

# เมื่อไม่มีใครอยู่ตรงกลาง

การเข้ารหัสข้อมูลที่ผ่านเซิร์ฟเวอร์ช่วยปกป้องเนื้อหา แต่การไม่มีเซิร์ฟเวอร์อยู่ตรงกลางช่วยตัดคำถามทิ้งไป ทั้งสองอย่างนี้ไม่เหมือนกัน

**พูดง่าย ๆ ก็คือ:** เมื่อคุณพูดคุยแบบตัวต่อตัวกับใครสักคน ไม่มีใครอื่นต้องสัญญาว่าคุณไม่ได้แอบฟัง พวกเขาไม่ได้ฟังเพราะพวกเขาไม่ได้อยู่ที่นั่น นั่นคือความเป็นส่วนตัวในรูปแบบที่แข็งแกร่งที่สุด: ไม่ใช่คำสัญญาของตัวกลางว่าจะทำตัวดี — แต่เป็นการไม่มีตัวกลางเลย

## คนสองคน บทสนทนาเดียว

เมื่อคนสองคนพูดคุยแบบตัวต่อตัวในห้อง ไม่มีใครอื่นต้องสัญญาว่าไม่ได้ยินอะไรเลย พวกเขาไม่ได้ยินเพราะไม่ได้อยู่ที่นั่น เมื่อคนสองคนส่งกระดาษจากมือหนึ่งไปยังอีกมือหนึ่ง ไม่มีใครตรงกลางที่ต้องสาบานว่าไม่ได้อ่านมัน เพราะไม่มีใครอยู่ตรงกลาง

สิ่งต่างๆ ส่วนใหญ่ในชีวิตประจำวันทำงานเช่นนี้ เราไม่ได้ทำข้อตกลงรักษาความลับกับอากาศที่ส่งผ่านเสียงของเรา หรือกับกระดาษที่เราถืออยู่ ความเป็นส่วนตัวของบทสนทนาไม่ได้ขึ้นอยู่กับคำสัญญาของคนกลาง เพราะมันไม่มีคนกลาง นี่คือรูปแบบหนึ่งของการรักษาความเป็นส่วนตัวที่แข็งแกร่งที่สุด: ไม่ใช่เพราะสิ่งใดหรือใครทำตัวดี แต่เป็นเพราะไม่มีสิ่งนั้นหรือใครคนนั้นอยู่เลย

เมื่อบทสนทนาย้ายไปสู่ช่องทางดิจิทัล สิ่งนี้จะเปลี่ยนไปโดยคำเริ่มต้น รูปแบบปกติคือ: คนสองคนเชื่อมต่อกับเซิร์ฟเวอร์ เซิร์ฟเวอร์รับข้อความ เข้ารหัสหรือเก็บไว้ในรูปแบบที่เข้ารหัส แล้วส่งให้ผู้รับ เซิร์ฟเวอร์อยู่ตรงกลาง เซิร์ฟเวอร์อาจจะซื่อสัตย์ อาจจะได้รับตรวจสอบ อาจจะทำเนื้องานภายใต้เขตอำนาจศาลที่เอื้ออำนวยและภายใต้นโยบายความเป็นส่วนตัวที่เข้มงวด ทั้งหมดนี้อาจเป็นเรื่องจริง แต่เซิร์ฟเวอร์ก็ยังคงอยู่ตรงกลาง

## ความแตกต่างระหว่างการเข้ารหัสกับการไม่เก็บข้อมูล (ตอนที่สอง)

ในบทความก่อนหน้านี้ของชุดเดียวกันนี้ เรายืนยันว่าการเข้ารหัสเนื้อหากับการไม่เก็บเมทาดาทานั้นไม่ใช่เรื่องเดียวกัน และมีอีกขั้นตอนหนึ่งที่ควรระบุให้ชัดเจน: การเข้ารหัสสิ่งที่ผ่านเซิร์ฟเวอร์กับการไม่มีเซิร์ฟเวอร์เลยนั้นก็ไม่ใช่เรื่องเดียวกันเช่นกัน

