Difi
Direktoratet for
forvaltning og ikt

Vedlegg A: Behandling i Standardiseringsrådet, HTTPS

Innhold:

- Saksframlegg til Standardiseringsrådets møte 20180925-A
- Oppsummering av høringssvar - HTTPS
- Oppdatert forslag til anbefaling - HTTPS

Difi
Direktoratet for forvaltning og ikt

Dato:	21.8.2018	Saksnr:	18/00643

Til:	Rune Karlsen
Kopi:	
Fra:	Seksjon for informasjonssikkerhet
Saksbehandler:	Håkon Styri

Saksframlegg til Standardiseringsrådets møte 25.09.2018

Anbefalte standarder for sikker datakommunikasjon

Dette forslaget gjelder endring av en eksisterende anbefaling[1] som ble innført 12.09.2017.

Formålet med standarden

Den eksisterende anbefalingen har til formål å oppnå sikker overføring av data til og fra nettsteder som tilhører virksomheter i offentlig sektor eller som brukes til tjenester som leveres av virksomheter i offentlig sektor. Dette omfatter både overføring av data mellom nettleser (sluttbruker) og nettjener, og mellom tjenester (API) som bruker protokollen HTTP.

Forslaget til endring opprettholder det beskrevne formålet. Formålet med endringen er å forbedre dette sikkerhetstiltaket og å presisere at sikker overføring av data til og fra nettsteder alltid skal brukes.

Hovedbegrunnelsen for forslaget er at endringer i nettlesere fra store leverandører i markedet og endringer i virkemåten til søketjenester representerer nye faktorer når nytteverdien av denne anbefalingen skal vurderes.

Kort om de foreslåtte endringene

Vi foreslår følgende endringer:

1. Vi foreslår at spesifikasjonen RFC 2817 kan benyttes som et alternativ til spesifikasjonen RFC 2818. Dette er en endring som ikke får konsekvenser for dem som allerede bruker RFC 2818, men åpner for muligheten til å velge en alternativ teknisk løsning. Endringen medfører derfor ingen økt kostnad.
2. For å understøtte at sikker kommunikasjon alltid brukes legges det til anbefalingen at spesifikasjonen RFC 6797 (HTTP Strict Transport Security) benyttes. Avhengig av virksomhetens eksisterende løsning kan denne endringen medføre en engangskostnad

[1] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen/grunnleggende-datakommunikasjon-0

ved endring av nettstedet, men denne endringen vil ikke medføre økte driftskostnader. Vi antar at engangskostnaden er lav.

3. For å etablere en standard for hvordan omdirigering av forespørsler som ikke bruker protokollen for sikker overføring av data skal gjøres beskrives dette i anbefalingen. Ønsket standard er at omdirigering fra HTTP til HTTPS gjøres til samme URL for å gjøre det mulig å etablere automatisk testing av etterlevelse. Denne endringen kan medføre at enkelte eksisterende nettsteder må endres. En slik endring vil medføre en engangskostnad, men medfører ingen driftskostnad. Vi antar at engangskostnaden er lav.
4. Difi vurderer å be om at denne anbefalingen gjøres obligatorisk. Dette gjøres for å sikre at denne anbefalingen i større grad blir fulgt av virksomheter i offentlig sektor.

Endring av referanser til de tekniske spesifikasjonene

Dagens tekst er som følger:

> «Det anbefales at offentlige kommunikasjonstjenester har støtte for HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230] og TLS 1.2 [RFC 5246].»

Difi foreslår å endre denne teksten til:

> «Det anbefales at offentlige kommunikasjonstjenester har støtte for Upgrading to TLS Within HTTP/1.1 [RFC 2817] eller HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230] og TLS 1.2 [RFC 5246]. Det anbefales at HTTP Strict Transport Security (RFC 6797) blir brukt.
>
> Dersom en tjeneste får en forespørsel med bruk at HTTP uten bruk av sikker overføring med bruk av TLS skal tjenesten svare ved omdirigering til samme URL med bruk HTTP over TLS.»

Det er viktig å påpeke at virksomhetene også må ha en god veiledning for å bruke standarden riktig. Den eksisterende veiledningen fra NSM er tilstrekkelig, men må oppdateres ved endring av anbefalingen for å bidra til at de over nevnte spesifikasjoner blir brukt på riktig måte.

