Qui suis-je et quelle est mon identité ?

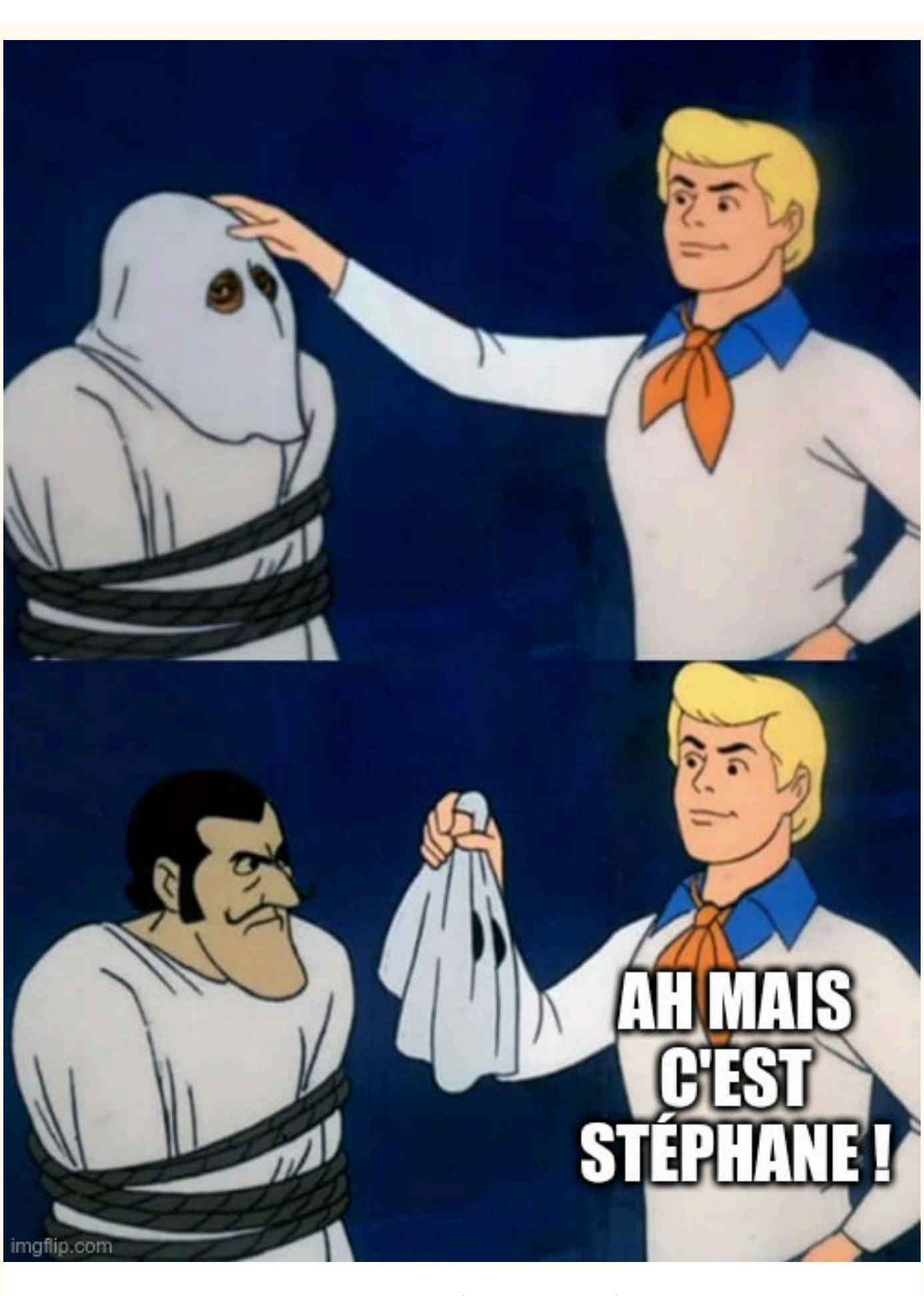
par Stéphane Bortzmeyer | 20 déc 2025 | 13 min

On parle souvent dans le monde numérique, par exemple à propos de l'Internet, d'**identité**. Un ministre annonce qu'on va avoir une « identité numérique ». Un article dans les médias dit qu'un harceleur en ligne utilisait « une fausse identité ». On vous explique qu'une fuite de données peut augmenter le risque d'« usurpation d'identité ». On vous dit que Google ou Meta sont « fournisseurs d'identité ». Qu'est-ce qui se cache derrière ce mot ?

