- 终端类型多样与社交认证
- 消费者应能够选择认证的设备、认证方式以及安全级别，这些设备可以是传统的网页，也可以是手机、平板等移动设备，认证方式可以是邮箱、手机，也可以是微信等社交认证。
- 商业智能与营销
- 企业希望将消费者身份与客户关系管理 CRM、市场与商业智能软件 BI、ERP 等系统打通，持续收集消费数据，评估消费者行为，以提供精准广告营销。
- 隐私保护与数据合规
- 企业受地区之间不同的各种隐私和数据保护法规的约束，消费者有权掌握个人数据。

3.1.1.4 物联网 IoT

与现有 IAM 系统需要支持身份量级相比，物联网引入了对指数级身份进行管理的需求。 安全行业正在看到一种范式转变，IAM 不再仅仅关注于管理人员，还管理着可能与网络相连的成千上万的“事物”。 在许多情况下，这些事物是断续连接的，可能需要与其他事物、移动设备和后端基础结构进行通信。有人将这个新的身份生态系统称为“IDoT”（Identity of Things）。IDoT 是指设备与人员、设备与设备、设备与应用程序/服务或人员与应用程序/服务之间的关系。

3.1.2 访问客体对象（各类应用、数据等）

访问客体是访问控制流程里被动的实体，它在访问控制的保护下，接受主体的访问。

传统的访问客体对象包括应用程序、网站、服务器、文件系统，这些客体对象是信息系统的肉眼可见的组成部分，企业建立 IAM 首先要规划企业雇员和各个组成系统的权限关系，保证正确的人才能访问相应的系统。

随着云计算和大数据的发展，对访问客体的颗粒度要求越来越细致，传统的应用级

访问控制已经不能满足要求，访问客体对象发展到服务 API 级别，甚至数据级别。不同的访问主体虽然都具有应用的访问权限，但是能使用的 API 和服务内容是不同的，能看到的数据也不同。

3.1.3 管理实体内容

身份管理是身份认证和访问控制的前提条件，访问主体和客体只有录入 IAM，并建立访问控制关系，才能使整个 IT 环境安全有序的运转。身份管理要管理的实体包含了维持这套体系运转的所有相关内容，主要有以下几个方面：

- 用户管理
- 用户生命周期管理，包括创建、删除、激活、归档、吊销、恢复等；用户类别和属性的管理，比如正式员工、临时员工等。
- 组织架构管理
- 管理企业的组织架构，包括组织层级的划分，比如单位、部门和岗位，各个层级的构建，以及员工规划等。
- 角色管理
- 管理用户的角色，包括角色生命周期的管理，角色组、静态角色和动态角色等。
- 账号管理
- 管理所有的账号信息，比如登录信息、所属的应用和身份等；
- 资源管理
- 管理访问客体，比如应用或服务管理、资源管理等。
- 权限与访问控制管理
- 管理访问主体与访问客体的访问控制关系。
- 根据权限管理类型的不同，权限管理的呈现会有很多差异。访问主体对访问客体发起访问请求，只有满足了访问客体相应的权限要求，访问请求才能真正到达访问客体。
- 策略管理
- 管理 IAM 的所有策略，比如：供应策略、密码策略、多因素策略等。
- 工作流管理
- 管理 IAM 工作流，包括：活动管理、工作流管理、请求管理。

- 审计与风控管理
- 记录管理员和用户访问的所有日志，收集系统安全事件，根据业务需要生成报告和报表，并同步到 SIEM 平台实现持续风险发现和安全运营。

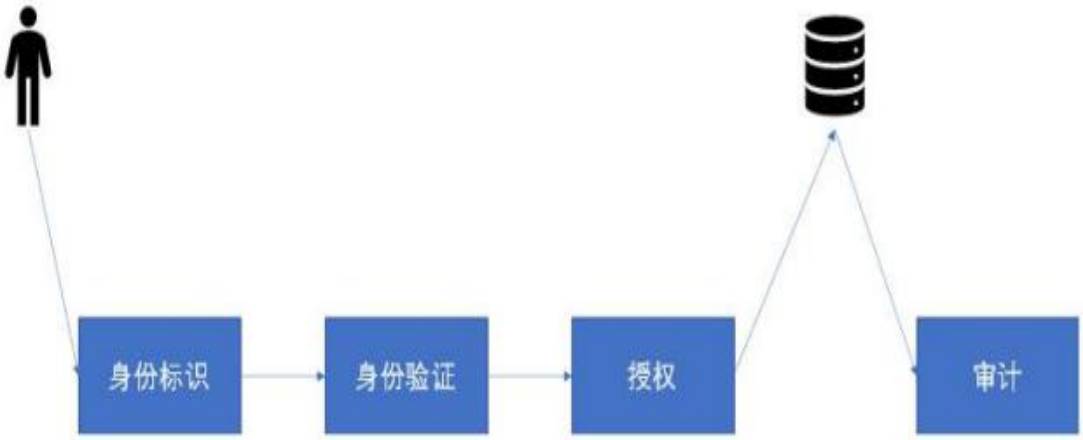
3.2 身份识别服务

身份识别服务使用数据分析等手段梳理各信息系统中的用户、账号数据，确认其对应的自然人，通过为每个自然人建立唯一的身份标识，与各系统中的账号进行身份关系匹配，确保每个自然人用户在所有系统中都有唯一明确的身份。

用户通过使用用户名或账号就能够提供身份标识。为了能够进行正确的身份验证，用户往往需要提供进一步的凭证，这些凭证可以是密码、密码短语、密钥、生物特征或令牌。这两种凭证项将与先前为该用户存储的信息进行比较。如果这些凭证与存储的信息相匹配，那么主体就通过了身份验证。但验证工作并未结束。

一旦用户提供了其凭证并且被正确标识了身份，用户试图访问的系统就需要确定该用户是否具有执行请求的动作所需的权限和特权。系统会查看某种访问控制矩阵或比较安全标签，以便验证该用户是否确实能够访问请求的资源和执行试图完成的动作。如果系统确定用户可以访问特定的资源，就会为该用户授权。

尽管身份标识、身份验证、授权与审计都具有完整和互补的定义，然而它们在访问控制过程中都有着自己明确的作用。一个用户可能能够顺利地通过网络上的身份标识和身份验证，但是可能不被授权访问文件服务器上的文件。另一方面，用户能够被授权访问文件服务器上的文件，但是在未顺利通过身份标识和身份验证之前，他们将无法获取这些资源。



用户在一个系统或区域内的动作应当可被审计。确保可审计的唯一方法是用户能够被唯一标识，并且用户的动作被记录在案。

3.3用户分类管理

3.3.1 目标

用户分类管理的目标是明确用户或用户所拥有账户的分类管理。以便企业能够依据用户，账户的分类情况，以最小授权为基准，在系统中赋予用户账户一定的权限，使用户可在工作职责范围内获取相应的信息。

用户的分类应以账户功能和使用目的为原则，形成统一的分类标准，并应用于不同的系统和平台。

3.3.2 责任

用户的账户分类应由企业信息安全部门负责管理和解释，管理细则需由管理层审阅通过并实施。

3.3.3 用户账户分类

用户账户对于可依照所有权分为终端用户账户和系统账户。终端用户账户从用户来源可分为内部账户，经销商、合作伙伴、供应商账户以及外部客户账户。系统账户包含一般系统内置账户，高权限系统内置账户，功能性账户以及一般支持性账户等。账户所

有者应了解该账户的使用目的，由企业信息安全部门确保账户权限遵照最小授权原则。

账户分类	分类说明	账户所有者
终端用户账户 To E	指内部员工的账户	内部员工
终端用户账户 To B	指经销商、合作伙伴、供应商账户	经销商、合作伙伴、供应商
终端用户账户 To C	指 C 端消费者账户	外部客户
高权限系统内置账户 Built-in Privileged Functional ID	随系统安装而产生的各种高权限账户(administrator，root，sa，LEP 等)	IT 基础架构团队
一般系统内置账户 System Functional ID	除高权限账户外的其他随操作系统，应用、数据库安装的账户	IT 基础架构团队
功能性账户 Functional ID	创建以支持基础架构子系统运营维护（日志，监控，备份，排错等）	IT 基础架构团队
	创建以支持信息安全子系统运营维护（防病毒应用，DLP,防火墙等）	信息安全团队
	创建以支持应用系统开发，运营维护	应用开发团队
	创建以支持系统，应用等特殊需求的账户（系统间通信等）	其他目标团队
一般支持性账户 Generic ID	非高权限账户用以支持系统或应用团队日常工作（系统状态巡检，日志查看，检查等）	系统及应用团队

3.3.4 功能性账户

当一个账户可在不同时间被不同的人用的账户即可称之为功能性账户。

一个功能型账户又可将其分类为高权限功能性账户(Privileged Functional ID)和非高

权限功能性账户(Non-Privileged Functional ID)。这类账户均可被系统或者被授权的用户在需要时，用来完成相应任务。

高权限功能性账户指的是那些拥有能够导致系统损坏的权限的账户。3.3.3 中的高权限系统内置账户(Built-in Privileged Functional ID)是高权限功能性账户的一种。

非高权限功能性账户指的是那些创建来完成单一任务的且不具有高权限的账户。

账户的可交互式访问：

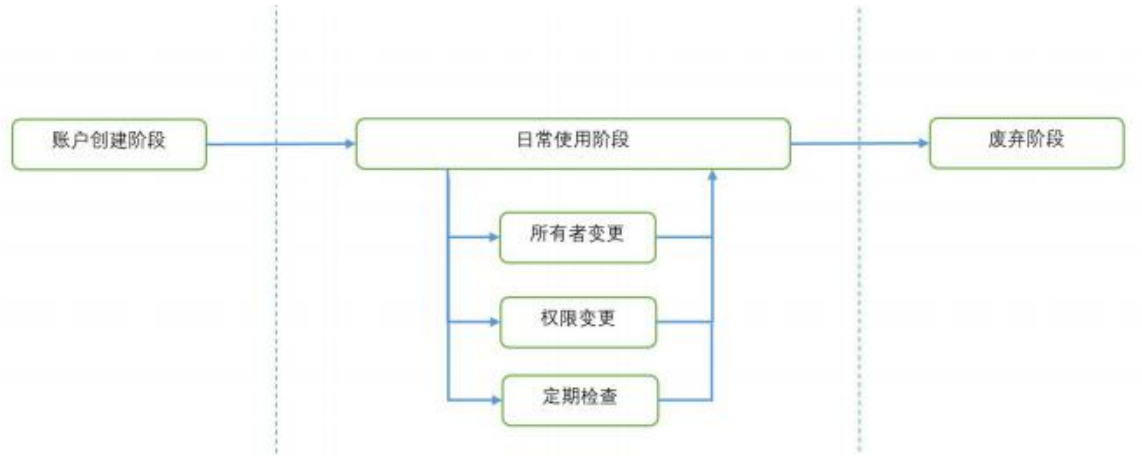
- 可通过本地控制端口登录系统
- 可通过网络远程登录系统

类型	创建时间	可交互式访问情况 (Interactive)	不可交互式访问情况 (Non-Interactive)
高权限系统内置账户 Built-in Privileged Functional ID	随系统或应用安装/升级自动创建	例如：Administrator,root,在服务器和数据库中的 sa，网络设备中的 local enabled password(LEP)	随系统或应用创建但账户设置为锁定或者禁用。没有初始密码。例如: Liunx 中的 lp，adm，raadmin，sudoadm 等
高权限功能性账户 Privileged Functional ID	在应用安装之前或之后按需创建的账户	为支持应用正常运行而创建，这类账户一般用于以下目的： 1）能启停服务或者运行批处理任务 2）进行单一的数据补丁任务，如插入，更新及删除 3）为应用服务器和数据库间通信 4）源代码部署 密码需要加密放入脚本或	这类高权限账户主要实现服务必要的功能，但不能交互式登录 比如：用来启停服务或者运行批处理的账户

		者嵌入应用	
非高权限功能性账户 Non-Privileged Functional ID	在应用安装之后按需创建的账户	a. 用于日常监控服务和进程，确保其工作正常的账户 b. 用于日常查询日志，查看一般信息的账户 该类账户应具有一下特征： 1）对非客户数据仅具有*读权限* 2）不应具有写权限 3）数据库中的客户数据必须已经有了适当屏蔽 4）包含客户数据的文件不能给予其读权限	不适用

3.4用户全生命周期管理

用户账号在系统或应用中的生命周期，应包含以下几个阶段：



- 建立阶段：账号应依据系统或应用的访问控制要求，在取得相应授权后，由用户管理部门负责创建账号。
- 存续阶段：账号一经建立，账号所拥有的权限和生效情况应通知所有者。
- 存续阶段-使用：账号拥有者应依据具体工作要求和账号使用流程，适当使用账号进行日常工作。
- 存续阶段-所有者变更：账号的所有者可能因人员流动，部门变动而改变。账号所有者应及时提交变更请求，得到授权，并由用户管理部门进行账号所有者的变更操作。
- 存续阶段-权限变更：账号在经由账户所有者确认，在符合系统或应用的访问控制要求的前提下，可进行权限变更以适应新的功能需要。
- 存续阶段-定期检查：账号应定期进行检查以使账号所有者确认其账号的存在，是否需要保留、变更权限或者删除。
- 废弃阶段：当账号经检查不再需要时，则由账户所有者或其授权人员提交删除请求，在系统和应用中删除账号。

高权限系统内置账户和一般系统内置账户

- 建立阶段：这两类账户随系统或应用的安装而创建，建立时已经包含系统或应用开发时定义的一些权限。账号所有者需要判断这类账号是否需要启用或禁用，权限是否需要变更。
- 存续阶段：
  - 所有者变更：当账号所有者需要变更时，应及时进行变更。
  - 权限变更：随着账号的日常使用，账号的权限会随功能的增减而发生变化。
  - 定期检查：账号所有者应定期检查账号使用情况，依据需要进行相应增减和变更。

- 废弃阶段：这两类账号一般随系统或应用的下线而废弃，不需另有流程进行单独处置。
- 终端用户账户
- 建立阶段：一般由用户入职开始，用户个人账号建立，其权限应按最小授权赋予。
-
- 存续阶段：
- 所有者变更：个人账号以便没有所有者变更问题。
- 权限变更：个人账号可根据工作要求，经访问控制检查和授权，赋予其系统或应用的使用权。该权限不应包含系统和应用的管理权限。
- 定期检查：账号所有者应定期检查账号使用情况，依据需要进行相应增减和变更。
- 废弃阶段：用户个人账号一般随用户的离职而删除。用户的系统和应用账号和权限也应及时删除。

功能性账户

建立阶段：由各系统或应用的管理团队中的账号所有者依据工作需要在系统或应用中创建权限单一的功能性账号并依据最小授权原则赋予功能性账户权限。

存续阶段：

所有者变更：账号所有者应在相应团队中，若所有者离职或不再适合担任该账号所有者，应进行所有者变更。

权限变更：账号所有者依据工作需要在系统或应用中创建权限单一的功能性账号并依据最小授权原则赋予功能性账户权限。

定期检查：账号所有者应定期检查账号使用情况，依据需要进行相应增减和变更。

废弃阶段：账号所有者应判断功能性账户是否不再需要，并提出删除请求进行删除。

一般支持性账户

建立阶段：该类账户应由个人拥有和申请，不能将账户分享给其他人使用。权限应限制在查询，查看等层面。

存续阶段：

所有者变更：当拥有该类账户的个人因离职或调岗等原因不再适合作为拥有者时，相应团队应将该账户分配给其他尚未拥有该类账户的员工。

权限变更：该类账户一般不会进行权限变更，若暂时没有合适的所有者，团队可申请将该账号禁用。

定期检查：账号所有者应定期检查账号使用情况。

废弃阶段：账号所有者应判断一般支持性账户是否不再需要，并提出删除请求进行删除。

3.5用户信息存储

目录服务是企业和云中安全性的基本组成部分之一。目录服务提供了通过唯一标识符和位置存储和标识的信息的有组织的存储库。

基于 X.500 标准的轻型目录访问协议（LDAP）是目录服务的主要协议。 LDAP 目录服务器中的每个条目都通过专有名称（DN）进行标识。在云环境中，身份和访问管理框架将目录服务大量用作身份和访问信息的安全存储库。对目录服务的访问应该是身份和访问管理解决方案的一部分，并且应该与所使用的核心身份验证模式一样强大。如果这些服务器托管在本地而不是云中，则 IAM 服务除了需要管理其访问权限的任何应用程序和服务之外，还需要连接到本地轻型目录访问协议（LDAP）服务器。

3.5.1 常见用户属性说明

Schema 的设计主要体现以下原则：

- 不改变 LDAP V3 中所定义的标准对象类和属性；
- 按照存储数据的类别进行类别划分，需要使用以定义标准属性的，从标准类继承获得；
- 所有扩展的对象类和属性都必须增加企业的前缀，XX 为公司名称的简称；
- 数据之间的层级关系通过属性关联的方式展现，减少一个条目的数据变化造成多个相关信息的修改。

按照企业应用系统特点，我们可以定义出需要扩展的 schema，但随着业务的发展，今后一定有 schema 的扩展要求，可以遵循 schema 的扩展原则和 schema 维护的要求进

行扩展，部分内容需要近详细的需求调研后进行具体的细化设计。

Schame 的设计将从下面几个方面进行，

条目类型	资源类型	对象类（objectclass）
用户	正式员工	Employee
	临时员工	ExternalPerson
组织架构	单位	Org
	部门	Dept
	岗位	Position
角色	角色组	container
	静态角色	groupOfNames
	动态角色	groupOfMembers
应用帐号		AppAccounts
资源	资源组	container
	资源	XX Resource
访问控制策略	ACL	Acls
	ACL Entry	AclEntry
资源保护策略	POP	Pops
数据字典		Direct

3.5.2 LDAP 存储方式

目录树是目录系统很重要的一个技术环节，目录树结构的合理性保障了目录服务为应用提供快速的响应，以下是目录树的设计原则：

1、能够清晰的展现目录结构和目录中所存储的数据；

2、针对不同类别的资源应当提供不同的存储容器；

3、各类资源的依赖关系需要通过属性关联的方式匹配；

4、采用树与扁平相结合的方式，即能够体现目录数据结构，又不影响目录条目变更造成的复杂操作；

5、目录树结构能够灵活的支持总部和企业应用对目录数据使用的要求；

6、目录数据（条目）的变化对应用的影响最小化。

一级目录节点定义

一级目录节点为 XX 的根节点，dc=xxx, dc=com，不可更改；

使用标准的对象类 objectclass: domain

二级目录节点一般按下面范围进行设计，资源节点采用 objectclass: container 作为对象类，各节点的类型说明如下：

节点名称	节点描述
cn=users	存储所有员工信息的节点
cn=orgs	存储所有组织架信息的节点
cn=roles	存储身份管理系统中用于管理使用的角色信息节点
cn=apps	存储应用系统使用的帐号信息节点
cn=resources	存储身份管理系统中管理的资源信息节点，资源信息包括：系统资源、应用资源等
cn=POPs	存储身份管理系统中对资源保护的策略信息
cn=ACLs	存储身份管理系统中对资源访问控制的信息
cn=directiory	存储身份管理系统中需要使用的标准化数据信息的节点

企业可选择的 LDAP 软件很多：

开源软件：OpenLDAP

商业软件：IBM Security Identity Manager

Oracle Director Server

Microfocus Director Server 等

3.5.3 其他存储方式

从数据库的角度看待区块链的存储机制会简单直观很多。在一个标准的关系型数据库中，存储一般分为日志存储、用户数据存储、以及索引存储三大类（有些数据库可能还包含大对象存储等）。

而区块链项目中基本所有的“账本”存储其本质就是交易日志存储。用户数据存储则根据项目不同而有选择性地采用。譬如说对于 UTXO 结构的区块链项目来说，其每个账号对应的余额直接保存在内存哈希表中（或类似 LevelDB 等嵌入式 KV 数据库中），因此不需要一个独立的外接用户数据存储模块。而类似 Hyperledger 等通用区块链框架则一般包含类似 State Store 等存储最终结果数据的模块。索引存储则在当前大部分区块链项目中均不存在。

要解决持久性问题，内存数据库也有相应的解决方案。这其中包括在集群里保存额外的数据副本，然后对数据库进行横向扩展，让系统能够在运行中不断将更新数据复制到一个或多个备用系统当中。

一些数据库系统还会定期将数据复制到磁盘系统，就是为了应对上述突然断电或系统宕机的情况。当然这时候就要在额外的负载和数据可恢复性方面做出权衡。

3.5.4 加密信息存储方式

3.5.4.1 敏感数据保护

IAM 中存储了必要的用户身份信息，这些信息包含了很多个人隐私信息，比如身份证号、电话号码、家庭住址等，为了避免信息泄露造成的风险，同时也为了应对日益严格的数据安全和隐私保护的法律法规，必须要对这些信息规划一定的保护措施。

敏感信息多种多样，不同的敏感信息的保护方式也不同。下面列举几种通用的敏感

数据保护方式：

- 数据脱敏

数据脱敏是指对某些敏感信息通过脱敏算法进行数据的变形，实现敏感隐私数据的可靠保护。脱敏过程不可逆转，敏感数据的真实值被转换成虚构的、但看起来逼真的值，原始值被永久改变且无法恢复。用户的身份证号、手机号、卡号、客户号等个人信息在对外提供时都需要进行数据脱敏。

- 完整性保护

完整性保护是指对需要保护的数据产生一个校验值，校验者重复生成过程一定会生成一个一样的校验值，一旦数据被更改，则生成的校验值会随之改变。完整性校验一般采用哈希、MAC、HMAC、签名等密码学方法。

在运行环境存在运维风险，或者为了防止入侵者篡改数据，使用完整性校验可以在运行中发现数据错误，从而阻断风险蔓延。

- 强加密

对于某些特别重要的数据，比如用密码、指纹等数据，可以采用强加密算法，比如对称加密算法。加密过程需要密钥，数据经过加密后，直接转变为不可见数据。这种方式结合专用密码设备做密钥存储和运算卸载，安全等级最高。

3.5.4.2 密码加密方式

毫无疑问，密码需要加密后再存储。假设一个非常简单的系统只存储了密码本身，而验证过程是一个简单的字符串比较。一个攻击者只要看一眼包含密码的文件或数据库的内容，那么密码就会遭到泄露。不幸的是，在实践中确实有很多类型情况会导致密码泄露，比如备份放置不当、硬盘报废但未被擦除、SQL 注入攻击等。

为了保护密码不被轻易盗取，可以采用以下几种方法：

- 哈希

哈希函数是单向函数，密码一旦被哈希函数运算成哈希值，则没人能反推出原始明文密码。使用哈希函数，服务器不再存储明文密码，而是存储密码哈希后的结果。每当需要验证密码时，只需要对外部送入的密码再做一次哈希，比对结果是否和存储的哈希值相同即可。

- 加盐

如果攻击者已经提前计算出了一批哈希值，并据此做出明文和哈希值的映射关系，则攻击者可以根据哈希碰撞来查找原始明文。简单的对密码做哈希无法阻止类似的攻击方式，比如字典攻击、彩虹表攻击。

加盐哈希不仅使用了哈希函数，还附件了一个因素：盐值。盐值是一种随机数据，这个随机数据（特别长）与明文密码一块参与哈希运算，能确保生成的哈希值是唯一的，即使多个用户使用相同的密码，添加唯一的盐值后能确保得到的哈希值仍是唯一的。同时长盐值加大了解密的难度，所以盐值要保持一定的长度，盐值长度应该至少和哈希函数的输出长度一致。

- 慢速

现代的计算机运算速度日新月异，攻击者受益于运算速度的更新，即使攻击方法不变，也能比之前更快的破解出更多的密码，然而密码复杂性和长度不可能一直增加。为了解决这个问题，我们要采用慢速的哈希算法，通过指定必须的哈希次数甚至时长，来减少硬件提升对攻击者的帮助。

- 强加密

如果有更强的安全要求，或者监管合规的要求，以上三种方法可能仍然不能满足安全需求，我们建议使用强加密算法，比如对称加密算法。

对称加密算法需要密钥来加密数据，加密密钥和数据应分开存储，即使数据被人盗取，没有密钥仍旧解不出明文。加密密钥应采用专用密码设备存储，专用密码设备提供高安全防护，具备运算速度快、非法操作密钥自动销毁等功能，密钥甚至无法导出，保证了密钥的安全，从而保证了数据的安全。

使用哈希保护密码时要选择正确的密码哈希函数，标准的哈希函数追求的是快速度，每秒可以进行几百万次运算，同时攻击者也可以每秒猜测几百万次密码。这些算法不是好的选择，因为速度慢的算法才能让攻击者更难破解数据。

下面列出的哈希函数专门用于加密密码，他们综合了上述所列方法在设计上专门放慢速度，让人更难破解：

- PBKDF2

PBKDF2 是 Password-Based Key Derivation Function 2 的简称，它在输入（密码）上应用一个伪随机函数（例如哈希，暗码或 HMAC），此外还会加盐。这个过程会重复多次，得出一个密钥。

- Bcrypt

Bcrypt 基于 Blowfish 算法的密钥导出函数，在保护密钥的过程中会加盐，而且具有适应能力。随着时间的推移，可以增加迭代次数，不断放慢速度，抵抗暴力攻击。

- Scrypt

Scrypt 是一个密钥导出函数，专门用于抵御大型硬件攻击，因为它需要大量内存，从而放慢了计算的速度。

最后需要指出，在中国境内应该使用国家密码管理局批准的算法。上述有些算法基于标准哈希函数，比如 PBKDF2，运算时需要传入标准哈希函数名称，默认使用 SHA 系列算法。如有条件，在中国境内应使用 SM3 算法。

3.5.4.3 密码加密存储方式

密码需要加密后再存储，直接存储明文密码会将系统暴露在巨大的风险中。用户信息的存储方式有多种，有些存储方式本身具备密码加密的能力，应用程序可以直接使用；另外一些存储方式对所有数据一视同仁，需要应用程序自行加密后再做存储。

3.5.4.3.1 LDAP 存储

密码通常存储在 LDAP 的 userPassword 属性中，userPassword 属性允许具有多个值，并且每个值都可以不同的形式存储。在身份验证过程中，LDAP 将遍历这些值，直到找到与提供的密码匹配的值，或者直到用完要检查的值为止。

LDAP 支持多种加密存储方案，供管理员选择。存储方案作为值的前缀存储，因此使用 Salted SHA1（SSHA）方案的哈希密码如下所示：

userPassword：{SSHA} DkMTwBl+a/3DQTxCYEApdUtNXGgdUac3

LDAP 支持的加密存储方案如下：

- SSHA password storage scheme

这是 SHA 算法的加盐版本，它被认为是 LDAP 支持的最安全的密码存储方案。例如下面所列密码，这些值表示相同的密码：

userPassword：{SSHA} DkMTwBl+a/3DQTxCYEApdUtNXGgdUac3

userPassword：{SSHA} d0Q0626PSH9VUld7yWpR0k6BlpQmtczb

- CRYPT password storage scheme

此方案使用操作系统的 crypt 哈希函数。它通常会产生传统的 Unix 风格的 13 个字符的哈希，但是在具有 glibc2 的系统上，它还可以生成更安全的 34 字节 MD5 哈希。

userPassword：{CRYPT} aUihad99hmev6

userPassword：{CRYPT} 1czBJdDqS$TmkzUAb836oMxg/BmIwN.1

CRYPT 方案的优点是，可以在不知道明文形式的情况下，将密码与现有的 Unix 密码文件进行传输。两种形式的隐窝都包含盐，因此它们对字典攻击具有一定的抵抗力。

- MD5 password storage scheme

  此方案仅采用密码的 MD5 哈希并将其以 base64 编码形式存储。

  userPassword：{MD5} Xr4ilOzQ4PCOq3aQ0qbuaQ ==

  尽管比明文存储更安全，但这不是一个非常安全的方案。MD5 算法速度很快，并且由于不添加盐，因此该方案容易受到字典攻击。

- SMD5 password storage scheme

  通过添加盐对基本的 MD5 方案进行了改进。例如，这两个值代表相同的密码：

  userPassword：{SMD5} 4QWGWZpj9GCmfuqEvm8HtZhZS6E=

  userPassword：{SMD5} g2/J/7D5EO6+oPdklp5p8YtNFk4=

  SHA password storage scheme

  像 MD5 方案一样，这只是通过 SHA 哈希过程来提供密码。SHA 被认为比 MD5 更安全，但是缺少盐会使该方案容易受到字典攻击。

  userPassword：{SHA} 5en6G6MezRroT3XKqkdPOmY / BfQ =

- SASL password storage scheme

  这其实不是一个真正的密码存储方案，它使用 userPassword 属性的值将密码验证委派给另一个进程进行验证。

  LDAP 可以使用 Cyrus SASL 支持的任何后端服务器来检查密码，选择范围非常广泛，可以使用本地文件，Kerberos，IMAP 服务器，另一个 LDAP 服务器或 PAM 机制支持的任何东西。

3.5.4.3.2 数据库存储

数据库对所有数据一视同仁，密码如果不做处理，直接将密码明文存储到数据库中是十分危险的。由于数据库本身不会对任何数据进行特殊处理，所以要求应用程序在将密码存进数据库前要先做加密处理。

对密码的加密可以采用加盐哈希算法，并结合特定的循环次数或时间限制，以抵消哈希的高速运算性能。应用程序应使用专门用于加密密码的算法，比如 PBKDF2、bcrypt、scrypt，这些算法在设计上故意放慢速度，让人更难以破解数据。不推荐使用标准哈希算法，比如 SHA 系列算法、MD5 算法，这些算法追求的是快速度，加密快然而解密也快，攻击者提升硬件条件可以有效的改善攻击效率。

盐值应该和密码的哈希值一起存储在数据库中，以便在验证密码时能够被应用程序获取。盐值对每个用户应该是不同的，并且是随机生成的。盐值长度应该至少和哈希函数的输出长度一致。盐值无需混淆或者再加密，但是仍然不能让任何人像用户名一样轻易获取到。

3.5.4.3.3 其他存储方式

密码一般与用户信息采用相同的存储方式，用户信息除了可以存储在 LDAP、数据库中之外，还有区块链存储、多媒体文件存储等存储方式。对于这些存储方式的密码存储，也应当与数据库存储类似，在存储前先做加密处理，再将加密后的哈希值与盐值存储下来。

3.5.5 用户其他凭证存储

LDAP 服务器必须支持允许属性存储证书的对象类。 特别是，您需要在 LDAP 服务器中存储证书颁发机构证书，证书撤销列表，证书撤销列表和最终用户证书。

CertificationAuthority 对象类实现了 AuthorityRevocationList，certificateRevocationList 和 cACertificate 属性。

inetOrgPerson 对象类支持 usercertificate（二进制）属性。

可以使用混合对象类 strongAuthenticationUser 将证书添加到非 inetOrgPerson 条目。

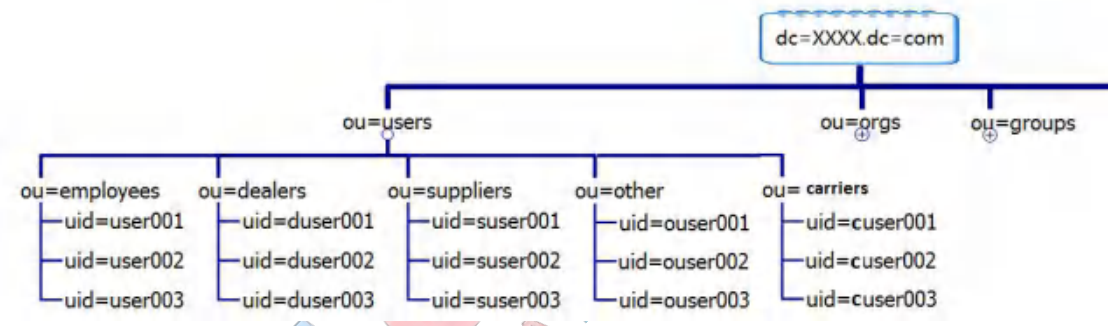
可以在 OpenLDAP 中包括必需的架构，包括以下架构到 slapd.conf 文件中。

FIDO、IFAA、TUSI 的共同特点是硬件隔离配合高强度的密码学算法来实现身份认证，实现轻量级、通用化、优良的用户体验。其核心思路是在终端侧通过 TEE 或 SE 实现硬件隔离用于实现密钥存储和密码算法运算，避免开放系统上的软件病毒、木马的攻击，在此基础上通过密码学算法为云端应用服务商和用户之间建立一套端到端的安全认证协议，这是业界公认的端到端可信安全技术框架。

3.5.6 其他实体存储说明

组织和角色在 LDAP 中的存储可以按照以下目录树来进行设计：

ou=employees 子树下，放置内部员工的信息

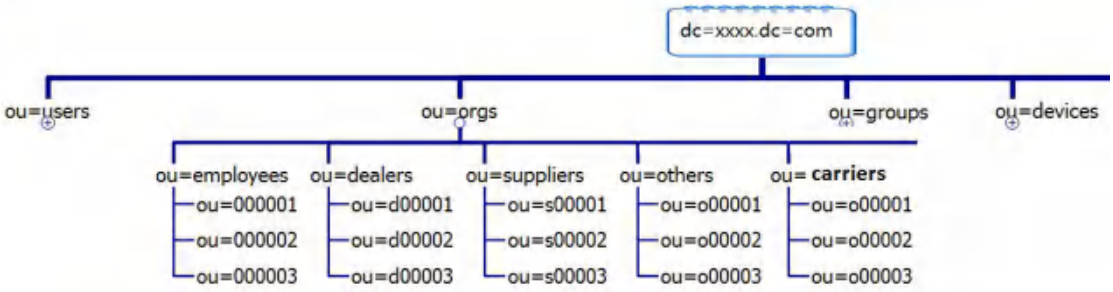


ou=dealers 子树下，放置经销商的信息

ou=suppliers 子树下，放置供应商的信息

ou=other 子树下，放置其他类型的用户信息

ou=carriers 子树下，放置承运商的信息



ou=employees 子树下，放置企业内部的组织信息

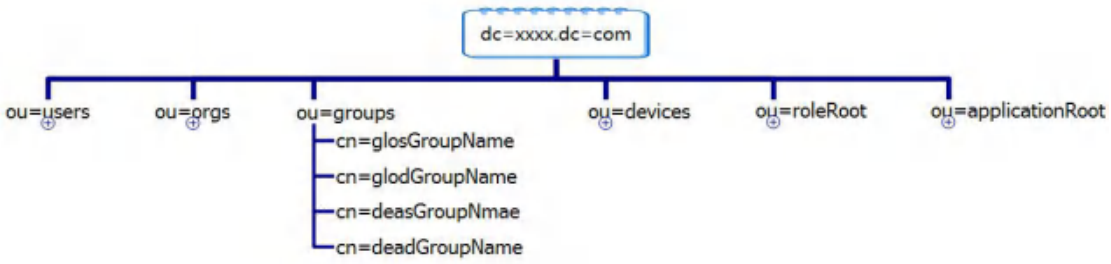
ou=dealers 子树下，放置经销商组织信息

ou=suppliers 子树下，放置供应商组织信息

ou=other 子树下，放置其他类型的组织信息

ou=carriers 子树下，放置承运商组织信息

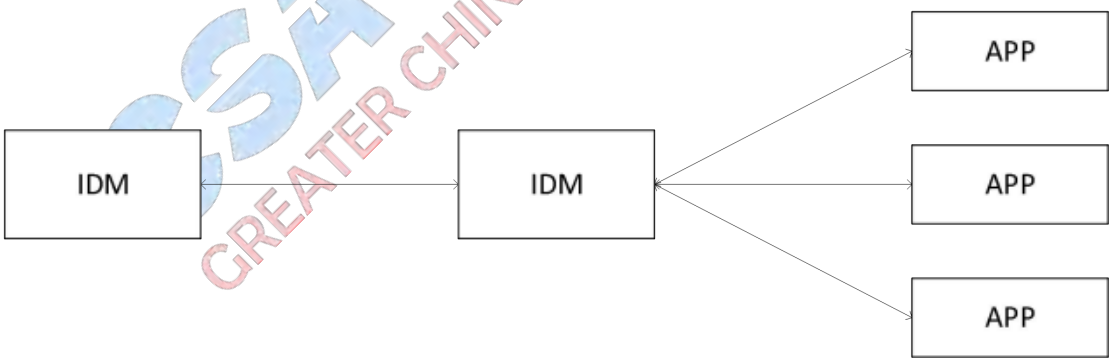
在 ou=groups 下存储所有组信息，包括内部员工组、经销商、供应商等，不同类型的组都存储在该节点下，如下图：



3.6用户的同步和回收能力

3.6.1 身份同步说明

在混合云的架构下，企业同时使用多个云，每个云都会有身份管理系统，身份管理系统之间、身份管理系统和应用系统之间需要进行身份同步，如下图：



系统之间身份同步需要充分考虑身份数据的隐私保护，具备数据访问控制和数据脱敏能力。数据同步可以采用多种同步方案：数据库同步、目录服务器同步、API 接口同步（分为推和拉）。

数据库同步：一般用于 IAM 为应用提供身份数据查询服务，IDM 开放身份相关的表，为应用系统提供数据库只读帐号，应用系统通过数据库查询接口查询身份信息。

目录服务器同步：一般用于 IDM 为应用提供身份数据查询服务，IDM 将身份信息

发布到 LDAP，应用系统从 LDAP 上查询身份信息。

API 接口同步：同时适用于身份管理系统之间、身份管理系统和应用系统之间的身份同步，相互之间通过 REST API 调用实现身份信息同步，如 SCIM 中定义的资源操作接口。在云化应用中，建议应用系统不要存储具体的身份信息，减少身份信息泄露的风险。

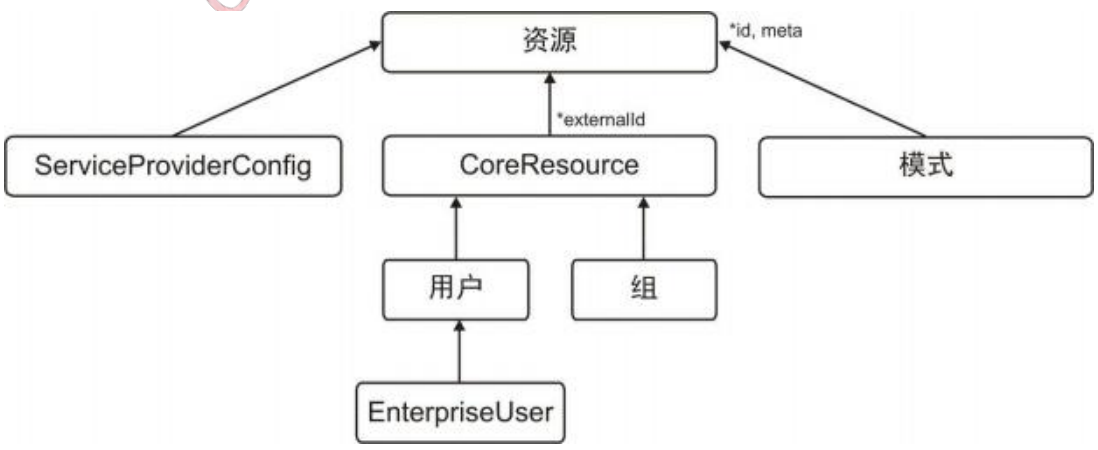
3.6.2 SCIM 协议介绍

跨域身份管理协议(SCIM) 是 IETF 制定一种用户和组管理的标准，目前共有 3 个版本，1.0 版本发布与 2011.12 月份，1.1 版本发布于 2012.7 月，当前最新的 2.0 版本，发布于 2015.9 月，内容详见 RFC7642, RFC7643 and RFC7644。

SCIM 适用于多租户的云应用身份管理，通过提供一个通用的用户模型和扩展模型，基于模型定义标准化的用户信息交换协议，从而降低用户管理操作的成本和复杂性。

SCIM2.0 建立在一个对象模型上，Resource 是顶级对象，所有其它 SCIM 对象都继承 Resource，Resource 具有 id、externalId 和 meta 属性。RFC7643 定义了扩展公共属性的 User、Group 和 EnterpriseUser。

其它对象都从其派生的对象模型构建，SCIM 当前具有三个直接从资源对象继承的对象，ServiceProviderConfiguration 和 Schema 用于发现且不包含任何用户信任，CoreResource 对象包含其两个子资源“用户”和“组”内的用户和组数据。



SCIM 对象模型

对资源的操作，SCIM 定义了一套 REST API，包含丰富但简单的操作集，支持从修改特定用户的特定属性到进行批量更新的所有内容：

1. 创建（create）： POST https://example.com/{v}/{resource}
2. 读取 (read)： GET https://example.com/{v}/{resource}/{id}
3. 替换 (replace)： PUT https://example.com/{v}/{resource}/{id}
4. 删除 (delete)：DELETE https://example.com/{v}/{resource}/{id}
5. 更新 (update)： PATCH https://example.com/{v}/{resource}/{id}
6. 搜索 (search)：GET https://example.com/{v}/{resource}？filter = {attribute} {op} {value} ＆sortBy = {attributeName}＆sortOrder = {ascending | downcending}
7. 批量（bulk）： POST https://example.com/{v}/Bulk

3.6.3 流程自动化介绍（含常规工作流说明）

（1）用户分发

- 管理员在 IDM 中制定最小化的分发策略，包括分发的范围、分发的属性等；
- 在 IDM 系统中新增机构、用户及用户组等信息；
- 新增数据经过审批生效后，按照分发策略将用户信息分发给应用系统；
- 应用系统收到用户信息后，开通帐号，并初始化权限。

（2）用户更新

- 在 IDM 系统中更新机构、用户及用户组信息；
- 更新数据经过审批生效后，按照分发策略将用户信息分发给应用系统；
- 应用系统收到更新信息后，对本地的身份信息进行更新。

（3）用户回收

- 在 IDM 系统中发起用户回收请求；
- 回收请求审批通过后，给应用系统发送回收消息。
- 应用系统收到消息后，进行用户回收响应。

3.7密码管理

身份管理平台提供了密码安全策略，所有的应用系统都需要满足该密码策略。同时也可以按照应用系统的安全等级定义不同强度密码策略，并屏蔽各应用系统的密码管理，由统一身份安全管理平台负责密码的增、删、改；在密码进行同步过程中要提供加密策略保证密码在传输过程中的安全。

3.7.1 密码管理策略

在身份管理平台中，典型的密码管理策略如下：

- 支持诸多认证机制，其中对静态口令需统一管理，在统一身份安全管理平台用户身份集中管理过程中需要强制实施口令策略，并支持灵活的口令策略设置、生存周期的设定。
- 支持用户密码修改、忘记密码处理、密码安全策略配置的管理。

3.7.2 密码修改、找回、重置

作为一个身份管理平台，一个重要的功能就是进行集中的密码策略管理。对于由集中用户身份管理系统来管理的帐户资源，在身份管理平台中都可以根据企业的安全策略来统一设定相应的密码策略。根据客户的企业信息安全策略，可在身份管理平台中设置相应的密码策略，例如：

- 至少 8 位长度；
- 至少包含 1 个字母，1 个数字；
- 密码不能和前 2 次相同；

同时，在密码修改页面上的显著位置提示用户密码的规则；

在使用了身份管理平台后，用户只需要记住自己在集中用户身份管理系统的用户口令，由于只需要记住一个用户名和口令，用户一般会选择使用更复杂一些的密码，从而能够提高密码的安全性。

当用户设置密码安全问题后，可以通过回答密码安全问题来重设密码，系统将自动重置用户的密码，并将新的随机密码发送到用户邮箱或者手机。密码挑战问题可由企业统一制定，也可以由用户自行设置，问题的数目也可以灵活设定。

3.7.3 密码安全管理说明

密码管理流程如下：

- 用户将在身份管理平台自助服务上修改密码，或通过安全认证服务器修改密码；
- 密码将从身份管理平台同步到所有的应用；
- 用户通过 AD 域或 Exchange OWA 中修改密码，通过 AD 密码反向同步插件同步到身份管理平台中进行统一密码修改；

3.8特权账号管理说明

根据 Verizon 的 2019 年数据泄露调查报告，在 2017 年确认的 2,216 个数据泄露事件中，201 个是由于特权滥用造成的。这样的统计数据深刻的提醒我们，不仅要保护特权帐户，还应关注与特权账号活动相关的会话的记录与管控，时刻保持警惕，防止异常访问。

3.8.1 特权访问管理和特权账户

特权账号是访问 IT 资产身份凭据，具有数据可见性和和信息系统控制权，掌握账号的人也就控制着 IT 资产。信息安全风险可以来自各方，心怀不轨的外包人员、粗心或有意为之的内部人员、带有经济甚至政治目的的黑客等，而他们往往只需找到特权账号凭证，就可以肆意窃取核心敏感数据，造成不可挽回的损失。因此，特权账号的保护是防止数据泄露和系统安全的最后一道防线，尽管业内权威一再提醒管理特权账户的重要性，许多特权帐户仍然未受到保护、不被重视或管理不善，使它们成为容易被攻击的目标。

在管理公司的特权账户时，首选是基于特权访问管理（PAM）。在 2019 年 6 月的 Gartner 安全和风险管理峰会上，首席信息安全官（CISO）应该关注的十大安全项目再次表明，特权访问管理（PAM）是其中最重要的。PAM 通过完全自动化定期扫描、检测新账户，并登记管理的应用程序，实施 PAM（特权访问管理）最佳战略。PAM 战略涵盖针对关键资产的特权访问控制（该内容也应涵盖针对身份及访问的管理计划），这是

保护机构数据安全的最好办法之一。

为了保护特权账户和支持访问的重要资源，需要制定好全面的控制措施，以便保护、监控、检测和响应所有特权账户活动。实施 PAM（特权访问管理）最佳战略，定期扫描网络、检测新账户，并进行登记管理。同时关注安全界随着企业发展的延伸，对安全管理战略要求的变化，时刻谨记网络犯罪与我们并不遥远。

3.8.2 特权访问管理实施步骤

1、建立特权账号台账，并对其进行集中化追踪

通过针对公司内部、外部网络上的全部关键资产、关联账户以及关联凭证进行有效的发现。随着公司发展的壮大、基础架构的扩展，IT 团队搜索发现资产信息，应对特权账户的增多情况，对其进行持续的跟踪管理。提供统一、集中的特权账号管理方案，满足企业内部对特权账号管理的需求。

特权账户管理支持自动发现类型，包括不限于主机设备、网络设备、数据库、中间件、文件服务、云资产等等。具备持续跟踪管理能力，能够自动化定期扫描和检测新账户，及时感知资产特权账号变化，并报表方式通知管理员。

2、安全集中存储特权账户凭证

特权账号类型是多种多样的，例如操作系统账号、数据库账号、中间件管理账号、网络设备管理账号、编程 APPID、云平台 Accesskey 等等，凭证也分为密码、SSH 密钥、证书、Access Key Secret、API 密钥等类型。

管理上摒弃过去那种本地化、单独分散式的管理方式，特别要避免员工单独掌握，明文记录、共享使用特权账号凭证。这种作法有面临大额风险，也会带来一系列问题，例如密码长期不更新、容易被窃取、账号活动无法跟踪。正确作法是，将所有特权帐户和凭证存储在一个集中的存储库中，采用安全可信加密算法存储凭证。同时，根据密码保护和等级保护要求，根据密码生命周期和强度策略对密码等凭证定期更换。

3、遵循最小特权原则

特权账号管理应遵循最小特权原则，所谓最小特权(Least Privilege)，指的是"在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权"。最小特权原则，则是指"应限定网络中每个主体所必须的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小"。

需要对用户的特权访问进行有效的管理与控制。正如高级网络安全中心（ACSC）所述，“根据用户职责限制其对操作系统和应用程序的管理权限。” 对于 PAM 管理员来讲，需要明确划分各 IT 成员的角色，使该角色仅具有其所需的最低访问权限。通过即时(JIT)特权访问的不同方法，以最好地平衡更改组织实践的预期努力与安全、风险和运营结果之间的关系，大幅减少以消除“常设”特权访问，确保有充分有效理由时给予访问特权，减小特权账号攻击面。

针对特定任务的临时性访问需求，特权账号管理产品应提供限时访问控制措施，例如审批临时特权申请和撤销，凭证回收更换等等。

4、特权会话管控

特权访问会话是基于任务驱动，确保会话访问有合理理由，并在允许访问时段给予最低访问权限。

特权会话的凭证应采用安全共享方式，例如通过一次性会话密钥替代账号凭证出现在客户端工具中，由特权账号管理系统实现单点登录到资产，降低特权账号凭证泄露的风险。另一方面对会话用户采用多重认证方式，确保用户身份真实性。

特权会话应支持本地、WEB 终端和远程工具等多种运维方式，支持常用运维协议审计，例如 SSH/TELNET/RDP/VNC/FTP/SFTP 等，提供会话实时监控和管控能力，跟踪和防止特权访问滥用。

5. 临时访问的控制实施

建立这样一个策略：当用户需要账户凭证访问某个远程资产时，强制要求他们给公司的 PAM 管理员发送访问申请。为增强安全控制，PAM 管理员将只为用户提供临时访问凭据的权限，同时可通过设置访问时间、在规定的访问时间到期时能够撤销访问权限并强制消除密码。进一步，PAM 管理工具还应可以在用户消除密码后自动重置密码。

6. 审计

全面的审计记录、实时警报和通知确实让工作变得更轻松，这些过程不仅记录了每个用户的操作，同时也实现了针对所有与 PAM 管理相关责任的明确及透明性。通过与内部事件管理工具的集成，将 PAM 活动事件与公司其它事件进行整合分析，智能识别异常并提供通知。这为综合事件分析，以及检测漏洞将提供了极大的帮助。

3.8.3 特权管理需特别关注问题

1 消除应用内嵌特权凭证

许多应用程序需要频繁访问数据库和其它应用程序，以实现数据存储和业务交互。通常通过在应用程序中嵌入带有明文凭据的配置文件或脚本的方式。而这种作法的风险是显而易见的，为不怀好意的黑客们提供了便捷的入侵途径。为解决该问题，即当应用程序需要使用其它应用程序或远程资产的特权帐户时，利用安全 API 直接查询特权账号凭证。解决在应用中普遍存在硬编码或配置中写死账号、密码等敏感配置信息的问题。填补应用、脚本、服务等非“人”使用特权账号安全审计的空白。T 团队可以利用安全 API，即当应用程序需要使用其它应用程序或远程资产的特权帐户时，利用安全 API 直接查询 PAM 工具。

2. 严格的自动密码重置

对于 IT 团队的管理而言，每个特权账户都使用同一个密码，能够使工作相对轻松容易许多，但是，这种方法却及其危险，会导致整个网络环境出现高危漏洞。想要安全管理特权账户，需要使用一个超强、独一无二的定期重置密码策略。为了消除固定密码以及未授权访问带来的安全隐患，需要将密码自动重置视为 PAM 策略中不可分割的一部分。

3. 针对弱权限用户，设定多重身份验证（针对员工及第三方人员）

根据 Symantec 的 2016 年互联网安全威胁报告，通过使用多重身份验证的方法，可以有效避免高达 80%的漏洞。在实际使用中，特权账户密码经常会由于各种安全管理漏洞会释放给普通员工和第三方人员，对于 PAM 管理员和用户而言，采用多因素身份鉴别，实施双重或多重身份验证可以保证敏感数据的访问安全。

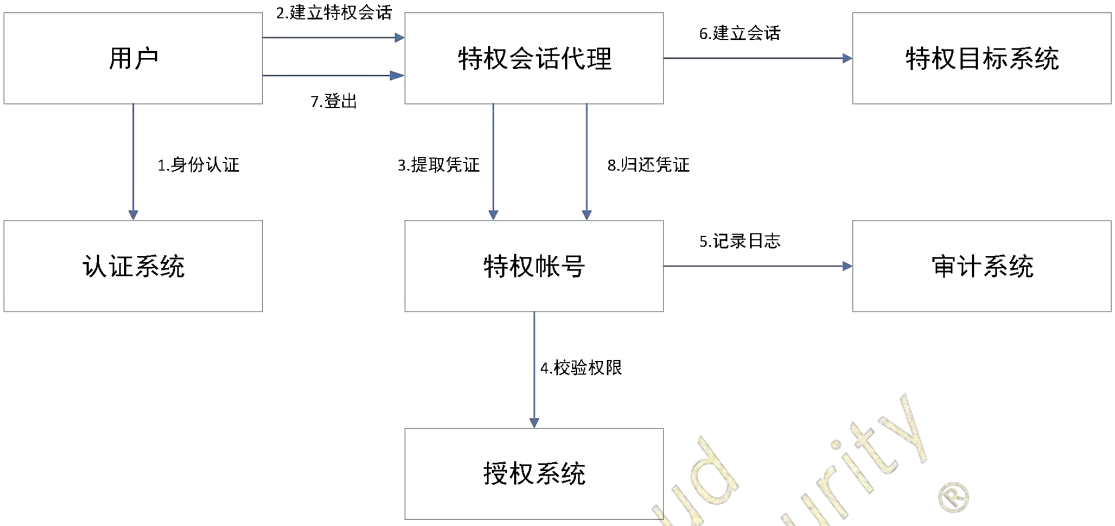
4、满足合规性要求

企业在满足内控管理需求外，还需要符合国家在等级保护和密码保护以及其他 PCI DSS, FISMA, NERC-CIP, SOX, 和 HIPAA 或行业规范的合规性要求。特权账号产品需要实现以下两点：

1) 完整记录特权访问信息。审计内容同时包含用户信息，时间戳和 IP 地址等一系列完整的特权会话相关内容

2) 回放存档会话录像，溯源用户操作。管理员可以通过回放来查看会话内容，以便在安全事件发生进行责任认定。

3.8.4 特权账户管理流程



流程说明：

1) 用户通过认证系统实现用户身份认证；
2) 用户通过权限会话代理（如堡垒机）向特权目标系统发起特权会话建立申请；
3) 代理向特权帐号系统申请特权凭证，申请中包含身份凭证、位置、时段等上下文信息；
4) 特权帐号系统向授权系统发起权限校验；
5) 权限系统根据身份凭证、位置、时间段等上下文信息进行权限验证，验证通过后给代理返回特权凭证，并记录日志；
6) 代理用凭证和目标系统建立会话，执行操作；
7) 操作完成后，登出目标系统；
8) 特权会话代理想归还特权凭证给特权帐号系统，并记录日志。

3.9身份管理的其他业务特征

3.9.1 多维组织

多维制组织结构是指由事业部、职能机构、地区等多种因素组成的一种大企业的管理组织结构模式。这种组织结构表现为一种立体形状的结构。在实际企业应用中，多以矩阵组织形式实现。

在多维组织下，单个用户具有多个身份，不同的身份对应不维度的组织、岗位、权

限。而在身份认证体系上，需要支持对一人多身份体系的管理。

3.9.2 一人多身份体系

在多维组织下，用户会具有 2 个以上的身份，而在 IAM 认证体系下，则需要为一个用户映射多种身份，执行不同的身份认证策略。并且不同的身份策略独立，相互隔离，不应存在身份合集。例如：企业某用户在不同的组织兼任职务，两个职务的身份不同，则用户需要不同的两种身份认证策略。

而 IAM 对于多身份体系的支持，已经成为产品设计、系统实施过程中的基础功能。

3.9.3 用户锁定与解锁

IAM 系统还应具备用户认证锁定与解锁的功能。用户锁定即在不删除用户认证信息下对用户认证进行临时冻结的操作，在锁定冻结状态下，一般会终止该用户所有认证权限，或仅保留基础权限。

实际应用场景中一般为手动操作锁定或安全策略出发锁定：

后台配置手动锁定

用户认证时触发安全策略锁定（密码错误超限、异地登录等）

风险控制模块侦测用户认证行为异常触发锁定

用户锁定只是对认证的临时冻结，在策略改变或风险消除后，还应对账号给予解锁。

（编号 1--于继万）信任的概念及信任模型及管理

4 登录认证

4.1 身份信任的概念及模型

1、身份信任的广义理解

数字认证是解决物理身份世界通向数字身份世界建立数字信任体系的基础手段，信任体系是网络空间安全的基础，信任体系治理的水平关乎个人、企业、社会数字化发展的成败，那什么是数字信任呢?