Begrunnelse for endring

Endring nummer 1 begrunnes med at det ikke er noen grunn til å utelukke en av de to likeverdige spesifikasjonene RFC 2817 og RFC 2818 når man skal velge teknisk løsning eller leverandør. Da må anbefalingen nevne begge spesifikasjonene.

Fordi målet med anbefalingen er at HTTPS alltid skal benyttes er det hensiktsmessig å legge til spesifikasjonen RFC 6797 som vil bidra til å oppfylle dette målet.

Mange nettsteder har behov for å bruke HTTPS som et sikkerhetstiltak for deler av nettstedet hvor det utveksles informasjon som medfører krav til konfidensialitet. Det gir i praksis ingen besparelse å bruke HTTPS kun på deler av et nettsted.

Forslaget til anbefaling omfatter ikke krav til hvilken type sertifikater som bør brukes eller krav til fremstilling av sertifikater (krav til sertifikatleverandør). Krav til sertifikater kan bidra til å redusere risiko ytterligere, men slike krav kan medføre høyere kostnader. Difi anbefaler at krav til sertifikater knyttes til risikovurdering av den enkelte tjeneste.

Det er viktig å understreke at bruk av HTTPS vil redusere risikoen for at brukere opplever at innholdet i tjenesten blir endret på veien mellom tilbyder av en tjeneste og brukerens nettleser. Dette gjelder ikke bare forskjellige typer angrep mot brukeren, men også tilfeller der et mellomledd legger reklame eller annen informasjon til den originale tjenesten. Bruk av HTTPS vil derfor medføre en fordel for brukere av tjenesten. Indirekte vil dette bidra til at brukere opprettholder tillit til virksomheter i offentlig sektor. Det er vanskelig å sette noen økonomisk verdi på disse fordelene.

Difi ønsker at Standardiseringsrådet skal vurdere om denne standarden bør bli obligatorisk. Begrunnelse for dette følger under.

Endringer i forutsetninger

Søketjenester vil rangere nettsteder som bruker HTTPS foran nettsteder som ikke bruker HTTPS. Bruk av HTTPS vil derfor være en fordel for synlighet for brukere som søker etter tjenesten, og for disse brukerne vil dette oppleves som bedre tilgjengelighet. Det er vanskelig å sette noen økonomisk verdi på denne fordelen.

Tidligere har nettlesere merket nettsteder som bruker HTTPS med en hengelås i adressefelt. Utviklingen går i retning av at nettlesere i stedet merker nettsteder som *ikke* bruker HTTPS som usikre. Enkelte nettlesere vil gjøre det vanskeligere for brukere å besøke usikre nettsteder. Dette vil i praksis bety dårligere tilgjengelighet til tjenester som bruker usikre nettsteder. Dersom offentlige virksomheter ikke bruker HTTPS er det sannsynlig at dette vil ramme brukernes tillit til tjenestene, og det vil påvirke nettstedenes tilgjengelighet negativt. Det er vanskelig å sette noen økonomisk verdi på denne ulempen.

Det er grunn til å anta at nettlesere og søketjenester også tiden fremover vil endre reglene for hvordan nettsteder som bruker sikker datakommunikasjon merkes eller på annen måte fremheves. Denne utviklingen kan medføre et behov for å endre anbefalingen dersom det er ønskelig å påvirke hvordan nettstedene til offentlig sektor fremstår i nettlesere og søketjenester.

Konsekvenser dersom eksisterende anbefaling ikke endres

Digitale tjenester som ikke bruker HTTPS eller som ikke har etablert HTTPS på en korrekt måte vil merket som usikre i nettlesere. Når tjenestene fremstår som usikre påvirker dette tilliten til tjenesten negativt. Nettlesere kan i tillegg etablere barrierer som gjør det vanskeligere for brukere å bruke tjenesten. Dersom eksisterende anbefaling ikke endres vil det øke risikoen for at slike tjenester er oppleves som utilgjengelige.

Det vil ha negative konsekvens dersom eksisterende anbefaling ikke endres.

Kostnader

De foreslåtte endringene kan medføre at virksomheter må gjøre endringer på eksisterende tjenester. Kostnaden for hvert enkelt nettsted vil variere avhengig av teknisk løsning og nettstedets kompleksitet.

