arXiv:2601.02254v1 [cs.CR] 5 Jan 2026

Vouchsafe：面向离线身份与信任的零基础设施能力图模型

Jay Kuri
Ionzero Inc.
jayk@ionzero.com

2025年12月22日

摘要

现代身份与信任系统往往会在最需要它们的环境中失效：灾区、断连或受损网络，以及审查或基础设施干扰等对抗条件下。这些系统依赖正常运行的网络来访问在线权威机构、解析器、目录和撤销服务，因此一旦通信不可用或不受信任，信任便无法得到验证。本文展示了无需此类基础设施即可实现安全身份与信任。我们提出零基础设施能力图（ZI-CG），该模型表明，身份、委托和撤销可以表示为自包含的签名声明，其有效性完全通过本地确定性评估来确定。我们进一步介绍 Vouchsafe，这是一个完整的可运行模型实例，采用包括 Ed25519、SHA-256 和结构化 JSON Web 令牌在内的广泛部署的基础原语构建，无需新的密码学技术或在线服务。结果表明，如今仅使用评估时提供的密码学数据，即可构建一种实用且可离线验证的信任基础层。

1 引言

1.1 研究动机

身份与信任是分布式系统中每一项安全决策的基础。无论是接受消息、授予访问权限，还是委派权限，系统都必须可靠地确定**参与者是谁**，以及**其是否获授权执行特定操作**。如今，这些判断几乎普遍依赖外部基础设施：证书颁发机构、DNS、身份提供商、目录服务、DID 解析器、撤销端点，以及其他在线事实来源。在这一范式中，身份并非自包含的；它是一项必须在别处解析的引用。

然而，安全身份与信任最为重要的环境——现场行动、灾害响应、自组对等网络、间歇性连接环境以及对抗条件——恰恰是无法假定基础设施可用的环境。网络可能离线、过载、分区、泄露，或遭到蓄意阻断。在这些情况下，身份无法查询，信任信息也无法获取，导致传统系统无法运行。

1.2 核心问题：基础设施即攻击面

除了脆弱性之外，这些依赖还带来了更深层的结构性漏洞：**身份与信任供应链中的每一项基础设施本身都是攻击面**。如果验证者必须查询的任何组件都可能遭到拦截、阻断、伪造、投毒、胁迫或其他干扰，那么身份与信任评估的正确性就会变得不确定。证书颁发机构历史上的安全失陷、撤销基础设施的故障、密钥服务器投毒、解析器劫持以及普遍存在的审查都表明，验证信任所需的基础设施往往是信任模型中最薄弱的环节。

因此，问题不仅关乎可用性，也关乎**认识论**：身份声明是否正确，取决于支持性基础设施是否正确且可访问。只要验证依赖外部解析，在发生服务中断、错误配置或对抗性干扰时，就无法保证身份与信任。

1.3 关键洞见：信任应仅凭数据即可验证

这些局限性促使我们采用一种不同的方法：**身份与信任应能直接根据所提供的数据进行验证**，而不依赖注册表、解析器、目录、在线状态信息或任何形式的同步全局状态等基础设施。要让身份与信任在网络分区、组织边界和对抗环境中保持可靠，就必须：

- **自主发起**- 无须任何权限方授予或注册身份
- **自包含**- 验证无须在线查询；并且
- **可在本地判定**- 任何一方都必须能够仅凭所提供的数据评估信任。

这一观察引出了**零基础设施能力图（ZI-CG）**的概念：这是一类信任模型，其中身份是自验证的，所有信任关系——包括委托、证明、撤销和身份终止——都表示为带签名且内容寻址的声明，并构成确定性的有向无环图。信任评估由此成为对该图进行的纯离线计算，而非由基础设施介导的过程。

与传统身份系统的一个核心区别在于，ZI-CG 将签名声明视为信任的基本单位。在具体系统中，这些签名声明以令牌的形式出现，无须外部基础设施即可验证。传统身份系统直接向主体赋予信任，而 ZI-CG 系统将每个令牌视为具体且可验证的断言或委托行为。因此，信任是根据身份所作出的声明来评估的，而不是孤立地根据身份本身来评估。

重要的是，这并未消除身份；相反，ZI-CG 将身份定义为一种密码学自验证参与者，能够对自身和他人作出经认证的声明，其信任来源于对这些声明的明确背书，而非账户或由基础设施维护的记录。

在本研究中，我们将身份与信任视为原语，必须确保它们在最受限的运行条件下仍然正确。验证者可能无法访问网络，无法联系可信基础设施，无法获取撤销状态，也无法确信任何解析器、注册表或同步机制可用或可信。因此，信任决策必须仅使用本地可用的数据进行计算。

ZI-CG 模型表明，身份、委托与撤销这一通常被视为依赖在线基础设施的综合问题，可以采用完全确定性的离线形式化。在此框架下，所有信任决策都可归结为对由签名声明构成的有限内容寻址图进行密码学验证和评估，无需依赖外部解析、可变全局状态或第三方权威机构。这表明，身份与信任的正确性可以直接且完全地从所提供的数据中推导得出。

在本研究中，我们将这些约束作为构建通用可离线验证的身份与信任模型的基础。我们对 ZI-CG 模型进行了形式化定义，并将 **Vouchsafe** 作为该模型的首个完整实现，证明了只使用标准且广泛部署的密码学原语，就能构建完全自包含的信任基础层。

1.4 贡献

本文作出了两项相辅相成的贡献：

1. **零基础设施能力图（ZI-CG）模型**。
   我们对一种信任与授权框架进行了形式化定义，其中身份、证明、委托、撤销和身份终止均表示为自包含且以哈希值链接的密码学声明。当所有信任相关状态都编码在签名令牌中，且信任评估是对有限令牌集执行的确定性本地计算、不依赖在线基础设施时，系统即符合 ZI-CG 规范。
2. **Vouchsafe 中的完整运行实例**。T
   o the best of our knowledge, Vouchsafe is the 首个完整实现 ZI-CG 模型的系统。Vouchsafe 提供自验证身份、范围限定证明与委托令牌、显式撤销与身份销毁语义，以及完全基于标准密码学原语的确定性离线评估程序。

为支持这些贡献，本文：

- **定义了一种自验证身份构造**，无需查找服务、解析器基础设施或预先存在的目录即可验证身份。
- **提出一种自认证令牌模型，**其中发行者身份、声明真实性和内容完整性均可仅通过令牌内容联合验证。

- **形式化一种基于能力的信任图，**该图由证明和委托声明构成，并通过数据承诺而非可变状态来执行明确的撤销和身份终止语义。
- **通过构造实现无环委托**，基于内容寻址引用，从声明中推导出严格偏序，从而无需外部检测或全局协调即可消除委托环。

- **规定确定性的授权语义**，基于单调范围收缩和最低需求能力满足；权限沿单条委托路径进行评估，绝不会通过路径组合而扩展。

- **提供完全离线的评估过程**，仅使用本地输入执行状态解析、能力图构建和授权决策，不受搜索策略或评估顺序影响。

- **分析模型及其实现的安全属性**，包括抵御替换攻击、图操纵、重放和基础设施攻陷的能力。

这些贡献共同表明，完全自包含的零基础设施信任基底不仅在概念上连贯，而且在实践中也可实现。下一节将本方法与已有工作进行对比，重点阐述其在身份解析、基础设施依赖和信任组合方面的假设差异。

2 背景与相关工作

去中心化信任、身份绑定和分布式授权存在于各种系统中，而这些系统对基础设施、身份解析和委托语义有着不同的假设。零基础设施能力图（ZI-CG）模型建立在多个研究方向已有思想的基础上，包括 SPKI、信任网系统、以密钥为中心的身份表示以及基于能力的授权。本节概述构成 ZI-CG 所处领域的主要概念框架。

2.1 身份与信任模型

公钥基础设施（PKI）

传统 PKI 系统使用由分层证书颁发机构签发的 X.509证书，将身份绑定到公钥。验证依赖于对证书链的评估，以及用于评估撤销状态的基础设施，例如 RFC5280 中描述的证书撤销列表（CRL）和在线证书状态协议（OCSP）服务。[1] PKI 提供全球命名和信任层级，身份则在外部定义。PKI 展示了机构信任锚如何构建身份绑定并实现全球互操作性。

PGP 与信任网

PGP 系统通过用户间签名建立信任，形成去中心化的“信任网”，其中人们互相为对方的密钥签名。身份表示通常将密钥与电子邮件地址、姓名等可读标识符结合起来，而密钥发现和撤销通常依赖公钥服务器。 [2] PGP 展示了如何通过社交方式构建去中心化信任关系，而无需集中式权威机构，但其语义可能因不同实现和用户实践而异。

去中心化标识符（DID）

去中心化标识符（DID）提供全局唯一的标识符，其相关元数据通过解析过程获取。解析会生成一份 DID 文档，其中指定公钥、元数据、服务端点和密钥轮换程序。DID 文档通过特定于方法的解析器获取，而这些解析器可能依赖区块链或其他注册表。DID 展示了一种将标识符与密码学密钥解耦的方案，但其解释需要外部基础设施。 [3]

基于账本的身份模型

区块链和分布式账本系统通过维护由全网共识机制管理、仅追加且由共识维护的日志，实现身份更新或凭证声明的防篡改发布和全局排序。 [4]这些系统依赖共识基础设施来建立可供多方引用的共享状态。它们展示了如何通过全球网络中的协调，实现信任锚定和凭证可见性的去中心化。

2.2 委托与授权框架

SPKI/SDSI

SPKI 和 SDSI 引入了以密钥为中心的命名、明确的授权证书，以及具有本地意义的身份作用域。SDSI 强调本地命名空间语义并关联本地名称，而 SPKI 则定义了证书格式和操作机制，以便直接通过密钥来表达授权和委托。 [5]这些系统探索了基于证书的信任图、非层级命名，以及去中心化环境中的撤销和新鲜度挑战。

Macaroons

Macaroons 通过链式限制条件实现授权；随着令牌被削弱，这些限制条件会逐步缩小允许的操作范围。它们采用嵌套式 HMAC 构造，旨在高效部署于 Web 和云服务中。 [6] 限制条件验证可能依赖共享密钥或在线检查。
Macaroons 展示了如何通过在持有者令牌中增量嵌入约束来细化能力。

Biscuit 授权令牌

Biscuit 令牌嵌入一系列签名区块，支持通过离线验证实现灵活的委托授权。Biscuit 将公钥签名与一种小型逻辑语言相结合，以表示直接包含在令牌中的事实、规则和检查。[7] 这种设计展示了如何将令牌携带的逻辑和链式签名编码为授权属性，使验证者能够在本地进行评估。

面向能力的组合

Miller 的 健壮组合 描述了一种基于能力的对象模型，其中权限通过持有引用来传递，而系统交互则通过控制引用的传播与使用受到限制。该研究将访问控制与并发控制视为分布式系统中管理对象间因果关系的相关问题。 [8]

该模型采用异步消息传递、承诺引用以及对部分故障的显式处理来构建，示例则取自 E 编程语言和分布式对象系统。

2.3 概念定位总结

纵观这些系统，可以看到若干反复出现的理念：身份可以由机构分配（PKI）、由社会建构（PGP）、通过解析器管理（去中心化标识符），或锚定于账本；授权可以通过证书（SPKI/SDSI）、链式权限衰减（Macaroons）、携带逻辑的令牌（Biscuit）或能力持有（能力系统）来表示。ZI-CG 模型采用了不同于上述方案的假设，本文后文将对此进行形式化讨论。本节旨在确立 ZI-CG 所依据的概念图景与术语。

3 零基础设施能力图（通用模型）

3.1 模型概述

零基础设施能力图（ZI-CG）模型为身份与信任提供了一种框架，即使完全不依赖在线基础设施，也能保持正确且可验证。传统系统依赖解析器、目录、撤销服务或可信权威机构。相比之下，ZI-CG 系统将所有信任相关信息表示为一组有限的、自包含的经密码学签名的声明。验证者仅使用本地令牌集即可解析身份、委托和撤销，无需外部查询或共享全局状态。
ZI-CG 背后的核心洞见是概念分离：信任评估不得依赖服务或网络的可用性。许多传统系统将这些问题混为一谈，要求信任评估器从在线服务获取信息。ZI-CG 系统通过确保身份绑定、能力传播以及撤销或销毁等状态变更都完整编码在签名声明本身中，避免了这种纠缠。信任由此成为计算问题，而非通信问题。

因此，ZI-CG 系统有两个主要组件：

1. 一组不可变的自验证令牌，使用签名数据和内容寻址数据对身份与信任关系进行编码。

2. 一种确定性评估过程，用于解释这些令牌，以完全离线的方式确定身份真实性、委托能力和撤销状态。

该模型不规定具体的令牌格式、身份字符串或消息编码，而是定义任何零基础设施信任系统都必须满足的结构约束，以确保在断连或对抗环境中运行的验证者始终能够得出一致的信任判断。

这些要素共同描述了 ZI-CG 系统的概念结构。接下来的章节将形式化该结构所引出的要求，并定义令牌语义和评估规则，使模型能够在离线环境中确定性地运行。

3.2 基本目标

ZI-CG 模型由两个基础目标指引，这些目标塑造了其结构与约束。 .