IDC 认为数字信任就是指可以在多个主体身份间的决策中反应其对彼此的信任程度。数字信任的发展包括 4 个阶段，即内部 IT 风险、共享 IT 资源风险、数字活动声誉、组织的声誉。而我们经常提到的，通常是指第一、第二个阶段，即企业在 IT 建设之初就要加强内部 IT 安全建设，伴随业务发展，IT 系统和外部机构有横向数据共享时，则要同时关注共享 IT 资源风险的安全，例如 API 的安全。事实上企业发展要一定规模，将会更为关注第三、第四个阶段，信任治理是一项重要的长期建设工作。

数字信任怎么度量？

评价某一主体的信任大小，包括 5 个关键要素，风险、安全、合规、伦理和社会责任、隐私。信任是相对的，因此我们在讨论信任的大小往往与主体所在的组织也就是信任域相关，在数字世界里，如果信任域理解错位就会产生安全风险，比如日益猖獗的电话诈骗，以及仿冒和中间人攻击都是因为信任错位导致。

2、在数字世界中信任是如何建立、传递和管理的

在数字世界中，信任是通过一定鉴别技术实现的，对某个企业主体的信任是依据组织的安全策略、服务的安全表现以及社会的伦理责任一起评判的，信任是动态的非静态的。因此对主体的信任管理必须有一个生命周期的视角。

信任的建立通常有两种方式，一种是集中式，存在一个可信根，这是信任的起点，然后通过可信根传递信任也就是构建信任链，一般通过密码算法（比如数字签名）保证传递过程中信任是不可改变的且经过相关实体背书的；另外一中是点对点方式，类似人之间的社交，通过 P2P 方式建立彼此的信任网。

当前基于可信根构建集中信任关系的案例有 PKI 体系和可信计算体系，在 PKI 体系中，信任链是依赖 CA 建立起来的，同一 CA 签发的证书所代表的身份互相信任，不同 CA 靠签署交叉信任链证书得以让信任在不同域传递。在可信计算体系中，信任根的可信性由物理安全、技术安全和管理安全共同确保，从信任根开始到软硬件平台、到操作系统、再到应用，一级度量认证一级、一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。我们说集中式信任体系需要一个可信根作为第三方信任的基础，但是并不是说集中式信任一定基于公钥体系才能建立，对称加密也是可以建立的，比如 kerberos 分布式认证机制就是完全基于对称加密采用两两预共享密钥的方式建立起来的。

基于点对点的信任关系建立，也就是信任网的建立，典型例子就是 PGP 信任网，

主要使用在邮件系统中，不同个体对其信任关系做签名声明，主体通过验证签名并计算对不同客体公钥的信任度来综合确定是否信任该邮件（就是该个体发送的），这种点对点的信任关系比较贴近个体的数字社会场景，未来在区块链中也大有可为。

身份信任按照主体客体及使用的场景差异可以分为设备信任、用户信任、应用信任、网络（流量）信任等，不同的信任类型需要的鉴别和传递技术也有差异，本章后面章节会展开详述。

4.2 认证类型及 MFA

4.2.1 相关定义

根据【ISO 19092:2008，定义 4.42】、【ISO/IEC 27040:2015，定义 3.27】使用以下两个或多个因素的鉴别：

— 知识因素，“个人知道的”；

— 拥有因素，“个人持有的”；

— 生物因素，“个人是什么或能够做什么的”。

【释义】

MFA 又被翻译为多因子认证、多因素验证、多因素认证，是一种计算机访问控制的方法，用户要通过两种以上的认证因素鉴别机制之后，才能得到授权，使用计算机资源。身份鉴别的实现原理就是把访问实体所提供的信息与某些保存下来的可以代表其身份的信息进行对比，以达到鉴别的目的。根据鉴别信息的不同，身份鉴别有多重方式：

（1） 知识因素：基于实体所知，验证实体已知什么，如口令、密码、PIN 码或通信短语（password）；

（2） 拥有因素：基于实体所有，验证实体拥有什么，如身份证、钥匙、智能卡、通信证、令牌等；

（3） 生物因素：基于实体特征，验证实体不可改变的特性，如指纹、声音、视网膜等生物学测定得来的标识特征；

通常认为，高风险业务应组合两类，或两类以上的要素进行身份鉴别，应确保采用的要素相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或泄露。

4.2.2 应用场景

1) 等级保护

2) 在《GBT22239-2019 信息安全技术网络安全等级保护基本要求》中，在通用要求部分，对于安全计算环境身份鉴别要求在第三级和第四级都明确提出：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

3) 可以采用多因素鉴别手段实现，将知识因素项限定为密码认证项，然后搭配其他因素项组成身份鉴别方案。

4) 零信任

5) 零信任安全架构并不要求在认证手段上必须在各种场景下都一视同仁的采用强身份鉴别的手段，而是同时支持可选的多种身份鉴别手段，并且将认证手段的强弱作为一个信任度量因子。认证手段的强弱直接影响主体的信任度，影响后续的访问控制判定。比如，终端具备 TPM、使用了人脸识别可以得到一个较高的信任评分，反之，用户如果只使用了用户名口令进行登录，那只能得到一个较低的信任评分，信任评分太低将禁止访问某些安全等级高的业务（可以提示用户进行二次认证，通过后允许访问）。

6) 在零信任安全架构实施中，一次性的用户认证机制无法确保用户身份的持续合法，即便是采用了强度较高的多因子认证手段，也需要通过持续认证手段进行信任评估。即多因素认证认证手段的叠加使用。

7) 特权账户管理

8) 因为可以访问公司最核心的信息，特权账户往往成为攻击者竞相追逐的目标，公司企业必须安全有效地管理特权访问。多因素身份验证可以确保只有正确的人能够访问关键数据的必要方法。这种方法还可以缓解恶意内部人“借用”同事密码的风险，防止内部人威胁。是特权账户管理常用的手段之一。

9) 为避免造成使用麻烦，只在必要的时间和位置实现 MFA 功能。通过定义哪些终端和资产需要受到最严格的保护，特权用户如果以共享账户登录系统，还需额外提供个人凭证，以便确认该特定会话是由该特定用户发起的。

10) 金融行业等高安全应用场景

11) 明确采用多因素认证的行业主要包括金融等高安全应用场景。金融行业标

准 JR/T 0068-2020《网上银行系统信息安全通用规范》明确指出：“高风险业务应组合选用下列要素对交易进行验证：一是客户知悉的要素，例如，静态密码等；二是仅客户本人持有并特有的，不可复制或者不可重复的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；三是客户本人生物特征要素，例如，指纹、虹膜等。应确保采用的要素相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或泄露。”

4.2.2.1 存在问题

1) 错误使用具有关联性的多种身份鉴别手段

2) 容易造成多因素身份鉴别使用错误的情况主要是两类：一是简单选取身份鉴别方式，未能分布到不同类别中；另一种是选取的身份鉴别方式之间有关联性，例如采用智能卡生成的密码，一旦智能卡出现系统性风险，则密码也不攻自破。

3) 多因素身份鉴别实施成本提升

4) 一般而言，多因素解决方案需要额外的投资来实施维护和维护成本。例如，大多数基于硬件令牌的系统都是专有的，由供应商每年收取年费，提升了用户的使用额外成本。而软件证书作为密码设施，其部署成本也是不容忽视的。

5) 无法防御某些攻击手段

6) 多因素认证可以大大减少在线身份盗窃和其他在线欺诈的发生率，攻击者不能再像单一认证手段被攻破以后那样，通过掌握密码永久访问受害者信息。然而，多因素认证方法仍然容易受到网络钓鱼，和中间人攻击。目前可证实多隐私身份鉴别对例如网络钓鱼和恶意软件等现代威胁无效。

4.2.3 认证方式介绍

（参考 1.2 的分类，继续展开每一类认证方式的介绍，适应的场景（比如人机、机机等等）包含优缺点）

4.2.3.1 口令认证

基于口令的认证方式是较常用的一种技术。在注册阶段，用户首先在系统中注册自

己的用户名和登录口令。系统将用户名和口令存储在内部数据库中，口令一般是长期有效的，因此也称为静态口令。当用户登录时，会将用户名及口令一同传递给后台进行验证匹配，验证通过既颁发登录令牌。静态口令的应用案例随处可见，如本地登录 Windows 系统、网上博客、即时通信软件等。

基于口令认证技术的优点是简单易用，缺点是安全性较低；存在窃听（HTTP,SMTP,TELNET 等应用层协议均采用明文方式传输口令）、重放（采用静态口令易受到重放攻击的威胁）、破解（穷举攻击、字典攻击、社交工程、窥探、垃圾搜索）等风险，已经成为当前身份鉴别方式中最薄弱的一环，尽可能采取其他免密方式代替它。如果确实不具备替换条件，建议增加以下方式提高安全性：

- 口令在存储时，请采用国密标准算法进行加密存储，并加入随机加密种子，确保即使相同的口令，加密后密文也不一样
- 口令验证失败次数超过指定次数后，锁定该账号一段时间，防止暴力破解
- 登录时添加图形验证码、滑块验证等方式，防止暴力破解
- 在提交口令前，需对口令进行加密传输，并通过加入时间戳使加密串仅在一段时间内有效，防止重放攻击
- 加入短信验证、OTP 认证之类的认证方式，组成双因素认证

4.2.3.2 密码认证

基于密码认证技术需要依靠密钥先为用户创建一对密钥，并把公匙放在需要访问的服务器上；客户端软件会向服务器发出请求，请求用用户的密匙进行安全验证；服务器收到请求之后，在该服务器目录下寻找公匙，然后把它和用户发送过来的公匙进行比较。若两密匙一致，服务器就用公匙加密结果并把它发送给客户端软件；客户端软件收到结果之后就可以用私密解密再把它发送给服务器。

4.2.3.3 智能卡认证

智能卡是一种内置集成电路的芯片，芯片中存有与用户身份相关的数据， 智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。

智能卡认证是通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。并且智能卡还存在被克隆的风险，但这点一般取决于智能卡的安全保护机制，它受限于智能卡被保护的对象价值，以及其生产成本的限制。

智能卡自身就是功能齐备的计算机，它有自己的内存和微处理器，该微处理器具备读取和写入能力，允许对智能卡上的数据进行访问和更改。智能卡被包含在一个信用卡大小或者更小的物体里（比如手机中的 SIM 卡就是一种智能卡）。智能卡技术能够提供安全的验证机制来保护持卡人的信息，并且智能卡的复制很难。从安全的角度来看，智能卡提供了在卡片里存储身份认证信息的能力，该信息能够被智能卡读卡器所读取。智能卡读卡器能够连到 PC 上来验证 VPN 连接或验证访问另一个网络系统的用户。

4.2.3.4 数字证书

数字证书的基本架构是公开密钥 PKI，即利用一对密钥实施加密和解密。其中密钥包括私钥和公钥，私钥主要用于签名和解密，由用户自定义，只有用户自己知道；公钥用于签名验证和加密，它可以被公开。数字证书的基本工作原理主要过程是：

第一，发送方在发送信息前，需先与接收方联系，同时利用公钥加密信息，信息在进行传输的过程当中一直是处于密文状态，包括接收方接收后也是加密的，确保了信息传输的单一性，若信息被窃取或截取，也必须利用接收方的私钥才可解读数据，而无法更改数据，这也有利保障信息的完整性和安全性。

第二，数字证书的数据签名类似于加密过程，数据在实施加密后，只有接收方才可打开或更改数据信息，并加上自己的签名后再传输至发送方，而接收方的私钥具唯一性和私密性，这也保证了签名的真实性和可靠性，进而保障信息的安全性。

4.2.3.5 生物特征认证介绍

生物特征认证技术是运用 who you are 方法，通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。使用传感器或者扫描仪来读取生物的特征信息，将读取的信息和用户在

数据库中的特征信息比对，如果一致则通过认证。

生物特征分为身体特征和行为特征两类。1）身体特征包括：声纹(d-ear)、指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和 DNA 等；2）行为特征包括：签名、语音、行走步态等。目前部分学者将视网膜识别、虹膜识别和指纹识别等归为高级生物识别技术；将掌型识别、脸型识别、语音识别和签名识别等归为次级生物识别技术；将血管纹理识别、人体气味识别、 DNA 识别等归为“深奥的”生物识别技术。

生物特征识别的安全隐患在于一旦生物特征信息在数据库存储或网络传输中被盗取，攻击者就可以执行某种身份欺骗攻击，并且攻击对象会涉及到所有使用生物特征信息的设备。

生物特征识别的易用性缺陷则在于，一旦用户的生物特征因为外部因素发生了变化，将无法通过认证，比如由于嗓子发炎导致的声音变化。

4.2.3.6 人脸识别

人脸识别技术是基于人的脸部特征信息进行身份识别的一种生物识别技术。用摄像机或摄像头采集含有人脸的图像或视频流，并自动在图像中检测和跟踪人脸，进而对检测到的人脸进行脸部识别的一系列相关技术，通常也叫做人像识别、面部识别。

人脸识别的优势在于其自然性和。自然性是指该识别方式同人类（甚至其他生物）进行个体识别时所利用的生物特征相同。不被察觉的特点是指识别方法不令人反感，并且因为不容易引起人的注意而不容易被欺骗。

在早期的人脸识别技术中，大多是通过动作引导来识别活体，比如摇头、张嘴等，而现在各厂商提高了其体验度，识别到人脸即可进行验证，不需再进行动作，而活体的验证，则放到后台由算法进行处理，比如进行一些照片的纹理检测等。

4.2.3.7 声纹识别

声纹识别（也称作说话人识别）就是基于语音的一种用于身份认证的生物特征识别技术，它能够让机器从语音中自动识别出说话者的身份。每个人都有独一无二的声纹，这一方面是由于每个人的声学器官在形状、大小上都各不相同，从而声音在音高、 音色等方面会存在差异；另一方面每个人都有自己独特的说话习惯，说话过程中 用词、

韵律、发音模式等也会存在不同。声纹的这种唯一性表明通过语音来识别说话人的身份是可行的。

声纹识别技术，是用电声学一起显示的携带言语信息的声波频谱，是一种通过声音判别说话人身份的技术。在进行声纹识别前，需要先采集用户声纹特征数据，建立声纹模型。当进行声纹认证时，客户端将需要认证的声纹数据传送至服务端认证，服务端将声纹数据与后台已采集的用户声纹数据进行匹配，给出匹配置信度得分，系统根据置信度得分判断用户的身份。

在信贷申请环节，一般需要用户亲自阅读一段固定的文字存在声纹库，并且同时提取其声纹特征。在信审过程中，系统自动将声纹与黑名单库中的声纹做比对，同时也能够跟最最近或者同区域的订单声纹做交叉对比，如果命中黑名单，则可调低信用级别甚至直接拒绝，而通过交叉比对，还能发现重复的联系人信息，提示重大欺诈嫌疑。此外声纹识别技术为公安行业带来以往战法的突破，助力科技强警，为案件侦破过程提供新的线索和证据，通过独特的算法，可在多人对话场景中进行精准的声纹识别，分离出单个说话人音频，并识别出每个人的说话内容，适用于公安动态布控、大型会议记录等应用场景。

4.2.3.8 指纹识别

指纹识别技术是根据人体指纹的纹路、细节特征等信息对操作或被操作者进行身份鉴定，指纹识别技术主要分为：点容式、光学式和超声波式，在通过表层镜面采集到指纹后，对采集的指纹进行质量评估，与指纹库中样本进行对比，最终确定合格信息。通过光学指纹传感器和电容式指纹传感器，进行用户指纹采集；　通过指纹模块进行总体特征和局部特征进行六大特征的提取，经过图像增强、计算方向图、二值化和细化等过程，获得指纹特征信息；将指纹图像转为数字特征，并以文件的格式或其他特定形式存储在上位机中；比较指纹特征点集合和数据库中指纹特征点集合的相似度，用代价函数表示相似程度，取合适门限给出该两组指纹特征是否来自同一枚指头的判断；

指纹识别技术是目前最方便、可靠和便宜的生物识别技术解决方案，在大规模应用方面具有很大的潜力，指纹识别系统几乎可以覆盖所有需要进行身份认证的系统和产品，刑侦领域采用 1:N 模式的指纹数据库检索，金融领域采用银行指纹密码储蓄、指纹密码登录、智能信用卡防伪、银行保管箱等业务的客户身份确认。

4.2.3.9 虹膜识别

虹膜识别技术是利用虹膜终身不变性和差异性的特点来识别身份的，每一个虹膜都包含一个独一无二的基于像冠、水晶体、细丝等特征的结构，虹膜识别系统主要由虹膜图像获取、图像预处理、特征提取、特征匹配、结论等部分组成。

虹膜图像获取使用特定的摄像器材对人的整个眼部进行拍摄；图像预处理对虹膜定位确定内圆、外圆和二次曲线在图像中的位置，虹膜图像归一化将图像中的虹膜大小，调整到识别系统设置的固定尺寸，图像增强针对归一化后的图像，进行亮度、对比度和平滑度等处理，提高图像中虹膜信息的识别率；特征提取采用特定的算法从虹膜图像中提取出虹膜识别所需的特征点，并对其进行编码；特征匹配将特征提取得到的特征编码与数据库中的虹膜图像特征编码逐一匹配，判断是否为相同虹膜，从而达到身份识别的目的。

在司法、公安、军队等系统中，采用基于虹膜识别技术的智能弹枪柜管系统、监狱互锁门禁系统，适用于稳定性高、精准度高的场景，金融领域在人员识别认证、ATM 机识别认证、智能金库门禁系统中发挥着不可替代的作用。

4.2.3.10 指静脉识别

静脉识别技术是一种生物特征识别技术，是利用人体静脉血液中的血红素具有对近红外光吸光的特性，通过静脉识别算法实现对人的身份识别，具有安全可靠、识别精度高等特点。指静脉识别由静脉图像采集、图像预处理、特征提取和编码、模式匹配共 4 个部分组成。

静脉图像采集通过红外线 CCD 摄像头获取手指、手掌、手背静脉的图像，将静脉的数字图像存贮在计算机系统中，实现特征值存储；图像预处理对图像感兴趣区域的提取、图像的尺寸归一化、图像的灰度归一化，得到大小统一、纹理信息清晰的图像；特征提取和编码基于静脉图像纹理结构特征或基于细节点的指静脉提取，包括静脉图像的分割、二值化、细化等操作，最终提出静脉结构特征；模式匹配将待测样本与数据库中特征模板进行对比，通过分类识别器进行静脉图像特征匹配，确认身份认证结果。

在金融领域，静脉识别技术也有一定应用，如银行的门禁系统、取款机、收银台等系统设备中都有运用及尝试，一定程度提升了身份识别的安全级别，也提升了身份识

别的准确度。指静脉识别技术利用静脉血管的纹理进行身份验证，具有操作简单、不易盗取、伪造难等特点。

4.2.3.11 掌静脉识别

掌静脉识别是静脉识别的一种，掌静脉识别通过红外线 CCD 摄像头取得个人掌静脉分布图，从掌静脉分布图依据专用比对算法提取特征值，将静脉的数字图像存贮在计算机系统中，将特征值存储。实时采取静脉图提取特征值，运用先进的滤波、图像二值化、细化手段对数字图像提取特征，同存储在主机中静脉特征值比对，采用复杂的匹配算法对静脉特征进行匹配，从而对个人进行身份鉴定。

手掌静脉生物识别技术可用于监狱管理的方方面面，从而真正帮助监狱实现管理职能化。掌静脉教育考试管理系统可用于防止考生冒名替考现象，杜绝违法作弊的源头，防止监考人员弄虚作假，数据批量处理、高安全、高效率、高精准。掌静脉社保管理系统有效杜绝养老金冒领现象，社会经济效益显著，受到全国社保机构的普遍关注，面向全国的整体方案规划，以期彻底解决冒领等问题，防止财政流失。

OTP 认证

动态口令（OTP，One-Time Password）又称一次性密码，是使用密码技术实现的在客户端和服务器之间通过共享秘密的一种强认证技术，是增强目前静态口令认证的一种非常方便技术手段。 动态口令的基本认证原理是在认证双方共享密钥，也称种子密钥，并使用的同一个种子密钥对某一个事件计数、或时间值、或者是异步挑战数进行密码算法计算，比较双方计算值是否一致进行认证。可以做到一次一个动态口令，使用后作废，口令长度通常为 6-8 个数字，使用方便。

动态口令认证需要解决双方加密对象的同步，同步机制有 3 种：时间型、事件型和挑战与应答型。时间同步原理是基于动态令牌和动态口令验证服务器的时间比对，基于时间同步的令牌，一般每 60 秒产生一个新口令，要求服务器能够十分精确的保持正确的时钟，同时对其令牌的晶振频率有严格的要求，这种技术对应的终端是硬件令牌；事件同步基于事件同步的令牌，其原理是通过某一特定的事件次序及相同的种子值作为输入，通过 HASH 算法中运算出一致的密码；挑战/应答常用于网上业务，在网站/应答上输入服务端下发的挑战码，动态令牌输入该挑战码，通过内置的算法上生成一个 6/8 位的随机数字，口令一次有效，这种技术应用最为普遍，包括刮刮卡、短信密码、动态令

牌也有挑战/应答形式。

4.2.4 认证协议介绍

4.2.4.1 **LDAP**

轻型目录访问协议（Lightweight Directory Access Protocol，简称 LDAP）1是基于 X.500 标准的轻量级目录访问协议，通过 IP 协议提供访问控制和维护分布式信息的目录信息。LDAP 是由互联网工程任务组（The Internet Engineering Task Force，简称 IETF）制定的，该协议常用在单点登录中，例如用户可以在多个服务器上使用同一密码，通常用于公司内部网站的登录中。

LDAP 目录组织方式是一种有层次的、树形结构，是一个为查询、浏览和搜索而优化的数据库，类似于文件目录一样。在树状信息中的基本数据单元是条目，而每个条目由属性构成，属性中存储有属性值。每个条目均有自己的 DN，DN 是该条目在整个树中的唯一名称标识，类似文件系统中带路径的文件名就是 DN。LDAP 目录条目可描述一个层次结构，这个结构可以反映一个政治、地理或者组织的范畴。在原始的 X.500 模型中，反应国家的条目位于树的顶端；接着是州或者民族组织。典型的 LDAP 配置使用 DNS 名称作为树形结构的顶端，下列是代表人、文档、组织单元和其他任何事务的条目。

LDAP 操作在一个客户机/服务器的体系

在 LDAP 中共有四类 10 种操作（如表 x 所示），LDAP 提供扩展操作，不同的 LDAP 厂商可根据自己的需求定义扩展操作。LDAP 中的安全模型主要通过身份认证、安全通道和访问控制来实现。目前主要的产品有 SUNONE Directory Server、IBM Directory Server、Novell Directory Server、Microsoft Active Directory 及 OpenLDAP 等。

[1] Howes, T; Smith, M; Good, G (2003). Understanding and Deploying LDAP Directory Services. Addison-Wesley Professional. ISBN 0-672-32316-8

编号	类别	操作
1	查询类	搜索、比较操作
2	更新类	添加条目、删除条目、修改条目、修改条目名
3	认证类	绑定、解绑定
4	其他类	放弃、扩展操作

4.2.4.2 PAP/CHAP

密码认证协议（Password Authentication Protocol，简称 PAP），是 PPP 协议集中的一种链路控制协议，主要是通过使用 两次握手提供一种对等结点的建立认证的简单方法，这是建立在初始链路确定的基础上的。

完成链路建立阶段之后，对等结点持续重复发送 ID/ 密码给验证者，直至认证得到响应或连接终止。PAP 并不是一种强有效的认证方法，其密码以文本格式在电路上进行发送，对于窃听、重放或重复尝试和错误攻击没有任何保护。因此仅适用于可以使用明文密码模仿登录远程主机的环境。

CHAP 通过三次握手验证被认证方的身份，在初始链路建立时完成，为了提高安全性，在链路建立之后周期性进行验证，目前在企业网的远程接入环境中用的比较常见。

它先由服务器端给客户端发送一个随机码 challenge，客户端根据 challenge 对口令进行加密，然后把这个结果发送给服务器端，服务器端从数据库中取出口令，同样进行加密处理。最后比较加密的结果是否相同。如相同，则认证通过，向客户端发送认可消息。

CHAP 是在网络物理连接后进行连接安全性验证的协议。因此它比 PAP 更加可靠。

4.2.4.3 SAML

安全断言标记语言（Security Assertion Markup Language，简称 SAML）定义了一个

用于交换身份验证和授权的 XML 框架[2]，SAML 是 OASIS 安全服务技术委员会的一个产品，于 2002 年 11 月宣布 SAML V1.0 规范成为一个 OASIS 标准，SAML 2.0 于 2005 年 3 月发布，协议的增强仍在通过附加的可选标准稳步增加。

SAML 规范定义了三个角色：委托人（通常为用户）、身份鉴别提供者（Identity Provider，IDP），服务提供者（Service Provider，SP）。SAML 在单点登录中大有用处，在 SAML 协议中，一旦用户身份被主网站（IDP）认证过后，该用户再去访问其他在主站注册过的应用（SP）时，都可以直接登录，而不用再输入身份和口令。SAML 协议的核心是: IDP 和 SP 通过用户的浏览器的重定向访问来实现交换数据。

在将身份断言发送给服务提供者（SP）之前，身份鉴别提供者也可能向委托人要求一些信息——例如用户名和密码，以验证委托人的身份。SAML 规范了三方之间的断言，尤其是断言身份消息是由身份鉴别提供者传递给服务提供者。在 SAML 中，一个身份鉴别提供者可能提供 SAML 断言给许多服务提供者。同样的，一个服务提供者可以依赖并信任许多独立的身份鉴别提供者的断言。

SAML 没有规定身份提供者的身份验证方法，他们大多使用用户名和密码，但也有其他验证方式，包括采用多重要素验证。诸如轻型目录访问协议 LDAP、RADIUS 和 Active Directory 等目录服务允许用户使用一组用户名和密码登录，这是身份鉴别提供者使用身份验证令牌的一个典型来源。许多流行的互联网社交网络服务也提供身份验证服务，理论上他们也可以支持 SAML 交换。

[2] http://saml.xml.org/saml-specifications

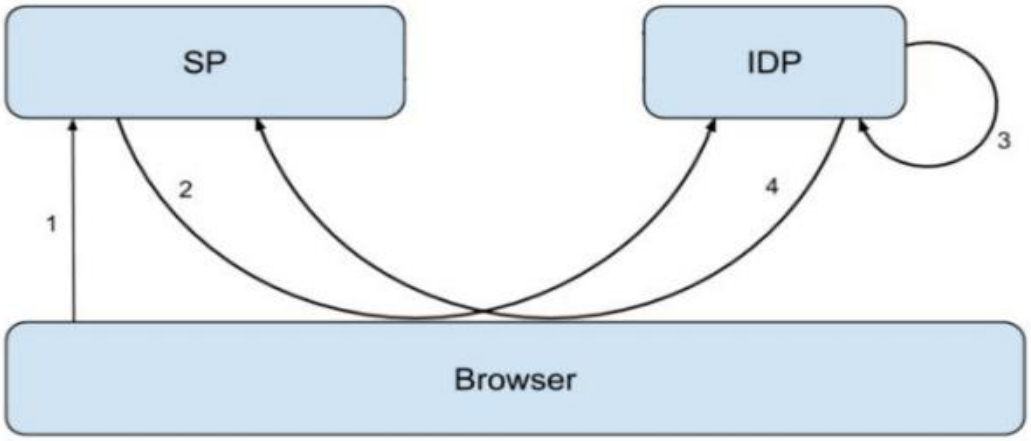


图 x SAML 协议流程

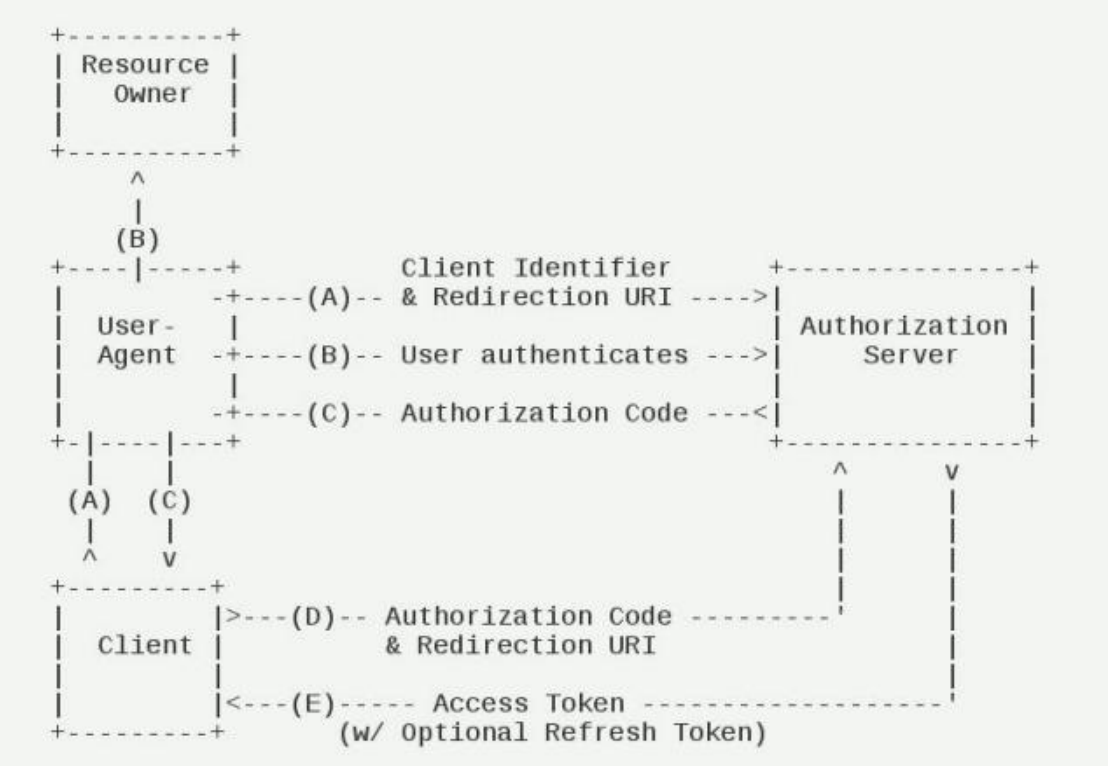
SAML 协议流程如下：

1. 用户通过浏览器访问 SP 的某个受保护的资源；
2. SP 鉴别到该用户未鉴权，于是将该用户重定向到 IDP 端；前提是该 IDP 是受 SP 信任的身份认证中心；
3. IDP 端通过自己的认证方式对该用户合法性进行认证；
4. 认证通过后，IDP 端生成响应后返回给 SP；SP 接收到 IDP 的响应后解析出用户认证信息，合法，则允许用户访问受保护的资源。

4.2.4.4 **Oauth**

OAuth 是标准授权协议，主要应用在委派访问，经常会用在用户授权网站或者应用程序访问自己在另一个网站上的信息,而不给他们密码的场景下.Amazon, Facebook, Google, Microsoft 和 Twitter 都使用这种机制允许用户与第三方应用程序或网站共享其帐户信息.

下图是标准的 OAuth 授权流程



（A）用户打开客户端以后，客户端要求用户给予授权。

（B）用户同意给予客户端授权。

（C）客户端使用上一步获得的授权，向认证服务器申请令牌。

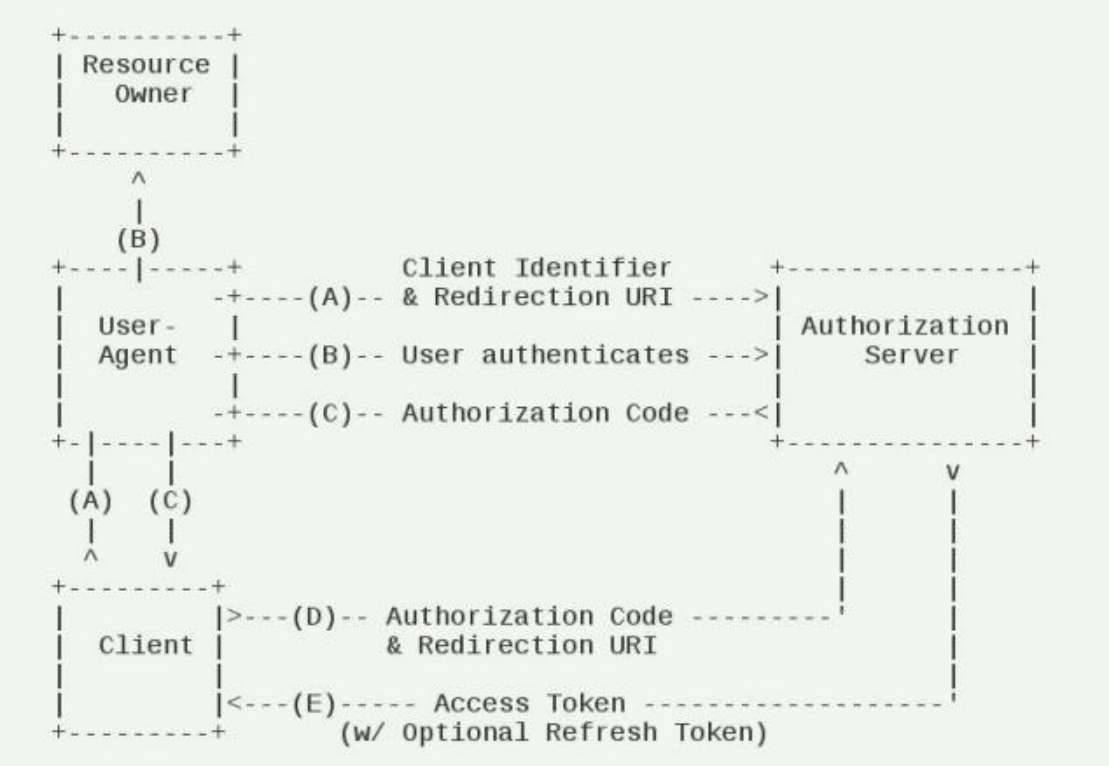
（D）认证服务器对客户端进行认证以后，确认无误，同意发放令牌。

（E）客户端使用令牌，向资源服务器申请获取资源。

（F）资源服务器确认令牌无误，同意向客户端开放资源。

OAuth 的核心就是向第三方应用颁发令牌，OAuth 2.0 规定了四种获得令牌的流程。

- 授权码（authorization-code）：第三方应用先申请一个授权码，然后再用该码获取令牌。这种方式是最常用的流程，安全性也最高，它适用于那些有后端的 Web 应用。授权码通过前端传送，令牌则是储存在后端，而且所有与资源服务器的通信都在后端完成。这样的前后端分离，可以避免令牌泄漏。



（A）用户访问客户端，后者将前者导向认证服务器。

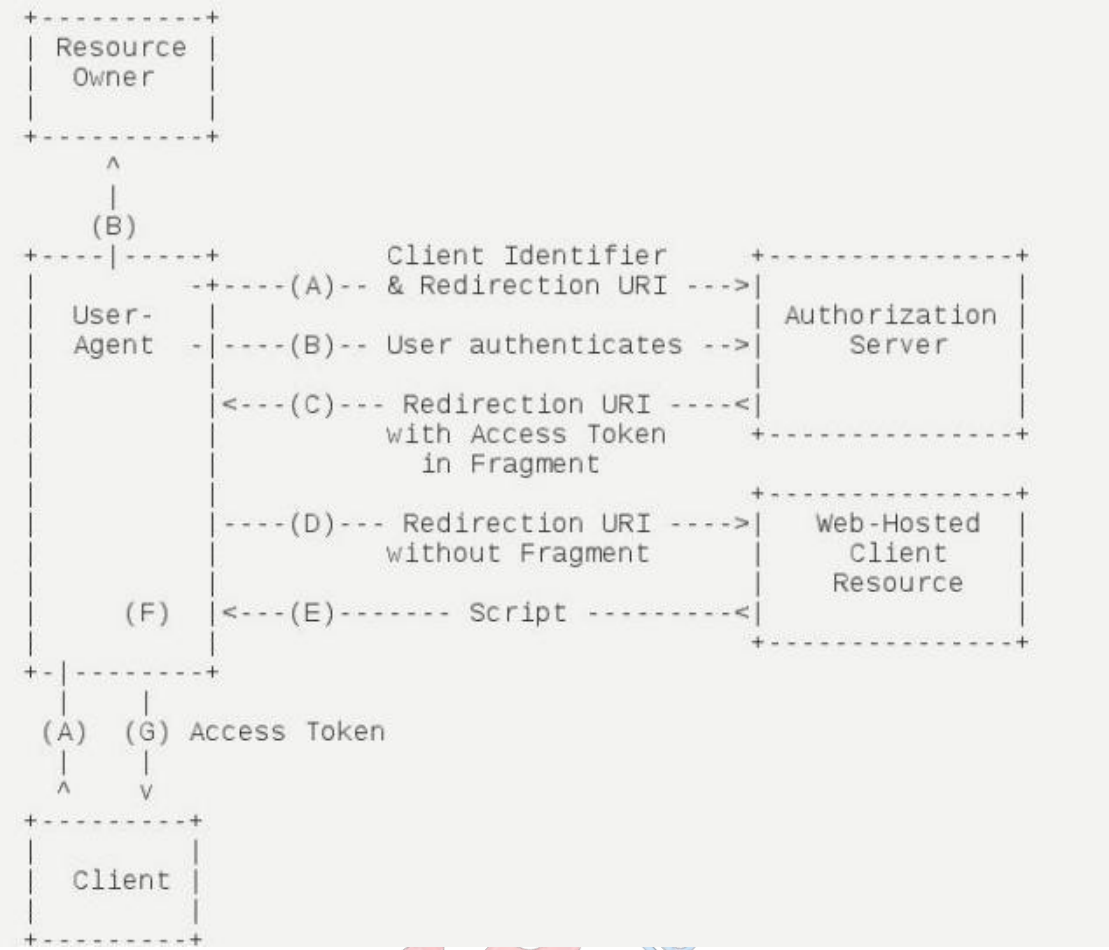
（B）用户选择是否给予客户端授权。

（C）假设用户给予授权，认证服务器将用户导向客户端事先指定的"重定向 URI"（redirection URI），同时附上一个授权码。

（D）客户端收到授权码，附上早先的"重定向 URI"，向认证服务器申请令牌。这一步是在客户端的后台的服务器上完成的，对用户不可见。

（E）认证服务器核对了授权码和重定向 URI，确认无误后，向客户端发送访问令牌（access token）和更新令牌（refresh token）

- 隐式授权（implicit）:针对没有后端的 Web 应用，必须将令牌储存在前端。这种方式没有授权码这个中间步骤。



（A）客户端将用户导向认证服务器。

（B）用户决定是否给于客户端授权。

（C）假设用户给予授权，认证服务器将用户导向客户端指定的"重定向 URI"，并在 URI 的 Hash 部分包含了访问令牌。

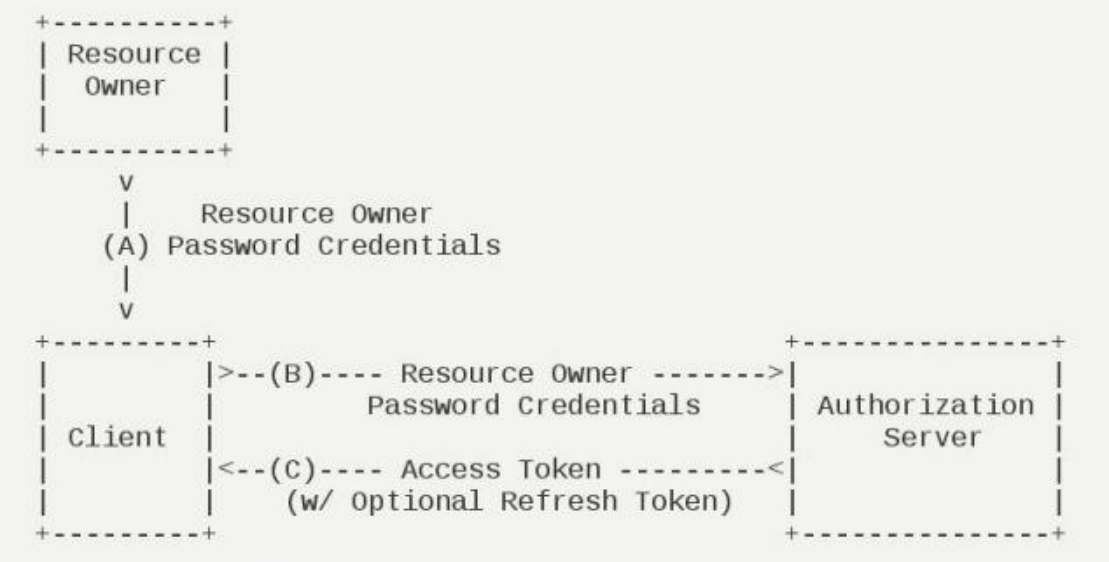
（D）浏览器向资源服务器发出请求，其中不包括上一步收到的 Hash 值。

（E）资源服务器返回一个网页，其中包含的代码可以获取 Hash 值中的令牌。

（F）浏览器执行上一步获得的脚本，提取出令牌。

（G）浏览器将令牌发给客户端。

- 密码式（password）：如果高度信任某个应用，也允许用户把用户名和密码，直接告诉该应用。该应用就使用用户的用户名和密码申请令牌。

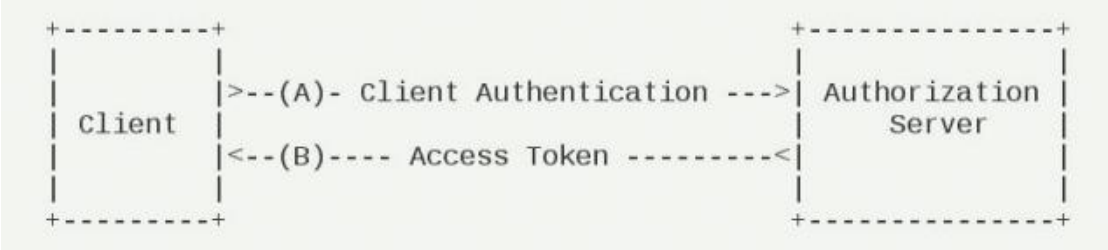


（A）用户向客户端提供用户名和密码。

（B）客户端将用户名和密码发给认证服务器，向后者请求令牌。

（C）认证服务器确认无误后，向客户端提供访问令牌。

- 客户端凭证（client credentials）：适用于没有前端的命令行应用，即在命令行下请求令牌。



（A）客户端向认证服务器进行身份认证，并要求一个访问令牌。

（B）认证服务器确认无误后，向客户端提供访问令牌。

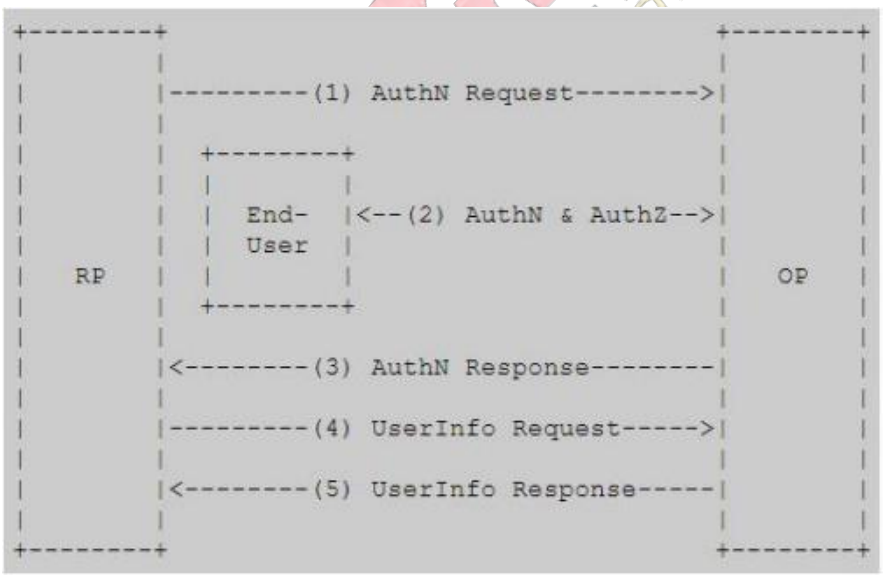
OAuth 2.0 是 OAuth 协议的最新版本，但不向下兼容 OAuth 1.0。OAuth 2.0 关注客户端开发者的简易性，同时为 Web 应用、桌面应用、手机和智能设备提供专门的认证流程。OAuth 2.0 规范和相关 RFC 由 IETF OAuth WG 开发,主要框架于 2012 年 10 月发布。

OAuth 是一个与 OpenID 互为补充的服务.由于 OIDC 是建立在 OAuth 2.0 之上的身份验证层，因此 OAuth 与 OpenID Connect（OIDC）直接相关。 OAuth 可以与授权策略标准 XACML 结合使用，其中 OAuth 用于所有权同意和访问委派，而 XACML 用于定义授权策略。

4.2.4.5 **OIDC**

OIDC(OpenID Connect) 是基于 OAuth 2.0 协议的身份认证协议，（Identity, Authentication）+ OAuth 2.0 = OpenID Connect。 它允许客户端基于授权服务器执行的身份验证来验证最终用户的身份，并以可互操作且类似于 REST 的方式获取有关最终用户的基本配置文件信息。OIDC 在 OAuth 2.0 提供了 Access Token 的基础上提供了 ID Token 来解决第三方客户端标识用户身份认证的问题。OIDC 的核心在于在 OAuth2 的授权流程中，一并提供用户的身份认证信息（ID Token）给到第三方客户端，ID Token 使用 JWT 格式来包装，得益于 JWT（JSON Web Token）的自包含性，紧凑性以及防篡改机制，使得 ID Token 可以安全的传递给第三方客户端程序并且容易被验证。此外还提供了 UserInfo 的接口，用户获取用户的更完整的信息。

实施 OpenID Connect 的 OAuth 2.0 身份验证服务器也称为 OpenID 提供程序（OP）。使用 OpenID Connect 的 OAuth 2.0 客户端也称为依赖方 （RP）。OIDC(OpenID Connect) 的交互步骤如下.



1.RP 发送一个认证请求给 OP；

2.OP 对 EU 进行身份认证，然后提供授权；

3.OP 把 ID Token 和 Access Token 返回给 RP；

4.RP 使用 Access Token 发送一个请求 UserInfo EndPoint；

5.UserInfo EndPoint 返回 EU 的 Claims。

根据应用的不同，OIDC 的工作模式也应该是不同的。如果是 JavaScript 应用程序，

那么使用浏览器开发工具的人就可以查看所有内容，建议 OIDC 使用隐式授权(Implicit)模式。如果是传统的应用程序，其中一些信息在前端传递（任何人都可以查看），但是后端可以保证令牌的安全存储，可以使用授权码（authorization-code）模式。还可以使用混合(Hybrid)模式，即包括授权码（authorization-code）和隐式授权(Implicit)。

4.2.4.6 **Kerberos**

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。

协议的安全主要依赖于参加者对时间的松散同步和短周期的叫做 Kerberos 票据的认证声明。 下面是对这个协议的一个简化描述，将使用以下缩写：

AS（Authentication Server）= 认证服务器

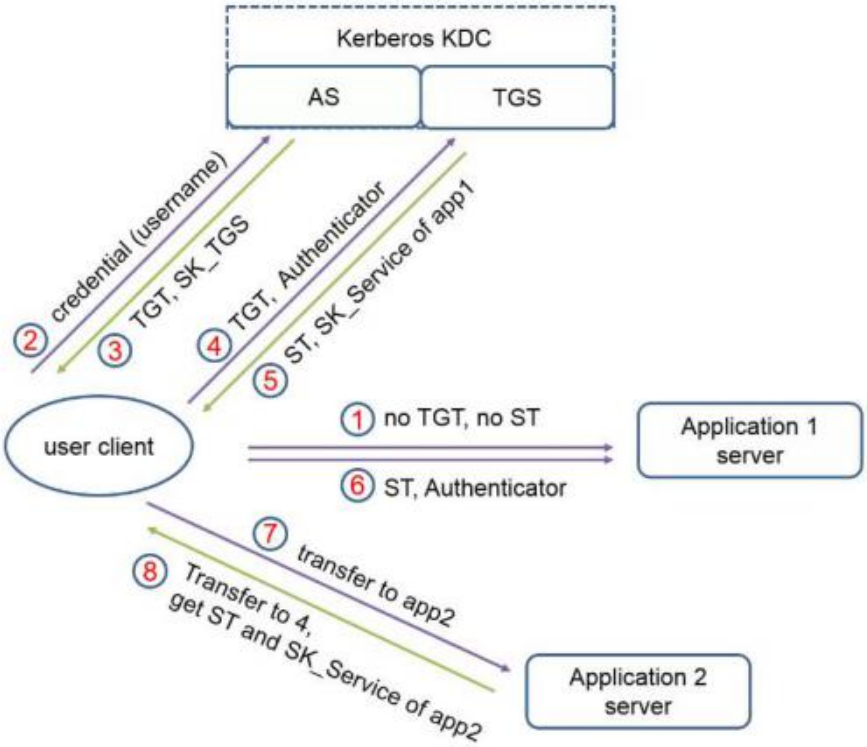
KDC（Key Distribution Center）= 密钥分发中心

TGS（Ticket Granting Server）= 票据授权服务器

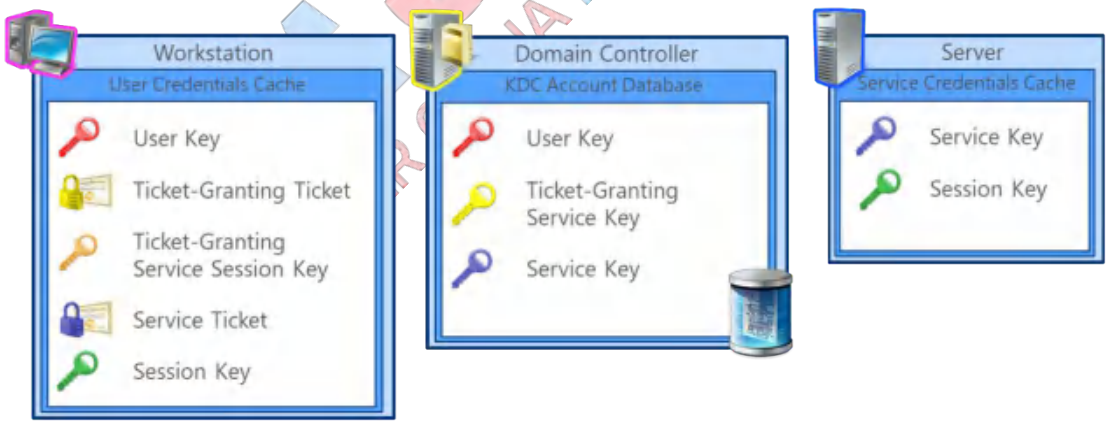
TGT（Ticket Granting Ticket）= 票据授权票据，票据的票据

SS（Service Server）= 特定服务提供端

ST（Service Ticket））= 服务票据



Kerberos 身份验证依赖于几种密钥和密钥类型进行加密。密钥类型可以包括长期对称密钥，长期非对称密钥和短期对称密钥。认证协议被设计为使用对称加密，这意味着发送方和接收方使用相同的共享密钥进行加密和解密。下图是微软在活动目录(Active Directory)的场景下，这几种密钥类型都有使用。



长期对称密钥：用户，系统，服务和域间密钥。长期对称密钥是从密码派生的。通过将密码文本传递给密码功能，将纯文本密码转换为密码密钥。用户密钥创建用户时，将使用密码来创建用户密钥。在 Active Directory 域中，用户密钥与用户对象一起存储在 Active Directory 中。在工作站上，用户登录时会创建用户密钥。系统密钥工作站或服务器加入 Windows 域时，它将收到密码。以与用户帐户相同的方式，使用系统帐户的密

码来创建系统密钥。服务密钥服务使用基于其登录帐户密码的密钥。同一领域中的所有 KDC 都使用相同的服务密钥。该密钥基于分配给 krbtgt 帐户的密码。每个 Active Directory 域都将具有此内置帐户。域间密钥为了进行跨域身份验证，KDC 必须共享一个域间密钥。然后，领域可以彼此信任，因为它们共享密钥。具有父子关系的 Active Directory 域共享一个域间密钥。此域间密钥是 Windows 2000 和 Windows Server 2003 中传递信任的基础。如果创建了快捷信任，则两个域将专门为其信任交换密钥。

长期非对称密钥：公钥。存储在智能卡上的公钥证书是 Microsoft Kerberos 身份验证实现中唯一的长期非对称密钥。

短期对称密钥：会话密钥。用于票证授予票证（TGT）和服务票证的会话密钥是短暂的，仅在该会话或服务票证有效时才使用。

4.2.4.7 **JWT**

Json web token (JWT)，是为了在网络应用环境间传递声明而执行的一种基于 JSON 的开放标准（(RFC 7519).该 token 被设计为紧凑且安全的，特别适用于分布式站点的单点登录（SSO）场景。JWT 的声明一般被用来在身份提供者和服务提供者间传递被认证的用户身份信息，以便于从资源服务器获取资源，也可以增加一些额外的其它业务逻辑所必须的声明信息，该 token 也可直接被用于认证，也可被加密。

JWT 是由三段信息构成的，将这三段信息文本用.链接一起就构成了 Jwt 字符串。第一部分我们称它为头部（header),第二部分我们称其为载荷（payload，类似于飞机上承载的物品)，第三部分是签证（signature).