รูปแบบแรก — มีเซิร์ฟเวอร์ตรงกลาง เนื้อหาถูกเข้ารหัส — ปกป้องเนื้อหาจากผู้ให้บริการเซิร์ฟเวอร์ พนักงานซ่อมบำรุง และผู้โจมตีจากภายนอกที่อาจเข้ามาแทรกแซงระบบ และนั่นคือสิ่งที่สำคัญ แต่มันไม่ได้กำจัดเซิร์ฟเวอร์ทิ้งไป เซิร์ฟเวอร์

ยังคงอยู่ที่นั่น ยังคงประมวลผลเมฆาตาตา ยังคงเป็นจุดที่อาจได้รับคำสั่งศาล การแทรกแซงทางกฎหมาย แรงกดดันทางการเมือง หรือการละเมิดความปลอดภัย มันยังคงเป็นจุดที่ต้องมอบความไว้วางใจให้กับใครบางคน

รูปแบบที่สอง — ไม่มีเซิร์ฟเวอร์ระหว่างปลายทางทั้งสอง — ไม่ได้ปกป้องเนื้อหาที่เข้ารหัสได้ดีไปกว่ากัน: หากการเข้ารหัสมีความแข็งแกร่ง เนื้อหาที่จะได้รับการปกป้องในทั้งสองกรณี สิ่งที่เปลี่ยนไปไม่ใช่เนื้อหา สิ่งที่เปลี่ยนไปคือคำถามที่ว่า «จะเกิดอะไรขึ้นกับเซิร์ฟเวอร์?» จะไม่มีความหมายอีกต่อไป เพราะไม่มีเซิร์ฟเวอร์ให้ต้องตั้งคำถามถึง

## ความไว้วางใจ การไม่มีอยู่ และความแตกต่างระหว่างทั้งสองอย่าง

ความไว้วางใจอาจได้รับการมอบให้ในที่ที่เหมาะสม บริษัทที่ซื่อสัตย์มีอยู่จริง ผู้ตรวจสอบที่เข้มงวดมีอยู่จริง กฎหมายที่เอื้อต่อผู้ใช้มีอยู่จริง บริการที่จริงจังซึ่งปฏิบัติตามสิ่งที่กล่าวมาทั้งหมดอย่างเคร่งครัดก็มีอยู่จริง ความไว้วางใจเมื่อมอบให้กับผู้ให้บริการที่สมควรได้รับ ก็ไม่ใช่ข้อตกลงที่แย่

แต่ความไว้วางใจ ไม่ว่าจะแข็งแกร่งเพียงใด ก็ยังคงเป็นความไว้วางใจ มันคือทางออกทางสังคม ไม่ใช่ทางออกทางเทคนิค บริษัทสามารถเปลี่ยนมือได้ เขตอำนาจศาลสามารถเปลี่ยนรัฐบาลได้ คำสั่งศาลอาจมาถึงในวันพรุ่งนี้ ช่องโหว่ใหม่ๆ อาจถูกค้นพบในเดือนหน้า สิ่งเหล่านี้ไม่ได้เกิดขึ้นจากความตั้งใจร้าย แต่มันเกิดขึ้นเพราะผู้ให้บริการยังมีตัวตนอยู่ และทุกสิ่งที่มีตัวตนย่อมต้องเผชิญกับเหตุการณ์ที่ไม่คาดฝันของโลก

การไม่มีผู้ให้บริการไม่ได้ขึ้นอยู่กับเหตุการณ์ที่ไม่คาดฝันเหล่านั้น คำสั่งศาลไม่สามารถเรียกขอข้อมูลจากเซิร์ฟเวอร์ที่ไม่มีอยู่จริงได้ ผู้โจมตีไม่สามารถเจาะระบบเซิร์ฟเวอร์ที่ไม่มีอยู่จริงได้ การเปลี่ยนแปลงนโยบายของบริษัทไม่สามารถส่งผลกระทบต่อข้อมูลที่บริษัทนั้นไม่เคยมี ประโยคสำคัญนั้นเรียบง่ายมาก: ข้อมูลที่ไม่มีอยู่ย่อมไม่สูญหาย

