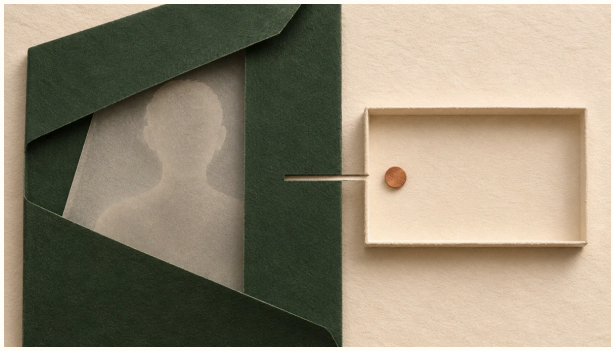


观点与分析

编辑日期: 2026年10月8日

证明你是谁，却不必告诉我你是谁

当一条更小的事实已经足够

在加利福尼亚州，数字驾照可以比塑料卡片少告诉商家一些事情，也因此更有用。持证人向电子核验设备证明自己达到某个年龄；核验方可能只收到“已超过规定年龄”的确认，而另一些交易才需要更多身份资料。州机动车管理局同时说明，数字驾照目前仍只在部分场所和服务中使用。真正新鲜的并不是驾照从钱包搬进了手机，而是一个过去要靠姓名、照片、住址和出生日期共同回答的问题，如今可以由一条小得多的事实回答：此人的年龄符合要求。1

这看似只是把一份大文件缩小，实质上却是在重画知识的边界。商家真正需要知道什么？不是顾客的姓名、生日、驾照号码，也不是与购买毫无关系的住址。他需要的是一个在法律和技术上具有可接受可信度的判断：此人是否达到规则规定的年龄？旧设计把近乎完整的个人档案交给店员，再指望他忽略其中大部分内容。新设计则试图让系统能够看到的内容，恰好等于它获准知道的内容。我们不再只问数据收集后如何保护，还要问它为什么一开始就被允许进门。

“身份”一词也因此发生变化。在现代数字系统里，它承担着多种不同工作，只因习惯，我们把这些工作都塞进了同一个名称。开立受“了解你的客户”（Know Your Customer，KYC）要求约束的银行账户时，真实姓名及其核验可能不可缺少；参加正式考试时，机构也可能必须确认来者正是报名者本人。但要证明自己是获认可大学的学生、居住在有权享受某项服务的地区，或在进入设施前完成了强制培训，所需事实未必是一份完整的人生档案。区别并不总在“身份”和“匿名”之间，而在于究竟要知道一个人，还是只要知道他具备某项属性。

从卡片到凭证

2025年7月，欧盟委员会提出一套年龄核验技术蓝图，让成员国和数字服务能够在不披露多余身份信息的情况下构建年龄资格证明。该月，蓝图开始在不同国家、平台和用户群体中测试与适配。10月发布的第二版加入了基于护照和身份证的方式，并说明方案纳入了零知识证明技术。到2026年4月，欧委会称应用已在技术上就绪，面向公民的提供将在之后进行；丹麦、法国、希腊、意大利和西班牙被列为正在适配该方案的国家。这些是开发、测试和部署计划的事实，并不证明本文写作时所有欧洲人都已在使用它。2

这套欧洲蓝图的抱负远不止改善登录窗口。签发年龄证明时，签发方依据国家身份、护照或其他获认可的核验方式等可信来源；而证明的使用原则上应与签发机构分离，使后者不会因持有人每访问一个网站就收到通知。数字服务只请求年龄门槛证明，系统据此决定允许或拒绝访问。我们过去总把两件事混在一起：确认信息来源真实，以及只使用其中一小部分。把它们拆开看似是细小的技术安排，却能避免一个人仅因反复证明普通资格，就留下可集中拼接的生活记录。2

2025年5月，万维网联盟（W3C）通过《可验证凭证数据模型2.0》（Verifiable Credentials Data Model 2.0）。其基本思想是：可信机构以一种可核验完整性与来源的方式，对个人或实体提出一组声明。大学可以证明学位，专业机构可以证明执照，政府部门也可以确认其登记册中的某项资格。模型把三方称为签发方（Issuer）、持有人（Holder）和验证方（Verifier）。这并不是一座全球统一数据库；它让可信声明能够在系统各异的机构之间流转，前提是各方对凭证含义与签发权限有共同理解。3

