**Engineer**

# ACME

das Protokoll, das Zertifikate automatisch ausstellt

## Was es ist

ACME, die Automatic Certificate Management Environment, ist das Protokoll, mit dem ein Programm bei einer Zertifizierungsstelle ein Zertifikat anfordert, die Kontrolle über die beantragten Namen nachweist und vor Ablauf des alten ein neues beschafft. Dabei füllt niemand ein Formular aus oder beantwortet eine Bestätigungsmail. RFC 8555 standardisierte es im März 2019. Die meisten Menschen begegnen ihm über die Zertifizierungsstelle Let's Encrypt.

Der Client beginnt mit einem eigenen Kontoschlüssel, getrennt vom Schlüssel jedes Zertifikats, und signiert damit jede Anfrage. Der Weg zum Zertifikat führt dann über fünf Ressourcen auf dem Server:

```
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
```

Mit einer Challenge weist der Client nach, dass er einen Namen kontrolliert. Der Server liefert einen Token. Der Client verbindet ihn mit einem Fingerabdruck des Kontoschlüssels, wodurch der Nachweis an dieses eine Konto gebunden wird, und veröffentlicht das Ergebnis dort, wo nur jemand mit Kontrolle über den Namen es ablegen könnte. Drei Challenge-Typen sind wichtig:

- **http-01** stellt den Wert unter dem Namen selbst als Datei an `/.well-known/acme-challenge/<token>` bereit. Die erste Anfrage der Zertifizierungsstelle erfolgt immer über unverschlüsseltes HTTP an Port 80.

- **dns-01** setzt einen Hash des Werts in einen TXT-Eintrag unter `_acme-challenge` des Namens. Nur dieser der drei Typen kann die Kontrolle über einen Wildcard-Namen wie `*.example.com` nachweisen.
- **tls-alpn-01**, im Februar 2020 durch RFC 8737 ergänzt, antwortet an Port 443 während eines TLS-Handshakes mit einem eigens vorgesehenen ALPN-Protokoll. Das passt zu einem Reverse Proxy, der Port 443 besitzt und Port 80 nicht nutzen kann.

Der im Juni 2025 veröffentlichte RFC 9773 ergänzte ACME Renewal Information, kurz ARI. Die Zertifizierungsstelle veröffentlicht für jedes ausgestellte Zertifikat ein empfohlenes Erneuerungsfenster. Der Client fragt dieses Fenster ab, statt es zu erraten. So kann die Stelle Erneuerungen etwa vor einem Massenwiderruf vorziehen, ohne dass jemand eine Konfigurationsdatei bearbeitet.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ACME?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

**Unsere Leistungen entdecken** Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

**1.000 RBAC-Regeln für sichere Linux-Server** Kontakt aufnehmen →

## Warum es wichtig ist

Ob Zertifikate noch von Hand erneuert werden können, ist keine Geschmacksfrage mehr. Es gibt inzwischen feste Termine dafür.

Das CA/Browser Forum legt die Regeln fest, denen alle öffentlich vertrauenswürdigen Zertifizierungsstellen folgen. Sein im April 2025 angenommener Beschluss SC-081v3 begrenzt die Laufzeit seit dem 15. März 2026 ausgestellter Zertifikate auf 200 Tage. Ab dem 15. März 2027 sinkt die Grenze auf 100 Tage, ab dem 15. März 2029 auf 47 Tage. Die Wiederverwendbarkeit eines Nachweises der Domainkontrolle sinkt parallel: von derzeit 200 Tagen auf 100 und schließlich nur noch 10. Unter den endgültigen Regeln braucht ein Name, dessen Zertifikat nach zwei Dritteln seiner Laufzeit erneuert wird, ungefähr jeden Monat ein neues Zertifikat. Fast jede dieser Erneuerungen benötigt eine neue Challenge.