Avertissement ajouté en dernière minute :

Le thème de l'identité est d'actualité en ce mois de décembre 2025, avec de nombreuses fuites de données personnelles, y compris depuis des organismes publics ou para-publics. Et ceci dans l'indifférence la plus totale des politiciens.

Ce n'est pas directement le sujet de cet article, mais cela donne à réfléchir sur la sécurité de l'identité « officielle », étatique.



Ah, mais c'est pas un méchant ! C'est Stéphane !

Il y a deux points importants derrière l'identité et notamment l'identité numérique : quelle est la **source** de l'identité et comment **prouver** son identité.

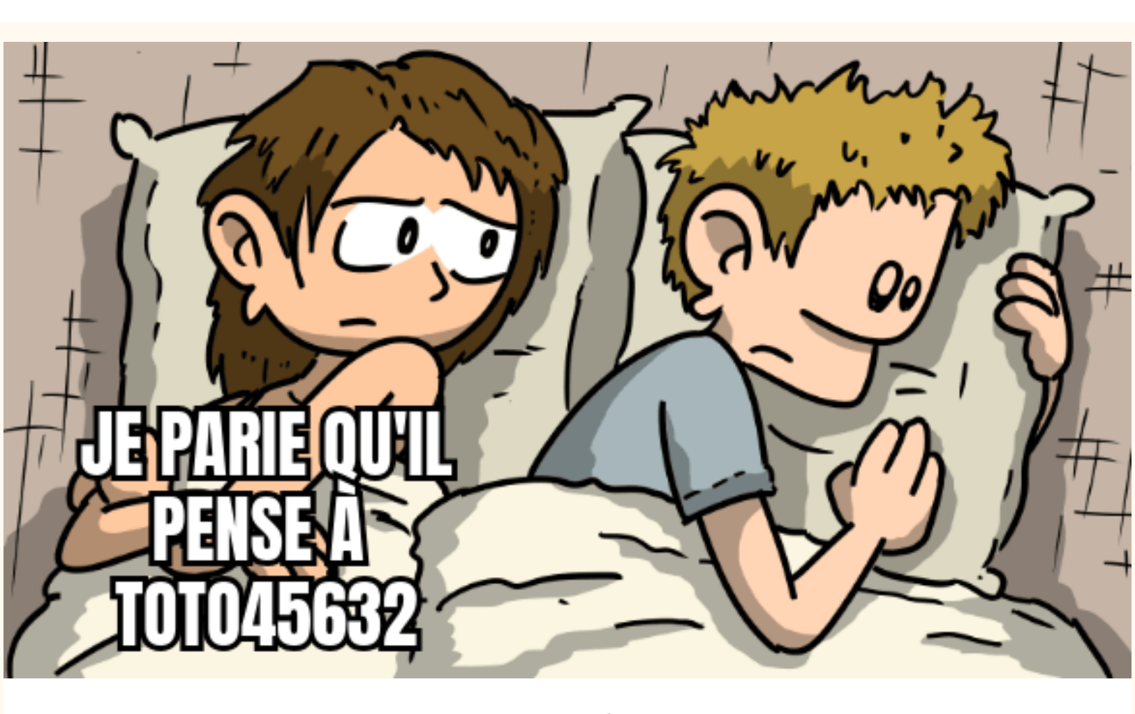
Définition approximative

Il existe d'innombrables définitions du concept d'identité (rien que la page Wikipédia sur l'identité numérique en liste beaucoup). Je me limiterai ici à l'identité au sens concret, ce que les autres voient de vous et qui se prouve par des moyens techniques en ligne.

L'identité, c'est ce qui permet d'avoir une traçabilité de ses actions et donc de sa réputation ou de ses droits et devoirs. Si je lis un article de Zythom et que je le trouve très intéressant, l'identité derrière ce nom va me permettre de juger, dans le futur, si je vais lire un nouvel article ou pas. Auprès de votre banque (ou de votre place de marché en cryptomonnaies), l'identité est ce qui fera que votre banque acceptera, ou pas, de faire un paiement, et pour quel montant : la banque a tracé vos précédentes actions (ajouter de l'argent sur le compte, en retirer), et déduira de la somme de ces actions si elle accepte l'opération demandée.

L'identité se matérialise souvent dans un **identificateur**, une suite de caractères qui vous est unique. Cela peut être « Toto45632 », « @bortzmeyer:underworld.fr », « Jean Durand » ou « 1709900166642 ». Dans certains cas, un identificateur simple ne suffit pas, et on ajoute des détails (« Jean Durand, né le 1 janvier 1970 à Chérence »).