G目标 1：为身份与信任提供可完全离线运行的安全密码学基础层

ZI-CG 系统必须使验证者仅凭本地提供的一组签名令牌，就能对身份进行身份验证、验证声明、确定受托权限并检测撤销。不能假设具备网络可达性或支持性基础设施。在网络分区、受限环境和对抗条件下，系统都必须保持正确。

目标 2：将信任评估与数据可用性彻底分离

现有身份系统通常将信任决策与数据检索绑定在一起。例如，解析身份、检查密钥、获取撤销状态或查询注册表，都需要活跃的基础设施。ZI-CG 将这些关注点分离开来。信任评估所需的全部信息都嵌入令牌本身，因此数据分发可以由任何合适的机制独立处理。这种机制可以是同步、异步、集中式或点对点的。当相关令牌可供验证者使用时，这些选择都不会影响信任计算的正确性。

这些目标促成了该模型的设计约束。以下各节将形式化一个系统必须满足的要求，以便其符合 ZI-CG 系统的资格，并描述由这些约束所衍生的令牌结构和评估语义。

3.3 设计约束与要求

要求 1：自解析身份

ZI-CG 系统要求采用一种身份格式，仅使用标识符本身及其所指向的公钥即可完成验证。确定某个身份是否正确绑定到某个密钥时，不得要求查询、解析器、元数据文档或外部权威机构的参与。在离线或对抗环境中运行的任何验证者都必须能够执行身份验证。这要求标识符编码足够的结构，使验证者仅通过计算即可确认其与密钥的绑定。如果没有自解析身份，身份验证就需要在线查询或外部基础设施，从而违反零基础设施约束。

要求 2：通过省略证明进行本地状态解析

所有与信任评估相关的状态变更（例如撤销或身份终止）都必须以签名令牌的形式表示在本地令牌集中。验证者通过省略已失效的令牌来确定有效状态，而不是查询外部列表或状态服务。由于 ZI-CG 验证者无法依赖网络连接或共享可变状态，所有撤销信息都必须能够仅使用本地可用的签名数据进行表达和验证。如果没有本地、数据驱动的状态解析，撤销就需要从外部权威机构获取信息，这将违反零基础设施约束。

要求 3：受限委托

权限委托必须始终削弱或保持能力不变，绝不能扩大能力。每个委托令牌都必须指定其认可的作用域，任何委托链的有效能力都必须是该链上各作用域的交集。在 ZI-CG 系统中，委托不能依赖策略引擎、外部授权服务或在线上下文。受托权限必须直接编码并限定在签名声明本身中，以保证其可预测且安全地传递。若没有受限委托，能力可能以需要外部策略或基础设施加以约束的方式扩大，这将违反零基础设施约束。

要求4：结构确定性与离线评估

信任评估必须是所提供令牌集和验证者所选信任根的确定性函数。向两个验证者提供相同输入时，无论环境或时机如何，它们都必须得出相同的信任结果。确定性可确保评估不依赖网络状态、共享全局状态或其他经由外部协调的因素。这一特性使断网验证者能够仅凭其持有的签名声明得出一致结论。若缺乏结构确定性，信任评估就需要外部协调来解决不一致，而这将违反零基础设施约束。
这些要求构成任何 ZI-CG 信任系统所需的最低结构条件。具体系统可以施加额外约束，但该模型至少要求满足这四项条件。

3.4 自验证信任声明

ZI-CG 系统中的所有信任断言均以自验证声明的形式表示。每条声明都编码为一个签名令牌，其中包含验证者确认其来源和完整性所需的全部信息。令牌包含签发者的公钥，且签发者标识符通过确定性的抗碰撞函数以密码学方式与该密钥绑定。令牌使用相应的私钥签名。因此，验证者无需进行任何外部查询，即可确定该声明只能由持有该私钥的一方生成，且其内容未被篡改。

3.5 非正式模型描述

给定一组自验证信任声明，ZI-CG 验证者仅根据其可用的签名令牌，通过推理来评估授权。整个过程不会查询任何外部服务、权威注册表或在线解析机制。因此，提交给验证者的令牌集定义了本次评估所涉及的全部信任相关信息。任何可能影响信任决策的签名声明都必须包含在该令牌集中。

该模型定义了四类令牌。**证明**记录其签发者所主张的事实陈述。**担保**通过为另一个令牌背书来表达委托信任，并可选择限制该背书的范围。**撤销**通过使被引用令牌失效，撤回先前的特定声明。**销毁**令牌表示签发者的身份不再有效，并且从此以后不应接受其任何声明。这四种令牌类型代表了基本模型中身份、委托和撤销所需的最小类别，但该框架并不限制系统为其他 purpose 定义额外的令牌类型。核心要求是，任何对信任评估至关重要的声明，都必须能够表示为验证者可获取的自验证令牌。

ZI-CG 模型不会直接将信任赋予身份。相反，信任附加于签发者所作出的具体签名声明。因此，担保令牌并不意味着通常意义上信任 Alice。它意味着 Alice 已经发布了一项具体且可验证的声明，针对特定 purpose 表示其对另一项声明的信任。这种从以身份为中心的信任转向以声明为中心的信任，是 ZI-CG 系统中能力传播和撤销运作方式的核心。

验证者通过构建反映这些关系的图来评估令牌集。首先验证并检查每个令牌集，以收集其中的任何撤销声明或销毁声明。随后，验证者对每个令牌执行遗漏证明检查。仅当撤销集不包含针对该令牌的撤销，且销毁集不包含针对其签发者的销毁时，该令牌才会作为节点加入图中。这种图结构自然源自令牌中的内容寻址引用，因为这些引用定义了各项声明之间的依赖和背书关系。此过程确保图中仅包含其有效性未被令牌集现有信息所否定的声明。由此形成的有向图代表了验证者统一的信任视图，因为节点被纳入图中，即表明不存在与该节点相关的撤销或销毁。在建立有效令牌图后，验证者接下来会确定其中编码的背书关系支持哪些能力。

构建此图后，能力便沿着担保令牌链传播。任意链所关联的有效能力由该路径上各个作用域的交集决定。此传播完全在图内进行，并且仅依赖状态解析后保留下来的签名令牌。结果是对信任进行确定性评估，且仅取决于令牌集的内容。无论在何处或何时进行评估，相同的令牌集始终会产生相同的信任结果。

ZI-CG 系统天然以参与者为中心。在大多数部署中，寻求行使某项能力的一方会出示证明其有权行使该能力的签名令牌。验证者也可能维护自行获取的令牌，例如反映组织策略或已知泄露情况的撤销令牌或销毁记录。在评估请求时，验证者会考虑参与者提供的令牌与其本地持有的令牌所构成的集合。评估过程对待这个合并后的集合，与对待任何其他令牌集完全相同；其正确性仅取决于验证者可获取的签名声明，而不取决于这些声明的获取方式。

下一节将给出形式语义，为上述令牌结构和评估规则赋予精确定义。

4 形式化模型

4.1 身份

在 ZI-CG 系统中，身份是一个字符串，只需使用该身份本身及与之关联的公钥即可进行验证。令 (I) 表示身份字符串的集合，(PK) 表示公钥的集合。令 ($\mathcal{M}$) 表示可选描述性组件或人类可读组件的空间，令 ($\mathcal{H}$) 表示抗碰撞摘要的空间。

ZI-CG 系统定义了两个确定性函数

$$\mathsf{parse} : I \to \mathcal{M} \times \mathcal{H} \tag{1}$$

$$\mathsf{id} : PK \times \mathcal{M} \to I \tag{2}$$

以及一个抗碰撞函数

$$h : PK \to \mathcal{H}. \tag{3}$$

直观而言，(id) 根据公钥和可选元数据构造身份字符串，而 (parse) 则从该字符串中恢复元数据和存储的摘要。

系统必须满足以下一致性性质。对于所有 $(pk \in PK) and (m \in \mathcal{M})$，令

$$i = \mathsf{id}(pk, m) \qquad \mathsf{parse}(i) = (m', d). \tag{4}$$

那么必须满足 $m' = m$并且

$$d = h(pk). \tag{5}$$

通过计算 $\mathsf{parse}(i) = (m, d)$，重新计算$d' = h(pk)$，并且仅当 $d' = d$时接受该绑定，从而验证身份 i 与公钥 pk 之间的绑定。

身份可以在 m中包含任意描述性内容，但所有此类内容都必须以保留这一自验证性质的方式纳入身份字符串。在该模型中，主体由其完整身份字符串标识，其中包含任何描述性元数据和由密钥派生的摘要；当且仅当两个主体的身份字符串完全相同时，才认为它们是同一主体。**因此，相同的公钥与不同的描述性内容结合，会产生不同的身份字符串，从而在模型中形成不同的主体。**
由于 h 具有抗碰撞性，且 id 是确定性的，因此在计算上不可行的是让两个不同的公钥在身份中产生相同的摘要部分；因此，若不破解底层哈希函数或编码，就无法构造两个身份字符串相同的不同主体。

这种自解析构造 确保无需外部查询即可进行身份验证，并且令牌中对身份的任何引用都可以仅凭令牌本身包含的信息正确解读，而这些信息对验证者是可用的。

4.2 令牌

ZI-CG 系统将所有信任相关信息编码为自验证、内容寻址的令牌，这些令牌可独立验证。

这一构造的一个关键属性是，每个令牌都构成一个自认证声明。与依赖外部机制来确立签名密钥有效性的传统签名对象不同，ZI-CG 令牌包含验证声明真实性和签发者加密身份所需的全部信息。签发者标识符、验证密钥材料和签名均位于令牌主体之中，因此验证者仅凭令牌本身即可验证声明。

此设计刻意消除了身份验证与声明验证之间的区别。在典型系统中，验证签名只能证明某个密钥对数据进行了签名，而要确定该密钥是否代表某个特定

身份，则需要通过证书、目录或解析器进行外部解析。相比之下，aZI-CG 令牌的结构使得成功完成签名验证的同时，也能确立签发者标识符与签名密钥之间的绑定。因此，令牌真实性仅取决于数据本身。

令牌分为三个层：签名层、通用主体层和载荷层。

4.2.1 签名层

令 T 表示所有令牌的集合。每个令牌 $t \in T$ 的形式为

$$t = \big(\mathsf{body}(t), \mathsf{sig}(t)\big) \tag{6}$$

其中，body(t) 是表示令牌语义内容的结构化对象，而 sig(t) 是数字签名。

Let

$$\mathsf{serialize}(\mathsf{body}(t)) \in \{0,1\}^* \tag{7}$$

是令牌主体的规范编码。使用发行者私钥对该编码进行签名。

为了将令牌的内容及其签发者唯一绑定起来，令牌的内容寻址标识符定义为

$$\mathsf{tid}(t) = H\big(\mathsf{serialize}(\mathsf{body}(t)) \,\|\, \mathsf{sig}(t)\big) \tag{8}$$

其中，H 是抗碰撞哈希函数，$\|$ 表示字节串联。值 tid(t) 充当模型中令牌 t的规范标识符。

这种构造确保对令牌主体或签名的任何更改都会产生不同的标识符。因此，令牌的含义和作者身份在密码学上绑定到一个不可变制品：令牌无法被更改、由不同身份重新签名，也无法在不更改其标识符并使所有对它的引用失效的情况下被重新解释。

4.2.2 UniversalBody 结构

令牌主体包含发行者身份字符串、发行者公钥和结构化载荷 :

$$\mathsf{body}(t) = \big(\mathsf{iss}(t), \mathsf{pk}(t), \mathsf{payload}(t)\big) \tag{9}$$

- iss(t) $\in I$ 是发行者身份字符串。
- pk(t) $\in PK$ 是签发者的公钥。
- payload(t)承载令牌的语义内容，定义如下。

iss(t)和pk(t)都包含在签名主体中。这可以防止攻击者替换身份或公钥，同时不改变令牌标识符并破坏签名。

令牌有效性包含两个组成部分：

签名有效性

$$\mathsf{sigvalid}(t) \iff \mathsf{verify\_sig}\big(\mathsf{pk}(t), \mathsf{serialize}(\mathsf{body}(t)), \mathsf{sig}(t)\big) \tag{10}$$

身份绑定有效性

使用第4.1节中的身份机制：

$$\mathsf{idvalid}(t) \iff \big(\mathsf{parse}(\mathsf{iss}(t)) = (m,d)\big) \;\wedge\; \big(d = h(\mathsf{pk}(t))\big) \tag{11}$$

令牌总体有效性

$$\mathsf{valid}(t) \iff \mathsf{sigvalid}(t) \wedge \mathsf{idvalid}(t) \tag{12}$$

验证者必须拒绝任何不满足任一条件的令牌。这些谓词确保每个被接受的令牌都经过正确签名，并且正确绑定到其声明的发行者身份。

4.2.3 载荷结构

T载荷描述了签发者所声明的内容。它具有一种由三个组成部分构成的通用结构 s:

$$\mathsf{payload}(t) = \big(\mathsf{kind}(t), \mathsf{typefields}(t), \mathsf{extra}(t)\big). \tag{13}$$

每个令牌都有一个**类型**，用于确定该令牌如何参与能力图，以及需要哪些额外字段:

$$\mathsf{kind}(t) \in \text{attest}, \text{vouch}, \text{revoke}, \text{burn}. \tag{14}$$

typefields(t) 组件包含**类型专用字段**，这些字段取决于令牌的类型。在模型层面，ZI-CG 要求具备以下最低结构:

- 如果 kind(t) = 是 attest，则令牌在 extra(t) 中仅携带断言。
$$\mathsf{typefields}(t) = \emptyset. \tag{15}$$
- 如果 kind(t) = 是 vouch，则
$$\mathsf{typefields}(t) = \big(\mathsf{ref}(t), \mathsf{scope}(t)\big) \tag{16}$$
其中，ref(t) 是被引用令牌 t' 的内容寻址标识符 tid(t')，而 scope(t) 则编码应用于该背书的衰减。
- 若 kind(t) = 为 revoke，则
$$\mathsf{typefields}(t) = \big(\mathsf{revoke\_target}(t), \mathsf{ref\_subj}(t)\big) \tag{17}$$
其中:
  – revoke_target(t) 是一个确定性选择器，可唯一标识由同一签发者签发的先前声明，– ref_subj(t) 是该先前声明引用的主体。
- 若 kind(t) = 为 burn，则
$$\mathsf{typefields}(t) = \big(\mathsf{ref\_id}(t)\big) \tag{18}$$
其中 ref_id(t) $\in I$ 必须等于 iss(t)。

后续章节将形式化说明 ref(t)、scope(t) 与 kind 如何共同作用以生成能力图和状态转换。extra(t) 组件表示任意特定于应用程序的**附加字段**或元数据。这些字段包括:

- 完全由签名覆盖,
- 包含在内容哈希 tid(t) 中，并且
- 可供应用程序解读,

但它们会被忽略 不属于 ZI-CG 核心评估语义的范畴。评估器的行为完全根据以下内容来定义 of

$$\mathsf{iss}(t),\ \mathsf{pk}(t),\ \mathsf{kind}(t),\ \mathsf{ref}(t),\ \mathsf{scope}(t),\ \mathsf{tid}(t) \tag{19}$$

以及令牌的有效性谓 了。这使系统能够扩展令牌内容，而无需改变底层的信任模式 l.

