Analyse · 16 mai 2026

← Précédent·Suivant →

Quand il n'y a personne au milieu

Chiffrer ce qui passe par un serveur protège le contenu. Ne pas avoir de serveur au milieu élimine la question. Ce n'est pas la même chose.

Deux personnes, une conversation

Lorsque deux personnes parlent face à face dans une pièce, personne n'a à promettre qu'il n'a rien entendu. Il n'a rien entendu parce qu'il n'était pas là. Lorsque deux personnes se passent un papier de la main à la main, personne au milieu n'a à jurer qu'il ne l'a pas lu. Il n'y a personne au milieu.

La plupart des choses dans la vie quotidienne fonctionnent ainsi. Nous ne signons pas d'accords de confidentialité avec l'air qui transmet notre voix, ni avec le papier que nous tenons. La confidentialité de la conversation ne repose pas sur la promesse d'un intermédiaire, car il n'y a pas d'intermédiaire. C'est l'une des formes les plus fortes d'intimité qui soit : non pas parce que quelque chose ou quelqu'un se comporte bien, mais parce qu'il n'y a rien ni personne.

Lorsque la conversation passe à un canal numérique, cela change par défaut. Le modèle habituel est le suivant : deux personnes se connectent à un serveur, le serveur reçoit le message, le chiffre ou le garde chiffré, et le remet au destinataire. Le serveur est au milieu. Le serveur peut être honnête. Il peut être audité. Il peut opérer dans une juridiction favorable et sous une politique de confidentialité stricte. Tout cela peut être vrai. Mais le serveur est au milieu.

La différence entre chiffrer et ne pas collecter (deuxième partie)

Dans un article précédent de cette même série, nous soutenions que chiffrer le contenu et ne pas collecter de métadonnées n'est pas la même chose. Il y a une étape supplémentaire qu'il convient de formuler clairement : chiffrer ce qui passe par un serveur et ne pas avoir de serveur n'est pas non plus la même chose.

Le premier modèle — serveur au milieu, contenu chiffré — protège le contenu de l'opérateur du serveur, de son personnel de maintenance, d'un attaquant externe qui compromettrait le système. Et c'est important. Mais cela n'élimine pas le serveur. Le serveur est toujours là. Il continue de traiter les métadonnées. Il reste un point qui peut recevoir une demande judiciaire, une intervention légale, une pression politique ou une faille de sécurité. Il reste un point qui nécessite de placer sa confiance en quelqu'un.

Le second modèle — ne pas avoir de serveur entre les deux extrémités — ne protège pas mieux le contenu chiffré : si la cryptographie est solide, le contenu est protégé dans les deux cas. Ce qui change n'est pas le contenu. Ce qui change, c'est que la question *« qu'en est-il du serveur ? »* n'a plus d'objet, car il n'existe pas de serveur sur lequel s'interroger.

Confiance, absence, et la différence entre les deux

La confiance peut être bien placée. Entreprises honnêtes existent. Auditeurs rigoureux existent. Législations favorables à l'utilisateur existent. Services sérieux qui respectent scrupuleusement tout ce qui précède existent. La confiance, lorsqu'elle est accordée à un opérateur qui la mérite, n'est pas un mauvais arrangement.

Mais la confiance, aussi solide soit-elle, reste de la confiance. C'est une solution sociale, pas une solution technique. Une entreprise peut changer de mains. Une juridiction peut changer de gouvernement. Un ordre judiciaire peut arriver demain. Une nouvelle vulnérabilité peut être découverte le mois prochain. Rien de tout cela n'arrive par mauvaise foi. Cela arrive parce que l'opérateur existe, et tout ce qui existe est sujet aux contingences du monde.

L'absence d'un opérateur n'est pas sujette à ces mêmes contingences. Une ordonnance judiciaire ne peut pas demander de données à un serveur qui n'existe pas. Un attaquant ne peut pas compromettre un serveur qui n'existe pas. Un changement dans la politique d'une entreprise ne peut pas affecter des données que cette entreprise n'a jamais eues. La phrase clé est simple : les données qui n'existent pas ne peuvent pas être perdues.

Sur l'argument légitime du côté serveur

Celui qui propose un service de messagerie professionnel avec serveur au milieu formule généralement trois arguments parfaitement valables. Premièrement, que le serveur est nécessaire pour garantir la livraison lorsque le destinataire est déconnecté. Deuxièmement, que le chiffrement du contenu est robuste et que l'opérateur ne peut donc pas le lire. Troisièmement, que le service respecte la législation européenne et que les données sont protégées par la loi.

