ประวัติย่อของตราประทับครั่ง

เป็นเวลาสี่ศตวรรษที่ครั่งสีแดงเพียงหยดเดียวช่วยรับประกันว่าไม่มีใครได้อ่านจดหมาย เราสูญเสียมันไปเมื่อก้าวเข้าสู่ยุคดิจิทัล แต่มันสามารถกู้คืนกลับมาได้

ก่อนที่จะมีกระดาษ

ความจำเป็นในการสื่อสารบางอย่างอย่างเป็นความลับไปยังผู้ที่อยู่ห่างไกลนั้นเก่าแก่กว่าตัวอักษร ในเมโสโปเตเมีย แผ่นจารึกดินเผาที่มีข้อความทางการหรือส่วนตัวจะถูกส่งไปในแคปซูลดินเผาเช่นกัน ซึ่งจะถูกประทับตราก่อนนำไปเผา: ความพยายามใดๆ ที่จะอ่านเนื้อหาข้างในจะต้องทำลายเปลือกหุ้มนั้น และผู้รับจะทราบได้ทันทีเพียงแค่ชำเลืองมองว่าแคปซูลนั้นมาถึงในสภาพสมบูรณ์หรือไม่ ในยุคโรมันคลาสสิก ม้วนคัมภีร์หนังจะถูกผูกด้วยเชือกและประทับตราด้วยขี้ผึ้งหรือตะกั่ว แนวคิดยังคงเหมือนเดิมเสมอ: นั่นคือเพื่อให้การอ่านโดยไม่ได้รับอนุญาตทิ้งร่องรอยทางกายภาพที่ลบไม่ออกไว้

ยุคของตราประทับครั่ง

เป็นเวลาหลายศตวรรษ ตั้งแต่ปลายยุคกลางจนถึงต้นศตวรรษที่ 20 เครื่องมือมาตรฐานสำหรับการสื่อสารลับในยุโรปคือกระดาษที่พับและประทับตราด้วยครั่ง ขี้ผึ้งที่หลอมละลายจะถูกหยดลงบนรอยต่อของรอยพับและประทับด้วยตราประจำตัวหรือตราประจำองค์กร มันไม่ใช่ของตกแต่งเพื่อความสวยงาม ทนายความ นักการทูต พ่อค้า และบุคคลทั่วไปต่างใช้มันด้วยเหตุผลเดียวกัน: หากครั่งยังคงสภาพสมบูรณ์และจำตราประทับได้ แสดงว่าเนื้อหายังไม่ถูกอ่าน แต่หากครั่งแตก การสื่อสารนั้นจะถือว่าถูกเปิดเผยก่อนที่จะมีการเปิดอ่านเสียด้วยซ้ำ

พลังของตราประทับครั่งไม่ได้อยู่ที่ราคาแพงหรือความเคร่งขรึม แต่มันอยู่ที่คุณสมบัติทางโครงสร้างที่เฉพาะเจาะจงมาก: ความพยายามใดๆ ที่จะแกะมันออกและติดกลับเข้าไปใหม่จะทิ้งร่องรอยที่มองเห็นได้ ไม่มีวิธีใดที่จะเปิดจดหมายที่ประทับตราแล้วได้อย่างเงียบเชียบ และนั่นหมายความว่าการรักษาความลับไม่ได้ขึ้นอยู่กับคำสัญญาของคนกลางคนใดเลย — ไม่ว่าจะเป็นคนส่งสาร คนขับรถม้า หรือเจ้าหน้าที่ไปรษณีย์ — แต่ขึ้นอยู่กับการออกแบบทางกายภาพของบรรจุภัณฑ์นั่นเอง มันคือความไว้วางใจที่ตั้งอยู่บนพื้นฐานของหลักฐาน ไม่ใช่คำพูดของใคร

การเปลี่ยนผ่านสู่ยุคดิจิทัล

โทรเลข โทรศัพท์ อีเมล การส่งข้อความในองค์กร การสื่อสารทางอิเล็กทรอนิกส์นำมาซึ่งความเร็ว การเข้าถึงทั่วโลก และต้นทุนต่อข้อความที่เกือบเป็นศูนย์ แต่มันก็ได้ทำลายการรับประกันแบบตราประทับครั่งลงไปด้วย โดยค่าเริ่มต้น ทุกข้อความจะผ่านคนกลางซึ่งเราสามารถตรวจสอบความซื่อสัตย์ของพวกเขาได้ผ่านเพียงคำสัญญาที่เขียนไว้ในเงื่อนไขการใช้บริการ การรับรองทางเทคนิค และการตรวจสอบที่คลุมเครือเท่านั้น ไม่มีอะไรที่เทียบเท่ากับหยดขี้ผึ้งที่แตกออกเพื่อเตือนเราได้เลย

