Engineer

Gemini

en let internetprotokol til at levere hypertekst

Hvad det er

Gemini er en applikationsprotokol til at hente dokumenter, hvor hele udvekslingen består af én krypteret forbindelse, én adresse fra klienten og ét svar fra serveren, hvorefter forbindelsen lukkes. Projektets egne dokumenter kalder den Gemini-protokollen; adresserne begynder med `gemini://`, et site, der serveres over den, hedder en kapsel, og netværket af kapsler kaldes Geminispace.

Projektet begyndte i juni 2019 under grundlæggeren Solderpunk, som stadig er dets »Benevolent Dictator«. Specifikationen, version 0.24.1, er frigivet til public domain under CC0 og beskriver protokollen som en gradvis forbedring af Gopher snarere end en afklædt udgave af HTTP. Projektets FAQ ser det fra den anden side: protokollen minder om noget mellem HTTP 0.9 og HTTP 1.0, med én slags forespørgsel, nogenlunde en `GET`.

Klienten forbinder til TCP-port 1965 – tallet henviser til den første bemandede Gemini-mission, der fløj i marts 1965 – og gennemfører et TLS-håndtryk; begge sider skal understøtte TLS 1.2 eller nyere. Den sender den absolutte URL efterfulgt af vognretur og linjeskift, og URL'en må højst fylde 1.024 bytes. Serveren svarer med én headerlinje: en tocifret statuskode, et mellemrum og en kort tekst, hvis betydning afhænger af koden. Koderne falder i seks grupper: 10–19 beder om input, 20–29 betyder succes, 30–39 omdirigerer, 40–49 er midlertidige fejl, 50–59 er permanente, og 60–69 handler om klientcertifikater. Ved succes er teksten en MIME-type, og indholdet følger som rå bytes uden komprimering og uden opdeling i bidder. Til sidst lukker serveren forbindelsen med TLS-beskeden close_notify, og det er sådan, klienten ved, at den har fået det hele.

Protokollen kan bære enhver slags fil, men den blev udformet sammen med sit eget dokumentformat, gemtext, der serveres som `text/gemini` .

Brug begrebet i en beslutning

Brug »Hvad er Gemini?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Et site, der er hurtigt, kan findes og kan redigeres af jeres egne folk, uden en regning for hver ændret sætning.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har udviklet 100 webapplikationer med HTML/HTML5 — 100 webapplikationer bygget

Har udviklet 100 webapplikationer med HTML/HTML5 Kontakt os →

Hvorfor det betyder noget

Det egentlige valg står sjældent mellem nettet og Gemini. Ifølge FAQ'en er protokollen ikke tænkt som afløser for hverken nettet eller Gopher, og den har et navn for at udgive det samme indhold over to eller tre af dem: bihosting og trihosting. Spørgsmålet for den, der ejer et site, er, om en ekstra hoveddør er værd at holde åben.

Det, protokollen giver, er privatliv, der er bygget ind fra starten. FAQ'en slår fast, at Gemini aldrig vil få noget, der svarer til headerne Cookie, Referer eller User-Agent. En forespørgsel er en URL og intet andet, så en server har meget lidt at registrere, selv hvis operatøren ville, og der kører intet script i læserens klient, som kan rapportere tilbage. FAQ'en regner »defensive non-extensibility« blandt prioriteterne bag designet: formaterne for forespørgsel og svar har ikke plads til et nyt headerfelt, så en senere version har intet sted at bringe sporing tilbage. For den, der udgiver ren tekst, er det hele pointen.

Prisen er meget af det, nettet har fået siden HTTP 1.0. Der er ingen cookies, så en kapsel, der skal genkende en tilbagevendende læser, beder i stedet om et klientcertifikat, som læseren selv skal oprette og passe på. Der er som udgangspunkt ingen certifikatudsteder: specifikationen anbefaler kraftigt Trust on First Use, eller TOFU, hvor klienten accepterer det certifikat, en server viser første gang, og fastlåser det bagefter. Dermed bliver serverens certifikat et langvarigt løfte. Krypteringen skjuler siden, men serverens navn rejser i TLS' Server Name Indication, og FAQ'en indrømmer, at værtsnavnet stadig lækkes. Læserne skal bruge en særlig Gemini-klient i stedet for en browser, så publikum er lille. Og store filer passer dårligt, fordi et svar hverken har en størrelse eller en kontrolsum.

Et team, der har brug for interaktive formularer, konti med adgangskoder, analyse eller et rigt layout, hører hjemme på nettet. Et team, der udgiver dokumenter og vil have en kanal uden cookies eller scripts på klientsiden, kan tilføje Gemini for meget lidt, så længe indholdet allerede findes som filer.

