

LEI：数字证书管理中的缺失要素

2020年8月25日，全球法人识别编码基金会（GLEIF）首席执行官 Stephan Wolf 发布文章《LEI：数字证书管理中的缺失要素-简单的整合如何能维护对未来数字经济的信任》¹，主要介绍了当前数字证书体系的缺陷及影响，提出将 LEI 集成到数字证书中的解决方案，并展望通过 LEI 实现的自动验证方案来解决不同数字系统间的身份信任问题。文章主要内容如下：

一、数字证书体系存在缺陷，信任系统易受到破坏

世界数字经济发展在很大程度上得益于数字证书的支持，通过数字证书使组织和个人的身份及活动得到认证，进而在数字化环境中得到商业伙伴的信任，但当前数字证书体系存在一些缺陷。一是法人实体通常持有来自不同证书方案和发行者的多个数字证书，身份认证信息被保存在全球范围内的多个独立数字系统中，证书之间缺乏“链接”，随着数字证书数量的增加，证书管理和维护所需要的时间和成本也随之增加。二是由于各系统使用各自本地语言等原因，使证书参考数据（例如名称，法律形式和地址）嵌入的文本字符串可能与证书发行者不同。在这种情况下通常需要进行手动检查，以确保所涉及的证书确实与内部数据库中交易对手的组织代表相匹配，且证书所包含的信息是最新的。三是法人实体发生名称、地址等重要信息变更时，需吊销证书重

¹ 文章详见 <https://www.gleif.org/en/newsroom/blog/the-lei-the-missing-ingredient-in-digital-certificate-management>

新发放，如果下游应用程序无法访问相关的吊销列表，则过时的信息将被保留。**四是**法人实体更新证书不及时，导致多个数字系统中的证书信息不一致，信任系统因此受到破坏。

二、集成 LEI 到数字证书中来解决缺陷问题

LEI 是基于 ISO17442 标准的由字母及数字组成的 20 位字符代码，每个 LEI 都包含有关实体所有权结构的重要信息，回答了“谁是谁”和“谁拥有谁”的问题，这对于降低企业交易风险至关重要。如果在发行数字证书时将 LEI 集成其中，那么它可以成为数字证书之间的公共链接，这样所有与实体相关的证书记录都将被联系在一起，使每个人更加安全地参与到全球数字市场当中，并且降低了调查和验证客户、合作伙伴和供应商相关信息复杂性和成本。为了促进 LEI 在数字证书中的应用，全球 LEI 基金会一直与诸如国际标准化组织 (ISO) 和欧洲电信标准协会 (ETSI) 等标准制定组织开展密切合作。如果将 LEI 集成到数字证书中，很多问题将得以解决。

1. LEI 将提供精确的自动验证功能。随着物联网和区块链等新兴数字解决方案的应用，企业实体将会更加频繁的使用数字证书，特别是数字证书技术现在已经获得了监管单位的支持，数字身份因此具备了更高的可靠性和信任度，这将进一步刺激对 LEI 可以实现的自动验证功能的需求。

2. LEI 将提供一致的数字连接。目前不同的数字 ID 系统基于不同的标准、密钥和加密，它们之间唯一的公共链接是实体名称，实体名称可以随时间发生变化。如果数字 ID 系统之间没有

一致的数字链接，自动化验证方法将总是会产生错误。LEI 将完美地提供这种一致的链接，进而巩固了其在数字经济中的可靠地位。

原文链接：

<https://www.gleif.org/en/newsroom/blog/the-lei-the-missing-ingredient-in-digital-certificate-management>