Engineer

Authentification multifacteur

Connexion exigeant au moins deux types de preuves distincts

Ce que c’est

L’authentification multifacteur, généralement abrégée MFA, n’accepte une identité revendiquée à la connexion que si plusieurs types de preuves l’étayent. NIST SP 800-63B-4, le guide fédéral américain sur l’authentification que suivent aussi de nombreuses organisations hors administration, en distingue trois : ce que vous savez, comme un mot de passe ; ce que vous possédez, comme un téléphone ou une clé de sécurité ; et ce que vous êtes, comme une empreinte digitale. Sa définition tient à un mot : le système doit exiger plusieurs types de facteurs distincts. Un mot de passe et la réponse à une question de sécurité ne forment donc qu’un facteur, car ce sont deux choses que vous savez. L’authentification à deux facteurs, ou 2FA, est le cas courant avec exactement deux facteurs.

Le guide accepte deux façons d’y parvenir. La première combine des authentificateurs distincts à facteur unique : un mot de passe, auquel on ajoute soit une application de téléphone affichant des codes à usage unique, soit une liste de codes de secours imprimés. La seconde utilise un authentificateur multifacteur unique, comme une clé de sécurité ou un téléphone : l’appareil détient une clé privée et ne l’utilise qu’après la saisie d’un code PIN ou la vérification d’une empreinte digitale. Le code PIN ou l’empreinte est alors un facteur d’activation. Il est vérifié sur l’appareil lui-même ; le serveur ne reçoit que le résultat, une signature vérifiable : un seul geste présente ainsi deux facteurs.

La biométrie y a une place limitée. Le NIST n’autorise une empreinte ou un visage que si un authentificateur physique participe aussi à l’authentification, jamais comme facteur isolé, et exige qu’une alternative non biométrique soit toujours proposée. Le guide précise que les caractéristiques biométriques ne sont pas secrètes : un visage se photographie, une empreinte se relève sur un objet touché par son propriétaire.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que l'authentification multifacteur ? » 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

Un mot de passe peut être copié à l'insu de son propriétaire : saisi sur une copie convaincante d'une page de connexion, deviné ou réutilisé sur un site dont la base est ensuite volée. La MFA rend ce mot de passe copié insuffisant à lui seul, car l'attaquant a encore besoin d'un élément d'une autre nature.

Le NIST en fait la base de son deuxième niveau d'assurance. À AAL2, l'utilisateur doit s'authentifier par deux facteurs, combinés dans un authentificateur ou fournis séparément ; cette combinaison doit inclure un authentificateur physique avec un mot de passe ou une comparaison biométrique. Les vérificateurs de ce niveau doivent proposer au moins une option résistante à l'hameçonnage, et les agences fédérales doivent imposer une authentification résistante à l'hameçonnage à leur personnel, leurs prestataires et leurs partenaires.

Les méthodes vendues sous ces trois lettres diffèrent davantage entre elles que la MFA d'un simple mot de passe ; le guide les classe clairement :

- **Les codes envoyés par SMS ou appel vocal** sont le seul type d'authentificateur que le NIST classe comme restreint. Ils restent utilisables, mais le vérificateur doit proposer une alternative sans cette qualification, informer l'utilisateur du risque et prévoir leur abandon. Changer le numéro de téléphone enregistré revient à associer un nouvel authentificateur, avec tous les contrôles que cela implique.
- **Les codes d'une application et les demandes de validation sur téléphone** sont acceptables à AAL2, mais ne résistent pas à l'hameçonnage : ce que la personne saisit ou approuve n'est pas lié au site demandeur.
- **Les authentificateurs cryptographiques liant leur réponse au site**, comme les clés d'accès et cartes à puce, résistent à l'hameçonnage. AAL3 en exige un dont la clé privée ne peut être exportée de son matériel.

Le courriel est volontairement absent de cette liste : le guide l'exclut comme canal d'authentification hors bande.

