Engineer

ACME

le protocole d'émission automatique de certificats

Ce que c’est

ACME, Automatic Certificate Management Environment, est le protocole par lequel un programme demande un certificat à une autorité de certification, prouve qu’il contrôle les noms demandés et revient en obtenir un nouveau avant l’expiration du précédent. Personne ne remplit de formulaire ni ne répond à un courriel de confirmation. La RFC 8555 l’a normalisé en mars 2019, et Let’s Encrypt est l’autorité par laquelle la plupart des personnes le découvrent.

Le client commence avec sa propre clé de compte, distincte de celle de tout certificat, et signe chaque requête avec elle. L’obtention d’un certificat passe ensuite par cinq ressources du serveur :

```
newAccount   register the account key once
newOrder     list the names the certificate should cover
authz        one authorization per name, each offering challenges
finalize     send a certificate signing request once all are valid
certificate  download the issued chain, then install it
```

Un défi permet au client de montrer qu’il contrôle un nom. Le serveur fournit un jeton ; le client l’associe à une empreinte de la clé de compte, qui lie la preuve à ce seul compte, puis publie le résultat là où seule une personne contrôlant le nom pourrait le placer. Trois types de défis comptent :

- **http-01** sert la valeur dans un fichier à `/.well-known/acme-challenge/<token>` sur le nom de domaine lui-même. La première requête de l’autorité passe toujours par HTTP non chiffré sur le port 80.
- **dns-01** place un hachage de la valeur dans un enregistrement TXT à `_acme-challenge` sous ce nom de domaine. C’est le seul des trois capable de prouver le contrôle d’un nom générique comme `*.example.com` .

- **tls-alpn-01**, ajouté par la RFC 8737 en février 2020, répond sur le port 443 pendant une négociation TLS utilisant un protocole ALPN dédié. Il convient à un mandataire inverse qui contrôle le port 443 sans pouvoir utiliser le port 80.

La RFC 9773, publiée en juin 2025, a ajouté ACME Renewal Information, ou ARI. L'autorité publie une fenêtre suggérée de renouvellement pour chaque certificat délivré, et le client demande cette fenêtre plutôt que de la deviner. L'autorité peut ainsi avancer les renouvellements, avant une révocation massive par exemple, sans modification d'un fichier de configuration.

Utilisez le concept pour prendre une décision

Utilisez « Que signifie ACME ? » 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

La possibilité de continuer à renouveler manuellement les certificats n'est plus une question de préférence. Elle est désormais assortie de dates.

Le CA/Browser Forum fixe les règles suivies par toutes les autorités reconnues publiquement. Son vote SC-081v3, adopté en avril 2025, plafonne à 200 jours les certificats délivrés depuis le 15 mars 2026. Le plafond passe à 100 jours le 15 mars 2027, puis à 47 jours le 15 mars 2029. La période de réutilisation d'une preuve de contrôle de domaine diminue en parallèle : 200 jours aujourd'hui, puis 100, puis seulement 10. Avec les règles finales, un nom renouvelé aux deux tiers de sa durée de validité nécessite un certificat neuf environ chaque mois, et presque chaque renouvellement un nouveau défi.

Let's Encrypt devance ce calendrier. Ses certificats standard durent actuellement 90 jours. À partir du 10 février 2027, ils dureront 64 jours, avec des autorisations réutilisables pendant 10 jours, puis 45 jours à partir du 16 février 2028, avec une réutilisation limitée à 7 heures. Son annonce déconseille le renouvellement manuel. L'autorité a aussi cessé les courriels de rappel d'expiration le 4 juin 2025 : même le filet de sécurité qui rattrapait un renouvellement oublié a disparu.

Le renouvellement manuel étant exclu, ACME devient le choix de base. Il reste à décider où placer ses composants :

- **Le défi.** http-01 est le point de départ simple pour un serveur unique répondant sur le port 80. dns-01 justifie sa configuration supplémentaire pour les noms génériques, plusieurs serveurs derrière un nom et les hôtes inaccessibles depuis Internet. tls-alpn-01 convient aux mandataires qui disposent du port 443, mais pas du 80.
- **Le client.** Il peut résider dans le serveur Web, fonctionner à côté avec un hook installant chaque nouveau certificat, ou sur une machine distincte qui valide centralement puis copie les certificats.
- **La supervision.** Un élément extérieur au client doit remarquer l'absence de renouvellement, car le client est justement ce qui vient d'échouer.

À quoi cela ressemble en pratique

Dans le cadre de la mission d'ingénierie DevOps, l'entreprise a retiré la gestion des certificats des mains humaines pour cent applications Docker sur des hôtes Ubuntu Linux, où Apache et Nginx servaient tous deux du trafic. ACME assurait chaque étape : délivrance, renouvellement avant expiration et déploiement de chaque certificat. Aucune étape n'attendait que quelqu'un se rappelle une date. Les cent applications ont conservé des certificats valides et le travail manuel a disparu.