但“可验证”并不是“真实”的同义词。标准本身提醒我们，能够验证凭证，不代表凭证中每项内容都符合现实。数字签名可以发现数据是否被篡改，也可以把数据与签发方相连；它却无法回到某个学年，确认持证人确实上过课，也无法叫来医生复核其签字的检查质量。若签发方数据库有误，错误信息也能装进极其精美的加密信封，稳稳地传向外部世界。因此，系统的起点是对机构及其流程的判断，而不只是挑选一种签名算法。3

选择性披露不等于不可关联

设想一份专业证书，包含姓名、出生日期、会员编号、认证日期和专业方向。一家工作平台只需核验某人是否持有特定专业的有效执照。第一种做法，也是行政思维最熟悉的做法，是发送整张证书；第二种是另发一份信息较少的版本；第三种则是让持有人拥有组合凭证，只披露此次交易要求的部分。这就是选择性披露（Selective Disclosure）。若他还能证明执照仍有效，或分数高于某个门槛，却不显示用于计算的原始数值，便进入了零知识证明（Zero-Knowledge Proofs）的范畴。这些不是可互换的营销术语，每一种都有不同的数学与安全边界。

2025年11月，互联网工程任务组发布RFC 9901，为签名JSON令牌规定选择性披露方式，即SD-JWT。签发方可以为不同字段生成加密摘要，持有人之后再决定向验证方展示哪些字段。例如，若字段从一开始就被设计成可独立披露，他可以证明“学生”身份，同时隐藏地址和电话号码。这确实减少了抵达对方的信息量；但它的名称和加密结构本身，并不能证明凭证的每一次展示都无法同此前的展示关联。4

市场上最隐蔽的误解正在这里发生。某应用可以因为不显示出生日期而声称尊重隐私，却在每次核验时发送同一个签名令牌或固定指纹，让两个合作网站能够相互比对。它们也许不知道姓名，却能知道在这里证明年龄的访客，与在那里证明年龄的是同一个人。RFC 9901明确指出这一限制：面对把原始凭证转交签发方的共谋验证方，SD-JWT这类基于加盐摘要的披露机制，无法保证签发方与验证方之间的隔离。字段被藏起来了，表面看不见的序列号却可能还在，足以替访客写出另一份履历。4

因此，设计者必须把三项性质分开。第一是数据最小化：验证方不应知道超出需要的内容。第二是不可关联性（Unlinkability）：两个验证方不能仅凭加密材料判断两次展示来自同一凭证。第三是持有人绑定（Holder Binding）：他人不能复制别人的凭证冒充自己的凭证。若第三项依赖一个各方都能识别的固定密钥，强化它可能削弱第二项。系统或许阻止了凭证共享，却追踪了每一次使用。这并非无解的矛盾，而是一组必须同时测试的设计条件；不能宣布在其中一项上获胜，就让其余问题闭嘴。

证明究竟证明了什么

最吸引人的数学方案并不从姓名开始，而从一道可以计算的命题开始。假设隐藏值代表出生日期，交易日期已知，系统要说服验证方二者之差达到许可年龄。简化地说：存在一个源自可信来源的原始值，使“核验当天年龄不低于十八岁”成立。只要证明可靠，验证方不必看到原值。但一个关键条件藏在其中：系统还必须证明隐藏的出生日期来自可信来源，而不是用户一分钟前自行填写。否则，我们得到的只是对一条虚构信息作出的漂亮数学证明。

零知识证明在理论上同时要求三点：命题为真时，验证方接受正确证明；没有正确见证者的人，除安全假设允许的极小概率外，不能说服系统相信假命题；证明不会泄露超出命题真假本身的隐藏见证。研究者分别称之为完备性（Completeness）、可靠性（Soundness）和零知识性（Zero Knowledge）。第三点并不表示“我已满十八岁”没有透露任何事实，只表示在相关数学模型中，证明不会泄露见证的其余部分。它也无法单独处理摄像头中的脸、网络地址或浏览器记录。5

并非任何可签名证书都能自动生成我们想要的任何证明。若签发方已经签发“年满18岁”这一属性，只展示该签名属性而不显示出生日期可能就够了；若签发内容只有出生日期，想在不透露它的情况下完成数值比较，就取决于密码方案、编码方式，以及如何证明签名与属性之间的关系。系统可能需要签发方派生的凭证，或适合这种计算的证明协议。在界面上贴上“ZKP”标签，并不会让任何条件的核验自动变得免费或可靠。工程难题不只是藏住数字，还要证明数字从何而来、它与条件有何关系、条件在何时有效。