Un point important est qu'une personne physique (ou une organisation) peut avoir plusieurs identités, pas forcément reliées entre elles, et que c'est à la fois légal et légitime. Aucune de ces identités n'est plus « réelle » qu'une autre, elles reflètent différents aspects de la personne. Pensez à la notion de marque pour une entreprise : la Société Anonyme des Huiles Duchmoll (que personne ne connaît) commercialise les pastilles « DuGenou » (dont tout le monde a entendu parler). Elle peut sortir un nouveau produit, sous une nouvelle marque (« DeCoude »), et ce sera une nouvelle « identité », une de plus. Pour une personne physique, « Toto45632 » peut être son identité sur Instagram et « Marine Dupont, cheffe de projet » son identité sur LinkedIn et elle ne souhaite pas forcément qu'on relie ces identités.



« Je parie qu'il pense à Toto45632 »

S'il n'y a pas de traçabilité, si vos actions en ligne ne peuvent pas être reliées les unes aux autres, c'est l'anonymat. Contrairement à ce qu'affirme un discours sécuritaire très répandu chez les politiciens et les médias, l'anonymat en ligne est extrêmement difficile à atteindre. Toute action laisse une trace numérique, qu'on peut, plus ou moins facilement, corréler à d'autres traces. Être anonyme, en ligne, nécessite des compétences techniques pointues et un soin de tous les instants. En général, quand un ministre ou un député parle de l'anonymat qui serait soi-disant la règle sur l'Internet, il parle juste de la difficulté à relier les identités en ligne à l'identité officielle de l'État. Et même cette difficulté cède vite lorsque l'enquête est menée sérieusement, comme le découvrent régulièrement des harceleurs qui se sont attaqués à une personnalité publique, croyant qu'ils étaient anonymes, et qui se retrouvent devant les tribunaux.

La source de l'identité

La source de l'identité, c'est le mécanisme social qui va attribuer à une personne, ou une organisation une identité et, en général, un identificateur. Si vous créez un compte Gmail en choisissant l'identificateur « rebeccaDu95 », c'est Google, propriétaire de Gmail, qui va décider si vous pouvez utiliser cet identificateur. Il pourrait être refusé pour des raisons syntaxiques (interdiction de certains caractères), sémantiques (certains mots peuvent être tabous) ou tout simplement parce qu'il est déjà pris. Par la suite, c'est la source de l'identité, le fournisseur d'identité, qui va vérifier, par divers moyens techniques, que c'est bien votre identité. Si vous avez déjà correspondu avec « rebeccaDu95@gmail.com », vous lirez ces messages (ou pas) en fonction de ces interactions préalables et, sinon, vous traiterez cette personne en inconnue. Le fait que « rebeccaDu95@gmail.com » soit, ou pas, la même personne que « Jean Durand, né le 1 janvier 1970 à Chérence » n'est pas forcément une information pertinente. Ce sont des identités différentes.

Le point important est que, contrairement à ce que peuvent faire croire certains discours, l'identité n'est pas forcément l'identité étatique, celle attribuée par l'état civil à votre naissance, et que l'État présente souvent comme « la seule vraie », comme « l'identité réelle ». Croire ou faire semblant de croire que « identité » désigne forcément cette identité étatique est un choix politique (et un mauvais choix, je précise).

Si vous êtes fan de Johnny Hallyday ou de Léna Situations, vous n'avez pas forcément besoin de connaître leur identité étatique (parler de leurs « vrais noms » serait erroné ; en quoi seraient-ils plus vrais que l'identificateur qu'ielles ont choisi, et sur lequel a été fondé leur carrière ?)

Des identificateurs comme « rebeccaDu95 » ou « Toto45632 » sont parfois qualifiés de « pseudonymes ». Le terme a l'intérêt de faire la différence avec l'anonymat, mais il est contestable parce qu'il privilégie une seule identité, en général l'identité étatique (comme « Jean-Philippe Smet » et « Lena Mahfouf »), reléguant les autres au statut de « pseudonymes ».

On peut parfois avoir une identité même sans avoir explicitement créé son compte et sans avoir d'identificateur. Meta crée ainsi un « profil fantôme » des utilisateurs qui interagissent avec ses plates-formes sans avoir de compte, profil fondé sur les informations disponibles, et qui servira si un jour cette personne se crée un compte Facebook ou autre.

