Engineer

ACME

protokollen som utsteder et sertifikat uten et menneske

Hva det er

ACME, Automatic Certificate Management Environment, er protokollen et program bruker når det ber en sertifikatutsteder om et sertifikat, beviser at det kontrollerer navnene det ba om, og kommer tilbake etter et nytt før det gamle går ut. Alt skjer mellom to programmer, uten skjema og uten bekreftelses-e-post underveis. RFC 8555 standardiserte protokollen i mars 2019, og Let's Encrypt er utstederen de fleste møter den gjennom.

Klienten har en egen kontonøkkel, holdt atskilt fra nøkkelen i sertifikatene, og signerer hver forespørsel med den. Selve bestillingen går så gjennom fem ressurser på serveren:

```
newAccount   registrer kontonøkkelen én gang
newOrder     list opp navnene sertifikatet skal dekke
authz        én autorisasjon per navn, hver med sine utfordringer
finalize     send en sertifikatforespørsel når alle er gyldige
certificate  last ned den utstedte kjeden og installer den
```

En utfordring (challenge) er måten klienten viser at den kontrollerer et navn på. Serveren gir klienten et token. Klienten setter det sammen med et fingeravtrykk av kontonøkkelen, noe som binder beviset til akkurat den kontoen, og publiserer resultatet et sted bare den som kontrollerer navnet, kan legge det. Tre typer utfordringer betyr noe i praksis:

- **http-01** legger verdien ut som en fil på `/.well-known/acme-challenge/<token>` under selve navnet. Utstederens første forespørsel etter filen går alltid over ren HTTP til port 80.

- **dns-01** legger en hash av verdien i en TXT-post på `_acme-challenge` under navnet. Den er den eneste av de tre som kan bevise kontroll over et jokertegnnavn som `*.example.com` .
- **tls-alpn-01**, som RFC 8737 la til i februar 2020, svarer på port 443 under et TLS-håndtrykk med en egen ALPN-protokoll. Den passer for en omvendt proxy som holder port 443 og må klare seg uten port 80.

RFC 9773, publisert i juni 2025, la til ACME Renewal Information, forkortet ARI. Utstederen publiserer et foreslått tidsvindu for å fornye hvert sertifikat den har utstedt, og klienten spør etter vinduet i stedet for å gjette. Dermed kan utstederen flytte fornyelser tidligere, f.eks. foran en massetilbakekalling, uten at noen må redigere en konfigurasjonsfil.

Bruk begrepet i en beslutning

Bruk «Hva er ACME?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Kontoer, passord og tilganger ordnet slik at folk har nøyaktig den tilgangen jobben krever, og de som slutter, mister den samme dag.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Skrev 1 000 RBAC-regler for å sikre Linux-servere — 1,000 tilgangsregler skrevet for å tette et sikkerhetshull

Skrev 1 000 RBAC-regler for å sikre Linux-servere Ta kontakt →

Hvorfor det er viktig

Om et menneske fortsatt kan fornye sertifikater for hånd, er ikke lenger et spørsmål om smak. Spørsmålet har fått datoer.

CA/Browser Forum fastsetter reglene alle offentlig betrodde utstedere følger. Avstemningen SC-081v3, vedtatt i april 2025, begrenser et sertifikat utstedt fra og med 15. mars 2026 til 200 dager. Grensen faller til 100 dager fra 15. mars 2027 og til 47 dager fra 15. mars 2029, og tiden et bevis på domenekontroll kan gjenbrukes, faller i takt, fra 200 dager nå til 100 og til slutt bare 10. Med de endelige reglene trenger et navn som fornyes etter to tredjedeler av levetiden, et nytt sertifikat omtrent hver måned, og nesten hver av de fornyelsene trenger en fersk utfordring.

Let’s Encrypt ligger foran den tidsplanen. Standardsertifikatene varer 90 dager i dag. Fra 10. februar 2027 varer de 64 dager, med autorisasjoner som kan gjenbrukes i 10 dager, og fra 16. februar 2028 varer de 45 dager, med gjenbruk

kuttet til 7 timer. Kunngjøringen fraråder selv manuell fornyelse. Let's Encrypt sluttet også å sende e-poster om utløp 4. juni 2025, så sikkerhetsnettet som fanget en glemt fornyelse, er borte.

Fornyelse for hånd er altså ute av bildet, og ACME er standardvalget. Det som gjenstår å bestemme, er hvor de bevegelige delene skal bo:

- **Utfordringen.** http-01 er den enkle starten for én server som svarer på port 80. dns-01 er verdt det ekstra oppsettet for jokertegnnavn, for flere servere bak ett navn og for verter internett ikke når. tls-alpn-01 hører hjemme i proxyer som holder port 443 og mangler port 80.
- **Klienten.** Den kan bo inne i webserveren, kjøre ved siden av den med et skript som installerer hvert nye sertifikat, eller kjøre på en egen maskin som validerer sentralt og kopierer sertifikatene ut.
- **Vakten.** Noe utenfor klienten må merke at en fornyelse har uteblitt, fordi klienten er nettopp den delen som akkurat har feilet.