2026年9月，W3C发布用于可验证凭证的BBS签名技术候选推荐草案。这些技术在按其性质正确使用时，可以生成只披露部分属性、且派生证明彼此不可关联的加密证明。9月文件不是最终推荐，而是处于实现测试阶段的草案。对一个喜欢把新兴技术包装成完整共识的市场而言，这个区别十分重要。即使加密材料本身具有很强的不可关联性，若用户随证明提交唯一信息，网站在浏览器里放入重复标识符，或协议之外仍保留另一条关联线索，应用层的使用仍可能被串联。6

当语境揭开加密遮住的内容

从证明走向具体的人，画面会再次变化。一个小型大学的学生若披露自己就读罕见专业、毕业于某一届，即使证明不含直接身份，两条真实信息也可能足以推断出姓名。又如一个三人团队中的员工证明自己有资格访问敏感系统，职位和时间也许已足以识别使用者。算法没有遭到攻破，是交互暴露了过窄的语境，把未知变成已知。衡量隐私不能只数数字卡片上留下多少空栏，还要看披露之后，持有人仍能混同于多大的群体。

还有一种知识更安静。网站也许不知道姓名和生日，却知道网络地址、设备类型、操作方式与访问时间；它也可以使用画像或商业分析组件，把本次登录与过去的活动相连。强协议能防止机构跨域关联加密证明，却不能阻止机构用其他方式追踪访客。反过来也一样：一个不具备数学不可关联性的凭证系统，仍可能拥有优秀的网络保护和数据留存制度。隐私不是某个软件库颁发的证书，而是要在服务的每一端共同测量的性质。

撤销、持有与“实时状态”悖论

当我们追问签发方时，欧洲蓝图的思路更清楚了。若平台在每次访问时都必须联系年龄凭证的签发机构，签发方就可能成为用户习惯的旁观者。离线核验，或精心设计的公钥与状态列表，可以缓解这一问题。然而凭证可能被撤销或过期，手机可能遗失，密钥也可能遭窃；验证方必须知道证书是否仍然有效。美国国家标准与技术研究院（NIST）2025年修订版指南要求属性包必须提供撤销方式，并建议设置有限有效期；同时警告，撤销状态核验服务不应让签发方得知某个特定凭证被某项特定服务使用。7

这便是“实时状态悖论”。我们希望证书无需联系签发方即可核验，避免它变成监视工具；同时又希望设备失窃、资格改变或执照撤销时，每个验证方都能立刻得知。不存在一种魔法，同时实现零通信、零撤销延迟和无人保存状态。现实只有架构与取舍：短有效期、不直接识别个人的公共状态账本、合适的未撤销证明、恢复与重发机制，以及因服务而异的风险边界。当机构宣传凭证“永不联系签发方”时，我们应追问：它怎样知道凭证昨天没有被撤销？

紧接着还有一个更实际的问题：站在手机屏幕前的是谁？若成年人取得年龄证明后转发给未成年朋友，协议的隐私性并不能挽救核验目的。因此，一些设计把凭证持有权绑定到受保护设备内的私钥，并要求钱包针对验证方发出的唯一挑战重新签名。随机数挑战（Nonce）降低旧消息被重放的可能，把响应绑定到特定接收方，则能防止给商家的证明被拿去另一平台使用。这些措施限制冒用和重放，却无法在没有其他手段的情况下确认，握着设备的人就是最初接受核验的那个人。78

加州实践在这里再次有意义，不是因为它抵达了理想终点，而是因为它把核验放回正确位置。机动车管理局强调，数字驾照并非卡片图片，展示应通过电子核验完成；它还建议用户不要简单地把驾照屏幕交给对方肉眼查看。商家与服务人员真正要做的是配备兼容读取工具，理解请求和接收的内容，并演练手机故障或读取器不可用的情形。如果钱包里的驾照尊重隐私，设备一坏，店员却要求用户交出完整证件照片，这种隐私还有什么意义？1

从实验室走向机构

我们可以设想更广泛的应用，但必须承认它们是设计假设，不是已经发生的成果。只面向学生的实习网站可以请求一所获认可机构签发的有效学籍证明；处理敏感数据的研究中心可以要求证明已完成近期伦理课程，而无需复制带编号的完整证书；若资格仅由地址属于某行政区决定，城市可以向该区居民提供福利，而不询问精确门牌；行业协会也可以确认从业者执照有效，却不披露另一份证件号码。在这些例子里，成功的标准是签发一个适合特定决策、可被核验的属性，而不是先复制整份文件，再删去不喜欢的内容。