- header

  jwt 的头部承载两部分信息：

  •声明类型，这里是 jwt

  •声明加密的算法 通常直接使用 HMAC SHA256

- playload

  Playload 就是存放有效信息的地方。这些有效信息包含三个部分

  - 标准中注册的声明(建议但不强制使用)
    - iss: jwt 签发者
    - sub: jwt 所面向的用户

- aud: 接收 jwt 的一方
- exp: jwt 的过期时间，这个过期时间必须要大于签发时间
- nbf: 定义在什么时间之前，该 jwt 都是不可用的.
- iat: jwt 的签发时间
- jti: jwt 的唯一身份标识，主要用来作为一次性 token,从而回避重放攻击。

■ 公共的声明

公共的声明可以添加任何的信息，一般添加用户的相关信息或其他业务需要的必要信息.但不建议添加敏感信息，因为该部分在客户端可解密.

■ 私有的声明

私有声明是提供者和消费者所共同定义的声明，一般不建议存放敏感信息，因为 base64 是对称解密的，意味着该部分信息可以归类为明文信息。

- signature

jwt 的第三部分是一个签证信息，这个签证信息由三部分组成：

•header (base64 后的)

•payload (base64 后的)

•secret

这个部分需要 base64 加密后的 header 和 base64 加密后的 payload 使用.连接组成的字符串，然后通过 header 中声明的加密方式进行加盐 secret 组合加密，然后就构成了 jwt 的第三部分。

注意：secret 是保存在服务器端的，jwt 的签发生成也是在服务器端的，secret 就是用来进行 jwt 的签发和 jwt 的验证，所以，它就是你服务端的私钥，在任何场景都不应该流露出去。一旦客户端得知这个 secret, 那就意味着客户端是可以自我签发 jwt 了。

JWT 最常见的场景是 Authentication（鉴权）。一旦用户登录，每个后续请求都将包含 JWT，允许用户访问该令牌允许的路由，服务和资源。单点登录是当今广泛使用 JWT 的一项功能，因为它的开销很小，并且能够轻松地跨不同域使用。还有 Information Exchange（信息交换） 场景。JSON Web Tokens 是在各方之间安全传输信息的好方式。因为 JWT 可以签名：例如使用公钥/私钥对，所以可以确定发件人是他们自称的人。此外，由于使用标头和有效载荷计算签名，因此您还可以验证内容是否未被篡改。

4.2.4.8 LTPA（是否需要放）

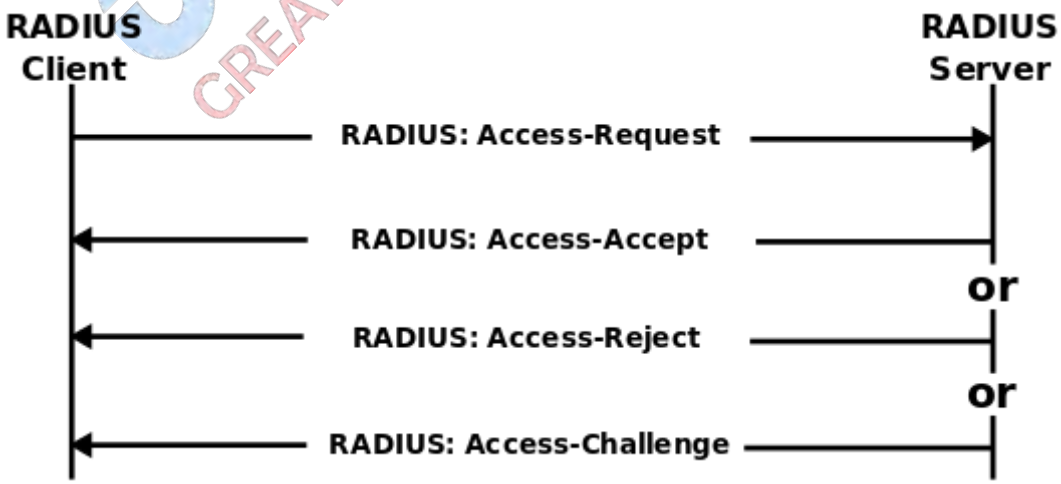
Lightweight third party authentication(LTPA)，轻量级第三方认证，支持在一个因特网域中的一组 Web 服务器之间使用单一登录的认证框架。LTPA 用于分布式、多应用程序服务器和机器环境。LTPA 通过密码术可支持分布式环境中的安全性。此支持允许 LTPA 进行加密、数字签名和安全地传输与认证相关的数据，并在以后对该签名进行解密和验证。IBM Websphere 和 Domino 产品中使用该技术。

4.2.4.9 Radius

RADIUS： Remote Authentication Dial In User Service，远程用户拨号认证系统由 RFC2865，RFC2866 定义，是应用最广泛的 AAA 协议。AAA 是一种管理框架，因此，它可以用多种协议来实现。在实践中，人们最常使用远程访问拨号用户服务（Remote Authentication Dial In User Service，RADIUS）来实现 AAA。

RADIUS 是一种 C/S 结构的协议，它的客户端最初就是 NAS（Net Access Server）服务器，任何运行 RADIUS 客户端软件的计算机都可以成为 RADIUS 的客户端。RADIUS 协议认证机制灵活，可以采用 PAP、CHAP 或者 Unix 登录认证等多种方式。RADIUS 是一种可扩展的协议，它进行的全部工作都是基于 Attribute-Length-Value 的向量进行的。RADIUS 也支持厂商扩充厂家专有属性。

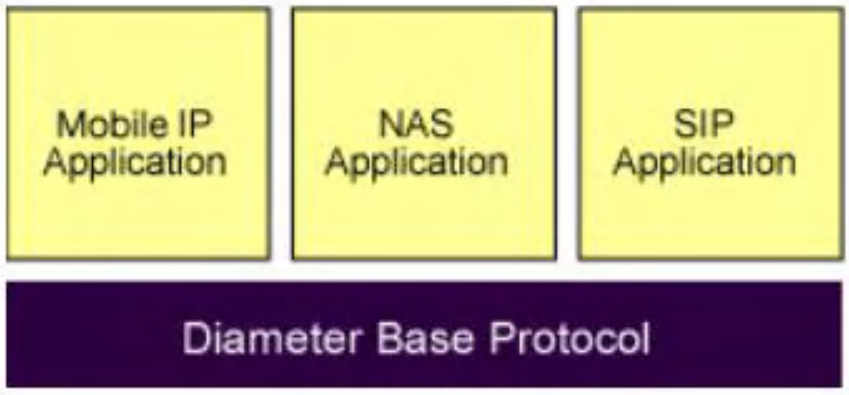
IEEE 提出了 802.1x 标准，这是一种基于端口的标准，用于对无线网络的接入认证，在认证时也采用 RADIUS 协议。



尽管 RADIUS 得到广泛应用，但是由于其本身的缺陷，协议已不能适应当前网络

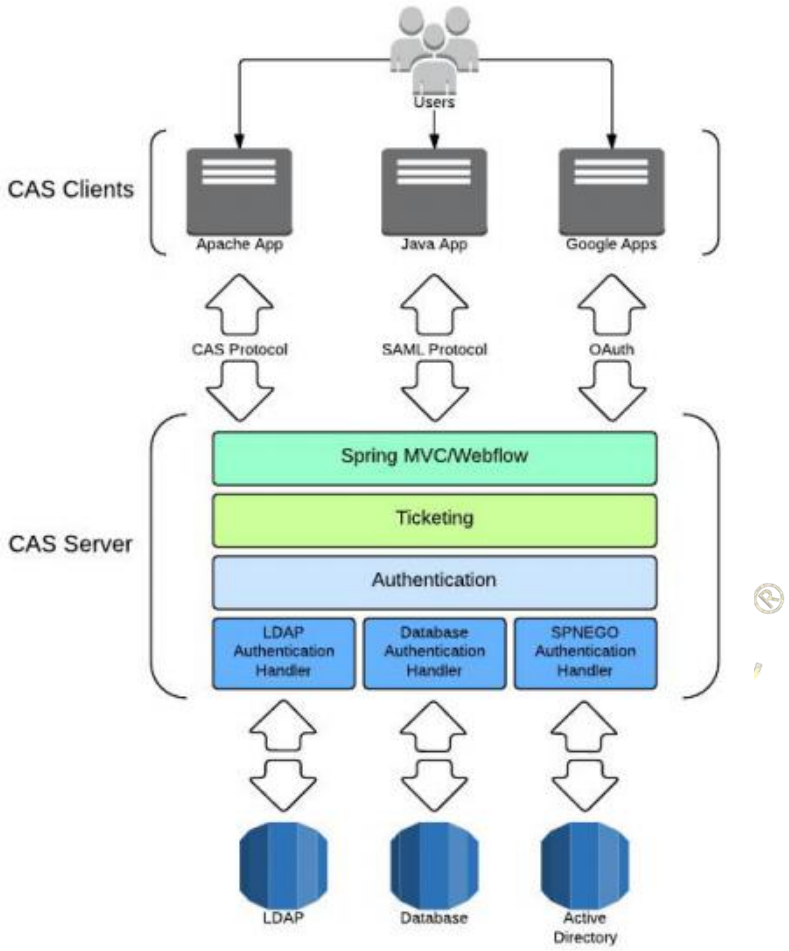
的发展。网络用户数量的增加、新接入技术的引入、网络规模的快速扩容以及越来越复杂的路由器和接入服务器的大量使用都对 AAA 服务提出了新的要求。因特网工程任务组(IETF)成立了 AAA 工作组，着手下一代 AAA 协议的研究开发。该工作组将 Diameter 协议定为下一代的 AAA 协议标准。Diameter 在保持与 RADIUS 协议兼容的同时还克服了 RADIUS 协议的许多不足。

Diameter 用传输控制协议(TCP)和信令控制传输协议(SCTP)取代 RADIUS 的 UDP 通信机制，具备连接建立与终止、对等节点能力协商和错误通知等特征,并且可以采用 IP 安全协议(IPsec)或者传输层安全(TLS)协议对连接加密。Diameter 协议兼容 RADIUS，消息格式与 RADIUS 消息相近。Diameter 头部包括版本、消息长度、命令标志、命令代码、应用代码、逐跳标志以及端到端标志域。头部之后是若干属性值对，携带的属性值对取决于消息的类型。下图说明了 Diameter 基本协议与各种 Diameter 应用程序之间的关系。

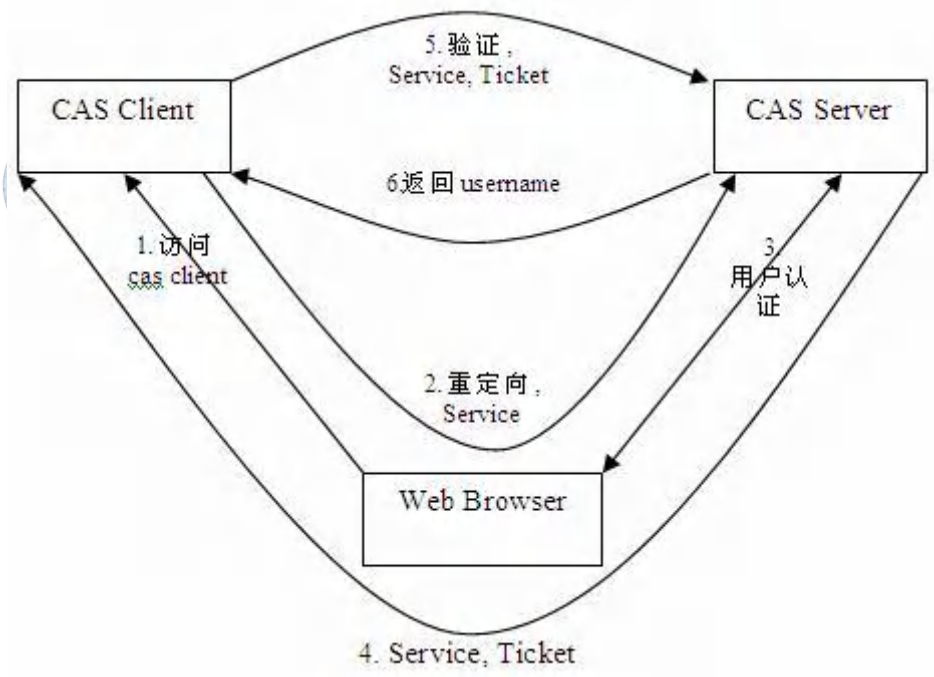


4.2.4.10 CAS

CAS 是 Central Authentication Service 的缩写，中央认证服务，一种独立开放指令协议。CAS 包括两部分: CAS Server 和 CAS Client。应用程序通过 CAS 的客户端，拦截校验用户请求是否通过认证，如果尚未认证，则重定向到 CAS 服务端的用户登录页面进行登录，登录成功后，会生成一个 ticket 给回应用程序，下次用户请求带着这个 ticket 就所向无阻。



下面是 CAS 最基本的协议过程：



主要有以下步骤：

1. 访问服务：客户端发送请求访问应用系统提供的服务资源。
2. 定向认证：客户端会重定向用户请求到服务器。
3. 用户认证：用户身份认证。
4. 发放票据：服务器会产生一个随机的 Service Ticket 。
5. 验证票据：服务器验证票据 Service Ticket 的合法性，验证通过后，允许客户端访问服务。
6. 传输用户信息：服务器验证票据通过后，传输用户认证结果信息给客户端。

4.2.5 典型认证场景

4.2.5.1 社交认证介绍

什么是社交媒体认证

社交认证是针对最终用户的单点登录。 使用来自社交网络提供商（例如 Facebook、Twitter 或微博、微信）的现有登录信息，用户可以登录第三方网站，而不必专门为该网站创建新帐户。 这简化了最终用户的注册和登录。

为什么要在应用中增加社交媒体认证

- 增加注册人数：根据 Web Hosting Buzz 的一项调查，86％的用户表示由于不得不在网站上创建新帐户而感到困扰。其中一些用户宁愿离开您的网站也不愿注册，这意味着向您的应用程序提供“社交登录”将增加您网站的注册数量。调查还指出，有77％的受访者表示“社交登录是一个不错的解决方案，应该在任何网站上都可以使用。”
- 访问更丰富的用户配置文件：社交网络提供商可以为您提供有关用户的其他信息，例如位置，兴趣，生日等。使用此数据，您可以将个性化内容定位到用户。
- 最新的个人资料：用户通常不会在使用的大多数应用程序中保持个人资料的更新，而是在社交网络中进行更新。因此，进行社交登录可确保您拥有有关用户的准确信息。
- 一键式返回体验：用户使用“社交登录”在您的应用程序中注册后，他们的返回体验将非常简单，因为他们很可能已登录到社交网络，只需单击一下就足以登录到您的应用程序。

社交媒体认证的步骤

1. 用户输入您的应用程序，然后选择所需的社交网络提供商。
2. 登录请求被发送到社交网络提供商。
3. 社交网络提供商确认用户身份后，当前用户将可以访问您的应用程序。 新用户将被注册为到应用程序中为新用户，然后登录到应用程序。

社交媒体认证的引入契机及隐私问题

OAuth 是用于访问委派的开放标准，通常用作 Internet 用户向网站或应用程序授予对其他网站上的信息的访问权限而又不给他们密码的一种方式。 亚马逊，谷歌，Facebook，微软和 Twitter 等公司使用此机制来允许用户与第三方应用程序或网站共享有关其帐户的信息。

社交媒体认证的引入原因，来源于社交媒体的兴起以及互联网应用的爆发式增长，社交媒体的兴起带来的是在少数几个大型社交平台上，拥有很庞大的用户群体，使每个用户都会必备这几个社交应用。而互联网应用的爆发式增长，则是用户会大量的尝鲜一些新应用，而那些繁琐的注册过程会阻碍用户去体验的兴致，另一方面带来的是口令认证带来的弊端，用户常常记不住自己设置的口令。虽然有一些应用会通过手机号来快捷注册，但一些安全意识比较强的用户，可能会比较抗拒一开始就提供手机号。

因此，社交媒体认证的兴起，是为多方共同带来好处的产物。对于用户来说，可以在不暴露敏感信息的情况下快速体验应用。而互联网应用则通过这种方式快速的让用户无门槛的了解自己，而对于提供社交媒体认证的服务方，则可以知道用户都对什么类型的应用感兴趣，从而衍生出更多服务或者场景（但这种行为收集，则涉及个人隐私问题，比如用户是否愿意让社交媒体认证提供商，知道自己平时都去使用哪些应用）。

4.2.5.2 设备认证介绍

设备认证

物联网设备允许授权的用户或设备访问资源，并拒绝恶意实体访问这些资源。它还可以限制授权用户或设备访问受损设备。此外，身份验证降低了入侵者建立与网关的连接机会，由此减少 DoS 攻击的风险。在安全的物联网通信中，在两个或多个实体之间的任何通信涉及访问资源之前，必须对每个参与实体进行验证，以确定其在网络中的真实身份。它意味着每个合法的节点或实体必须有一个有效的身份，以便参与通信。

身份验证过程通常依赖于用户名和密码的使用。例如，在传统的互联网上，网站要求用户名和密码认证用户，而浏览器使用 SSL 协议对网站进行认证。但物联网的一个争论点是，通常部署在通信系统核心的设备和大多数生态系统的终端节点都是由传感器组成的（在某些情况下是 RFID 标签）。这些终端设备用于收集信息，并将收集到的信息传送到各个平台。

因此，在这些硬件缺乏身份验证的情况下，黑客们可以轻易连接到这些传感器，也可以访问数据，或者进行广泛的恶意活动。考虑到它们中的大多数都是电量有限的节点，而且计算和内存资源有限，目前支持设备认证的主流方案主要有两种：

第一种是基于 PKI 的安全认证方案；在物联网应用 PKI，即是将各个设备作为主体，在进行工作之前需要申请设备自身的设备证书，在与外界交互过程中使用证书来进行身份认证。在使用 PKI 的情况下，系统可以较好的保证通信双方的身份可信，但由于公钥密码算法运算较多所以相对耗时。与此同时，由于各设备的证书都需要同一个 CA 系统进行审核发放和查询，且证书存储会占用设备的空间，如果设备的数量达到千万级乃至上亿的话，系统性能会受到很大影响，因此 PKI 较为适合设备数量不大且多为端到云通信的物联网系统。

第二种是由云厂商提供的 IoT 认证服务，以阿里云的 IoT 设备身份认证 Link ID^{2}和腾讯云 IoT 设备身份认证 IoT TID 服务为代表。云厂商提供密钥分发中心和认证中心两个服务。分发中心采用硬件加密机和安全存储技术，确保密钥云端生成和存储的安全；与合作伙伴的安全产线对接，确保密钥安全烧录到各种安全等级的载体上。客户将安全载体集成到物联网设备，基于设备端和云端的 SDK，调用云端认证中心提供的设备认证、信息加密等接口，建立安全通道，保障业务数据的不可抵赖性、完整性和保密性。此类技术提供了更加 优化的算法，大幅度减少了存储占用和计算量，对弱计算能力的嵌入式 MCU 也可运行，并支持在弱网低速率环境下接入。

设备认证方案还在快速发展阶段，业界不断寻求安全性和轻量化之间的平衡点，目前还未有统一的标准解决方案。为了实现为了实现物联网的标准化安全解决方案，还需要各种标准化机构来共同协调它们之间的工作。

4.2.5.3 联邦认证

1、基本概念

目前越来越多的企业对自己内部系统采取集中式身份管理，这样做的好处是简化用户管理，用户数据可以通过服务跳转的方式非常方便的访问，但是不同企业之间应用的单点登录却很难通过统一身份认证来实现，如何实现企业间的单点登录成为了优化用户体验的核心问题之一。而且，随着不同企业信息系统规模的不断增长，把企业用户的所有信息全部收集到一个地方，也存在着极大个人信息泄露的风险，联邦认证很好的解决了这些问题。

联邦身份是一种可以让企业与合作伙伴、供应商、客户等的用户身份信息安全地联系在一起的概念。为了建立跨域的单点登录，参与的多个安全域之间需要建立信任，构成身份联盟，利用联邦身份（Federal Identity）实现跨域的单点登录。

2、实现方式

Microsoft Passport、LiSPerty Alliance 和 AOL 公司的 Magic Carpet 都致力于为基于用户身份验证开发出一种标准的、联合性的身份体系结构，以便使得应用程序可以访问多个联盟成员网络。

Microsoft Passport 是一种私有服务，需要使用 Microsoft Hotmail 和 Microsoft MSN Network 中基本的身份验证系统。

LiSPerty Alliance 较多地依赖于安全声明标记语言(Security Assertion Markup Language，SAML)实现。对于 SAML 的介绍详见 4.5.3。

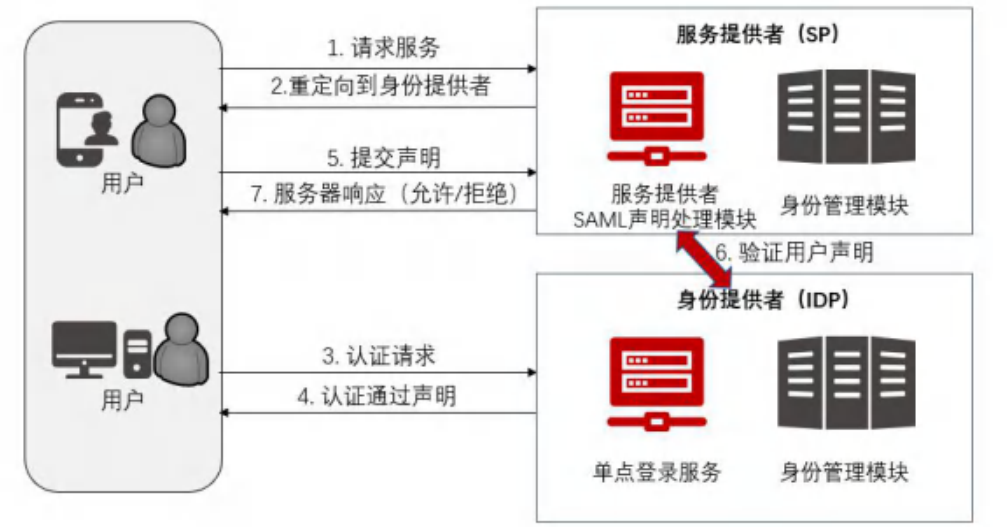
由于身份联盟受到 5 个不兼容的协议(SAML1．0 和 SAML1．1、自由联盟 ID—FF1．1 和 ID—FF1．2 以及 ShiSPSPoleth) 问题的困扰，给企业和客户的应用带来了麻烦，延缓了发展，2005 年 3 月 OASIS 批准了 SAML2．0 版。SAML2．0 消除了阻碍进一步采用身份联盟的最大障碍——多协议复杂性，因而大大改变了身份联盟的局面。SAML2．0 说明了实现联盟的两个角色。服务提供者是为用户提供应用或 WeSP 服务的实体，而身份提供者负责认证用户。服务提供者和身份提供者交换信息，以实现单点登录和退出。在进行单点登录时，身份提供者负责创建包含用户身份的 SAML 声明，然后安全地将这个声明发送给服务提供者。服务提供者负责在让用户访问之前验证 SAML 声明的有效性。

3、联邦认证核心原理概述

1）认证登录流程

身份联盟的参与者主要包括：用户、服务提供者(SP)和身份提供者(IDP)。其中用户通常是使用浏览器（也可以是具有特定功能的 API 或 WeSP 服务）请求服务的。身份联

盟技术首先建立不同用户之间公信的身份提供者（IDP）作为第三方公信验证机构，然后使用 SAML 实现了需要建立信任的不同成员(不同域)之间的跨域单点认证（具体登录流程如下图）。其身份数据库之间是通过其它方法实现同步的，比如采用数据库同步技术或离线批更新技术等。



图：联邦认证过程

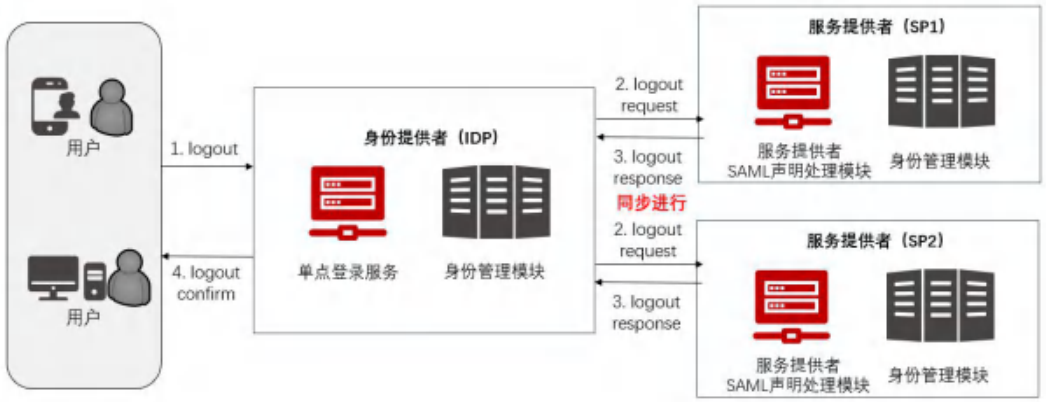
上述描述的认证过程包括：

1. 用户向 SP 申请服务；
2. SP 将用户重定向到 IDP，请求身份认证；
3. 用户向 IDP 提交身份认证信息；
4. IDP 判断身份认证通过后构造身份声明，并保存声明在本地，将用户重定向到 SP；
5. 用户提交身份声明给 SP；
6. SP 向 IDP 请求验证此声明，验证后 IDP 返回身份验证声明；
7. SP 再根据此身份验证声明来响应用户的服务请求；

2）用户注销流程

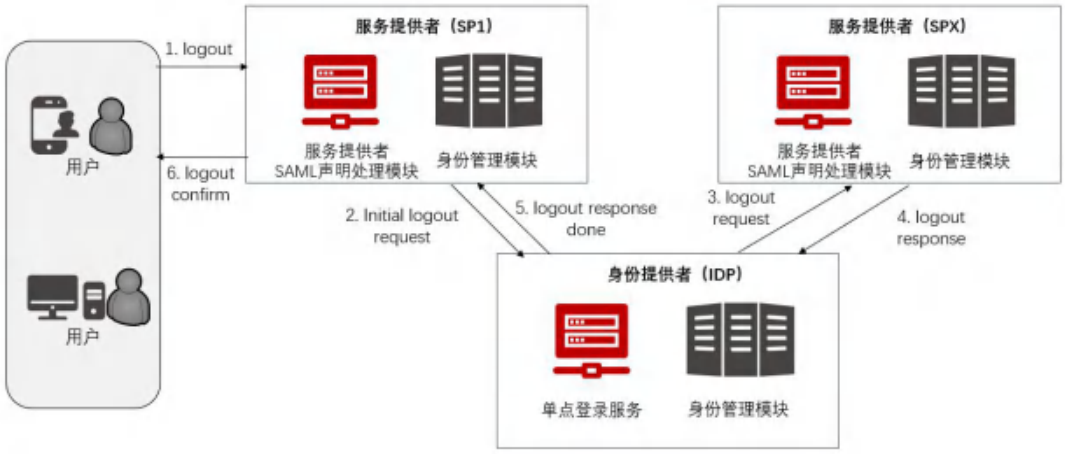
用户登录后，在 IDP 和 SP 上均建立了会话当用户不再使用系统时，则需要在 IDP 和 SP 上同时注销身份，即单点注销。实现单点注销可以通过 IDP 或某个 SP 一次性完成。使用 IDP 实现单点注销的流程如下图所示，IDP 收到用户发出的 logout 请求后，对注册的 SP 轮询发出 logout request 请求，待收到所有 SP 的 logout response 后，向用户发

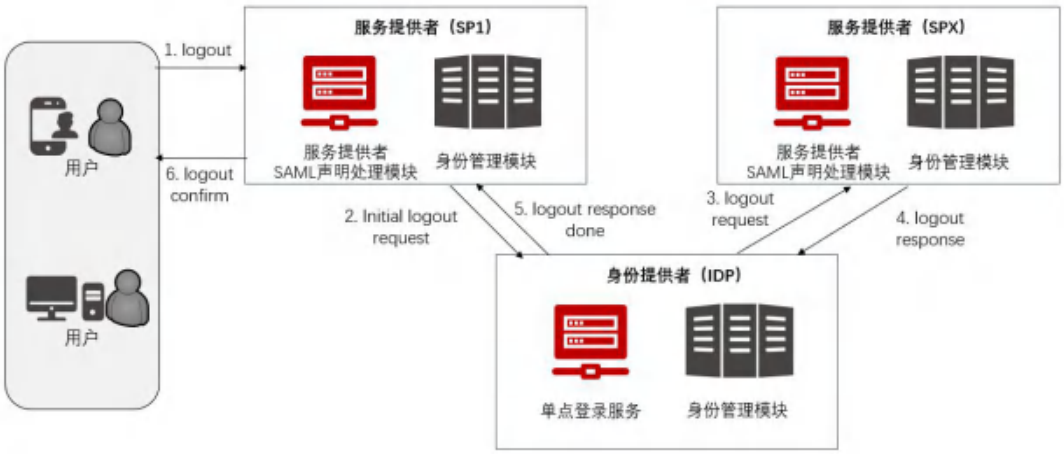
出 logout confirm 消息，注销成功，如果没有收到任意一个 SP 的 logout response 消息，则向用户返回出错信息。



图：从 IDP 上进行单点注销

使用 SP 的注销的方式如下图所示，用户向某 SP 发出 logout 指令后，SP 即向 IDP 发出 initial logout request 请求，IDP 则轮询注册的其他 SP，发出 logout request 请求，收到全部响应后，向发出 initial logout request 请求的 SP 发送 logout response done 消息来证明所有响应已收到，该 SP 则向用户返回 logout confirm 消息，注销成功，如果失败也如前面同样方式处理。





图：从某个 SP 上进行单点注销

3）账号映射原理

由于 SP 和 IDP 系统均保留了各自的用户管理和授权模块，因此就存在着 IDP 用户名与各 SP 用户名之间的对应问题。解决这个问题的方法有两个：一是在 IDP 上实现帐号映射模块，由各 SP 的管理员修改 IDP 用户名和 SP 用户名之间的对应关系，IDP 在生成断言时则根据对应关系修改成各 SP 对应的用户名。另一种方法是在两个 SP 上编写帐号复制模块，定时或手工从 LDAP 服务器导入用户名，然后再由 SP 管理员根据情况修改授权设置。

4）应用价值

联邦认证是企业身份和访问管理战略的关键组成部分，提供了多项业务优势。对于企业而言，联邦认证增强了企业与业务合作伙伴进行合作、为客户提供新型服务的能力，并且保护了企业资源，降低了成本。对于用户而言，联邦认证使服务访问更加便捷，提高了工作效率；提供了更广泛的访问信息与服务；有效保护了个人信息。

4.2.5.4 多端融合认证

多端融合认证介绍：

随着网络通信的显著改善和智能移动设备的普及，企业迅速利用这些基础架构来增强身份验证过程。多端融合认证是采用多个独立并分离的网络或者通讯线路，多个分离的通讯线路用户都提供相应认证因素，这种认证方式称之为多渠道认证（Multi-Channel Authentication）或者带外的通道认证 （Out-of-Band authentication），

即称为带外 “out-of-band”。通过与主要通道之外的身份和交易验证的机制，就称为多端融合认证。

多端融合认证的特性也带有通过将多因素身份验证（MFA）的功能，多因素认证通常指:你知道的东西(比如密码),你拥有的东西(比如硬件令牌或手机),你有什么东西(例如你的指纹、声纹、人脸)相互组合进行认证，但对多渠道没有要求。多端融合认证要通过多渠道和带外的通道认证来完成认证的流程和终端的设备通常都要再线上运作。

多端融合认证流程：

我们也许都遇到过这样的场景，当使用电话银行时，银行雇员会使用顾客开户时留下的个人信息作为问题进行提问，比如你的住址、生日来进行身份认证，这种认证方式实现起来非常简单，并且普遍，但缺少了隐私性，客户也许会担忧自己的 PII (Personally Identifiable Information) 被银行雇员泄露，更加安全一点的方法有通过预设电话服务密码来实现身份验证，在银行提供电话服务或远程业务办理时，先由客户在电话上输入自己预设的服务密码，银行系统验证通过后才能提供服务，这种方法避免了 PII 信息泄露，但还是有被中间人攻击、恶意键盘记录攻击、偷窥等社会工程学等方式进行攻击，泄露凭证、密码的风险。

现在的攻击者通过网络就可以操作用户的账号进行转账、交易支付，而进行操作的就好像是用户本人，网络犯罪更加难以防范，只有账户真正的主人才知道是不是他们本人在进行合法操作，以往，用户需要服务商提供预警信息，但这样的预警难以防范网络威胁，现在，服务商反而需要用户提供预警信息，银行才能知道用户账户被恶意操作，才能防范网络犯罪，所以通过合适的机制来赋予用户权限可以提高系统的安全性。

以前，如果银行注意到用户的账户交易异常，他们可以通过电话要求进行验证，以确保交易者的真实身份和意图，现在电子商务的规模让这种人工介入的方式变得越来越难以实施，通过传统的网络数据通道之外的通道，与在线行为自动化的同步交互，成为有效的替代办法，使用带外身份验证系统，通过这个带外通道，进行更多因素的认证，例如：手机信息推送，手机扫描登录，手机软令牌，手机人脸认证，基于 FIDO 的指纹、人脸认证，是确认交易者身份的有效方案；同时，系统可以给用户提供更多的业务流程和交易细节，让用户有再次确认或者取消操作的机会，是保证身份安全的有效方法。

威胁与带外认证带来的好处

威胁类型	特点	带外认证有效性描述
中间人攻击	劫持用户与交易服务器之间的会话，修改交易	通过带外通道，用户可以对交易的细节进行确认或者取消，也可以给服务方提供告警
盗窃可信凭据	恶意软件攻击、键盘记录攻击等获取用户可信凭据，密码等	用获取的可信凭据使用合法用户身份登录系统的操作细节，通过带外通道，交互给真正的用户，用户有机会可以确认或者取消操作，并可以反馈报警
偷窥等社会工程学攻击	通过肩窥，或者技术手段监测、按键音猜测等社会学攻击手段获取用户密码	攻击者可以伪造身份证件金融卡和获得用户密码，当同时攻破运营商的语音网络和移动数据网络，有巨大的技术障碍；同时也给用户提供再次确认和取消账户操作的机会

多端融合认证的场景：

使用以下用例来说明带外认证技术为用户提高安全，方便易用。

场景：访问银行网站，传呼中心或银行分支机构的自助服务终端时的使用。

1. 手机通话登录

当用户在 PC 端登录网银系统或敏感系统时，系统可以通过拨打用户预留的手机号，通过 AI 或者预设语音提示对用户的操作进行确认，当用户在手机上确认后，PC 端登录才能完成，用户如果在手机上进行否认登录，还可以需要登录或者向服务商发出警报。

2. 手机推送登录

当用户在 PC 端操作网银系统或敏感系统时，系统可以向用户手机上安装的移动应用发送推送通知，用户看到推送细节后，后可以进行确认、取消，甚至报警。

3. 手机扫描登录

当用户在 PC 端操作网银系统或敏感系统时，系统的界面可以展示二维码，让用户使用服务商提供的移动应用扫描，扫描完成后，用户查看登录细节，进行登录确认或取消。

4. 手机推送登录/手机扫描登录 + 手机生物认证授权

当用户在 PC 端操作网银系统或敏感系统时，可以将推送或扫描与生物认证进行整合，完成认证授权。

- 系统的界面可以展示二维码，让用户使用服务商提供的移动应用扫描，扫描完成后，使用国际认证标准 FIDO 实现的生物认证让用户进行登录授权，或者交易授权。
- 系统可以向用户手机上安装的移动应用发送推送通知，用户点击推送后可以进行确认或取消，更加安全的方式是使用国际认证标准 FIDO 实现生物认证授权，让用户在手机端进行指纹或人脸认证来确认用户的登录或交易操作。

多端融合认证总结：

多端融合认证给用户再次确认或者取消操作机会的同时，给系统增加了一层保护，给网络威胁增加了一层障碍。攻击者要么放弃进一步的行动，要么需要进行更多技术尝试，这个尝试的过程，就会遗留更多的足迹信息，给系统更多的信号和更多的时间进行分析和判断。

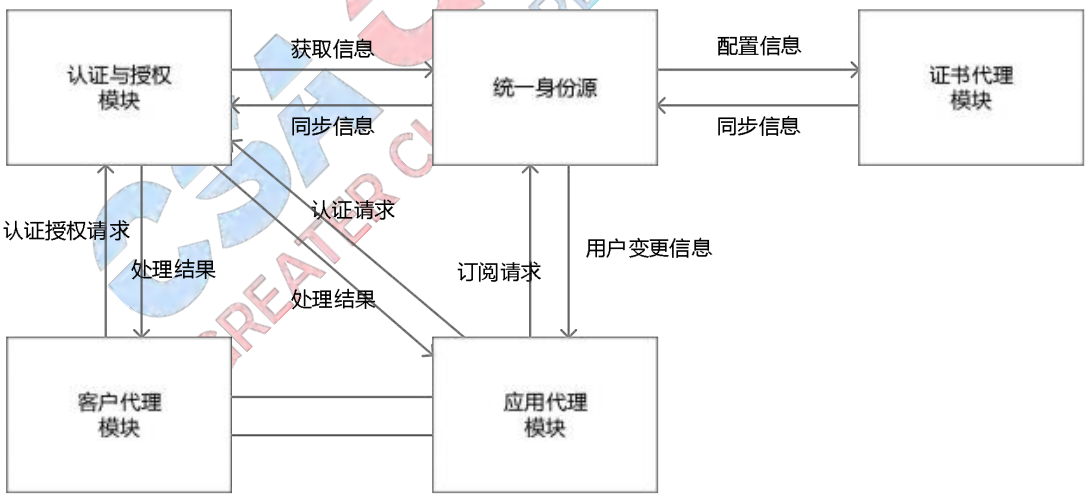
多端融合认证在手机上实现后，可以让用户密切使用的移动设备发挥它的重要作用，作为双通道多因素的认证手段，成为身份认证过程的一部分，并可参与业务或交易的一些重要环节，提供系统与用户更多的交互，建立更强大的安全机制。

多端融合认证提供人脸、SMS、软令牌、指纹等多种方式的认证机制，让用户不再仅仅依靠一种通信通道和方式来完成身份验证和重要业务流程验证，让那些以劫持用户通信会话为目标的高级攻击更难以得逞。并且带外身份认证系统可以完全独立运行，充分尊重用户隐私，不涉及原有用户信息、部署简单、管理方便、维护简单、不需要携带硬件、无需麻烦的售后维护，用户可以根据环境和场景选择喜欢的认证方式。

4.2.6 单点登录（包括原理、单点登出、会话管理、跨模式、跨浏览器等单点形式）

单点登录（Single Sign On，简称 SSO）提供一种企业控制用户访问企业资源的解决方案，它允许用户进行一次身份验证，即可获得对连接到 SSO 系统的所有企业资源的访问权，它通过一个凭据提供对多个独立应用系统的联合访问，包括单点登录与单点登出。

一、实现 SSO 系统的主要功能模块



认证与授权模块，负责为用户和应用系统提供认证和授权服务。该模块能够与客户代理与应用代理协商实现用户/应用系统的身份认证，还为用户授权应用系统当中的角色并发放访问应用系统的授权票据。

应用代理模块和客户代理主要以软件的形式布置在客户端和应用系统上，负责客户端和应用系统端的认证与授权的具体工作，跟认证与授权模块配合实现基于代理和经纪

人的单点登录服务。

统一身份源模块存储访问应用系统的用户信息和应用系统信息，信息来源是证书代理从证书服务器（若有）同步过来的用户/应用系统信息以及后续的对用户/应用系统新增、删除和变更的信息。统一身份源模块还向认证与授权模块同步对应的用户/应用系统信息，同时如果认证与授权模块发送获取信息的请求，则对它进行处理。此外，还应为应用系统提供订阅服务，根据应用系统上报的订阅条件，向应用系统同步符合订阅条件的用户变更信息，实现对用户信息的实时同步。此模块通常采用 LDAP（AD）等目录服务器，详情参考认证协议章节部分，用户数据同步主要采用 SCIM 协议，详情参看第三章 SCIM 协议章节部分。

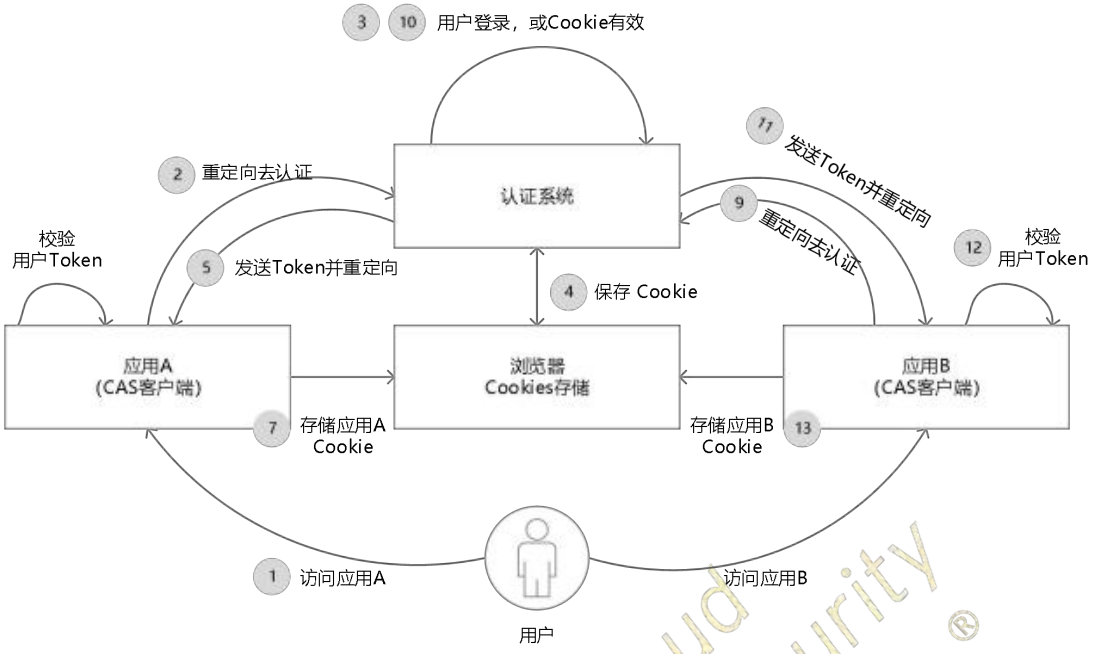
证书代理模块负责统一身份模块和证书服务器之间的用户/应用系统信息的实时同步，保证系统中用到的用户/应用系统信息和证书服务器上的信息一致。

二、实现 SSO 的主要技术

(1) 基于 Cookies

用户登录系统之后，用户的身份认证信息记录到 Cookies 中。当用户要访问应用服务器提供的资源时，应用服务器从 Cookies 获取信息来验证用户身份。而基于浏览器的 B/S 架构的 Web 应用主要采用此方法实现单点登录，大家所熟知的 CAS 就是基于此方法实现，是当前普遍用到的实现 Web 应用的单点登录方法。

基于 CAS 的单点登录系统分为服务端和客户端，它们分别负责全局会话的保持和局部会话的保持。服务端即认证系统，负责全局会话的创建、销毁和验证；客户端将集成到业务系统内，负责局部会话的创建、销毁和验证。如下图所示，展示了 CAS 单点登录系统的单点登录的认证逻辑交互图。



用户首次访问时，重定向到认证系统登录页，返回登录表单给浏览器，用户提交用户名和口令，认证系统验证后，在认证系统域名下设置全局 Cookie，成功后携带 ticket 重定向到应用系统（CAS 客户端），CAS 客户端向认证系统验证 ticket 有效性，返回验证信息，CAS 客户端创建局部会话 Cookie，重定向回原地址，应用系统返回资源。

第二次访问该系统，会在该域名下存上一步写的 Cookie，请求该系统时携带 Cookie，所有 filter 不会拦截请求，直接返回资源。

用户首次访问其他应用时，该应用域名下不存在局部会话，所以重定向到认证系统进行登录认证，此时访问服务端的请求中携带了全局 Cookie，认证系统发现此客户端已经登录，所以生成 ticket 并重定向回 CAS 客户端，CAS 客户端向认证系统验证 ticket 有效性，返回验证信息，CAS 客户端创建局部会话 Cookie，重定向回原地址，应用系统返回资源。

CAS 非常方便有效的实现了浏览器与应用之间的资源访问的认证与授权，随着业务的发展，应用与应用之间存在互相访问的情况越来越多，CAS 早期不支持该功能，应用间的资源互访通常采用 SOAP 协议、或 OAuth 等协议来完成。而在 CAS 的后续版本中提供了代理模式，同样支持应用间的资源访问认证与授权。

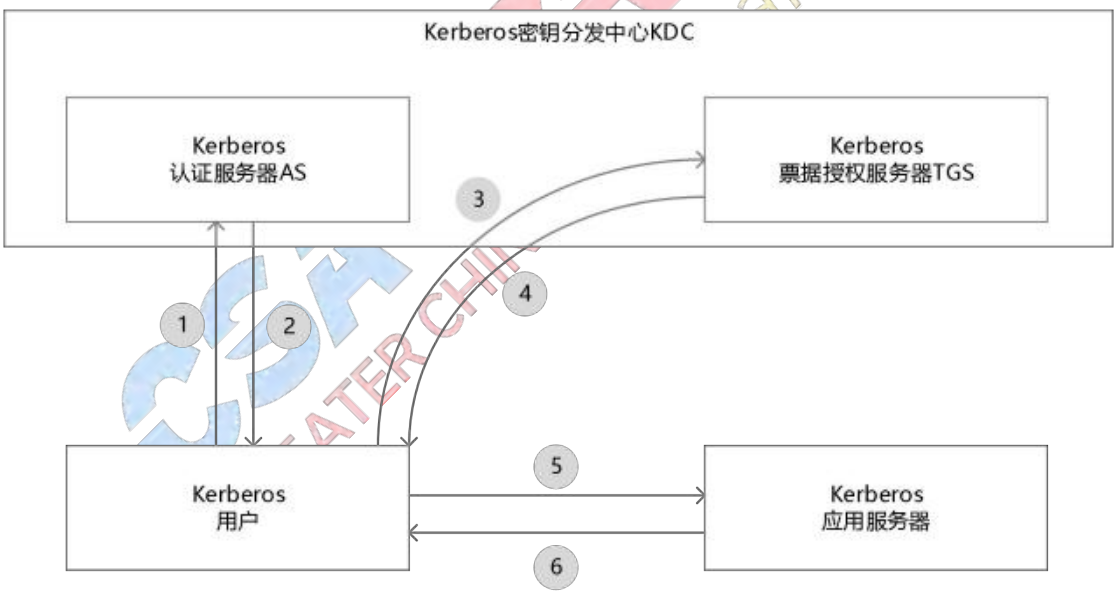
(2) 基于经纪人（Broker-based）

该方法是一种特定服务器（称为认证服务器）专门对用户进行统一身份认证和统一身份管理。而且给用户分发一个数字身份标识供访问应用服务器时使用。它介于用户和

应用服务器之间，以经纪人的身份负责验证用户的身份。由于经纪人可以存储用户的电子身份和认证信息，因此为数据库减轻了管理工作，且为用户身份认证提供了“可信赖的第三方”。例如 Kerberos、Sesame、IBM KryptoKnight（凭证库思想）等都采用了此方法实现单点登录，适用于 C/S 模型。

Kerberos 是一种基于对称密钥技术的身份认证协议，它作为一个独立的第三方身份服务，可以为其他服务提供身份认证功能，且支持 SSO（即客户端身份认证后，可以访问多个服务）。它使用了一个由认证服务器和票据授权服务器组成的密钥分发中心（KDC）。网络上的所有实体都和密钥分发中心共享了一套密钥。由于该密钥只有实体本身和密钥分发中心才能知道，因此可以证明实体的真实身份。密钥分发中心分为两个相互通信的实体，生成一个会话密钥，该会话密钥可以加密实体之间互相传输的消息。Kerberos 认证机制的核心工作基于能够证明用户身份的票据，可以保护实体免受窃听和重放攻击。

Kerberos 的认证流程包括 6 个步骤，如下图所示：



1) 用户首先向 Kerberos 认证服务器 AS 请求一个可以跟票据授权服务器进行通信的票据及会话密钥。用户向 AS 发送认证请求，请求信息包含用户唯一标识和票据授权服务器标识，申请可以跟票据授权服务器通信的票据和会话密钥。
2) Kerberos 认证服务器 AS 验证该用户的唯一标识是否存储在数据库中，如果数据库中有记录，则生成一个 Client——TGS 会话密钥，并使用 Client——AS 的会话密钥加

密；且生成用于用户访问 TGS 的票据许可票据 TGT，使用票据授权服务器的密钥对其加密，并将此消息一起返回给请求的客户端用户。

3) 用户接收认证服务器返回的信息后，解密获得用于跟票据授权服务器通信的会话密钥，然后向票据授权服务器发送用于认证的票据许可票据和访问请求消息，该访问请求消息使用 Client——TGS 的会话密钥加密。

4) 票据授权服务器使用会话密钥解密接收到的消息，根据解密得到的时间戳验证用户的身份。如果验证用户身份成功，就产生一个用于客户端用户和应用服务器通信的会话密钥并向用户签发服务许可票据 ST，这些信息都使用票据授权服务器和用户之间的会话密钥进行加密。

5) 用户解密票据授权服务器发来的信息，得到与应用服务器通信的会话密钥，并向远端应用服务器提交服务许可票据 ST 和用户自己生成的认证信息。

6) 应用服务器比较用户发送的服务许可票据 ST 里的信息和认证信息。如果两者中包含的基本信息相同，就向用户提供相应的服务。用户接收到应用系统的确认信息后，对其解密获得时间戳并验证其合法性，从而应用服务器的身份也可以得到反向认证。

(3) 基于代理（Agent-based）

该方法提供了一个代理程序，布置在各个应用服务器之前用于自动替各个应用服务器验证用户的身份。代理程序可以布置在客户端，替用户发送身份认证请求，减少客户端应用程序的认证工作；代理程序也可以布置在应用服务器上，介于应用服务器的认证系统和客户端认证方法之间扮演一个翻译的角色。例如 SSH（SecureShell）采用的就是基于代理的方法。

(4) 基于代理和经纪人（Agent and Broker-based）

该方法是上述（2）和（3）的有效结合。基于代理的方法最突出的有点是可以减轻应用程序的改造负担，基于经纪人的解决方案最突出的优点是可以把认证工作集中起来，而基于代理和经纪人的解决方案具备了基于经纪人方法的集中认证和基于代理减少对应用程序改造的优点，因此具有很明显的优势，是普遍用到的实现单点登录的方法。

(5) 基于网关（Gateway-based）

在这中解决方案中，客户端一定要用网关软件，只有通过特定的网关才可以使用各种应用服务器提供的受保护资源，网关将一切应用都隔离出来。客户端可以使用各种应

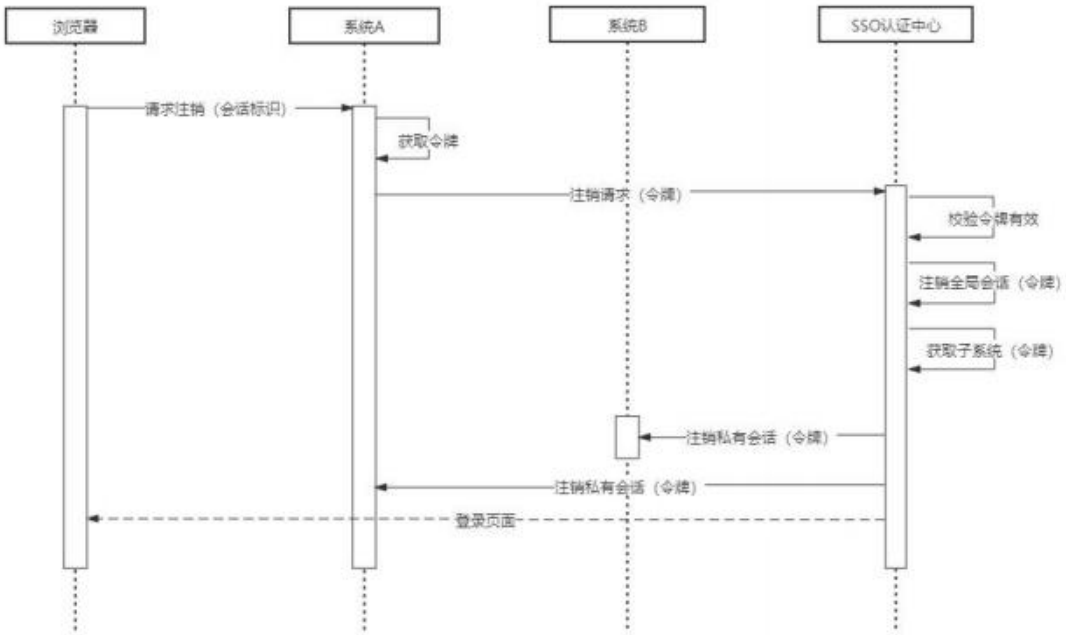
用服务器提供的受保护资源，网关将一切应用都隔离出来。客户端用户成功通过网关的身份认证之后才可以得到访问引用服务器的权限。若可以使用 IP 地址识别置于网关背后的应用服务，则能够在网关上创建一个基于 IP 地址的响应规则，如果将该响应规则和网关上的存储用户信息的数据相结合，则可以利用网关实现单点登录。网关将客户端用户的身份信息记录下来，避免重复的认证请求处理和授权请求处理。