On parle parfois d'« identité souveraine » lorsqu'elle a été définie uniquement par vous, sans aucune participation d'une entité extérieure à vous. C'est le cas par exemple avec des logiciels de communication pair-à-pair.

Prouver son identité

Ce n'est pas tout d'avoir une identité, on peut être obligé de la prouver, ce qu'on appelle s'**authentifier**. Si je me présente à la porte de l'Élysée en disant que je suis Emmanuel Macron, président de la République, gageons qu'on ne me laissera pas entrer sans vérification. Même chose si je me connecte au site Web de ma banque pour retirer de l'argent, ou bien si je veux me connecter à mon instance fédivers (un réseau social décentralisé) pour ensuite envoyer des messages. Si n'importe qui pouvait le faire, la réputation du titulaire de l'identité en souffrirait injustement.

Prouver son identité, ou bien certaines caractéristiques liées à l'identité, comme l'âge, la nationalité ou d'autres attributs, est un problème ancien. Les Romains de l'Antiquité y pensaient déjà. (Comment Saint Paul prouvait-il qu'il était citoyen romain ?)

Il existe des cadres de gestion de l'authentification comme l'eIDAS de l'Union Européenne mais je ne trouve pas qu'ils éclaircissent cette question très riche, c'est plutôt le contraire.

Souvent on confond la source de l'identité avec le mécanisme de preuve, d'authentification. Ainsi, des systèmes comme eIDAS cités plus haut ne créent pas du tout de nouvelle identité (cela reste l'identité étatique classique), uniquement des nouveaux moyens (numériques et non plus papier) de la prouver et donc de l'utiliser.

Les différentes méthodes pour prouver une identité ont des caractéristiques très différentes : elles sont plus ou moins sûres, et plus ou moins pratiques d'utilisation. En outre, comme souvent dans le monde numérique, les commerciaux qui essaient de vous vendre telle ou telle technique d'authentification n'expliquent pas forcément bien ces caractéristiques, en admettant qu'ils les comprennent eux-mêmes.

En ligne, sur des réseaux comme l'Internet, une des techniques les plus utilisées pour prouver son identité est le classique mot de passe. C'est une technique simple, aussi bien pour la personne qui programme le système d'authentification que pour la personne qui s'authentifie. Par contre, elle a plusieurs défauts de sécurité : le mot de passe doit être difficile à deviner (donc, il ne faut pas utiliser « azerty123 »), il faut le mémoriser (il est très recommandé d'utiliser un logiciel gestionnaire de mots de passe) et il faut le communiquer au service auprès duquel on s'authentifie (comme disait ma grand-mère, un secret qu'on partage n'est plus un secret). Par exemple, en cas d'hameçonnage (vous savez, le message qui dit « ici votre banque, nous avons détecté un mouvement de fonds suspect, connectez-vous en `https://secure-bank.example.ly/confirm` pour vous authentifier et confirmer que c'est bien vous »), une fois que le mot de passe a été transmis à la fausse banque, il a fuité, il n'y a pas d'autres solution que de le changer.

Pour la même raison, toute méthode d'authentification qui, comme les mots de passe, repose sur une information que vous envoyez à la plate-forme d'en face, et qu'elle pourra réutiliser, est dangereuse. Envoyer une copie de ses documents d'identité étatique est par exemple très imprudent. (Au moins, ajoutez un filigrane, comme le permet l'excellent service `https://filigrane.beta.gouv.fr/`.)

