**Engineer**

# ACME

protokollet som utfärdar ett certifikat utan en människa

## Vad det är

ACME, Automatic Certificate Management Environment, är det nätverksprotokoll som ett program använder för att be en certifikatutfärdare om ett certifikat, bevisa att det styr över namnen det bad om och komma tillbaka efter ett nytt innan det gamla går ut. Programmet sköter hela vägen, utan formulär att fylla i eller bekräftelsemejl att svara på. RFC 8555 gjorde protokollet till standard i mars 2019, och Let’s Encrypt är den utfärdare de flesta möter det genom.

Klienten börjar med en egen kontonyckel, skild från nyckeln i något certifikat, och signerar varje begäran med den. Vägen till ett certifikat går sedan genom fem resurser på servern:

```
newAccount   registrera kontonyckeln en gång
newOrder     ange namnen som certifikatet ska täcka
authz        en auktorisering per namn, var och en med utmaningar
finalize     skicka en certifikatbegäran (CSR) när alla är giltiga
certificate  hämta den utfärdade kedjan och installera den
```

En utmaning (challenge) är sättet klienten visar att den styr över ett namn. Servern lämnar ut en token. Klienten fogar ihop den med ett fingeravtryck av kontonyckeln, vilket knyter beviset till just det kontot, och publicerar resultatet där bara den som styr över namnet kan lägga det. Tre typer av utmaning är värda att känna till:

- **http-01** lägger värdet som en fil på `/.well-known/acme-challenge/<token>` under själva namnet. Utfärdarens första förfrågan går alltid över vanlig HTTP till port 80.

- **dns-01** lägger en hash av värdet i en TXT-post på `_acme-challenge` under namnet. Det är den enda av de tre som kan bevisa kontroll över ett jokertecken som `*.example.com` .
- **tls-alpn-01**, som RFC 8737 lade till i februari 2020, svarar på port 443 under en TLS-handskakning med ett särskilt ALPN-protokoll. Den passar en omvänd proxy som äger port 443 och inte kan använda port 80.

RFC 9773 från juni 2025 lade till ACME Renewal Information, ARI. Utfärdaren publicerar ett föreslaget tidsfönster för förnyelse av varje certifikat den har utfärdat, och klienten frågar efter fönstret i stället för att gissa. Då kan utfärdaren tidigarelägga förnyelser, t.ex. inför en massåterkallelse, utan att någon behöver redigera en konfigurationsfil.

Använd begreppet i ett beslut

Använd ”Vad är ACME?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Konton, lösenord och behörigheter ordnade så att alla har exakt den åtkomst deras arbete kräver, och de som slutar förlorar den samma dag.

**Se våra tjänster** Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Skrev 1 000 RBAC-regler som säkrar Linux-servrar — 1,000 åtkomstregler, skrivna för att täppa till en säkerhetslucka

**Skrev 1 000 RBAC-regler som säkrar Linux-servrar** Hör av er →

## Varför det spelar roll

Om en människa fortfarande kan förnya certifikat för hand är inte längre en smaksak. Frågan har fått datum.

CA/Browser Forum sätter reglerna som varje allmänt betrodd utfärdare följer. Forumets omröstning SC-081v3, antagen i april 2025, begränsar ett certifikat som utfärdats från och med den 15 mars 2026 till 200 dagar. Taket sjunker till 100 dagar från den 15 mars 2027 och till 47 dagar från den 15 mars 2029, och tiden som ett bevis på kontroll över en domän får återanvändas sjunker i samma takt, från 200 dagar nu till 100 och sedan till bara 10. Med de slutliga reglerna behöver ett namn som förnyas vid två tredjedelar av livslängden ett nytt certifikat ungefär en gång i månaden, och nästan varje sådan förnyelse kräver en ny utmaning.

Let’s Encrypt ligger före det schemat. Dess certifikat gäller i dag 90 dagar som standard. Från den 10 februari 2027 gäller de 64 dagar, med auktoriseringar som kan återanvändas i 10 dagar, och från den 16 februari 2028 gäller de 45 dagar,

med återanvändningen nedskuren till 7 timmar. Det egna tillkännagivandet avråder från manuell förnyelse. Den 4 juni 2025 slutade Let’s Encrypt dessutom att skicka påminnelser via e-post när ett certifikat närmar sig utgången, så även skyddsnätet som fångade en bortglömd förnyelse är borta.

Manuell förnyelse är alltså inget alternativ, och ACME är standardvalet. Det som återstår att bestämma är var de rörliga delarna ska bo:

- **Utmaningen.** http-01 är den enkla starten för en enskild server som svarar på port 80. dns-01 är värd sitt extra arbete för jokertecken, för flera servrar bakom ett namn och för en värddator som internet inte når. tls-alpn-01 hör hemma i proxyer som håller port 443 och saknar port 80.
- **Klienten.** Den kan bo inne i webbservern, köras bredvid den med ett skript som installerar varje nytt certifikat, eller köras på en separat maskin som validerar centralt och kopierar ut certifikaten.
- **Vakten.** Något utanför klienten måste märka när en förnyelse uteblir, eftersom det är klienten som just har fallerat.