(6) 基于令牌（Token-based）

Security Dynamics SecurID 是一个物理的令牌模型，该模型由用户身份识别码即 PIN（Personnel Identification Number）和一个小型的数字发生器组成。首先设定一个时间间隔，并在该时间间隔内，数字发生器生成一个跟令牌唯一对应且只能由一个程序接受的密码，该数字发生器的时钟应该与提供身份鉴别的叫做 ACE 的服务器的时钟保持同步。

三、单点登出

单点登出的关键在于统一身份认证中心要实时监控全局会话的状态，当全局会话注销时，需要及时通知所有关联子系统注销局部会话；若某子系统局部会话销毁后，要及时通知统一身份认证中心去销毁全局会话。单点登出的时序图如下图所示：



5 访问控制与权限管理

5.1访问控制模型说明

5.1.1 访问控制的概念和作用

访问控制是按主体身份及其所归属的某项定义组来限制主体对某些资源或功能的使用的一种技术。对于访问控制，NIST 有如下定义：“访问是一种利用计算机资源去做某件事情的的能力，访问控制是一种手段，通过它这种能力在某些情况下被允许或者受限制（通常是通过物理上和基于系统的控制）。”

访问控制的目的就是确保特定的数据和资源能够在合适的时间和地点，被合适的主体正确地访问和利用。访问控制主要有以下作用：

1. 防止非法主体进入受保护的网络（区域）；
2. 允许合法主体访问受保护的网络资源；
3. 防止合法主体对受保护的网络资源进行非授权的访问。

IAM、权限管理、访问控制三者的关系：

IAM（身份和访问管理）是一种集中式的数字身份管理和资源访问授权的机制，用于授予或拒绝用户对系统的访问，并确定可以授予他们的访问级别（如只读、读写、执行等）。IAM 的目的是控制主体对客体的访问，以防止未经授权的数据泄露和修改。IAM 包括四个步骤：标识、认证、授权和问责。

权限管理是对主体和客体之间的交互关系进行控制和调节的机制，对应 IAM 的授权过程。

访问控制是为保护网络资源不被非法和非授权访问而采取的措施，可以完全独立于 IAM 实现，但是当需要对访问主体进行身份认证和权限管理时，会与 IAM 之间发生交互，而权限管理则通常被视为访问控制的基础。

5.1.2 主要的访问控制模型

访问控制模型是规定主体如何访问客体的一种架构。1985 年美国军方发布《可信

计算机系统评估准则》（Trusted Computer System Evaluation Criteria，TCSEC，也称“桔皮书”），描述了两种著名的访问控制模型，自主访问控制（DAC）和强制访问控制（MAC）。20 世纪 90 年代，大量专家学者和研究机构先后提出了不同类型的基于角色的访问控制模型（RBAC），其中美国 George Mason 大学信息安全技术实验室（LIST）提出的 RBAC96 模型得到了广泛认可。近年来，业内出现了一种基于属性的访问控制模型(ABAC)，被认为是可以弥补 RBAC 不足的新一代访问控制技术。随着动态安全能力越来越受到业界的关注，美国国家安全局（NSA）提出了一种风险自适应的访问控制模型（RAdAC）。本节将着重对上述访问控制模型进行说明。

5.1.3 自主访问控制（Discretionary Access Control，DAC）

自主访问控制（Discretionary Access Control，DAC）是根据主体（如用户、进程或 I/O 设备等）的身份及其所属的组来限制其对客体的访问。所谓的自主，是因为对某个客体拥有控制权的主体可以直接（或间接）地将对该客体的一种或多种访问权自主地授予其他主体，并在随后的任何时刻将这些权限回收。自主访问控制中，用户可以针对被保护对象制定自己的保护策略。

1、DAC 的具体实现

- 访问控制列表（Access Control List，ACL）

ACL 是最早也是最基本的一种自主访问控制实现方式。它的原理非常简单：每一项资源，都配有一个列表，这个列表记录的就是哪些用户可以对这项资源执行哪些操作（只读/读写/执行等）。当用户试图访问这项资源时，系统会首先检查这个列表中是否有关于当前用户的访问权限，从而确定当前用户可否执行相应的操作。总的来说，ACL 是一种面向资源的访问控制模型，它的控制或保护机制是围绕“资源”展开的。

例如，对于一个文件对象，有如下的 ACL：

File1	
Alice	read, write
Bob	read

表示 Alice 可以对该文件进行读写操作，Bob 只能读取。

由于 ACL 的简单性，使得它几乎不需要任何基础设施就可以完成访问控制。但同时它的缺点也是很明显的，一方面，由于需要维护大量的访问权限列表，ACL 在性能上有

明显的缺陷；另一方面，对于拥有大量用户与众多资源的应用，管理访问控制列表本身已变成非常繁重的工作。

- 访问控制矩阵（Access Control Matrix，ACM）

ACM 是通过矩阵形式描述主体和客体之间的权限分配关系。对每个主体而言，都拥有对哪些客体的哪些访问权限；而对客体而言，又有哪些主体可以对它实施访问；将这种关连关系加以阐述，就形成了访问控制矩阵。其中，特权用户或特权用户组可以修改主体的访问控制权限。

	Asset 1	Asset 2
Role 1	read, write, execute, own	execute
Role 2	read	read, write, execute, own

访问控制矩阵的实现很易于理解，但是查找和实现起来有一定的难度，而且，如果用户和文件系统要管理的文件很多，那么控制矩阵将会成几何级数增长，这样对于增长的矩阵而言，会有大量的空余空间。

- 访问控制能力列表（Access Control Capabilitis List，ACCL）

能力是访问控制中的一个重要概念，它是指请求访问的发起者所拥有的一个有效标签（ticket），它授权标签表明的持有者可以按照何种访问方式访问特定的客体。ACCL 是以用户为中心建立的访问权限表，其实现与 ACL 正好相反。

UserA	
File1	read, write
File2	read

定义能力的重要作用在于能力的特殊性，如果赋予哪个主体具有一种能力，事实上是说明了这个主体具有了一定对应的权限。能力的实现有两种方式，可传递的和不可传递的。一些能力可以由主体传递给其他主体使用，另一些则不能。

2、DAC 的典型应用场景

DAC 常见于文件系统，LINUX，UNIX、WindowsNT 版本的操作系统都提供 DAC 的支持。在实现上，先对用户鉴权，然后根据控制列表决定用户能否访问资源。用户控制权限的修改通常由特权用户或者管理员组实现。

3、DAC 的不足之处

DAC 最大缺陷就是对权限控制比较分散，比如无法简单地将一组文件设置统一的权

限开放给指定的一群用户。同时，由于资源所有者（特权用户）的权限太大，无意间就可能泄露信息。此外，一旦系统遭遇特洛伊木马攻击，并且攻击者成功获取了特权账户权限，则系统中所有资源都将遭到侵害。

5.1.4 强制访问控制（Mandatory Access Control，MAC）

MAC 是为了弥补 DAC 权限控制过于分散的问题而诞生的。在 TCSEC 中有如下定义："一种限制访问客体的手段，它以包含在这些客体中的信息敏感性和访问这些敏感性信息的主体的正式授权信息（如清除）为基础"。

1、MAC 策略

在 MAC 模型中，主体和客体分别被赋予一定的安全级别，主体能否访问客体由双方安全级别之间的关系决定。MAC 通常具有系统硬性限制，即系统强制主体服从访问控制策略，是一种强加给访问主体的访问方式。

MAC 利用下读/上写来保证数据的保密性,利用上读/下写来保证数据的完整性。

（1）向下读（rd，read down）：主体安全级别高于客体信息资源的安全级别时允许查阅的读操作；

（2）向上读（ru，read up）：主体安全级别低于客体信息资源的安全级别时允许的读操作；

（3）向下写（wd，write down）：主体安全级别高于客体信息资源的安全级别时允许执行的动作或是写操作；

（4）向上写（wu，write up）：主体安全级别低于客体信息资源的安全级别时允许执行的动作或是写操作。

2、MAC 安全标签

安全标签是附加在主体和客体上的一组安全属性信息。MAC 为访问主体和受控对象（客体）提供两类安全标签，一类是具有偏序关系的安全等级标签，另一类是非等级化的分类标签，它们是实施强制访问控制的基本依据。系统通过比较主体和客体的安全标签来决定一个主体是否能够访问某个客体。用户程序不能更改它自己以及任何其他客体的安全标签。

多级安全（MultiLevel Secure, MLS）是最常见的强制访问控制策略。在实际的应用中，可以通过访问控制标签列表（ACSLL）来限定一个用户对一个客体目标访问的安全

属性集合。当用户在请求访问一个客体时，系统会判断它的安全级别是比所请求访问的客体高还是低，如果低的话，拒绝访问，如果高的话可以访问。通过分级的安全标签实现了信息的单向流通。

3、MAC 模型举例

MAC 模型中最著名的是 Bell-LaPadula 模型和 Biba 模型，其他较为常见的模型如 Chinese Wall 模型等。以下分别进行简单介绍。

（1）Bell-LaPadula（BLP）模型

Bell-LaPadula 模型通常是处理多级安全信息系统的设计基础，客体在处理绝密级数据和秘密级数据时，要防止处理绝密级数据的程序把信息泄露给处理秘密级数据的程序。BLP 模型的出发点是维护系统的保密性，具有只允许向下读（即不上读，NRU）、向上写（即不下写，NWD）的特点，可以有效地防止机密信息向较低安全级别的系统泄露。

（2）Biba 模型

Biba 模型是和 BLP 模型相对立的模型，Biba 模型改正了被 BLP 模型所忽略的信息完整性问题，但在一定程度上却忽视了保密性。Biba 模型使用不下读（NRD）、不上写（NWU）的原则来保证数据的完整性，在实际的应用中主要是避免应用程序修改某些重要的系统程序或系统数据库，这样可以使资源的完整性得到保障。

（3）Chinese Wall 模型

Chinese Wall 模型一般是用于多边安全系统（也就是多个组织间的访问控制系统）中的安全模型，应用在可能存在利益冲突的组织中，最初是为投资银行设计的。Chinese Wall 模型有两条基本原则：一是用户必须选择一个它可以访问的区域；二是用户必须自动拒绝来自与用户所选区域的利益有冲突的其他区域的访问。这种工作模式同时包含了 DAC 和 MAC 的属性，银行家可以选择为谁工作（DAC），一旦选择了之后，它就只能为这个客户工作(MAC)。一个典型的例子就是防火墙内部与外网相连的一台服务器，假如这台服务器暴露在外网之中，那么就禁止其转发数据，也就是说该服务器只能与外网通信，不能与内部网络通信。

4、MAC 的优缺点

MAC 策略一旦被制定，用户无法改变它。这种访问控制模型可以增强系统的安全性，因为它基于策略，任何没有被显式授权的操作都不能执行。MAC 一般在最重视保

密性的机构或者其他等级观念强烈的行业中进行开发和实现，如军事系统。

MAC 的主要问题在于：

实现工作量较大,授权管理不方便,不够灵活。

过于强调保密性，对系统连续工作能力（可用性）方面考虑不足。

5.1.5 基于角色的访问控制（Role-Based Access Control, RBAC）

RBAC 是实施面向企业安全策略的一种有效的访问控制方式。其基本思想是，对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限。将用户和权限进行分离，彼此相互独立，使权限的授予更加灵活。管理员不必在每次创建用户时都进行分配权限的操作，只要分配用户相应的角色即可，而且角色的权限变更比用户的权限变更要少得多，这样将简化用户的权限管理，减少系统的开销。

1、RBAC 支持的安全原则

- RBAC 支持以下公认的安全原则：最小特权原则、责任分离原则和数据抽象原则。
- 最小特权原则：通过限制分配给角色的权限的多少和大小来实现，分配给某用户对应角色的权限只要不超过该用户完成其任务的需要即可；
- 责任分离原则：通过在完成敏感任务过程中分配两个责任上互相约束的两个角色来实现，例如在清查账目时，需要设置财务管理员和会计两个角色同时参加。
- 数据抽象原则：借助于抽象许可权的概念实现，如在账目管理活动中，可以使用信用、借方等抽象许可权，而不是使用操作系统提供的读、写、执行等具体的许可权。
- RBAC 并不强迫实现这些原则，安全管理员可以配置 RBAC 模型使其不支持这些原则。因此，RBAC 支持数据抽象的程度与 RBAC 模型的实现细节有关。

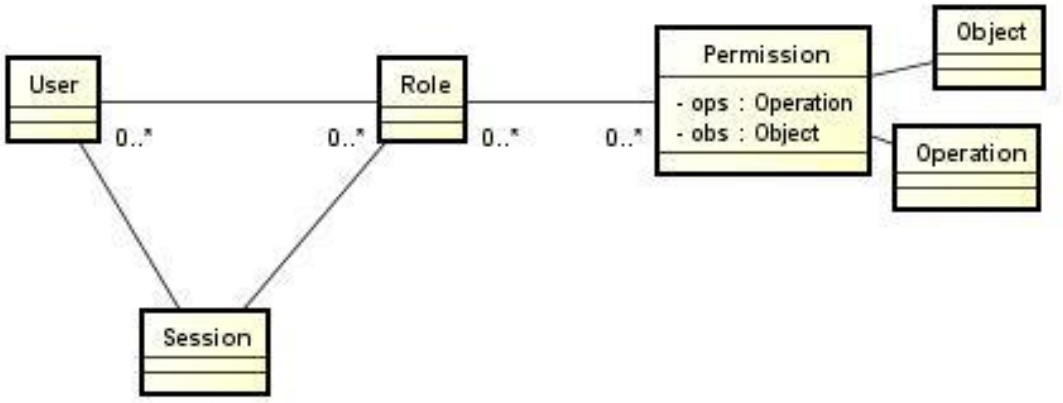
2、RBAC 概念模型

业界广为认可的 RBAC96 是一个模型族，其中包括 RBAC0~RBAC3 四个概念性模型。

（1）基本模型 RBAC0

RBAC0 定义了能构成一个 RBAC 控制系统的最小元素集合。RABC0 是 RBAC 的核心，其他版本都是建立在 RBAC0 的基础上的。

RBAC0 模型中包括用户（User）、角色（Role）、会话（Session）和权限（Permission）等 4 类实体集合。其中权限包括操作（Operation）和对象（Object）两个元素。下图展示了用户、角色、访问权限和会话之间的关系。

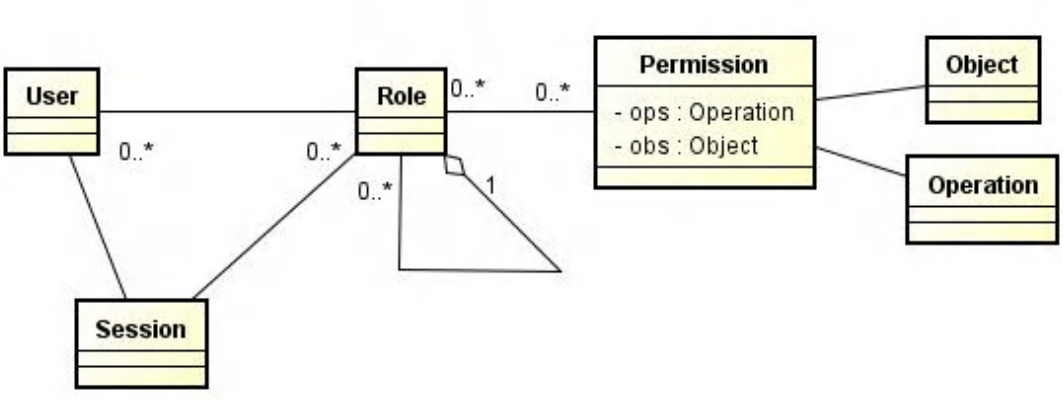


每个角色至少具备一个权限，每个用户至少扮演一个角色；可以对两个完全不同的角色分配完全相同的访问权限；会话由用户控制，一个用户可以创建会话并激活多个用户角色，从而获取相应的访问权限，用户可以在会话中更改激活角色，并且用户可以主动结束一个会话。

用户和角色可以是多对多的关系，权限和角色也是多对多的关系。一个用户在不同的场景下可以拥有不同的角色，例如项目经理也可以是项目架构师等；当然一个角色可以给多个用户，例如一个项目中有多个组长，多个组员等。一个角色可以拥有多份权限，同一个权限也可以授给多个角色。

（2）高级模型 RBAC1

RBAC1 在 RBAC0 模型基础上增加了角色分级的概念，即角色之间存在上下级的关系。同时引入角色间的继承关系，一个角色可以从另一个角色继承权限，并且在拥有其他角色权限的同时，自己还可以关联额外的权限。这种设计可以给角色分组和分层，一定程度简化了权限管理工作。

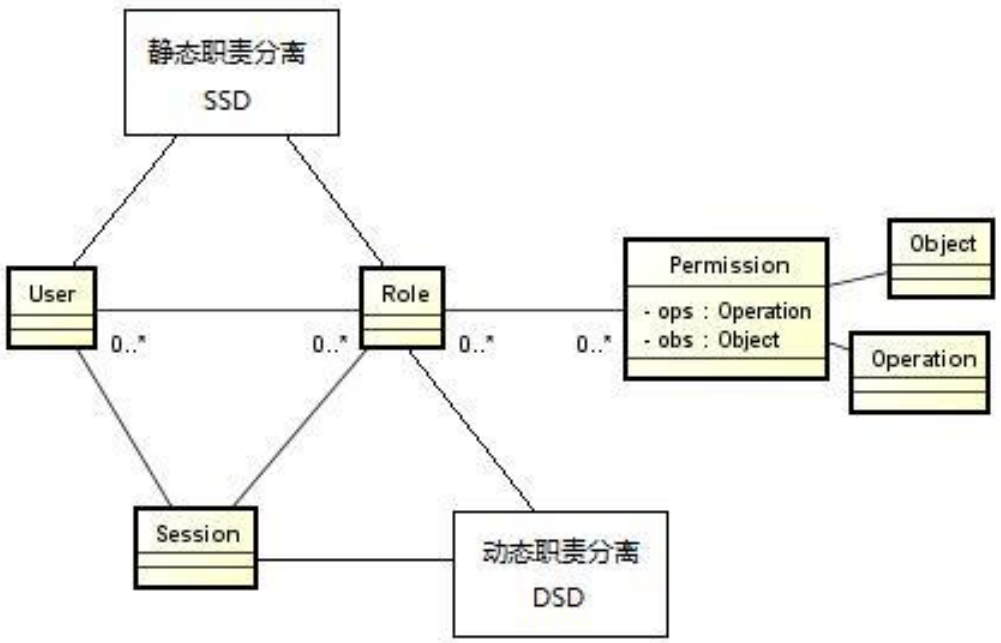


角色间的继承关系可分为一般继承关系和受限继承关系。一般继承关系仅要求角色继承关系是一个绝对偏序关系，允许角色间的多继承。而受限继承关系则进一步要求角色继承关系是一个树结构，实现角色间的单继承。

（3）高级模型 RBAC2

RBAC2 在 RBAC0 基础上增加了一些限制，强调 RBAC 的不同组件在配置方面的一些限制。

RBAC2 模型中添加了职责分离关系。RBAC2 的约束规定了权限被赋予角色时，或角色被赋予用户时，以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。职责分离包括静态职责分离 (Static Separation of Duty，SSD)和动态职责分离 (Dynamic Separation of Duty，DSD)。



SSD 是用户和角色的指派阶段（授权阶段）加入的，主要是对用户和角色有如下约

束:

a、互斥角色：同一个用户在两个互斥角色中只能选择一个，例如要么是会计，要么是出纳，不能兼任；

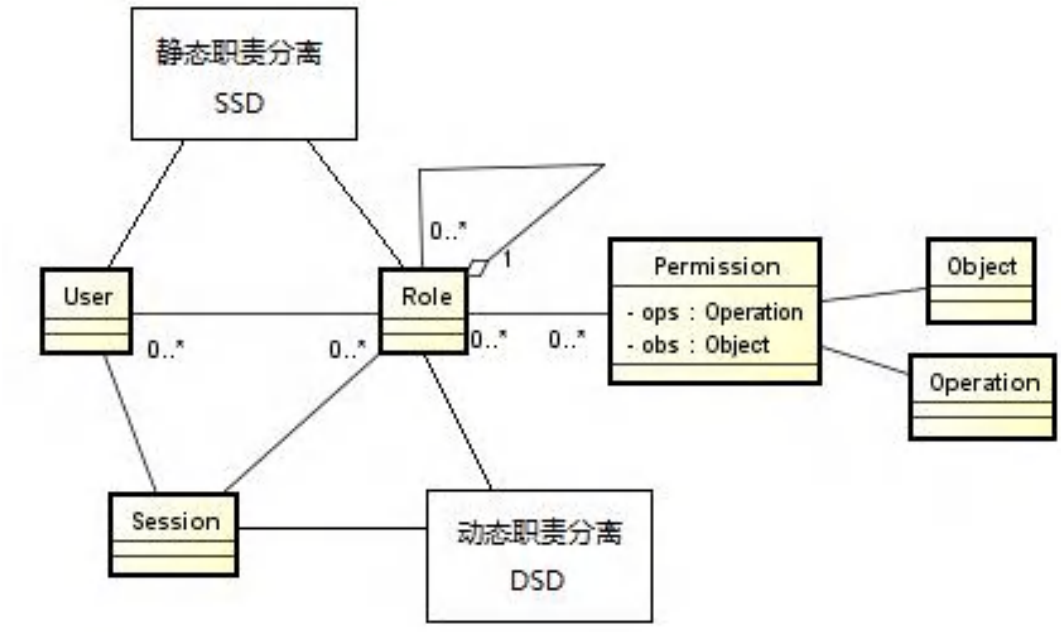
b、基数约束：一个用户拥有的角色是有限的，一个角色拥有的权限也是有限的，例如一个公司的领导岗位是有限的，每个领导岗的权限也是有限的；

c、先决条件约束：用户想要获得高级角色，首先必须拥有低级角色，例如先要成为经理，之后才能升为总监。

DSD 是会话和角色之间的约束，可以动态的约束用户拥有的角色，例如一个用户可以拥有两个角色，但是运行时只能激活一个角色。

（4）统一模型 RBAC3

RBAC3 包含了 RBAC1 和 RBAC2，利用传递性，也把 RBAC0 包括在内。这些模型就构成了 RBAC96 模型族。



3、RBAC 的优缺点

RBAC 相对于 ACL 最大的优势就是它简化了用户与权限的管理，通过对用户进行分类，使得角色与权限关联起来，而用户与权限变成了间接关联。RBAC 模型使得访问控制，特别是对用户的授权管理变得非常简单和易于维护，因此有广泛的应用。但是它也有自身的缺点，那就是由于权限是以角色为载体分配的，如果某一角色下的个别用户需要进行特别的权限定制，如同加入一些其他角色的小部分权限或去除当前角色的一些权

限时，RBAC 就无能为力了。此外，由于 RBAC 模型没有提供操作顺序控制机制，使得 RBAC 模型很难应用于那些要求有严格操作次序的实体系统，例如在购物控制系统中要求系统对购买步骤进行控制，在客户未付款之前不应让他把商品拿走，RBAC 模型对此也无能为力。

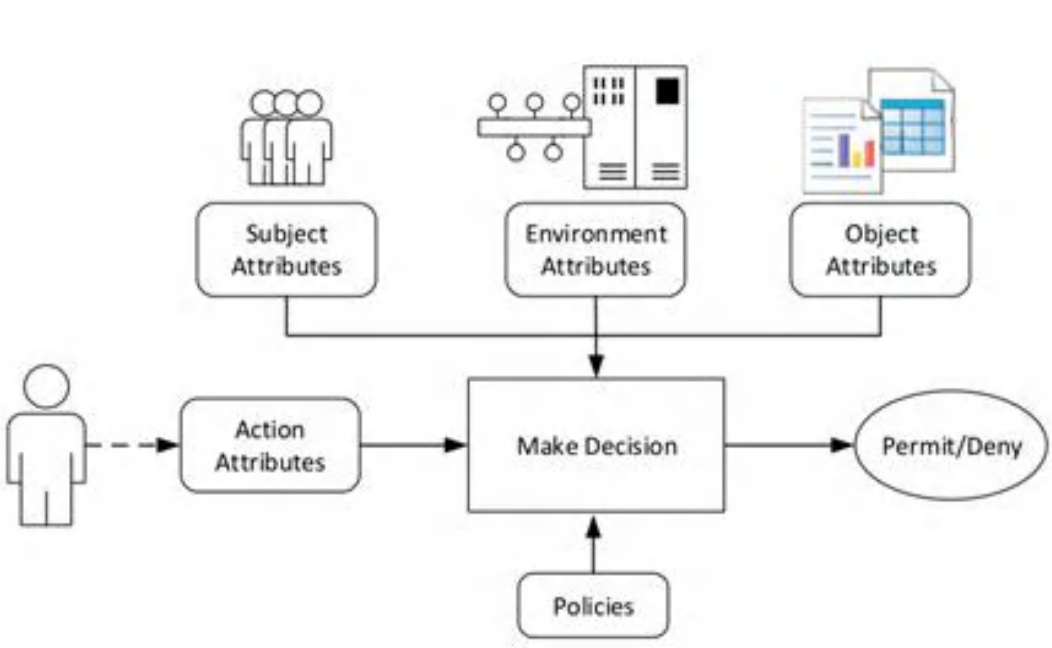
5.1.6 基于属性的访问控制（Attribute-Based Access Control, ABAC）

ABAC 是一种为解决行业分布式应用间可信关系的访问控制模型,它能够解决开放网络环境下资源保护所面临的细粒度问题以及网络系统所面临的大规模用户问题，为未来的开放网络环境提供了较为理想的访问控制策略方案。

1、ABAC 基本概念

现实中的实体可以通过实体特性（组合）来进行有效区分，这种可以对实体进行区分的实体特性称为实体属性。ABAC 利用相关实体(如主体、客体、环境)的属性作为授权的基础来研究如何进行访问控制。使用实体属性这个核心概念对主体、客体、权限及授权约束进行统一描述，用属性或属性组来区分不同的实体，用实体属性之间的关系对安全需求进行形式化建模，以期有效解决分布式开放环境下的细粒度访问控制和大规模用户动态扩展问题。

基于这样的目的,可将实体的属性分为四类：主体属性（如用户名、所在部门、所在用户组、职务、年龄等），环境属性（如访问客户端 IP、当前时间等），行为属性（如读取、修改、添加、删除等）和对象属性（如 URL、文件、数据库表、分类分级标签等),这与传统的基于身份的访问控制（IBAC）不同。在基于属性的访问控制（ABAC）中，访问判定是基于请求者和资源具有的属性，请求者和资源通过属性来标识，而不像 IBAC 那样只通过 ID 来标识，这使得 ABAC 具有足够的灵活性和可扩展性，同时使得安全的匿名访问成为可能，这在大型分布式环境下是十分重要的。



图：NIST 的 ABAC 模型

ABAC 把实体属性（组）概念贯穿于访问控制策略、模型和实现机制中，把与访问控制相关的时间、实体空间位置、实体行为、访问历史等信息当作主体、客体、权限和环境的属性来统一建模，通过定义属性之间的关系描述复杂的授权和访问控制约束，能够灵活的进行访问控制。不同于常见的将用户通过某种方式关联到权限的方式，ABAC 是通过动态计算一个或一组属性是否满足某种条件来进行授权判断的，更适合大规模用户场景的使用需要。目前 ABAC 已经应用于 WEB 服务、网格计算、信息共享和消息管理中。

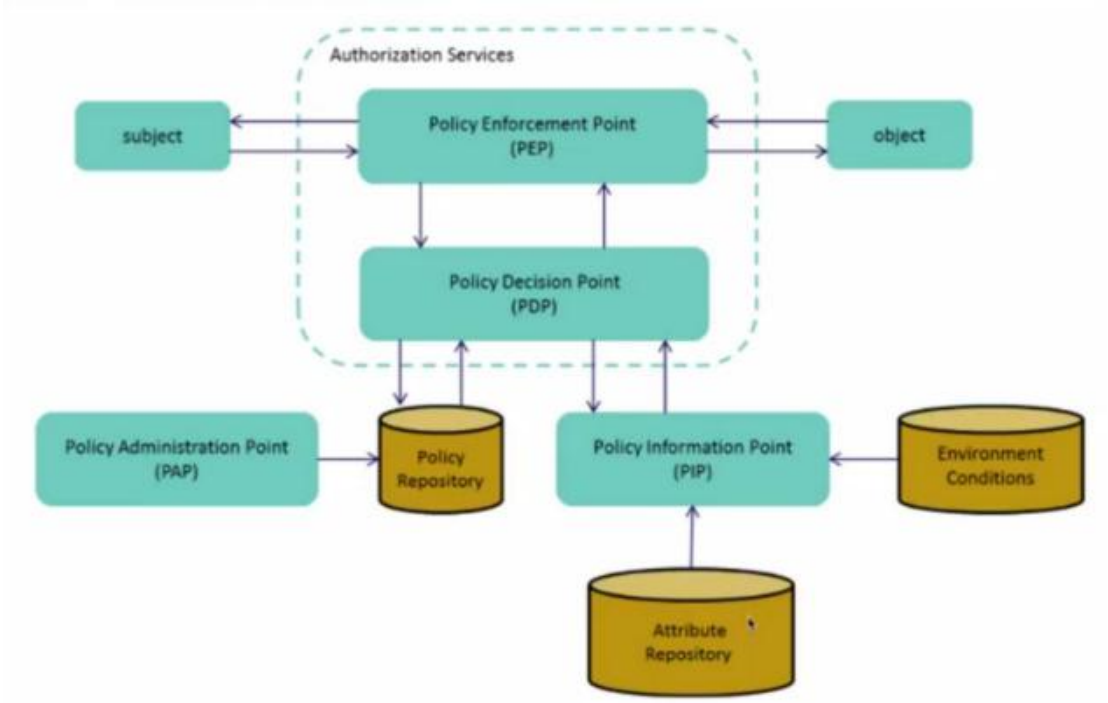
2、ABAC 体系结构

ABAC 的参考体系结构如图所示，该体系结构包括策略执行点（PEP）、策略决策点（PDP）、策略信息点（PIP）和策略管理点（PAP）四个服务节点。此外，PDP 和 PEP 功能可以是分布式的或集中式的，它们构成所谓的授权服务（AS）。对于访问请求，此体系结构的工作流描述如下：

（1）PEP 从经过身份验证的主体截获访问请求，并将该请求发送到 PDP。

（2）PDP 根据 PAP 生成的访问策略和查询 PIP 得到的主题、对象、环境等属性进行访问决策。

（3）PDP 给出的最终决策结果被发送给 PEP，然后 PEP 根据 PDP 的决策完成访问请求。

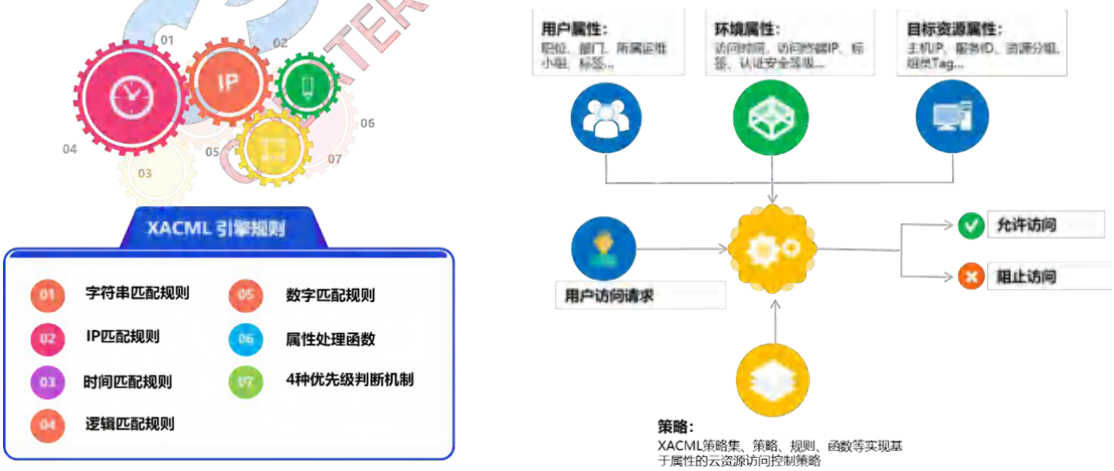


图：NIST 的 ABAC 参考体系结构

上述体系结构中还包括两个存储库和多个环境感知模块。两个存储库分别存储和管理公共访问规则和实体属性，环境感知模块可以获取与请求相关的当前时间的环境信息，其中这些信息可以包括当前时间、位置、威胁级别、设备类型等。

3、ABAC 实现方法

可扩展访问控制标记语言(Extensible Access Control Markup Language，XACML)是目前 ABAC 唯一的国际公开标准，已经在全球范围内被广泛采用，XACML 灵活的扩展性及丰富的规则及函数是实现复杂访问控制规则的科学选择。



图： 基于 XACML 的 ABAC 策略

XACML 支持多种逻辑表达式和属性类型，具有很强的策略表达能力，非常适合对

这种细粒度的大数据存储访问控制模型进行授权描述。同时具有可扩展性，能够支持大数据环境下的灵活、动态访问控制的需求。

4、ABAC 优缺点

ABAC 具有如下优点：

- 支持集中化管理；
- 可以按需实现不同颗粒度的权限控制；
- 不需要预定义判断逻辑，减轻了权限系统的维护成本，特别是在需求经常变化的系统中；

缺点则包括：

- 权限判断需要实时执行，规则过多会导致性能问题；
- 定义权限时，不能直观看出用户和对象间的关系，规则如果稍微复杂一点，或者设计混乱，会给管理者维护和追查带来麻烦。

跟 RBAC 相比，ABAC 对权限的控制粒度更细，如控制用户的访问速率。但是由于 ABAC 实现相对复杂，目前仍无法完全取代 RBAC。实际开发中可以结合 RBAC 角色管理的优点和 ABAC 的灵活性一起使用。

5.1.7 风险自适应访问控制（(RAdAC,Risk-Adaptable Access Control)）

在大规模应用场景中，安全管理员可能缺乏足够的专业知识，无法准确地为用户指定其可以访问的数据。风险自适应的访问控制是针对这种场景的有效解决方法。

1、RAdAC 概述

风险自适应访问控制（Risk-Adaptable Access Control，RAdAC）是美国国家安全局（NSA）研究的下一代动态访问控制方法，能够根据当前平台状态以及特殊情况灵活动态地对用户进行授权，给用户提供最严格的访问策略。由于系统在不同状态下（如网络繁忙、系统异常、用户违规操作、数据传输出错等）的访问安全风险是不一样的，因此，RAdAC 能提供动态的多级安全（Multi Level Security，MLS）级别的访问。RAdAC 具备动态分析安全风险和操作需求的能力，能够对分布式平台的访问安全风险进行评估，并与用户进行交互以确认其访问资源的必要性，最后综合两者对用户访问权限进行判定。

2、RAdAC 实现方法

RAdAC 是一种动态访问控制机制，通过实时评估用户操作需求并计算授权访问风险来动态调整访问控制策略。RAdAC 包含以下三部分：安全风险测量（Security Risk Measurement，SRM）、操作需求测定（Operational Need Determination，OND）以及最终访问决定（Final Access Decision，FAD）。

- 安全风险测量（SRM）：SRM 会根据用户的操作行为、用户状态、环境因素、上下文、访问目标特征等多种特性通过阈值判定、加权等计算方式得出本次访问风险值（实际是一个风险范围）。同时 SRM 还需具备一定的机器自学能力，例如当用户在操作中多次访问核心数据资源，则必须提高风险等级。
- 操作需求测定（OND）：OND 使得用户在特殊情况下能够超越风险判定访问某资源。传统方式下，用户属于一个部门或者拥有某几个角色，能够访问的资源都是固定的，但是在紧急情况或者风险较大的时候，用户可能需要拥有超过自身权限的访问能力。系统需要结合用户权限和访问要求来得到最后的操作需求判定。
- 最终访问决定（FAD）：FAD 根据 SRM 和 OND 的结果，通过访问决定函数（Access Decision Function，ADF）来做出最终结果。由于用户每次操作的风险值和需求都是变化的，因此在多级安全系统中，用户的最终访问结果并不是固定的。FAD 的结果是二进制值，允许或拒绝。

3、RAdAC 优点

与当前较流行的 RBAC 算法相比，RAdAC 具有如下优点：

（1）平台扩展性好：RAdAC 可以在数据库或 XACML 的基础上，增加对平台安全性、用户属性的判定，依据相应的判定函数实施访问判决，克服了传统方式下的缺陷。

（2）策略灵活：目前大部分平台的安全策略工作采用 XACML 提供的集中式策略合成算法，为了数据的安全访问，往往直接遵守最小特权原则（deny override），无法根据具体情况作出不同判断。RAdAC 根据当前风险等级和操作需求，灵活确定资源访问权限，在保证数据安全的同时，尽可能满足访问需求。

5.1.8 基于策略的访问控制（Policy-Based Access Control，PBAC）

PBAC 是当前和未来的最佳授权方法，因为 PBAC 结合了 RBAC 和 ABAC 的最佳特性。PBAC 是 IAM 架构现代化的核心。

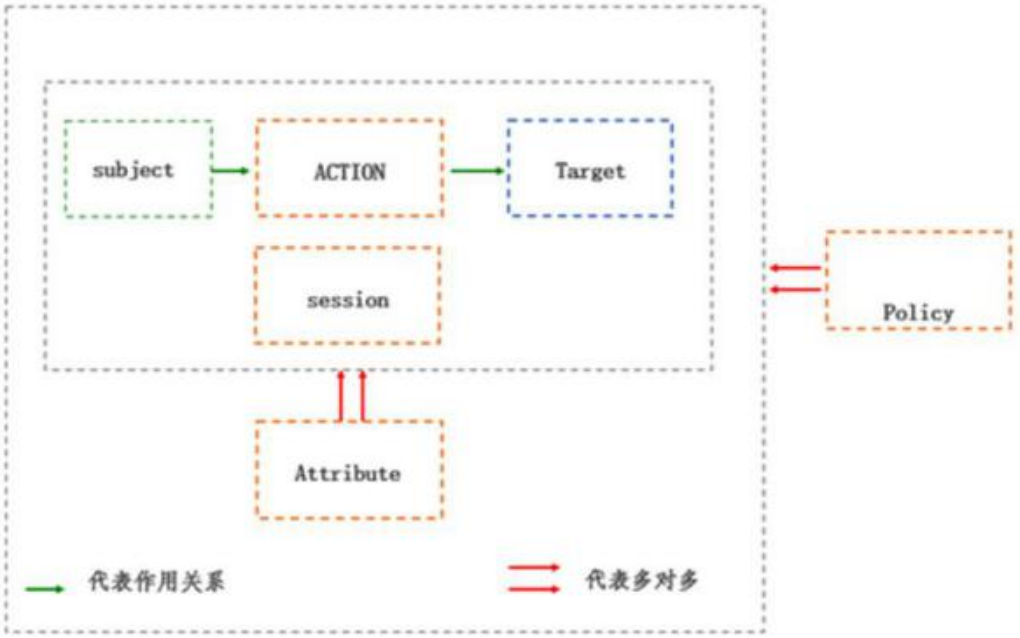
1、PBAC 基本概念

PBAC 是一种以策略为核心，用策略控制系统访问会话请求的安全模型。PBAC 描述了如何依据一个集中的策略池来确定某个主体是否有权限访问某个对象。

PBAC 涉及的内容有两个方面：一方面是访问控制技术，它包括会话特性的描述管理、会话实体的逻辑关系刻划等；另一方面是基于策略的应用技术，特别是基于策略的安全防护技术，主要有安全策略描述语言的制定、策略的管理及应用、策略的可用性及一致性推理等。

2、PBAC 组成结构

PBAC 基本模型由如下要素组成：



（1）SUBJECT：表示模型的会话主体集。

（2）TARGET：表示模型的会话客体集。

（3）ACTION：表示模型的会话行为集。

（主体集、客体集和行为集与 RBAC 模型的定义一致。）

（4）SESSION：表示模型的会话集，它是主体对客体发起的一次行为请求，与 RBAC 不同，基本模型会话中不含有对会话相关的约束条件描述。

（5）ATTRIBUTE：表示模型的属性集，用于描述模型会话相关的约束条件，具体有主体属性、客体属性和会话环境属性。与传统的访问控制模型如 RBAC 不同，PBAC 基本模型将会话约束条件独立描述，并用属性进行统一管理。

（6）POLICY：表示模型的策略集。与传统的访问控制模型不同，PBAC 基本模型不采用根据模型的主体角色权限等约束条件间接描述策略的控制模式，直接制定了独立于访问控制执行机制的策略管理方法。

PBAC 基本模型各要素间关系如下：

（1）SA：主体属性指派，SA 是会话主体（SUBJECT）和属性（ATTRIBUTE）之间的多对多关系。

（2）TA：客体属性指派，TA 是会话客体（TARGET）和属性（ATTRIBUTE）之间的多对多关系。

（3）SEA：会话属性指派，SEA 是会话（SESSION）和属性（ATTRIBUTE）之间的多对多关系。

（4）SAP：会话属性策略指派，SAP 是会话（SESSION）、属性（ATTRIBUTE）和策略（POLICY）间的多对多关系。

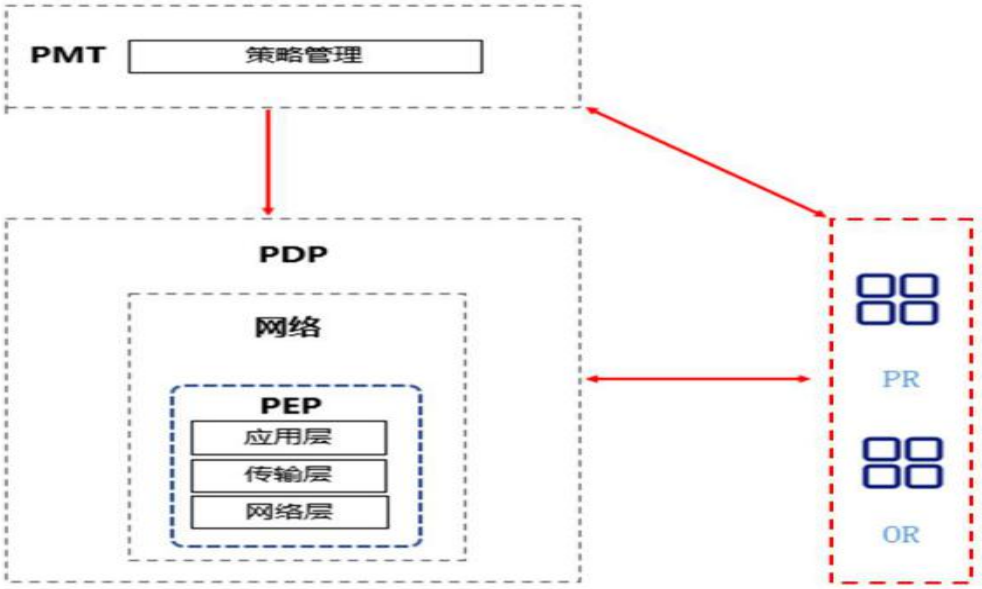
SA、TA、SEA、SAP 在系统初始化时由管理员进行配置。当系统需求发生变化时，可由管理员对 SA、TA、SEA、SAP 等进行修改配置。

PBAC 基本模型的一般执行方式可表示为：

对于给定的 attribute 条件下的 session，有 if（session, attribute, policy）∈SAP then do session，即系统的会话请求与其属性配置条件应符合策略规则。

3、PBAC 应用举例

基于策略的网络安全防护框架以策略为核心，实现网络访问控制服务,其在网络驱动层采用 PBAC 模型实现，典型应用框架如下：



整个框架由 PMT、PR、OR、PDP、PEP 组成，根据业务应用不同可以定制其他配套控制设施。

- 策略管理平台（PMT）：根据计算环境中的访问控制安全需求制定策略规则。
- 策略池（PR）：存储和检索所有的策略规则。由唯一的、负责计算访问决策的策略决策点（PDP）进行访问。
- 对象池（OR）：存储和管理会话相关变量，维护实体对象的属性变量配置信息及特征变量配置信息。
- 策略决策点（PDP）：根据会话中的实体信息、会话属性和会话相关策略进行决策，判定访问控制行为是否执行。
- 策略执行点（PEP）：根据策略决策结果执行访问控制会话请求。

在管理和运行方式上，首先由 PMT 收集与访问控制相关的对象、状态及行为信息，然后根据安全需求配置访问控制策略。主体（Subject）访问一个客体（Target）的请求被策略执行点（PEP）截获，然后 PEP 将其转发到策略决策点（PDP）。PDP 可以从对象池（OR，同策略信息点 PIP）获取到主体、客体和当前的环境信息。这些信息用来从策略池（PR）中获取可以适用的规则。PDP 把规则组合成适用的策略，计算组合后的访问决策，并最终将决策返回给 PEP。如果 PDP 授权允许访问，PEP 将这个请求转发给客体。

PBAC 模型的已知应用包括：

- 由 OASIS 定义的 XACML（扩展的访问控制标记语言），使用 XML 来表达授权规则和采用该模式后的访问决策。

- Symlabs 的联合身份访问管理系统（Federated Indentity Access Manager Federation）是一个实现了身份联合管理的身份管理系统。其组件中包含了策略执行点和策略决策点。
- 基于策略的准入控制组件框架（Components Framework for Policy-Based Admission Control）作为 Internet 2 项目的组成部分，是一个用于认证网络组件的框架。它基于 5 个主要的组成部分："访问请求"（AR）、"策略执行点"（PEP）、"策略决策点"（PDP）、"策略池"（PR）、"网络检测点"（NDP）。
- XML 和应用层防火墙也使用这个策略模式。
- SAML（安全断言标记语言）是 OASIS 定义的 XML 语言标准，用于安全域之间认证和授权数据的交换。SAML 可以用来传递授权决策。

4、PBAC 优缺点

PBAC 的优点包括：

- PBAC 可简化访问控制和智能化权限设置

在 PBAC（基于策略的访问控制）下，授权不依赖于任何特定的实现（如 XACML），并且可以用自然语言设置策略，如"团队领导只能在工作日的上午 9 点到下午 6 点之间，授予团队成员对项目的访问权限"。这使得管理大量用户和数据更加简单。

- PBAC 支持环境控制

如果存在只应在某些计算机上查看的敏感文件，则可以轻松设置策略以限制非必要的访问。

- PBAC 策略可以基于需求快速调整

例如，如果工程师在紧急情况下需要访问特定对象，他们可以在紧急情况下在有限的时间内被授予立即访问权限。

- PBAC 能帮助用户更好满足合规要求

PBAC 通过隔离数据访问、控制访问蔓延，甚至阻止授权用户以危险方式访问数据，使遵守 GRC 和 GDPR 等法规变得更加容易。

- PBAC 更具有灵活性，也更安全

因为访问请求是用标准格式提出的，制定访问决策可以独立于执行访问决策。PBAC 能支持多种执行机制，并独立于策略决策点，所以可以单独完善改进各执行机制。该模型可以支持访问控制矩阵（ACM）、基于角色的访问控制（RBAC）、访问控制的多级

安全模型（MLS）等。同时，因为任何访问都是间接的，因而减少了非法的访问，提高了安全性。

当然，PBAC 模型也面临下述潜在的问题：

- 可能影响受保护系统的性能，因为集中的策略决策点/策略池/对象池（策略信息点）子系统可能成为整个系统的瓶颈。
- 增加系统复杂性。
- 需要增加措施保护访问控制信息。

5.2权限管理要素和系统设计

访问控制是为用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理，防止对信息的非授权篡改和滥用。访问控制的主要作用是：保证用户在系统安全策略下正常工作、拒绝非法用户的非授权访问请求、拒绝合法用户越权的服务请求。从这一定义，可以明确的看到访问控制的核心就是权限管理。

权限管理，一般是指根据系统设置的安全规则或者安全策略，用户可以访问而且只能访问自己被授权的资源，不多不少。

5.2.1 权限管理的基本要素

在进行权限管理系统设计和选择的时候，首先需要考虑权限管理系统的核心对象模型.对象模型中包含的基本元素主要有：用户（Users）、用户组（Group）、角色（Role）、控制对象（Resource Class）、访问模式（Access Mode）、操作（Operator）。主要的关系有：分配角色权限 PA（Permission Assignment）、分配用户角色 UA（Users Assignmen），分别描述如下：

（1）控制对象：是系统所要保护的资源（Resource Class），可以被访问的对象。资源的定义需要注意以下两个问题：

- 资源具有层次关系和包含关系。例如，网页是资源，网页上的按钮、文本框等对象也是资源，是网页节点的子节点，如可以访问按钮，则必须能够访问页面。
- 这里提及的资源概念是指资源的类别（Resource Class），不是某个特定资源的实例（Resource Instance）。资源的类别和资源的实例的区分，以及资源的粒度的细分，有利于确定权限管理系统和应用系统之间的管理边界，权限管理系统需要对于资源

的类别进行权限管理，而应用系统需要对特定资源的实例进行权限管理。两者的区分主要是基于以下两点考虑：

- 一方面，资源实例的权限常具有资源的相关性。即根据资源实例和访问资源的主体之间的关联关系，才可能进行资源的实例权限判断。 例如，在管理信息系统中，需要按照营业区域划分不同部门的客户，A 区和 B 区都具有修改客户资料这一受控的资源，这里“客户档案资料”是属于资源的类别的范畴。如果规定 A 区只能修改 A 区管理的客户资料，就必须要区分出资料的归属，这里的资源是属于资源实例的范畴。客户档案（资源）本身应该有其使用者的信息（客户资料可能就含有营业区域这一属性），才能区分特定资源的实例操作，可以修改属于自己管辖的信息内容。
- 另一方面，资源的实例权限常具有相当大的业务逻辑相关性。对不同的业务逻辑，常常意味着完全不同的权限判定原则和策略。

（2）用户：权限的拥有者或主体。用户和权限实现分离，通过授权管理进行绑定。

用户仅仅是纯粹的用户，用来记录用户相关信息，如用户名、密码等，权限是被分离出去了的。用户（User）要拥有对某种资源的权限，必须通过角色（Role）去关联。

（3）用户组：一组用户的集合。在业务逻辑的判断中，可以实现基于个人身份或组的身份进行判断。系统弱化了用户组的概念，主要实现用户（个人的身份）的方式。

（4）角色：权限分配的单位与载体。角色通过继承关系支持分级的权限实现。例如，科长角色同时具有科长角色、科内不同业务人员角色。角色是使用权限的基本单位，拥有一定数量的权限，通过角色赋予用户权限，对于基于角色的访问控制模型，访问权按角色名分组，资源的使用受限于授权给假定关联角色的个体。

（5）操作（权限）：完成资源的类别和访问策略之间的绑定。

权限指用户根据角色获得对程序某些功能的操作，例如对文件的读、写、修改和删除功能。

（6）分配用户角色 UA：实现用户和角色之间的关联关系映射。

一个用户（User）可以隶属于多个角色（Role），一个角色组也可拥有多个用户，用户角色就是用来描述他们之间隶属关系的对象。用户（User）通过角色（Role）关联所拥有对某种资源的权限，例如：

用户（User）列表：

UserID	UserName	UserPwd
1	张三	xxxxxx
2	李四	xxxxxx

RoleID	RoleName	RoleNote
01	系统管理员	监控系统维护管理员
02	监控人员	在线监控人员
03	调度人员	调度工作人员
04	一般工作人员	工作人员

角色（Role）列表：

用户-角色分配列表：

UserRoleID	UserID	RoleID	UserRoleNote
1	1	01	用户“张三”被分配到角色“系统管理员”
2	2	02	用户“李四”被分配到角色“监控人员”
3	2	03	用户“李四”被分配到角色“调度人员”

从这一过程列表可以看出，用户所拥有的特定资源可以通过用户角色来关联。

（6）分配角色权限 PA：实现操作和角色之间的关联关系映射。

一个角色（Role）可以拥有多个权限（Permission），同样一个权限可分配给多个角色。

角色（Role）列表：

RoleID	RoleName	RoleNote
01	系统管理员	监控系统维护管理员
02	监控人员	在线监控人员
03	调度人员	调度工作人员
04	一般工作人员	工作人员

权限（Permission）列表：

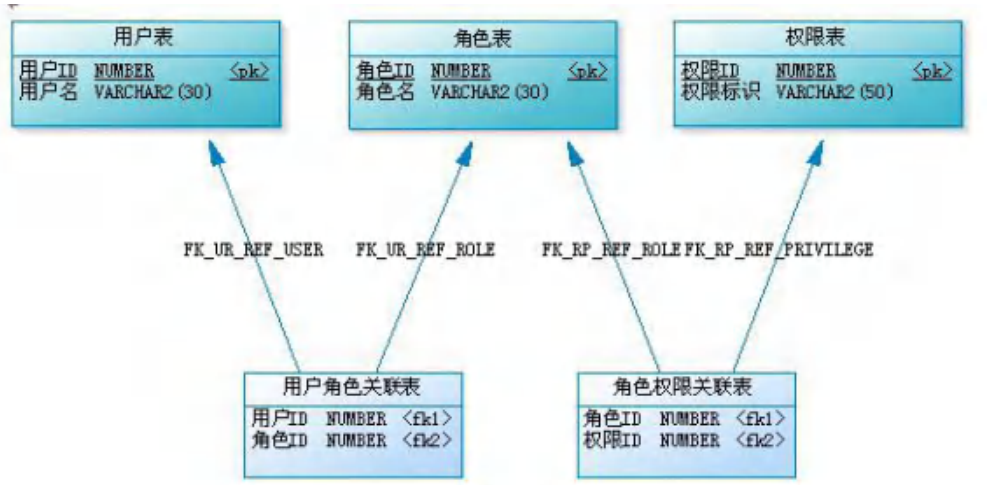
PermissionID	PermissionName	PermissionNote
0001	增加监控	允许增加监控对象
0002	修改监控	允许修改监控对象
0003	删除监控	允许删除监控对象
0004	察看监控信息	允许察看监控对象

角色权限（Role_Permission）分配列表：

RolePermissionID	RoleID	PermissionID	RolePermission Note
1	01	0001	角色“系统管理员”具有权限“增加监控”
2	01	0002	角色“系统管理员”具有权限“修改监控”
3	01	0003	角色“系统管理员”具有权限“删除监控”
4	01	0004	角色“系统管理员”具有权限“察看监控”
5	02	0001	角色“监控人员”具有权限“增加监控”
6	02	0004	角色“监控人员”具有权限“察看监控”