À quoi cela ressemble en pratique

Le code d'une application d'authentification est le second facteur le plus courant ; la RFC 6238, de mai 2011, le définit en quelques pages. À l'enregistrement, le serveur génère une clé secrète et la transmet à l'application, généralement par code QR : les deux côtés possèdent alors la même clé. Pour produire un code, chacun divise le temps Unix courant par un pas de temps, de 30 secondes par défaut, et prend le quotient entier comme compteur. Il calcule un HMAC de ce compteur avec la clé et ramène le résultat à un nombre de quelques chiffres en base dix, selon la méthode HOTP définie par la RFC 4226 en 2005, qui exige au moins six chiffres. En Python, tout le calcul tient en quelques lignes :

```
import hashlib, hmac, struct

def totp(key: bytes, unix_time: int, digits: int = 6, step: int = 30) -> str:
    counter = struct.pack(">Q", unix_time // step)
    mac = hmac.new(key, counter, hashlib.sha1).digest()
    offset = mac[-1] & 0x0F
    code = struct.unpack(">I", mac[offset:offset + 4])[0] & 0x7FFFFFFF
    return str(code % 10**digits).zfill(digits)

print(totp(b"12345678901234567890", 59, digits=8))  # 94287082
```

Les vecteurs de test de la RFC utilisent cette clé ASCII de 20 octets et huit chiffres. 59 secondes après l'époque de référence, le compteur vaut 1 et la variante SHA-1 donne 94287082, résultat affiché par la fonction ; le code à six chiffres d'une application serait constitué des six derniers, 287082. Aucun accès réseau n'intervient dans le calcul : l'application fonctionne donc en mode avion et le serveur doit conserver sa propre copie de la clé de chaque utilisateur.

Vérifier un code consiste à refaire ce calcul sur le serveur puis à comparer. La RFC 6238 recommande d'accepter au plus un pas de temps antérieur pour couvrir le délai réseau, et interdit d'accepter une seconde fois un code déjà utilisé avec succès.

Une clé d'accès remplace le secret partagé par une paire de clés. Selon Web Authentication Level 3, recommandation du W3C depuis le 25 août 2026, l'authentificateur crée une paire pour un seul site, identifié par son domaine, et ne donne au serveur que la clé publique. À la connexion, le navigateur transmet l'origine à laquelle il est réellement connecté et l'authentificateur signe le défi du serveur avec cette origine : une signature produite sur un domaine ressemblant au vrai est donc inutilisable sur le vrai domaine. Avec un code PIN ou une empreinte exigés pour utiliser la clé, une clé d'accès constitue un authentificateur multifacteur en une étape. WebAuthn appelle identifiants multiappareils les clés d'accès copiées entre les appareils d'une personne ; le NIST accepte ces clés synchronisées à AAL2, mais pas à AAL3, car une clé synchronisable est par définition exportable.

Activer la MFA est la partie facile. Décider qui doit l'utiliser, quelles méthodes comptent selon le contexte et que faire quand quelqu'un perd son téléphone relève de l'administration des comptes, au sein de l'organisation plus large des accès. Le service de gestion de la sécurité et des accès de ce site décrit cette organisation : comptes, mots de passe et permissions configurés pour donner à chaque personne exactement les accès nécessaires à son travail et les retirer le jour de son départ.

Où les problèmes surviennent

Une page d'hameçonnage relaie le code. Un code à usage unique est un nombre lu puis saisi par l'utilisateur ; rien n'y indique le site qu'il regardait. Une page ressemblante qui transmet mot de passe et code au vrai site pendant le pas de temps se connecte en son nom. Le NIST précise donc qu'aucun authentificateur dont la sortie est saisie à la main ne compte comme résistant à l'hameçonnage, et que la façon d'arriver sur la fausse page ne change rien. La solution lie la réponse au vérificateur : par son domaine, comme WebAuthn, ou au canal TLS lui-même, comme les certificats clients et cartes à puce. Exigez l'une de ces méthodes pour les administrateurs et proposez-la à tous les autres.