Det er viktig at virksomhetene regelmessig tester sine tjenester for å verifisere at sikker datakommunikasjon er satt opp korrekt. Feil bruk av standarden kan medføre at nettlesere gir brukere varsel om at tjenesten er usikker, eller at nettleseren oppretter en barriere for bruk av tjenesten som vil påvirke tilgjengeligheten. Regelmessig testing av at denne standarden følges vil være et kostnadselement for drift, men vil ikke utgjøre noen stor del av driftsutgiftene.

Når et nettsted går fra å bruke usikret til å bruke sikker overføring av data til og fra brukere vil det kreve økt bruk av CPU-ressurser for kryptering og dekryptering av data, men økningen er i praksis liten. HTTPS medfører også en liten forsinkelse (noen millisekunder) ved oppkobling av hver forbindelse. Dette er faktorer som kan medføre noe høyere driftskostnader. Dersom den tekniske løsningen for nettstedet støtter protokollen HTTP/2 vil bruk av sikker overføring muliggjøre en langt mer effektiv og raskere overføring av data. Dette er en faktor som kan bidra til lavere driftskostnader. Vær oppmerksom på at dette avsnittet omtaler driftsutgifter knyttet til den eksisterende anbefalingen.

Kostnader for sertifikater

Ett kostnadselement som har vært diskutert ved tidligere behandling av standard for sikker datakommunikasjon er knyttet til sertifikater. Endringer i markedet har ført til at det er flere leverandører som tilbyr en enkleste klasse type sertifikater som det ikke er knyttet avgifter til å utstede eller fornye. For virksomheter vil det være en lav engangskostnad for å etablere rutiner for å bestille og fornye slike sertifikater, men denne typen sertifikater kan redusere kostnadene knyttet til å etablering og drift av sikker datakommunikasjon.

Difi vil understreke at det bør gjøres en risikovurdering av hver enkelt tjeneste før man velger hva slags sertifikat som bør brukes. For viktige tjenester bør sertifikat med utvidet validering (EV) benyttes.

Begrunnelse for endring til obligatorisk standard

Difi vurderer å be om at anbefalingen endres til å bli en obligatorisk standard. Ulempen ved at enkelte tjenester oppleves som utilgjengelige er en vesentlig faktor i denne vurderingen. Det er viktig å opprettholde tillit til tjenester som leveres av virksomheter i offentlig sektor. En obligatorisk standard er også et effektivt et virkemiddel for å unngå at digitale tjenester levert av virksomheter i offentlig sektor merkes som usikre av nettlesere eller av søketjenester.

Forslag A – HTTPS – Oppsummering av høringssvar

Det følgende er en oppsummering av vesentlige merknader fra svarene på høringen med kommentarer fra Difi.

Vedrørende bruk av TLS 1.2 har høringssvarene fra Buypass AS, Passordninja AS og Helse Midt-Norge påpekt at IETF etter at forslag A ble sendt ut på høring har publisert RFC 8446 TLS 1.3. Buypass har uttalt at «I det konkrete forslaget til endringer nevnes spesielt HTTP/1.1 og TLS 1.2, men vi vil også anbefale bruk av HTTP/2 (RFC 7540) og TLS 1.3 (RFC 8446) som er siste versjoner av disse protokollene.»

Difi er kjent med at RFC 8446 TLS 1.3 er publisert og at status på RFC 5246 TLS 1.2 med dette er satt til foreldet. Teksten for både gjeldende anbefaling og i forslag A vil bli oppdatert som følge av dette. Det er for øvrig viktig å merke seg at nettstedene fortsatt må støtte TLS 1.2 ettersom det er mange brukere som ikke har programvare for den nyeste versjonen av TLS.

Fordi RFC 7540 HTTP/2 i praksis krever HTTPS ser ikke Difi noen hensikt i å anbefale denne spesifikasjonen på nåværende tidspunkt.

Vedrørende forslaget om å legge til RFC 2817 som et likestilt alternativ til RFC 2818 har Uninett AS en argumentasjon som understøtter en påstand om at «de to standardene i realiteten er langt fra likeverdige.» Uninett konkluderer med at «RFC 2817 må regnes som forlatt teknologi uten en eksistensberettigelse» og anbefaler at forslaget om å legge til RFC 2817 strykes.