由以上例子中的角色权限关系可以看出，角色权限可以建立角色和权限之间的对应关系。

综合一下，基于 RBAC 模型的权限管理模型也可以用数据视图形象表示如下：



（图：RBAC权限模型）

5.2.2 权限管理系统设计

权限系统由三大部分构成：用户管理、角色管理、权限管理

用户权限系统的核心由以下三部分构成：创造权限、分配权限和使用权限。

（1）创建权限（Permission），在设计和实现系统时会划分。创建权限信息，指定系统模块具有哪些权限。

（2）系统管理员（Administrator）创建用户和角色，并且指定用户角色（User－Role）和角色权限（Role－Permission）的关联关系。

1) Administrator 具有创建用户、修改用户和删除用户的功能

2) Administrator 具有创建角色和删除角色的功能

3)Administrator 具有建立用户和角色、角色和权限的关联关系功能

（3）用户（User）使用 Administrator 分配给的权限去使用各个系统模块。

5.2.3 用户管理

用户管理是创建用户账号的一个过程，拥有账号之后，就可以登录系统。用户管理包括账号的创建、删除、冻结、解冻等操作。创建账号之后，使用对应账号可以登录系统，删除或者冻结账号之后，账号无法继续登录系统。

姓名、账号、密码为必须要素。其他的要素可根据企业自身需求增加，比如：手机号码、生日、联系地址、性别等信息。

账号创建完毕之后，需要为用户赋予角色（即在企业中的任职情况，如销售经理、销售主管、出纳、会计等）。

5.2.4 角色管理

权限系统中的角色大概率跟企业的组织架构是一致的，企业组织架构中的人在什么岗位要做什么事情？权限系统中的用户是什么角色被允许看那些东西进行什么操作？是一种对应关系，所以 企业架构的岗位、岗位职责跟别对应了权限系统的角色、权限。

在企业中一个人可以兼任多个岗位，一个岗位也可能有多个人，所以岗位与人是多

对多的关系。

岗位之间会有从属关系，比如：销售经理下设销售主管、销售主管下设销售专员，最终构成了组织架构，一般是树形关系。

角色管理需要我们可以灵活的配置角色，而且可以设置从属关系。

创建完毕角色之后，我需要为角色赋予权限（其在企业中对应岗位需要做什么事情，允许看到什么内容，进行什么操作？）

5.2.5 权限管理

权限一般是跟企业中的岗位职责对应的，在企业实际运营过程中，为了保证用户的隐私、企业数据的安全性，会对不同岗位设定不同的限制。比如客服不允许给用户退款转账，新媒体运营专员不允许查看用户手机等隐私信息，非高层管理者不允许批量导出用户信息等。

总结起来，我们可以将权限分为两大类：数据权限和操作权限。

（1）数据权限

数据权限，就是角色可以看到哪些内容（包括能看到哪些页面、字段、区域）

-页面：假设有 10 个页面，管理员只给某个角色开通了 10 个中的 2 个页面查看权限，那么该角色就只能看到这 2 个菜单。

-字段：假设某个菜单对应的页面列表中有 15 个字段，角色 A 被允许查看所有字段，角色 B 只允许查看其中的 10 个字段，那么 A 和 B 看到的内容就不同。

-区域：假设为角色 A 开通了全国的数据查看权限，为 B 开通了北京的数据查看权限，那么 A 就可以看到全国的数据，B 就只能看到北京地区的收据。

（2）操作权限

操作权限就是角色可以进行哪些操作？包括增删改。比如客服不允许上下架商品，商品审核专员不允许操作退款等，都属于操作权限的控制，每个操作都可以有权限控制。

5.3 常见云原生权限策略说明

随着云计算服务产业的蓬勃发展，这种可计量 IT 服务模式，已经成为替代用户本地自建 IT 服务的主流趋势。而在实际应用中，用户对于服务资源的权限管理需求也逐渐显现出来。以企业用户为例，所使用的云资源需要多个操作者协同使用、维护，在

不同的场景下各自的操作权限需求不同，特别在信息安全、操作合规的要求下，对于操作者的分级分权要求十分强烈。所以各家云计算厂商在产品发展中均逐渐提供了面相用户的 IAM 功能。下文将以 AWS 为例，介绍云计算服务 IAM 功能的实现方案。

5.3.1 AWS Identity and Access Management (IAM)简介

AWS IAM 在云计算功能中是以 WEB 服务模式向用户提供使用功能，帮助用户安全地控制用户对 AWS 资源的访问权限，可以控制哪些人可以使用 AWS 资源（身份验证）以及可以使用的资源和采用的方式（授权）。

AWS IAM 提供的主要功能：

1. 增强安全性

提供用户和组的权限管理能力，并指定他们可以访问的 AWS 服务 API 和资源，默认状态下启用安全保护；用户只有被明确授予了权限，才能访问 AWS 资源。

2. 精确控制

能够使用权限精确控制用户对特定 AWS 服务和资源的访问权限。例如，终止 EC2 实例或读取 Amazon S3 存储桶中的内容。

3. 临时凭证

除了直接给用户和组分配访问权限外，IAM 还允许创建角色。通过角色定义一组权限，然后让通过验证的用户或 EC2 实例承担这些角色，通过授予对您定义资源的临时访问权限改善安全状况。

4. 分析访问

提供授权与操作行为的数据分析能力。可以使用 IAM 访问分析器来辨识可以从 AWS 外部访问的资源。例如，可以使用针对的 Amazon S3 存储桶、AWS KMS 密钥、Amazon SQS 队列、IAM 角色和 AWS Lambda 函数的策略验证所分配的公共和跨账户权限。另外，IAM 通过为您提供 IAM 实体上次使用服务时间的时间戳，可以帮助您轻松识别和删除不使用的权限。

5. 灵活的安全证书管理

支持以数种方式验证用户，具体取决于他们要如何使用 AWS 服务。可以指定一组安全证书，包括密码、密钥对和 X.509 证书。对访问 AWS 管理控制台或使用 API 的用户强制实施 Multi-Factor Authentication (MFA)。

6. 利用外部身份验证系统

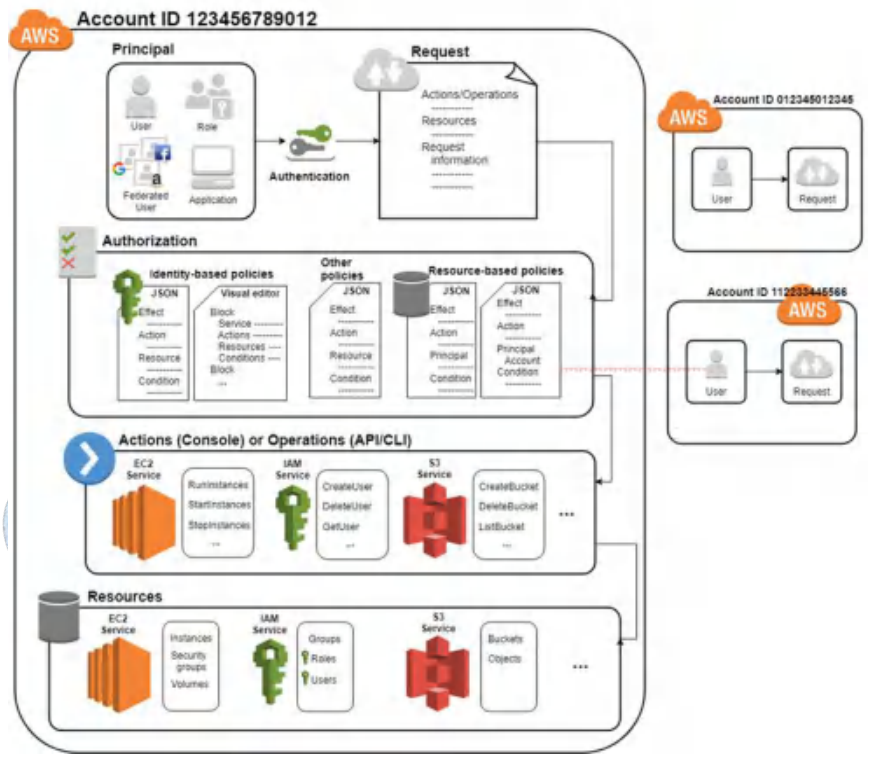
可以使用 IAM 来用您的现有身份系统向员工和应用程序授予对 AWS 管理控制台和 AWS 服务 API 的访问权限。 AWS 支持从公司系统（如 Microsoft Active Directory）以及基于标准的身份提供商进行集成认证。

7. 无缝集成到 AWS 服务

IAM 可以应用在到大多数 AWS 服务中。在 AWS 管理控制台中的定义每个服务的访问控制权限。

5.3.2 AWS Identity and Access Management (IAM)运行原理

AWS IAM 的整体功能设计遵循 RBAC 权限模型，也是基于角色或用户组维度的权限认证与授权。



- 资源（Resources）

存储在 IAM 中的用户、组、角色、策略和标识所映射的服务资源（应用程序）。

- 身份（Identities）

IAM 资源对象，用于标识和分组。将策略附加到 IAM 身份。其中包括用户、组和角色。

- 实体（Entities）

AWS 用于身份验证的 IAM 资源对象。这些用户包括 IAM 用户、联邦用户和承担 IAM 角色。

- 用户（Principals）

使用 AWS 帐户根用户、IAM 用户或 IAM 角色登录 AWS 并向 AWS 发出请求的人或应用程序。

- 请求（Request）

当尝试使用 AWS 管理控制台、AWS API 或 AWS CLI 时，该主体将发送请求呼叫 AWS。请求包括以下信息：

1.行动或行动-主体想要执行的行动或操作。这可以是 AWS 管理控制台中的操作，也可以是 AWS CLI 或 AWS API 中的操作。

2.资源-执行操作或操作的 AWS 资源对象。

3.用户-使用实体(用户或角色)发送请求的个人或应用程序。有关主体的信息包括与主体用于登录的实体关联的策略。

4.环境数据-有关 IP 地址、用户代理、SSL 启用状态或一天中的时间的信息。

5.资源数据-与所要求的资源有关的数据。这可以包括信息，如 DynamoDB 表名或 AmazonEC 实例上的标记。

6.AWS 将请求信息收集到请求上下文，用于评估和授权请求。

- 认证

使用主体的凭据对主体进行身份验证(登录到 AWS)以向 AWS 发送请求。若要以根用户身份从控制台进行身份验证，必须使用电子邮件地址和密码登录。作为 IAM 用户，请提供您的帐户 ID 或别名，然后提供您的用户名和密码。要从 API 或 AWSCLI 进行身份验证，必须提供访问密钥和密钥。还可能要求您提供其他安全信息。

- 授权

AWS 使用来自请求上下文的值来检查应用于请求的策略。然后，它使用策略来确定是允许还是拒绝请求。大多数策略都存储在 AWS 中，如 JSON 文件并指定主体实体的权限。

- 执行动作

请求经过身份验证和授权后，AWS 将批准您请求中的操作或操作。操作由服务定

义，包括可以对资源执行的操作，例如查看、创建、编辑和删除该资源。

5.3.3 AWS IAM Policy 权限策略机制介绍

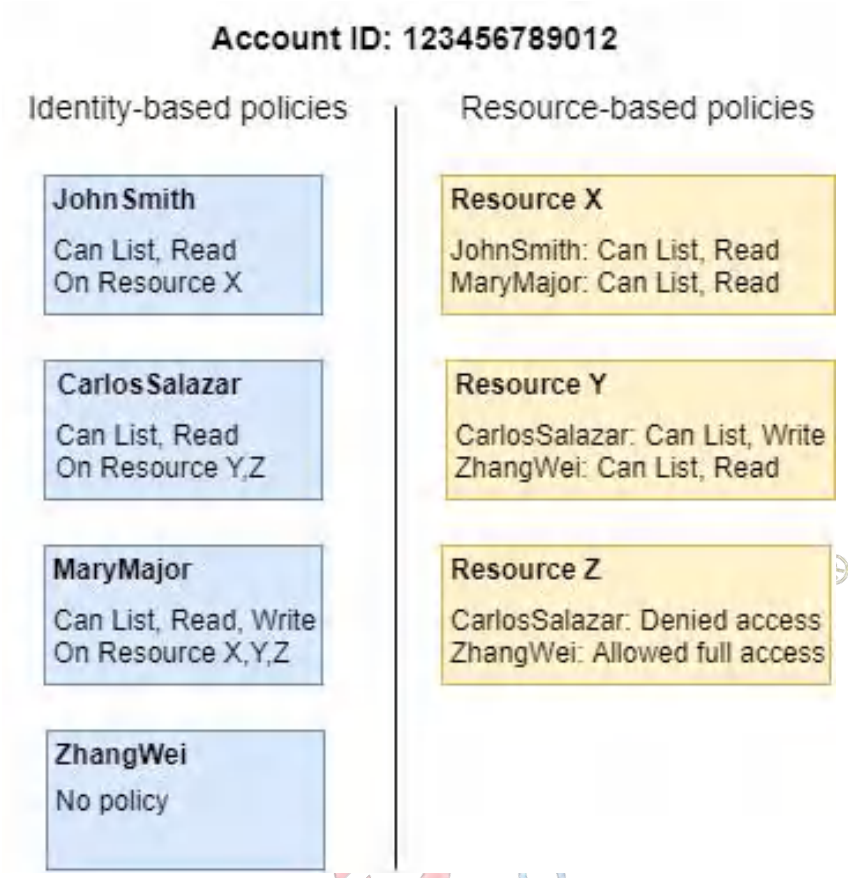
通过对 AWS IAM 的基本功能与运行原理介绍，可以看出在权限管理的设计上与一般大型应用系统方式基本相同。在实际功能实现上 AWS Policy 在 IAM 中的应用却可以称之为在本领域的最佳实践，让繁琐复杂的权限策略可以用结构化的策略文件进行描述与执行，大大降低了权限分配与执行的难度，能够更为灵活的支持权限策略的设计与分配执行。

AWS IAM 通过策略（Policy）来定义权限（Permissions），基本的类型有：、

- Identity-based policies 基于身份的政策-将管理策略和内联策略附加到 IAM 标识(用户、用户所属组或角色)。基于标识的策略向标识授予权限。
- Resource-based policies 基于资源的政策-将内联政策附加到资源中。基于资源的策略最常见的例子是 AmazonS 3 桶策略和 IAM 角色信任策略。基于资源的策略将权限授予策略中指定的主体.主体可以在与资源相同的帐户中，也可以在其他帐户中。
- Permissions boundaries 权限边界-使用托管策略作为 IAM 实体(用户或角色)的权限边界。该策略定义基于身份的策略可以授予实体但不授予权限的最大权限。权限边界不定义基于资源的策略可以授予实体的最大权限。
- Organizations SCPs 基于组织-使用 AWS 组织服务控制策略(SCP)为组织或组织单位(OU)的帐户成员定义最大权限。SCPS 限制基于身份的策略或基于资源的策略授予帐户内实体(用户或角色)的权限，但不授予权限。
- Access control lists (ACLs)访问控制列表(ACL)-使用 ACL 控制其他帐户中哪些主体可以访问附加 ACL 的资源。ACL 类似于基于资源的策略，尽管它们是唯一不使用 JSON 策略文档结构的策略类型。ACL 是向指定主体授予权限的跨帐户权限策略。ACL 不能向同一帐户内的实体授予权限。
- Session policies 会话策略-在使用 AWSCLI 或 AWSAPI 承担角色或联邦用户时传递高级会话策略。会话策略限制角色或基于用户身份的策略授予会话的权限。会话策略限制创建的会话的权限，但不授予权限

而最常使用的有两类：一种是 Identity-based policy（策略基于身份），另一种是

Resource-based policy（策略基于资源）。



IAM Policy 用 JSON 描述，可以理解为权限的声明文档，基本格式如下：

- Version: "2020-06-11": 版本号
- Statement: 具体策略的内容，可以是一个或者多个
- Effect: 执行结果 Allow 或者 Deny
- Action: 具体执行的操作操作，
- Resource: 具体的资源

用户向 AWS 发起认证请求后，系统会根据映射关系，查找执行 Policy 文件，而一个用户或者角色主体上，可以拥有多个不同的 Policy。

系统会检查 Policy 请求上下文的每个策略。如果单个策略拒绝请求，AWS 将拒绝整个请求并停止评估策略。这就是所谓的显否认。因为请求是默认拒绝，只有当请求的每一部分都被适用的策略所允许时，IAM 才会批准请求。整体遵循以下规则：

- 默认情况下，所有请求都被隐式拒绝。(或者，默认情况下，AWS 帐户根用户可以完全访问。)

- 基于身份的策略或基于资源的策略中的显式允许覆盖此默认设置。
- 如果存在权限边界、组织 SCP 或会话策略，则可能会使用隐式拒绝覆盖允许。
- 任何策略中的显式拒绝覆盖任何允许。

5.4数据权限管理方式（如通过 API 网关完成鉴权）

随着物联网、云计算和大数据的深入应用，数据呈现爆发性的增长，海量数据进入数据仓库后，再以服务的方式对应用系统开放数据，实现数据价值最大化。Forrester 对全球企业组织的网络安全决策者进行的一项调查发现，有 51%的受访者表示在过去 12 个月中至少有一次潜在的数据泄露。因此，如果缺乏对海量数据进行统一、安全、规范的权限管理，会造成数据泄露，带来严重后果。在数据权限管理方式中，需要做好以下几方面工作：

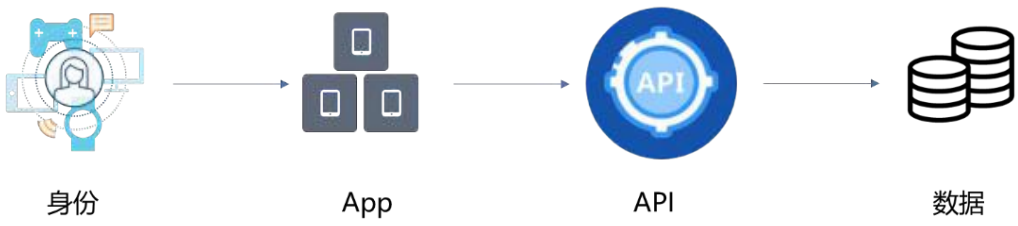
人员标签化：根据业务特性，对访问人员（主体）打上能够区分数据访问权限的标签，比如人员级别、角色等；

数据标签化：根据业务特性，对数据进行分类分级，打上相应的标签。比如，在数据对象上打上数据类别标签和级别标签，在数据行和数据列上打上级别标签；

数据授权：在权限管理系统中，将人员的标签和数据标签作为授权属性，基于这些属性制定主体（人）对客户（数据）的授权策略，比如 3 级人员能访问 3 级以下的数据。

身份传递：应用系统调用数据服务时，需要传入用户的身份令牌（由身份认证系统颁发，不可伪造），将真正调用数据服务的用户身份传递给访问控制决策执行模块。

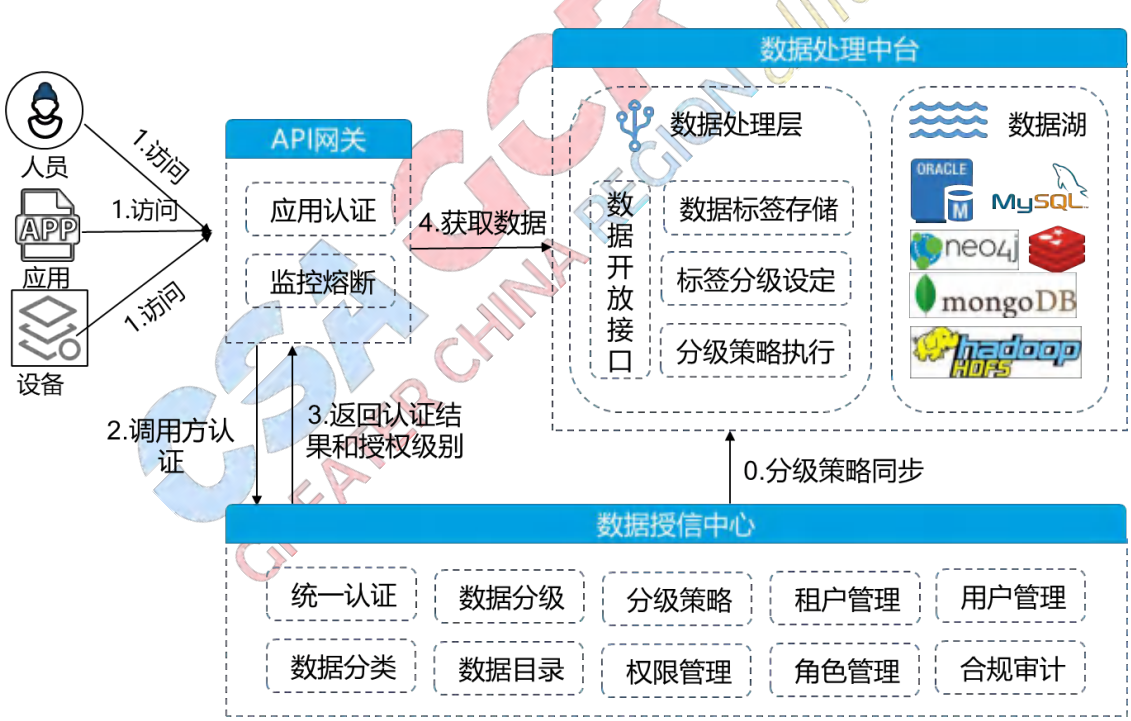
数据访问控制：访问控制决策执行模块从策略管理模块同步访问控制策略，并进行缓存。应用系统调用数据服务接口时，决策执行模块从接口中获取访问人员的身份令牌，从身份令牌获取访问人员信息和人员属性，将访问控制策略转化成访问请求过滤参数，附加在原来的请求中，从而实现数据过滤。



5.4.1 数据分级

数据权限管理需对信息系统的数据及用户操作行为进行分级，基于“角色、数据、操作”对操作权限进行控制，达到不同角色对不同级别的数据，对应拥有不同操作级别的要求，从而更加精细化地保障数据安全。依据信息系统数据在泄露或被非法处理后对国家安全、公共秩序、公共利益、党政机关及事业单位、法人或其他非政府组织及个人的合法权益的危害程度来确定级别，可分为公开级、普通级、敏感级、重要级、秘密级等多个级别。同时结合用户操作可能对数据造成的危害，将用户操作划分为低风险、中风险及高风险操作，通过强化审批等管理手段及加强系统权限模块、日志审核等技术手段对用户操作进行控制，达到角色默认权限“最少够用”，中、高风险操作事前有审批、事中有控制、事后有审计的目的。

5.4.2 API 网关鉴权



完成数据分级后，通过数据授权中心，根据访问者的上下文环境来判断在哪个时刻该返回什么级别的数据给对方。用户访问数据时，首先通过 API 网关完成调用方认证，并返回用户授权级别。同时采用 API 网关来配合完成限流，熔断、降低等服务。

5.5 权限定编定岗

访问控制实质上是对资源使用的限制，决定主体是否被授权客体或资源执行某种操作，是保障系统安全不可或缺的重要组成部分。目前，主要有 3 种不同类型的访问控制：自主访问控制（ＤＡＣ）、强制访问控制（ＭＡＣ）和基于角色的访问控制（ＲＢＡＣ）。自主访问控制（ＤＡＣ）是目前计算机系统中实现最多的访问控制机制，如Ｗｉｎｄｏｗｓ操作系统。强制访问控制（ＭＡＣ）是强加给访问主体的，即系统强制主体服从既定的访问控制策略，主要应用于军事方面。这两种访问控制方式都只适用于特定的领域，具有一定的局限性。基于角色的访问控制（ＲＢＡＣ）引入了角色的概念，在授权主体和客体之间增加的角色这个中间层，实现了主客体的逻辑分离，具有一定的通用性。但ＲＢＡＣ在实际的应用中仍然存在一些问题，如：角色的继承机制有缺陷，会造成某些角色的权限过大；权限定义较模糊、笼统，不够清晰；无法满足“同角色不同人员不同权限”的需求。基于上述原因，本文提出一种扩展的ＲＢＡＣ新模型，引入了“岗位”概念，有效地弥补了传统ＲＢＡＣ的不足。

基于岗位的 RBAC 新模型要素包括组织、岗位、角色、菜单、账号、规则。其中， 各个要素之间的关系如下：

（1）组织和岗位构成了权限管控的框架，需要与系统内的业务运行情况保持一致；

（2）角色是为了便于授权，通过将功能紧密相关的菜单进行绑定从而形成，通过将角色分配给岗位，形成了岗位的授权；

（3）账号是访问业务系统的实体，通过将账号关联到岗位，从而实现了账号的授权；

（4）规则是授权过程中需要满足的合规要求，包括不可以同时授予互斥权限以及敏感权限只允许分配特定岗位。

各个要素之间紧密协同，构建起权限管控的有机架构如下：

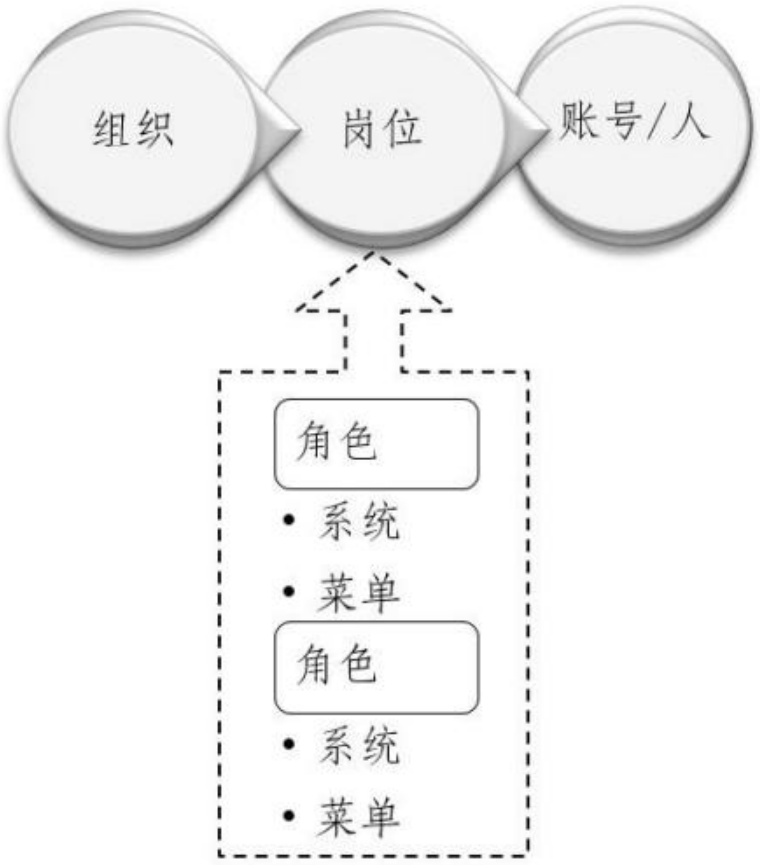


图 1 权限管控要素

作为权限管控的框架，需要根据业务系统内覆盖的业务组织情况，搭建起权限管控的组织架构，并且当业务组织发生调整的时候，及时在相应的权限管理系统内进行同步更新，从而反映业务组织的实际情况。

在搭建起权限管控组织后，需要梳理出业务系统内所涉及的业务岗位，并将业务岗位关联在组织下，该业务岗位需要体现用户在业务系统内的真实身份，反映出业务实际，通常比 HR 的岗位要更细化。

在完成岗位设计后，角色可以与岗位关联，账号也可以与岗位关联，从而实现以岗定权。为保持与业务实际一致，当业务岗位发生变化的时候，需要及时在相应的权限管理系统内进行更新。

5.6权限合规与互斥

5.6.1 职责分离原则和互斥

职责分离（SoD：Separation of Duty）作为一个安全原则，当需要两个或多个不同的用户对完成一个交易或相关的交易负责时，职责分离用来阐述多用户控制策略。这个原则的目的就是通过多个不同的用户负责某个活动或任务以分散权利和责任来减少欺诈行为，确保没有人能够进行一项高风险的操作的所有步骤。职责分离原则实施以后，减少了欺诈的风险，此外，还有利于操作人员相互间发现无意中犯的错误。

职责分离有两种模式：

- 静态职责分离(Static Separation of Duty)：用户无法同时被赋予有冲突的角色。
- 动态职责分离(Dynamic Separation of Duty)：用户在一次会话（Session）中不能同时激活自身所拥有的、互相有冲突的角色，只能选择其一。

为了实现职责分离，在授权模型中添加了职责分离管理，规定了权限被赋予角色时，或角色被赋予用户时，以及当用户在某一时刻激活一个角色时所应遵循的强制性规则。一般通过互斥约束来实现职责分离策略，主要包括以下约束:

- 互斥角色: 同一用户只能分配到一组互斥角色集合中至多一个角色，支持责任分离的原则。互斥角色是指各自权限互相制约的两个角色。比如财务部有会计和审核员两个角色,他们是互斥角色,那么用户不能同时拥有这两个角色,体现了职责分离原则
- 基数约束: 一个角色被分配的用户数量受限；一个用户可拥有的角色数目受限；同样一个角色对应的访问权限数目也应受限，以控制高级权限在系统中的分配
- 先决条件角色: 即用户想获得某上级角色,必须先获得其下一级的角色

静态互斥角色（SMER）约束是互斥约束最常见的种类，而基于角色静态职责分离约束与静态职责分离策略形式上最接近。

5.6.2 建设业务授权管理系统的必要性

在企业的高速发展和全面信息化建设，ERP、CRM、SRM、计划、预算等核心业务系统越来越多，信息化工程的应用在为集团带来巨大经济绩效的同时，也对自身的管理、

协调、运营和可持续发展提出了巨大的挑战。核心应用系统访问与授权是信息系统管控工作的难点，如何确认用户授权的合规性，加强用户授权的管理，已是当前面临的重要问题。用户业务授权管理关注的核心包括： 用户在系统内所授予的授权是否合理； 是否存在授权最小化、以岗定权、不相容业务操作是否分离等问题； 系统中关键、敏感的操作或数据是否只能够被限定的人员所访问等。此外，以岗定权、职责分离、敏感权限授权管理是企业全面风险管理、企业商业秘密保护以及上市公司业务合规性的基本规范。

同时，因为缺乏自动化的业务授权管理系统，具有以下问题：

（1）为避免信息系统用户职责分离不清产生的舞弊风险， 应当按照不同业务的控制要求，通过信息系统中的权限管理功能控制用户的操作权限， 避免将不相容职责的权限授予同一用户。在实际操作过程中，因缺少整体的访问与授权管理业务标准、统一视图和自动化平台工具，无法系统性整改，只能靠手工逐个处理，效果不易持续；

（2）各应用系统的使用对象广、用户基数大、授权类型多，情况复杂。涵盖企业总部及分支机构，涉及业务合作伙伴、外包人员、系统实施人员，人员众多、类型也复杂。多个系统用户数目庞大，不同系统内还有数量众多的各类系统角色、授权类型，各种用户与权限的组合有上千万种， 单纯靠手工管理， 费时、费力，效果不理想。

（3）高层缺乏可视化的授权视图，例如，某一个员工搞不清楚自己在几个系统有什么样授权权限，其上级领导也无法对此进行了解和监督，因此会导致信息系统权限混乱、无序，从而对公司的正常运营和管理产生直接威胁。

（4）各应用系统存在分头管理，标准、机制不统一。应用系统访问与授权管控的归口部门、执行部门、管理目标、管理流程、管理手段尚未统一和标准化，系统管控还主要依赖相关人员的个人意识、经验来管理， 人工的检查往往存在绕过该控制的风险，未深入到事务代码层级， 缺少跨模块和跨系统的职责互斥检查，容易遗漏。

（5）缺乏自动化系统平台支撑，管理手段有待提升。ERP 等应用系统的访问与授权管控包括：授权的申请、审批、监控、审计等。各操作环节都手工处理，主要依赖线下手工单据流转，缺少自动化平台工具支撑，难以合理、充分管控，导致授权管控的效果并不理想。

因此，在大型企业中需要建设业务授权管理系统。首先是建设一套完整、科学的授权及合规性控制管理体系框架，然后导入符合最佳实践的授权与合规性管理流程、技术

标准，通过实施管控系统从而固化管控流程，满足授权及合规性控制管理目标。

5.6.3 SAP（治理、风险、合规）系统用户权限管控

SAP（Governance Risk Compliance）系统用户权限管控是 SAP BASIS 的重要职责，因其工作量大且相对复杂，细致，在 SAP 系统中通常作为一个相对独立的部分来实施。作为企业业务平台之外的外挂系统，专注于企业如何防范风险、如何规避企业在业务经营过程中所可能发生的各类风险和不合规性行为，是帮助企业进行风险防护的安全盾牌。

SAP 系统用户要完成某项工作需要运行相应的事务码，不同的事务码可以在系统中进行不同的动作。SAP 系统中的权限会被外部顾问设计成用户名---角色（岗位）---事务代码。外部顾问会根据公司部门，岗位把事务代码按组分好，最后加给用户。而权限问题的产生，是基于 SAP 系统权限检查的机制：即用户在 SAP 系统中进行事务操作时，系统将会检查用户相应事务的权限。SAP 系统的权限控制是基于事务码(Transaction / Menu)和授权对象的，其中，通常所说的授权对象则是权限控制的最小单位。角色是 SAP 系统中权限的集合，可能包含一个或数个事务码，也可能包含一个或数个权限对象。同一类工作使用 SAP 的目的和常用的功能都是类似的，当我们把某类工作需要的权限都归到一个集合中这个权限集合就是“角色”(Role)。

SAP 系统另一重要特点即权限是累加的。用户可以拥有多个 SAP 角色，所有角色的权限累加在一起成为用户的最终权限。

从授权实践来看，SAP 系统权限合规问题的产生分布在权限管控的各个节点，包括岗位信息收集和分析、各层次角色设计与创建、用户权限申请、审批和开通的各个环节。同时，权限合规管控绝不仅仅是局限于权限管理员的技术活，而是一个充满互动的系统工程，需要企业用户、系统各模块业务方、企业合规管理方等多个部门参与，甚至发挥主导的作用。而 SAP 合规管控平台的作用是更方便、更全面、更及时的让权限管控相关方获得不合规信息，从事前、事中、事后三个时间维度提供权限授予、审批和管控依据，保障授权最小、足够、及时、合理且合规，业务正常有序开展。

随着越来越多的业务系统接受合规管理，纳入企业审计工作范围。除延请外部机构进行的审计外，企业内部也会采用权限合规管控系统适时或定期对业务系统进行用户安全和权限审计，以发现不再合适的授权、不再合理的权限设计，从而达到持续优化、控制风险的目的。

5.7权限定期审阅

仅仅是事前的权限控制策略有时候也不能杜绝所有越权行为，仍然存在通过不当途径获得未授予的特权的可能，比如黑客攻击越权方式、权限管理员舞弊等，也有可能存在误授权或者过度授权。另外，伴随业务的发展，组织架构、岗位和人员都会发生相应的变化。因此，需要定期对权限进行审阅，及时识别其中的问题，并进行整改。

在企业实际执行权限定期审阅的过程中，需要明确定期审阅场景，基于前述基于 RBAC 模型的要素构成，企业权限定期审阅建议涵盖如下场景，同时如下列示了各个场景的审阅维度和审阅关注点。

场景编号	审阅场景	编号	审阅维度	审阅关注点
1	权限风险规则库审阅	1.1	现有规则业务定义审阅	现有业务定义是否适用于当前业务情景
				业务活动描述是否准确且便于理解
		1.2	现有规则技术定义审阅	业务活动和操作、操作和权限对象的对应关系是否准确
				是否存在已经停用的系统操作/权限对象
		1.3	是否需要新增规则	系统是否存在新增功能，如存在需要
				确认新增业务功能是否适用于现有业务活动
				如不适用需要确认是否需要针对新增功能建立新的规则
		1.4	补偿性控制描述审阅	对补偿性控制的描述进行审阅，确保补偿性控制具有可操作性
		1.5	补偿性控制落实审	抽查分配了补偿性控制的用户，是否

			阅	按照补偿性控制规定进行相关的业务操作
2	角色审阅	2.1	角色命名	目前系统中角色是否存在与角色命名规范不相符的角色
		2.2	角色对应操作	审阅角色设计合理性，确认角色对应操作是否与角色定义的功能相符
		2.3	角色风险审阅	角色内部是否存在 SOD 冲突
3	岗位审阅	3.1	岗位命名	对补偿性控制的描述进行审阅，确保补偿性控制具有可操作性
		3.2	岗位对应角色	抽查分配了补偿性控制的用户，是否按照补偿性控制规定进行相关的业务操作
		3.3	岗位风险审阅	岗位内部是否存在 SOD 冲突
				岗位是否存在不符合岗位职责的敏感访问权限
4	用户权限审阅	4.1	普通用户账号状态审阅	审阅用户账号状态是否合理，例如 180 天内未使用的账号是否进行锁定
		4.2	普通用户账号权限审阅	用户拥有权限涉及的职责分离及敏感访问风险权限是否应当移除。
				用户超出职责本身的冗余权限是否应当移除。
5	紧急账号审阅	5.1	紧急账号使用审阅	每次应急账号使用后审阅应急账号使用记录和申请原因是否一致。

参考文献：

[1] 王伟全，张学平，基于岗位抽象的角色权限控制模型设计与实现[J]．软件导刊，2012年1月

［2］普继光．基于角色的访问控制系统的设计和应用［Ｄ］．成都：电子科技大学，２００４．

［3］王电化．基于角色访问控制的研究［Ｄ］．天津：天津工业大学，２００５．

［4］刘萍．基于角色的访问控制（ＲＢＡＣ）及应用研究［Ｄ］．成都：电子科技大学，２００４．

5.8权限挖掘

当前基于角色的权限控制模型（RBAC）已经成为互联网、企业信息系统的主流权限管理模式。RBAC 模型是通过角色、资源、约束来对信息系统的权限进行描述，其具备的直观性强、扩展性高、管理简便的优点，一直以来得到行业的认可，成为信息系统选择权限模型时的首选方案。

但随着企业信息系统的大型化、复杂化，尤其是在云计算、分布式、服务化的发展趋势下，在实际应用过程中也出现了很多实际问题。如：例 1.大型企业组织结构复杂，岗位繁杂，工作边界模糊，逐渐难以应用标准的角色描述定义权限约束，造成角色用户化。例 2.多业态、虚拟组织逐渐引入企业业务模式中，使得信息系统也逐渐由单域向多域进化，用户在每个域下权限均不相同，标准角色集在多域下很难被定义。所以在近些年针对于信息系统权限的治理方法逐渐被提出，并形成了如角色工程治理方法论，通过引入角色挖掘方法与算法模型，对信息系统的权限描述、约束进行设计与过程进行可靠的治理，充分发挥 RBAC 模型的优势。

5.8.1 角色工程

角色工程是用工程技术的方法建立一个正确，完全和有效地角色集，并完成用户-角色和角色-权限的分配，角色与角色之间的继承关系。通过角色工程方法的应用，可以在系统进行权限模型设计时，通过算法较为准确的梳理出标准角色，形成最优角色集，最大限度覆盖系统用户的权限需求，同时满足权限管理要求（最优角色、最小授权）。目前角色工程方法主要分为两种：自上而下（Top-Down），自下而上（Bottom-Up）。

- 自上而下（ Top-Down） 方法是通过分析企业的业务流程，抽象出一个角色集，基于人的主观判断定义角色集，然后完成角色-权限的分配关系，最后构造出 RBAC 系统。自顶向下方法获取的角色更接近企业的需求，具有一定的语义含义，如某些角

色对应于某个部门的某个职位的职责。但是其也有自身的缺陷，比如获取角色的时间代价很大，在一个分工明确的庞大的组织结构中，角色的数目将会很大，RBAC 管理的代价也会随之增大。

- 自下而上（ Bottom-Up） 的方法，即首先构建企业或者系统中用户与权限分配关系，然后利用某些算法思想产生角色集，最后完成角色-权限的分配关系以及构造 RBAC 系统。在此方法下角色挖掘的概念。角色挖掘即应用数据挖掘的方法论，引入权限挖掘算法，使得通过自动化程序进行算法运算，得出最优角色集的方法。目前已经提出的算法有：CompleteMiner 算法，FastMiner 算法，HP Role Minimization 等等。并且已经在后续算法中引入了机器学习能力，使得角色挖掘的精准性持续提高。但也存在运算出的角色集跟企业实际组织关联性弱，没有实际意义的情况。
- 智能分析

基于人工智能机器学习方法的引入，结合自上而下的体现实际、自下而上的自动分析的优点，通过在自下而上角色挖掘的基础上，引入机器学习方法模拟人工自上而下分析的过程，并将结果作为影响因子，参与到角色挖掘的自动运算中。这样即可较为理想的得出角色挖掘结果。目前此类方法还多处于研究状态，未有实际可靠算法产生，但必将成为后续权限智能治理的发展趋势。

6 审计与风控

6.1 常见身份审计项说明

经过多年的安全建设，我们采取了保护、检测、响应恢复等一系列的安全措施。审计管理作为安全措施中关键一环，可用于监控和管理企业信息系统和应用程序中的审计和遵循性。审计管理将用户所有的操作日志集中记录管理和分析，既对用户行为进行监控，还通过集中的审计数据进行数据挖掘，以便于事前预警，事中审计，事后追责。

身份审计通常是指对企业范围内身份数据的系统捕获、分析和响应，以确保遵循内部和外部的策略与法规。

身份安全审计管理主要以日志的形式记录谁进入系统、用什么设备、访问时间、停留时长、来自哪里、查看哪些内容、操作哪些内容等，透过用户行为进一步解析系统的访问量、设备访问组成、平均访问时长、访客来源、时段、路径等。无论是同步至 IAM

的数据信息还是从 IAM 进行审批并分发至各业务系统的数据信息，都会通过日志的方式记录，包括操作审计信息、访问审计信息、数据审计信息等。相关技术或者运维人员可以通过对应的日志、月表等形式进行记录查看，快速对问题进行追溯及查看。

身份审计提供了用于审计用户帐户权限和访问权限的功能，还提供了另一项用于维护和证明合规性的功能。这些功能是基于策略的合规性和定期访问查看。

常见身份审计项如下：

1、对账号分配情况的审计。包括主账号与自然人的对应关系，主账号与从账号的对应关系，主账号的创建时间、创建人，从账号的创建时间、创建人，将从账号分配给从账号的分配时间、分配者，主、从账号的有限期、密码更改规则等。

2、对账号授权的审计。包括查询主、从账号的访问权限，查询资源的授权访问者，权限的分配时间、分配者等。

3、对登录过程的审计。包括什么人用什么账号在什么时间登录了什么系统，什么时间登出等。

4、对身份认证的审计。包括成功的身份认证统计，失败的身份认证统计等。尤其对于失败的身份认证，要求能够给出详细的时间戳、登录位置（IP 或 MAC 地址）、登录凭证、请求身份认证的系统等信息。

5、对登录后用户行为的审计。如果集中授权模块能够达到实体内部资源级，或者应用经过改造后能够向集中审计模块提供日志记录，或者集中审计模块能够读取应用的日志记录，集中安全审计模块还可以对登录后的用户行为进行审计，包括用户访问了哪些资源、对资源进行了什么操作等，在此基础上可以实现对误操作过程的追溯。

6.2事后审计方式说明

事后审计一般由企业内部审计或聘用外部审计进行周期性的身份管理和访问控制的审计工作。查明所有与访问控制和身份管理相关的内部管理活动是否符合公司访问控制要求和制度,是否遵循标准作业流程及相应系统和应用的管理手册进行用户账号管理。

6.2.1 定期审计和不定期审计

定期审计,可按年度或季度进行的对身份管理和访问控制的审计

不定期审计,可根据需要随时进行对身份管理的日常操作进行审查,为出现的未授权账号使用,权限滥用导致的客户信息泄露等情况寻找原因和漏洞。

6.2.2 审计对象

身份管理的全生命周期过程中,应保留包括但不限于以下信息,以便事后审计

1. 创建、修改、删除、密码重置、解锁等动作的用户请求
2. 用户请求的授权
3. 系统或应用的访问控制矩阵(如有)
4. 审计日志

6.2.3 审计事项注意

日常用户申请应得到适当的申请授权,授权人负有对申请人权限的确认工作,以确定是以最小授权的原则赋予权限。授权人应由企业自行依据自身情况做出适当安排,授权人列表应及时更新并进行维护。系统或应用的访问控制矩阵应由系统或应用团队负责维护,并按年度进行检查。有效的用户请求应包含用户的申请,有效的授权以及权限要求符合访问控制矩阵。

审计日志需要包括以下信息，以便追溯：

1.用户创建,修改,删除的时间

2.操作人员账号及操作时间

3.状态更改之前及之后的值

6.2.4 对高权限账户的审计

高权限账户的密码是否被妥善保管。

对高权限账户的申请和使用流程,是否完整。同步检查变更及事件管理中的高权限账户申请和使用情况。

6.2.5 账号的定期检查

所有用户拥有的账号，包括个人账号和有所有者的功能性账号，都需要定期检查。

用户对所检查的账号应标注有保留，删除或更改权限等标记。其中更改权限和删除请求应及时处理，并保留处理信息。

6.3风险发现以及可持续检测

6.3.1 风险发现以及可持续检测概述

账号身份存在误用、滥用、冒用等情况。不当的账号身份使用，可能导致被访问数据资源被泄露、窃取、篡改。账号身份的风险识别不应局限于认证的时间点，对账号身份的持续使用也需进行检测。贯穿账号身份使用的风险发现与检测，能够规避高风险的账号接入，异常账号的持续使用。

风险检测分析时，需对认证信息、授权信息、以及用户所处的运行环境信息进行统一收集、分析。对于不满足认证特征的用户，认定其处于高风险的访问状态，拒绝其接入至网络进行访问。在用户访问过程中，持续计算评估用户的行为风险状态，高风险访问状态的拒绝接入，低风险访问状态的允许接入。其它风险状态，需要补充身份证据信息，增加用户身份的可信度后，才允许接入。账号身份的风险发现以及可持续检测过程如下图所示：

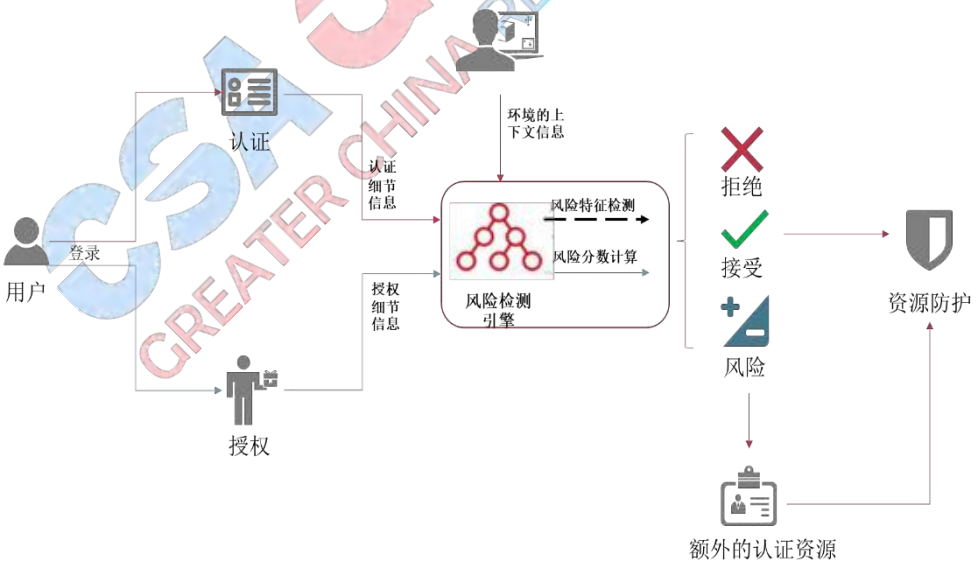


图 1 风险发现检测框架

账号身份使用的风险发现以及可持续检测，主要有风险特征检测和风险分数计算两种方式。风险特征检测的风险发现是一种基于规则检测风险的方式，主要用于检测认证阶段的风险。风险分数计算是一种量化评估的持续检测风险的方式，主要用于检测持续

访问阶段的风险。

6.3.2 风险特征检测

在账号认证阶段，可以通过特征检测的方式，实现合规性检查。根据合规标准要求、单位内部的账号访问要求，设定合规检测集合。合规检测集合中的合规检查项来源于账号访问要求的拆解与映射。合规检查项是识别身份存在的风险的最小检测项。初次认证或者访问不同级别的资源时，会开展身份合规检测，发现安全风险。

当用户访问不同级别的资源时，会自动切换到不同的合规检测集合。当用户从访问低级资源，切换到访问高级资源时。合规检测集合将自动切换到高级检测规则。当用户从访问高级资源，切换到访问低级资源时，合规检测集合将自动降级，且不开展检测任务。当同时访问高级资源和低级资源时，将按照高级检测策略执行。

6.3.3 风险分数计算

持续性的账号风险识别与访问风险检测，可以通过风险分数评分的方式实现。对于用户的访问情况进行持续风险评估，需要考虑授权风险的累积，程序的运行环境、用户的历史访问行为。

每一个对象被授权使用，都意味着风险的累积。在量化评分之前，需做一些预先的准备工作，充分定义授权对象使用存在的风险。在安全管理员的统筹下，不同管理员根据自身的职责不同，负责定义不同对象的授权使用风险值。风险值的设定对象主要包括用户账号、系统角色、合规规则、用户等。不同的管理员，对所负责资源、服务的重要程度了解的最为清楚。所以设定风险的参数能够较为准确的反应资源所需的安全性。

结合资源授权风险，收集用户访问属性、区域属性、设备状态、最近认证设备、最近授权的位置、HTTP 请求参数、时间、速率等各类访问参数，进行综合分析计算，形成风险指标值。风险指标值代表该次访问的风险级别。

风险值的计算有多种类型，常见类型如下所示：

1. 求和。对关注的所有风险值进行逐项相加，计算总体风险。
2. 加权求和。对关注的风险值进行逐项加权求和。根据实际情况，动态调整权重系数，计算总体风险。
3. 单向递增。对于单向递增的风险，设定基础风险值，以及递增步长，逐步增加风险

值。

4. 单向递减。对于单向递减的风险，设定基础风险值，以及递减步长，逐步减小风险值。
5. 求均值。对于需要平均值进行反应的风险情况，对所有风险值进行逐项相加，然后除以项数和。
6. 加权平均。对于需要加权平均值进行反应的风险情况。对所有风险值进行逐项加权相加，然后除以项数和。根据实际情况，动态调整权重系数。
7. 算法模型。对于复杂风险的计算需要建立数学模型，进行多维指标的综合计算。

6.4 UEBA

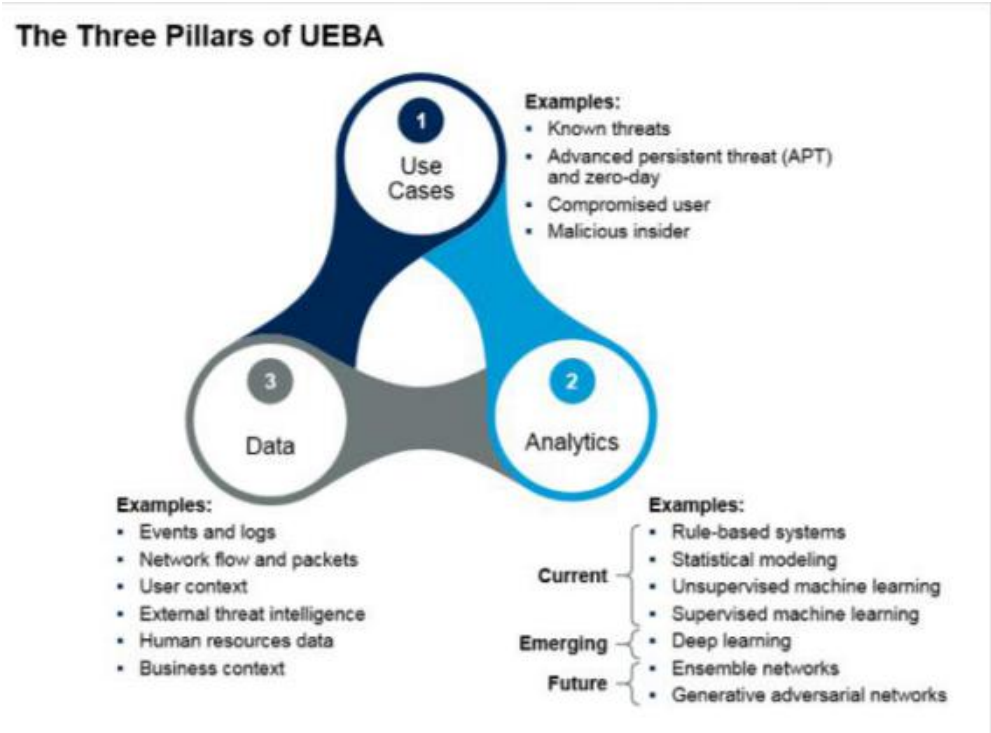
用户和实体行为分析(UEBA)是使用分析来构建跨越时间和对等组的用户和实体(主机、应用程序、网络流量和数据存储库)的标准配置文件和行为。与这些标准基线不一致的活动被表示为可疑的，应用于这些异常的打包分析可以帮助发现威胁和潜在事件。企业寻求的最常见的用例是检测恶意的内部人员和渗透到其组织的外部攻击者(受损害的内部人员)。

UEBA 将此分析扩展到用户以外的“实体”和“事件”，例如路由器，服务器和端点。 UEBA 解决方案比早期的 UBA 方法更强大，因为它们可以检测跨多个用户，IT 设备和 IP 地址的复杂攻击。

用户和实体行为分析首先从系统日志中收集有关用户和实体正常行为的信息。然后，这些系统应用高级分析方法来分析数据，并建立用户行为模式的基线。然后，UEBA 连续监视实体行为，并将其与相同实体或相似实体的基准行为进行比较。

该分析的目的是检测与“正常”模式有偏差的任何异常行为或实例。例如，如果特定用户每天定期下载 10 MB 的文件，但突然下载了千兆字节的文件，则系统将能够检测到此异常并发出潜在安全威胁的警报。