Slik ser det ut i praksis

I rollen som DevOps-ingeniør tok selskapet sertifikatarbeidet ut av menneskehender for hundre Docker-applikasjoner på verter med Ubuntu Linux, der både Apache og nginx betjente trafikken. ACME tok seg av hvert steg: utstedelse, fornyelse før utløp og utrulling til vertene. Hele syklusen gikk av seg selv, uavhengig av om noen husket en dato. Alle de hundre applikasjonene beholdt gyldige sertifikater, og håndarbeidet forsvant.

Utrullingen er steget det er lett å undervurdere. Apache og nginx leser et sertifikat når de starter eller lastes inn på nytt, og fortsetter å servere den kopien. En klient som bare skriver en ny fil, har dermed fornyet ingenting en besøkende kan se. Der Apache og nginx deler en flåte, trenger hver av dem sin egen omlasting når et nytt sertifikat lander.

Selskapets eget nettsted viser den andre ordningen, der klienten er webserveren. Caddy fornyer nettstedets sertifikat fra Let's Encrypt selv. Caddy snakker ACME innebygd og trenger ikke noe eget verktøy, så det finnes ikke noe utrullingssteg å glemme.

Hvor det går galt

Valideringen går ut på tid eller gir 404, selv om nettstedet lastes fint i nettleseren. http-01-forespørselen kommer inn på port 80, og noe på veien er feil: en brannmur eller en sikkerhetsgruppe i skyen som bare åpner 443, en omdirigering til andre porter enn 80 og 443, eller en lastbalanserer som sender forespørselen til en server som aldri fikk tokenet. Let's Encrypt følger opptil ti omdirigeringer, og bare til de to portene. Hold port 80 åpen, server utfordringsstien fra hver backend eller fra delt lagring, og bytt til dns-01 der port 80 er utilgjengelig.

DNS-API-nøkkelen på webserveren kan skrive om hele sonen. Et jokertegnnavn krever dns-01, så klienten trenger en måte å lage TXT-poster på, og den enkleste nøkkelen å få tak i kan ofte endre hver eneste post kontoen eier. Blir webserveren kompromittert, kan angriperen omdirigere e-post og alle andre navn også. Bruk en nøkkel begrenset til `_acme-challenge` -postene der leverandøren tilbyr det, pek `_acme-challenge` med en CNAME til en sone som er satt av til domenevalidering, eller valider fra en egen maskin og kopier sertifikatene over. DNS-endringer tar tid å spre seg, så klienten må kanskje vente opptil en time før den ber om domenevalidering.

Etter en ny utrulling kommer nye containere opp uten sertifikater. Hver container ber om sitt eget sertifikat når den starter, og holder det bare i sitt eget filsystem, så hver omstart spør på nytt. Rull ut ofte nok, eller start mange samtidig, så avviser utstederens rate limits de ekstra bestillingene. RFC 8555 har et eget navn på feilen, `rateLimited` . Let's Encrypt advarer om at i verste fall får ingen av instansene et sertifikat. Hold sertifikater og nøkler i varig lagring, og la en ny instans bruke et gyldig sertifikat derfra før den bestiller et nytt.

En fast fornyelsestimer lar sertifikatene gå ut når levetiden krymper. Jobben fornyer f.eks. hver 60. dag, et tempo tilpasset sertifikater på 90 dager. Et sertifikat på 64 dager gir den timeren fire dagers margin, og et på 45 dager går ut omtrent to uker før timeren slår til. RFC 9773 nevner faste intervaller som en av vanene som hindrer utstederne i å endre levetidene. Slå på ARI der klienten støtter det. Let's Encrypt råder til å sjekke ARI minst to ganger i døgnet og, som en reserve, å fornye når en tredjedel av levetiden gjenstår.

Klienten melder suksess, og de besøkende ser fortsatt det gamle sertifikatet. Den nye filen ligger på disken, men ingenting ba webserveren laste inn på nytt, eller utrullingshooken lastet inn én server av flere. Det gamle sertifikatet blir

stående i drift til det går ut. La klientens utrullingshook laste serveren inn på nytt, og overvåk sertifikatet som faktisk serveres, sjekket utenfra, i stedet for filen:

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

Les mer

- RFC 8555: Automatic Certificate Management Environment (ACME) — kontoer, bestillinger, autorisasjoner og utfordringene http-01 og dns-01.
- RFC 9773: ACME Renewal Information (ARI) Extension — fornyelsesvinduet en utsteder foreslår for hvert sertifikat.
- RFC 8737: ACME TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension — utfordringen tls-alpn-01, som besvares helt og holdent på port 443.
- Challenge Types — Let’s Encrypts egen sammenligning av de tre utfordringene, med begrensningene til hver.
- Decreasing Certificate Lifetimes to 45 Days — datoene for kortere sertifikater hos Let’s Encrypt, og rådene deres om fornyelse.
- Ballot SC-081v3 — avstemningen i CA/Browser Forum som fastsetter grensene på 200, 100 og 47 dager.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er ACME?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/acme/