## ว่าด้วยข้อโต้แย้งที่สมเหตุสมผลของฝั่งเซิร์ฟเวอร์

ผู้ให้บริการส่งข้อความระดับมืออาชีพโดยมีเซิร์ฟเวอร์อยู่ตรงกลางมักจะยกข้อโต้แย้งสามประการที่สมเหตุสมผลอย่างยิ่ง ประการแรก เซิร์ฟเวอร์จำเป็นเพื่อรับประกันการส่งข้อความเมื่อผู้รับออฟไลน์ ประการที่สอง การเข้ารหัสเนื้อหานั้นแข็งแกร่ง ผู้ให้บริการจึงไม่สามารถอ่านได้ ประการที่สาม บริการนี้ปฏิบัติตามกฎหมายของยุโรปและข้อมูลได้รับการคุ้มครองตามกฎหมาย

ข้อโต้แย้งทั้งสามประการเป็นเรื่องจริง แต่ไม่มีข้อใดเปลี่ยนธรรมชาติของเรื่องนี้ เป็นเรื่องจริงที่เซิร์ฟเวอร์ช่วยให้สามารถจัดเก็บข้อความเพื่อรอการส่งในภายหลังได้ และก็เป็นเรื่องจริงเช่นกันที่การส่งข้อความในภายหลังสามารถแก้ไขได้ด้วยวิธีอื่น ผ่านโปรโตคอลการสื่อสารโดยตรงระหว่างอุปกรณ์ที่ได้รับการพัฒนามานานหลายทศวรรษและใช้งานอยู่ในปัจจุบัน เป็นเรื่องจริงที่การเข้ารหัสเนื้อหาในระหว่างการส่งนั้นมีความแข็งแกร่งในบริการที่ได้มาตรฐาน และเป็นเรื่องจริงที่กฎหมายยุโรปคุ้มครองผู้ใช้มากกว่าที่อื่นๆ หลายแห่ง

ประเด็นไม่ได้อยู่ที่ว่าบริการที่มีเซิร์ฟเวอร์อยู่ตรงกลางนั้นถูกกฎหมายหรือไม่ หรือปลอดภัยหรือไม่ หรือปกป้องเนื้อหาหรือไม่ สิ่งเหล่านี้อาจเป็นไปได้ มันถูกกฎหมาย และมักจะปลอดภัย ประเด็นคือการมีเซิร์ฟเวอร์อยู่ตรงกลางคือการเลือกเชิงสถาปัตยกรรม ไม่ใช่ความจำเป็นทางเทคนิค และทุกการเลือกย่อมมีผลตามมา สถาปัตยกรรมที่มีเซิร์ฟเวอร์อยู่ตรงกลางย่อมสร้างตัวละครที่ต้องได้รับความไว้วางใจขึ้นมา สถาปัตยกรรมที่ไม่มีเซิร์ฟเวอร์อยู่ตรงกลางไม่ต้องทำเช่นนั้น

## สิ่งที่กฎหมายกล่าว และสิ่งที่สถาปัตยกรรมทำ

GDPR ไม่ได้กำหนดรูปแบบสถาปัตยกรรมที่เฉพาะเจาะจง แต่กำหนดผลลัพธ์: การเก็บข้อมูลขั้นต่ำ (data minimization), วัตถุประสงค์ที่จำกัด, การคุ้มครองตั้งแต่การออกแบบและโดยค่าเริ่มต้น, ความสามารถในการแสดงการปฏิบัติตามกฎหมาย บริการที่มีเซิร์ฟเวอร์อยู่ตรงกลางสามารถปฏิบัติตามข้อกำหนดเหล่านี้ได้ทั้งหมด ส่วนบริการที่ไม่มีเซิร์ฟเวอร์อยู่ตรงกลางสามารถปฏิบัติตามข้อกำหนดหลายอย่างได้โดยโครงสร้างสร้าง ไม่ใช่โดยการประกาศ การเก็บข้อมูลขั้นต่ำสุดขีด — คือการไม่เก็บสิ่งใดที่ไม่จำเป็นอย่างยิ่งต่อการส่งข้อความ — เป็นเรื่องง่ายมากเมื่อไม่มีเซิร์ฟเวอร์ที่จะสามารถเก็บอะไรได้เลย