这一定义为令牌提供了一个通用的自验证基础，ZI-CG 模型的其余部分均构建于此之上。接下来的小节将利用这些结构来定义令牌集、通过遗漏证明进行状态解析，以及能力图的构建。

4.3 令牌类型语义

基于第 4.2 节所述的一般令牌结构，本节将说明定义 ZI-CG 模型的四种令牌类型的语义：证明、担保、撤销和销毁。这些语义描述了每种令牌类型如何影响状态、委托以及最终的能力评估。

令 T_{valid} 表示满足 有效(t) 的令牌集，定义见第4.2节。下文若干处会非正式地提及清理后的令牌集 T_{clean}，它由应用撤销和销毁语义后仍然保留的有效令牌构成。

第 关于4.4 给出了 T_{clean} 的形式化定义，以及构造它的遗漏证明规则。

4.3.1 证明令牌

证明令牌具有

$$\mathsf{kind}(t) = \text{attest} \qquad \mathsf{typefields}(t) = \emptyset \tag{20}$$

其载荷仅由 extra(*t*) 构成，其中编码了签发者所断言的事实声明。ZI-CG 模型不会对这些声明施加内在结构或真实性条件，而是将其视为应用层声明；评估器是否接受或拒绝这些声明，取决于其是否信任令牌本身。

形式上，证明令牌

- 不会在能力图中引入边，
- 不会改变撤销状态或销毁状态，且
- 可以成为担保令牌或撤销令牌的目标。

尽管证明令牌本身不会诱导委托边或能力传播，但其自认证结构使其即使单独使用也很有价值。证明令牌构成了一项可验证的事实陈述，其来源可以直接根据令牌内容确定，无需依赖目录、证书或外部解析。在签发者已为应用程序所知晓或被策略接受的应用程序中，此类令牌可以直接作为经认证的断言使用，而不依赖任何额外的担保或基于图的信任组合。

ZI-CG 模型将证明视为经认证声明的最小原语，在此基础上可以叠加委托、衰减和撤销等更丰富的信任语义。然而，证明令牌的正确性和可验证性并不取决于这些机制是否存在，而只取决于声明本身的密码学自认证。

证明令牌 t 仅当其存在于清理后的令牌集 T_{clean} 中，并且根据后文定义的委托语义可从信任根到达时，才会贡献其所断言的事实。核心 ZI-CG 模型不考虑额外内容(*t*)的内部结构；只要令牌已被判定为可信，应用程序能够解释这些声明即可。

4.3.2 担保令牌

担保令牌表示对另一个令牌的委托背书。它包含

$$\mathsf{kind}(t) = \text{vouch} \qquad \mathsf{typefields}(t) = \big(\mathsf{ref}(t), \mathsf{scope}(t)\big) \tag{21}$$

其中：

- ref(*t*)携带被背书令牌的令牌标识符：

$$\mathsf{ref}(t) = \mathsf{tid}(u) \tag{22}$$

  对于某个令牌 $u \in T_{\text{valid}}$，其类型(*u*)为 $\in$ {证明，担保}。
- scope(*t*)是一个**能力集合**，scope(*t*) $\subseteq S$，它限定了委托的范围。因此，担保可以一次授权多项能力，但沿路径传播时，所有能力都会受到衰减。

通俗地说，担保令牌 t 表示，签发者 iss(*t*) 接受被引用令牌 u 所表达的声明或权限，但受 scope(*t*) 所述范围的限制。应用撤销和销毁语义后仍然有效的担保令牌，会在能力图中形成有向边。这些边表示权限从担保令牌的签发者向被引用令牌的主体传播，并且该权限已被削弱。

担保令牌只能引用证明令牌或担保令牌。对于类型为撤销或销毁的令牌，ZI-CG 求值语义会忽略对它们的引用，因为此类令牌不表示可委派的权限。

如果 ref(*t*) 与任何经过状态解析后仍然有效的令牌的标识符都不匹配，该担保令牌就不会对图产生任何影响。此类担保令牌在语法上有效，但对于能力传播而言，在语义上不起作用。

4.3.3 撤销令牌

A 撤销令牌用于撤回其签发者作出的特定先前声明或背书。它具有

$$\mathsf{kind}(t) = \text{revoke} \tag{23}$$

其类型专用字段同时标识被撤回的先前声明及该先前声明的主体。在模型层面，

$$\mathsf{typefields}(t) = \big(\mathsf{revoke\_target}(t), \mathsf{ref\_subject}(t)\big). \tag{24}$$

通俗地说，撤销令牌声明：

“我，iss(t)，不再为先前由 revoke_target(t) 标识的、关于主体 ref_subject(t) 的声明背书。”

这两个字段必须同时提供，以确保撤销操作能够明确标识签发者先前的一项行为，并且无法通过替换或修改目标声明，将撤销操作转向另一个主体。

当且仅当满足以下条件时，撤销令牌 r 才会指向令牌 u：

1. u 是一项证明或担保：
$$\mathsf{kind}(u) \in \{\text{attest}, \text{vouch}\} \tag{25}$$
2. 签发者匹配：
$$\mathsf{iss}(r) = \mathsf{iss}(u) \tag{26}$$
3. 撤销目标匹配 u：
$$\mathsf{matches\_target}(r, u) \tag{27}$$
4. 主体匹配：
$$\mathsf{ref\_subject}(r) = \mathsf{ref\_subject}(u) \tag{28}$$

当值 revoke_target(r) 可在所提供的令牌集中，确定性地从 iss(r) 签发的所有令牌中唯一标识令牌 u 时，当且仅当谓词 matches_target(r, u)成立。

模型要求　对于任意给定的撤销令牌 r，最多只能有一个令牌 u 满足 matches_target(r, u)。

对于证明令牌，声明本身被视为其自身的主体。

撤销的作用是从有效状态中移除目标声明。构造清理后的令牌集 T_{clean} 时，任何存在满足上述谓词的撤销令牌 r 的声明令牌 u 都会从T_{clean}中排除。此机制不会移除这些声明引用的主体令牌；撤销仅消除签发者先前作出的证明或背书。其他各方仍可继续就同一主体签发自己的声明。

撤销令牌本身仍属于 T_{clean}（但须满足其自身的有效性以及任何适用的销毁语义），从而确保任何收到相同令牌集的评估器都能看到其效果。

为保持简单，并确保能力图仍为无环图，撤销令牌不会以其他撤销令牌或销毁令牌为目标。撤销具有单调性：添加撤销令牌只会移除撤销者签发的证明令牌和担保令牌，从而减少可用的委托路径或被接受的声明；它绝不会恢复已被移除的权限。

4.3.4 销毁令牌

销毁令牌会在模型中终止一个身份。它具有

$$\mathsf{kind}(t) = \text{burn} \qquad \mathsf{typefields}(t) = \big(\mathsf{burn}(t)\big), \tag{29}$$

其中 burn(t) 表示应视为不再有效的身份。

为确保销毁令牌只会终止其自身身份，我们要求销毁令牌所引用的身份必须是该销毁令牌本身的身份：

$$\mathsf{burn}(t) = \mathsf{iss}(t). \tag{30}$$

给定 T_{valid}，一个销毁令牌 n b 会匹配签发者与已注销身份相符的所有有效令牌。对于任何令牌 $u \in T_{\text{valid}}$，

$$\mathsf{burned\_by}(u, b) \iff \mathsf{burn}(b) = \mathsf{iss}(u). \tag{31}$$

构建清理后的令牌集 T_{clean} 时，会排除任何至少被一个销毁令牌销毁的令牌 u。销毁令牌本身仍保留在 T_{clean} 中（除非它们无效，或被更严格的策略移除），因此只要它们存在，其效力就会持续。

销毁语义比撤销更强。撤销仅适用于单个被引用声明，而销毁则适用于已注销身份曾发布的所有声明，包括证明、背书和撤销。与撤销一样，销毁的效果是单调的。添加销毁令牌只会从有效状态中移除权限，且无法通过模型中的任何其他令牌撤销这一效果。

为简化推理，并保留销毁作为身份终止的预期含义，模型假设销毁令牌不会以其他销毁令牌为目标。同一身份可以有多个销毁令牌，但这些令牌是冗余的；除单个销毁令牌的效果外，它们不会改变最终状态。

这些令牌类型语义描述了单个令牌如何影响系统最终的有效状态。下一节将形式化令牌集以及遗漏证明过程，该过程结合撤销和销毁语义来构建清理后的令牌集 T_{clean}，并以此作为能力图构建和委托评估的基础。

4.4 T_{clean} 的状态解析与构建

状态解析是指验证者移除其效力已因撤销或身份终止而被取消的令牌的过程。其结果是清理后的令牌集 T_{clean}，这是用于能力图构建和评估的唯一令牌集。所有状态解析均完全在本地进行，且仅取决于提供给评估器的令牌。

4.4.1 输入令牌集与应用程序级筛选

设 T 为提供给评估器的令牌集。

ZI-CG 模型有意不规定应用程序如何获取 T，或选择纳入哪些令牌。应用程序可以从一个或多个参与者或数据源构建 T，并可应用所需的任何筛选策略。典型示例包括：

- 时间有效窗口，
- 上下文相关性，
- 基于策略的排除，
- 大小或范围限制。

这些过滤决策完全发生在调用 ZI-CG 评估器**之前**。该模型假设，T中存在的所有令牌都旨在参与信任计算，而未出现在 T 中的令牌与评估无关。

拥有可靠本地时间概念的应用程序，可以选择将令牌过期字段作为其过滤逻辑的一部分进行解读。过期不会改变 ZI-CG 语义；它只决定令牌是否包含在 T中。过期机制一经启用，便会发挥自然衰减机制的作用：随着签发者定义的有效期结束，委托和证明会自动逐渐失效。在实际部署中，这可以大幅减少对显式撤销的需求，因为过期授权会在评估前从 T 中排除。重要的是，在该模型中，忽略过期不会扩大有效权限，而遵循过期规则则可能移除原本会对信任图有所贡献的令牌。因此，应用程序可以采用基于时间的过滤来加强运行安全，而无需让 ZI-CG 核心模型依赖任何外部机制。

4.4.2 有效令牌集

有效令牌集 T_{valid} 由 T 中所有满足以下条件的令牌组成：

- 结构有效性，
- 使用嵌入的公钥进行正确的签名验证，
- 签发者标识符与公钥之间正确的身份绑定。

正式来说，

$$T_{\text{valid}} = \{t \in T \mid \mathsf{valid}(t)\} \tag{32}$$

4.4.3 销毁谓词

销毁令牌表示，必须忽略特定身份所发布的所有声明。

对于任意令牌 $u \in T_{\text{valid}}$，定义：

$$\mathsf{burned}(u) \iff \mathsf{kind}(u) \neq \mathsf{burn} \ \wedge \ \exists b \in T_{\text{valid}} \text{ such that } \mathsf{kind}(b) = \mathsf{burn} \wedge \mathsf{burn}(b) = \mathsf{iss}(u). \tag{33}$$

如果存在一个有效的销毁令牌，且其引用的身份与 u 的签发者相匹配，则令牌 u 会被销毁。销毁语义适用于所有非销毁令牌类型，包括证明、背书和撤销令牌。此谓词不会移除销毁令牌本身，因此无论何处存在这些令牌，其效果都仍然可见。

4.4.4 撤销谓词

撤销令牌会撤回此前由同一身份签发的特定证明或担保。

使用第 4.3.3 节中定义的匹配规则，定义：

$$\mathsf{revoked}(u) \iff \exists r \in T_{\text{valid}} \text{ such that } \mathsf{revokes}(r, u) \tag{34}$$

当且仅当 撤销$(r,\ u)$ 满足第 4.3.3 节中定义的目标条件时成立。

撤销不适用于销毁令牌或其他控制令牌，也不会直接移除由其他身份签发的主体令牌。它只会移除执行撤销的签发者先前作出的特定声明。

4.4.5 清理后的令牌集

清理后的令牌集定义为从 T_{valid} 中移除所有已销毁和已撤销的令牌：

$$T_{\text{clean}} = \{u \in T_{\text{valid}} \mid \neg\mathsf{burned}(u) \wedge \neg\mathsf{revoked}(u)\} \tag{35}$$

