Análise · 16 de maio de 2026

← Anterior·Seguinte →

Cando non hai ninguén no medio

Cifrar o que pasa por un servidor protexe o contido. Non ter servidor no medio elimina a pregunta. Non son o mesmo.

Dúas persoas, unha conversa

Cando dúas persoas falan cara a cara nunha habitación, ninguén ten que prometer que non ouviu nada. Non ouviu porque non estaba. Cando dúas persoas pásanse un papel dunha man á outra, ninguén no medio ten que xurar que non o leu. Non hai ninguén no medio.

A maior parte das cousas na vida cotiá funcionan así. Non asinamos acordos de confidencialidade co aire que transmite a nosa voz, nin co papel que sostemos. A privacidade da conversa non descansa sobre a promesa dun intermediario, porque non hai intermediario. Esa é unha das formas máis fortes que existe de ser privado: non porque algo ou alguén se comporte ben, senón porque non hai algo ou alguén.

Cando a conversa trasládase a unha canle dixital, isto cambia por defecto. O modelo habitual é o seguinte: dúas persoas conéctanse a un servidor, o servidor recibe a mensaxe, cífraa ou gárdaa cifrada, e entrégalla ao destinatario. O servidor está no medio. O servidor pode ser honesto. Pode estar auditado. Pode operar nunha xurisdición favorable e baixo unha política de privacidade estrita. Todo iso pode ser certo. Pero o servidor está no medio.

A diferenza entre cifrar e non recoller (segunda parte)

Nun artigo anterior desta mesma serie sostemos que cifrar o contido e non recoller metadatos non son o mesmo. Hai un paso máis alá que convén formular con claridade: cifrar o que pasa por un servidor e non ter servidor son tampouco o mesmo.

O primeiro modelo —servidor no medio, contido cifrado— protexe o contido do operador do servidor, do seu persoal de mantemento, dun atacante externo que comprometa o sistema. E iso é importante. Pero non elimina ao servidor. O servidor segue aí. Segue procesando metadatos. Segue sendo un punto que pode recibir un requirimento xudicial, unha intervención legal, unha presión política, ou unha fenda de seguridade. Segue sendo un punto que require depositar confianza en alguén.

O segundo modelo —non haber servidor entre os dous extremos— non protexe mellor o contido cifrado: se a criptografía es sólida, o contido vai protexido en ambos casos. O que cambia non é o contido. O que cambia é que a pregunta *«que pasa co servidor?»* deixa de ter obxecto, porque non existe servidor sobre o que preguntar.

Confianza, ausencia, e a diferenza entre ambas

A confianza pode estar ben depositada. Empresas honestas existen. Auditores rigorosos existen. Lexislacións favorables ao usuario existen. Servizos serios que cumpren escrupulosamente con todo o anterior existen. A confianza, cando se concede a un operador que a merece, non é un mal arranxo.

Pero a confianza, por sólida que sexa, segue sendo confianza. É unha solución social, nunha solución técnica. Unha empresa pode cambiar de mans. Unha xurisdición pode cambiar de goberno. Unha orde xudicial pode chegar mañá. Unha vulnerabilidade nova pode descubrirse o mes que vén. Nada disto sucede por mala fe. Sucede porque o operador existe, e todo o que existe está suxeito ás continxencias do mundo.

A ausencia dun operador non está suxeita a esas mesmas continxencias. Unha orde xudicial non pode pedir datos a un servidor que non existe. Un atacante non pode comprometer un servidor que non existe. Un cambio na política dunha empresa non pode afectar a datos que esa empresa nunca tivo. A frase clave é sinxela: os datos que non existen non se poden perder.

Sobre o argumento lexítimo do lado do servidor

Quen ofrece un servizo de mensaxería profesional con servidor no medio adoita formular tres argumentos perfectamente válidos. Primeiro, que o servidor é necesario para garantir a entrega cando o destinatario está desconectado. Segundo, que o cifrado do contido é robusto e por tanto o operador non pode lelo. Terceiro, que o servizo cumpre a lexislación europea e que os datos están protexidos pola lei.

