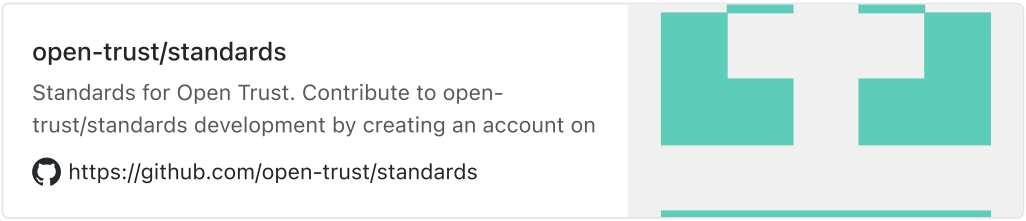
Open Trust 可信开放标准

最新版本在 Github 推进：



初期文稿

背景

云计算、大数据、移动互联网、物联网等信息技术正在以加速的态势推进社会的数字化转型，为各行各业带来了创新的生产力，也带来了极大的复杂性。

集成、打通、安全、开放成为企业信息系统扩展能力边界、开拓市场的最大挑战。把自己的 API 能力开放出去，把别人的 API 能力集成进来，是企业 IT 服务最大的刚需。

Open Trust 定义

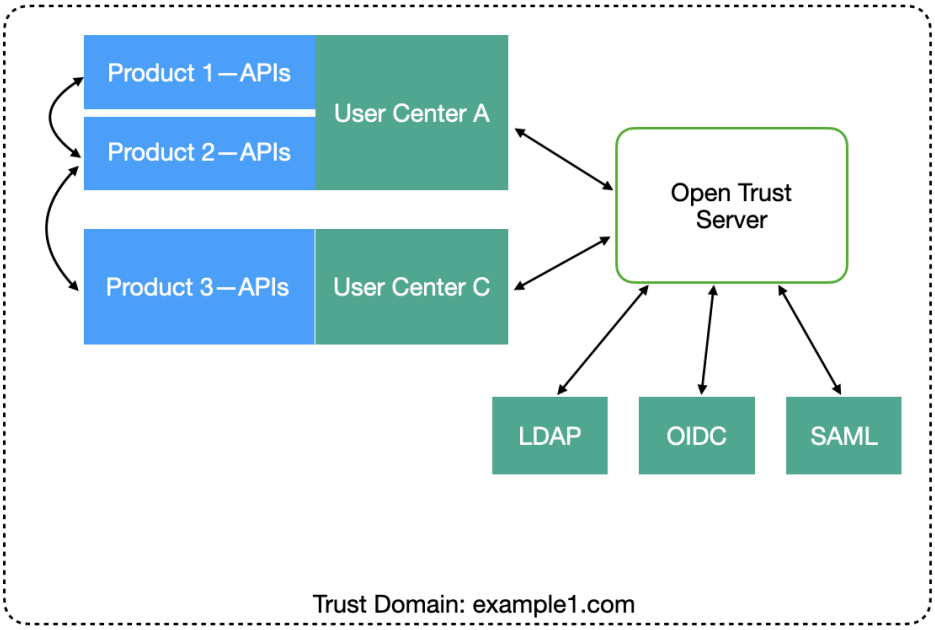
Open Trust 致力于为云原生软件提供一种安全、开放、标准的接口能力，让云原生软件彼此之间的连接打通变得简单可行，让“用 API 连接世界万物”成为可能。

与 Zero Trust 零信任架构不同，Zero Trust 的目标是让企业的网络资源访问变得开放、安全，Open Trust 的目标是让整个世界的网络资源访问变得开放、安全、标准。Open Trust 是云原生生态的基础设施，是数字经济时代的基本要求。

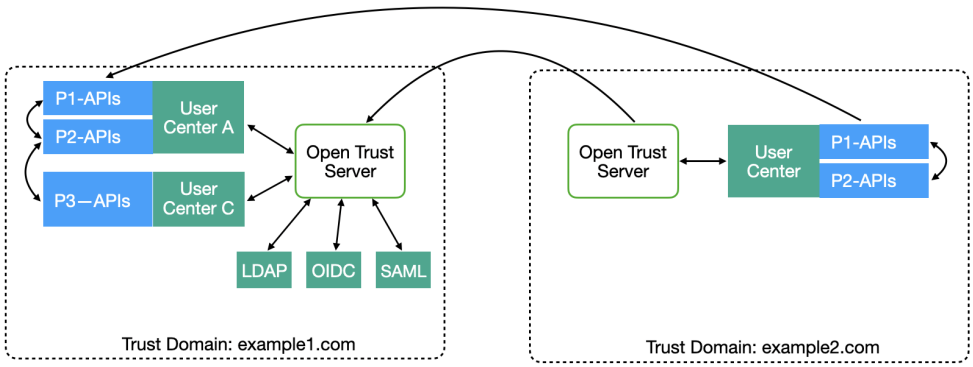
Open Trust 的核心能力包括：

1. 为信任域 Trust Domain 内的访问主体（包括人 User，设备 Robot，应用 Application，服务 Service，系统 System 等）提供统一的数字身份 ID 和身份签发、验证机制；
2. 不同信任域可以通过简单的联合绑定机制，以可信的身份跨信任域访问 API 资源；
3. 为 API 资源服务方提供标准、简洁、灵活的访问权限控制机制，确保 API 资