สำหรับการใช้งานทั่วไปในชีวิตประจำวันที่ไม่ละเอียดอ่อน สถาปัตยกรรมแบบมีเซิร์ฟเวอร์นั้นสมเหตุสมผลอย่างยิ่ง และความไว้วางใจในผู้ให้บริการที่มีมาตรฐานก็เป็นข้อตกลงที่ยอมรับได้ สำหรับการใช้งานอื่นๆ — เช่น การใช้งานที่เกี่ยวข้องกับความลับทางวิชาชีพที่ได้รับการควบคุม, การใช้งานที่มีความรับผิดชอบเชิงจรรยาบรรณ, การใช้งานที่เกี่ยวข้องกับข้อมูลที่ละเอียดอ่อนเป็นพิเศษ — การไม่มีจุดที่ต้องมอบความไว้วางใจไม่ใช่เรื่องฟุ่มเฟือย แต่มันคือข้อได้เปรียบเชิงโครงสร้าง

## สำหรับผู้อ่านมืออาชีพ

คำถามที่ควรตั้งขึ้นเมื่อเผชิญกับบริการสื่อสารระดับมืออาชีพ ซึ่งคุณเคยกันดีจากบทความก่อนๆ ในชุดนี้ จะสมบูรณ์ยิ่งขึ้นด้วยคำถามเชิงสถาปัตยกรรมอีกเพียงข้อเดียว:

1. มันเข้ารหัสเนื้อหาในระหว่างการส่งหรือไม่? (น่าจะใช่)
2. มันสร้างและจัดเก็บเมทาดาทาเกี่ยวกับผู้ที่จับคู่ด้วยและเวลาที่คู่หรือไม่? (น่าจะใช่)
3. มีเซิร์ฟเวอร์อยู่ในเส้นทางระหว่างอุปกรณ์ของคุณกับของผู้รับหรือไม่?
4. หากมี: ใครเป็นผู้ดูแลระบบ อยู่ภายใต้เขตอำนาจศาลใด และต้องเกิดอะไรขึ้นพวกเขาถึงจะยอมส่งมอบข้อมูลเกี่ยวกับฉัน?
5. หากไม่มี: คำถามก่อนหน้านี้ทั้งหมดจะไม่มี ความหมาย

ความแตกต่างระหว่างทั้งสองประเภทไม่ใช่เรื่องของระดับความเข้มข้น แต่เป็นเรื่องของชนิด เมื่อถึงเวลาต้องอธิบายให้ลูกค้า คนใช้ หรือเพื่อนร่วมงานฟัง คำอธิบายที่ซื่อสัตย์ที่สุดก็คือคำอธิบายที่ง่ายที่สุด: แบบหนึ่งมีคนอยู่ตรงกลาง ส่วนอีกแบบหนึ่งไม่มี

---

*บทความนี้จบวงจรเริ่มต้นของ Cuadernos Lacre หลังจากพูดถึงเรื่องการเข้ารหัส เมทาดาทา และความลับทางวิชาชีพ เราก็ได้เติมเต็มภาพรวมเชิงสถาปัตยกรรม: การเข้ารหัสเนื้อหากับการไม่มีเซิร์ฟเวอร์อยู่ตรงกลางเป็นคนละเรื่องกัน ทั้งสองอย่างอาจถูกกฎหมาย แต่มีเพียงอย่างเดียวที่กำจัดจุดที่ต้องมอบความไว้วางใจทิ้งไปได้*