ตราประทับครั่งดิจิทัล

คุณสมบัติที่ทำให้ตราประทับครั่งมีพลังไม่ใช่ตัวครั่งเอง แต่เป็นสิ่งที่มันเป็นตัวแทน: ความสมบูรณ์ที่ตรวจสอบได้โดยการออกแบบ (integrity by design) โดยไม่จำเป็นต้องไว้วางใจบุคคลที่สาม คุณสมบัตินี้สามารถสร้างขึ้นใหม่ได้ในโลกดิจิทัล แม้ว่าจะต้องใช้องค์ประกอบสองอย่างแทนที่จะเป็นอย่างเดียว อย่างแรกคือตราประทับเข้ารหัส (cryptographic seal) — ลายนิ้วมือ SHA-256 ที่ปรากฏที่ท้ายบทความแต่ละบทของสื่อสิ่งพิมพ์นี้คือตราประทับครั่งดิจิทัลในความหมายตามตัวอักษร: การแก้ไขเนื้อหาใดๆ จะเปลี่ยนลายนิ้วมือนี้อย่างเห็นได้ชัด เช่นเดียวกับขี้ผึ้งที่แตกออกซึ่งฟ้องว่ามีการอ่านโดยไม่ได้รับอนุญาต อย่างที่สองคือสถาปัตยกรรมของช่องทางสื่อสาร: เมื่อไม่มีเซิร์ฟเวอร์อยู่ตรงกลางระหว่างคนสองคนที่สื่อสารกัน ก็ไม่มีคนกลางที่จำเป็นต้องได้รับความไว้วางใจ การรวมกันของทั้งสององค์ประกอบ — ความสมบูรณ์ที่ตรวจสอบได้และการไม่มีคนกลาง — ช่วยสร้างสิ่งที่ขี้ผึ้งสีแดงบนกระดาษพับได้ทำหน้าที่ในชีวิตประจำวันมาตลอดสี่ศตวรรษขึ้นมาใหม่ในรูปแบบดิจิทัล

ชื่อ

สื่อสิ่งพิมพ์นี้ใช้ชื่อว่า Cuadernos Lacre (สมุดบันทึกตราประทับครั่ง) เพราะตราประทับครั่งไม่ใช่ของประดับทางประวัติศาสตร์ แต่เป็นคุณสมบัติทางเทคนิคที่จับต้องได้: ความสมบูรณ์ที่ตรวจสอบได้โดยโครงสร้างสร้าง (integrity by construction) โดยไม่มีคำสัญญาจากผู้ให้บริการรายใด บทความแต่ละบทในชุดนี้จะวิเคราะห์ส่วนหนึ่งของแนวคิดเดียวกันนี้ในเวอร์ชันดิจิทัลร่วมสมัย: การเข้ารหัส, เมทาดาตา, ความลับทางวิชาชีพ, สถาปัตยกรรมการสื่อสาร, กรอบกฎหมายของยุโรป ชื่อนี้ยังเป็นวิธีเตือนใจว่าการรักษาความลับไม่ใช่บริการที่มีไว้ให้เช่าซื้อ แต่เป็นคุณสมบัติของช่องทางที่ข้อมูลไหลผ่านนั่นเอง

แหล่งข้อมูลและการอ่านเพิ่มเติม

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (บทที่เกี่ยวกับการประทับตราบนแผ่นจารึกและ bullae ของเมโสโปเตเมีย)
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. บทที่เกี่ยวกับตราประทับครั่งในฐานะเครื่องมือรับรองความสมบูรณ์และความเป็นเจ้าของผลงาน
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. การกำหนดหลักการตราประทับครั่งในยุคใหม่: การรับประกันที่ปลายทาง ไม่ใช่ในช่องทางสื่อสาร

ถัดไป → การเข้ารหัสไม่ได้หมายถึงความเป็นส่วนตัว: Metadata บอกอะไรเกี่ยวกับคุณบ้าง

บทความล่าสุด

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

↓ Markdown ↓ ข้อความธรรมดา ↓ PDF

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั่ง · SHA-256 afa91b68347497e2467542e4ece1fb0005ab7132e892e9203af431c802b87729

ES

Cuadernos Lacre · สิ่งพิมพ์ของ Menzuri Gestión S.L. ·
เขียนโดย R.Eugenio · เรียบเรียงโดยทีมงาน Solo2

เว็บไซต์นี้ไม่มีการใช้คุกกี้และไม่มีการโหลดทรัพยากรจากบุคคลภายนอก เราใช้ตัวนับผู้เข้าชมแบบไม่ระบุตัวตนที่โฮสต์เอง (Umami บนเซิร์ฟเวอร์ยุโรปของเรา) และใช้ JavaScript ขั้นต่ำที่จำเป็นสำหรับการเลือกธีมสว่าง/มืดเท่านั้น ไม่มีการติดตาม ไม่มีการทำโปรไฟล์ ไม่มีการแชร์ข้อมูล หากคุณต้องการติดตามเรา: RSS