Let’s Encrypt liegt vor diesem Zeitplan. Seine Standardzertifikate gelten heute 90 Tage. Ab dem 10. Februar 2027 gelten sie 64 Tage, mit 10 Tagen Wiederverwendbarkeit der Autorisierung. Ab dem 16. Februar 2028 gelten sie 45 Tage, und die Wiederverwendung wird auf 7 Stunden verkürzt. Die eigene Ankündigung rät von manueller Erneuerung ab. Seit dem 4. Juni 2025 versendet Let’s Encrypt außerdem keine Ablauf-Erinnerungsmails mehr. Damit entfällt auch das Sicherheitsnetz, das eine vergessene Erneuerung noch auffangen konnte.

Manuelle Erneuerung scheidet damit aus, ACME ist der Normalfall. Zu entscheiden bleibt, wo seine beweglichen Teile liegen:

- **Die Challenge.** http-01 ist der einfache Einstieg für einen einzelnen Server an Port 80. dns-01 rechtfertigt den zusätzlichen Einrichtungsaufwand für Wildcards, mehrere Server hinter einem Namen und Hosts, die aus dem Internet nicht erreichbar sind. tls-alpn-01 passt zu Proxys mit Port 443, aber ohne Port 80.
- **Der Client.** Er kann im Webserver stecken, daneben mit einem Hook zur Installation neuer Zertifikate laufen oder auf einem getrennten Rechner zentral validieren und Zertifikate verteilen.
- **Die Überwachung.** Etwas außerhalb des Clients muss bemerken, wenn eine Erneuerung ausgeblieben ist. Denn gerade der Client ist dann der ausgefallene Teil.

## Wie es in der Praxis aussieht

In der Rolle als DevOps Engineer wurde die Zertifikatsarbeit für hundert Docker-Anwendungen auf Ubuntu-Linux-Hosts automatisiert, auf denen sowohl Apache als auch Nginx Anfragen bedienten. ACME übernahm jeden Schritt: Ausstellung, Erneuerung vor Ablauf und Bereitstellung jedes Zertifikats. Kein Schritt wartete darauf, dass sich jemand an ein Datum erinnerte. Alle hundert Anwendungen behielten gültige Zertifikate, und die Handarbeit entfiel.

Die Bereitstellung wird leicht unterschätzt. Apache und Nginx lesen ein Zertifikat beim Start oder Neuladen und liefern anschließend diese Kopie weiter aus. Ein Client, der nur eine neue Datei schreibt, hat daher nichts erneuert, was ein Besucher sehen kann. Nutzen Apache und Nginx denselben Serverbestand, braucht jeder von ihnen nach dem Eintreffen eines neuen Zertifikats einen eigenen Reload.

Die eigene Website zeigt die andere Anordnung, bei der der Client der Webserver ist. Hier erneuert Caddy das Zertifikat selbst bei Let's Encrypt. Caddy beherrscht ACME direkt und benötigt kein getrenntes Werkzeug. Deshalb gibt es keinen Bereitstellungsschritt, der vergessen werden könnte.

## Wo es schiefgeht

**Die Challenge läuft in ein Zeitlimit oder liefert 404, obwohl die Website im Browser lädt.** Die http-01-Anfrage kommt an Port 80 an, und auf ihrem Weg stimmt etwas nicht: eine Firewall oder Cloud-Sicherheitsgruppe öffnet nur 443, eine Weiterleitung führt zu einem anderen Port als 80 oder 443, oder ein Load Balancer schickt die Anfrage an einen Server, der den Token nie erhalten hat. Let's Encrypt folgt höchstens zehn Weiterleitungen und nur zu diesen beiden Ports. Halten Sie Port 80 offen, stellen Sie den Challenge-Pfad auf jedem Backend oder aus gemeinsamem Speicher bereit und wechseln Sie zu dns-01, wenn Port 80 nicht verfügbar ist.