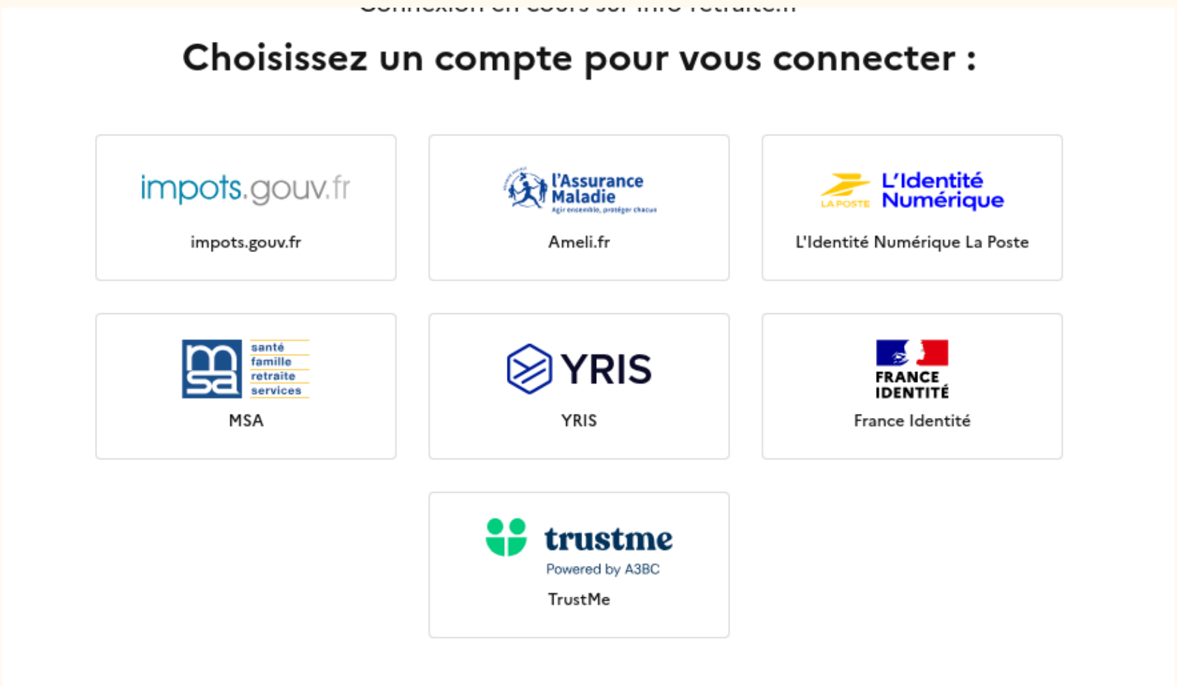
Il existe d'innombrables autres méthodes d'authentification. Aucune n'est parfaite, quoi que puisse en dire le marketing, qui nous assomme régulièrement de propagande sur le thème « plus besoin de mémoriser un mot de passe grâce à notre méthode sophistiquée absolument sécure ». Si vous entendez de tels discours publicitaires, il faut creuser pour voir quels sont les inconvénients de cette méthode d'authentification. Il y en a forcément, puisqu'on ne vit pas dans un monde idéal. Par exemple, la biométrie, qui a souvent été présentée comme méthode idéale, cumule les inconvénients : en cas de compromission, on ne peut pas changer ses empreintes digitales ou sa rétine et elle est réutilisable par le serveur auprès duquel on s'est authentifié.

Comme exemple d'une méthode d'authentification qui ne nécessite pas d'envoyer des informations qu'un attaquant pourrait réutiliser, on peut citer WebAuthn (ex-FIDO), où les merveilles de la cryptographie dite « asymétrique » sont utilisées pour prouver votre identité à un service en ligne sans lui donner d'information d'authentification. Ainsi, même si sa base de données est complètement piratée, le pirate ne pourra pas se faire passer pour vous. Mais cela veut dire qu'il faut prendre soin de la clé privée que vous devez garder (sur un ordinateur ou bien un petit truc spécialisé que vous mettez dans le port USB de l'ordinateur). Si vous perdez cette clé privée, vous ne pouvez plus vous connecter, si elle est prise par un attaquant, il peut se faire passer pour vous. Je le répète, il n'y a pas de solution idéale.

On suggère parfois de combiner deux techniques, ce qu'on nomme l'authentification à deux (ou plus) facteurs. Le risque d'usurpation devient alors plus faible, mais le risque de ne pas pouvoir se connecter, parce qu'on a perdu un des deux facteurs, augmente.

Puisqu'on a parlé de cryptographie asymétrique, notons qu'il existe donc des techniques d'authentification très sûres et qui ne nécessitent pas d'utiliser l'identité étatique. Elles sont par exemple utilisées pour les cryptomonnaies (votre identité sur Bitcoin est une clé privée qui, comme son nom l'indique, n'est jamais transmise, à personne). C'est une très bonne solution technique mais, comme indiqué plus haut, si vous perdez la clé privée, vous ne pourrez plus vous authentifier. Ces identités souveraines, et authentifiées par cryptographie asymétrique, sont également utilisées dans des systèmes comme PGP (Pretty Good Privacy, pour la sécurité du courrier électronique), Signal ou SimpleX (messagerie instantanée).

L'authentification peut être déléguée à un ou plusieurs fournisseur(s) d'identité, ce qui augmente la souplesse du système. C'est le cas du système FranceConnect. Il n'existe pas de « compte FranceConnect ». Quand un site Web veut vérifier votre identité étatique via FranceConnect, ce dernier agira uniquement comme intermédiaire avec des fournisseurs d'identité comme les impôts ou Ameli (la Sécurité Sociale) et ce sont ces fournisseurs qui vous authentifieront, pas FranceConnect.