Le déploiement est l'étape facilement sous-estimée. Apache et Nginx lisent un certificat au démarrage ou au rechargement et continuent à servir cette copie. Un client qui écrit seulement un nouveau fichier n'a donc rien renouvelé de visible pour le visiteur. Lorsqu'Apache et Nginx partagent un parc, chacun nécessite son propre rechargement à l'arrivée d'un nouveau certificat.

Le site de l'entreprise illustre l'autre organisation, où le client est le serveur Web. Ici, Caddy renouvelle lui-même le certificat du site auprès de Let's Encrypt. Caddy utilise ACME nativement, sans outil distinct : aucune étape de déploiement ne peut donc être oubliée.

Où les problèmes surviennent

Le défi expire ou renvoie 404, alors que le site se charge dans un navigateur. La requête http-01 arrive sur le port 80 et rencontre un problème : pare-feu ou groupe de sécurité cloud n'ouvrant que 443, redirection vers un port autre que

80 ou 443, répartiteur envoyant la requête vers un serveur n'ayant jamais reçu le jeton. Let's Encrypt suit jusqu'à dix redirections, uniquement vers ces deux ports. Gardez le port 80 ouvert, servez le chemin du défi depuis chaque serveur applicatif ou un stockage partagé, et passez à dns-01 si le port 80 est indisponible.

La clé d'API DNS du serveur Web peut réécrire toute la zone. Un nom générique nécessite dns-01, donc un moyen de créer des enregistrements TXT. L'identifiant le plus facile à obtenir permet souvent de modifier tous les enregistrements du compte. Si le serveur Web est compromis, l'attaquant peut aussi rediriger la messagerie et tous les autres noms. Utilisez des droits limités aux enregistrements `_acme-challenge` si le fournisseur le permet, faites pointer `_acme-challenge` par CNAME vers une zone réservée aux défis, ou validez depuis une autre machine puis copiez les certificats. La propagation DNS prend du temps : le client peut devoir attendre jusqu'à une heure avant d'annoncer à l'autorité que le défi est prêt.

Après un redéploiement, les nouveaux conteneurs démarrent sans certificat. Chaque conteneur demande son certificat au démarrage et ne le conserve que dans son propre système de fichiers ; chaque redémarrage recommence donc la demande. Redéployez assez souvent ou démarrez-en beaucoup à la fois, et les limites de débit de l'autorité refusent les commandes supplémentaires. La RFC 8555 nomme cette erreur `rateLimited`. Let's Encrypt avertit que, dans le pire cas, aucune instance n'obtient de certificat. Conservez certificats et clés dans un stockage durable, et faites utiliser à toute nouvelle instance un certificat valide de ce stockage avant d'en commander un.

Une périodicité fixe de renouvellement laisse les certificats expirer lorsque leur durée diminue. La tâche renouvelle par exemple tous les 60 jours, rythme adapté aux certificats de 90 jours. Un certificat de 64 jours ne laisse que quatre jours de marge, et un de 45 jours expire environ deux semaines avant le déclenchement. La RFC 9773 cite les intervalles fixes parmi les habitudes empêchant les autorités de modifier les durées. Activez ARI si le client le prend en charge. Let's Encrypt conseille de le consulter au moins deux fois par jour et, comme secours, de renouveler lorsqu'il reste un tiers de la durée de validité.

Le client annonce un succès, mais les visiteurs voient encore l'ancien certificat. Le nouveau fichier est sur disque, mais rien n'a demandé le rechargement du serveur, ou le hook n'en a rechargé qu'un parmi plusieurs.

L’ancien certificat reste servi jusqu’à expiration. Rechargez le serveur depuis le hook de déploiement du client, et surveillez le certificat réellement servi, vérifié de l’extérieur, plutôt que le fichier :

```
openssl s_client -connect example.com:443 -servername example.com \
    </dev/null 2>/dev/null | openssl x509 -noout -enddate
```

Pour aller plus loin

- RFC 8555 : Automatic Certificate Management Environment (ACME) — comptes, commandes, autorisations et défis http-01 et dns-01.
- RFC 9773 : ACME Renewal Information (ARI) Extension — la fenêtre de renouvellement suggérée par une autorité pour chaque certificat.
- RFC 8737 : ACME TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension — le défi tls-alpn-01, entièrement traité sur le port 443.
- Types de défis — comparaison des trois défis par Let’s Encrypt, avec les limites de chacun.
- Réduction de la durée des certificats à 45 jours — calendrier des certificats plus courts de Let’s Encrypt et conseils de renouvellement.
- Vote SC-081v3 — le vote du CA/Browser Forum fixant les plafonds de 200, 100 et 47 jours.

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 « Que signifie ACME ? » 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/acme/