**หมายเหตุจากบรรณาธิการ:** เมื่อ Cuadernos เหล่านี้เอ่ยชื่อบริษัทหรือผลิตภัณฑ์ ไม่ใช่เพื่อการกล่าวหา ผู้ที่สร้างสรรค์สิ่งเหล่านั้นได้ทำงานที่คนนับล้านได้ใช้และชื่นชอบ สิ่งที่เรากำลังชี้ให้เห็นคือเรื่องเชิงโครงสร้าง — รูปแบบธุรกิจ ไม่ใช่แบรนด์แบรนด์ต่างๆ ถูกยกมาเป็นตัวอย่างเพราะเป็นสิ่งที่ผู้อ่านรู้จัก

## แหล่งข้อมูลและการอ่านเพิ่มเติม

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. ข้อความพื้นฐานของหลักการที่ว่า การรับประกันของระบบควรดำเนินการที่ปลายทางทั้งสองด้าน ไม่ใช่ในช่องทางกลาง

- กฎระเบียบ (EU) 2016/679, มาตรา 25 — การคุ้มครองข้อมูลตั้งแต่การออกแบบและโดยค่าเริ่มต้น
- กฎระเบียบ (EU) 2016/679, มาตรา 5.1.c — หลักการเก็บข้อมูลขั้นต่ำ
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. บทที่เกี่ยวกับสถาปัตยกรรมที่ลดการเก็บข้อมูลโดยโครงสร้างสร้าง

[← ก่อนหน้าGDPR และการส่งข้อความในระดับมืออาชีพ: ทำโมคนส่วนใหญ่ถึงละเมิดกฎโดยไม่รู้ตัวถัดไป → Schrems II](#)  
[ห้าปีให้หลัง](#)

## บทความล่าสุด

- [การวิเคราะห์ · 18 พฤษภาคม 2026 ความเป็นส่วนตัวที่แท้จริง vs ความเป็นส่วนตัวที่จบบวย: คำถามที่คุณควรตั้งกับตัวเอง](#)
- [การวิเคราะห์ · 18 พฤษภาคม 2026 Self-hosting ในฐานะการปฏิบัติทางวิชาชีพ](#)
- [แนวคิด · 18 พฤษภาคม 2026 คำ 24 คำ: อัตลักษณ์การเข้ารหัสคืออะไร](#)

ดาวน์โหลดบทความนี้เก็บไว้เพื่อใช้งานได้ทุกที่ที่คุณต้องการ

[↓ Markdown](#) [↓ ข้อความRSS](#) [↓ PDF](#)

ไฟล์จะถูกดาวน์โหลดลงในอุปกรณ์ของคุณ คุณสามารถบันทึก นำเข้าสู่ Solo2 หรือแชร์ได้ทุกที่ตามต้องการ Cuadernos จะไม่กำหนดปลายทางแทนคุณ

ตราประทับครั้ง · SHA-256 b7954467ec300dde6009993be2e2bea349cabf5cf0aa6b9e9cd6b23f560e6b58b

Cuadernos Lacre · สิ่งพิมพ์ของ [Menzuri Gestión S.L.](#) ·  
เขียนโดย R.Eugenio · เรียบเรียงโดยทีมงาน [Solo2](#)

เว็บไซต์นี้ไม่ใช่คุกกี้และไม่โหลดทรัพยากรจากบุคคลภายนอก ใช้ตัวนับการเข้าชมแบบไม่ระบุตัวตนที่โฮสต์เอง (Umami บนเซิร์ฟเวอร์ยุโรปของเรา) และ JavaScript ขั้นต่ำที่จำเป็นสำหรับส่วนควบคุมสองอย่างในส่วนหัว: ธีมสว่างหรือมืด และตัวเลือกภาษา ไม่มีเครื่องมือติดตาม ไม่มีการสร้างโปรไฟล์ ไม่มีการแชร์ข้อมูล หากคุณต้องการติดตามเรา: [RSS](#)