Choisissez un compte pour vous connecter :

Fin 2025, voici la liste des fournisseurs d'identité que FranceConnect proposait au visiteur.

(Attention à ne pas confondre FranceConnect avec FranceConnect+, qui est très différent.)

Je l'ai dit, il n'existe pas de solution d'authentification parfaite et le choix va donc dépendre des critères qu'on privilégie. Ainsi, certaines techniques d'authentification peuvent être néfastes pour la vie privée. Si, pour empêcher les mineurs d'accéder aux sites Web pornographiques, on demande qu'un tiers puisse prouver aux sites en question que vous êtes majeur, la seule inscription auprès de ce tiers montrera votre intention de visiter des sites porno, ce qui n'est pas idéal pour la vie privée. (Même si parfois certains essaient de brouiller le problème en parlant de « double anonymat ».)

De même, certaines solutions d'authentification soulèvent des problèmes quant à l'autonomie stratégique des utilisateurices, et des pays. Si vous gérez un site Web et que vous proposez une authentification par le fournisseur d'identité qu'est Google, vous agissez comme rabatteur bénévole pour cette grosse entreprise étatsunienne, puisque vous encouragez vos visiteurs à confier des données à Google.

Le quotidien Le Monde propose d'abord de s'authentifier en utilisant un compte Google ou un compte Apple.

Conclusion

Ce n'était qu'un bref survol de la question très riche et très complexe de l'identité, notamment numérique. Je voulais surtout insister sur le fait que l'identité n'était pas forcément l'identité étatique, et qu'il faut bien séparer la définition d'une identité, de la ou des technique(s) qui seront utilisées pour vérifier cette identité.

Article précédent Article suivant

Classé dans : Droits numériques, Enjeux du numérique, Libertés numériques
authentification , identité

Qui a publié cet article ? Articles récents

Stéphane Bortzmeyer

3 Réponses

soso 21 décembre 2025

Petit correctif, WebAuthn n'est pas « ex-FIDO » comme mentionné dans l'article. WebAuthn et FIDO existent tous les deux. FIDO est le standard définit par l'alliance FIDO, qui est plus général que ce que les navigateurs implémentent, et WebAuthn est l'API JavaScript proposé par les navigateurs pour y avoir accès.

D’ailleurs le lien sur le mot FIDO pointe vers U2F, qui lui est le prédécesseur de FIDO et WebAuthn qui les remplacent désormais.

Répondre

Stéphane Bortzmeyer

21 décembre 2025

OK, j’ai du mal avec ces nouvelles techniques, souvent mal documentées en prime (et encore, je n’ai pas parlé des passkeys !). Le point important est qu’on continue à en inventer des nouvelles, mais sans toujours expliciter leurs forces et faiblesses. (S’authentifier via WebAuthN n’est pas forcément très sécurisé si la clé privée est sur une clé physique qui n’a pas d’autre protection que la nécessité de l’avoir en main.)

Répondre

Cigaes

21 décembre 2025

J’ai un peu regardé WebAuthn, et j’ai conclu que c’était plus un mécanisme pour augmenter l’allégeance à Google ou Apple qu’un vrai mécanisme pour faire de l’authentification générique sur le web.
Aucune vraie sécurité ne viendra avec l’attitude « ne cherchez pas à comprendre, la machine programmée par notre compagnie s’occupe de vous » qui préside au web depuis des années.

Répondre

Laisser un commentaire

Votre adresse e-mail ne sera pas publiée. Les champs obligatoires sont indiqués avec *

Commentaire *

Pour toutes demandes d’**aide, questions ou idées d’améliorations** sur les services de Framasoft, merci de nous contacter plutôt sur **contact.framasoft.org**.

Nom *

E-mail *

Site web

Laisser un commentaire

Framasoft

- L’association
- Notre manifeste
- Contacter Framasoft
- État des services
- Prout

Communauté

- Le forum de Framasoft
- Participer
- Bénévolat valorisé
- Partenaires
- Charte de modération

Framablog

- Entraide
- Guides et astuces
- Mentions légales
- CGU
- Crédits

Suivre Framasoft

Newsletter

Votre courriel S’abonner

Nous envoyons environ 4 messages par an pour vous informer sur l’essentiel de nos actions (voir les archives).