A viaszpecsét rövid története

Négy évszázadon át egy csepp piros viasz garantálta, hogy senki sem olvasott el egy levelet. Ezt elvesztettük a digitális korszakba lépve. Visszaszerezhető.

A papír előtt

Az igény arra, hogy bizalmasan közöljünk valamit valakivel, aki távol van, ősibb, mint az írás. Mezopotámiában az adminisztratív vagy magánüzeneteket tartalmazó agyagtáblákat szintén agyagból készült tokokban küldték, amelyeket kiégetés előtt lezártak: bármilyen kísérlet a tartalom elolvasására a burok feltörését jelentette, és a címzett egyetlen pillantással tudta, hogy a tok sértetlenül érkezett-e. A klasszikus Rómában a pergamentekercseket zsinórral kötözték át, és viasszal vagy ólommal zárták le. Az elv mindig ugyanaz volt: hogy minden illetéktelen olvasás eltörölhetetlen fizikai nyomot hagyjon.

A viaszpecsét korszaka

Több évszázadon át, a középkor végétől a 20. századba nyúlóan, a bizalmas levelezés kanonikus eszköze Európában a hajtogatott és viaszpecséttel lezárt papír volt. A megolvadt viaszt a papírlap illesztésére öntötték, és személyes vagy intézményi bélyegzővel nyomták meg. Ez nem volt díszítő elem. A közjegyzők, diplomaták, kereskedők és magánszemélyek ugyanazon logika mentén használták: ha a viaszpecsét sértetlen volt, és a bélyegző felismerhető, a tartalmat nem olvasták el; ha eltört, a levelezés már a kinyitása előtt kompromittálódott.

A viaszpecsét ereje nem az árában vagy az ünnepélyességében rejlett. Egy nagyon specifikus szerkezeti tulajdonságában állt: minden eltávolítási és visszahelyezési kísérlet látható nyomokat hagyott. Nem volt mód egy lezárt levél csendes felnyitására. Ez pedig azt jelentette, hogy a bizalmasság nem egy közvetítő — a futár, a kocsis, a postás — ígéretétől függött, hanem a boríték fizikai kialakításától. Ez bizonyítékon alapuló bizalom volt, nem valakinek a szaván.

A digitális átállás

A távíró, a telefon, az e-mail, a vállalati üzenetküldés. Az elektronikus kommunikáció sebességet, globális elérést és szinte nulla költséget hozott üzenetenként. De magával vitte a viaszpecsét garanciáját is. Alapértelmezés szerint minden üzenet olyan közvetítőkön megy keresztül, akiknek az integritását csak szolgáltatási feltételekbe írt ígéreteken, műszaki tanúsítványokon és átláthatatlan auditokon keresztül tudjuk ellenőrizni. Nincs semmi, ami egy törött viaszcsepphez hasonlóan figyelmeztetne minket.

Egy digitális viaszpecsét

A tulajdonság, amely a viaszpecsétnek erőt adott, nem maga a viaszpecsét volt, hanem az, amit képviselt: a tervezésből adódóan ellenőrizhető integritás, anélkül, hogy egy harmadik félben kellene bízni. Ezt a tulajdonságot digitális síkon is újra lehet építeni, bár egy helyett két elemmel. Az első a kriptográfiai pecsét — a kiadvány minden cikkének alján található SHA-256 lenyomat szó szerint egy digitális viaszpecsét: a tartalom bármilyen módosítása láthatóan megváltoztatja a lenyomatot, éppúgy, ahogy a törött viasz elárulta az illetéktelen

olvasást. A második a csatorna architektúrája: amikor két kommunikáló ember között nincs középen szerver, nincs olyan közvetítő sem, akinek bizalmat kellene szavazni. E két elem — az ellenőrizhető integritás és a közvetítő hiánya — kombinációja digitális értelemben reprodukálja azt, amit négy évszázadon át a hajtogatott papíron lévő piros viasz a mindennapokban tett.

A név

Ez a kiadvány azért viseli a Cuadernos Lacre nevet, mert a viaszpecsét nem történelmi dísz, hanem egy konkrét műszaki tulajdonság: konstrukcióból fakadóan ellenőrizhető integritás, bármely operátor ígérete nélkül. A sorozat minden cikke kortárs digitális változatában elemzi ugyanezen gondolat valamely részét: titkosítást, metaadatokat, szakmai titoktartást, kommunikációs architektúrát, az európai jogi keretet. A név emellett egy módja annak is, hogy emlékeztessünk: a bizalmasság nem egy bérelt szolgáltatás, hanem magának a csatornának a tulajdonsága, amelyen az információ áramlik.

Források és további olvasnivalók

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992. (fejezetek a táblák és a mezopotámiai bullák lezárásáról).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Fejezetek a viaszpecsétről mint az integritás és a szerzőség eszközéről.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. A viaszpecsét elvének modern megfogalmazása: a garanciák a végpontokon vannak, nem a csatornában.

Következő → A titkosítás nem azonos a magánélettel: mit árulnak el Önről a metaadatok

Legutóbbi olvasmányok

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vigye magával ezt a cikket, ahová csak szüksége van rá.

↓ Markdown ↓ Egyszerű szöveg ↓ PDF

A fájl letöltődik az Ön eszközére. Onnan elmentheti, importálhatja a Solo2-be, vagy megoszthatja bárhol. A Cuadernos nem dönt Ön helyett a fájl sorsáról.

Viaszpecsét · SHA-256 57e0e3dba7a97421eb8219ebccc7fad75d285d8eac06f64eda58996d30f5d73d
ES

Cuadernos Lacre · A Menzuri Gestión S.L. kiadványa ·
írta R.Eugenio · szerkesztette a Solo2 csapata.