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.

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 zigilatuak: 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, diplomatikoek, 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, telefonoa, 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 teknikoen 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, ordezkatzen zuena baizik: diseinu bidezko osotasun egiaztagarria, hirugarren batengan konfiantzarik izan beharrik gabe. Ezaugarri hori plano digitalean berreraiki daiteke, nahiz eta elementu bakar baten ordez bi erabili. Lehenengoa zigilu kriptografikoa da —argitalpen honetako artikulu bakoitzaren oinean agertzen den SHA-256 aztarna, zentzu literalean, lakre-

zigilu digital bat da: edukiaren edozein aldaketak aztarna nabarmen aldatzen du, argizari hautsiak baimenik gabeko irakurketa salatzen zuen bezala. Bigarrena kanalaren arkitektura da: komunikaten 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.

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: metadatuek zutaz diotena

Azken irakurketak

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 ordez erabakitzen.

Lakre-zigilua · SHA-256 41a367f687ed7fd8f4183a0a1c9d91df18973946d2b433d98c1c61e21082e160
ES

Cuadernos Lacre · Menzuri Gestión S.L.ren argitalpena ·
R.Eugeniok idatzia · Solo2 taldeak editatua.