A brief history of wax sealing

For four centuries, a drop of red wax guaranteed that no one had read a letter. We lost it transitioning to the digital age. It is recoverable.

Before paper

The need to communicate something confidentially to someone far away is older than writing. In Mesopotamia, clay tablets with administrative or private messages were sent inside clay envelopes, sealed before baking: any attempt to read the content required breaking the envelope, and the recipient knew at a glance if the envelope arrived intact. In classical Rome, parchment scrolls were tied with string and sealed with wax or lead. The idea was always the same: that any unauthorized reading would leave an indelible physical trace.

The era of the wax seal

For several centuries, from the end of the Middle Ages well into the 20th century, the canonical tool of confidential correspondence in Europe was folded paper sealed with wax. Melted wax was poured over the fold and impressed with a personal or institutional seal. It was not ornamental. Notaries, diplomats, merchants, and private individuals used it with the same logic: if the seal was intact and the impression recognizable, the content had not been read; if it was broken, the correspondence was compromised even before opening it.

The strength of the wax seal was not in its cost or solemnity. It lay in a very specific structural property: any attempt to remove and replace it left visible traces. There was no silent way to open a sealed letter. And that meant that confidentiality did not depend on the promise of any intermediary—the messenger, the coachman, the postal officer—but on the physical design of the envelope itself. It was trust based on evidence, not on anyone's word.

The digital transition

The telegraph, the telephone, email, corporate messaging. Electronic communication brought speed, global reach, and almost zero cost per message. It also took away the guarantee of the wax seal. By default, every message passes through intermediaries whose integrity we can only verify through promises written in terms of service, technical certifications, and opaque audits. There is nothing equivalent to a drop of broken wax to warn us.

A digital wax seal

The property that gave strength to the wax seal was not the wax itself, but what it represented: verifiable integrity by design, without the need to trust a third party. That property can be reconstructed in the digital plane, although with two elements instead of one. The first is the cryptographic seal—the SHA-256 hash that appears at the bottom of every article in this publication is, literally, a digital wax seal: any modification of the content visibly changes the hash, just as broken wax betrayed unauthorized reading. The second is the architecture of the channel: when there is no server in the middle between two communicating people, there is no intermediary who

needs to be trusted. The combination of both elements—verifiable integrity and absence of an intermediary—reproduces, in digital terms, what red wax on folded paper did every day for four centuries.

The name

This publication is called Cuadernos Lacre because sealing wax (lacre) is not a historical ornament, but a specific technical property: verifiable integrity by construction, without the promise of any operator. Each article in the series analyzes, in its contemporary digital version, some part of that same idea: encryption, metadata, professional secrecy, communications architecture, the European legal framework. The name is also a way of remembering that confidentiality is not a service you hire, but a property of the channel itself through which the information flows.

Sources and further reading

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (chapters on sealing tablets and Mesopotamian bullae).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Chapters on the wax seal as an instrument of integrity and authorship.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Modern formulation of the wax seal principle: guarantees at the ends, not in the channel.

Next → Encryption Is Not Privacy: What Metadata Tells About You

Recent readings

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Take this article wherever you need it.

↓ Markdown ↓ Plain text ↓ PDF

The file is downloaded to your device. From there, you can save it, import it into Solo2, or share it as you wish. Cuadernos does not decide the destination for you.

Wax seal · SHA-256 ac6da496dd633eb5936fa3c170063a85630f764cdc56f657d523810813353d43

ES

Cuadernos Lacre · A publication of Menzuri Gestión S.L. ·
written by R.Eugenio · edited by the team of Solo2.