UEBA 包括三个主要组件，这些组件对其功能至关重要：



数据分析使用有关用户和实体“正常”行为的数据来构建它们正常行为的配置文件。然后可以应用统计模型以检测异常行为并警告系统管理员。

数据集成意味着 UEBA 系统能够将各种来源的数据（例如日志，数据包捕获数据和其他数据集）与现有安全系统进行比较。

数据用例是 UEBA 系统传达其发现结果的过程。 通常，这是通过发出请求让安全分析人员调查异常行为来完成的。

使用 UEBA 的最佳实践

1、培训员工

正确使用 UEBA 系统的最重要要素之一是确保您的员工拥有使用这些系统所需的知识和技能。网络安全备忘录模板可以使您了解网络安全对您的员工的重要性，您应该全年提高安全意识和网络安全最佳实践。对于 UEBA 系统而言，对于任何其他类型的安全软件而言都是如此。

考虑内部威胁

与 UEBA 系统一起使用时，一个更具体的技巧是确保在制定规则和策略来检测攻击时确保考虑整个威胁状况。 UEBA 的主要优点之一是，您可以像从组织外部一样有效地检测内部威胁，但前提是您已经配置了系统以寻找内部威胁。

锁定访问

与您使用的任何其他系统一样，保护 UEBA 系统的安全也取决于您向适当的员工授予适当的特权。不要让所有人都可以访问您的 UEBA 系统-而是只有相关的团队成员才能看到此数据，并且他们也应该是从系统中接收警报的唯一人员。

提防特权升级

不要将非特权用户帐户视为无害。黑客通常会将这些帐户作为目标，然后尝试提升特权以渗透敏感系统。 UEBA 系统可以帮助检测未经授权的特权升级，因此您应该配置软件以警告您任何此类情况。

使用其他工具

不要将 UEBA 流程和工具视为入侵检测系统（IDS）等基本监视系统的替代品。UEBA 系统是对传统监控基础结构的补充，而不是其替代品。

UEBA 和访问管理

利用 UEBA 进行授权和自适应访问管理用例。自适应访问是连续自适应风险和信任评估（CARTA）方法的 IAM 特定实例。 “自适应访问控制技术概述”将自适应访问控制定义为上下文感知访问控制的一个实例，它结合了信任提升和其他动态风险缓解技术，可以在访问时平衡信任与风险。例如，风险评分可用于动态调整用户的访问级别，或使用多因素身份验证（MFA）要求用户重新进行身份验证。自适应访问的身份分析功能应是选择访问管理解决方案的首选功能。

UEBA 和身份治理与管理

身份治理和管理（IGA）供应商使用 UEBA 来启用行为和身份分析用例，例如异常检测，动态对等组分析，登录分析和访问策略分析。

身份分析使 IGA 市场朝着更具预测性和规范性的分析方向发展，例如，允许对工作流批准进行动态风险评估。较低风险的访问请求批准可以自动进行，而无需经理或应用程序所有者的手动批准。可以根据这些分数实时验证访问请求，从而将传统上以合规性为重点的 IGA 平台转变为面向风险的“即时治理”引擎。身份分析可以计算风险指标，例如登录活动的高峰，异常登录行为，流氓或异常访问，被遗弃和处于休眠状态的帐户，对敏感的非结构化数据的访问或违反职责分离（SOD）的行为。

7 CIAM 体系说明

7.1.1 CIAM 定义

随着软件的边界拓展到我们生活的方方面面，统一管理身份的需求也不断拓展边界，以企业为核心，由内而外，企业也开始管理外部的海量顾客身份，由此诞生了针对互联网用户的顾客身份管理（Customer Identity & Access Management 简称 CIAM）。

顾客身份访问管理 (CIAM) 技术与传统的企业身份访问管理 (IAM) 技术侧重点有很大区别，传统 IAM 技术旨在管理员工对内部系统的访问。而 CIAM 技术则不同，它的设计初衷是帮助企业尽可能从客户概况数据中挖掘价值。企业身份访问管理 (IAM) 更关注权限的细化、CIAM 更关注业务的融合体验。

CIAM 平台需要助力企业打造无缝、流畅的客户体验，因此需要平滑接入各种社交平台登录、身份验证或流程管理等任务，并且 CIAM 平台还需要帮助全球企业遵守各种不断变化的隐私性法规，满足企业跨公共网络保护个人数据的关键需求。

表概述了传统 IAM 和 CIAM 之间的主要区别：

传统 IAM	CIAM
侧重于企业内部员工的身份安全统一管理。	侧重于面向客户、多渠道网站(Web、移动、IoT)上的 客户身份统一管理，向客户提供一体化数字服务体验。
企业规模从几十个到几万个用户，每个用户一个身份。	最多可扩展至数亿个用户，甚至几十亿个消费者身份管理。
用户通常由企业内部提供，主用户数据通常由 HR 或主数据系统提供。	顾客自行注册并生成自己的用户特定数据。
用户是已知和受控的个体如:员工、承包商、合作伙伴。传统身份提供程序通常是一个内部 IT 系统。	用户是未知的(注册前)并可能创建多个虚假帐户。众多分散的身份提供程序:通过第三方社交登录以及传统注册登录，例如：微信、QQ、 微博等。
企业统一提供门户和管理规范	需要良好的用户体验和注册流程
为管理和运营目的而收集的员工档案数据。	为极为关键的业务目的(交易、营销、个性化、

	分析和商业 智能)而收集的顾客档案数据。
通常与 HR 和 ERP 系统集成。	与营销和销售自动化技术、分析系统以及安全和合规性解决方案组成的广泛环境集成。
仅在严格控制的同构公司环境中管理个人数据和用户隐私、偏好、许可。	处理受各种隐私和数据保护法规约束的个人数据，这些法规要求允许用户查看、修改和撤消偏好和许可设置。

7.1.2 CIAM 非功能性要求

基于通过安全识别新客户、提供个性化服务和提供相关通畅体验来获得新的忠诚客户。打造 CIAM 平台基本要求有如下要求。

顺畅的客户体验

根据不同业务的独特需求，定制灵活的注册与社交认证界面和流程，进而为客户提供顺畅的体验。

安全识别访客

使用业界安全技术标准，如单点登录、基于风险的身份验证、多因子身份验证和免密身份验证，保障每个用户的认证安全。

为企业建立统一的客户视图

建立索引式动态数据库，集中存储用户画像数据，结合数据分析技术打造个性化的体验。

符合隐私性和数据合规标准

在确保数据安全可靠的同时，CIAM 系统需要专注于企业和客户的关系。并确保在云端和企业内部数据中心的合规性和数据安全性。在 CIAM 系统中，隐私保护是非常重要的要求。

以下章节也会针对 CIAM 系统关注的用户隐私提出要求。

7.2用户隐私许可

用户使用相关互联网资源和软件的时候，经常会收到隐私许可的提示，提示用户确

认和许可使用。确认隐私许可完毕，相关企业就可以收集和使用客户的数据。用户隐私许可关系到客户的信任，也给企业带来巨大的安全和风险问题，各国政府都在修改消费者隐私保护规则。

对于需要管理用户信息和保密数据的企业或者组织而言，有效的隐私保护手段越来越受到重视。目前，隐私保护的实施方向主要集中在三个方面：司法机构立法以及权威机构制定行业内隐私保护规范，提高互联网用户个人隐私保护意识，在互联网应用中加入加强隐私保护的技术实现。

世界各国立法主要有三种概念：个人数据、个人隐私与个人信息。以“个人数据”称谓的主要以欧盟成员国及受其影响较大的国家，如法国《资料保护法》、挪威《资料登录法》和欧盟新通过的数据保护法案《通用数据保护指令》（GDPR）；以“个人隐私”称谓的主要有普通法国家，如美国《隐私权法》、加拿大《隐私权法》、澳大利亚《隐私权法》和 PDPA《新加坡隐私法》；使用“个人信息”概念的，如奥地利《信息保护法》、韩国《公共机构之个人信息保护法》，以及俄罗斯《俄罗斯联邦信息、信息化和信息保护法》等；我国香港地区 PDPO《香港隐私法》，则以资料、隐私来概括个人信息。

我国也陆续颁布、实施了一系列法律、规范，例如《中华人民共和国网络安全法》，强调了中国境内网络运营者对所收集到的个人信息所应承担的保护责任和违规处罚措施。在《中华人民共和国网络安全法》中，公民个人信息安全的保护被放在了重要位置。2019 年 12 月国家网信办、工业和信息化部、公安部、市场监管总局联合出台了《App 违法违规收集使用个人信息行为认定方法》。其中明确“要求用户一次性同意打开多个可收集个人信息的权限、用户不同意则无法使用”可被认定违法违规。

信息通信管理局要求各互联网企业严格遵守相关法律法规，遵循合法、正当、必要的原则收集使用个人信息，不得收集服务所必需以外的用户个人信息，不得将信息用于提供服务之外的目的，不得非法向他人出售或提供个人信息，同时进一步优化服务协议、用户隐私政策和手机权限调用说明，切实保障网用户知情权和选择权，维护用户合法权益。

隐私保护法律法规和行业规范之间，有一些基本的特性，这些基本特性作为隐私保护技术实现的主要原则和依据。这些原则主要包括：

1)通知原则(Notice)：信息管理者在收集信息时需要通知当事人收集个人信息的目

的、个人信息已遭收集的事实、信息管理者的身份、当事人修改信息的途径；

2)数据完整性(Data integrity)：信息的收集和使用应该与使用目的相一致，重新获得当事人同意或者获得法律授权或者是公开的个人信息情况除外；

3)选择原则(Choice)：个人信息管理者适当时应提供当事人就其个人信息收集、利用和披露行使选择权；

4)访问原则(Access)：为符合所需要的利用目的，个人信息应维持正确、完整并加以更新；

5)安全原则(Security)：个人信息管理者应妥善地维护个人信息，防止未经授权获得、损毁、利用、修改或披露个人信息；

6)传递原则(Onward Transfer)：当事人应被赋予合理的获知、更正、补充、修正或删除被持有的个人信息的机会，在信息向第三方传递时，信息管理者负有负责执行通知和授权访问的义务；

7) 责任原则(Enforcement)：个人信息管理者应负遵守上述原则的责任。第七点是法律规范中常使用的责任原则，其余六点可作为互联网应用中隐私保护的目标和隐私保护策略制定的规范。

在整个隐私保护的流程当中，企业通过用户隐私许可得到用户的同意和授权。企业应采取适当手段保护客户的隐私。每当客户提供给企业敏感信息时，企业应采取合理的技术保护客户的敏感信息，并且保护已存储的个人信息。在未得到客户的许可之前，企业不能把任何个人信息提供给无关的第三方（包括公司或个人）。

一个合格的用户隐私许可，可以帮助企业清晰明确向客户展示使用的条款和隐私政策，为后期企业捕捉、记录、存储和使用提供知情同意信息，从而保障企业和客户的利益。

7.3 用户授权同意

用户授权同意是管理获取用户信息和响应客户对使用其个人和敏感数据的授权过程。大多数隐私法规要求消费者和客户提供授权，用户授权同意后公司或组织才能使用个人数据使用的权利。 公司或者组织必须获得用户授权的同意（无论是明示的还是隐含的），未经授权提供用户个人信息等侵害用户权益的情况是违规违法行为。

企业应为客户更改同意书提供清晰明显的工具或方法。 用户授权同意条款可以通

过表单上的隐私或同意按钮、应用程序中的设置或客户交流中的同意选项。

企业的信息管理员可以获得完整的用户授权同意审计记录应对合规性检查，同时客户也应该可以随时查看和更改授权同意相关内容。当条款和政策发生变化，系统可以通知客户更新他们的设置，并重新获取用户授权同意，让客户需要知道自己的数据如何被使用。

企业需要进行哪些控制才能有效地进行用户授权同意管理？

- 如何使用个人数据。
- 是否将个人数据与合作伙伴共享。
- 如果将使用个人数据和将向客户提供其他优惠。
- 是否出于研究或分析目的共享个人数据。

组织如何获得同意选择？

- 书面合同。
- Web 表单中的复选框。
- 在应用程序中设置。
- 回复电子邮件。
- 对口头问题的口头答复。

有效的同意管理有哪些关键要求？

- 自动的 Web 通知以获得同意。
- 存储客户同意选择的数据库。
- 客户交流应用程序和广告合作伙伴添加/撤回同意的工作流程。
- 报告和审核功能可查看总体同意统计数据以及个人的同意偏好和历史记录。

用户授权同意是企业受客户信赖的基本过程，让客户随时随地对他们偏爱的品牌或者企业做出知情同意。让客户真正同意提供自己个人信息，赢得最终用户的信赖和忠诚。

用户授权同意是企业受客户信赖的基本过程，让客户随时随地对他们偏爱的品牌或者企业做出知情同意。让客户真正同意提供自己个人信息，赢得最终用户的信赖和忠诚。

8 IDaaS 体系说明（Identity As A Service）

8.1 IDaas 的定义

8.1.1 背景

现代企业面临着为成千上万个用户在访问众多应用程序时，提供安全的身份管理、身份验证、集中授权和单点登录（SSO），确保每个用户仅具有最小访问权限的挑战。同时在用户身份全生命周期管理以及对法规遵从性方面给企业增加了复杂性。通过身份和访问管理（IAM）软件能解决上述挑战。同时，云计算正在重塑 IT 和企业的运营方式，基于身份即服务、云化的 IAM 解决方案（IDaaS）得到快速发展。

传统 IAM 能支持本地应用程序的身份与访问管理，但对于基于软件即服务（SaaS）的应用中，如大数据分析、物联网等场景中，本地 IAM 使用受限，部署昂贵、复杂且耗时，并容易出现安全漏洞。身份即服务（IDaaS）是在云上部署的基于 SaaS 的 IAM 解决方案。IDaaS 提供了端到端的企业级 IAM 服务，可为移动计算、大数据分析和物联网提供无缝 SSO 集成。通过云，组织可以获得简化的 IT 架构，快速的系统部署，更低的总拥有成本（TCO），以及增强的功能以实现数字化转型目标。

8.1.2 定义

IDaaS 的核心是基于云的 IAM 软件即服务（SaaS）产品。IDaaS 利用具有云服务功能的成熟 IAM 解决方案的功能，使用经过验证的体系结构来提供技术优势并满足业务目标，并为高级集成功能打开了大门。

IDaaS 作为基于云的 IAM 解决方案，需具备以下几个核心特征，并且与供应商无关：

»SaaS 产品提供云计算体系结构的所有优势：尽管云服务提供商在其基础架构上维护 IAM，但此部署模型为 SaaS（而不是 IaaS 或 PaaS），因为消费者仅通过批准的界面（Web 浏览器，API 等）访问 IAM 软件，并且不负责管理或维护基于云的资产。

»多租户架构，其中有多个客户以安全的方式共享相同的云 IAM 基础架构：这种区别可确保客户确实在接收云部署的解决方案，而不是从其他托管提供商部署的本地 IAM（伪装成云）。

»对本地和基于云的应用程序的混合支持：组织既拥有本地应用程序，又具有分布式，移动和云托管的应用程序； IDaaS 解决方案支持越来越多的本地应用程序。

成熟的 IDaaS 解决方案固有的强大功能是基于云的应用程序可以深入到消费者的数据中心，向外移动用户以及跨其他基于云的应用程序（通过 SaaS，PaaS 或 IaaS 托管）的能力。

由于 IDaaS 是从云托管的，因此无论其位置或拓扑如何，它都支持应用程序：

»本地企业用户»位于全球任何地方的移动用户»基于 Web 或 SaaS 的应用程序，例如 MS Office 365，Salesforce，Google Apps， Workday 或 ServiceNow

»在 IaaS 或 PaaS 云环境中托管的应用程序

IDaaS 之所以功能强大，是因为作为 SaaS 应用程序，它能够到达存在网络（甚至无线）连接的任何地方，而无需客户现场的硬件。

8.2IDaaS 的技术特征

伴随着企业整体接受云方案，将越来越多的本地基础架构和应用迁移上云后，身份成了企业不得不面对的一个话题。企业需要拥有一套能够适用于纯云环境、多云环境甚至横跨 SaaS、IaaS、PaaS 的统一的身份管理方案。IDaaS 的出现就是为了解决这样的问题，并且 IDaaS 正在变得越来越成熟。在 Gartner 的 2019 年 IAM 魔力象限中，能力最强的如 Okta、Microsoft Azure AD 都是 IDaaS 的产品与方案。从功能实现上来讲，IDaaS 已经是一个非常完整的 IAM 方案了，我们就不再赘述 IAM 的功能。这里我们简单列举一下 IDaaS 相较传统 IAM 所具备的特点和优势。

8.2.1 高可用性

IDaaS 服务提供商一般都有 SLA 的保障。IDaaS 基于云基础架构，因此在高可用性上，可以充分利用云基础架构的灵活性。多数据中心、多可用区、就近接入与验证，已经成为 IDaaS 服务商的标准配置。

8.2.2 深度分析

IDaaS 平台每天都会处理海量的认证请求，会包含请求的各种相关信号，如浏览器、

IP 地址、设备信息、时间等等，这些信息大量沉淀后，将会给 IDaaS 平台提出挑战，如何使这些数据产生价值。依托于这些海量数据以及 IDaaS 平台自身的技术能力，主流 IDaaS 平台都会通过大数据与 AI 技术来为最终用户服务。目前 IDaaS 一般会提供如下的附加功能：

1. 身份分析：这将通过 BI 展现整体的身份与授权的使用情况以及风险情况，从多个维度提供给 IT，让 IT 了解整体的 IDaaS 的验证和使用情况。
2. 安全与审计服务
   a) 基于用户及实体行为分析(UEBA)的外部风险识别
      i. 通过了解企业组织内或者大多数企业用户的正常登陆行为作为基线，可以快速定位出可能存在风险的特定用户以及特定登陆请求。如非常用地、常用设备、常用时间的登陆行为等。
      ii. 由于近年来针对用户身份的攻击行为越来越普遍，IDaaS 也逐步建立起自己完善的威胁情报信息，这些信息也会通过内置或增值服务的方式提供给最终用户，如来自僵尸网络的 IP 登陆、凭据已泄露的用户等等。
      a) 基于用户及实体行为分析(UEBA)的内源威胁识别（Insider Threat）：传统企业在面临外部入侵风险的同时，越来越多 IT 开始重视来自于内部员工的威胁。对于信息的有意或无意的滥用，会对企业造成比外部威胁更大的威胁。由于 IDaaS 继承了企业的大部分乃至所有的业务系统的验证，因此从用户的登陆、授权、访问的分析出发，可以结合 AI 技术，给到企业 IT 关于内源威胁更多的信息与建议。

8.2.3 易于集成

对于 IDaaS 提供商而言，如果支持用户业务和身份系统的快速对接，是必须考虑的。大部分 IDaaS 会从以下几个场景简化对接。

a) 与现有身份系统的对接，比如与 Active Directory。

对于这样的场景，大多数 IDaaS 都会提供工具，通过简单的配置，将现有身份系统与 IDaaS 打通，保证原有身份系统快速迁移到 IDaaS 中。

b) 对接第三方的 SaaS 应用

目前越来越多的企业会使用第三方的 SaaS 云服务，如 salesforce，Office 365 等等。

IDaaS 厂商往往以及内置支持了上千种的主流 SaaS 应用，企业 IT 只需要简单配置，就可以实现 IDaaS 对于 SaaS 应用的验证和授权的接管。

c) 对接第一方自研应用

对于这样的场景，IDaaS 需要提供主流协议的支持，如 OAuth2、OpenID、Saml2.0、WS-Fed 等等，与此同时，也需要提供主流开发平台的 SDK，来简化开发者接入的开发过程。

此外，对于企业内网的传统应用，无法进行改造的，IDaaS 也需要提供对应的 Web 网关（反向代理），能够在企业进行部署，与传统应用进行对接。这样，对于遗留的老的业务系统，也可以通过现代化的验证方式，来进行验证和授权。

8.3IDaaS 的使用场景

8.3.1 单点登录

随着业务系统越来越多，特别是各种类型的 SaaS 应用，企业的 SSO(单点登陆)的需求越来越强烈。一个统一的身份、一次登陆，即可访问所有其他有权限访问的应用，无需再次登陆。已经成为改善用户体验的重要因素。

IDaaS 平台，提供良好的对于 OAuth2、OIDC、SAML、LDAP 等国际标准的适配，能够快速帮助用户将 SaaS 应用、自研应用进行接入。同时，在接入后，能够通过 IDaaS 平台设置策略，来控制用户访问应用的权限与策略，提升安全性。

同时 IDaaS 平台也会提供响应的应用门户，提供一共统一的 SSO 应用入口，帮助用户在登陆后，快速找到可访问的应用，并且无需再次登陆。

8.3.2 自助服务

传统身份系统如 Active Directory，一般都要求在内网环境进行最终用户的自助服务，如重置密码、申请权限等。传统 IT 的 helpdesk 有相当大量的服务请求，都是与密码相关的。

由于 IDaaS 是纯 SaaS 的服务，因此最终用户可以在任意时间、任意地点、任意设备来访问 IDaaS 所提供的服务。因此对员工提供自助服务，将能够极大减少 helpdesk 的服务量并提升用户的体验。一般 IDaaS 所提供的用户自助服务包括：

1. 密码重置
2. 多因素验证选项配置，如手机号码设置、PIN 码设置、OTP 应用配置等
3. 权限申请

8.3.3 身份保护

8.3.3.1 多因素认证

针对于身份的攻击，大多数是通过各种技术手段完成凭据窃取，从而突破防线。因此 MFA（多因素认证）越来越受到重视。而在启用 MFA 后，90%以上的身份攻击行为将可以被阻挡在外。最终用户将必须在输入用户名和密码后，再经过一次多因素认证，方可登陆成功。

在 IDaaS 平台，常用的多因素认证技术包括：二次验证手机应用、软件 Token 的 OTP、基于硬件 Token 的 OTP、短信、电话、生物识别等。

当然，现在也有非常多 IDaaS 平台，会按照当前登陆用户的行为（UEBA）来智能判断是否需要自动启用多因素认证，这是在安全和用户体验之间寻找一个高效的平衡点。

8.3.3.2 弱密码检查

由于现在对于密码爆破的手段越来越多，也越来越丰富，我们传统的密码复杂度已经无法满足对于密码安全性的要求。很多用户会设置满足复杂度的密码，但是确实实实在在的弱密码，比如 Password01!。

IDaaS 平台会维护更完备的密码复杂度要求，除了传统的复杂度要求以外，也会维护已知的常见弱密码库，并保持更新，用于防止用户设置常见弱密码。同时，也会支持管理员设置禁用密码，特别是去禁用一些与公司名、组织名非常相近的密码，以防止密码被暴力破解。

8.3.3.3 无密码验证

我们知道启用多因素认证，将大大提高用户名和密码的安全性，那么如何更近一步呢？如果我们从根本上就取消了密码呢？

如今，企业安全部门已经通过生物识别、PIN 码、非对称加密技术逐步开始无密码化的进程。同时，新的行业标准如 WebAuthN、FIDO2 的出现，为我们提供了跨平台实现无密码化的标准。这些标准主要是希望通过目前已经在企业里使用的指纹识别、智能手机、摄像头等等来取代密码。无密码化将帮助企业提供一个易于用户使用并且更高安全的验证方式。

在 IDaaS 平台上，无密码化支持也已经非常丰富，通常他们除了开发自己的软件应用外，还会积极与 FIDO 以及硬件厂商合作，推进无密码化技术的推广。

8.3.4 B2B 场景

如今，绝大多数的公司都需要与外部的客户、合作伙伴、供应商、承包商进行协作，也需要开放一定的内部系统的访问权限给到这些外部的人员，用来提高协作的效率。但是企业的 IT 如何去管理和维护这些外部用户的身份呢？

因此企业之间的联合身份认证与管理，就随之产生。通过 IDaaS 的 B2B 联合身份认证，合作伙伴的员工依然通过自身的验证系统进行验证，验证后对于企业应用的授权和访问管理，由 IDaaS 侧统一管理。

借助于 B2B 场景，外部用户可使用自己的身份管理解决方案，因此省去了 IDaaS 用户管理外部身份。主要有以下三点：

a) 外部用户使用自己的身份和凭据；
b) 不需要管理外部帐户或密码。
c) 不需要同步外部帐户或管理帐户生命周期

8.3.5 B2C 场景

身份和凭据管理是一个非常重要的环节，对于企业来讲，当他们提供给消费者端应用以及服务时，身份验证也是一个必不可少的环节。并且如何便捷得与第三方的身份系统（如微信、微博、Facebook 等等）进行对接以简化用户的注册和登陆过程，也是企业经常要考虑的部分。同时，由于收集了大量消费者的数据，安全和隐私保护往往有更高的要求和标准。

因此通过 IDaaS 平台提供的 B2C 功能，可以使用 IDaaS 统一管理对消费者的身份管理，通常会提供以下能力。

a) 自定义消费者注册、登陆、个人信息管理，将 UI 和流程自定义成符合企业要求的元素。

b) 通过标准协议如 OAuth 2.0, OpenID Connect, SAML 2.0, and WS-Federation 与第三方消费者端身份提供者进行联合身份认证，比如微信、微博、Facebook、Hotmail 等。

c) 隐私保护选项。提供因此策略说明以及配置，是否追踪或者分享用户登陆行为以及使用情况。

d) 用户管理与登陆分析。管理消费者端注册的用户，包括多因素认证、安全策略以及登陆分析与审计。

8.3.6 特权账号管理

IDaaS 维护了应用的身份与授权，因此 IDaaS 的管理员或者高权限的账号显得极为重要。企业希望能够减少拥有访问敏感信息和资源的特权账号的分配。因此 IDaaS 都会提供特权账号管理的功能。

一般特权账号管理，在 IDaaS 测，会通过以下手段来进行特权账号的管理：

a) 提供 JIT(just-in-time)的访问模式，即使用时提权，使用后降级到普通用户权限。

b) 提供自定义权限时间，仅在设定时间内权限有效，时间超出后，权限自动回收。

c) 提供审批流，用户需要特权时，须提供说明并获得审批后才会授予特权。

d) 通过多因素认证提高特权账号的登陆安全性。

e) 定期对特权账号进行汇总，确保无多余特权，做到及时回收。

f) 详细的特权使用审计报告

8.3.7 合规与审计

随着全球对于隐私保护的监管越来越强，由于 IAM 平台储存了大量的用户信息，对于 IAM 平台也提出了同样的要求。由于 IDaaS 是 SaaS 服务，根据云服务的责任共担模型，企业是无需关心应用、主机与网络以及物理和基础架构的安全和合规的。大多数的 IDaaS 厂商都会提供其相关标准证书或者说明，比如针对于 GDPR、HIPPA、等保等。

这将大大减少企业 IT 在一块的精力的投入，让企业可以更专注于数据以及终端的合规与审计。

9 IoT 身份管理体系说明

9.1物体身份唯一标识说明

物联网（IoT）以我们尚未完全了解的方式影响企业，社会，文化和个人。将物理设备和服务连接到个人和企业已广泛部署。物联网应用涉及关键基础设施，重要的国家产业，产业应用，广泛的数据收集以及许多业务场景，再加上物联网终端的庞大规模和复杂的部署环境，物联网面临着复杂的安全风险。

物联网设备必须更好地管理，监视，保护和集成物联网以支持各种用例。这个新兴且无处不在的物联网生态的基础需要可扩展的方法来确定如何识别，保护和访问设备以及这些设备收集的数据，以防止物联网引起的安全风险。

将身份应用于物品与将身份应用于人基本相同。 为了识别一个用户，我们将该用户的属性集合存储，以便从识别该用户，同样适用于物联网设备的身份。 设备还应具有一些可用于唯一标识该设备的属性。 并且应该有一种机制来存储它们并对其进行处理。 这导致开发了一个新的身份和访问管理（IAM）类别，称为物联网身份（IDoT – Identity of Things），该类别支持物联网设备的独特性，关系和权限。一个有效的物联网生态系统必须考虑安全性和身份验证是实现该目标的一种方式，无论是涉及工业互联网还是简单地利用物联网设备的优势来补充运营流程。

物联网身份服务还必须支持与物联网设备关联的各种形式的硬件标识符的身份验证。由于大多数传统的 IAM 供应商都处于全面支持此类别的早期阶段，因此很多企业最初通过利用具有物联网扩展功能的云和平台提供商以及围绕主要物联网硬件提供商设备构建的新兴生态系统来识别和管理物联网设备。我们将扩展这些基于战术筒仓的方法，将传统的 IAM 系统演变为支持物联网身份（IDoT）。

9.1.1 物体身份标识类型

物联网身份用于产品以方便产品认证，防伪验测，溯源追踪，更能提高供应链透明度来杜绝假冒和/或不合格商品，以确保您的食品质量和产品安全。

物品的身份就如同产品的出生证明，用于跟踪产品流向，即从厂家到消费者，消费者的信息通过隐私授权也可以被企业利用。目前物品的标识常用的有条形码、普通二维

码、双层二维码、NFC、RFID 等。企业把标签附加到产品。品牌或产品制造商，可授权他们的渠道伙伴使用智能手机扫描产品，从而了解物流和产品渠道。而顾客也可自行使用智能手机扫描，了解产品信息和验证产品身份。

在这么多的物品身份标签中，不同的场景需要不同类型标签选择，来方便最终用户和企业使用。企业在选择便利的标签的同时，也要考虑成本、普通用户使用习惯和投入回报率。因为智能手机的流行和成本的考虑，目前标签二维码和防伪二维码使用比较常见。

每种物品标签类型都有其优点，也可用于记录产品的不同状态。下方是最常见的物体标识。

防伪防复制的二维码

防伪二维码将唯一数码水印和相应产品身份信息增加到普通的二维码，然后再经过序列化和加密后得出的结果。因此这种防伪二维码具有防复制的安全特性，防伪二维码可以直接印在产品包装、标签和文件上，若标签一旦被复制，在扫描复制品的过程中，顾客就会得到警告信息

快速响应码（二维码）

可直接打印到产品包装上（节省成本）

可提供产品信息

近场通信（NFC）标签

产品的当前状态（工厂密封/ 开封）

可提供有关产品的信息

通常隐藏在产品中

射频识别（RFID）标签

产品的当前状态（原厂密封或开封）

适用于仓库批量产品标签扫描，便于更新状态

可提供有关产品的信息

通常隐藏在产品中

条形码

支持一维条形码

可直接打印到产品包装上（节省成本）

可提供产品信息

9.1.2 选择物体身份唯一标识关键标准

每种物体身份标识类型都有其优点，也可用于记录产品的不同状态。针对不同的物品类型和使用场景，可以选择不同的标识达成使用的目标。总体来讲选择物体身份唯一标识关键标准需要考虑以下因素。

1. 产品能可靠认证，不会引起歧义
2. 诸目标团体应该能使用易于使用的工具来轻易阅读功能
3. 特征具有防篡改彰或无效彰的效果
4. 采用这些功能不会对制造商现有的生产过程产生影响
5. 采用的功能应该能融入现有的供应链和零售环境中
6. 为业务决策提供即时的数据

9.2IoT 身份互联方式（人物互联、物物互联）（说明互联方式即可采用的认证手段）

物联网的身份认证所面临的挑战要比传统的互联网大的多。主要体现在：物联网哑终端设备应用环境恶劣，容易遭受物理破坏、恶意篡改和信息的窃取；物联网哑终端设备更新升级困难，无法及时对安全漏洞进行修补，致使攻击者利用漏洞获取身份信息，与其它节点设备进行通信；物联网哑终端设备存储、计算、通信资源受限，对于资源需求较高的安全加密、数字证书等传统的认证技术则无法应用。因此，物联网中的设备在身份认证方面需要解决物联网终端设备、用户的基于身份伪造和泄露的攻击，保证认证信息的安全。

物联网身份互联的方式分为人物互联和物物互联这两大类。其中人物互联主要包括物联网用户与物联网应用平台的互联（即用户与应用互联），以及物联网用户与物联网终端设备的互联（即用户与哑终端互联）；而物物互联主要包括物联网感知终端设备间的互联（即哑终端间互联），物联网应用平台与感知终端设备的互联（即应用与哑终端间互联），物联网应用平台间的互联（即应用间互联），以及物联网应用平台与物联网存储服务器的互联（即应用与平台存储间互联）。

9.2.1 人物互联

对于物联网用户的身份认证，主要是通过有效的技术手段来确认该用户的身份，并根据确认的身份确定其是否具有相应的权限对物联网应用平台或终端进行操作。需要注意的是，因为物联网应用场景的复杂性，实际认证过程中需要结合实际的应用场景进行身份认证方式的选择。根据在认证过程中是否需要连接身份认证服务器，可将用户身份认证分为离线认证和在线认证两种。离线认证则是用户的身份认证凭据存储在物联网终端设备中（如用户设置的账号密码或者录入的生物特征等），在认证的过程中，无需连接平台的身份认证服务器即可完成用户身份的认证。在线认证则是在认证的过程中，需要连接到平台的身份认证服务器来完成对用户身份的认证和管理，如通过远程人脸识别等。

用户与应用互联

物联网用户（包括人类用户和数字用户）与物联网应用平台的互联，实现了用户与

物联网平台的数据交互。人类用户通常使用某种数字设备与物联网平台进行交互；而数字用户则是通过 API 与物联网平台交互。

物联网的网络信道远比传统网络复杂的多，安全机制往往不像传统互联网和移动互联网那么完备，容易导致与用户认证相关的敏感信息的泄露。因此，物联网用户与物联网应用平台的身份认证多采用双向认证的方式实现在线认证。从而保障信令和用户数据的安全传输。采用的认证手段有静态口令认证、动态口令认证、生物特征识别认证以及多因素认证等。

除此之外，还可采用基于 Token 的身份认证机制，Token 中文含义是令牌，即保存于物联网应用系统中用于验证用户身份的一种凭据。当物联网客户端（包括用户或者终端设备）发起登录或连接请求时，物联网平台服务器会根据用户或者终端设备的注册信息，生成一串用于用户访问凭据的字符串，并将其反馈给客户端作为 Token 令牌。它可以较好的解决传统的口令身份认证机制在存在大量异构感知设备的物联网应用中的局限性问题。

采用的身份认证手段有令牌认证、口令认证、生物特征识别及双因素认证等，根据不同的物联网应用场景选用不同的认证方式。

用户与哑终端互联

物联网用户与哑终端设备的互联则是实现了用户与哑终端设备的一个交互。物联网用户可直接访问并使用物联网哑终端设备，也可通过物联网控制设备间接访问和使用物联网哑终端设备。在用户和终端节点的通信过程中，需要互相认证来确保网络的安全性。

由于哑终端设备更新升级困难，无法及时修补安全漏洞，攻击者可利用设备安全漏洞获得节点的身份和口令信息，假冒身份与其他节点进行通信。因此，物联网用户与哑终端设备的身份认证多采用双因子认证的方式实现离线认证。除此之外，还可以采用基于口令的认证技术（即账号密码方式）、生物特征识别技术、轻量级认证技术等实现认证。在物联网应用中，通常将账号密码信息提前预置在物联网设备中。当需要连接时，通过验证账号密码的正确性来确定物联网设备或用户的合法性。该技术的优点是简单易用，但是其安全性较低，存在账号密码被窃听或者重放攻击的威胁，一般通过强化口令的复杂性来增强其安全性，过于复杂的口令又会导致用户记忆的不便。因此，出现了轻量级认证技术，它可以更好的满足物联网终端设备存储、计算、通信资源有限情况下的身份认证问题。

采用的身份认证手段有口令认证、轻量级认证等，根据不同的物联网应用场景选用不同的认证方式。

9.2.2 物物互联

在物联网系统中，哑终端设备涉及物体的身份识别和数据信息的采集；信息安全涉及哑终端设备身份的可靠性、数据传输的保密性、数据存储的安全性等。物联网通信网络除了具有一般网络所面临的信息泄露、信息篡改、重放攻击、拒绝服务等威胁外，还面临着终端设备节点被攻击者物理操纵，获取终端设备敏感数据信息的威胁。对于上述的问题，传统的针对终端设备的身份认证和对数据加密处理的机制，由于过于复杂而在物联网系统中不适用。如常用的基于公共秘钥基础设施（PKI）体系的身份认证系统，通常需要建立证书授权（CA）中心，并采用非对称加密算法，需要终端设备具有较强的运算、存储能力。

因此，对于物联网系统的身份认证，通常采用硬件加密技术和对称加密算法来实现。而加密就是为了实现数据的保密，防止信息的泄漏。加密的方式分为软加密和硬加密两种。软加密是采用软件的方式对数据进行加密处理，而硬加密是采用硬件技术在芯片内部完成数据的加密。按加密方式的不同，又分为对称加密和非对称加密两类。物联网系统的身份认证通常采用基于芯片级的认证方式来实现数据加密和身份认证。

哑终端间互联

哑终端间互联主要指终端节点与终端节点之间以及终端节点与接入网关之间的互联。哑终端的主要功能是实现对物体信息的采集、识别和控制，包含感知终端和控制设备。物联网控制设备中具备身份认证代理模块，通过该模块可实现用户身份的认证。一方面，物联网控制设备可直接或者通过网关间接连接到网络并与平台服务器进行交互，实现身份认证操作和各类物联网应用；另一方面，物联网控制设备可通过近场通讯协议（如蓝牙、ZigBee 等）实现与设备之间的通信，实现对设备的访问或控制。

由于物联网哑终端设备分布在户外且无人值守，容易遭受物理破坏、篡改、仿冒和信息窃取。因此，需要通过身份认证来确定哑终端设备的真实性、可靠性。而对于资源受限的哑终端设备而言，传统的非对称密钥算法显然无法适用于哑终端设备的身份认证。因为非对称加密算法需要更高的计算能力及资源的消耗。因此，对于成本和性能受限的哑终端，多采用双向认证、加密传输等实现身份的认证；对于能力较强，要求较高

的强终端，则采用数字证书、加密认证等技术实现身份的认证；对于快速响应处理场景下的终端，对时延要求较高，传统的加解密、数字签名等安全操作可能会影响业务性能，则需要采用轻量级的身份认证。

对于哑终端设备的身份识别，当前存在多种技术可以验证其真实性，如基于身份 ID 标识的条形码和 RFID 技术、基于物体属性的雷达技术和红外线技术等。通常采用的手段是通过在哑终端设备上灌入安全加密协议，完成数据在芯片内加密，以密文的形式在网络上传输，从而实现数据的保密；通过在哑终端设备上灌入认证协议，实现哑终端设备的身份认证，有效的防止设备被恶意替换，并可保证平台服务器获取数据来源的真实可靠性。

采用的身份认证手段有基于轻量级公钥算法（如：椭圆曲线）的认证技术、基于预分配密钥的认证技术、随机密钥预分布的认证技术以及基于单项散列函数的认证技术等，根据不同的物联网应用场景调用不同的认证方式。

应用与哑终端间互联

物联网应用平台与哑终端设备的互联，实现了终端设备与平台的数据交互。构成了终端与平台的互联互通。从而使得物联网应用平台可以监控终端设备的状态信息以及数据信息等，同时终端设备可以接收平台的数据，实现设备的更新以及远程运维管理。

由于物联网应用平台与哑终端设备的互联是建立在传输层网络的基础之上。因此，需要考虑物联网传输层不同架构的网络互联互通的需求，以及传输层面临异构网络跨网认证等的安全问题。对于上述问题，可以综合利用点到点加密机制和端到端加密机制确保传输层的安全。此外，由于物联网上传输的数据包未加密和签名，易发生被窃听、篡改、伪造以及发送者抵赖等问题。因此需要采用 SSL/TLS 和 IPSec 等协议，提供通信加密和认证功能，保证通信双方数据传输的安全。

对于物联网哑终端设备与平台间的可信身份认证，则是需要为每个哑终端设备分配一个唯一的标识，并且为每个设备分配相应的设备认证秘钥。标识和设备认证秘钥能够保存在物联网设备的安全存储区，不能被篡改，且设备认证秘钥的私钥部分不能够被读取或复制。

物联网平台通过校验设备标识，以及验证设备认证秘钥签名有效性等方式进行确认。验证通过后，可对该设备进行安全设置，如下发秘钥等。物联网应用平台可根据具体的应用场景确定物联网设备身份认证的方式，不过一般而言，可结合使用该设备的唯

一标识、设备秘钥或者激活过程中配置的工作秘钥等来实现对设备身份的可信验证。

采用的身份认证手段有口令认证、标识认证及证书认证等，根据不同的物联网应用场景调用不同的认证方式。

应用间互联

物联网应用平台间的互联实现了物联网应用平台间数据的交互、共享。打破了传统网络的边界，真正实现了万物互联。

在物联网应用系统中，为了防止各种的假冒攻击，在执行数据访问操作之前，需要在客户和数据库服务器之间进行双向的身份认证，如分布式数据库服务器与平台服务器之间进行数据传输时的身份验证。著名的 Kerberos 协议就是一种基于对称密码体制的身份认证协议。在该协议中各站点从一个密钥管理中心获得与目标站点通信用的密钥，从而进行安全通信。该协议的优点为支持单点登录、双向认证、可以防止网络窃听和重放攻击。但是该协议应用场合存在一定的局限性。因为密钥管理中心负责管理和分发大量密钥，容易造成系统性能瓶颈，而且系统内必须有一个被所有站点信任的密钥管理中心。

为了简化站点间通信密钥的分发，物联网应用系统一般采用基于公钥密码体制的双向身份认证技术。从而在每个站点都生成一个非对称密码算法的密钥对，其中的私钥由站点自己保存，公钥则通过可信的渠道分发给其他站点。这样任意两个站点均可利用获得的公钥信息相关验证身份。

主流的身份认证集成协议有 SAML 协议、JWT 协议、Oauth 协议、OpenID 协议等。可信站点之间的授权消息通常使用安全断言标记语言（SAML）发送，这个开放协议规范定义了一个 XML 框架，用于在安全 authori 之间交换安全断言。SAML 实现了跨不同供应商平台的互操作性，提供了身份验证和授权服务。它允许用户的帐户信息被第三方服务使用，而不暴露密码。

采用的身份认证手段有用户名/密码、数字证书、动态口令以及生物特征识别认证等，不同的物联网应用场景选用不同的认证方式。

应用与平台存储间互联

物联网应用平台与物联网存储服务器的互联，实现了物联网平台数据的存储、备份，以及平台与服务器间的数据交互。用户可以通过物联网应用平台实现与物联网存储服务器的数据交互。

物联网业务系统和平台使用的基础环境及组件包括虚拟机、云平台、数据库、各类中间件、web 应用等，由于软件本身设计或业务处理流程存在漏洞，使得物联网应用平台与存储服务器之间存在认证绕过、非授权访问、篡改数据、服务中断等的安全风险。因此，需要在物联网应用客户端与存储服务器间进行双向的身份认证，并且建立安全的通信。

物联网应用客户端与存储服务器间的认证是通过认证组件或服务器证书实现的。认证组件则是对连接到存储服务器的用户进行用户标识，再通过口令认证或证书认证的方式进行身份的鉴别；服务器证书（SSL 证书）则是安装在服务器设备上，用来证明服务器的身份以及进行通信加密。服务器证书可以用来防止欺诈钓鱼站点。SSL 证书主要用于服务器（应用）的数据传输链路加密和身份认证。

采用的身份认证手段有用户名/密码、数字证书、动态口令等。不同的应用场景对于不同价值的数据选用不同的身份认证方式。

9.3 常见 IoT 身份互联场景说明

IoT（Internet of Things，物联网）被广泛认同已经成为世界信息发展的新一代浪潮，其用户端延伸扩展到了物品层面，通过 IoT 技术进行物品与物品之间的信息交换和通信，最终实现万物互联的远景目标。IoT 技术在物流运输、车辆交通、保健医疗、家居家装、建筑建工、零售电商、工业生产及农业生产等众多行业都获得广泛的应用。

同时，IoT IAM 身份与访问管理系统在不同行业应用实例中，其身份互联方式也有着各具特色的行业特点，下文针对智慧物流、智慧交通、智慧医疗及智能家居四大类应用场景进行相关说明。

9.3.1 智慧物流

IoT 技术赋能传统物流行业，聚力提升物流行业信息能力，打造智慧物流新业态。智慧物流是以 IoT 技术、大数据技术、人工智能技术等信息技术为支撑，在物流行业的运输、仓储、包装、装卸、流通、配送及信息服务等各个环节实现全流程信息监管、信息感知、数据分析及智能化信息处理的新型物流生态。智慧物流新业态的实现能大大降低物流行业自身物流成本，提升物流效率，提高企业利润，同时帮助上下游相关生产行业降低物流费用负担、提高货物运输效率。IoT 技术作为智慧物流业态发展最重要的技

术支撑，主要应用于物流仓储出入库、物流货物全程溯源、物流运输查询与监测以及相应物流智能终端设备等方面。这其中包含两个层面的身份认证识别及身份互联管理的场景应用，**第一个层面**是以仓储出入库业务应用为代表的**物品到物品**的身份认证及互联场景；**第二个层面**是以物流业务应用中全程溯源为代表的**人与物品**的身份认证及互联场景。

仓储出入库业务（物-物）

将 IoT 技术应用于物流仓储中，打造智能仓储管理系统，提高仓储出入库效率，扩大仓储容量利用率，减少仓储出入库人工劳动强度及人工费用成本。在仓储出入库业务流程中，智能仓储管理应用系统作为业务应用平台，配套识别设备、智能分拣设备、入库设备（包括托盘输送系统、周转箱输送系统、机器人、AGV 穿梭车等）共同构成业务应用主体，待出入库物品构成业务应用客体。主、客体设备物品均应具有身份唯一标识，包括被动身份标识或主动身份标识。被动身份标识是需要业务主体主动对其进行身份识别的标识技术，常见被动身份标识包括一维条形码、二维条形码、支持 RFID 识别的标识、支持 NFC 识别的标识等；主动身份标识主要指能够主动连接业务主体进行身份识别的身份标识技术，常见主动身份标识包括具有相应功能的芯片、模组及终端等。

业务应用过程中，业务平台通过应用主体扫码机、RFID 或 NFC 等设备识别待操作业务客体物品标识，识别物品身份标识信息及环境特征等信息。结合平台仓储系统策略

以及 IAM 策略，借助配套智能分拣、入库设备（包括托盘输送系统、周转箱输送系统、机器人、AGV 穿梭车等）将业务客体物品高效快速进行出入库操作。IAM 识别业务系统主体与客体身份信息（条码、芯片、模组），结合业务环境条件（位置、时间、流程）进行动态行为评估，判断物联设备安全接入条件，结合 IAM 策略验证通过后，完成主客体与业务平台间身份识别互联。如：1，在物流仓储过程中，平台识别到一个非法客体设备，IAM 会拒绝主体对其进行互联操作；2，在物流仓储过程中，平台识别到一个合法客体设备，但在策略禁止时间段出现在不被允许区域，IAM 会拒绝主体对其进行互联操作，并对该客体设备标识动态评估降级；3，在物流仓储过程中，平台发现主体设备对客体设备操作异常，IAM 会断开主客体互联认证，并对该主客体设备动态报警提示。

物流查询与监测业务(人-物)

通过 IoT 技术可以针对物流货物构建全流程、智能化、可追溯的查询网络业务系统，如食品、药品等需要高信赖物品的溯源业务，保障食品安全、药品安全；通过应用在车辆的 GPS 来进行运输管理，可对物流车辆及货物进行实时监控、全程的跟踪、定位。一方面，可以进行车辆调度，提供车辆的报警功能，使货物在运输过程中变得更加安全；另一方面，实现了突发情况下的车辆紧急救援。在货物运输过程中，将货物、司机以及车辆行驶情况等信息高效的结合起来，提高运输效率、降低运输成本，降低货物损耗，清楚地了解运输过程中的一切信息。在物流货物查询与监测业务流程中，业务查询业务系统构成应用平台，查询人构成业务主体，待查物流货物及载体构成业务客体。业务主体与业务平台应用之间具备身份认证识别能力，IAM 可以根据业务主体身份证书、网络环境（五元组）、业务行为等相关信息，对其进行访问授权管理。IAM 对业务客体具有相应身份识别能力，包括识别车载终端、验证货物唯一不可变查询码、验证码等。

物流物品业务查询监测应用过程中，查询人主体通过业务应用平台使用货物唯一查询码及验证码（或权限证书）进行物流货物查询。待查物品客体应标识对应唯一查询码的不可篡改标识以防止货物调换，且货物查询验证码应有防泄漏功能。IAM 认证业务主体查询人信息（身份证书、网络环境、业务行为等），通过认证后仅有业务访问权限的查询人能够获取互联权限。IAM 识别业务系统主体与客体身份信息，结合业务环境条件进行动态行为评估通过后，完成主客体与业务平台间身份识别互联。如：1，客体物流物品自身带有涂层防伪标签的识别码，IAM 识别涂层破损，断开业务互联，并动态将该物品自身物流业务高风险告警；2，IAM 识别待查客体物品识别码复用或篡改，断开业务互联，并动态将该物品涉及物流运输主体高风险告警。

物流载体业务查询监测应用过程中，查询人主体通过业务应用平台与待查物流载体（陆运货车、水运货船、空运货机）进行身份互联。IAM 认证业务查询人信息（身份证书、网络环境、业务行为等），通过认证后仅有业务访问权限的查询人能够获取互联权限。IAM 识别业务系统主体与客体身份信息，结合业务环境条件进行动态行为评估通过后，完成主客体与业务平台间身份识别互联。如：1，客体物流载体处于异常区域，IAM 断开业务互联，并动态将该载体自身物流业务高风险告警；2，IAM 识别主体查询人证书异常、操作区域高风险、行为高风险等情况，断开业务互联，并动态将该主体高风险

告警。

9.3.2 智慧交通

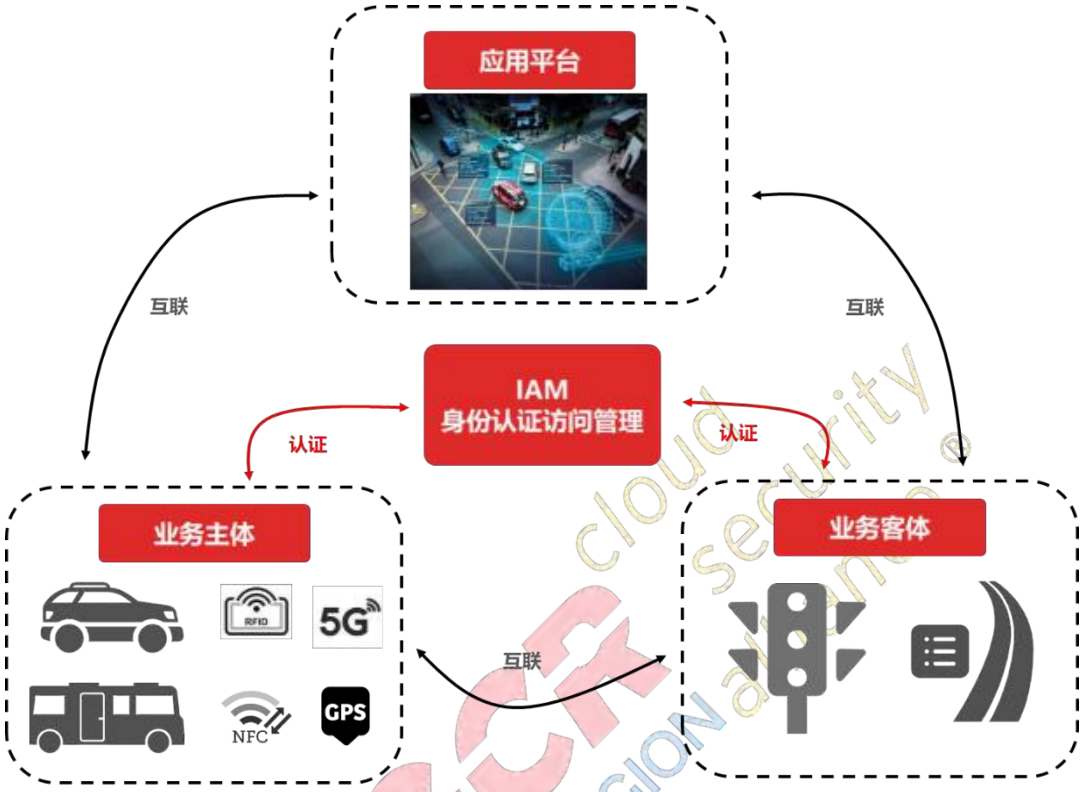
智慧交通是指在交通领域中充分利用 IoT 技术、云计算技术、大数据技术、人工智能技术等，通过数据汇集分析，对交通管理、车辆出行、车辆能源管理等交通领域全方面管理进行技术支撑。智慧交通推动交通运输更安全、更高效、更便捷、更环保的运行发展，带动交通运输相关产业转型升级，特别是在车联网、车辆识别、无感付费以及国家重点发展新能源汽车充电桩相关业务方面起到创新推进作用。IoT 技术是智慧交通领域重点支撑技术，下文对 IoT 技术在车辆信息识别查询业务及新能源充电桩业务进行身份互联场景说明。