**Der DNS-API-Schlüssel auf dem Webserver kann die gesamte Zone umschreiben.** Eine Wildcard braucht dns-01, also benötigt der Client eine Möglichkeit, TXT-Einträge anzulegen. Die am einfachsten erhältlichen Zugangsdaten dürfen häufig sämtliche Einträge des Kontos ändern. Nach einem Einbruch in den Webserver könnte ein Angreifer damit auch E-Mail und jeden anderen Namen umleiten. Verwenden Sie Zugangsdaten, die auf `_acme-challenge` -Einträge beschränkt sind, sofern der Anbieter das unterstützt. Alternativ verweist `_acme-challenge` per CNAME auf eine eigene Challenge-Zone, oder die Validierung läuft auf einem getrennten Rechner, der die Zertifikate kopiert. DNS-Änderungen verbreiten sich nicht sofort. Der Client muss deshalb unter Umständen bis zu einer Stunde warten, bevor er die Challenge als bereit meldet.

**Nach einer erneuten Bereitstellung starten neue Container ohne Zertifikate.** Jeder Container fordert beim Start ein eigenes Zertifikat an und speichert es nur im eigenen Dateisystem. Jeder Neustart fragt deshalb erneut an. Bei häufigen Bereitstellungen oder vielen gleichzeitigen Starts verweigern die Ratenlimits der Zertifizierungsstelle weitere Aufträge. RFC 8555 gibt dem Fehler einen eigenen Namen: `rateLimited` . Let's Encrypt warnt, dass im schlimmsten Fall keine Instanz ein Zertifikat bekommt. Halten Sie Zertifikate und Schlüssel in dauerhaftem Speicher. Eine neue Instanz sollte zuerst ein dort vorhandenes gültiges Zertifikat verwenden, bevor sie eines bestellt.

**Ein fester Erneuerungstakt lässt kürzere Zertifikate ablaufen.** Der Auftrag erneuert etwa alle 60 Tage, passend zu 90-Tage-Zertifikaten. Bei 64 Tagen bleiben vier Tage Reserve; ein 45-Tage-Zertifikat läuft ungefähr zwei Wochen vor dem nächsten Aufruf ab. RFC 9773 nennt feste Intervalle als eine der Gewohnheiten, die Zertifizierungsstellen an Laufzeitänderungen hindern. Aktivieren Sie ARI, wenn der Client es unterstützt. Let's Encrypt empfiehlt, es mindestens zweimal täglich abzufragen und als Rückfallregel zu erneuern, wenn noch ein Drittel der Laufzeit verbleibt.

**Der Client meldet Erfolg, Besucher sehen weiterhin das alte Zertifikat.** Die neue Datei liegt auf der Platte, aber niemand hat den Webserver zum Neuladen aufgefordert, oder der Hook hat nur einen von mehreren Servern neu geladen. Das alte Zertifikat bleibt bis zum Ablauf im Einsatz. Laden Sie den Server über den Deploy-Hook des Clients neu und überwachen Sie von außen das tatsächlich ausgelieferte Zertifikat statt die Datei:

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

## Weiterführende Lektüre

- RFC 8555: Automatic Certificate Management Environment (ACME) — Konten, Aufträge, Autorisierungen sowie http-01- und dns-01-Challenges.
- RFC 9773: ACME Renewal Information (ARI) Extension — das von der Zertifizierungsstelle vorgeschlagene Erneuerungsfenster pro Zertifikat.
- RFC 8737: ACME TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension — die vollständig über Port 443 beantwortete tls-alpn-01-Challenge.
- Challenge-Typen — Let's Encrypts eigener Vergleich der drei Verfahren mit ihren jeweiligen Grenzen.
- Verkürzung der Zertifikatslaufzeit auf 45 Tage — Let's Encrypts Termine für kürzere Zertifikate und seine Empfehlungen zur Erneuerung.
- Beschluss SC-081v3 — die Abstimmung des CA/Browser Forums, die die Grenzen von 200, 100 und 47 Tagen festlegt.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

**Preise ansehen** Kontakt aufnehmen →

# Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist ACME?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

**Unsere Leistungen entdecken**

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

**Mit Sorgfalt und Liebe gestaltet von D.**

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

**Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.**

**Gedruckt von https://engineer.company/de/glossary/acme/**