换言之：

- 由已销毁身份签发的令牌将被丢弃，
- 由其签发者明确撤销的证明和背书将被丢弃，
- 所有其他有效令牌均予以保留。

销毁和撤销语义具有单调性。将此类令牌添加到 T 只能从 T_{clean} 中移除更多令牌，绝不会恢复已被移除的令牌。由此产生的令牌集 T_{clean} 代表验证者对所提供令牌集中所有与信任相关的陈述当前状态的完整、自包含视图。它为下一节的能力图构建和委托语义奠定基础。

4.5 能力图构建

给定清理后的令牌集 T_{clean}，ZI-CG 模型将委托结构表示为一个有向图，其中节点是可委托陈述，边则由仍然有效的担保令牌生成。该图为下一节的能力评估提供结构基础。图构建完全确定，仅取决于 T_{clean}。

4.5.1 节点

能力图的节点集由状态解析后保留的所有可委托声明组成。形式化地，

$$V = \{u \in T_{\text{clean}} \mid \mathsf{kind}(u) \in \{\text{attest}, \text{vouch}\}\}. \tag{36}$$

每个节点 $u \in V$ 代表一条可能参与委托和能力传播的信任陈述。控制令牌（包括撤销和销毁令牌）会影响 T_{clean} 的构建，但不会作为节点出现在能力图中。

4.5.2 来自担保令牌的边

有向边仅由 T_{clean}中的担保令牌产生。直观而言，担保令牌 v 会形成一条从其签发者指向被引用声明、代表委托关系的边，前提是该令牌在状态解析后仍然有效。

形式上，边集 $E \subseteq V \times V$ 定义为

$$E = \{(v, u) \mid v \in V,\ \mathsf{kind}(v) = \text{vouch},\ \mathsf{ref}(v) = \mathsf{tid}(u),\ u \in V\} \tag{37}$$

如果担保令牌 v 引用的令牌未出现在 T_{clean} 中，则不会创建边。在这种情况下， v 仍是一个孤立节点。这反映了这样一个事实：对已移除或从未提供的声明所作的背书，无法影响委托。

4.5.3 边上的作用域标签

每个担保令牌都携带一个作用域值，用于约束其传递的权限。设 S 表示范围空间，$\mathsf{scope}(v) \in S$ 表示与担保令牌 v 关联的作用域。

对于每条边 $\mathsf{e}\,(v,\ u) \in E$ 源自担保令牌 v，该边会标注担保的作用域 :

$$\mathsf{scope}(v, u) = \mathsf{scope}(v). \tag{38}$$

这些作用域标签在图构建期间不会被解释。它们用于评估阶段，通过对路径上各条边的作用域求交集，计算与该路径关联的有效能力。因此，图构建会记录后续能力评估所需的结构和作用域信息，但自身不执行任何策略推理。

4.5.4 生成的能力图

与清理后的令牌集 T_{clean} 关联的能力图是这一对

$$G(T_{\text{clean}}) = (V, E), \tag{39}$$

其中， V 和 E 如上所定义，且每条边 $(v,\ u) \in E$都带有作用域标签 $\mathsf{scope}(v,\ u)$。

这种构建方式具有几个重要特性。

- **局部性**。 图结构完全由 $T_{\text{清理后的令牌集}}$决定。不查询任何外部状态、解析器或注册表。
- **确定性**。 对于任何固定的 $T_{\text{清理后的令牌集}}$，图 $G(T_{\text{清理后的令牌集}})$ 都是唯一确定的。给定相同的清理后令牌集，两个评估器将构建出完全相同的图。
- **删除下的单调性**。 如果从 $T_{\text{清理后的令牌集}}$中移除令牌，得到的图就是移除相应节点及其所有关联边后的图。移除令牌不会引入新边。
- **无环结构**。 由于担保令牌通过内容寻址标识符引用其他令牌，因此令牌只能引用在其创建之前就已存在的声明。这在令牌之间形成严格偏序，并保证生成的能力图无环。撤销和销毁语义只会移除节点或边，因此会保持无环性。因此，下一节中的评估过程可以将委托视为沿有限有向路径传播，而无需外部环检测机制。

能力图 $G(T_{\text{clean}})$ 捕获了状态解析后保留下来的所有潜在委托和背书结构。下一节将定义如何结合验证者选定的信任根，利用该图计算特定令牌和作用域的有效能力。

4.6 能力评估

能力评估用于确定，在给定清理后的令牌集 T_{clean} 以及验证者的受信主体集合及其关联作用域的情况下，特定令牌 t 是否获授权拥有所请求的权限范围。评估是一项本地计算，从待评估的令牌开始，沿委托边向后搜索，直到找到作用域兼容的受信主体，或穷尽所有可能的路径。

评估过程的输入包括：

- 清理后的令牌集 $T_{\text{清理}}$,

- 主体令牌 $t \in T_{\text{清理}}$ 待评估对象,
- 受信主体集 R,
- 请求范围$s_{\text{请求}} \subseteq S$。

目标是确定：相对于配置的受信主体， t 是否获授权使用 s_{req}中的所有能力。

4.6.1 受信主体

设 Id 为身份集， S 为范围空间。受信主体是一个身份，以及验证者愿意授予该身份的最大范围。形式上，验证者提供一个有限集合

$$R \subseteq \mathsf{Id} \times S \tag{40}$$

其中每个二元组 $(i,\ s\_r) \in R$ 表示身份 i 受信，但仅限于包含在 s_r中的能力。没有任何身份会被默认视为在所有作用域中都受信。信任始终受明确指定的根范围限制。

4.6.2 指向主体的委托路径

设 $G(T_{\text{clean}}) = (V,\ E)$ 为第 4.5 节定义的能力图，其中 $V = \{u \in T_{\text{clean}} \mid \text{类型}(u) \in \{\text{证明、担保}\}\}$。
从**委托路径** t是节点的有限序列

$$p = (n_0, n_1, \cdots, n_k) \tag{41}$$

满足：

- $n_k = t$,
- $(n_j,\ n_{j+1}) \in E$ 对所有 $0 \le j < k$。

若路径 p 的第一个节点是由该身份签发的令牌，则该路径以受信主体 $(i,\ s_r) \in R$ 为根：

$$\mathsf{iss}(n_0) = i. \tag{42}$$

只有此类路径与能力评估相关。图中未以 t 为终端节点的路径，或初始签发者不属于 R 的路径，在判断 t 是否获授权时均会被忽略。
令 $\mathsf{Vouch}(p)$ 表示沿该路径出现的担保令牌集合：

$$\mathsf{Vouch}(p) = \{n_j \mid 0 \le j < k,\ \mathsf{kind}(n_j) = \text{vouch}\}. \tag{43}$$

4.6.3 路径作用域与衰减

作用域是能力的集合，委托声明和终端声明都可以约束沿委托路径传递的权限。每个担保令牌 v 都带有一个显式的作用域值 $\mathsf{scope}(v) \in S$，而每个受信主体 $(i,\ s_r)$ 都会提供一个根范围 s_r，用于限定验证者最初授予的最大权限。

虽然证明令牌不会引入委托边，但它们可能会声明作用域约束，以限制其所代表声明的适用性。这些约束会参与委托路径终端节点处的范围衰减。
令 $\mathsf{tscope}(u) \in S$ 表示令牌 u所声明的范围。对于担保令牌和证明令牌，$\mathsf{tscope}(u) = \mathsf{scope}(u)$。如果证明令牌未声明明确的作用域约束，则在范围方面将其视为不受约束，因此 $\mathsf{tscope}(u) = S$。

在实践中，能力评估从主体令牌 t开始，该令牌通常是证明令牌。如果主体声明了作用域约束，则该约束会限制从任何以 t为终点的委托路径中推导出的所有权限。路径上的后续担保令牌可能会进一步削弱权限，而根范围 s_r 则提供了总体上限。

给定一个受信主体 $(i, s_r) \in R$ 以及一条委托路径

$$p = (n_0, n_1, \cdots, n_k = t), \tag{44}$$

该路径以（i, s_r）为根，其有效范围定义如下：

$$\mathsf{scope}(p) = s_r \cap \bigcap_{v \in \mathsf{Vouch}(p)} \mathsf{scope}(v) \cap \mathsf{tscope}(t). \tag{45}$$

如果 Vouch(p) 为空，则将担保令牌的交集视为整个范围空间，因此有效范围简化为

$$\mathsf{scope}(p) = s_r \cap \mathsf{tscope}(t). \tag{46}$$

如果委托路径 p 的有效范围非空，则称其为**可接受**：

$$\mathsf{scope}(p) \neq \varnothing. \tag{47}$$

范围衰减具有单调性。通过添加更多担保令牌来扩展路径，只会缩小或保持有效范围，不可能扩大范围。证明令牌同样会限制范围，但不会传播权限。这确保权限不会通过委托或组合声明而增长，并且所有有效能力都受路径上遇到的最严格约束所限制。

4.6.4 对请求范围的接受

请求以一组所需能力的形式表示

$$s_{\text{req}} \subseteq S. \tag{48}$$

评估器必须根据当前信任配置和清理后的令牌集，判定主体令牌 t 是否至少获授权具备 s_{req} 中的能力。

令牌 $t \in T_{\text{clean}}$ 针对请求范围 s_{req} 被**接受**，当且仅当在 $G(T_{\text{clean}})$ 中至少存在一条委托路径 p，满足：

1. p 终止于 t；2. p 以某个受信主体（i, s_r） $\in R$
为根；3. 路径范围满足最低要求范围：

$$s_{\text{req}} \subseteq \mathsf{scope}(p). \tag{49}$$

接受条件会独立评估每条委托路径。不同路径的范围绝不会合并或融合。仅当从受信主体到 t 的一条可接受路径**保留了 s_{req} 中的所有能力时，令牌才获授权用于该请求**。如果不存在这样的路径，模型将判定 t未获授权用于请求范围。

定义接受谓词：

$$\text{接受}(T_{\text{clean}},\ t,\ R,\ s_{\text{req}}) \iff \exists p \text{ 使得 } p \text{ 是一条以某个（}i, s_r\text{）} \in R, p \text{ 为根、终止于 } t, \text{ 且 } s_{\text{req}} \subseteq \text{范围（}p\text{）}. \tag{50}$$

4.6.5 评估函数与确定性

给定清理后的令牌集和信任配置，能力评估函数回答的是：特定令牌是否支持请求范围。其定义如下：

$$\mathsf{Eval}(T_{\text{clean}}, t, R, s_{\text{req}}) = \begin{cases} \text{accept} & \text{if } \mathsf{Accept}(T_{\text{clean}}, t, R, s_{\text{req}}) \text{ holds} \\ \text{reject} & \text{otherwise} \end{cases} \tag{51}$$

Eval 涉及的所有组成部分都仅由以下因素决定：

- $T_{\text{干净}}$，由第 4.4 节的状态解析规则生成，

- 主体令牌 t,
- 受信主体集 R,
- 请求范围s_{req}。

从 T_{clean} 进行图构建是确定性的，路径范围通过固定的集合交集计算得出，而接受谓词是关于路径的纯逻辑条件。因此，能力评估具有确定性：如果两个评估器收到完全相同的输入T_{clean}，t，R，s_{req}，它们就会构建出相同的图，识别出相同的候选路径集，计算出相同的路径范围，并得出相同的接受或拒绝决定。

4.6.6 实现注意事项

ZI-CG 模型并未规定用于发现路径的特定搜索策略。不过，范围的衰减特性为高效评估提供了天然的机会。在从 t 开始进行反向搜索时，实现可以沿每条部分路径维护当前累积范围。一旦该累积范围变为空，或不再包含请求范围 s_{req}，就可以放弃这条部分路径。这种提前终止不会改变 Eval 的语义；它只是避免探索不可能满足接受条件的路径。

总之，ZI-CG 系统中的能力评估是一种局部的、目标导向的计算，从主体令牌开始，搜索来自具有特定范围的受信主体的单条可接受委托链。权限绝不会通过组合多条路径而扩大。权限只会沿着通过状态解析且仍与请求范围兼容的单条路径发生衰减。

4.7 其他确定性求值器

尽管能力检查是本模型中描述的主要评估方式，但 ZI-CG 并不将评估器局限于该特定查询。只要满足以下三个条件，任何针对图 $G(T_{\text{clean}})$ 的计算都符合 ZI-CG 规范：

1. **局部性** - 结果仅取决于 T_{clean}、验证者的受信主体以及显式查询参数。2. **确定性**- 相同的输入必须产生相同的输出。3. **范围衰减** - 从委托中推导出的权限绝不能超出单条可接受路径所允许的范围

s.