## Så ser det ut i praktiken

Som DevOps-ingenjör tog företaget certifikatarbetet ur mänskliga händer för hundra Docker-applikationer på värdar med Ubuntu Linux, där både Apache och nginx tog emot trafik. ACME skötte varje steg: utfärdade varje certifikat, förnyade det före utgången och driftsatte det. Varje steg i kretsloppet gick utan att någon behövde komma ihåg ett datum. Alla hundra applikationer behöll giltiga certifikat, och det manuella arbetet försvann.

Driftsättningen är det steg som är lätt att underskatta. Apache och nginx läser in ett certifikat när de startar eller laddas om och fortsätter sedan att servera den kopian, så en klient som bara skriver en ny fil har inte förnyat något som en besökare kan se. Där Apache och nginx delar på en servermiljö behöver var och en laddas om för sig när ett nytt certifikat landar.

Företagets egen webbplats visar det andra upplägget, där klienten är webbservern. Där förnyar Caddy själv webbplatsens certifikat från Let’s Encrypt. Caddy talar ACME inbyggt och behöver inga separata verktyg, så det finns inget driftsättningssteg att glömma.

# Var det går fel

**Valideringen tar för lång tid eller ger 404, fast webbplatsen öppnas fint i en webbläsare.** Förfrågan för http-01 kommer in på port 80, och något på vägen är fel: en brandvägg eller en säkerhetsgrupp i molnet som bara öppnar 443, en omdirigering som leder till en annan port än 80 eller 443, eller en lastbalanserare som skickar förfrågan till en server som aldrig fick token. Let's Encrypt följer upp till tio omdirigeringar, och bara till de två portarna. Håll port 80 öppen, servera utmaningens sökväg från varje backend eller från delad lagring, och byt till dns-01 där port 80 inte kan användas.

**DNS-nyckeln på webbservern kan skriva om hela zonen.** Ett jokertecken kräver dns-01, så klienten behöver ett sätt att skapa TXT-poster, och den behörighet som är lättast att få är ofta en som kan ändra varje post kontot äger. Om någon bryter sig in på webbservern kan angriparen styra om e-post och alla andra namn också. Använd en nyckel som är begränsad till `_acme-challenge` -posterna där leverantören erbjuder det, peka `_acme-challenge` med en CNAME mot en zon som är avsatt för domänvalidering, eller validera från en separat maskin och kopiera över certifikaten. DNS-ändringar tar tid att sprida sig, så klienten kan behöva vänta upp till en timme innan den ber om domänvalidering.

**Nya containrar startar utan certifikat efter en omdriftsättning.** Varje container ber om sitt eget certifikat när den startar och sparar det bara i sitt eget filsystem, så varje omstart frågar på nytt. Driftsätt om tillräckligt ofta, eller starta många på en gång, så nekar utfärdarens hastighetsgränser de extra beställningarna. RFC 8555 ger felet ett eget namn, `rateLimited` , och Let's Encrypt varnar för att ingen av instanserna i värsta fall får något certifikat. Lägg certifikat och nycklar i beständig lagring, och låt en ny instans använda ett giltigt certifikat därifrån innan den beställer ett.

**En fast förnyelsetimer låter certifikaten gå ut när livslängden krymper.** Jobbet förnyar t.ex. var 60:e dag, en takt som var avpassad för certifikat på 90 dagar. Ett certifikat på 64 dagar lämnar den timern fyra dagars marginal, och ett på 45 dagar går ut ungefär två veckor innan timern slår till. RFC 9773 pekar ut fasta intervall som en av vanorna som hindrar utfärdare från att ändra livslängder. Slå på ARI där klienten stöder det. Let's Encrypt råder dig att kontrollera det minst två gånger om dagen och, som reserv, att förnya när en tredjedel av livslängden återstår.

**Klienten rapporterar framgång och besökarna ser fortfarande det gamla certifikatet.** Den nya filen ligger på disken, men ingenting sade åt webbservern att ladda om, eller så laddade skriptet om en server av flera. Det gamla certifikatet är kvar i drift tills det går ut. Ladda om servern från klientens driftsättningshook, och övervaka certifikatet som faktiskt serveras, kontrollerat utifrån, i stället för filen:

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

## Läs mer

- RFC 8555: Automatic Certificate Management Environment (ACME) — konton, beställningar, auktoriseringar och utmaningarna http-01 och dns-01.
- RFC 9773: ACME Renewal Information (ARI) Extension — tidsfönstret för förnyelse som en utfärdare föreslår för varje certifikat.
- RFC 8737: ACME TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension — utmaningen tls-alpn-01, som besvaras helt på port 443.
- Challenge Types — Let’s Encrypts egen jämförelse av de tre utmaningarna, med begränsningarna för var och en.
- Decreasing Certificate Lifetimes to 45 Days — Let’s Encrypts datum för kortare certifikat och dess råd om förnyelse.
- Ballot SC-081v3 — omröstningen i CA/Browser Forum som sätter gränserna 200, 100 och 47 dagar.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

**Se vad det kostar** Hör av er →

# Gör begreppen praktiska

Fråga hur ”Vad är ACME?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/acme/