Engineer

Authentification

la preuve qu'une requête vient de l'identité déclarée

Ce que c’est

L’authentification est la vérification qu’un système effectue avant d’accepter une identité déclarée : une personne dit « je suis ce compte », et le système demande une preuve que seul le détenteur devrait pouvoir produire. Les ingénieurs l’abrègent souvent en authn, et les interfaces appellent ce moment « se connecter » ou « ouvrir une session ».

L’identification est la déclaration elle-même, comme saisir un nom d’utilisateur. L’authentification est la preuve de cette déclaration. L’autorisation est une décision distincte, prise ensuite, sur les actions permises à l’identité désormais connue. Même HTTP brouille la frontière : la RFC 9110 nomme 401 « Unauthorized », tout en le définissant comme une requête sans identifiants d’authentification valides et en imposant un en-tête WWW-Authenticate expliquant comment les fournir. Le code pour « nous savons qui vous êtes et la réponse reste non » est 403 Forbidden.

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer realm="api"
```

Les preuves sont de plusieurs types, généralement appelés facteurs. Ce que vous savez est un mot de passe ou un code PIN. Ce que vous possédez est un téléphone, une clé de sécurité matérielle ou un fichier de clé privée. Ce que vous êtes est une empreinte ou un visage. L’authentification multifacteur associe deux catégories différentes, pour qu’un voleur obtenant l’une manque encore de l’autre. Deux mots de passe constituent toujours un seul facteur.

Une grande partie n'implique aucune personne. Les services se présentent des jetons d'API, et SSH en montre clairement la forme machine : la RFC 4252 fait de « publickey » l'unique méthode obligatoire dans chaque mise en œuvre. Le client prouve la possession d'une clé privée par une signature : la clé ne traverse jamais le réseau. La connexion unique déplace la vérification. Avec OpenID Connect, le fournisseur d'identité authentifie l'utilisateur et remet à l'application un jeton d'identité signé, sans qu'elle voie de mot de passe. Les passkeys, fondées sur l'API Web Authentication du W3C, gardent une clé privée sur l'appareil, limitée à un site. Elles signent ensemble le défi du serveur et l'origine réellement contactée par le navigateur, afin qu'un domaine ressemblant ne reçoive rien qu'il puisse rejouer.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que l'authentification ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des comptes, mots de passe et droits attribués selon les besoins exacts de chaque poste, puis retirés le jour du départ.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Pourquoi c'est important

Chaque autre contrôle suppose celui-ci réussi. Permissions, journaux d'audit, limites de débit et facturation sont tous indexés par une identité. Si la vérification qui l'a établie est faible, chacun s'applique fidèlement à la mauvaise personne. Une ligne disant qu'un administrateur a supprimé une table enregistre le compte auteur ; seule une bonne authentification permet d'en déduire qui l'a fait.

La décision pratique est la force nécessaire pour chaque entrée, et NIST SP 800-63B fournit l'échelle la plus claire pour choisir. Son premier niveau d'assurance, AAL1, accepte un facteur. AAL2 en exige deux, avec au moins une option résistant à l'hameçonnage proposée par le vérificateur. AAL3 exige un authentificateur résistant à l'hameçonnage dont la clé privée n'est pas exportable. Le guide tranche sur un choix populaire : les codes saisis manuellement, envoyés par SMS ou affichés dans une application, ne résistent pas à l'hameçonnage. Rien ne lie leurs chiffres au site qui les a demandés.

La révision 4, qui a remplacé la révision 3 le 1er août 2025, tranche aussi plusieurs débats sur les mots de passe. Un mot de passe utilisé comme seul facteur doit compter au moins 15 caractères ; celui utilisé uniquement en connexion multifacteur au moins 8. Les vérificateurs ne peuvent imposer d'autre règle de composition ni de changement périodique, mais doivent forcer un changement en cas de preuve de compromission. Les nouveaux choix sont comparés à une liste de mots courants ou compromis, le refus est expliqué, et le stockage est salé et haché avec un mécanisme à facteur de coût. Les échecs consécutifs contre un authentificateur sont plafonnés à 100. Pour les sessions AAL2, le guide recommande une nouvelle vérification au moins toutes les 24 heures et après une heure sans activité.

Notre recommandation en découle. Si les utilisateurs possèdent déjà un compte chez un fournisseur d'identité compétent, laissez-le vérifier et acceptez sa réponse signée : un mot de passe que l'application ne stocke jamais ne peut jamais être divulgué par elle. Si elle doit conserver des mots de passe, suivez littéralement 800-63B plutôt que de mémoire et placez une méthode résistant à l'hameçonnage devant toute fonction administrative.