在这些约束下，评估器可以执行其他分析，例如枚举有效的委托路径、检查每条路径上剩余的作用域，或执行可达性查询或审计查询。这些计算不会改变授权语义；它们说明，ZI-CG 提供了一种通用基础，仅依赖局部令牌集即可进行确定性信任推理。

5 Vouchsafe：ZI-CG 模型的完整实现

Vouchsafe 是一个可运行的系统，以具体、可部署的形式实现了零基础设施能力图（ZI-CG）模型。它仅使用广泛可用的基本技术：身份以统一资源名称编码，令牌序列化为 JSON Web 令牌（JWT） [9] ，并采用 JWS 签名 [10], ；内容寻址使用 SHA-256，身份和签名则使用 Ed25519 [11]。参考实现以 JavaScript 编写，可在现代网页浏览器和 Node.js 中运行，展示了 ZI-CG 系统能够在普通客户端设备上运行，无需专用基础设施。

本节介绍 Vo uchsafe 如何实现第 4 节中的抽象机制。我们的目标并非提供完整的正式 at 规范，而是展示如何 在实践中实现模型的每项要求。

5.1 身份构造

Vouchsafe 身份编码为以下统一资源名称： form

urn:vouchsafe:<标签>.<哈希值> (52)

其中 <标签> 是具有人类可读意义的标识符，而 <哈希值> 是根据发行者公钥生成的抗碰撞摘要。在实现中， <哈希值> 计算为小写、无填充的 Base32 编码（RFC-4648第6节） [12] ，其输入是发行者SHA-256哈希值，即发行者的原始公钥字节。原始公钥字节从 DER 编码的公钥中提取，并排除所有编码元数据。标签不包含在哈希值中；它是不会影响身份绑定的元数据。

每个 Vouchsafe 令牌都包含两项声明：

- iss：发行者身份，必须是符合以下形式的 Vouchsafe URN：urn:vouchsafe:<标签>.<哈希值>。
- iss_key：发行者公钥，以 DER 编码的主体公钥信息结构进行编码，并经 Base64 编码后包含在令牌中。

按照第4.1节的表示法，Vouchsafe 通过以下方式实现

$$i = \mathsf{id}(pk, m) \tag{53}$$

通过标签元数据 m和公钥哈希值 pk构造统一资源名称，并实现

$$\mathsf{validate}(i, pk) \tag{54}$$

by:

1. 解析 iss 以恢复 <哈希值>。2. 解码 iss_key 以获取 DER 编码的公钥。3. 从 DER 结构中提取原始公钥字节。4. 计算 $\mathrm{base32}_{\mathrm{lc,\ np}}(\mathrm{SHA256}(\mathrm{raw}(pk)))$。5. 检查计算结果是否与 <哈希值>匹配。

仅对提取出的原始公钥字节进行哈希处理，可确保身份派生不受语义等效的 DER 编码影响，并且仅取决于密码学密钥材料。

令牌验证期间，库使用 `iss_key`验证 JWS 签名，然后检查 `iss_key` 是否满足此统一资源名称绑定。只有当签名有效，且其 `iss` 和 `iss_key` 满足身份绑定函数时，令牌才会被接受为自验证令牌。这以完全离线的方式实现了第 3.3 节的自解析身份要求，以及第 4.1 节的身份模型。

5.2 令牌编码与签名

Vouchsafe 使用 JWS 和 Ed25519 签名，将所有 ZI-CG 令牌编码为签名 JWT。JWT 载荷（即令牌主体）包含发行者身份和公钥，以及实现 ZI-CG 令牌结构所需的最少字段。
从结构上看，主体的形式如下：

$$\mathsf{body}(t) = \big(\mathsf{iss}(t), \mathsf{pk}(t), \mathsf{payload}(t)\big) \tag{55}$$

其中：

- iss 编码 iss(t)，且必须是 Vouchsafe URN。
- iss_key 编码 pk(t)，即与 iss 对应的公钥。
- 载荷包含：
  – 类型：以 `vch:` 开头的字符串，用于标识令牌类型（证明、担保、撤销或销毁）。– `jti`：必需的、由签发者唯一分配的令牌标识符（UUID）。同一签发者不得重复使用。二元组（`iss`，`jti`）用于标识特定的声明行为，并作为撤销的目标以及应用程序级引用。– `sub`：主体声明的 `jti` 。其解释由令牌类型确定，具体如下所述。– 类型特定声明，用于实现第 4.3 节中的字段：* `vch_iss`、`vch_sum` 用于担保和撤销令牌，它们共同通过签发者和内容哈希标识主体令牌。* 撤销对象用于撤销令牌，用于标识被撤回的先前令牌。* 销毁对象用于销毁令牌，用于标识即将终止的身份。* 用途 用于担保和证明令牌，以一组能力字符串的形式编码范围。

令 $\mathsf{jwt}(t) \in \{0,1\}^*$ 表示令牌 t 在线路上传输时所使用的精确 JWS 紧凑序列化字符串。基于内容的令牌标识符计算如下：

$$\mathsf{tid}(t) = \mathsf{SHA256}\big(\mathsf{jwt}(t)\big). \tag{56}$$

由于 $\mathsf{jwt}(t)$ 包含受保护标头、载荷和签名，因此对令牌内容、签名密钥或签名的任何更改，都会使签名验证和内容标识符同时失效。

由背书和撤销令牌引用的主体令牌，通过 (sub, vch_iss, vch_sum) 标识，其中 vch_sum是主体令牌按签发和传输时的原始 JWS 紧凑序列化字符串计算出的 SHA-256 哈希值的十六进制编码，而不是重新编码或重构后的表示。这样便实现了第 4.3.2 节中的抽象 $\mathsf{ref}(t)$ 字段，并确保主体引用采用内容寻址。

标准 JWT 声明（如 iat、nbf 或 exp）可以存在，并由应用程序用于时间策略，但 ZI-CG 模型并不要求这些声明，且它们不直接参与图构建或能力评估。核心评估器仅依赖身份字段（iss、iss_key）、签发者本地声明标识符 jti（以及 iss）、类型特定声明（sub、vch_iss、vch_sum、撤销、销毁、purpose）和签名。

借助这一结构，Vouchsafe 实现了第 4.2节所述的自验证令牌抽象：每个令牌的来源和完整性都可以仅凭其内容及标准 JWS 签名语义进行验证，而图构建和状态解析所需的所有引用都以内容寻址字段的形式编码在令牌主体中。

5.2.1 声明与主体识别不变量

每个 Vouchsafe 令牌都包含一个必需的 jti 字段，其值为新生成的 UUID。同一签发者不得重复使用 jti。二元组 (iss, jti) 唯一标识由该身份签发的特定声明。

所有令牌类型均统一使用 sub 字段，通过声明的 jti 来标识主体声明。对于证明令牌和销毁令牌，该声明是自引用的，且 sub 等于令牌自身的 jti。对于担保令牌和撤销令牌，sub 等于被担保或讨论的主体令牌的 jti。

撤销令牌区分被撤回的声明与该声明所指向的主体。revokes 字段通过 jti 标识先前的声明行为，而三元组 (sub, vch_iss, vch_sum) 则标识该声明所适用的主体令牌。只有声明标识符和主体引用都完全匹配时，撤销才生效。

声明身份（iss、jti）与内容身份（sub、vch_iss、vch_sum）的分离，使得撤销某个特定的发行者行为时，可以同时防止将其重定向到不同的主体，或指向原始令牌的修改版本。

5.3 令牌类型与模型对应关系

所有 Vouchsafe 令牌都采用第 5.2 节中的通用结构：iss、iss_密钥、类型、jti、sub，以及一组类型特定声明。应用程序可以使用任意额外声明，核心评估器会忽略这些声明。本节仅介绍实例化第 4.3 节定义的四类令牌所需的字段。

5.3.1 证明令牌

证明令牌的类型为 = “vch:attest”。sub 字段标识令牌本身，且必须与 jti 相等；其他负载声明则编码关于该主体的声明。

用模型的术语来说，这些令牌的类型(t)为 = attest。其类型特定内容仅作为数据附加在图中的节点上；评估器的任务是判断该节点是否可信，而不是解释经证明的声明。

5.3.2 背书令牌

背书令牌实现委托信任，且携带类型 = "vch:vouch"。它们使用三个对模型至关重要的字段：

- sub：被背书主体令牌的 jti，
- vch_iss：该主体令牌签发者的身份，
- vch_sum：主体令牌在线传输时所用 JWS 紧凑序列化的精确 SHA-256 哈希值，

合在一起，(sub、vch_iss、vch_sum) 可在 T_{valid} 中唯一标识一个主体令牌。这实现了第 $\mathsf{ref}(t)$ 节 4.3.2 中的抽象引用，并可防止用内容相似的其他令牌替换该令牌。purpose 声明提供了委托范围，其被解释为一组能力字符串，并由此实例化 $\mathsf{scope}(t) \subseteq S$。

在该模型的记法中，担保令牌实现

$$\mathsf{typefields}(t) = \big(\mathsf{ref}(t), \mathsf{scope}(t)\big) \tag{57}$$

其 $\mathsf{ref}(t)$ 源自 (`sub`、`vch_iss`、`vch_sum`) 以及 $\mathsf{scope}(t)$源自 `purpose`。能够保留到 T_{clean} 中的担保令牌，会在能力图中产生带有这些作用域标注的有向边，如第 4.5 节所述。
由于主体引用采用内容寻址，担保令牌只能引用签发时已存在的令牌，从而确保能力图在构造上无环。

5.3.3 撤销令牌

撤销令牌用于撤回先前的声明，其类型为 = "vch:revoke"。它们使用：

- sub：主体令牌的 jti，其背书或断言正被重新审议，
- vch_iss：该主体令牌签发者的身份，
- vch_sum：主体令牌在线路上传输时所用的 JWS 紧凑序列化的 SHA-256 哈希，
- revokes：要撤销的特定先前背书或证明的 jti。

三元组 (`sub`，`vch_iss`，`vch_sum`) 在第 $\mathsf{ref\_subject}(t)$ 节中实例化了 4.3.3，而`revokes` 实例化了 $\mathsf{revoke\_target}(t)$。撤销令牌只有在满足以下条件时才与较早的声明匹配：

1. revokes 与较早令牌的 jti 匹配，且
2. (sub, vch_iss, vch_sum) 与该较早声明所引用的主体令牌匹配。

在构建 T_{clean}时，任何匹配的担保或证明都会被移除。这是第4.4节所述基于省略证明的撤销语义的具体实现。

5.3.4 销毁令牌

销毁令牌会终止一个身份，其类型为 = "vch:burn"。它们是严格自指的声明，并使用一个与模型相关的字段：

- burns：签发者身份 iss。

只有当 burns 与令牌的签发者身份 iss 完全相同时，销毁令牌才有效。指定任何其他身份的销毁令牌均无效，必须在结构验证期间予以拒绝。
与证明令牌一样，销毁令牌也具有自指性：sub 字段等于令牌自身的 jti。因此，销毁表示某个身份明确声明不应再被信任。

在模型的表示法中，销毁令牌实现 $\text{销毁}(t) = \mathsf{iss}(t)$，定义见第 4.3.4 节。在状态解析期间，如果 T_{valid} 中存在有效的销毁令牌，评估器会在构造 T_{clean} 之前，移除所有签发者身份 iss 与已销毁身份相匹配的令牌。

该约束确保身份终止严格遵循自我主权原则。任何身份都不能撤销、暂停或终止其他身份。无论在 ZI-CG 模型中还是在 Vouchsafe 中，都不存在可将身份权限委托给第三方或由第三方行使该权限的机制。

5.3.5 ZI-CG 模型元素与 Vouchsafe 字段之间的映射

为明确抽象的 ZI-CG 模型与具体的 Vouchsafe 实现之间的对应关系，表 1总结了模型层面的概念如何通过 JWT 声明实现。

此映射明确体现了 Vouchsafe 中声明身份与内容身份之间的分离。jti 字段标识签发者执行的特定声明行为，而 vch_sum 则承诺被引用令牌的精确编码内容。结合发行者身份，这些字段实现了 ZI-CG 中的引用、委托、撤销和销毁概念，无需依赖外部解析或可变基础设施。

ZI-CG 概念	Vouchsafe 字段	备注
身份 $i \in I$	`iss`	根据签发者公钥派生的 Vouchsafe URN。
公钥 $pk \in PK$	iss_密钥	DER 编码的公钥，在 JWT 中以 Base64 编码。
令牌 t	JWS 紧凑型 JWT	已签名的、自包含的声明。
令牌标识符 tid(t)	SHA-256(jwt(t))	线上传输的 JWS 紧凑序列化的精确哈希值。
声明标识符	(iss, jti)	声明行为的发行者本地标识符。
主体引用 ref(t)	(sub, vch_iss, vch_sum)	指向主体令牌的内容寻址引用。
令牌类型 kind(t)	`kind`	vch:attest、vch:vouch、vch:revoke、vch:burn。
委托范围 scope(t)	purpose	能力字符串集合。
撤销声明	（iss，revokes）	标识被撤回的先前声明行为。
已注销身份	burns	被终止的身份；必须与 iss 相同。

表 1：ZI-CG 抽象模型元素到 Vouchsafe JWT 字段的映射。

5.4 状态解析与 T_{clean} 的构建

Vouchsafe 使用 ZI-CG 状态解析过程，其结构与第4.4节中定义的三阶段结构相同。评估器从应用程序提供的令牌集 T开始，对每个令牌进行解码和有效性验证，生成 T_{valid}，收集所有撤销和销毁操作，然后通过省略任何有效性与所提供声明相矛盾的令牌，构建 T_{clean}。由此得到有效状态，图构建和能力评估将在该状态上运行。

5.4.1 T_{valid} 的验证与构建

T 中的每个令牌首先使用标准 JWT 处理流程进行解码。只有满足以下条件，验证才会成功：

1. 内嵌签名通过 iss_ 密钥验证。2. 身份绑定正确：

$$\text{iss} = \texttt{urn:vouchsafe:}\text{label} \cdot \text{base32}\big(\text{SHA256}(\text{raw}(\texttt{iss\_key}))\big) \tag{58}$$

其中哈希值由从 `iss_`密钥 中提取的原始公钥字节，使用第 5.1 节定义的相同算法和编码重新计算。

未通过任一检查的令牌将被排除。剩余令牌构成 T_{valid}。
仅出现在 T_{va} 中的令牌　　关联 参与撤销和销毁语义；无效令牌不会对状态解析产生影响　　n.