Les trois arguments sont vrais. Aucun ne change la nature du problème. Il est vrai qu'un serveur permet de stocker des messages pour une livraison différée ; il est également vrai que la livraison différée peut être résolue d'une autre manière, par le biais de protocoles de communication directe entre appareils, affinés depuis des décennies et opérationnels aujourd'hui. Il est vrai que le chiffrement du contenu en transit est robuste dans les services sérieux. Et il est vrai que la législation européenne protège les utilisateurs plus que celle de bien d'autres endroits.

La question n'est pas de savoir si les services avec serveur au milieu sont légaux, ni s'ils sont sûrs, ni s'ils protègent le contenu. Ils peuvent l'être, ils sont légaux et ils sont généralement sûrs. La question est que le fait d'avoir un serveur au milieu est un choix architectural, pas une imposition technique. Et chaque choix a des conséquences. Une architecture avec serveur au milieu génère nécessairement un acteur auquel il faut faire confiance. Une architecture sans serveur au milieu non.

Ce que la loi dit, et ce que l'architecture fait

Le RGPD n'exige pas de modèle architectural concret. Il exige des résultats : minimisation des données, finalité limitée, protection dès la conception et par défaut, capacité de démontrer la conformité. Un service avec serveur au milieu peut répondre à toutes ces exigences. Un service sans serveur au milieu en respecte plusieurs par construction, et non par déclaration. La minimisation absolue — ne rien collecter qui ne soit strictement nécessaire pour livrer le message — est triviale lorsqu'il n'existe pas de serveur capable de collecter quoi que ce soit.

Pour les usages quotidiens non sensibles, une architecture avec serveur est parfaitement raisonnable, et la confiance en un opérateur sérieux est un arrangement valable. Pour les autres usages — ceux qui relèvent du secret professionnel réglementé, ceux qui entraînent une responsabilité déontologique, ceux qui touchent à des informations particulièrement sensibles — l'absence d'un point de confiance n'est pas un luxe, c'est un avantage structurel.

Pour le lecteur professionnel

Les questions qu'il convient de se poser face à un service de communication professionnel, déjà familières d'articles précédents de cette même série, se complètent d'une seule question architecturale supplémentaire :

1. Chiffre-t-il le contenu en transit ? (Probablement oui.)
2. Génère-t-il et stocke-t-il des métadonnées sur qui je parle et quand ? (Probablement oui.)
3. Existe-t-il un serveur sur le chemin entre mon appareil et celui du destinataire ?
4. S'il existe : qui l'opère, dans quelle juridiction, et que devrait-il se passer pour qu'il livre des données sur moi ?
5. S'il n'existe pas : les questions précédentes n'ont pas d'objet.

La différence entre les deux catégories n'est pas de degré, mais de type. Au moment de l'expliquer à un client, à un patient ou à un collègue, la formulation la plus honnête est aussi la plus simple : dans l'une, il y a quelqu'un au milieu ; dans l'autre, non.

Cet article clôt le cycle initial de Cuadernos Lacre. Après avoir parlé du chiffrement, des métadonnées et du secret professionnel, nous complétons le tableau architectural : chiffrer le contenu et ne pas avoir de serveur au milieu sont des choses différentes. Les deux peuvent être légales ; une seule élimine le point de confiance.

Sources et lectures complémentaires

- Saltzer, J. H. ; Reed, D. P. ; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Texte fondateur du principe selon lequel les garanties d'un système doivent être implémentées aux extrémités, pas dans le canal intermédiaire.
- Règlement (UE) 2016/679, art. 25 — protection des données dès la conception et par défaut.
- Règlement (UE) 2016/679, art. 5.1.c — principe de minimisation des données.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Chapitres sur les architectures qui minimisent la collecte par construction.

← PrécédentRGPD et messagerie professionnelle : pourquoi la majorité est en infraction sans le savoirSuivant →CUADERNOS_LIST_SCHREMS_TITLE

Lectures recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Emportez cet article où vous en avez besoin.

↓ Markdown ↓ Texte brut ↓ PDF

Le fichier est téléchargé sur votre appareil. À partir de là, vous pouvez l'enregistrer, l'importer dans Solo2 ou le partager comme vous le souhaitez. Cuadernos ne décide pas de la destination pour vous.

Cachet de cire · SHA-256 330e9bdb27ebb0be4705465fd18df6d9ab4b47af5628f9692c1296af0d74c48f

Cuadernos Lacre · Une publication de Menzuri Gestión S.L. ·
écrite par R.Eugenio · éditée par l'équipe de Solo2.