

# Sinettivahan lyhyt historia

Neljän vuosisadan ajan pisara punaista vahaa takasi, ettei kukaan ollut lukenut kirjettä. Menetimme tämän siirtyessämme digitaaliseen aikaan. Se on palautettavissa.

## Ennen paperia

Tarve viestiä jotain luottamuksellisesti kaukana olevalle on vanhempi kuin kirjoitustaito. Mesopotamiassa hallinnollisia tai yksityisiä viestejä sisältävät savitaulut lähetettiin savikapseleissa, jotka sinetöitiin ennen paistamista: mikä tahansa yritys lukea sisältö pakotti rikkomaan kääreen, ja vastaanottaja tiesi yhdellä silmäyksellä, saapuiko kapseli ehjänä. Klassisessa Roomassa pergamenttirullat sidottiin narulla ja sinetöitiin vahalla tai lyijyllä. Idea oli aina sama: jokaisen luvattoman lukukerran tuli jättää peruuttamaton fyysinen jälki.

## Sinettivahan aikakausi

Useiden vuosisatojen ajan, keskiajan lopulta aina 1900-luvulle asti, Euroopan kanoninen työkalu luottamukselliseen kirjeenvaihtoon oli taitettu ja sinettivahalla sinetöity paperi. Sulanut vaha kaadettiin taitteen päälle ja siihen painettiin henkilökohtainen tai virallinen leima. Se ei ollut koristeellinen. Notaarit, diplomaatit, kauppiat ja yksityishenkilöt käyttivät sitä samalla logiikalla: jos sinettivaha oli ehjä ja leima tunnistettavissa, sisältöä ei ollut luettu; jos se oli rikki, kirjeenvaihto oli vaarantunut jo ennen avaamista.

Sinettivahan voima ei ollut kalleudessa eikä juhlallisuudessa. Se oli hyvin erityisessä rakenteellisessa ominaisuudessa: mikä tahansa yritys poistaa se ja laittaa se takaisin jätti näkyviä jälkiä. Sinetöityä kirjettä ei voinut avata äänettömästi. Ja se tarkoitti, että luottamuksellisuus ei riippunut minkään välittäjän — lähettilään, ajurin tai postivirkailijan — lupauksesta, vaan kääreen fyysisestä suunnittelusta. Se oli näyttöön perustuvaa luottamusta, ei kenenkään sanaan.

## Digitaalinen siirtymä

Lennätin, puhelin, sähköposti, yritysviestintä. Elektroninen viestintä toi nopeuden, globaalin ulottuvuuden ja lähes nollakustannukset viestiä kohden. Se vei myös mennessään sinettivahan takuun. Oletusarvoisesti kaikki viestit kulkevat välittäjien kautta, joiden eheyden voimme tarkistaa vain käyttöehdoissa annettujen lupauksen, teknisten sertifikaattien ja läpinäkyvämmien tarkastusten kautta. Mikään ei vastaa särkynyttä vahapisaraa, joka varoittaisi meitä.

## Digitaalinen sinettivaha

Ominaisuus, joka antoi sinettivahalle voiman, ei ollut sinettivaha itse, vaan se, mitä se edusti: suunnittelun kautta todettavissa olevaa eheyttä ilman tarvetta luottaa kolmanteen osapuoleen. Tämä ominaisuus voidaan rakentaa uudelleen digitaalisella tasolla, joskin kahden elementin avulla yhden sijasta. Ensimmäinen on kryptografinen sinetti — jokaisen tämän julkaisun artikkelin alalaidassa näkyvä SHA-256-sormenjälki on kirjaimellisesti digitaalinen sinettivaha: mikä tahansa sisällön muutos muuttaa sormenjälkeä näkyvästi, aivan kuten särkynyt vaha paljasti luvattoman lukemisen. Toinen on kanavan arkkitehtuuri: kun kahden viestivän henkilön välillä ei

oli palvelinta, ei ole välittäjää, jolle pitäisi antaa luottamusta. Näiden kahden elementin yhdistelmä — todennettavissa oleva eheys ja välittäjän puuttuminen — toisintaa digitaalisesti sen, mitä taitetun paperin päällä oleva punainen vaha teki neljän vuosisadan ajan päivittäin.

## Nimi

Tämän julkaisun nimi on Cuadernos Lacre, koska sinettivaha ei oli historiallinen koriste, vaan tietty tekninen ominaisuus: rakenteen kautta todettavissa oleva eheys ilman minkään operaattorin lupaus. Sarjan jokainen artikkeli analysoi nykyaikaisessa digitaalisessa versiossaan jotakin osaa tästä samasta ideasta: salausta, metatietoja, ammattisalaista, viestintäarkkitehtuuria, Euroopan oikeudellista kehystä. Nimi on myös tapa muistuttaa, ettei luottamuksellisuus ole palvelu, joka ostetaan, vaan sen kanavan ominaisuus, jota pitkin tieto kulkee.

## Lähteet ja lisälukemista

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (luvut savitaulujen ja mesopotamialaisten bullien sinetöinnistä).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Luvut sinettivahasta eheyden ja tekijyyden välineenä.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Sinettivahaperiaatteen moderni muotoilu: takuut päissä, ei välikanavassa.

[Seuraava → Salaus ei ole sama kuin yksityisyys: mitä metatiedot kertovat sinusta](#)

## Viimeaikaiset lukemiset

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Ota tämä artikkeli mukaasi minne tarvitset.

[↓ Markdown](#) [↓ Pelkkä teksti](#) [↓ PDF](#)

Tiedosto ladataan laitteellesi. Voit tallentaa sen, tuoda sen Solo2-sovellukseen tai jakaa sen haluamallasi tavalla. Cuadernos ei pääätä tiedoston kohtaloa puolestasi.

Sinetti · SHA-256 53a0e106aa5acddefcc3c3d4aa96568a7cba6420032ee4e5df6af868be24ec1b

ES

Cuadernos Lacre · [Menzuri Gestión S.L.](#) -julkaisu · kirjoittanut R.Eugenio · toimittanut [Solo2](#)-tiimi.

Tämä sivusto ei käytä evästeitä eikä lataa kolmannen osapuolen resursseja. Käytämme itse isännöityä anonyymiä kävijälaskuria (Umami, eurooppalaisella palvelimellamme) ja vain välttämätöntä JavaScriptiä teeman valintaan. Ei seurantaa, ei profiilointia, ei tietojen jakamista. Jos haluat seurata meitä: [RSS](#).