5.4.2 撤销和销毁的提取

评估器从 T_{valid} 中提取两类会影响状态解析的控制令牌：

- **销毁令牌**，用于终止某个身份，并抑制该身份发布的所有声明。
- **撤销令牌**，用于撤回同一身份先前发布的特定声明。

撤销　令牌通过两个不同的引用进行解析，这两个引用必须共同匹配先前的声明　　t.
首先，通过以下三元组确定已撤销声明的主体：

- sub：主体令牌的 jti，
- vch_iss：该主体令牌的发行者身份，
- vch_sum：该主体令牌最初签发时的确切 JWS 紧凑序列化字符串的 SHA-256 哈希。

这些字段共同标识被引用的确切主体令牌，将其发行者及其完整的线上编码内容都纳入承诺。这可以防止撤销被转向其他主体，或指向同一令牌的修改版本。

其次，通过以下信息标识要撤回的特定先前声明：

- 撤销项：被撤销的担保令牌或证明令牌的 jti。

撤销令牌仅在以下情况下与先前的声明匹配：

1. 撤销的签发者与被引用声明的签发者相同，且
2. 撤销值与该声明的 jti 匹配，且
3. 主体引用（sub, vch_iss, vch_sum）与该声明引用的主体令牌完全匹配。

只有满足所有这些条件时，撤销才会生效。在构建 T_{clean} 时，任何匹配的担保或证明令牌都会从有效状态中排除。

销毁令牌会被独立处理。销毁令牌指定一个身份，其全部声明历史都必须被屏蔽。存在有效的销毁令牌时，该已注销身份签发的所有令牌都会在图构建之前被移除。
只有出现在 T_{valid} 中的撤销和销毁令牌才会参与状态解析。无效、格式错误或未经身份验证的控制令牌不会产生任何影响。这使模型能够仅凭本地可用的签名数据实现遗漏证明语义。

5.4.3 构造 T_{clean}

当且仅当令牌 $t \in T_{\text{valid}}$ 未根据状态解析规则被销毁或撤销时，才会将其纳入清理后的令牌集 T_{clean} 。

F通常，当且仅当满足以下所有条件时，才会将令牌 $t \in T_{\text{valid}}$ 纳入 T_{clean} ：

1. **该令牌并非由已注销身份签发**。如果存在销毁令牌 $b \in T_{\text{valid}}$ ，使得 $\text{burns}(b) = \text{iss}(t)$，
则会将 t 从 T_{clean}中排除。
2. **该令牌未被适用的撤销令牌指定为目标**。
撤销令 令牌 $r \in T_{\text{valid}}$ 适用于先前令牌 t ，当且仅当以下所有条件均成立 ：
   - t 是担保令牌或证明令牌，
   - $\text{iss}(r) = \text{iss}(t)$，
   - $\text{revokes}(r) = \text{jti}(t)$，
   - 主体引用完全匹配，也就是说， r 中的 sub、vch_iss 和 vch_sum 与 t 携带的相应主体引用一致。

   如果存在此类撤销令牌，则 t 将从 T_{clean} 中排除。

在 T_{valid} 中，同时满足这两个条件的所有令牌都会保留在 T_{clean} 中。因销毁或撤销而被排除的令牌将被完全省略，不参与后续的图构建或能力评估。
此过程实现了 ZI-CG 遗漏证明规则：仅当提供的令牌集不包含由同一身份签发的任何相互矛盾的签名声明时，该声明才会继续有效。
这一仅执行计算的过程会生成一个 T_{clean} ，表示所提供令牌集内所有与信任相关的声明的当前状态的完整且自包含视图。

5.5 能力图构建

一旦计算出 T_{clean} ,Vouchsafe 评估器将按如下方式构建能力图 $G = (V,\ E)$。

5.5.1 节点

所有**剩余、未撤销且未销毁的令牌**均作为节点添加：

$$V = \{u \in T_{\text{clean}} \mid \text{kind}(u) \in \{\text{attest}, \text{vouch}\}\} \tag{59}$$

在构建 T_{clean} 的过程中，撤销和销毁效应已经应用。其声明已被撤回或签发者已被销毁的令牌，在该阶段就已移除，因此从未出现在图中。 G 的节点恰好是根据模型的状态解析规则仍然有效的声明。

5.5.2 边

只有担保令牌会产生边。对于每个担保令牌 $t \in T_{\text{clean}}$，三元组 (sub, vch_iss, vch_sum) 用于标识一个主体令牌 $u \in T_{\text{clean}}$。如果多个令牌具有相同的 jti，但编码不同，则只有编码JWT哈希值与 vch_sum 匹配的令牌才符合条件。如果存在这样的令牌，评估器便会添加一条有向边 $t \to u$，并将其标签设为根据 t 的用途声明推导出的委托范围。如果 T_{clean} 中不存在匹配的主体令牌，该担保便不起作用，也不会产生任何边。

5.5.3 结果

由此生成的有向图 $G(T_{\text{clean}})$ 恰好包含所有保留下来的声明和委托，以及它们关联的作用域。此时，该图已包含在 ZI-CG 模型下进行正确信任评估所需的全部信息；能力评估引擎只需遍历该图并求作用域的交集，无需进一步修改令牌集。

通过内容寻址引用的使用，从构造上确保无环性。对于每个担保令牌，vch_sum 定义为主体令牌完整编码后的 JWT 字符串的 SHA-256 哈希值。这要求先完整构造主体令牌，才能创建担保。因此，$G(T_{\text{clean}})$ 中的边始终从后创建的令牌指向较早创建且其编码已固定的令牌。根据 SHA-256 的标准假设，这可以防止构造相互引用的令牌集，因此对于任何有效的 Vouchsafe 令牌集，能力图 $G(T_{\text{clean}})$ 都是有向无环图。

5.6 Vouchsafe 中的能力评估

能力图构建完成后 G（T_{clean}），Vouchsafe 会遍历图并交集计算范围约束，从而执行能力评估，具体按照第 4.6 节中 ZI-CG评估模型的规定进行。在此阶段，不会进一步修改令牌集或图结构。

在 Vouchsafe 中，范围通过证明和担保令牌携带的 purpose 字段表示。purpose 值是由空格分隔的能力标签集合，并被解释为作用域集合。受信主体配置有相应的根用途集合，用于限定验证者最初授予的最大权限。

评估从待考察的主体令牌开始，并通过检查在 G（T_{clean}）中终止于该令牌的委托路径来推进。沿每条此类路径，有效用途通过对受信主体的根用途、路径上每个担保令牌声明的 purpose 值，以及终端证明声明的任何用途约束进行交集计算得出。这与第 4.6 节定义的路径范围计算直接对应。

当且仅当存在至少一条从受信主体到主体令牌的委托路径，且其有效用途包含所有请求的能力时，请求才会被接受。不同路径上的用途值绝不会合并。只有单条可接受路径保留了完整的请求范围时，授权才会成功。

由于路径遍历和用途交集仅基于 $G(T_{\text{clean}})$、主体令牌、配置的受信主体以及请求的用途进行，Vouchsafe 中的能力评估具有确定性。任何接收相同输入的两个评估器都会计算出相同的路径范围，并得出相同的接受或拒绝决定。

6 安全分析

本节分析零基础设施能力图（ZI-CG）模型及其 Vouchsafe 实现的安全属性。我们阐述安全契约、威胁模型和残余风险；此处的保证是相对于验证者在标准 Ed25519 和 SHA-256 假设下对签名令牌进行的本地计算而言的。

6.1 安全契约与范围

ZI-CG 旨在通过令牌结构和本地验证来确保信任声明的完整性和来源，而非依赖可信服务或分发渠道。本小节概述安全契约以及模型的预期范围。

模型级保证。 在 Ed25519 和 SHA-256 的标准假设下，正确实现结构验证和 T_{clean} 构造的验证者可获得以下保证：

- **声明的完整性：** 令牌无法在不使其签名失效的情况下被修改。
- **来源真实可信：** 每个获接受的令牌都绑定到一个发行者身份和公钥，从而防止针对固定身份的密钥替换。

- **图不可变性：** 担保和撤销令牌按内容绑定到其主体，从而防止在没有密钥泄露或哈希碰撞的情况下，追溯性地改写或拼接现有边。
- **权限局部性：** 令牌不赋予任何环境权限；声明仅相对于验证者的可信根和请求范围才有效。

- **确定性评估：** 对于固定的清理后的令牌集和验证者配置，任何正确的实现都会得出相同的信任决策，从而支持可复现的审计。

残余风险与非目标。 ZI-CG 不试图保证应用声明在语义上的真实性、不试图防范端点失陷，也不试图确保各方对令牌可用性达成全球一致。控制基础设施的对手可以影响评估时哪些有效令牌可用，但若没有密钥泄露，就无法更改任何已签发令牌所述的内容。因此，主要的残余攻击面在于密钥泄露、销毁令牌和撤销令牌的分发，以及验证者策略配置。

6.2 威胁模型

我们假设对手能够：

- 通过用于分发令牌的任何机制观察、注入、修改和重放消息。
- 试图冒充身份、伪造声明或操纵委托结构。
- 向验证者提交任意令牌集，包括规模庞大或经过精心挑选的令牌集。
- 泄露部分主体的私钥。

我们假设不存在可信基础设施和可信分发渠道。验证者的评估逻辑和本地配置均假定未遭泄露。环境的所有其他方面，包括传输、存储和令牌库，都可能受到对手控制。

6.2.1 假设与局限

本分析基于以下明确假设：

- **密码学假设。** Ed25519 签名方案能够抵御选择消息攻击，且 SHA-256 具有抗碰撞性和抗原像性。

- **正确评估。** 验证者会正确实施令牌结构验证，并构建清理后的令牌集 T_{clean}，其中包括销毁和撤销处理。省略这些规则会改变模型，并可能使本节所述的保证失效。

- **令牌可用性。** 该模型未规定令牌的分发或同步方式。能够阻止或延迟相关销毁令牌或撤销令牌交付的对手，可能导致验证者继续接受在令牌集更完整时会被拒绝的声明。

- **策略配置。** 受信主体集合和初始范围属于本地策略。如果这些配置有误，评估过程仍会忠实地计算出相对于验证者预期策略而言不正确的授权结果。

鉴于这一威胁模型，我们可以 分析陈述完整性、图操纵、密钥泄露语义以及剩余的攻击 ck 由令牌引入的表面 可用性和分发。

6.3 声明的完整性和真实性

在 ZI-CG 中，与信任相关的 声明以签名令牌的形式表示。只有满足以下条件，令牌才会被视为结构有效： if:

1. 签名可通过嵌入的签发者公钥 `iss_`密钥进行验证；并且 2. 发行者身份 `iss` 已根据 Vouchsafe URN 派生规则（第 5.1_节）正确地绑定到 iss密钥。

在第 6.2 节所述的密码学假设下，不持有签发者私钥的对手无法生成一个能够验证为由该身份签发的新令牌，也无法修改已签发令牌中的任何字段而不导致其签名失效。

这些属性保证了声明的真实性和来源，但不保证其语义正确性。发行者可能会提出误导性、错误或欺骗性的应用层声明，同时仍然生成结构上有效的令牌。判断应用特定声明的真实性或适当性不属于 ZI-CG 模型的范畴，必须通过应用策略或外部验证机制来强制执行。

6.4 图级攻击

6.4.1 替换和图重写

在令牌结构有效且签发者经过身份验证的情况下，一个顺理成章的下一步攻击是尝试将恶意令牌插入现有的委托图，例如将担保重定向到另一个主体，或追溯更改主体令牌的内容。

在 Vouchsafe 中，担保令牌和撤销令牌通过以下三个字段标识其主体：

- sub：主体令牌的 jti，
- vch_iss：主体令牌的发行者身份，
- vch_sum：主体令牌最初签发时，其精确的 JWS 紧凑序列化字符串的 SHA-256 哈希。

若要更改背书或撤销所针对的令牌，攻击者必须生成另一个令牌，使其 JWT 编码具有完全相同的 SHA-256 哈希值，且由同一身份签发。在 SHA-256 的抗碰撞假设下，这不可行。同样，修改主体令牌本身也会改变其编码表示，从而改变 vch_sum，破坏链接。

因此，令牌一经签发，能力图的结构便由其签名内容固定。攻击者可以添加新令牌，但无法改写现有令牌的含义，除非：

- 获取签发者的私钥，或
- 找到 SHA-256 的碰撞。

此外，即使攻击者能够获取签发者的私钥，创建任何内容有所更改的新令牌，也会使所有指向该令牌的背书中的 vch_sum 失效，破坏链接并使这些背书无法生效。

6.4.2 无环性与防止递归委托

在 ZI-CG 以及因此在 Vouchsafe 中，所有委托边都由担保令牌产生；这些令牌通过对主体令牌完整编码后的 JWT 字符串计算内容寻址哈希值来引用其主体。由于只有在主体令牌完全构造完成后才能计算此哈希值，因此担保令牌只能引用在逻辑上和时间上先于自身的令牌。特别是，令牌无法对自身（或依赖于自身的令牌）进行内容寻址，否则就需要在 vch_sum 中产生哈希碰撞。

