# 火漆印章简史

四个世纪以来，一滴红蜡保证了无人读过信件。在向数字时代的过渡中，我们失去了这一点。它是可以恢复的。

## 在纸张出现之前

向远方某人机密传达信息的需求比文字的出现还要古老。在美索不达米亚，写有行政或私人信息的泥板被装入同样由泥土制成的外壳中，并在烘烤前密封：任何试图阅读内容的举动都会破坏外壳，收件人一眼就能看出外壳是否完好无损。在古典罗马，羊皮纸卷轴用绳子绑起来，并用蜡或铅密封。其理念始终如一：任何未经授权的阅读都必须留下不可磨灭的物理痕迹。

## 火漆印章时代

在中世纪末期到20世纪初的几个世纪里，欧洲机密通信的经典工具是折叠并用火漆印章密封的纸张。将熔化的蜡倒在纸张的接缝处，并盖上个人或机构的印章。这并非装饰。公证人、外交官、商人和个人都遵循相同的逻辑来使用它：如果火漆印章完好无损且印章清晰可辨，则内容未被阅读；如果它被破坏，信件在打开之前就已泄密。

火漆印章的力量不在于其昂贵或庄重，而在于其非常具体的结构特性：任何试图将其移除并重新贴上的尝试都会留下明显的痕迹。没有任何悄无声息地打开密封信件的方法。这意味着保密性不依赖于任何中间人——信使、马车夫或邮政官员——的承诺，而是取决于包装本身的物理设计。这是一种建立在证据基础上的信任，而不是任何人的言辞。

## 数字化过渡

电报、电话、电子邮件、企业即时通讯。电子通信带来了速度、全球覆盖以及几乎为零的单条信息成本，但同时也摧毁了火漆印章的保障。在默认情况下，每条信息都要经过中间人，而我们只能通过服务条款中写下的承诺、技术认证和不透明的审计来验证他们的诚信。不再有等同于破裂蜡滴的物理痕迹来警告我们。

## 数字火漆印章

赋予火漆印章力量的特性不是火漆印章本身，而是它所代表的意义：通过设计实现可验证的完整性，而无需信任第三方。这一特性可以在数字领域中重构，只不过需要两个元素而不是一个。第一个是加密印章——每篇本刊物文章底部出现的SHA-256散列字面意义上就是一个数字火漆印章：对内容的任何修改都会明显地改变散列，就像破裂的蜡会暴露未经授权的阅读一样。第二个是渠道架构：当两个通信的人之间没有服务器时，就不存在需要信任的中间人。这两个元素的结合——可验证的完整性和中间人的缺失——在数字层面上重现了四百年来折叠纸上红蜡在日常中所起的作用。

# 名称

本刊物名为Cuadernos Lacre，因为火漆印章不是一件历史装饰品，而是一种具体的数字特性：通过结构实现可验证的完整性，无需任何运营商的承诺。该系列中的每篇文章都在其当代数字版本中分析了同一理念的某个部分：加密、元数据、职业保密、通信架构、欧洲法律框架。这个名字也是一种提醒：保密性不是一种外包服务，而是信息流通渠道本身的一种属性。

## 来源及延伸阅读


- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 （关于密封泥板和美索不达米亚印玺的章节）。
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. 关于火漆印章作为完整性和作者身份工具的章节。
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. 火漆印章原则的现代阐述：保障应存在于端点，而不是渠道中。



下一页 →加密不等于隐私：元数据揭示了您的哪些信息


## 最近阅读


- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE


随身携带本文，以备不时之需。


↓ Markdown ↓ 纯文本 ↓ PDF


文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。


火漆印章 · SHA-256 ce028c9079d65d307292fb2909ceb72ac59b5159a1515e82d11f90bfc721d421

ES


Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。

本网站不使用 Cookie，也不加载第三方资源。它使用自托管的匿名访问者计数器（位于我们欧洲服务器上的 Umami），并仅使用最少量的 JavaScript 来处理您的亮色/暗色主题偏好。无追踪器，无画像分析，无数据共享。如需关注我们：RSS。