源能被安全的开放给目标访问主体使用。



> 信任域内，各种用户账号系统通过 Open Trust 打通，各种业务 API 基于 Open Trust 信任机制进行调用。



不同的信任域，通过联合绑定机制，让业务 API进行跨信任域的调用

Open Trust 架构

Open Trust 包含 Open Identity、Open Authentication、Open Access Control 三个核心组件。

Open Identity 身份标准

身份是信任的基石，任何开放网络的访问都必须先鉴定访问主体的数字身份，访问主体可以是人、设备、应用、服务、系统等。访问客体也有数字身份，可以是人、组织、事物、应用、接口、数据、计算能力等，我们称之为资源。资源被访问时必须先验证访问主体是否有相关权限。

Open Identity 定义了一套联盟机制的统一数字身份标准，不需要侵入信任域已有

的业务系统身份系统。Open Identity 作为 Sidecar 与业务身份系统打通，不同信任域则通过 Open Identity 的标准接口互通。当然，对于新业务系统，也可以直接使用 Open Identity 的数字身份。

Open Authentication 身份鉴定标准

Open Authentication 定义了一套基于 PKI 公钥体系的数字身份分发、鉴定标准，并提供相关 SDK，支持信任域内和跨信任域的网络访问身份鉴定。Open Authentication 是访问主体侧的服务能力。

开发者使用相关 SDK 即可快速开发出受保护的应用、服务 API，不再需要自己设计加密、签名验证机制；也能轻松调用基于 Open Authentication 的开放 API，不再需要面向不同系统实现不同的访问签名机制。

Open Access Control 资源访问控制标准

IAM（身份和访问管理）服务模块可以分为三类：身份、认证、授权。但现有 IAM 能力主要集中在前两个方面，而授权通常由开发人员和应用程序所有者负责，因为它离业务太近，权限需求太复杂。然而，资源访问控制却是安全的核心。

Open Access Control 定义了一套简洁但能满足复杂业务需求的资源访问控制系统，它是资源（访问客体）侧的服务能力。

Open Access Control 可以分为两种，一种是面向用户的（人或设备作为访问主体），控制用户访问各种系统资源的权限；另一种是面向系统的（应用或服务作为访问主体），控制系统访问其它系统资源的权限。

参考文章

1. 奇安信《零信任架构及解决方案》
2. 谷歌 BeyondCorp 系列论文合集
3. GB/T 35273—2020：信息安全技术 个人信息安全规范
4. https://cloud.google.com/beyondcorp/
5. https://cloud.google.com/identity
6. https://cloud.google.com/iap
7. https://cloud.google.com/iam
8. https://aws.amazon.com/identity/
9. https://aws.amazon.com/iam/
10. https://aws.amazon.com/cognito/
11. https://aws.amazon.com/ram/
12. https://www.microsoft.com/zh-cn/security/business/identity

13. https://www.microsoft.com/zh-cn/security/business/zero-trust
14. https://www.aliyun.com/product/ram
15. https://www.aliyun.com/product/idaas
16. https://www.plainid.com/
17. https://www.sailpoint.com/
18. https://www.openpolicyagent.org/

规范协议

1. RFC7515: JSON Web Signature (JWS)
2. RFC7516: JSON Web Encryption (JWE)
3. RFC7517: JSON Web Key (JWK)
4. RFC7638: JSON Web Key (JWK) Thumbprint
5. RFC7518: JSON Web Algorithms (JWA)
6. RFC7519: JSON Web Token (JWT)
7. RFC7642: System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements
8. RFC7643: System for Cross-domain Identity Management: Core Schema
9. RFC7644: System for Cross-domain Identity Management: Protocol
10. NIST Special Publication 800-207: Zero Trust Architecture
11. NIST Special Publication 800-63-3: Digital Identity Guidelines
12. NIST Special Publication 800-57: Recommendation for Key Management
13. NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information
14. NIST Special Publication 1800-3: Attribute Based Access Control
15. https://www.w3.org/TR/did-core/
16. https://www.w3.org/TR/vc-data-model/
17. https://www.w3.org/TR/json-ld11/
18. https://www.w3.org/TR/vc-data-model/
19. https://spiffe.io/
20. https://identity.foundation/