因此，如果不破坏 SHA-256 的抗碰撞性，或不在令牌存在之前预先计算其编码，就不可能构造相互引用或循环的委托结构。在标准密码学假设下，所得到的能力图因此是一个有向无环图。

此属性可防止递归自我背书、无限委托循环以及通过循环实现的范围放大。它通过密码学数据依赖关系强制实现，而不是依靠评估期间的过程性检查或环检测。

6.4.3 重放与陈旧令牌

由于令牌是自包含且可验证的，只要旧令牌在结构上仍然有效，且尚未被撤销或根据应用策略被替代，攻击者就可以重放这些令牌。ZI-CG 模型有意将撤销和身份终止视为显式的数据添加，而不是与网络状态或时间绑定的隐式规则。

这带来了两个特性：

- 对于任何固定令牌集，评估结果都是确定性的。将相同令牌重放给不同的验证者，会产生相同的结果。

- 针对重放过时权限的保护由销毁令牌和撤销令牌提供，也可通过短有效期或签发策略等应用层约束实现，而不是依赖基础设施检查。

ZI-CG 中的令牌不携带环境权限或全局权限。令牌的作用始终根据验证者本地配置的可信根和请求范围进行评估。在不同的应用程序或上下文中重放有效令牌，无法赋予额外权限，除非该验证者明确信任该签发者在相关范围内的权限。

该模型保证相对于所提供令牌集的正确性。外围系统有责任确保将相关的撤销令牌和销毁信息提供给需要它们的验证者，或者确保令牌的有效期有限。

6.4.4 令牌集泛洪攻击

攻击者可以尝试通过提交一个极大的令牌集来发动拒绝服务攻击，以最大限度地增加验证和图遍历的工作量。ZI-CG 模型并未排除此类情况；任何接受无界输入的系统都可能过载。
Vouchsafe 评估器提供了两种不会改变模型的实用缓解措施：

- **基于信任根的提前拒绝**。 如果令牌集中不包含由验证者可信集合中的任何身份签发的令牌，评估器可以在构建完整图之前提前失败。
- **基于请求的能力进行范围限定的搜索**。 评估从目标令牌和请求范围开始，并在任一路径上只要累积范围变为空或彼此不相交，就立即停止。无法促成成功结果的令牌和路径不会被完全探索。

在实践中，许多部署会倾向于采用足够小、能够高效评估的委托结构。独立于典型使用模式，实现可以对令牌集大小、索引工作量或图探索深度施加保守限制，以约束对抗性环境下最坏情况下的资源消耗。这类限制属于运营层面的防御措施，用于限制提交给 ZI-CG 评估器的工作负载。

除了单纯的令牌数量之外，对手还可能尝试构造会最大化遍历深度或延迟范围消除的病态委托结构，例如冗长且受到严格削弱的委托链。这些情况代表了任何基于图的授权系统的最坏情况输入。ZI-CG 不会在模型层面消除这类情况，但其严格的范围削弱语义使评估器能够在不改变正确性的情况下，提前剪除不可行的路径。

这些策略降低了评估对抗性令牌集的成本，但拒绝服务仍是实际部署时需要考虑的问题。 or
实现。

6.5 密钥泄露与身份销毁

如果攻击者获取了与某个身份签发者对应的私钥，就可以签发任意新令牌，使其看起来像是源自该身份。与所有基于签名的系统一样，这代表着彻底泄露：对于任何尚未收到矛盾声明的评估器而言，攻击者与合法身份将无法区分。

泄露受信根 身份的后果，在性质上比泄露下游身份严重得多。如果攻击者获取了验证者的受信主体集 R 中某个身份的私钥，就能签发新的证明和背书，从而引入以该受信身份为根的全新委托路径。这些路径可能会授权第三方声明或能力，而合法发行者绝不会认可这些内容。

ZI-CG 提供了一种有助于缓解密钥泄露的机制。密钥已泄露的身份可以签发销毁令牌。指定 iss 的 vch:burn 令牌会彻底终止一个身份。一旦出现此令牌，该身份签发的所有声明都会从 T_{clean} 中移除，从而阻止过去和未来的令牌继续被使用。销毁是唯一能够彻底阻止泄露的密钥继续影响评估的操作，包括阻止其从受信任的根引入新的委托路径。销毁被刻意设计为不可逆：一旦观察到销毁令牌，之后的任何声明都无法恢复对该身份的信任。
由于销毁令牌本身也是普通的签名声明，获得私钥的攻击者也可以签发有效的销毁令牌。这会产生一种有趣的双重效应：

- 拒绝服务：合法所有者失去使用该身份的能力，且无法恢复；
- 自我限制效应：攻击者也会同时摧毁自己继续滥用已泄露身份的能力，因为观察到销毁令牌的评估器会排除所有后续声明。

这种二元性直接源于 ZI-CG 的语义：一旦私钥泄露，模型便无法区分合法签发与恶意签发。因此，身份销毁既是攻击，也是缓解措施。任何撤销策略都无法恢复对该身份的信任，而 ZI-CG 中也没有任何机制可以“收回”该身份。

有意不设任何机 制允许某个身份终止另一个身份；身份销毁只能由身份自身签发。 ct.
销毁令牌的实际效果完全取决于其传播。未收到该令牌的评估器会继续将泄露身份先前的声明视为有效。这反映了任何仅依据本地可用签名数据建立信任的系统所固有的局限。

部署方可以选择限制高权限身份的使用、缩短令牌生命周期，或积极传播销毁令牌，以缩小漏洞窗口。然而，底层原则不变：密钥泄露会不可逆地摧毁身份，只有销毁令牌——无论由合法持有方还是攻击者签发——才能终止其权限。

6.6 确定性与一致性

由于所有信任相关状态都编码在令牌中，并且图构建和能力评估都是以下各项的纯函数：

- 清理后的令牌集 $T_{\text{清理}}$，
- 验证者的受信主体集 R，以及
- 请求范围 $s_{\text{请求}}$，

对于相同的输入，任何两个正确的实现都会得出相同的结果。其不依赖于任何隐藏的网络状态、同步时钟或外部注册表。

这一特性有两个安全后果：

- **分区之间的一致性**。 看到相同令牌集的不同验证者，即使处于断开连接或对抗环境中，也会得出相同的信任决策。

- **可审计性**。 通过对记录的令牌集和配置重新运行评估，可以重建并审计信任决策。由于不存在外部依赖，此类审计具有可复现性。

确定性无法阻止对手扣留令牌，但它能确保验证者之间的任何分歧都可由他们所见数据的差异解释，而不是由模型中的歧义造成。

6.6.1 信任根配置错误

受信主体及其关联根范围的选择，是每个验证者作出的本地策略决策。如果验证者为受信身份分配了过于宽泛的根范围 s_r，ZI-CG 评估将通过有效的委托路径，在 s_r 内如实传播权限，从而可能授予非预期的能力。

如第 4.6.1 节所定义，信任根始终配置为成对的 $(i,\ s_r) \in R$，并且 s_r 明确限定了身份 i 所获信任的能力范围。任何身份都不会被默认视为在所有作用域内受信，因此 ZI-CG 不允许无界信任根。所有授权结果均受验证者所选根范围的限制。

ZI-CG 通过沿每条委托路径强制执行范围衰减，并使令牌集中的所有信任关系都清晰明确且可审计，从而减轻此类错误配置的影响。然而，它无法阻止验证者选择比预期更宽泛的根范围。根据设计，错误的信任根配置会导致授权决策出错，而非模型失效。

在实际操作中，可通过为可信根谨慎设计范围，并针对支撑授权决策的令牌集审计这些决策，来应对这一风险。

6.7 令牌分发与残余攻击面

ZI-CG 模型有意将信任评估与数据可用性分开。本文中的所有正确性属性，均以验证者实际持有的令牌集 T 为前提。这消除了评估循环中的在线依赖，但并未解决令牌分发问题。相反，令牌分发成为剩余的主要攻击面。

6.7.1 针对分发的攻击

控制令牌传输或存储信道的对手可以尝试发动以下几类攻击：

- **压制：** 阻止某些令牌的送达，尤其是会减少或撤销先前授予的能力的销毁令牌或撤销令牌。

- **分区：** 确保不同的验证者看到全局令牌集的不同子集，从而产生彼此不同但在本地保持一致的信任决策。

- **延迟：** 减缓新声明的传播，使一些验证者继续依据过时信息运行。
- **泛洪攻击：** 提供数量极大或经过精心构造的令牌集，试图耗尽验证者资源，详见第6.4节。

这些攻击都无法使验证者接受签名或身份绑定无效的令牌，也无法改变验证者已持有的令牌的含义。它们的作用仅限于在评估时影响**哪些有效令牌可用**。

该模型将用于分发令牌的机制视为范围之外。部署可以采用任何传输或存储机制，只要能够满足应用程序对可用性和及时性的要求。分发不会影响令牌有效性，但可能决定验证者在多长时间内使用不完整的令牌集运行。

6.7.2 以参与者为中心的呈现模型的影响

尽管分发仍然是一个攻击面，ZI-CG 以参与者为中心的结构显著限制了成功攻击所能造成的影响。

在典型部署中，寻求授权的实体会出示用于证明其请求的能力合理性的令牌。评估器从参与者提供的这组令牌开始，并可选择将本地持有的令牌（例如撤销令牌或销毁令牌）纳入其中。这会带来三个重要后果。

第一，**扣留令牌不会增加权限**。T_{clean} 中的所有能力都必须有明确的委托链作为依据，且委托具有递减性。省略令牌只会减少可能的授权证据，而不会产生新的授权。无法通过隐藏信息来构造额外特权。

第二，能产生实质影响的主要分发攻击，是**压制或延迟发送撤销和销毁令牌**。如果撤销令牌或销毁令牌始终未能送达验证者，该验证者可能会继续接受签发者原本打算撤回的先前委托。即使如此，这种攻击的影响也有限：

- 它无法扩展现有背书中最初授予的权限。
- 它无法沿任何路径扩展作用域；只能阻止这些作用域更早地被缩减。
- 一旦验证者的令牌集内存在销毁或撤销令牌，其效果便根据评估规则确定性地产生，且不依赖任何进一步的基础设施。

第三，参与者会自然地受到激励，提供支持所需操作的启用令牌。未能提供完整链条只会导致拒绝。参与者无法通过省略自己的令牌来获得额外能力，因为链条中的任何缺失环节都会使该链条无法使用。

在许多部署中，验证者会维护自己的禁用令牌存储库（销毁和撤销令牌）。这些令牌可以通过任何便于应用程序使用的分发机制获取，并且只会相对于参与者提供的令牌集移除权限。这种混合方式保留了零基础设施评估语义，同时进一步限制了参与者或其控制下的中介机构对撤销抑制的影响。

6.7.3 残余风险总结

综上，这些属性意味着：

- 剩余的攻击面在于令牌分发的**完整性和及时性**，而不在于评估过程的正确性。

- 成功的分发攻击可以**延迟或阻止现有权限的减少**，但无法创建新的能力，也无法将作用域扩展到最初委托且尚未撤销的范围之外。
- 验证者之间信任决策的差异，可归因于它们所接收的令牌集不同，而非模型存在歧义或依赖可变基础设施状态。

ZI-CG 通过将信任决策固化到签名的内容绑定令牌中，并采用确定性本地评估，缓解了广泛依赖可变状态或基础设施介导的信任重写的攻击。残余风险集中在密钥泄露和令牌可用性上。虽然撤销和销毁令牌提供了撤回权限以及终止受损身份的方式，但在对抗性密钥盗窃，以及会阻止及时向必须应用这些令牌的验证者交付撤销和销毁令牌的压制、延迟或分区情况下，这些风险仍然存在。

7 潜在应用

ZI-CG 模型仅利用评估器可获得的令牌集，即可提供可离线验证的身份、委托和撤销功能。本节重点介绍三类具有代表性的系统，在这些系统中，ZI-CG 消除了依赖基础设施的信任模型所存在的结构性失效模式，从根本上改变了可行或可靠的方案范围。

7.1 断连与对抗性环境

ZI-CG 无需网络访问、同步时钟或与外部权威机构联系，即可进行信任评估。身份和授权所需的全部信息都由所呈现的令牌携带，并在本地完成评估。这支持在连接间歇性中断、不可靠或被有意禁用的环境中运行。

灾害响应、临时野外作业、物理隔离设施，以及遭受审查或基础设施干扰的环境中，都会出现此类情况。在这些情境下，传统授权系统可能失效，因为信任决策依赖于连接基础设施，而这些基础设施可能已退化、不可信或无法访问。

在这些情况下，人们往往还需要跨越行政或组织边界进行协调，却通常没有预先建立联邦或共享信任基础设施。ZI-CG 支持此类协调，同时保留对信任决策的本地控制。
通过将信任决策固化为签名的内容绑定令牌，并采用确定性的本地评估，ZI-CG 使访问控制、委托和撤销即使在通信中断时也能继续运作。

7.2 无可信信道的自验证声明

ZI-CG 系统中的证明包含验证其来源和完整性所需的全部信息，因此任何验证者都能在离线状态下、无需第三方确认即可验证声明。此类证明可通过任何机制分发，包括不可信网络、公共信道、物理介质，或二维码等印刷形式。