Sådan ser det ud i praksis

engineer.company er selv en kapsel på `gemini://engineer.company`. Kolofonen nævner Agate som det program, der besvarer Gemini-forespørgsler, ved siden af Caddy til nettet, Gophernicus til Gopher og Tor til onion-tjenesten. Alle fire læser den samme mappe med filer, så én udrulning opdaterer dem alle. Det er FAQ'ens bihosting strakt til fire kanaler og gjort på den billigste måde: kapslen er blot én læser mere af en mappe, som hver udrulning alligevel fylder, frem for et ekstra site, der skal holdes i takt.

Samme side er ærlig om den begrænsning, der er beskrevet ovenfor. Den skriver, at Gemini og Gopher hver vil have sin egen klient i stedet for en browser, og at Gopher sender oplysninger om, hvilken side du læser, i klartekst. Gemini krypterer det, men det netværk, du læser fra, ser stadig, hvilken adresse du bad om. Det er FAQ'ens lækkede servernavn, set fra læserens stol i stedet for designerens.

Siden om privatliv skelner mellem applikationernes adgangslog og styresystemets logfiler. Gemini- og Gopher-applikationerne fører ingen adgangslog; siden september 2026 registrerer deres daglige tællere kun det samlede antal forespørgsler. Gopher har desuden en forbindelseslog i styresystemet, som indeholder kildeadressen; den log slettes efter 30 dage.

Hvor det går galt

De fleste problemer med Gemini viser sig i første linje af et svar, og den linje kan læses i hånden med intet andet end OpenSSL:

```
printf 'gemini://engineer.company/\r\n' |
  openssl s_client -quiet -connect engineer.company:1965 \
    -servername engineer.company
```

Den første linje, der kommer tilbage, er headeren, for denne kapsel `20 text/gemini;lang=en`, og siden følger efter den.

Faste læsere bliver advaret om, at kapslen måske er under angreb. Klienter, der følger specifikationen, gemmer fingeraftrykket og udløbsdatoen for det første certifikat, de ser. Et andet certifikat, før den dato er passeret, regnes som et muligt tegn på et man-in-the-middle-angreb. En operatør, der laver et nyt certifikat ved hver udrulning eller flytter kapslen til en ny maskine uden nøglen, udløser den advarsel hos hver eneste fast læser. Tag backup af nøgle og certifikat sammen med resten af serveren, udsted certifikatet med lang gyldighed, og skift det først efter den udløbsdato, klienterne allerede har registreret.

Et søgefelt svarer med status 59. Et svar med status 10 beder læseren om en linje input, og klienten sender den tilbage som query-delen af den samme URL, procentkodet. URL'en må højst fylde 1.024 bytes, og en server skal afvise alt, der er længere, som en ugyldig forespørgsel. Et langt svar fylder grænsen hurtigt, og tekst uden for ASCII fylder den hurtigere: et »ø« er to bytes i UTF-8 og seks tegn, når det er procentkodet. Bed om korte svar, og brug status 11 til følsomt input som en adgangsfrase, så klienterne lader være med at vise den på skærmen.

Læsere bliver logget ud mellem siderne. Protokollen har ingen cookies, så sessionstilstand, der holdes på nettets måde, overlever ikke fra den ene forespørgsel til den næste. En kapsel, der skal vide, hvem der spørger, svarer med status 60, læserens klient opretter et certifikat, og serveren genkender det ved de følgende forespørgsler. Specifikationen begrænser certifikatet til den vært og port, der bad om det, og til den ønskede sti og alt under den, så læg alle sider, der skal bruge identiteten, under én sti. Skriv på siden, hvad certifikatet bruges til, for læseren skal sige ja til det.

En stor download bliver afbrudt, og ingen opdager det. Et svar har hverken længde eller kontrolsum, så en overførsel, der stopper halvvejs, kan ligne en, der blev færdig, bortset fra den manglende close_notify. Vejledningen i god praksis foreslår, at filer over 100 MiB hellere serveres på anden vis. Læg store filer på HTTPS, og link til dem fra kapslen; en Gemini-side må linke til en URL med et hvilket som helst skema.

Læs mere

- Gemini network protocol specification — forespørgsler, alle statuskoder, brugen af TLS og fastlåsning af certifikater i ét kort dokument.
- Project Gemini FAQ — projektets mål, sammenligningen med HTTP og Gopher og projektets eget svar på kritikken af TOFU.

- Best practices for Gemini implementations — filnavne, store filer, grænser for omdirigeringer og TLS-indstillinger.
- History of Project Gemini — hvordan en idé fra Gopherspace i 2019 voksede til et netværk for sig, fortalt af projektet selv.

Ordliste

Vælg ud fra jeres faktiske vilkår

Beskriv arbejdsgangen, de eksisterende grænseflader og de brugere, der har brug for ændringen. Vi kan definere en testbar leverance og en overdragelse, der gør teamet i stand til at vedligeholde løsningen.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er Gemini?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/gemini/