Analysis · May 16, 2026

← Previous·Next →

When no one is in between

Encrypting what passes through a server protects the content. Not having a server in between eliminates the question. They are not the same.

Two people, one conversation

When two people talk face to face in a room, no one has to promise they heard nothing. They didn't hear because they weren't there. When two people pass a piece of paper from one hand to the other, no one in the middle has to swear they didn't read it. There is no one in the middle.

Most things in everyday life work like this. We don't sign confidentiality agreements with the air that transmits our voice, nor with the paper we hold. The privacy of the conversation does not rest on the promise of an intermediary, because there is no intermediary. That is one of the strongest ways to be private: not because something or someone behaves well, but because there is no something or someone.

When the conversation moves to a digital channel, this changes by default. The usual model is as follows: two people connect to a server, the server receives the message, encrypts it or stores it encrypted, and delivers it to the recipient. The server is in the middle. The server may be honest. It may be audited. It may operate in a favorable jurisdiction and under a strict privacy policy. All of that may be true. But the server is in the middle.

The difference between encrypting and not collecting (part two)

In a previous article in this same series, we argue that encrypting content and not collecting metadata are not the same. There is a step further that should be stated clearly: encrypting what passes through a server and not having a server are also not the same.

The first model—server in the middle, encrypted content—protects the content from the server operator, from its maintenance staff, from an external attacker compromising the system. And that is important. But it does not eliminate the server. The server is still there. It continues to process metadata. It remains a point that can receive a subpoena, legal intervention, political pressure, or a security breach. It remains a point that requires placing trust in someone.

The second model—no server between the two ends—does not protect the encrypted content better: if the cryptography is solid, the content is protected in both cases. What changes is not the content. What changes is that the question *"what about the server?"* ceases to have an object, because there is no server to ask about.

Trust, absence, and the difference between them

Trust can be well placed. Honest companies exist. Rigorous auditors exist. User-friendly laws exist. Serious services that strictly comply with all of the above exist. Trust, when granted to an operator who deserves it, is not a bad arrangement.

But trust, however solid, remains trust. It is a social solution, not a technical one. A company can change hands. A jurisdiction can change government. A court order can arrive tomorrow. A new vulnerability can be discovered next month. None of this happens in bad faith. It happens because the operator exists, and everything that exists is subject to the contingencies of the world.

The absence of an operator is not subject to those same contingencies. A court order cannot request data from a server that does not exist. An attacker cannot compromise a server that does not exist. A change in a company's policy cannot affect data that the company never had. The key phrase is simple: data that does not exist cannot be lost.

On the legitimate server-side argument

Whoever offers a professional messaging service with a server in the middle usually formulates three perfectly valid arguments. First, that the server is necessary to guarantee delivery when the recipient is offline. Second, that the encryption of the content is robust and therefore the operator cannot read it. Third, that the service complies with European legislation and that the data is protected by law.

All three arguments are true. None change the nature of the matter. It is true that a server allows storing messages for delayed delivery; it is also true that delayed delivery can be solved in another way, through direct device-to-device communication protocols refined for decades and operational today. It is true that the encryption of content in transit is robust in serious services. And it is true that European legislation protects users more than that of many other places.

The question is not whether services with a server in the middle are legal, nor whether they are secure, nor whether they protect the content. They can be, they are legal, and they are usually secure. The question is that having a server in the middle is an architectural choice, not a technical imposition. And every choice has consequences. An architecture with a server in the middle necessarily creates an actor that must be trusted. An architecture without a server in the middle does not.

What the law says, and what the architecture does

The GDPR does not require a specific architectural model. It requires results: data minimization, purpose limitation, data protection by design and by default, the ability to demonstrate compliance. A service with a server in the middle can meet all these requirements. A service without a server in the middle meets several of them by construction, not by declaration. Absolute minimization—not collecting anything that is not strictly necessary to deliver the message—is trivial when there is no server that can collect anything.

For non-sensitive everyday uses, a server architecture is perfectly reasonable, and trust in a serious operator is a valid arrangement. For other uses—those bearing regulated professional secrecy, those involving ethical responsibility, those touching particularly sensitive information—the absence of a point of trust is not a luxury, it is a structural advantage.

For the professional reader

The questions that should be asked of a professional communication service, already familiar from previous articles in this series, are completed with just one more architectural question:

1. Does it encrypt content in transit? (Probably yes.)
2. Does it generate and store metadata about who I talk to and when? (Probably yes.)
3. Is there a server on the path between my device and the recipient's?
4. If it exists: who operates it, in what jurisdiction, and what would have to happen for them to hand over data about me?

5. If it doesn't exist: the previous questions are irrelevant.

The difference between the two categories is not one of degree, but of kind. When the time comes to explain it to a client, a patient, or a colleague, the most honest formulation is also the simplest: in one there is someone in the middle; in the other, no.

This article closes the initial cycle of Cuadernos Lacre. After talking about encryption, metadata, and professional secrecy, we complete the architectural picture: encrypting the content and not having a server in the middle are different things. Both can be legal; only one eliminates the point of trust.

Sources and further reading

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Foundational text of the principle according to which the guarantees of a system must be implemented at the ends, not in the intermediate channel.
- Regulation (EU) 2016/679, art. 25 — data protection by design and by default.
- Regulation (EU) 2016/679, art. 5.1.c — data minimization principle.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Chapters on architectures that minimize collection by construction.

← PreviousGDPR and Professional Messaging: Why Most Are Non-Compliant Without Knowing ItNext →CUADERNOS_LIST_SCHREMS_TITLE

Recent readings

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Take this article wherever you need it.

↓ Markdown ↓ Plain text ↓ PDF

The file is downloaded to your device. From there, you can save it, import it into Solo2, or share it as you wish. Cuadernos does not decide the destination for you.

Wax seal · SHA-256 50ed016af6f46d383c0531bf9302bd34f990c0a8e5e8e1f05b7ef8f4cc36c120

Cuadernos Lacre · A publication of Menzuri Gestión S.L. ·
written by R.Eugenio · edited by the team of Solo2.