这些特性支持在离线或不受信任的环境中传递可验证的真实信息。代表性用途包括将真实声明与数字资产或实物资产关联，以及用于无法或不希望进行在线验证的库存管理或供应链工作流程。在这些场景中，声明可以在本地记录、离线审计，并在之后同步，而不会削弱原始证明所提供的信任保证。

7.3 无需中央权威机构的去中心化委托

ZI-CG 支持参与方之间在限定范围内进行受限委托，无需中央权威机构、全局命名空间或共享信任基础设施。权限通过明确的签名声明来表达，任何持有相关令牌集的评估器都可以独立验证这些声明。

这种委托模型非常适合点对点和去中心化应用，在这些场景中，参与者必须授予和行使有限权限，而不依赖集中式访问控制服务。在 ZI-CG 系统中，一个身份可以通过签发担保令牌向另一个身份委托权限；该令牌本身还可以根据衰减和撤销规则进一步委托。每个参与者都在本地评估有效权限，无需联系委托方，也无需依赖全局可信的铸造方或解析器。

信任关系可以通过可移植令牌动态建立、约束或撤回，使去中心化系统能够适应参与者和角色的变化，而无需将集中式基础设施引入信任路径。

8 局限性与未来工作方向

零基础设施能力图（ZI-CG）模型有意保持狭窄。它聚焦于自验证身份、可验证声明、能力委派与衰减、撤销，以及基于一组令牌的确定性评估。本节介绍由此产生的局限性，并概述可进一步探索其他机制或互补层的方向。这些局限性并不削弱模型内评估的正确性，而是界定了应当如何理解和部署 ZI-CG 的边界。

8.1 未规定分发模型

ZI-CG 未规定用于发现、分发或存储能力令牌的任何机制。这确实是一项局限性：应用程序必须决定如何将令牌传递给评估器。不过，这也是模型有意保留的一个方面。通过仅定义信任评估语义，ZI-CG 将分发问题与授权正确性分离开来。

这种分离具有实际和研究层面的意义。在部署时，系统可以根据自身环境选择合适的分发方式，从简单的文件传输到更复杂的同步方案。在研究方面，ZI-CG 提供了稳定的评估基础，可与实验性的分发和同步模型结合使用。这样便能固定评估过程，从而将信任行为的变化直接对应到分发参数的变化。功能完备的 JavaScript 实现降低了开展此类实验的门槛，使研究人员仅凭现代网页浏览器即可进行这些研究。

8.2 缺乏全局、实时的正确性保证

ZI-CG 模型保证针对给定令牌集进行确定性评估。它并不试图提供全球同步的世界视图，也不对授权或撤销编码任何关于单一且最新的全球真相的概念。

需要更强新鲜度或全局一致性保证的系统，必须将 ZI-CG 与相关机制配合使用，以获取、维护并向每个评估器提供适当的令牌集。

进一步探索同步机制，或可发现一些模式，在与 ZI-CG 离线优先评估模型保持兼容的同时，提供更强的一致性保证。

8.3 不含时间语义的生命周期管理

ZI-CG 有意将时间排除在模型之外。它不引用时钟、时间戳、过期时间窗口或新鲜度保证。这样一来，在计时基础设施可能不可用、不可靠或存在争议的环境中，仍能保持确定性评估。

当存在可靠的本地时间概念时，应用程序可以将时间约束作为外部策略叠加在 ZI-CG 之上。然而，ZI-CG 本身定义能力语义时不嵌入生命周期语义，从而避免依赖同步时钟或全局时间一致。

零基础设施环境中的信任期限和过期问题仍属于应用层面的考量。通过非时间性或粗粒度时间性方法来限制权限，仍是有待进一步研究的开放课题。

8.4 身份与主体：绑定与连续性

ZI-CG 身份是密码学上自验证的参与者。该模型描述了此类身份如何作出声明、委托、削弱或撤销能力，以及评估器如何验证这些断言。它并未涉及身份如何对应现实世界主体，也未定义密钥轮换、继承或连续性机制。

这种区分是有意为之。一方面，它实现了一种简洁且可移植的主体绑定形式：任何控制相应私钥的主体，都可以在能够出示签名声明的任何场合，声明对该身份的所有权。另一方面，需要对主体连续性、恢复、继承或轮换作出更强保证的应用程序，必须在 ZI-CG 模型之外定义这些机制。

对于有此需求的应用程序，如何在保留 ZI-CG 零基础设施假设的同时，将长期主体绑定到密码学身份，仍是有待进一步研究的开放课题。

8.5 范围定义的表达能力

ZI-CG 刻意采用了一种简单的能力范围模型：每项能力都表示为一个文本字符串，并通过委托链上的集合交集来实现衰减。这种设计使评估完全具有确定性，并确保随着背书的组合，权限只会减少。

尽管这种简洁性带来了清晰的结构和强大的安全属性，但也限制了能力定义的表达能力。许多现实世界中的授权领域涉及结构化或参数化能力、数值约束，或无法轻易映射为扁平字符串的上下文敏感权限。

虽然许多此类约束可在应用层处理，但仍有机会探索更丰富的范围表示，在保留 ZI-CG 核心不变量——确定性、单调衰减和无基础设施验证——的同时，允许对权限进行更复杂的描述。未来研究可以探讨如何在不损害这些保证的前提下引入额外的表达能力。

8.6 面向用户的标识符与消歧

ZI-CG 并不试图定义一个全局且具有人类可理解意义的命名空间。这是有意为之：该模型关注的是自验证身份及其密码学语义，而非这些身份如何命名、显示或由人类解读。全局唯一性由完整身份字符串保证；面向用户的表示则留给应用程序处理。

随着基于密钥的标识符日益普及，实际系统必须解决面向人的消歧问题。原始密码学标识符不适合直接由人进行比较，而且该模型并未规定应如何在用户界面中为身份添加标签、注释或加以区分。

面向人的消歧方法，例如命名方案、上下文标签，或根据标识符生成的可视化表示，都与 ZI-CG 兼容，但仍不在其范围之内。如何理解此类机制在不损害自验证身份的安全性或信任语义的前提下，提升易用性，仍是有待进一步研究的开放问题。

8.7 与基础设施丰富的系统集成

ZI-CG 中的“零基础设施”要求专门针对评估器：信任决策所需的所有信息都必须包含在所提供的令牌集中。虽然 ZI-CG 支持离线信任系统，但该模型并不限制评估器所处的更广泛系统。ZI-CG 风格的语义与在线部署兼容，也可与目录、分发服务或策略引擎共存，而不改变核心评估保证。

这为未来研究提出了一个互补方向：如何将 ZI-CG 信任语义纳入传统在线系统。自验证且可组合的令牌或许能减少对权威中介的依赖、提高可审计性，或简化分布式授权逻辑。反过来，在线基础设施可以高效传播 ZI-CG 令牌，同时在评估时保留离线可验证性。

总结
上述局限性直接源于 ZI-CG 的设计目标：定义一个完全基于自验证声明的完整离线优先身份与信任模型。所指出的大多数领域体现的是有意设定的边界，而非功能缺失。通过将模型限定于本地可验证声明和确定性评估，ZI-CG 在受限或对抗条件下仍能保持简单、易于分析且稳健。

未来工作自然聚焦于探索如何更好地支持并扩展这一离线优先信任基础层，包括分发与同步模型、有效期和过期的替代方案、更具表达力且具确定性的范围语义，以及面向用户的密钥派生身份系统消歧技术。ZI-CG 将信任评估与这些问题解耦，因此可以独立研究和演进这些机制，而不与核心信任模型纠缠或重新定义它。

9 结论

大多数现代身份与授权系统都依赖在线基础设施：解析器、目录、撤销服务和同步时钟。而在最需要安全协作的环境中，这些假设恰恰难以成立，包括受损网络、遭入侵的基础设施和断网现场作业。本文表明，身份与信任并非必须依赖此类服务。通过将身份视为自验证的公钥绑定标识符，并将授权建模为由签名能力声明构成的图，零基础设施能力图（ZI-CG）模型使信任决策取决于数据，而非基础设施。

我们将 ZI-CG 形式化为一种能力系统，基于不可变的内容寻址令牌，并具备单调衰减、显式撤销以及针对给定令牌集的确定性评估。随后，我们在 Vouchsafe 实现中实例化了这一模型，展示了如何利用当代密码学实现必要的基本机制，并将其部署于网页浏览器和通用计算设备等常见环境中。

安全分析表明，在标准假设下，ZI-CG 能抵御针对传统基础设施的一系列结构性攻击，包括解析器失陷、可变目录状态和静默凭证改写，同时明确列出剩余攻击面，以便进行审计。

从概念上讲，ZI-CG 及其 Vouchsafe 实例对“在线基础设施是必要信任根”这一假设提出了挑战。核心问题在于，授权关系的全部可验证状态（包括签发和撤销）能否编码进签名令牌中，使评估器只需依赖所提供的令牌集和本地策略，而无需依赖外部服务。在此模型中，评估器只需令牌集和本地策略配置，就能在网络中的任何位置，甚至完全脱离网络，得出相同的决策。该模型与实现共同证明，完整且独立于基础设施的信任基础层在理论上是可靠的，在实践中也是可实现的。

未来工作仍有许多机会，包括探索更丰富的能力词汇、与零基础设施运行相兼容的生命周期语义，以及面向大规模部署的专用分发机制。这些都是在核心 ZI-CG 模型基础上自然延伸的方向。ZI-CG 及其 Vouchsafe 实例提供了一套完整且自包含的评估引擎，应用程序如今即可采用。我们希望这项工作能为进一步研究，以及构建即使在基础设施缺失时仍能保持信任属性不变的系统奠定基础。

10 个制品

本文提出的 ZI-CG 模型已在开源的 Vouchsafe 规范和参考实现中得到完整实例化。

- **Vouchsafe 规范 (v2.0.2)：** [13]
  https://doi.org/10.5281/zenodo.18012080
- **Vouchsafe JavaScript 实现 (v2.0.2)：** [14]
  https://doi.org/10.5281/zenodo.18012093

两个制品均以 BSD 三条款许可证发布。参考实现发布在 npm 上，适用于 or 在浏览器和服务器中使用 r 环境。

11 致谢

感谢 Tom Vilot，他以友善却持之以恒的怀疑态度，与我进行了坦诚且求真务实的讨论，尤其是在本项工作的早期阶段。这些讨论促使我更清晰地阐述观点，并提升了后续定义和说明的精确性。

我也由衷感谢我的妻子 Rebecca Kuri。她的耐心、鼓励和始终如一的支持，使这项工作得以完成。在工作的多次迭代中，她始终愿意倾听；在需要时，她也坚持让我保持平衡。这些都对我坚持完成这项艰巨而漫长的工作至关重要。

引用

[1] David Cooper、Santosh Santarosa、Stephen Farrell、Simon Josefsson 和 Russ Housley。《互联网 X.509 公钥基础设施证书和证书吊销列表（CRL）配置文件》。载于*RFC 5280*（互联网标准）。IETF，2008年5月。[2] Alexander Ulrich、Ralph Holz、Peter Hauck 和 Georg Carle。《调查 OpenPGP 信任网络》。载于 Vijay Atluri 和 Claudia Diaz 编，《style id='5'>计算机安全——ESORICS 2011，第 489–507 页，柏林、海德堡，2011年。Springer Berlin Heidelberg。[3] W3C DID 工作组。《style id='8'>去中心化标识符（DID）v1.0，2022年7月。[4] Yuki Ezawa、Shohei Kakei、Yoshiaki Shiraishi、Masami Mohri 和 Masakatu Morii。《面向以用户为中心的资源共享的基于区块链的跨域授权系统》。《style id='11'>Blockchain: Research and Applications，4(2):100126，2023年。[5] Ronald L. Rivest 和 Butler Lampson。《SPKI/SDSI 中的证书链发现》。载于第*14*届 *IEEE* 计算机安全基础研讨会（*CSFW-14*）论文集，第 162–172 页。IEEE 计算机学会，2001年。[6] Ásgeir Gunnarsson Birgisson、Joe Politz、Úlfar Erlingsson、Atul Taly、Mark Vrable 和 Michael Lentczner。《Macaroons：用于云中去中心化授权的带上下文限制条件的 Cookie》。载于第*21*届网络与分布式系统安全研讨会（*NDSS '14*）论文集。互联网协会，2014年。[7] Biscuit 安全团队。《Biscuit 授权令牌规范》，2024年。官方参考文档。[8] Mark Samuel Miller。《健壮组合：迈向访问控制与并发控制的统一方法》。博士论文，约翰斯·霍普金斯大学，美国马里兰州巴尔的摩，2006年5月。[9] Michael Jones、John Bradley 和 Nat Sakimura。《JSON Web 令牌（JWT）》。载于*RFC 7519*（互联网标准）。IETF，2015年5月。[10] Michael Jones、John Bradley 和 Nat Sakimura。《JSON Web 签名（JWS）》。载于*RFC 7515*（互联网标准）。IETF，2015年5月。[11] Michael Jones 和 Joseph Salter。《JSON 对象签名与加密（JOSE）中的 CFRG 椭圆曲线 Diffie-Hellman（ECDH）和签名》。载于*RFC 8037*（信息性）。IETF，2016年1月。[12] Simon Josefsson。《Base16、Base32 和 Base64 数据编码》。载于*RFC 4648*（互联网标准）。IETF，2006年10月。[13] Jay Kuri。ionzero/vouchsafe：Vouchsafe 规范 v2.0.2，2025年12月。[14] Jay Kuri。ionzero/vouchsafe-js：Vouchsafe JavaScript 库 v2.0.2，2025年12月。