

Lakre-zigiluaren historia laburra

Lau mendez, argizari gorri tanta batek bermatzen zuen inork ez zuela gutun bat irakurri. Aro digitalera pasatzean galdu genuen. Berreskuragarria da.

Elkar ulertzeko: Gutun batek lakrea zuenean, edonork ikusten zuen zigilua ukitu gabe zegoen ala ez. Hautsita bazegoen, norbaitek zu baino lehenago irakurri zuen. Lau mende horrela. Aro digitalak ziurtasun hori bota zuen — eta gehienek ez zuten nabaritu ere egin falta zela.

Papera baino lehen

Urrun dagoen norbaiti zerbait isilpean komunikatzeko beharra idazkera bera baino zaharragoa da. Mesopotamian, administrazio- edo mezu pribatuak zituzten buztinezko tabletak buztinezko kapsula barruan bidaltzen ziren, egosi aurretik zigilatua: edukia irakurtzeko edozein saiakerak bilgarria apurtzera behartzen zuen, eta hartzaileak begiratu hutsarekin bazekien kapsula osorik iristen zen. Erroma klasikoan, pergamino-biribilkiak kordelarekin lotzen ziren eta argizariz edo berunez zigilatzen ziren. Ideia bera zen beti: baimenik gabeko edozein irakurketak arrasto fisiko ezabaezina uztea.

Lakre-zigiluaren aroa

Hainbat mendez, Erdi Aroaren amaieratik XX. mendean sartu arte, Europan korrespondentzia konfidentzialerako tresna kanonikoa papera tolestua eta lakre-zigiluz zigilatua izan zen. Argizari urtua pleguaren lotunean isurtzen zen eta zigilu pertsonal edo instituzional batekin inprimatzen zen. Ez zen apaingarria. Notarioek, diplomatikoen, merkatariek eta partikularrek logika berdinarekin erabiltzen zuten: lakre-zigilua osorik bazegoen eta zigilua ezaguna bazen, edukia ez zen irakurri; apurtuta bazegoen, korrespondentzia konprometituta zegoen ireki aurretik ere.

Lakre-zigiluaren indarra ez zegoen kostuan ezta solemnetasunean ere. Ezaugarri estruktural oso zehatz batean zegoen: kentzeko eta berriro jartzeko edozein saiakerak arrasto ikusgarriak uzten zituen. Ez zegoen zigilatutako gutun bat isilik irekitzeko modurik. Eta horrek esan nahi zuen konfidentzialtasuna ez zegoela bitartekari baten hitzaren mende —mezulariarena, kotxe-gidariarena, posta-ofizialarena—, baizik eta bilgarriaren diseinu fisikoaren mende. Ebidentzian oinarritutako konfiantza zen, ez inoren hitzean.

Trantsizio digitala

Telegrafoa, telefona, posta elektronikoa, korporazio-mezularitza. Komunikazio elektronikoak abiadura, irismen globala eta mezu bakoitzeko ia zero kostu ekarri zituen. Baina lakre-zigiluaren bermea ere ezabatu zuen. Defektuz, mezu oro zerbitzu-baldintzetan idatzitako promesen, ziurtagiri teknikoaren eta auditoria opakoen bidez soilik egiazta dezakegramos osotasuna duten bitartekarietatik igarotzen da. Ez dago ohartaraziko gaituen argizari hautsi baten baliokiderik.

Lakre-zigilu digital bat

Lakre-zigiluari indarra ematen zion propietatea ez zen lakre-zigilua bera, ordezkatzeko zuena baizik: diseinu bidezko osotasun egiaztagarria, hirugarren bategan konfiantzarik izan beharrik gabe. Ezaugarri hori plano digitalean berreraiki daiteke, nahiz eta elementu bakar baten ordezkari bi erabili. Lehenengoa zigilu kriptografikoa da —argitalpen honetako artikulu bakoitzaren oinean agertzen den SHA-256 azterna, zentzu literalean, lakre-zigilu digital bat da: edukiaren edozein aldaketak azterna nabarmen aldatzen du, argizari hautsiak baimenik gabeko irakurketa salatzen zuen bezala. Bigarrena kanalaren arkitektura da: komunikatzen diren bi pertsonen artean zerbitzaririk ez dagoenean, ez dago konfiantza eman behar zaion bitartekaririk. Bi elementu horien konbinazioak —osotasun egiaztagarria eta bitartekaririk eza— digitalizatu egiten du lau mendez paper tolestuaren gaineko argizari gorriak egunero egiten zuena.

Izena

Argitalpen honek Cuadernos Lacre izena du, lakre-zigilua ez delako apaingarri historiko bat, propietate tekniko zehatz bat baizik: eraikuntza bidezko osotasun egiaztagarria, operadore baten promesarik gabe. Serieko artikulu bakoitzak, bere bertsio digital garaikidean, ideia horren zatiren bat aztertzen du: enkriptatzea, metadatuak, sekretu profesionala, komunikazio-arkitektura, Europako lege-esparrua. Izena, konfidentzialtasuna kontratatzen den zerbitzu bat ez dela gogorarazteko modu bat ere bada, informazioa zirkulatzen den kanalaren propietatea baizik.

Editore-oharra: Cuadernos hauek enpresak edo produktuak aipatzen dituztenean, ez da akusatzeko. Horiek eraikitzen dituztenek milioika lagunek erabiltzen eta estimatzen duten lana egiten dute. Seinalatzen duguna estrukturala da —eredua, ez marka. Markak adibide gisa agertzen dira, irakurleak ezagutzen dituenak direlako.

Iturriak eta irakurgai gehiago

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (buztinezko tabletak eta bullae mesopotamiarrak zigilatzeari buruzko kapituluak).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Lakre-zigilua osotasun eta autoretza tresna gisa aztertzen duten kapituluak.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Lakre-zigiluaren printzipioaren formulazio modernoa: bermeak muturretan, ez tarteko kanalean.

[Hurrengoa → Enkriptatzea ez da pribatua izatea: metadatuak zutaz diotena](#)

Azken irakurketak

- [Analisisa · 2026ko maiatzaren 18a Pribatutasun erreala vs itxurazkoa: geure buruari egin beharreko galderak](#)
- [Analisisa · 2026ko maiatzaren 18a Self-hosting praktika profesional gisa](#)
- [Kontzeptua · 2026ko maiatzaren 18a 24 hitzak: zer den identitate kriptografiko bat](#)

Eraman artikulu hau zurekin behar duzun lekura.

[↓ Markdown](#) [↓ Testu arrunta](#) [↓ PDF](#)

Fitxategia zure gailura deskargatuko da. Bertatik gorde, Solo2ra inportatu edo nahi duzun lekuan parteka dezakezu. Cuadernosek ez du helburua zure ordezkari erabakitzen.

Lakre-zigilua · SHA-256 72835f7a3b1fb15d2916c1f90d09e2d9ac6bc9f9644a66b305d59369a6ba062e

Cuadernos Lacre · [Menzuri Gestión S.L.](#)ren argitalpena ·
R.Eugeniok idatzia · [Solo2](#) taldeak editatua.

Webgune honek ez du cookierik erabiltzen eta ez du hirugarrenen baliabiderik kargatzen. Bisita-kontagailu anonimo ostatu bat erabiltzen du (Umami, gure Europako zerbitzarian) eta goiburuko bi kontroletarako beharrezkoa den gutxieneko JavaScripta: gai argia edo iluna, eta hizkuntza-hautatzailea. Jarraipenik gabe, profilatuta gabe, daturik partekatu gabe. Jarraitu nahi badiguzu: [RSS](#).