涉及金钱的系统很快会暴露口号的边界。在要求客户尽职调查的法域内开立银行账户时，银行不能用一句抽象的“此人年满十八岁”，替代其依法识别客户身份的义务。金融行动特别工作组（FATF）2020年3月发布的数字身份指南指出，在“了解你的客户”流程中使用数字方案，取决于身份系统的可靠程度与金融关系的风险；数字核验是提高合规准确性的工具，而不是逃避尽职调查的捷径。机构仍可以少收集交易不需要的属性，也可让另一方核验次级资格，而不再次披露全部细节。隐私不是忽视义务，而是知道义务从哪里开始、收集欲望在哪里结束。9

这也会改变企业竞争的结构。平台过去以“方便核验”为由，收集每个用户的生日、地址和证件副本，实际上是在积累一个巨大而危险的信息资产，其中许多内容也许根本不是服务所需。每多一条记录，机构就要保护它、规定留存期、解释用途，并在适用制度要求时，在泄露后通知主管部门或个人。信息从营销燃料变成伴随机构多年的责任。只接收可信资格证明的一方可以缩小数据攻击面，但仍必须保护核验日志、会话限制和留存的欺诈事件。这里的经济问题并不只是删掉数据库，而是在知识责任变成安全事故之前，选择机构愿意承担什么。

欧盟规则也因此具有实际意义。2024年11月关于欧洲身份钱包的实施条例谈到，只向获授权方传输最低必要数据，并将不同交易分离以降低关联性；它还把属性请求和请求方核验纳入已知框架。并非技术独自说服企业不要索取姓名，而是注册与治理方式允许人们追问：请求方是否有正当理由索取它？技术标准提供手段，制度规则决定何时、在何种边界内使用。10

签名再强，也无法消除社会层面的约束。没有新手机的人怎么办？设备与密钥遗失怎么办？因登记资料冲突而无法取得原始证件怎么办？不愿把私人手机交给雇主的人怎么办？若“隐私保护的默认设计”成为进入公共服务的唯一通道，它也可能变成新的排斥之门。系统需要获承认的替代路径，需要既安全又不会被欺诈者接管的恢复流程，需要纠正来源错误的机制，也需要明确谁应为拒绝有效证明负责。这些并不是密码学论文之外的温柔点缀，而是系统离开实验室后仍能成立的条件。

机构可以被看作问题的发布者，而不是关于人的事实的收藏者。每次交互，系统都在问：这个人现在是否有权做这件事？问题越明确，答案越可能被限制在必要范围；问题越含糊，数据清单就越容易因“以防万一”而膨胀。因此，建设尊重隐私的服务，第一步不是选择钱包或采购加密证明，而是拆开决策本身：什么属性会改变结果？谁有权证明它？有效多久？只知道属性存在是否足够，还是为了防止一项权利被重复领取，必须识别具体个人？

最后一个问题揭开补助与一次性权利的设计难题。机构也许既想确认申请人有资格领取一次补助，又不想建立一份能跨服务追踪其活动的总档案。单纯证明“有资格”，并不能阻止同一个人提交十次。可以设计仅在本项目内有效的假名标识或一次性令牌，但该标识不能反过来成为全球追踪钥匙。一些密码方案支持特定作用域的假名，BBS草案也讨论了其派生方式。然而公共服务中的真正设计任务，是在项目内防止重复领取，同时保持项目外不可关联，并允许当事人复核错误。无法执行规则的保密会削弱公众信任；没有边界的执行则会削弱隐私。6

披露预算

为了不让这些原则沦为公关用语，我提出一项初步工程测试，称为“披露预算”。它不是现有监管标准，也不是已发表的实验结果，而是一套可检验的设计框架。机构先用一句话写明要作出的决定，再为每项属性列出：必要性、来源、谁能看到原值、谁只能看到证明、留存多久、不同使用能否被关联。随后做两轮对抗测试：先汇总虚拟验证方的记录，寻找重复线索；再假设其中一方与签发方合作，检验能否从展示痕迹锁定特定持有人。最后测试撤销凭证、手机遗失、请求重放与网络失败。字段减少并不等于成功，如果另一条固定痕迹仍然允许追踪。