Le numéro de téléphone fait office de facteur. Un code SMS arrive chez la personne vers laquelle l'opérateur mobile achemine ce numéro à cet instant. Le NIST cite parmi les menaces l'attaquant qui a convaincu l'opérateur de rediriger le numéro de la victime et reçoit ensuite le code. Avant un envoi par SMS ou appel vocal, les vérificateurs devraient rechercher des signes comme un changement récent de SIM, un portage de numéro ou un changement d'appareil. Gardez les SMS comme solution de repli plutôt que méthode principale, et exigez une connexion complète avant de modifier le numéro enregistré.

Approuver, approuver, approuver. Une demande de validation avec un simple bouton « Approuver » demande une décision, pas une preuve. Un attaquant possédant déjà le mot de passe peut provoquer des demandes jusqu'à ce que l'utilisateur, lassé, en accepte une. Le NIST appelle cela la fatigue d'authentification et n'accepte plus les parcours fondés sur la seule approbation : un secret doit passer d'un canal à l'autre, par exemple un nombre affiché sur l'écran de connexion à saisir sur le téléphone. Le choisir dans une courte liste ne suffit pas, car l'utilisateur peut simplement deviner. Limitez aussi le nombre de demandes envoyées depuis la dernière connexion réussie, comme le recommande le guide.

La récupération saute le second facteur. Un lien « téléphone perdu » qui ne demande que le mot de passe ou envoie un lien de réinitialisation par courriel transforme la MFA en option que l'attaquant peut refuser. Pour les comptes AAL2, le NIST exige l'une de ces méthodes de récupération : deux codes de récupération obtenus par des méthodes différentes, un code et un authentificateur à facteur unique encore associé au compte, ou une nouvelle vérification de l'identité. Chaque récupération doit entraîner l'envoi d'une notification à l'utilisateur. Plus largement, un facteur ne doit jamais permettre d'obtenir un authentificateur d'une autre nature : le mot de passe seul ne doit pas suffire à imprimer de nouveaux codes de secours.

Le code est accepté deux fois ou trop longtemps. Un code de six chiffres a un million de valeurs possibles : sa force vient des règles qui l'entourent. Un vérificateur acceptant plusieurs pas de temps de part et d'autre de l'instant courant, ou un code déjà utilisé, offre à l'attaquant ayant vu un code une fenêtre pour le réutiliser. Conservez le dernier pas de temps accepté par utilisateur et rejetez tout pas antérieur ou égal ; limitez la fenêtre à l'unique pas que la RFC 6238 autorise pour le délai, et plafonnez les échecs consécutifs : le NIST n'en permet pas plus de 100 avant désactivation de l'authentificateur.

Les secrets initiaux côtoient les mots de passe. Les codes d'application sont symétriques : le serveur détient la clé de chaque utilisateur et quiconque copie ces clés peut produire des codes valides pour tous les comptes. Le NIST exige une protection forte des clés et un accès limité aux composants logiciels qui en ont besoin. Ne les conservez pas dans des colonnes en clair à côté des empreintes de mots de passe. Chiffrez-les avec une clé conservée dans un stockage de secrets distinct et ne laissez les lire que par le service qui vérifie les codes.

Pour aller plus loin

- NIST SP 800-63B-4 : définitions et acronymes — définitions de l'authentification multifacteur, de l'authentificateur multifacteur et de la résistance à l'hameçonnage dans le guide actuel.
- NIST SP 800-63B-4 au Computer Security Resource Center — notice de publication : juillet 2025, remplace SP 800-63B.
- RFC 6238 : TOTP — algorithme des mots de passe à usage unique fondés sur le temps, vecteurs de test et règles de dérive d'horloge.
- RFC 4226 : HOTP — algorithme à compteur sous-jacent, dont la troncature à six chiffres ou plus.
- Web Authentication, Level 3 — spécification du W3C derrière les clés d'accès, avec identifiants liés à l'origine et clés d'accès synchronisées.

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 multifacteur ? » 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/multi-factor-authentication/