Īsa vaska zīmoga vēsture

Četrus gadsimtus sarkanā vaska piliens garantēja, ka vēstuli neviens nav lasījis. Mēs to pazaudējām, pārejot uz digitālo ēru. To var atgūt.

Pirms papīra

Nepieciešamība konfidenciāli paziņot kaut ko tālumā esošai personai ir vecāka par rakstību. Mesopotāmijā māla plāksnītes ar administratīviem vai privātiem vēstījumiem tika sūtītas arī māla kapsulās, kuras pirms apdedzināšanas apzīmogoja: jebkurš mēģinājums izlasīt saturu lika saplēst apvalku, un saņēmējs no pirmā acu uzmetiena saprata, vai kapsula ieradusies neskarta. Klasiskajā Romā pergamenta ruļļus sēja ar auklu un aizzīmogoja ar vasku vai svinu. Ideja vienmēr bija viena un tā pati: jebkurai neatļautai lasīšanai bija jāatstāj neizdzēšamas fiziskas pēdas.

Vaska zīmoga ēra

Vairākus gadsimtus, no viduslaiku beigām līdz pat 20. gadsimtam, Eiropas konfidenciālās sarakstes kanoniskais instruments bija salocīts papīrs, kas aizzīmogots ar vaska zīmogu. Izkusušo vasku uzlēja papīra savienojuma vietai un nospieda ar personīgo vai institucionālo zīmogu. Tas nebija ornaments. Notāri, diplomāti, tirgotāji un privātpersonas to izmantoja ar to pašu loģiku: ja vaska zīmogs bija neskarts un zīmogs atpazīstams, saturs nebija lasīts; ja tas bija salauzts, sarakste bija kompromitēta vēl pirms tās atvēršanas.

Vaska zīmoga spēks neslēpās tā dārdzībā vai svinīgumā. Tas slēpās ļoti konkrētā strukturālā īpašībā: jebkurš mēģinājums to noņemt un uzlikt atpakaļ atstāja redzamas pēdas. Nebija neviena klusa veida, kā atvērt aizzīmogotu vēstuli. Un tas nozīmēja, ka konfidencialitāte nebija atkarīga no neviena starpnieka — kurjera, ormaņa, pasta ierēdņa — solījuma, bet gan no paša fiziskā apvalka dizaina. Tā bija uzticēšanās, kuras pamatā bija pierādījumi, nevis kāda vārdi.

Digitālā pāreja

Telegrāfs, telefons, e-pasts, korporatīvā ziņapmaiņa. Digitālā komunikācija ienesa ātrumu, globālu sasniedzamību un gandrīz nulles izmaksas par ziņojumu. Tas arī iznīcināja vaska zīmoga garantiju. Pēc noklusējuma katrs ziņojums iet caur starpniekiem, kuru integritāti varam pārbaudīt tikai ar rakstiskiem solījumiem pakalpojumu sniegšanas noteikumos, tehniskajiem sertifikātiem un nepārredzamiem auditiem. Nav nekā līdzīga salauztai vaska lāsei, kas mūs brīdinātu.

Digitālais vaska zīmogs

Īpašība, kas vaska zīmogam deva spēku, nebija pats vaska zīmogs, bet gan tas, ko tas pārstāvēja: pārbaudāma integritāte pēc dizaina, bez nepieciešamības uzticēties trešajai pusei. Šo īpašību var atjaunot digitālajā telpā, lai gan ar diviem elementiem viena vietā. Pirmais ir kriptogrāfiskais zīmogs — SHA-256 nospiedums, kas parādās katra šīs publikācijas raksta apakšā, tiešā nozīmē ir digitālais vaska zīmogs: jebkura satura izmaiņa acīmredzami maina nospiedumu, tāpat kā salauztais vasks nodeva neatļautu lasīšanu. Otrais ir kanāla arhitektūra: ja starp

diviem sazināšanās dalībniekiem nav servera, nav neviena starpnieka, kuram būtu nepieciešams uzticēties. Abu elementu kombinācija — pārbaudāma integritāte un starpnieka neesamība — digitāli atveido to, ko četrus gadsimtus sarkanā vaska lāse uz salocīta papīra darīja katru dienu.

Nosaukums

Šīs publikācijas nosaukums ir Cuadernos Lacre, jo vaska zīmogs nav vēsturisks rotājums, bet gan konkrēta tehniska īpašība: konstruktīvi pārbaudāma integritāte bez jebkāda operatora solījuma. Katrs sērijas raksts savā mūsdienu digitālajā versijā analizē kādu šīs idejas daļu: šifrēšanu, metadatus, profesionālo noslēpumu, sakaru arhitektūru, Eiropas tiesisko regulējumu. Nosaukums ir arī veids, kā atgādināt, ka konfidencialitāte nav pakalpojums, ko mēs nolīgstam, bet gan paša informācijas aprites kanāla īpašība.

Avoti un papildu literatūra

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (nodaļas par plāksnīšu un Mesopotāmijas bullu aizzīmogošanu).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Nodaļas par vaska zīmogu kā integritātes un autorības instrumentu.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Mūsdienīga vaska zīmoga principa formulēšana: garantijas galapunktos, nevis kanālā.

Nākamais → Šifrēt nenozīmē būt privātam: ko par jums saka metadati

Jaunākie lasījumi

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Paņemiet šo rakstu līdzi tur, kur jums nepieciešams.

↓ Markdown ↓ Parasts teksts ↓ PDF

Fails tiks lejupielādēts jūsu ierīcē. No turienes varat to saglabāt, importēt Solo2 vai kopīgot jebkur. Cuadernos nepieņem lēmumu par galamērķi jūsu vietā.

Vaska zīmogs · SHA-256 cbf2fe260011a1d3f165c660764a128e48f22a2ddbfca432ed3bffd60175e7fe

ES

Cuadernos Lacre · Menzuri Gestión S.L. publikācija ·
autors R.Eugenio · rediģējusi Solo2 komanda.