最重要的指标也不能只是“有多少用户完成核验”。还应测量：在不披露多余信息的情况下作出正确决策的比例；有效证明被拒的比例；虚假声明被接受的比例；撤销传播所需时间；被迫退回完整证件披露的案例比例；以及在特定威胁模型下，验证方之间实现关联的可能性。样本还应覆盖配置较低的设备，以及年龄、数字技能不同的用户。系统可以通过密码学测试，却在服务测试中失败；界面也可以非常顺滑，却让伪造凭证比纸张时代更快获得信任。

随着这些系统成熟，一个新市场会出现，但它不应是“出售新身份”的市场。有人专门签发属性证明，有钱包保护持有人的密钥，有验证方管理属性请求策略，也有机构维护信任标准和获认可机构的密钥，还有工具评估隐私并测试抗欺诈能力。真正值得构建的价值，不是知道更多关于人的事情，而是能够依赖更少的知识。这也解释了为何发布一款写着“去中心化身份”的漂亮应用还远远不够。钱包可以在用户手机上，所有决策却仍被一家运营者垄断的白名单控制；签发方也仍可能在每次使用时收到信号。存储位置去中心化，不代表决策权也已去中心化。

还有一种哲学诱惑需要抵抗：有人会说，最尊重人的系统应当对他一无所知。但负责任的服务有时确实需要可验证事实，也需要明确的问责。目标不是让每位公民变成幽灵，而是让机构拥有的知识，与它管理的权利或风险相称。有些门前，姓名是正当条件；另一些门前，知道姓名只是没有功能的知识越界。我们也不能让零知识证明承担解决所有法律与社会冲突的承诺。它的力量在于扩大数学上可证明、同时不必披露全部见证的范围；至于应该证明什么、向谁证明、谁有权提出要求，密码学无法单独作答。

机构的克制

加州数字驾照讲述的是从暴露整张卡片向只呈现所需属性的部分转变。欧洲尝试讲述的是：机构希望把信任签发与使用监视分开，同时经历仍不应被夸大为全面完成的开发与部署阶段。SD-JWT提醒我们，选择性披露未必意味着凭证不可追踪；BBS工作则指向更深一层的展示痕迹保护，但必须区分草案与最终

标准。NIST指南又提醒我们，撤销、密钥保护和错误处理不是身份系统的脚注，而是其真实性的一部分。这些案例并非在争夺“加密最多”的称号，它们只是逐层揭开一个长期被证件照片遮住的问题。

它们也可能带来数字系统里少见的美德：机构的克制。服务只询问足以让它作出决定的内容，并在抵达边界后停下。届时，最大的成就既不是人成功藏起姓名，也不是复杂证明在快速处理器前通过，而是机构学会区分核验的权利与求知的好奇。几十年来，我们一直在教设备如何到处认出我们。现在该教它更难的一课：在一件具体事情上相信我们，然后合上档案，把余下的人生还给本人。

来源与参考资料

[1] California DMV, Mobile Driver's License FAQs — 持续更新的官方页面；查阅于2026年11月9日。

[2] European Commission, Blueprint for an age verification solution — 第一版于2025年7月发布，第二版于同年10月发布；2026年4月宣布技术就绪；页面于2026年9月22日更新。

[3] W3C, Verifiable Credentials Data Model v2.0 — W3C Recommendation，2025年5月15日。

[4] IETF, RFC 9901, Selective Disclosure for JSON Web Tokens — 2025年11月发布；参见第4节与第10.1节。

[5] Goldwasser, Micali, Rackoff, The Knowledge Complexity of Interactive Proof Systems — SIAM Journal on Computing 18(1)，1989年2月。

[6] W3C, Data Integrity BBS Cryptosuites v1.0 — Candidate Recommendation Draft，2026年9月10日；并非最终Recommendation。

[7] NIST, SP 800-63C, Digital Identity Guidelines: Federation and Assertions — 2025年Revision 4最终版；参见第5.4节。

[8] OpenID Foundation, OpenID for Verifiable Presentations 1.0 — 2025年Final规范。

[9] FATF, Guidance on Digital ID — 2020年3月6日。

[10] European Commission, Implementing Regulation (EU) 2024/2982 — 2024年11月28日，见EUR-Lex。

[11] NIST, Zero-Knowledge Proof, Cryptographic Glossary — 官方术语资料；查阅于2026年11月。