À quoi cela ressemble en pratique

Lorsque l'entreprise a transféré son code source sur son serveur git, l'authentification était la première responsabilité d'exploitation d'une forge. Celle choisie privilégie SSH et ne possède aucune interface Web d'administration : l'entrée est donc une clé. Une session anonyme est refusée, comme une session sans clé, et chaque dépôt déclaré est en plus marqué privé. Le point d'écoute vérifiant ces clés, sur le port 23231, n'accepte que l'interface de bouclage. Toute connexion extérieure passe donc d'abord par un bastion, sans agrandir la surface déclarée du pare-feu.

Le même problème prend une autre forme à l'échelle d'une organisation. Dans un rôle antérieur d'ingénieure infrastructure, le travail consistait à consolider identités et accès entre M365, 1Password, Red Hat SSO et OKTA SSO, où des personnes différentes avaient accordé des permissions ponctuelles au fil du temps. Le moindre privilège a été imposé, et les arrivées et départs standardisés pour révoquer rapidement les accès plutôt que les laisser persister. Le risque d'accès non autorisé a fortement baissé et les accès sont devenus auditables : l'équipe pouvait enfin répondre à « qui peut atteindre ceci, et pourquoi ? ».

L'authentification a aussi un visage, jugé par ses messages d'erreur. Sur la connexion d'une application à un grand fournisseur de messagerie, le message disait que le mot de passe était incorrect. Il était correct ; le fournisseur exige un mot de passe propre à l'application pour les clients tiers et refuse celui du compte, aussi soigneuse soit sa saisie. Le message a été réécrit pour nommer le fournisseur, préciser cette exigence et indiquer où créer ce mot de passe. Un test provoque désormais ce refus et exige la présence du nom du fournisseur et du type d'identifiant requis, empêchant le retour discret de l'ancien texte.

Où les problèmes surviennent

- **Le message accuse l'utilisateur pour une cause située ailleurs.** Compte verrouillé, mot de passe expiré, horloge décalée du générateur de codes et fournisseur demandant un autre identifiant deviennent tous « mot de passe incorrect ». La personne ressaisit quelque chose qui ne fonctionnera jamais. Nommez la cause sur laquelle elle peut agir, en gardant une réponse identique pour un compte existant ou absent afin de ne pas fournir une liste de noms valides.
- **Une page d'hameçonnage relaie le code en temps réel.** La personne saisit mot de passe et code à six chiffres sur une copie, qui transmet les deux au site réel dans le pas de temps de 30 secondes que la RFC 6238 recommande en l'absence d'autre réglage. Les codes à usage unique bloquent l'utilisation de mots de passe volés et réutilisés ; ils protègent peu contre un relais en temps réel. Les clés liées à l'origine, comme les passkeys, ne signent que pour un site : c'est pourquoi le NIST les classe comme résistantes à l'hameçonnage, contrairement aux codes saisis.
- **Les identifiants survivent à leurs détenteurs.** Le départ ferme le compte d'annuaire, tandis qu'une clé SSH dans `authorized_keys`, un jeton d'accès personnel et un mot de passe administrateur partagé continuent à fonctionner. Chaque identifiant nécessite un responsable, un lieu de consignation et une date de réexamen.
- **La session reste valide longtemps après la connexion.** Un cookie ou jeton de plusieurs mois est un mot de passe à longue mèche. La déconnexion doit terminer la session sur le serveur, pas seulement supprimer le cookie d'un navigateur. Un jeton autonome jamais revérifié par le serveur reste utilisable jusqu'à expiration, quoi qu'il arrive au compte.
- **La récupération de compte est l'entrée la plus faible.** Une connexion forte accompagnée d'un lien de réinitialisation par courriel fait de la boîte de messagerie le véritable identifiant. La récupération mérite le même examen que l'entrée principale, car l'attaquant choisira la plus faible.

Pour aller plus loin

- NIST SP 800-63B-4 — texte actuel : niveaux d'assurance, minimum de 15 caractères et critères de résistance à l'hameçonnage.
- NIST SP 800-63B, révision 3 — guide de 2017 conservé en ligne, indiqué comme remplacé par la révision 4 depuis le 1er août 2025.
- RFC 9110, section 11 : HTTP Authentication — défi et réponse derrière 401, WWW-Authenticate et l'en-tête Authorization.
- RFC 4252 : The SSH Authentication Protocol — connexions par clé publique, mot de passe et hôte selon SSH.
- RFC 6238 : TOTP — dérivation de codes courts depuis un secret partagé et l'horloge.
- Web Authentication, Level 3 — API W3C derrière les passkeys et identifiants à clé publique limités à l'origine.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que l'authentification ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/authentication/