车辆信息识别查询（物-物，人-物）

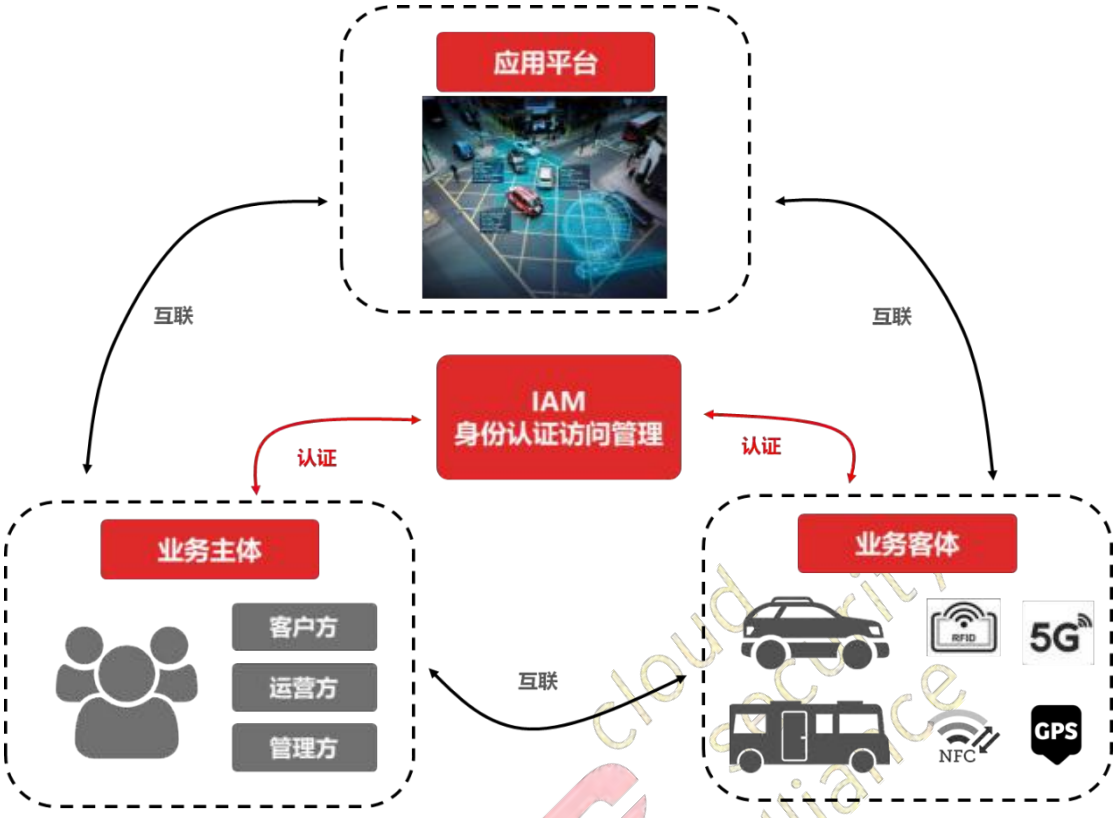
促进智慧交通能够更广泛应用，针对车辆信息高效、准确、安全的识别尤为重要。以车辆为信息感知对象，借助新一代信息通信技术，实现车辆与车辆、车辆与人、车辆与路网、车辆与平台之间的网络互联，提升车辆整体智能水平，提供安全、高效、智能的交通服务，提高交通运行效率，优化社会交通服务智能水平。车辆信息识别查询业务应用十分广泛，比如公共汽车出入站运行情况识别、高速公路车辆扣费识别、车辆公共停车位计费识别、车辆无人驾驶（辅助驾驶）等，这其中包含两个层面的身份认证识别及身份互联管理场景应用，**第一个层面**是以车辆无人驾驶（辅助驾驶）为代表的**车辆与车辆**的身份认证及互联场景；**第二个层面**是以公共汽车运行状况查询为代表的**人与车辆**的身份认证及互联场景。

无人驾驶或辅助驾驶是依靠车内计算机系统为主的智能驾驶系统来实现无人驾驶或辅助驾驶功能，车辆通过车载传感系统感知道路及周围环境，并与运行平台智能互联，运行平台收集大量互联车辆终端信息，自动规划车辆行车路线并控制车辆预定行驶目标。业务应用中车辆周围环境反馈、信号灯、路网信息等构成业务客体，行驶车辆构成业务主体，云端大数据分析管理中心构成应用平台。发起自动驾驶辅助功能的车辆主体具有芯片级身份认证标识，一般借助车辆唯一车架号在车辆三电系统中内置识别模块，包含车联网卡、4G 卡、车载 GPS 模块、RFID、NFC 等多种技术模式。业务主体车辆向运营平台发起业务互联申请，运营平台 IAM 综合认证车辆信息，并结合车辆操作行为、车辆运行状况动态评估访问行为，通过相关认证后，完成主客体与业务平台间身份识别

互联，授权主体车辆接入平台开启无人驾驶或辅助驾驶等功能；运营平台 IAM 识别认证业务其他客体身份信息，确保获取到的路网信息、信号灯状态等数据提供主体身份可信。



公共汽车运行状态查询利用车载 GPS 及 4G 网络等技术实时与运行中心平台进行数据通信，运行中心根据车辆运行状态及路况状态动态调整车辆运行任务，同时待乘乘客和调度人员可以通过运营平台查询车辆位置及出入站信息等运营状态，优化出行计划。在业务场景中，待乘乘客、调度人员等查询人员构成业务主体，运行车辆及路况状态等构成业务客体，运营业务平台可以对主客体进行身份认证并授权访问行为。业务主体向业务平台发起应用访问或操作时，IAM 对主体人员进行身份认证，结合访问人员身份信息、密码、生物特征、操作终端状态等信息，动态进行权限管理。业务客体车辆搭载具有身份认证功能的车载终端设备，能够向业务平台反馈车辆自身信息、路况信息及场站点位信息等，IAM 识别车载终端身份信息，根据车辆计划班次、预计运营位置等信息作为参考，动态授权业务平台与车辆间身份互联权限。

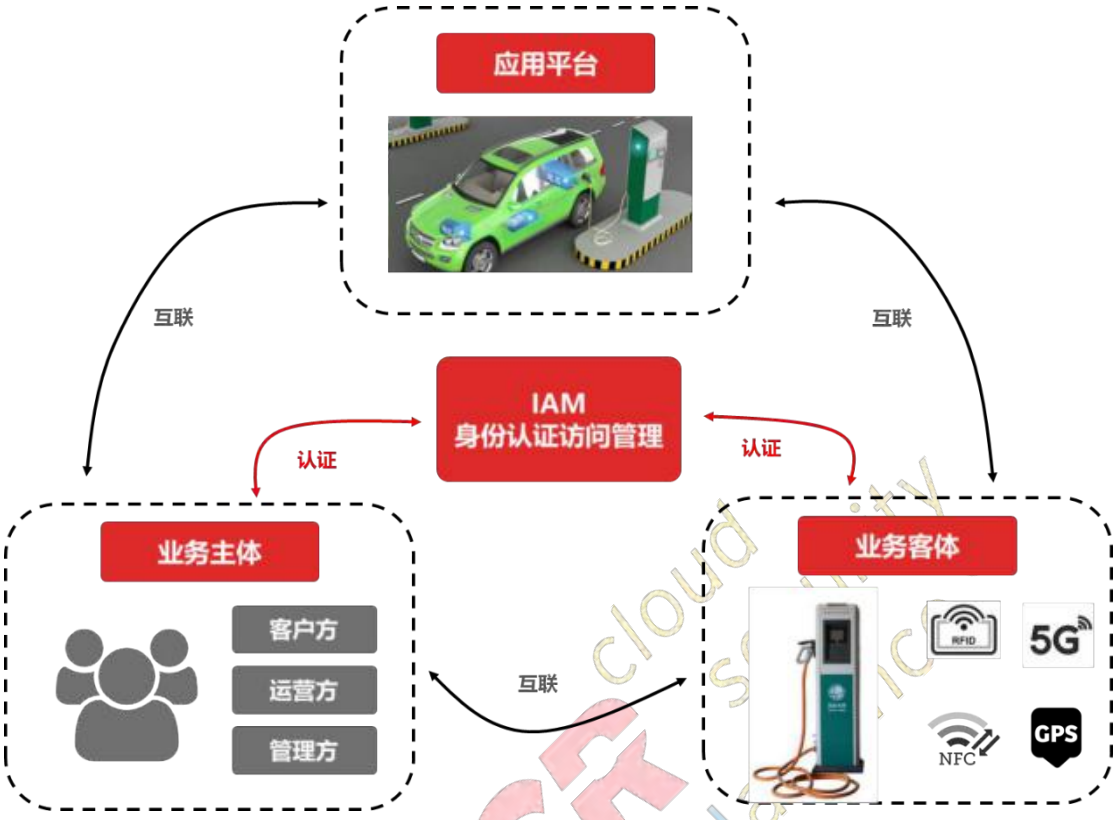


汽车充电设备（人-物，物-物）

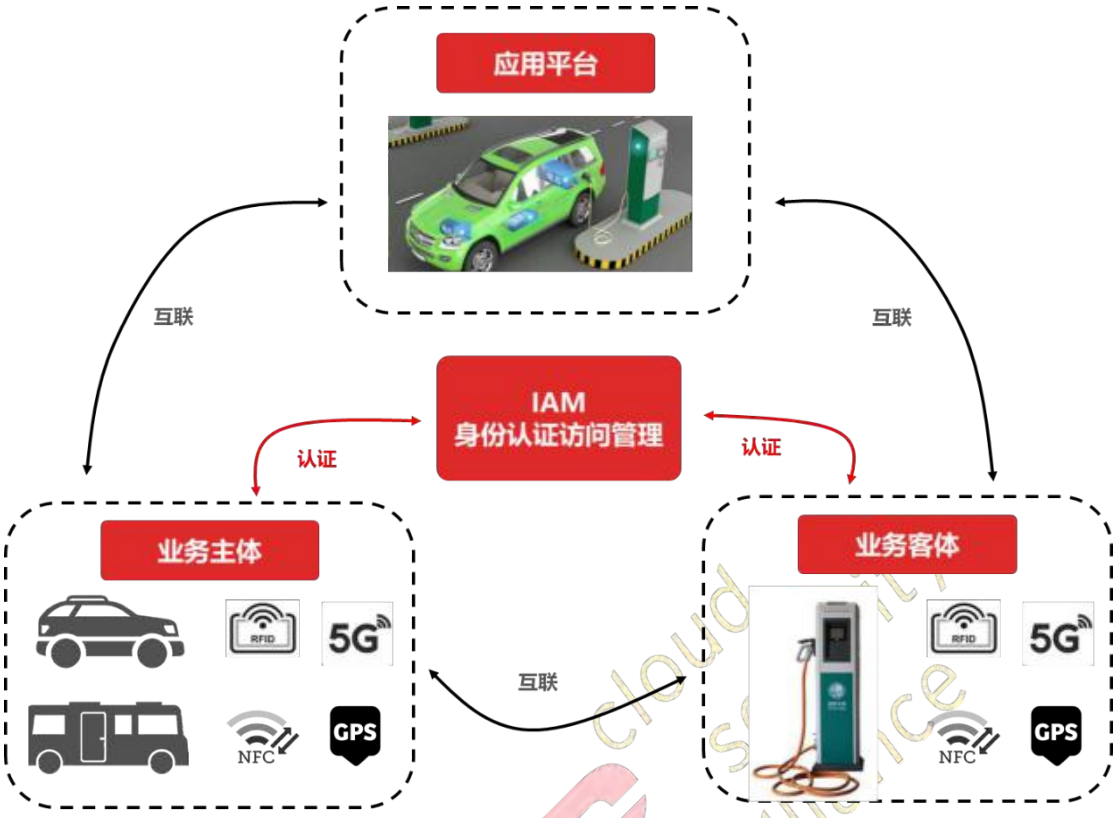
我国传统汽车产业发展较晚，在汽车工业领域与国外仍有较大差距，发展“电动新能源汽车”是我国实现汽车工业弯道超车的可行之路之一；同时，我国电力能源结构“峰谷效应”明显，大力发展以电能为直接能源的电动新能源汽车有助于解决我国电力储能及峰谷调节作用。在电力新能源汽车领域中，充电设备的高效、便捷、安全运营工作是助力智能交通新能源汽车新业态发展的重要支撑。在公用充电设备运营业务过程中涉及包括使用人员识别、操作终端识别、充电设备认证、充电车辆认证在内的众多身份识别授权过程，这其中主要包含两个层面的身份认证识别及身份互联管理场景应用，**第一个层面**是以人使用公共充电设备涉及的**人与充电设备**之间身份认证及互联场景；**第二个层面**是汽车充电业务过程中的**充电设备与车辆**之间的身份认证及互联场景。

以国家电网公共充电桩付费业务过程为参考依据，充电桩等充电设备构成业务主体，充电车辆及充电操作人员及终端设备构成业务客体，云端大数据分析管理平台构成业务应用平台。客体操作人可通过国家电网统一 NFC 充电卡与充电桩主体进行身份认证互联；客体操作人终端设备可使用充电桩平台生产一次性识别码（二维码等）进行终端认证；客体操作人可以通过与国家电网预存账户密码口令进行身份认证；客体充电车辆可以通过车载身份芯片通过充电电缆通讯接口与业务主体充电桩进行通讯身份认证。

IAM 认证业务主体充电桩业务状态、标识信息，认证通过后与业务平台数据通讯互联。



车辆充电与充电桩对接充电过程中，业务平台通过网络与充电设备组建通讯链路，识别认证充电设备 SIM 卡、物联网模块或物联网芯片等身份认证模组芯片，充电桩设备通过充电电缆与待充车辆进行通讯。以国标 GB-T27930-2015 中要求为例，充电桩主体设备需要监测待充客体汽车电池电压状态、车辆状态、以及车辆身份信息，结合来自业务平台 IAM 授权的连接管理命令进行充电业务。



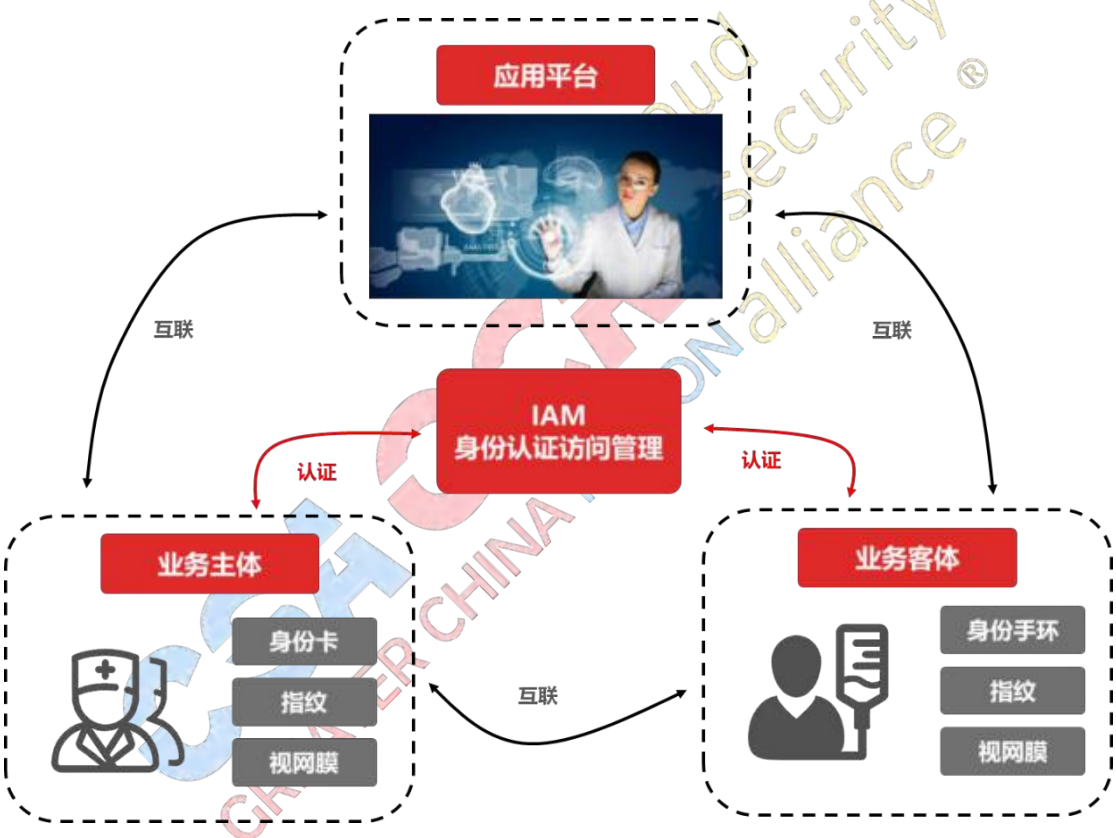
9.3.3 智慧医疗

寄托以 IoT 技术、大数据技术、人工智能为代表的新兴技术为医疗行业带来新的增长势能，“智慧医疗”已经成为政府、企业和民众推动的医疗行业发展新形态，这其中既包含如终端无人自助挂号业务、电子病历查询业务、自助健康检查业务等医院传统业务的信息化新发展，又包含远程医疗诊断、远程手术处置、医疗穿戴设备结合治疗处置等新型业务的智能化新创新。我们以远程医疗及医疗穿戴设备为例进行关于 IAM 身份认证访问管理相关场景分析。这其中主要包含两个层面的身份认证识别及身份互联管理场景应用，**第一个层面**是以远程医疗、远程处置为代表的**人与医疗设备**的身份认证及互联场景；**第二个层面**是以医疗穿戴设备结合治疗设备为代表的**物品与物品**的身份认证及互联场景。

远程医疗（人-物）

各地医疗资源分布不均，部分偏远地区缺乏良好的医疗服务的现状是世界各国都面对的客观现状，伴随着 5G 技术、IoT 技术的发展，开展远程会诊，远程急救、远程手术、远程监护、辅助治疗的新兴医疗方式不断发展进步。远程医疗过程中业务系统利用智能医疗仪器检查用户各类指标参数上传平台，医疗人员通过平台数据实现远程医疗，

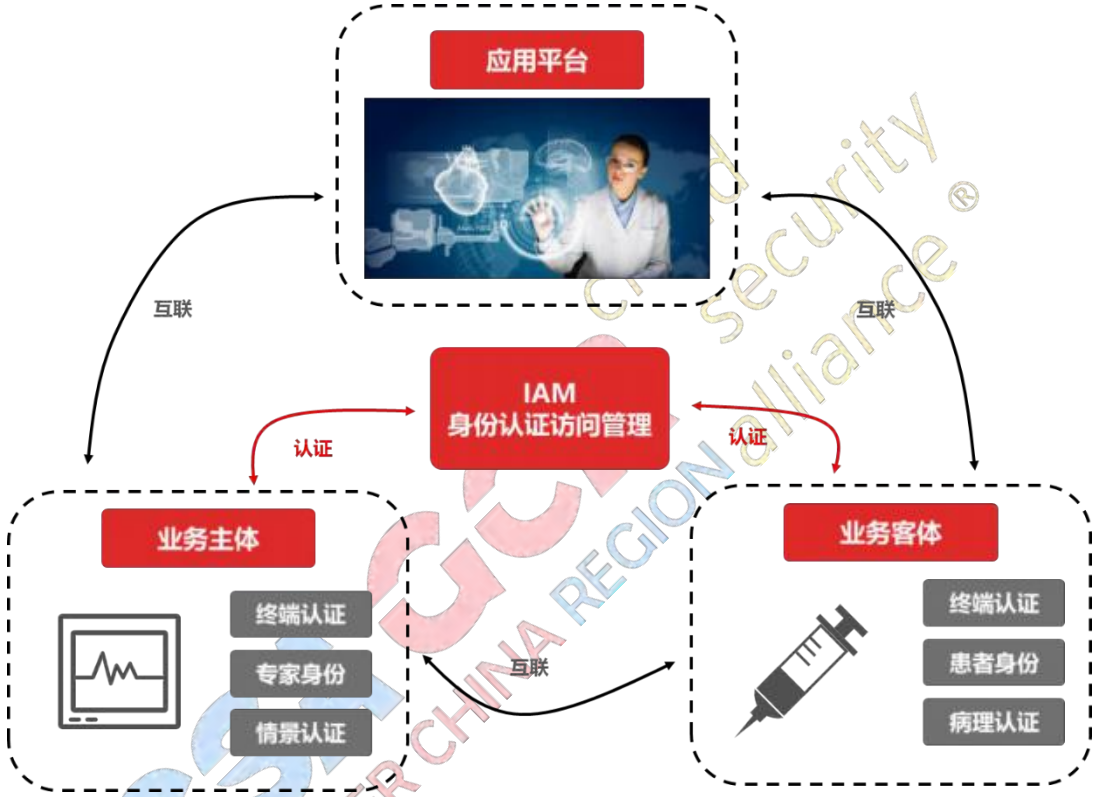
借助 IoT 设备感知及设备操作能力进而实现远程手术的可能性。在业务过程中，患者及众多医疗检测处置仪器构成业务客体。治疗团队构成业务主体，智能医疗管理系统为业务平台。在业务过程中，患者应具有唯一身份信息的人员手环，并结合生物特征（指纹、视网膜识别等）进行身份认证，业务平台通过 IAM 对业务客体进行身份认证，进而管理相关访问操作权限；医疗团队人员应具有专用人员胸牌，并结合生物特征（指纹、视网膜识别等）进行身份认证，业务平台通过 IAM 对业务主体进行身份认证，根据医疗人员身份信息，结合相应病例情况，分配相关访问操作权限；医疗资源应具有唯一不可篡改物资标签，用于 IAM 系统识别医疗资料身份，获得相应权限，只有通过身份认证的设备与物资才能够提供给医疗业务平台使用。



医疗穿戴设备（物-物）

随着以 IoT 技术、大数据技术为代表的科学技术的进步，医疗设备的发展迅速，近年来，可穿戴式设备的设计发展也是越来越人性化、智能化。医疗行业与可穿戴设备也日渐结合，医疗技术与智能便捷的可穿戴设备相结合，使患者在部分医疗过程中更加高效精准。可穿戴医疗设备其真正意义在于植入人体、绑定人体，识别人体的体态特征、状态。时刻监测我们的身体状况、运动状况、新陈代谢状况，还会让我们动态、静态的生命、体态特征数据化，其真正价值在于让生命体态数据化，可穿戴医疗设备可以实时

监测血糖、血压、心率、血氧、体温、呼吸频率等人体健康指标。在一些如糖尿病、心脏病等慢性疾病持续治疗过程中配合治疗设备更有助于患者的康复治疗。在业务过程中，远程治疗团队及辅助治疗设备构成业务主体，患者使用众多医疗可穿戴设备构成业务客体，医疗可穿戴设备大数据分析管理中心为业务应用平台。IAM 识别主体身份信息，比如治疗团队人员信息、辅助治疗设备终端认证信息等，授权其与业务客体身份互联并获取业务数据。IAM 识别众多客体医疗穿戴设备身份认证信息，确保设备身份合法，结合患者病情及治疗方案，动态授权其与业务主体互联通讯。



9.3.4 智能家居

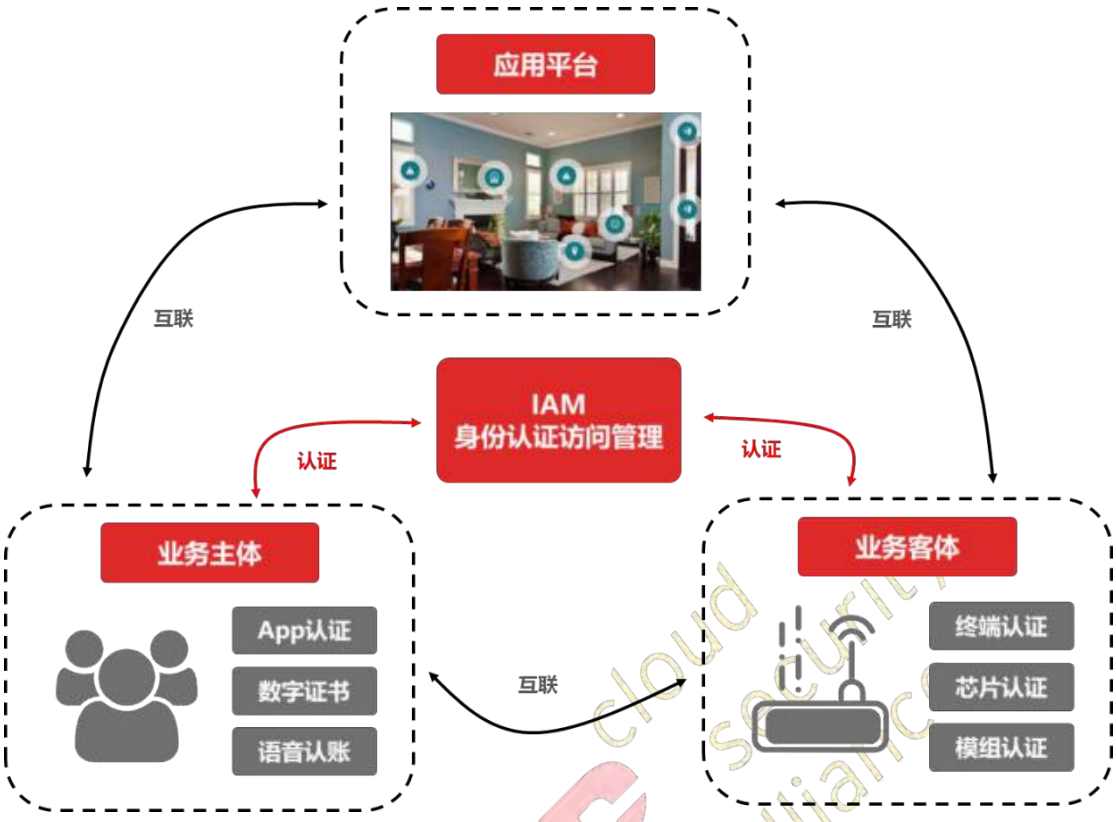
智能家居是在互联网影响之下的物联化体现，智能家居通过 IoT 技术将家中各种设备联接到一起，如：空调、灯具、电视、窗帘、门窗、安防等等。与普通家居相比，智能家居不仅具有传统的居住功能，还兼备建筑、网络通信、信息家电、设备自动化，全方位的信息交互功能，甚至为各种能源费用节约资金。智能家居设备间的通讯建立在不安全的信道上，一个非法行为可能通过获取智能设备的访问权限来破坏家居安全，比如通过非法身份控制智能门锁开关功能。因此，通过安全的身份认证方法保障智能家居网络在授权控制下的安全访问尤为重要。这其中包含两个层面的身份认证识别及身份互联

管理场景应用，**第一个层面**是智能家居业务应用中**人对物品**控制涉及的身份认证及互联场景；**第二个层面**是智能家居业务应用中各类智能设备通过应用平台**物品与物品**之间互联的身份认证及互联场景。

单品控制（人-物）

智能家居构建家居生活新方式，智能设备使用者通过 App、语音等方式操作具有智能控制功能的家居设备，家庭网关是智能家居 IoT 的核心部分，主要完成家庭内部网络各种不同通信协议之间的转换和信息共享，以及与外部通信网络之间的数据交换功能，同时网关还负责家庭智能设备的管理和控制。在智能家居针对使用者对各类智能设备控制使用业务应用场景中，使用智能设备的人构成了业务主体，众多智能设备构成了业务客体，云端数据管理中心为业务应用平台。业务主体与业务网关应用之间具备身份认证识别能力，IAM 可以根据业务主体身份证书、网络环境（五元组）、业务行为等相关信息，对其与业务网关的访问进行授权管理。业务客体与业务网关应用之间具备身份识别能力，IAM 识别客体身份信息，管控其与业务网关间的互联授权管理。

智能家居单品控制应用过程中 IAM 对使用者主体身份认证，在 **App 控制场景**下，IAM 可以通过密码、证书、指纹、面部识别等识别因素进行使用者身份认证，并结合使用者 App 环境风险，行为习惯记录等动态进行访问权限管控；在**语音控制场景**下，IAM 可以通过使用者声音指纹、语音解锁、常用词汇识别等识别因素进行使用者身份认证，动态授权使用者与网关平台的互联权限。如：1，业务主体使用者 App 频繁登陆操作、针对设备异常启停操作、异常时间操作等，IAM 断开使用者主体与业务网关间的互联，并要求使用者多因子认证登陆确认；2，业务主体使用者语音控制情景下，IAM 识别语音指纹，对不满足声音特点的操作智能拒绝互联操作，需要使用者主体多因子认证后训练语音识别。

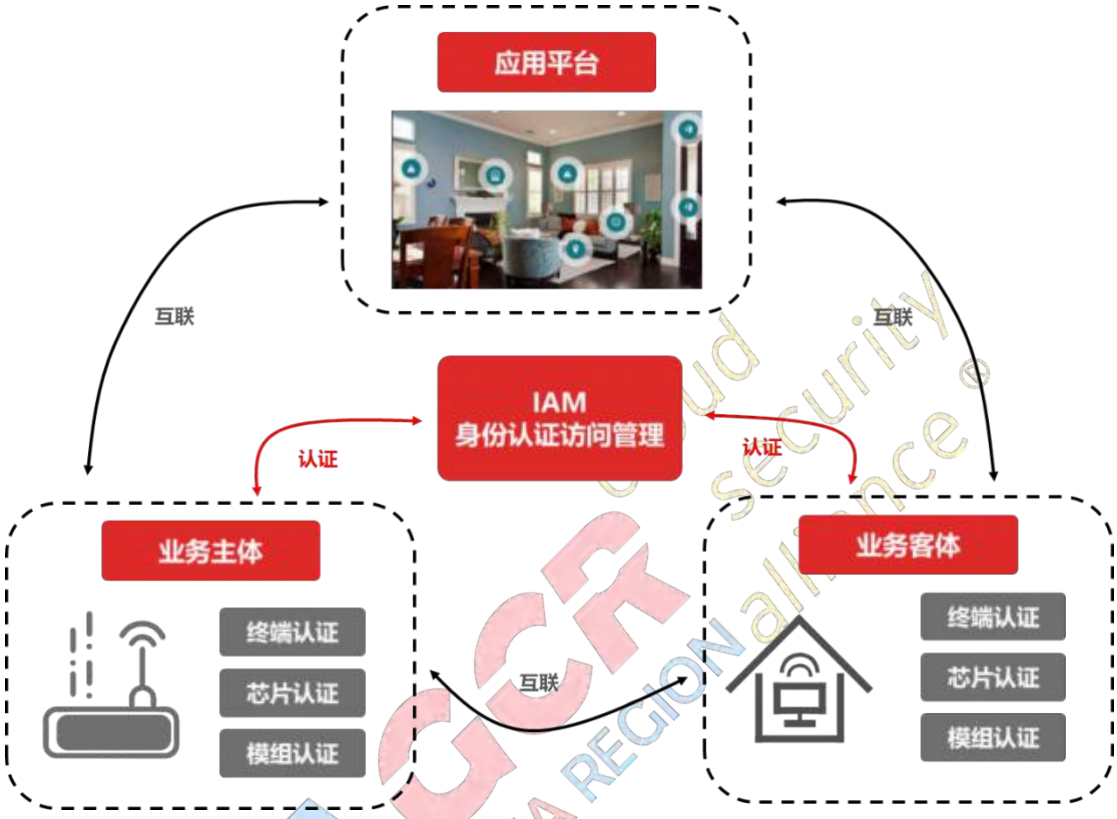


平台集成（物-物）

智能家居众多终端将智能化设备的所有功能集成起来，使智能家居建立在一个统一的平台之上。首先，实现家庭内部网络与外部网络之间的数据交互；其次，还要保证能够识别通过网络传输的指令是合法的指令，而不是非法操作。智能家居将众多情景关联模式进行设备与设备间的交互通信操作。比如打开家门触发门窗感应器，根据不同触发事件时间分析是回家行为、还是离家行为，进一步操作诸如其他照明、制冷、安防系统。在智能家居高度平台化、集成化的物物互联场景下。业务网关构成业务主体，众多智能家居设备构成了业务客体，智能家居统一管理平台为业务应用平台。业务主体业务网关应用与平台之间具备身份认证识别能力，IAM 可以根据业务主体身份证书、网络环境（五元组）、业务行为等相关信息，对其与业务网关的访问进行授权管理。业务网关应用具备对业务客体唯一身份识别能力，IAM 识别客体身份信息，管控其与业务网关间的互联授权访问。

智能家居平台集成应用过程中 IAM 对主体进行身份认证，识别业务网关状态包括设备信息、工作状态、授权权限及接入客体设备等，通过识别业务网关芯片标识信息，允许平台授权接入的设备互联通信，拒绝非法接入设备及故障设备的互联。IAM 对客体智能设备进行身份认证授权，通过客体设备唯一标识码进行与主体业务网关的身份互联

认证。如：1，业务主体平台识别某一个业务网关处于未被允许接入的网络中，IAM 断开平台与业务网关互联通讯，并持续对其进行状态查询。2，业务网关识别接入智能设备存在重复或篡改的身份标识，IAM 断开业务网关与不安全智能设备互联通讯，并持续对其进行状态查询。



10 IAM 与零信任的关系

10.1 IAM 在零信任中的作用

10.1.1 IAM 对于零信任的支撑作用

IAM 作为零信任的核心支撑技术，管理不同用户和实体的身份权限。甚至可以说，零信任架构是借助身份和访问管理（IAM）框架实现对人/设备/系统的全面、动态、智能的访问控制。IAM 产品在支持任何企业中实施零信任基础结构方面发挥着非常重要的作用，通过以下几个方面的关键支撑作用，助力零信任安全架构的实施

1、IAM 为零信任构筑身份基础

零信任作为一种网络安全基础，其信任关系来自于所有参与对象的身份验证。这种

端到端的信任关系是由每一个参与单元一起构成的，即网络中的所有用户、设备、应用程序等，零信任架构基于身份而非网络位置来构建访问控制体系，首先需要为访问控制中所有对象赋予数字身份，所有对象基于身份进行验证。对于客户端而言，身份就包括所使用的网络帐户以及所分配给该帐户的所有关联属性，都可以用于用户身份的自动验证；企业必须通过统一身份管理技术确保用户始终是企业信任的用户，才能为其提供企业应用程序和数据访问权。

管理和设置用户访问权限对于零信任实施访问权限至关重要，特别是在零信任端到端的基于会话的精细化权限管理要求下，需要一个强大的 IAM 系统予以支撑。如果企业仅仅知道用户是谁并不意味着用户对其所有资源有自由支配权。每个应用程序以及应用程序内部权限都是需要控制的。

2、IAM 为零信任提供身份持续有效性验证

企业需要一个稳定、强壮的统一自动化身份验证管理系统，企业通过定义它拥有哪些资源、其成员是谁、以及需要资源的成员使用什么样的访问方式来保护资源，IAM 系统需要管理所有资源的身份验证。身份认证系统要根据交易的风险提供自适应的认证技术，系统要保持身份认证的持续性，关注用户行为和场景变化，让企业可以随时掌握用户真实访问记录。

利用容易在网络钓鱼诈骗中被黑客入侵或窃取的密码，使用 MFA 对用户凭据进行额外的安全保护可以抵御威胁参与者破坏网络的企图。IAM 通过人性化多因素身份验证（MFA）来支持零信任架构的认证和访问。

此外，组织可以应用基于风险的（或逐步增强的）身份验证来动态评估相关的风险。采用场景认证的机制，如地理- 位置和时间因素等计算风险，使企业对用户访问场景收集数据，用户的行为实时进行认证。

3、IAM 支持零信任实施最小权限策略

零信任最初的重点就是将资源限制为按需访问，并仅授予执行任务所需的最低特权，零信任架构采用微分割（分域）方式，将公司的 IT 环境拆分成易于单独授权的安全区域，以保护公司应用和数据资源，这种做法可以限制黑客为了访问和破坏更敏感的数据而从网络的一部分“跳”到另一部分的机会。同时，设置授权和批准的主体为包括用户、应用程序和设备的动态组合，则需要根据一定的访问上下文，为访问主体组合设定其所需的最小权限。

IAM 采用“最小特权”和“即时权利”的原则，通过使用单个控制层来确定每个应用程序和子应用的访问策略。只允许每个用户访问他们所需的最基本的资源，如果用户的凭据在安全事件中受到损害，通过最小权限来降低风险。

现代访问管理（AM）解决方案允许组织为内部部署环境和私有云环境部署这些网关，以通过集中定义和管理的动态策略集保护应用程序和 API。使用 OAuth 和 OpenID Connect 等现代身份协议可以确保遵循最佳安全实践，以抵御当今和未来的威胁。

4、IAM 支持零信任架构实施动态和实时的访问控制

在零信任环境中，管理资源、用户和访问权限方面存在复杂性，各种物体之间关系的排列是非常复杂的。因此，IAM 系统还将在管理用户、用户的访问权限和访问策略方面发挥关键作用，并消除各种系统的竖井管理系统。IAM 系统不仅集中了管理功能，还提供了一个具有访问信息的中央存储库，以便组织能够更好地了解用户及其访问权限，并从各种角度（如资源）查看相同的信息。这将使组织能够实现更好的身份访问治理，并更快地响应法规遵从性问题。

5、IAM 通过单点登录技术支持零信任实施对资源访问

零信任架构最终是打通资源访问路径，在 IAM 单点登录技术的支持下，得到很好的用户体验。在传统的模型中，企业使用基于密码保险存储和密码重放的 SSO 解决方案。这种简单的 SSO 模型有一些安全缺陷。为了与现代 SaaS 应用程序和其他资源集成，组织必须实现联邦 SSO，如 SAML、Open ID Connect、Oauth 等标准协议。

联合 SSO 使用签名（或令牌）替换密码，从而最小化攻击向量。它还利用标准在合作伙伴、供应商和客户之间安全地交换用户信息，使组织能够更好地控制谁可以访问哪些信息和资源，而不管这些资源位于何处以及用户选择访问哪些类型的设备。使用联合 SSO，用户只需验证一次，然后使用该验证会话访问他们被授权使用的所有应用程序。

6、IAM 帮助零信任实现有效身份治理

访问控制需要身份治理和授权策略的管理作为基础支撑。现代企业都面临内部员工、客户、合作机构、外包人员等不同的身份，零信任安全并不寄希望于以一套大一统的管理逻辑和流程朗阔万千，而是对不同的身份进行分类分析和梳理，制定不同的身份生命周期管理流程。同样，对现代企业来说，很难一次性厘清信息化系统中各种用户、角色、系统的当前访问权限，只有通过部署身份分析系统，对当前系统的权限、策略、角色进行智能分析，发现潜在的策略违规并触发工作流引擎进行自动、或人工干预的策

略调整，实现身份治理闭环。

IAM 支持零信任实施有效身份治理，解决孤立帐户问题，因为它们常常被忽略作为潜在的威胁载体。通常情况下，一个备用的“管理员”帐户可能会在数周、数月或数年内无人注意。同时，保持对特权用户和普通用户在网络中所做的所有更改的审计跟踪有助于审计人员分析，配置实时警报，以便在发生任何异常活动时通知 IT 安全团队。特别是对于违背职责分离原则，发生权限互斥等权限管理异常行为时，可以予以发现。

10.1.2 IAM 对零信任支撑实例

零信任是一种安全理念，对基于边界防护的网络安全架构进行了颠覆，引导网络安全建设从有边界走向无边界。零信任安全架构所依赖的身份认证与访问控制能力由 IAM 技术提供，借助 IAM 技术实现身份认证、访问控制、审计追溯。

（1）BeyondCorp 项目中的 IAM

Google 的 BeyondCorp 项目基于零信任安全理念构建，为业内实践零信任安全架构提供了参考。

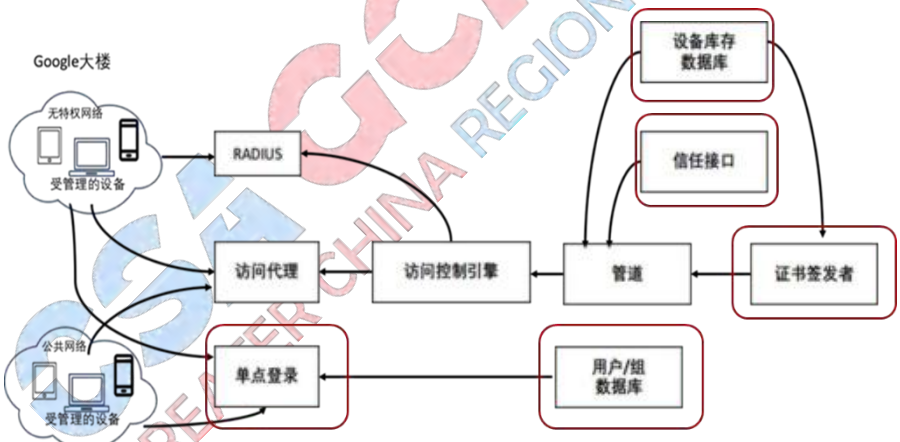


图 Google　BeyondCorp 访问过程

上图中红框的模块都借助了 IAM 技术，可见 IAM 技术是零信任安全架构重要的组成部分，实现了统一登录认证、身份管理、身份授权。用户/组数据库模块负责统一身份管理功能，对所有用户的身份生命周期管理，当有人员身份变更时，数据库会及时更新；单点登录模块负责统一认证功能，提供了一个集中的认证门户，对所有请求访问资源的用户进行双因子认证；设备库存数据库负责可控设备管理功能，持续收集、处理、发布已知设备的状态变化；证书签发者负责为可信的设备签发专用的设备证书，证书是可信设备的唯一标识；信任接口，通过查询多个数据源动态分配给设备、用户信任等级，

访问控制引擎将参考信任等级进行授权。

（2）远程办公场景下的 IAM

当前远程办公成为了企业办公必备的模式，这种新的工作模式给企业带来了全新的网络安全挑战。暴露在互联网上的远程访问 VPN 设备、移动应用增加了网络暴露面；攻击者利用 VPN 自身漏洞突破网络边界、横向移动；大量 BYOD 设备的环境安全难以保障；不同接入人员的身份和权限管理混乱。

在零信任安全架构下，通过 IAM 技术对所有发起访问的人员、设备进行身份认证，授予访问业务系统的最小权限。在业务访问过程中，零信任的信任接口通过大数据和机器学习技术对终端、访问行为、环境因素进行持续评估，发生异常行为时，实时地借助 IAM 技术对访问认证策略和访问权限进行调整。

（3）应用服务数据交换场景下的 IAM

随着软件功能不断扩展、用户负载量逐渐增长等发展问题，应用程序由单体架构过渡到微服务架构。通过 API 接口进行服务连接和数据传输的过程中，往往带有大量的敏感数据，API 接口成为被攻击的热点目标。API 接口面临的威胁有数据泄露、未授权访问等。

在零信任安全架构下，应用数据安全调用场景需要适配多样化的接口和多样化的计算环境，将接口统一调用，结合 OAuth2、JWT、OpenID 等 IAM 认证方式实现统一的身份认证和统一的授权管理。在应用数据调用过程中，零信任的信任接口对访问应用进行信任评估，通过限流、熔断、降权等手段保障服务的可用性。

10.1.3 零信任实施过程中对 IAM 的保护

（1）零信任缩减 IAM 账户凭证被盗后风险

正确实施零信任，信息安全和弹性策略以及最佳实践可降低攻击者通过被盗凭据或内部攻击获得广泛访问的风险。零信任原则基于网络位置没有隐式信任，这意味着攻击者需要破坏现有的帐户或设备才能在企业中立足。正确实施的零信任架构应该防止受到破坏的帐户或资产访问其正常权限或访问模式之外的资源。这意味着针对攻击者感兴趣的资源具有访问策略的帐户将成为攻击者的主要目标。

攻击者可能使用网络钓鱼，社交工程或攻击的组合来获取有价值帐户的凭据。根据攻击者的动机，“有价值”可能意味着不同的含义。例如，企业管理员帐户可能很有价

值，但对财务收益感兴趣的攻击者可能会考虑可以访问同等价值的财务或付款资源的帐户。实施 MFA 进行网络访问可以降低从受感染帐户访问的风险。但是，就像传统企业一样，具有有效凭据（或恶意内部人员）的攻击者仍可能能够访问已被授予帐户访问权限的资源。例如，具有有效人力资源员工的凭据和企业拥有资产的攻击者或受到攻击的员工可能仍然能够访问员工数据库。

零信任架构增强了抵抗这种攻击的能力，并防止了任何受损的帐户或资产在整个网络中横向移动。如果泄露的凭据未被授权访问特定资源，则将继续拒绝它们访问该资源。此外，与传统的基于边界的网络中发生的情况相比，上下文信任算法更有可能检测到该攻击并对其做出快速响应。上下文 TA 可以检测出异常行为的访问模式，并拒绝受到破坏的帐户或内部人员对敏感资源的威胁访问。

（2）零信任采用隔离方案保护 IAM 账户关键数据

零信任架构攻击者将针对网络中的关键数据展开攻击，例如存储访问所属资源的账户信息、策略信息等，因为零信任架构将提供足够的保护，保证它们应该具有最严格的访问策略，并且只能从指定（或专用）管理员账户进行访问。

用户身份认证对于零信任网络非常重要，用户身份信息非常敏感，为安全保护好用户的身份信息，需要最小化存储数据。维护基础身份记录的系统并不需要存储所有身份信息，最好明确地分开存储不同的用户数据。记录系统只需要存储可以识别个人身份的关键性信息，比如可以只存储用户名或其他一些简单的个人信息，以便在用户忘记凭证时帮助其恢复身份。衍生系统可以使用此记录系统中的权威 ID 来存储额外的用户信息。

同时，用户身份信息的存储和保护还应与认证方式相关联，不同的认证方式应采用不同的数据存储和隐私保护方法。比如：

1）基于密码的认证方法：密码是常用的认证机制，只要密码设置的得当，密码验证仍然具有一定的价值。每个应用和服务应选取不同的、位数足够长且难以猜测的密码，但是对于用户来说密码管理有一定的难度，用户可以利用密码管理器来管理多个高强度密码，从而有效降低数据泄露风险。同时，任何时候不能以明文形式存储密码、存储密码时应加密散列值。

2）基于时间的一次型口令：这种认证方法要求用户随时间改变口令，该方式要求用户和服务之间共享一个随机的种子秘钥，种子秘钥和当前时间戳结合，使用散列算法形成一次性口令。所以，种子秘钥在用户设备和认证服务器上的存储非常重要，RFC 6238

标准建议硬件设备存储加密的秘钥，并限制对硬件设备中加密数据的访问。

3）基于证书的认证方法：证书通过一个高强度的私钥生成，再使用签发 CA 的私钥对证书进行签名。对证书进行任何修改都会造成 CA 的签名无效，因此证书可以最为任何信任其签发 CA 的服务的认证凭证。为保证证书认证机制的安全性，可以在特定硬件设备上产生和存储私钥防止数字盗窃。

4）基于安全令牌的认证方法：安全令牌认证方法将用户身份与硬件设备绑定，安全令牌可生成用户凭证/私钥，且凭证信息永远不会离开硬件令牌。这种认证方法面临的风险主要是硬件令牌设备被盗或被滥用的问题。同时，建议使用口令或生物特征等附带额外认证因子的安全令牌。

5）基于生物特征的认证方法：该认证方法主要是通过用户生物特征进行认证，该方法更安全便捷。基于生物特征的认证方法依赖于物理特征的精准度，攻击者会利用这种特性，欺骗传感器，从而通过认证。同时，某些生物特征泄露会被攻击者窃取并复制，从而欺骗认证系统。

6）单点登录认证（SSO）：单点登录认证下，用户通过集中授权进行认证后获得令牌，在用户后续与其他服务进行通信时，向这些服务提供带令牌的请求，通过安全的传输通道向认证服务验证这些令牌的合法性。这可以将认证与服务进行解耦。但是这种认证下，控制平面只负责对初次请求进行授权，剩下的所有认证授权都交由服务负责，这与零信任网络中用户信任级别是动态变化的，所以在使用 SSO 方式时要提前评估。

10.2 零信任发展对 IAM 带来的挑战

随着零信任的持续演进，以身份为基石的架构体系逐渐得到业界主流的认可，伴随着云计算、移动互联网、物联网、5G 等新技术的崛起，零信任架构体系作为快速适配新应用场景的解决方案，被寄予厚望。作为零信任基础支撑技术的 IAM，也将面对以下的挑战。

10.2.1 全面身份化的挑战将进一步拓展 IAM 对象类型

零信任通过 IAM 实现设备、用户、应用等实体的全面身份化，采用设备认证、用户认证、应用认证等多种技术手段，从 0 开始构筑基于身份的信任体系，建立企业全新的身份边界。为了适配新应用场景，IAM 将完成客观世界对象的身份数字化过程，支持

万物互联的身份认证技术、以及不同类型数字化身份的属性管理。

（1）支持设备互联的身份认证技术

在万物互联的时代，物已经成为了重要的参与实体，其基数已经远远超出了人。因此，仅仅为人创建身份是远远不够的，需要建立全面的“实体”身份空间，包括：用户、设备、应用和接口等，都需要具备唯一的数字身份。通过全面的身份化，实现对网络参与的各个实体在统一的框架下进行全生命周期管理。对于设备的身份标识、身份认证、可信，一直以来都是难题，谷歌采用的方法也是一个管理借鉴的思路：根据各代服务器设计的不同，将启动链的信任建立在可锁定的固件芯片、运行谷歌编写的安全代码的微控制器或上述谷歌设计的安全芯片上。每台服务器上都有自己的特定身份标识，该标识可以与硬件信任根和机器启动时使用的软件绑定。该身份标识用于验证与机器上底层管理服务之间的 API 调用。同时，谷歌还开发了自动化系统，以确保服务器上运行最新版本的软件堆栈（包括安全补丁），来检测和诊断硬件和软件问题，并在必要时将机器从服务中删除。

物联网极大地扩张了需要管理的机器身份数量，并赋予了普通消费者设置、管理以及保护这些机器身份，并监管机器间相互通信方式的责任。需要注意的是，设备、机器人以及 IoT 设备如今都需要访问计算和数据资源，所以它们也都必须纳入 IAM 管理的范畴内。

（2）进程、容器、工作负载等身份标识技术

随着数据中心的建立，进程与进程之间通信同样需要认证，而现今使用广泛的标识（IP 地址），并不适用于进程与进程之间的通信，如：Kubernets 为每个进程指派一个 IP 地址，但是多个软件服务可能共享同一个 IP 地址。同时，基于 IP 地址的标识机制还存在访问控制列表的规模过大、潜在的 IP 地址伪造等问题。要实现进程与进程之前的安全通信，需要更细粒度的标识，需要构建工作负载特有的身份标识体系。目前，不同的软件平台对与工作负载标识的方法不同，相互之间不能兼容，且没有一个具有互操作性、能完美的与客户系统兼容的标识。通用安全身份框架（SPIFFE：Secure Product Identity Framework For Everyone）提供了统一的工作负载身份解决方案。通用安全身份框架主要包括三部分内容：统一工作负载身份标识、身份标识证书、API 规范及约束，通过开源项目 SPIRE（SPIFFE 运行环境）实现。

10.2.2 适配复杂环境的挑战进一步扩展了 IAM 的适用环境

当前，全球已进入数字化转型时期，传统 IT 开始向以数据和业务为核心的新一代 IT 转变，其典型特征是以“云大物移智工”等技术为支撑，企业普遍通过采用新技术，帮助企业提升决策水平、构建新型业务模式，实现产业升级。现今严峻的安全态势和数字化转型浪潮下的新安全需求都促使了身份与访问控制成为信息系统架构安全的第一道关口，零信任安全正是拥抱了这种技术趋势，其核心就是重构访问控制。从企业数字化转型和 IT 环境的演变来看，零信任落实实践的关键就是适配复杂环境。

（1）适配复杂网络基础环境的技术

作为基础平台的云计算技术发展迅猛，云计算硬件和网络体系经过多次结构化重组，互联互通的安全体系持续演进。同时，随着边缘计算技术的不断完善，边缘计算在本地执行计算和分析的思想也越来越被接受，云网融合、云边协同成为新的基础架构，承载网络可根据各类云服务需求按需开放网络能力，实现网络与云的敏捷打通、按需互联，并体现出智能化、自服务、高速、灵活等特征，极大的满足物联网、新兴的 AI、以及机器学习等部分场景在敏捷连接、实时业务、数据优化、安全与隐私等方面的计算需求。

零信任架构面向被保护资源的网络环境发生了极大的变化，通信模式不断变化、流量模式也不断进化发展，想要成功保护服务资源，就必须为每个应用创建细粒度的访问权限策略以放行所需访问，并封禁所有不当请求，同时策略变更速度和形式也必须适配应用的变更。就要求 IAM 也同步适配网络环境、通信模式和响应速度，以及基于会话的端到端实体身份管理和认证，能够支撑零信任架构在新技术环境下提供精准服务。

对于云化环境的支持的 IAM 解决方案正在开始推迟，专门针对云环境设计的 IGA 解决方案，帮助用户访问网络内资源之外的环节。

（2）灵活的服务扩展能力

伴随信息化系统基础环境日新月异的发展，软件开发、服务模式也加速更新迭代。以容器、微服务、DevOps 为代表的云原生技术，以敏捷的数据驱动、精细化运营为特征的数据能力复用技术，支撑企业快速在云上部署具有更高敏捷性、弹性和云间可移植性的应用系统和大数据服务系统，在云间实现上、下层的数据应用连接，边缘计算在本地执行计算和分析，松耦合服务带来业务的重用、服务的编排助力业务的快速响应和创新……现代应用一般由模块组件动态构成，采用容器化、微服务和工作负载均衡技术。

同时，数据中台和业务中台分离、网络飞地的大量出现、拥有多个数据中心，在数个远程地点放置服务器和计算资源，以及拥有一个或多个公共云及云提供商的情况如今并不鲜见。应用系统无论从形态、部署位置、服务模式都发生了翻天覆地的变化。IAM 技术作为零信任架构的基础身份设施，自身也面临这一挑战，需要使用容器、微服务、服务网格、编排等技术实现灵活的水平扩展，支持异构系统互操作支持和端到端的安全加密.