Os tres argumentos son certos. Ningún cambia a natureza do asunto. É certo que un servidor permite almacenar mensaxes para entrega diferida; tamén é certo que a entrega diferida pode resolverse de outra forma, mediante protocolos de comunicación directa entre dispositivos refinados desde hai décadas e operativos hoxe. É certo que o cifrado do contido en tránsito é robusto nos servizos serios. E é certo que a lexislación europea protexe aos usuarios máis que a de moitos outros lugares.

A cuestión non é se os servizos con servidor no medio son legais, nin se son seguros, nin se protexen o contido. Poden selo, son legais, e adoitan ser seguros. A cuestión é que ter un servidor no medio é unha elección arquitectónica, non unha imposición técnica. E cada elección ten consecuencias. Unha arquitectura con servidor no medio xera necesariamente un actor no que hai que confiar. Unha arquitectura sen servidor no medio non.

O que a lei di, e o que a arquitectura fai

O RGPD non esixe un modelo arquitectónico concreto. Esixe resultados: minimización de datos, finalidade limitada, protección desde o deseño e por defecto, capacidade de demostrar o cumprimento. Un servizo con servidor no medio pode cumprir todos estes requisitos. Un servizo sen servidor no medio cumpre varios deles por construción, non por declaración. A minimización absoluta —non recoller nada que non sexa estrictamente necesario para entregar a mensaxe— é trivial cando non existe un servidor que poida recoller algo.

Para os usos cotiáns non sensibles, unha arquitectura con servidor é perfectamente razoable, e a confianza nun operador serio é un arranxo válido. Para os outros usos —os que levan segredo profesional reglado, os que conlevan responsabilidade deontolóxica, os que tocan información especialmente sensible— a ausencia dun punto de confianza non é un luxo, é unha vantaxe estrutural.

Para o lector profesional

As preguntas que convén facerse ante un servizo de comunicación profesional, xa familiares de artigos anteriores nesta mesma serie, complétanse cunha soa pregunta arquitectónica máis:

1. Cifra o contido en tránsito? (Probablemente si.)
2. Xera e almacena metadatos sobre con quen falo e cando? (Probablemente si.)
3. Existe un servidor no camiño entre o meu dispositivo e o do destinatario?
4. Se existe: quen o opera, en que xurisdición, e que tería que ocorrer para que entregase datos sobre min?
5. Se non existe: as preguntas anteriores non teñen obxecto.

A diferenza entre as dúas categorías non é de grao, senón de tipo. Chegado o momento de explicarllo a un cliente, a un paciente, ou a un colega, a formulación máis honesta é tamén a máis sinxela: nunha hai alguén no medio; na outra, non.

Este artigo pecha o ciclo inicial de Cuadernos Lacre. Tras falar do cifrado, os metadatos e o segredo profesional, completamos o cadro arquitectónico: cifrar o contido e non ter servidor no medio son cousas distintas. As dúas poden ser legais; só unha elimina o punto de confianza.

Fontes e lectura adicional

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Texto fundacional do principio segundo o cal as garantías dun sistema deben implementarse nos extremos, non na canle intermedia.
- Regulamento (UE) 2016/679, art. 25 — protección de datos desde o deseño e por defecto.
- Regulamento (UE) 2016/679, art. 5.1.c — principio de minimización de datos.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Capítulos sobre arquitecturas que minimizan a recolección por construción.

← AnteriorRGPD e mensaxería profesional: por que a maioría incumpre sen sabeloSeguinte →CUADERNOS_LIST_SCHREMS_TITLE

Lecturas recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Leva este artigo onde o necesites.

↓ Markdown ↓ Texto plano ↓ PDF

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 4e91abf7c4e0a776b619680e7f308b6f1e1b10581d90cf731b0a2cbfb0885f6d

Cuadernos Lacre · Unha publicación de Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada polo equipo de Solo2.