10.2.3 复杂组织关系的挑战进一步提升 IAM 的扩展能力

（1）IAM 的复杂关系管理扩展性要求

零信任架构采用的身份管理机制是渐进式的，以统一的管理要求分步骤实施，在梳理常用的、公共的访问权限并进行基于角色的策略配置后，采用自助服务机制，由业务部门和用户自主发布和申请访问权限，兼容多种不同的身份生命周期管理流程。同时，自动触发身份管理的评估审批流程，保证安全的可控性和自组织性。但是，随着新技术环境下的系统越来越复杂，对于 IAM 的全生命周期管理要实现跨租户、跨账号体系、跨端、跨用户渠道、跨应用、跨生态的支持，对于 IAM 的扩展性和管理要求提出越来越高的要求。

一些管理提供商正在发展成为全栈（full-stack）一站式商店，以满足用户的所有身份需求。谷歌发布了完整的“身份即服务”产品，其使用了开放标准：云身份（Cloud Identity）。云身份服务列表非常广泛，其单点登录支持 SAML 2.0 和 OpenID，并且可与数百种外部应用协作，包括 Salesforce、SAP SuccessFactors 和 Box，以及 G Suite 应用程序（如 Docs 或 Drive）等。对于使用谷歌云计算平台（GCP）资源的组织来说，Cloud Identity 还提供了额外的控制功能，用于管理跨现场及云基础设施的混合环境用户及群组。

（2）区块链等自主主权身份催化新一代的 IAM

自主主权身份是搭建在区块链上的数字身份，也是用户对数字身份掌控度最高的形式，从此用户不再将自己拥有的身份数据进行严密托管，并反复证明“我是我”，此类数字身份因为结合了区块链的去中心化、分布式、共识机制、哈希加密等特性，因此在自主、安全、可控层面更上一层楼。简而言之，自我主权身份使用户在网上也能够以“亲自证明”相同的方式对自己进行身份验证。用户可以存储自己的个人识别数据，而不必将其提交到某个公司管理的集中化数据库中，随着全球主要公司和政府努力“消灭密

码”，可以预见的是，在线身份识别和管理方式也正面临一场巨变。整合区块链有可能在很大程度上改变 IAM，催化新一代的 IAM。

目前，区块链这种分布式账本平台正被广泛用于提供数字身份。在业务方面，基于 IBM 区块链的 SecureKey 是加拿大第一家专门用于受监管行业的数字身份网络。而 Shocard 则是一家面向企业的区块链式 IAM 和单点登录（SSO）解决方案。Evernym 是一个信用社数字身份平台，其并非建立在区块链基础上，而是建立在开源分布式账本平台 Sovrin 上。其中，Sovrin 的工作方法名为“自我主权身份”（self-sovereign identity），这是一种个人合法身份，每个人可以选择愿意透露的信息。如果你是 Sovrin 网络的一员，可以构建和维护自己的身份声明组合。你可以挑选和选择在任何特定情况下共享哪些数据。借助身份声明组合，你可以逐渐拥有、构建和控制自己的在线身份。避免了让某人未经授权就能访问你的银行和信用账户这一风险，因为除非通过你发布的身份声明，否则那些账户永远无法识别。

目前，Accenture 和微软已经联手创建了基于区块链的身份基础设施，以帮助联合国为全世界 100 多万名没有官方身份认证的人（比如难民）提供了合法身份证明。

11 IAM 实践案例分享

11.1 IAM 体系案例研究

IAM 体系的实际架构与所属组织的实际情况紧密相关，因此很难用一个统一的通用实践来说明上述章节的内容是如何融合的。

11.1.1 IAM 体系与所属组织之间典型关系

一般大型集团公司中典型组织，可以分为管理组织、人力组织、法人组织、财务组织（或核算组织）、虚拟组织五类。

1） 管理组织指在企业内各个信息系统内存储的身份信息的组织体系，通常用来描述企业建设的信息系统的用户的层级结构。

2） 人力组织指在企业内使用的人事管理组织体系，通常用来描述员工上下级汇报关系和组织的管理单元。

3） 法人组织指具有法人资格享有民事权利和承担民事义务的企业的组织体系。

4） 财务组织（或核算组织）指在企业内依据财务或成本职能部门的要求建立的组织体系，通常用来描述对企业内的预算、核算进行管理单元。

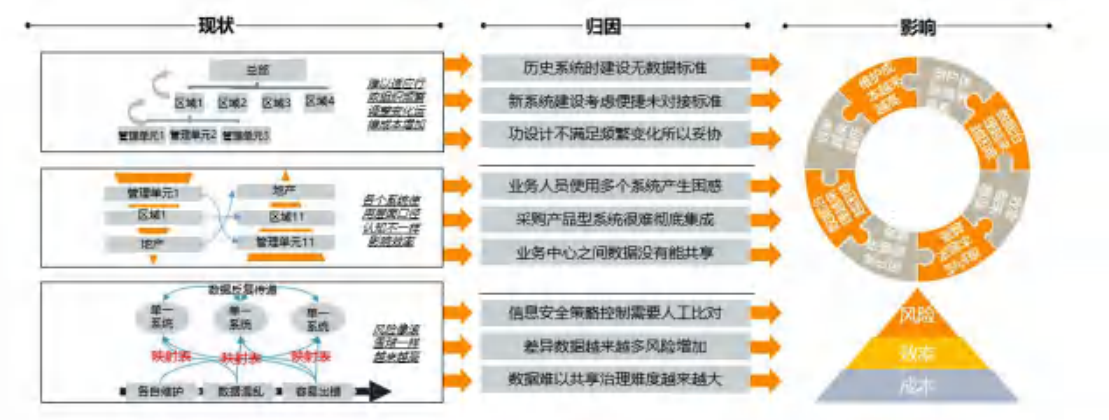
5） 虚拟组织指在企业内正式或非正式的组织体系，通常用来描述一些跨越职能并且具有一定目标工作的组织体系，比如 XXX 工作筹备组、XXX 监督委员会、XXX 生产协调工作组。另外，还有一些虚拟组织并没有正式任命而是一些满足工作沟通的群组。

6） 以上五种类型的组织在 IAM 体系内进行相关管理，目标是在企业内建设的各个信息系统中的账号、组织和权限之间架起一座通畅的桥梁，IAM 是企业内信息化规划蓝图重要部分。

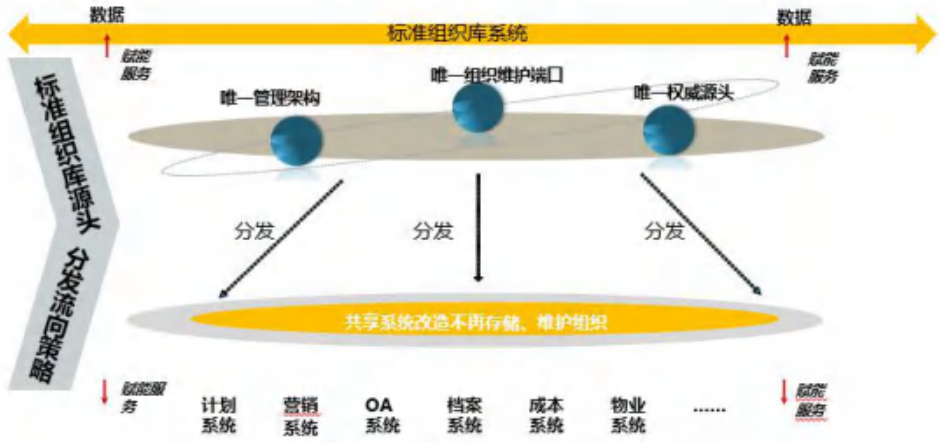
11.1.2 IAM 体系在企业实践中的典型问题

相比技术而言，企业 IT 人员如何良好的运营管理 IAM 体系的可能会提出新的挑战。在日常生活中，由于公司经营管理的调整、治理架构的变化以及新业务发展往往会在 IAM 体系的使用时，产生更多新的问题。在某些情况下，使用 IAM 体系并严格执行可能会带来更多的工作任务。例如，公司行政管理部门发布虚拟组织后还需要考虑后续人员变更情况与虚拟组织的消亡。

企业内经常用到的信息系统是分部门建设与管理的。这就产生了数据孤岛，阻碍了数据的共享与正常管理，一些企业由于缺少统一的 IT 规划、历史包袱沉重导致 IAM 身份管理体系很难发挥实质管理作用。全面的 IAM 体系的搭建可以消除用户认为他们只需要满足他们单一需求的看法。



缺乏前瞻性的规划与设计是有风险的，这种风险应该被评估和量化。有时只有当内部问题与管理风险被频繁暴露出来企业才会采购 IAM 管理相关产品。很有可能的是当发生了法律责任风险后才会反思并做出反应，然后疲于寻找相关文件和信息系统进行安全审查。IAM 管理体系的地位需要在组织内得到提升，不应该被视为是低级别和低优先级的功能，更多时候它应该被首先规划与设计的甚至是第一优先级的。



为了解决上述问题，有些企业使用 IAM 相关产品进行一体化管理满足不同管理维度和不同层级分发的诉求，通过一体化管理一致的描述了标准组织源头和分发流向策略，通过数据属性描述和它们之间的关系加深了用户的理解，另外对于特定的应用或具体的项目也能够有数据模型及其定义、规范、映射和管理流程解决数据混乱的问题，降低企业的信息化建设管理成本，提升工作效率并降低信息安全风险。

重新定义组织（身份）数据的管理层级是将复杂的问题转变具体的解决措施（简单化）的必经步骤，金字塔中每一层对应一种不同的管理措施。

组织标准数据层，它是权威的组织数据标准，需要进行全局并且统一的运营管理，它由企业内的业务管理部门审核保障权威性并作为数据资产的一部分。

组织共享数据层，包含企业内部分信息系统之间共享的组织数据，与组织标准数据不同，它在局部是统一的，是组织标准数据的延伸。

组织全量数据层，包含企业内所有信息系统的身份数据，由于不具重复被使用的需要，一般由信息系统的运维管理人员进行维护。

设计企业内身份数据的分层级管理架构，必须考虑决定投入多少时间和精力到构建和维护企业的组织（身份）数据模型上。通过构建组织（身份）数据模型可以实现按质量分层级管理数据,数据质量的提升就像爬楼梯一样,逐步柔性变革提升质量。随着时间的推移，企业内信息化建设的需求会发生变化，随之带来身份数据模型各个层级的内容通常会扩展。对于一个良好的数据模型应该考虑不同层级增量和迭代方式保障模型更长的生命周期。

上图示例可以清晰的展示组织标准数据层、组织共享数据层和组织全量数据层之间

的关系和工作中的使用情况。在复杂的场景使用中可以通过 IAM 相关产品对操作权限与相应职责划分不同策略,建立协调、合作的工作关系,确保实现明确的身份管理数据认责机制。

其中组织标准数据层是集中管理的，它基于信息安全的单一存储，能够满足不同的管理视角的使用需求并明确数据获取职责与数据的依赖管理。组织共享数据层能够满足不同的细颗粒度数据管理需求它能够在自己的领域内能够保持完全一致。

在企业中使用 IAM 相关产品构建这些组织（身份）数据模型是一个长期的过程，下面通过研究几个不同行业的相对完整地实现了 IAM 体系的案例，可以帮助我们更好地理解在不同的业务背景下如何设计和实现满足自身的身份治理和安全访问控制需求的解决方案。

11.2 中通 IAM 一帐通平台

第一个案例是中通 IAM 一帐通平台。该项目的重点任务是支撑中通零信任安全架构的部署实施，提供统一的访问控制相关的服务支持，主要包括身份治理服务、帐号管理服务、认证服务、授权服务、审计服务、应用管理服务、策略服务和资源管理服务等。

中通从 2016 年开始 IAM 相关服务的建设，最初是为了实现免密登录系统，从而彻底解决几十万个网点工作人员习惯性设置弱口令、经常忘记密码、密码随意出借等痛点。随着零信任安全架构的不断演化推进以及集团内生态圈业务的蓬勃发展，对 IAM 相关服务提出了更高的要求，因此诞生了中通 IAM 一帐通平台，目前仍然处于快速迭代过程中。

具体介绍一帐通前，简要介绍中通集团的业务背景。中通目前是全球快递业务体量最大的公司，2019 年全年快递业务量达到 121.2 亿件，已经保持了近五年的行业龙头地位，此外生态圈内的快运、云仓等业务做到了行业排名靠前。2016 年中通登录美国纽交所，市值超过 250 亿美元，中通全网有三十多万员工，快递服务网点将近三万多个，快运服务网点一万多个，仓储总面积 160 多万平方米，覆盖了全国绝大部分城市和乡镇。在快递主业的带动下，中通积极拓展上下游生态业务，建立了快运、云仓、国际、商业、金融、传媒、航空和智能板块，正逐步向平台公司和生态公司迈进。

可以想象这种规模和量级的业务在爆发式发展过程中，对公司的数字化治理，特别是对信息系统的身份治理和访问控制，必然会带来前所未有的挑战。由于中通员工规模

庞大，办公网点分布在全局各地，同时有大量的 IOT 设备参与到业务流程，人员、设备和应用等与企业资源之间的交互及认证方式多种多样，因此导致人员管控力度非常微弱以及整体的边界安全访问控制体系非常不稳定。从业务角度看，不同的系统需要提供服务的用户群体多种多样且部分有交叉，总体上包括内部员工、外部消费者以及上下游供应链上的商业实体，具体的功能需求和用户交互方式既有共性也有明显的差异性，导致重复开发访问控制功能并频繁爆出各种漏洞，业务上共性数据资源也无法融合互助，形成信息孤岛。另外为了满足各类业务需求，需要对接上线大量各类来源和部署方式的应用系统，包括自研和外采的，物理机、虚拟化和容器化部署的，本地部署、私有云部署和公有云部署的，那么对众多的异构系统如何做好统一安全访问控制的集成是非常大的挑战。最后业务原因人员流动性高，组织架构变更频繁，各类访问控制的变更需要能够更加自动化地完成，同时需要支持以受保护的资源为中心，能够结合设备、环境、上下文、信任评估结果等因素实施动态访问控制。

基于上述面临的挑战以及实施零信任安全架构的迫切需求，中通对一帐通平台的设计提出了如下四个目标。一是全面身份化支持，使用统一身份安全框架，将客观世界的对象抽象和分类为逻辑上具备不同属性的身份，如人员、设备、应用、API 等，实现支持万物互联的身份认证技术，为后续的访问控制和互操作奠定基础。二是复杂组织架构和多元业务模型的支持，针对中通这种具有几十万人横跨多个业务单元、面向众多不同终端客户的商业组织，全面支持面向消费端的 B2C（Business-to-Consumer）、面向内部员工的 B2E（Business-to-Employee）、面向商业端的 B2B（Business-to-Business）三种用户群体，满足跨租户、跨帐号体系、跨 SSO、跨平台和客户端、跨用户群体、跨应用的需求，以及认证和身份源分离的联邦认证等多认证方式的支持。三是对基于混合云架构下的异构系统对接的支持，通过容器、微服务、服务网格、服务编排等云原生技术，将各个功能组件解耦，建立多个相互隔离的中台服务，实现灵活的水平扩展和异构系统互操作支持，真正打通本地数据中心、云、办公等网络边界，全面从网络层访问控制升级为应用层全流量深度检测的动态访问控制。四是结合资源中心实现基于策略的访问控制，通过策略进行自动化的授权变更，同时做到基于身份的正向鉴权和面向资源基于策略的反向鉴权，并在资源层面对所有操作进行分类分级和自动化的日志记录及审计。

虽然中通一帐通平台项目采用的设计方案和具体技术不一定能够适用于其他组织，但是各类组织面临的安全访问控制方面的风险和挑战是类似的，因此相关的特别是面向

未来的安全架构设计原则是完全可以借鉴的。

11.2.1 一帐通平台的主要组件

如上图所示，一帐通平台由众多相互协作的中心化组件构成，设计思路是尽可能地解耦各个内部组件并作独立部署，将身份、帐号和组织架构相关基础数据抽离出来单独做成身份中心，结合认证中心、权限中心、应用中心、资源中心、策略中心、证书中心、管理控制台以及开放 API、SDK 等构成一套完整的 IAM 服务架构体系，可以灵活地与各类应用在不同的层级进行无缝对接，同时支持面向内部员工的应用、面向消费者的消费端应用、面向上下游供应链的商业端应用、外采的三方应用的认证授权集成以及混合云架构下部署在公有云上的 SaaS 应用，实现企业的应用无论部署到哪，无论是自研还是外采，都可以共享一套强大灵活的安全访问控制基础设施，从而解决异构系统集成和安全管控以及身份全生命周期的安全治理问题。

一帐通的典型工作流程，首先是用户或设备等身份的认证授权，通过认证中心的单点登录模块将认证请求转发到对应认证协议进行处理，根据请求上下文连接到身份中心配置好的身份提供商 IDP，结合证书中心，执行 MFA 多因子认证编排策略，经过一系列的交互成功认证后下发访问令牌，用户携带相关访问令牌发起目标资源的操作请求，分布在操作请求路径上的策略执行模块按需去认证中心校验令牌的合法性以及到权限中心拉取授权，从策略中心同步相关策略完成鉴权以及执行相关的风控操作，如果通过校验满足访问控制策略，则放行本次的资源操作请求，但无论校验结果如何都要记录审计日志。本质上这套访问控制措施是以更灵活及更细粒度的方式来管控对受保护资源的任何操作，既能基于身份实现正向访问控制，也能基于资源和策略实现反向访问控制，其

中更灵活和更细粒度是体现在身份、权限、策略、资源和资源操作的严格定义上，事实上这一点至关重要，如果不能通过独立的中心化组件把以上实体定义清晰和有效隔离，那么将无法实现功能强大的基于策略的访问控制。接下来将简要说明一帐通的部分组件及相关扩展功能。

11.2.2 全面身份化的身份中心和证书中心

身份是任何安全基础架构的基石，任何安全信任都是构筑在身份安全的基础之上。从保障万物互联的安全访问控制需求看，任何对象都需要建立对应的身份实体，既包括客观存在的物理实体也包括抽象的逻辑实体，通常可以分为人员、设备、应用、API 等几大类，把上述定义的身份实体、身份实体的关联属性如帐号和组织架构以及相关 API 操作聚合为身份中心，对身份中心包含的所有元素的全生命周期的管理和控制定义为身份治理。通过全面身份化的底层设计，结合具体场景下最佳的认证方式，可以方便地支持设备与设备、人员与设备、组件与组件、服务与服务以及人员与人员等的安全交互。目前业界也有仍在发展中的相关标准和实现，如 SPIFFE 规范定义了一种身份及身份制作标准，能够支持在云原生环境中对服务进行身份验证，而 SPIRE 是 SPIFFE 规范在各种平台上的代码实现。

身份中心支持创建多个帐号体系，满足不同类型用户群体的需求，每一个帐号体系下还可以建立各种类型的帐号组，如根据组织架构自动建立的、根据角色建立的等，帐号组实际上可以包含支持各类身份的帐号，如人员身份、机器人身份、设备身份等。值得一提的是，组织架构类型的帐号群组，可以与人事管理系统联动，由系统自动创建，除了可以辅助人员入职时结合权限中心进行自动授权外，还可以自动加入或者退出内部协作 IM 工具的沟通群组，更好地帮助提升协同办公的效率和安全性。

为了打造安全的身份标识并遵循业界现有的标准，一帐通基于传统 PKI 设计了证书中心，重点在性能和扩展性方面做了特别的优化。证书中心主要涉及证书签发、证书轮换以及证书吊销三部分的功能，典型工作流程是新的终端设备和新的服务上线前自动提交证书申请到证书服务集群，由证书服务集群作为代理向 CA 发起请求，申请到证书后由证书服务集群转发到申请者。证书轮换由证书申请者按照一定的规则自动重复上述申请流程即可，证书吊销申请和证书吊销查询服务也统一由证书服务集群作为代理，在身份认证时由服务提供方通过接口实时查询是否吊销，在控制台实现即时吊销身份功能。

11.2.3 兼容并包的认证中心

一帐通平台的设计目标之一是支持混合云架构，那么必然需要支持和各类异构系统进行安全认证的集成及互操作，主要通过以下三点实现，一是认证与身份数据源（IDP）的分离，在控制台既可以配置使用自有身份中心提供的身份数据源也可以配置调用远程第三方的身份数据源；二是与授权数据的整合，在认证过程中仅对身份做认证，不牵涉鉴权也不拉取授权数据，若认证成功，则根据配置从本地权限中心或者远程第三方拉取授权数据，与身份数据整合后发送到认证应用；三是对各类认证协议的广泛支持，兼容业界普遍使用的认证协议或数据同步规范，如 OIDC、OAuth2、SAML2、SCIM、LDAP、FIDO2 等。

11.2.4 集中化的权限中心

权限中心定位是集中的权限配置和存储平台，对外提供统一的管理控制台、增删改查接口及相关 SDK。与传统的权限模块相比，权限中心既不涉及鉴权也不提供授权服务，只提供强大的集中化的权限配置服务，支持跟权限相关功能特性的配置需求，如菜单及菜单权限、按钮或者动作行为权限、基于自定义数据维度的数据权限及权限范围设置、角色配置、权限职责分离等，实现横跨同一帐号体系下所有应用的权限的统一接入和集中管理审计。在权限模型方面，我们采用 RBAC 用于对资源的正向访问控制，如控制某些角色可以查看哪些模块或者哪些范围的数据，采用 PBAC 对资源进行反向的访问控制，如对某个资源某次特定的访问操作必须匹配哪些策略或者满足设定的信任值区间。一个典型的权限配置过程包括定义资源、定义资源操作、定义访问的身份实体，若需要基于身份属性、资源属性或者资源操作等定义更复杂的权限需求，如添加自动化权限变更任务，则可以在下述的策略中心添加特定的权限策略。

11.2.5 灵活使用策略中心

为了构建敏捷和现代化的身份基础设施，一帐通设计规划了策略中心用于实现基于策略的访问控制，从而打造更加动态智能的授权体系。策略中心由策略管理点（PAP）、策略信息点（PIP）、策略决策点（PDP）、策略生成点（PGP）和策略执行点（PEP）等模块组成，能够完成各类策略的全生命周期管理和运营。其中策略管理点负责策略及

策略集的创建、展示、组合、分配、冲突处理、撤销和删除等，策略信息点负责接入信任评估结果、请求上下文、资源中心相关数据、权限中心相关数据等并进行格式化，策略决策点主要负责策略的计算、合并、诊断信息输出、决策结果输出等，策略生成点主要负责策略的格式化、输入对接、分发等，策略执行点负责集成到多渠道的可信执行器，实现最新策略结果的自动发现并输出到可信执行器。策略中心的策略定义是泛化的，不与任何具体的身份实体、资源、资源操作相绑定，是在运行态通过上下文进行实例化，但策略可以表示身份实体、资源和资源操作以及其属性和方法之间的任何关联，这些关联是通过一系列预先定义好的规则原语并结合下述的资源中心进行定义和解析。通过灵活使用策略中心，一帐通可以做到在管理态灵活配置访问控制策略，同时在运行态实现动态计算参与执行策略的各类元素。

11.2.6 资源中心和合规审计

不管是基于策略的访问控制还是零信任安全架构，都对清晰的资源定义有明确的需求，因此一帐通设计规划了资源中心。资源中心定位为一个中心式的数据仓库，作为底层基础组件，提供了统一的数据出口、入口以及完备的数据订阅消费和同步机制，为所有一帐通组件之间共享数据及保持数据一致性搭建了桥梁，并负责与外部系统的数据对接，其本质上是一个升级版的配置管理数据库（CMDB）。资源是一切可以抽象为具体数据表征的对象，如身份实体、被操作对象、操作行为等，它们的属性在资源中心可以使用标签来方便地创建和聚合查询，通过缓存和异步更新技术保障整个平台的高可用和数据的及时性。一帐通平台中另外一个重要的模块是合规审计，系统上线前需要通过合规审计，特别要注意面向消费者端的用户隐私保护，其中国际业务需遵循当地的法律法规，系统上线后进行定期审计，持续跟进最新的法律法规并保障合规，并且聚焦在及时发现处理各类审计异常。

11.2.7 使用应用中心和扩展工作台

一帐通平台还设计开发了应用中心组件以及扩展配套了的安全工作台，应用中心负责应用的管理和发布等，工作台是在用户终端安装的生产力工具，用户可以在工作台上方便安全地接入各类应用，本质上是一个提供全渠道多端安全协作的工作负载平台，借助于工作台移动端的扫码、动态码、推送等功能得以取代传统的静态密码认证方

式，实现了具备良好用户体验的双因子认证，再配合实人认证以及活体检测等风控校验措施，极大地提升了整个平台和接入应用的安全性。

11.2.8 经验总结

中通一帐通平台经过了几年的迭代开发和实施，取得了一批比较显著的产出，如工作台用户 30w+，数百个应用实现了统一权限集中管控，全网实现了免密登录和智能人脸核验，对高危操作实施基于策略的访问控制，与第三方厂商的软硬件对接实现了精细化的办公网络准入控制等。在这个过程中，安全团队始终面临着一系列的挑战和问题，这些挑战和问题随着项目的推进和上线也逐一得到解决，希望总结的以下四点经验教训可以为寻求实现类似解决方案的企业少踩一些坑，节省一些时间。第一点是做好沟通，首先是向上沟通，因投入成本较大，实施周期漫长且容易出各种状况，需管理好相关方期望并得到决策层的强力支持和极大的包容，其次是与各业务产品部门做好充分的沟通获得理解和支持，因为大量实施工作需要各业务产品部门协助配合改造，并且有可能影响线上业务系统的可用性。第二点是尽力避免影响业务，首要考虑业务系统的高可用性以及可维护性，优先级要高于安全性，要避免导致线上故障特别是长时间大规模的服务不可用事故，因此需要尽可能地在不影响业务运营的情况下同步进行开发和部署，并着力打造强大的故障监控响应和恢复能力。第三点是拥有配置合理充足的人才团队，包括设计规划、产品研发、安全专家和实施支持等，因为技术难度和整体工作量都比较大，需要极强的工程能力和较大规模且稳定的核心团队，特别要重点建设有维护高可用、系统稳定性运营经验的人才梯队。第四点是尽可能借鉴业界最佳实践以及优秀开源项目，站在巨人肩膀上更有质量也更有效率。

11.3 碧桂园权限中台实践探索之路

11.3.1 中台概念的由来

坊间流传最广的说法是，2014 年马云考察了芬兰的游戏公司 Supercell，发现对方不是按项目划分开发和运营团队，而是所有游戏团队共用开发，每个前端团队可以做到非常轻量化从而实现灵活机动。而这个共用的开发平台被称为“中台”。 受到启发，

回国后马云开始在阿里内部普及中台理念，并于 2015 年正式提出中台战略，推动“大中台，小前台”的组织和业务架构变革。

但据比升技术 CEO 钟华（原阿里巴巴中间件首席架构师）介绍，这并不是阿里中台的起点，在此之前阿里的中台雏形其实已经孕育了 7 年之久。而这就要从 2008 年阿里在淘宝内部孵化出天猫（原名淘宝商城）说起。 最开始时，天猫只是淘宝事业部下面的一个部门，淘宝抽调了一拨人去支持天猫的产品开发和运营工作。由于天猫发展迅速，在阿里内部的战略意义越发重大，阿里很快就成立了一个与淘宝事业部平级的天猫事业部，但天猫的开发任务当时仍由淘宝的技术团队负责。 可想而知，分家不分工肯定会出问题。淘宝有限的开发资源自觉不自觉地就会优先倾斜本事业部，因此天猫的很多产品开发需求就总得不到及时响应。但完全分成独立的两摊事，为天猫配齐完整的项目开发和运营团队阿里又觉得浪费，因为淘宝和天猫的产品架构很相似（都有用户管理、商品管理、交易管理、店铺管理、购物车等模块），两套开发团队重复造轮子没必要。为此，2009 年阿里决定成立共享业务事业部，并将其定位为与淘宝和天猫平级的事业部，由其支撑后二者相同的开发需求，并将开发出来的应用变成可被任意业务调用的服务。而这个共享业务事业部就是阿里双中台之一的业务中台的原型。

原本为同时支撑淘宝和天猫而创的共享业务事业部，后来为阿里整个集团搭建业务中台奠定了基础，最早的 1688 和后来并购的飞猪、优酷、饿了么、口碑等业务也纷纷借助共享服务体系顺滑地接入了阿里生态。

11.3.1.1 阿里的中台是否能照搬到传统企业

虽然中台起源于阿里，阿里当前也在积极推动中台商业化落地，并愿意为传统企业提供咨询服务，但阿里毕竟是科技企业，和传统企业的组织状况以及业务结构千差万别。

“阿里是平台，没有生产制造等环节，因此传统企业很难照搬阿里的中台实施经验”。

韩振强（卓诗尼 CIO）

11.3.1.2 传统企业面临的信息化问题

先说阿里的业务中台，其雏形共享业务事业部创立的缘由，是为了解决淘宝和天猫

在开发资源争夺上的矛盾，貌似解决的只是阿里自家问题，但钟华认为，这其实是一个时代的缩影。

在 20 年前，中国的企业界尤其是大企业圈子里也闹腾过一段升级改造的浪潮，名为信息化升级。原因是随着企业规模不断扩大，业务越来越纷杂，过去手工记账的方式已经无法支撑企业进一步的发展，于是众企业纷纷从国外引进企业管理系统。 随着企业业务不断增多，子公司、分公司不断创立，多年来企业在内部部署的 ERP、CRM、OA 等管理系统越来越多。渐渐的，这些原本帮助企业提升效率的工具，反过来变成了阻碍企业继续发展的桎梏。

“但系统越多，系统之间打通和数据同步的难度就越大，信息中心对于业务部门诉求的快速响应也就越发力不从心。”

由于这些 IT 系统往往是自上而下部署实施的，而且传统企业的 IT 部门一般只负责评估需求和系统招投标，而没有能力对系统的设计做长远规划，因此就会出现重复造轮子的资源浪费现象。就像当年的淘宝和天猫，淘宝已经开发了购物车功能，到了天猫还得再开发一次。但这还只是过去系统部署方式的弊端之一。

而且，越大的公司，上的系统越多，类似问题也就越严重。然而在韩振强看来，这样的问题在传统的信息化理念下几乎是无解的，“过去的信息化理念是把业务流程固化在系统当中，追求系统本身的稳定性，系统建成后最好就不要再改动。但是当下的市场环境要求前端的业务部门必须能经常变、快速变，而后台的系统也必须跟着变。”

11.3.1.3 中台的核心作用

中台的作用就是帮助企业实现“核心能力的复用和核心资源的共享”，从而支撑更低成本的创新试错。

“中台不是一个产品或 IT 开发项目，而是一种理念，或一种方法论。”这听起来貌似很抽象，但他指明了企业要想拥有中台，不是部署一套软件系统那么简单。

陈吉平（袋鼠云创始人兼董事长）

以上内容摘自虎嗅 APP 《中台的中场战事》一文

11.3.2 碧桂园的权限中台

碧桂园权限中台也是基于“核心能力复用以及核心资源共享”的中台理念，把权限

管理作为中台应用的切入点，进入创新探索，于 2019 年 11 月启动了《碧桂园权限中台》的建设工作。

11.3.2.1 产品设计分析

11.3.2.1.1 现状分析

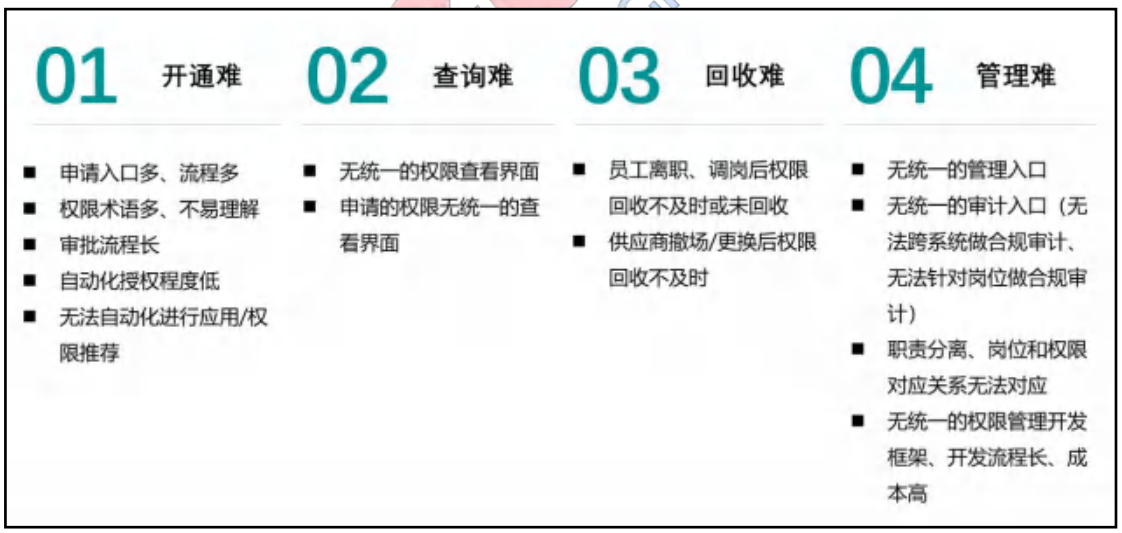
权限管理面临的问题：

- 业务系统多：目前登记在册的有 300+套系统；
- 重复造轮子现象严重：各系统各自建设权限模块；
- 用户应用端：

用户申请系统权限时，申请不同系统界面各不相同，用户较难理解，体验差。

- 运维端：

由于申请权限体验差，本来用户可以自助完成的操作，被转化为运维工作，导致权限授权运维工作量大，这是由于权限申请与权限分配没有打通，权限授权需要运维人员根据申请单信息进行人工判断，手工授权，容易产生误操作。



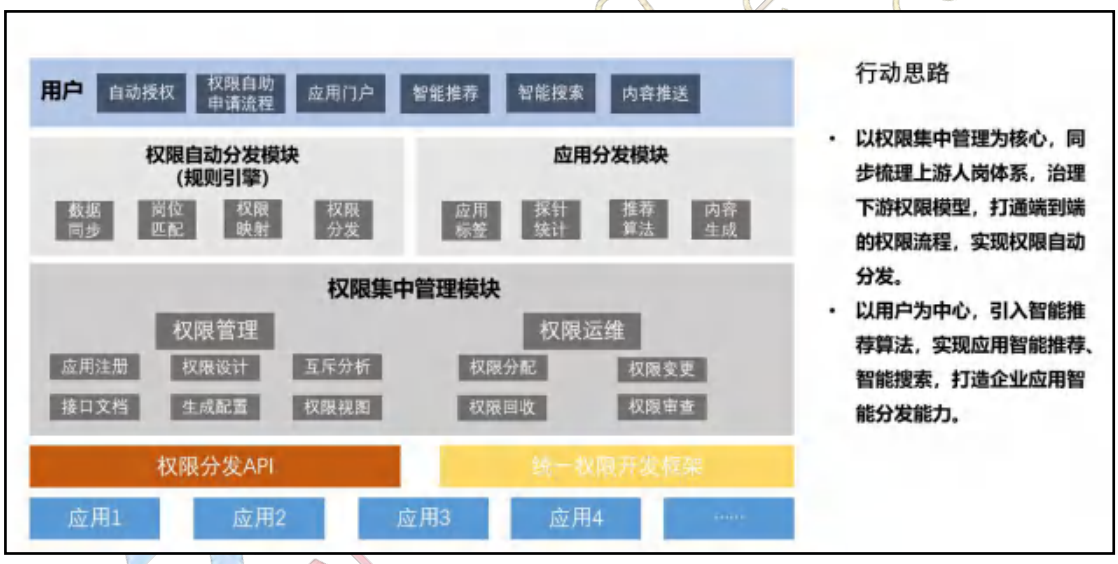
业务现状

11.3.2.1.2 解决方案

- 建设一个权限中心，面向普通用户，解决权限申请难的问题；
- 建设一个权限中台，面向开发、运维人员，解决权限统一管理，权限模块重复

开发的问题。

产品定位



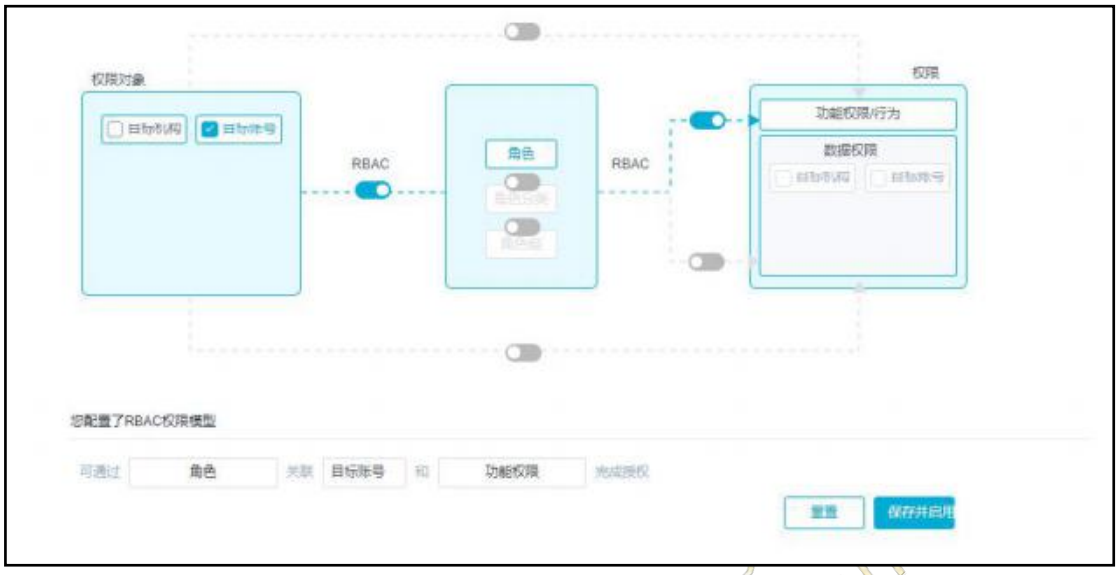
业务架构

11.3.2.2 产品研发过程

11.3.2.2.1 如何适配这么多系统？

经过对现有系统的调研，我们发现大部分系统采用的权限管理模型分 2 大类，分别是 RBAC（基于角色访问控制）和 ACL（访问控制列表），但同时存在一个问题，即每个系统在以这 2 大权限模型类别为前提下，又会存在个性化的部分，而个性化部分正好

是中台开发上的难点所在，因为中台的定位是平台型产品，不是要给每个系统做定制开发，于是我们初步确定必须有一套抽象程度较高的机制来适配每个系统的权限管理模型，最终经过多轮讨论与评审，确定采用图片化的定义方式，定义各系统的权限模型：



权限模型定义

11.3.2.2.2 如何让用户感受到申请权限很容易？

我们调研了各业务系统申请权限的操作，发现权限申请存在以下几个特点：

- **让用户做：**需要用户填写的信息较多，数据形式没有结构化，很多跟权限申请并无关系，或可以通过系统后台获取，无须用户手动填写；
- **让用户想：**与权限相关的属性较难理解，没有使用用户的业务语言进行表述，内部隐含逻辑较多，用户难以理解；
- **让用户烦：**用户通过找流程申请，而不是找系统，而流程名称类似，容易出错，造成查找难。

现有某系统申请页面

权限中心通过对各系统的申请需求进行抽象，设计出一个统一申请界面，该界面会根据系统的权限模型进行页面适配，比如系统只有功能权限，则表单上只显示功能权限申请相关字段，如果该系统既有功能权限又有数据权限，则显示功能及数据权限字段：

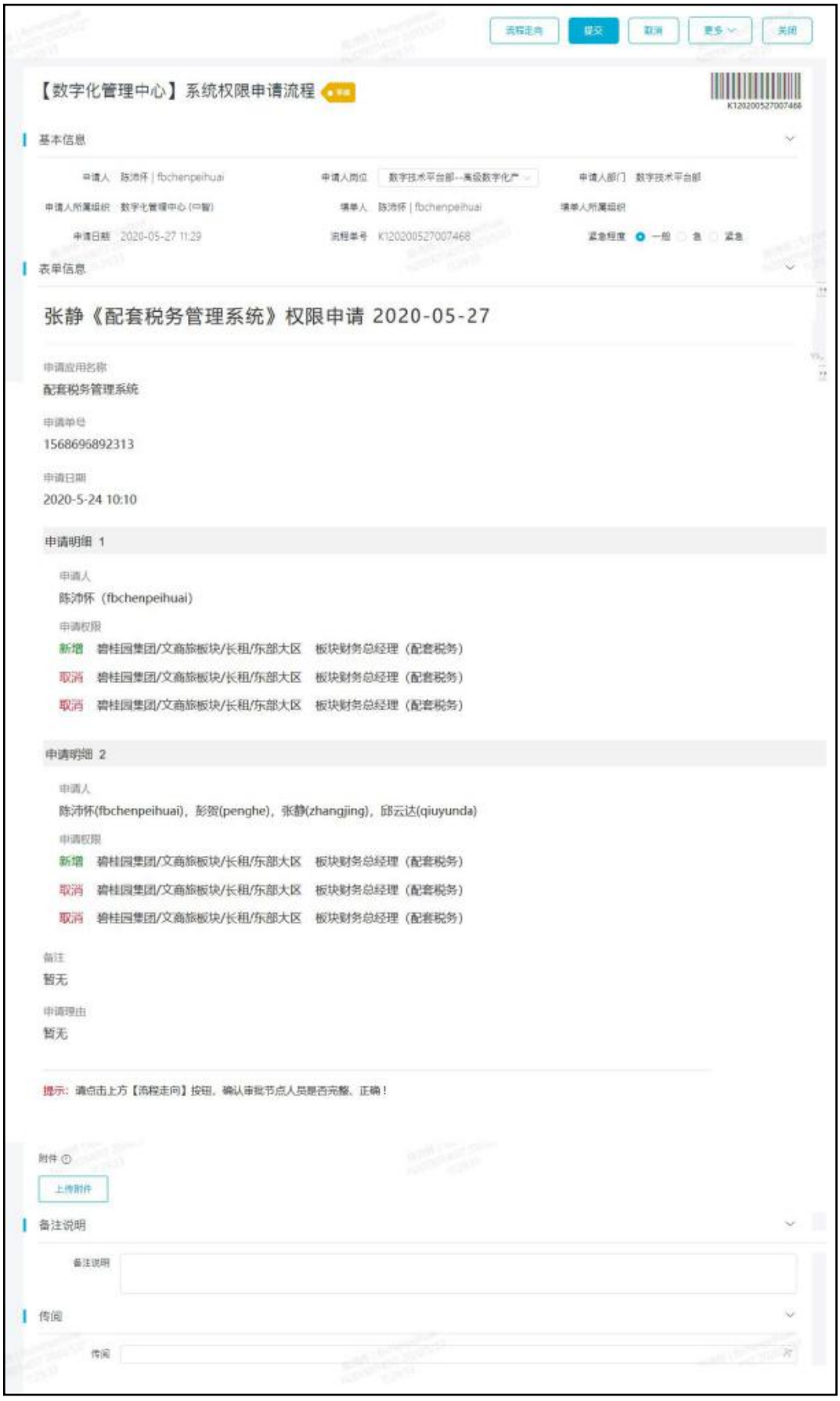
只申请功能权限的申请页面

同时申请功能权限和数据权限

的申请页面

11.3.2.2.3 如何实现权限申请一站式服务？

权限中心通过与集团已有的流程平台 K2 进行对接，实现权限申请与流程审批无缝对接，流程审批通过后，自动将权限推送至业务系统，无须运维人员干预。



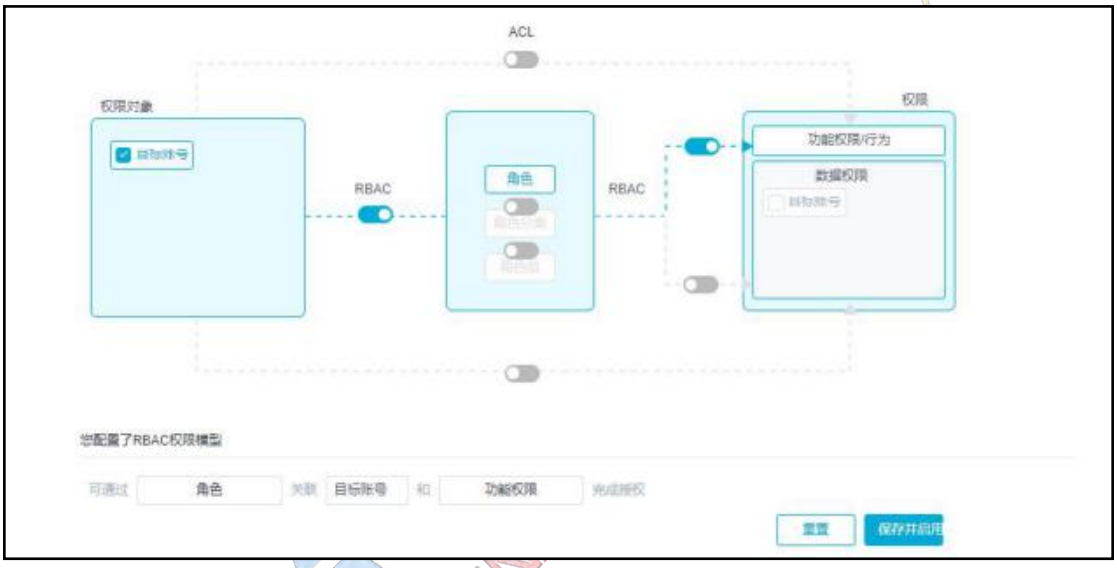
跳转至 K2 的申请页面

11.3.2.3 产品实例应用

- **首个接入中台的试点系统：**产品全生命周期管理平台（DPLM）
  - 产品特点：

  典型的 RBAC 权限模型；

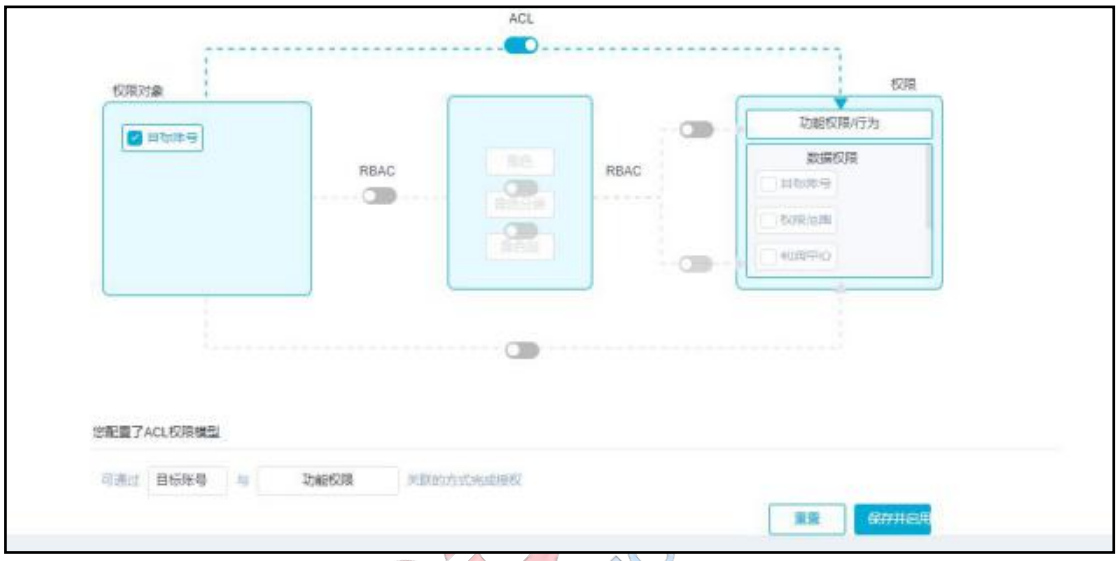
  - 业务需求：授权需求多，用户权限申请需求多，用户权限变更频繁
  - 配置权限模型：



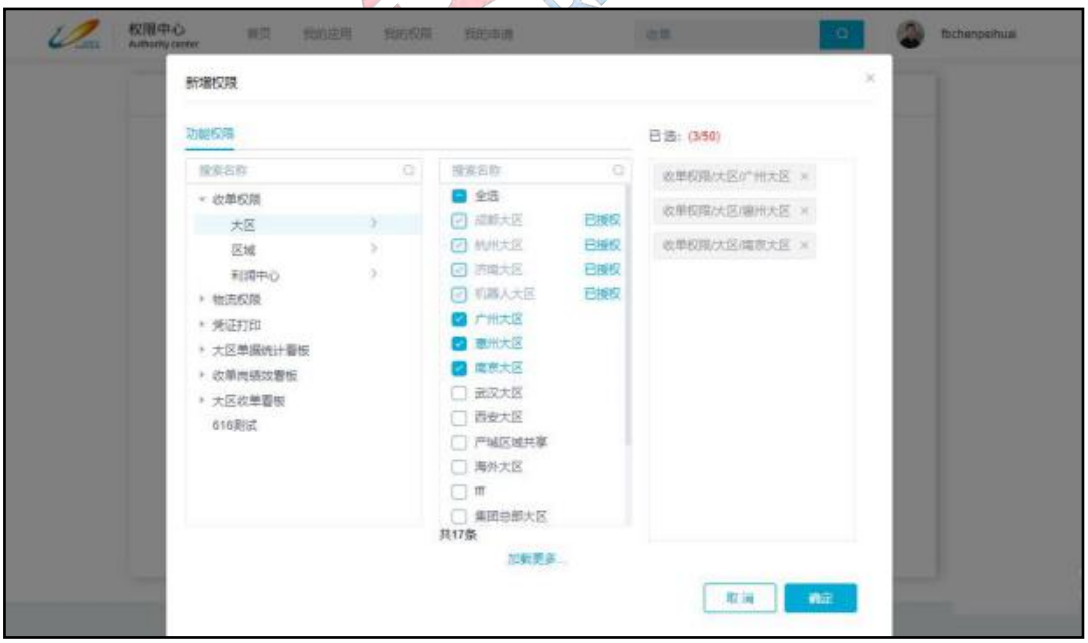
  - 用户权限申请：

- **首个财务类试点系统：**财务收单管理系统
  - 产品特点：

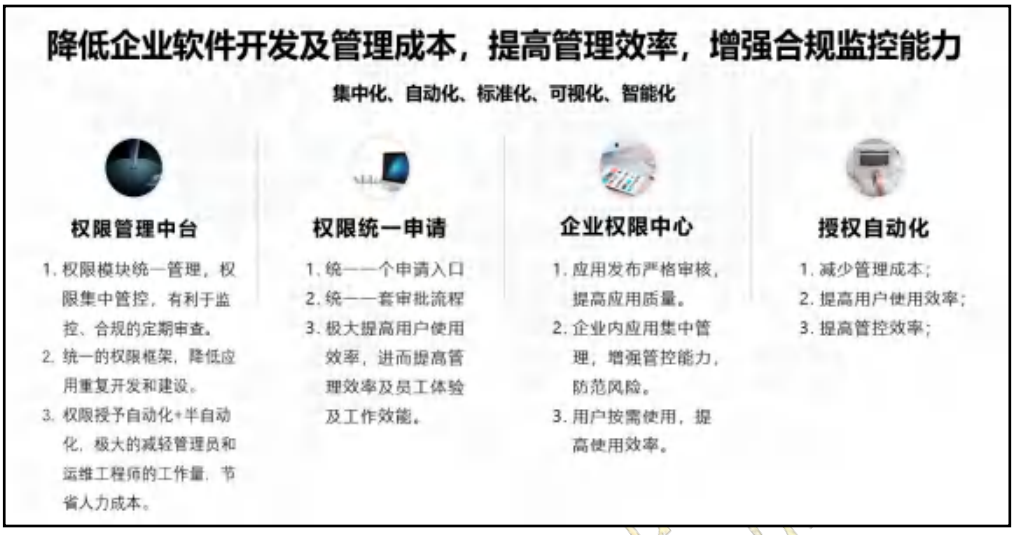
    需要申请功能权限与数据权限；
  - 业务需求：现状无实现线上申请，造成申请邮件多，运维量大，误操作多
  - 配置权限模型：



  - 用户权限申请：



11.3.2.4 项目成果及价值



11.3.2.5 总结

中台不是一个产品，而是一个方法论，其关键是“核心能力的复用和核心资源的共享”，企业可结合自身实际情况进行产品本地化，最终能实现提升企业效率，降低企业成本，即是中台价值最好的体现。

12 总结

本白皮书对 IAM 的核心概念和内容边界进行了较为全面的说明，从业务、技术、安全、政策等多个维度阐述了 IAM 的行业背景和发展情况，描述了 IAM 在一个信息化企业或组织中的定位和重要性。随着当前信息化的快速发展和深度改革，为了能够进一步提升企业客户体验和内部管理效率，应对更为复杂的安全挑战，IAM 体系的建设正日益变得重要，需要企业和组织进行持续性的规划和投入。本白皮书从 IAM 最核心的几大内容进行全面的分析，覆盖了身份管理、登录认证、访问控制、权限管理、审计风控等内容。

身份是 IAM 中的核心主体，账号管理、认证与访问控制、权限管理、审计风控的场景、方案和过程都将围绕身份展开，身份管理章节详细阐述了身份管理的对象及其属性，随着信息化涵盖范围逐步扩大，身份管理的范围也从传统的企业内部人员延伸到供应商、合作伙伴、客户，甚至从“人”的身份更进一步到“物”的身份管理。该章节还

详细阐述了身份管理过程中应当关注的内容，如账号的类别、身份数据的存储、回收与供给以及每个身份的全生命周期闭环流程等，在 IAM 实施过程中可提供参考和指导作用。

身份认证是各项信息化活动过程中业务交互的前置条件和重要过程，在登录认证和访问控制章节中，列举了多种常见的认证方式，包括传统的密码、口令认证，也包含了近几年逐渐普及的各类生物认证和社交认证，并针对这些认证方式进行了具体介绍，包括这些认证方式的特点、应用场景及其优缺点，可作为选用的参考。对于集中式认证体系，介绍了应用广泛的各类认证协议，在不同信息化平台、不同网络环境、不同终端类型中可以采用的常见标准协议，旨在使认证、登录和访问控制过程更高效、用户体验更好、更灵活和更安全。

用户在完成身份认证之后即开始接入相应的信息化资源，开展具体的业务操作，在实际操作过程中，根据用户的身份和分工不同，应当拥有不同的资源访问和操作权限。权限管理章节描述了 IAM 在统一身份和统一认证的基础上进一步把信息化系统内的各项权限包括功能权限和数据权限纳入了统一管理。该章节详细介绍了多种常见的权限模型及其应用场景，IAM 试图在不同平台、不同资源类型和不同权限管理要求的信息化系统中构建一套合理合规的统一权限管理体系，旨在使各信息化系统的权限管理从分散到集中、低效到高效、混乱到可视可控、不合规到合规、僵化到智能化的方向进行转变。

为了使企业和组织的信息化资产得到更安全的保护，审计和风控相当重要。审计与风控章节详细介绍了在 IAM 体系下审计和风控的理念和方式方法，旨在从身份角度为企业和组织在信息化服务的过程中提供事前预警、事中控制和事后追溯的能力。

此外，IAM 在不断完善传统能力的同时全面发展了 CIAM、IDaaS、DID、零信任等新形态，本白皮书在这几方面也做了较为详细的介绍，在当前快速发展的信息化、数字化浪潮中，IAM 也在积极应对更广泛的场景和更严峻的挑战。

本白皮书最后从 IAM 实践角度提供了一些思路和案例，企业或组织在 IAM 具体实施过程中可以进行参考和比对，形成符合自身特点的最佳实践。

IAM 所涉及的技术和框架体系，从静态走向动态，从单一服务形态走向多生态体系，并且逐渐成为信息化建设的基础安全平台，成为零信任核心组件。未来 IAM 还将随着业务需要、技术变更等有着更多的变化与发展。CSA 也将持续关注，并对 IAM 白皮书进行阶段性更新！在此，感谢小组所有成员的贡献和付出!

邮箱：info@c-csa.cn

官网：https：//c-csa.cn