Difi kan ikke se at EU-kommisjonens rådgivende ekspertgruppe Multi Stakeholder Platform on ICT Standardisation har uttalt noen tvil om eksistensberettigelsen til RFC 2817 i sin behandling av de to standardene. Difi vil likevel ta til følge argumentasjonen om at RFC 2817 og RFC 2828 i praksis ikke er likeverdige når målsetningen er at all kommunikasjon mellom nettsteder og brukere skal være kryptert. Difi vil derfor trekke forslaget om å legge til standarden RFC 2817 som et alternativ til løsninger som bruker den eksisterende anbefalingen RFC 2818.

Uninett har også en kommentar vedrørende RFC 6797 HSTS. Den vesentlige delen av kommentaren er som følger: «Selv om målsetningen er at sikker kommunikasjon alltid skal brukes er det ikke gitt at RFC 6797 i et hvert tilfelle er den beste veien til å oppnå dette. […] Dersom det er publisert et større antall pekere til http-adresser (både internt og eksternt) vil dette kunne gi en marginal forbedring av responstiden ved at nettleserne ikke trenger å ta turen innom redigeringssiden for hver nye adresse, men ulempen er at de som vedlikeholder nettstedet ikke får logget hvilke adresser som er berørt og hvor de er publisert, noe som kan gjøre det vanskeligere å nå målet om at adressene skal være med https i første omgang.»

Uninett har to alternative forslag angående RFC 6797. Det ene alternativet er å stryke forslaget om å bruke RFC 6797. Det andre alternativet er å endre teksten slik at den beskriver en løsning med omdirigering av forespørsler med et mulig tillegg om når RFC 6797 kan brukes. Uninetts forslag er som følger: «Dersom en tjeneste mottar en forespørsel med bruk av HTTP skal tjenesten svare med

omdirigering til samme URL med bruk av HTTPS» og tillegget «RFC 6797 kan benyttes i tillegg til dette dersom nettstedets administrator ikke har behov for detaljert logginformasjon om redigeringen.»

Difi vil fastholde at det er ønskelig å anbefale bruk av RFC 6797, men at det er hensiktsmessig å legge inn en tekst som gjør det klart at dersom man ved drift av nettstedet har behov for å logge forespørsler som buker HTTP i stedet for HTTPS, så er dette en tilstrekkelig begrunnelse for å ikke bruke RFC 6797.

Arbeids og velferdsdirektoratet (NAV) kommenterer i forbindelse med RFC 6797: «burde det ha kommet spørsmål om anbefalinger på max-age parameteren i tillegg?» Difi vurderer at det er hensiktsmessig å legge anbefalinger om dette i en veiledning. Det samme gjelder kommentaren fra Uninett om å advare mot HTTP Public Key Pinning (HPKP).

Statistisk sentralbyrå (SSB) har i sitt svar uttalt at de «ønsker imidlertid å poengtere at sertifikater på offentlige nettsider bør komme fra godkjente utstedere, slik at man slipper å få advarsler på eksempelvis om signerte sertifikater benyttes.» Nasjonal sikkerhetsmyndighet (NSM) har uttalt at «NSM anbefaler å bruke sertifikater utstedt fra en tiltrodd tredjepart. Etter flere hendelser med sertifikatutstedere og angrep ved hjelp av sertifikater, anbefaler NSM at sertifikater utstedt under norsk lovgivning benyttes.»

Buypass AS skriver følgende: «Det anbefales at «viktige tjenester» benytter sertifikater med utvidet validering (EV). Vi vil i denne anledning gjøre oppmerksom på at med Lov om elektroniske tillitstjenester (LOV-2018-06-15-44) som implementerer eIDAS-forordningen i Norge, introduseres en ny kvalifisert tillitstjeneste, «kvalifiserte sertifikater for nettstedsautentisering» (QWAC – Qualified Web Authentication Certificate). Dette kan betraktes som en ny sertifikattype som er underlagt felles europeiske reguleringer og ikke bare en bransjestandard slik EV-sertifikatene er. QWAC er basert på samme valideringer og kontroller som utvidet validering (EV), men har noen tillegg. Dette er en sertifikattype med svært høye sikkerhetskrav og sertifikatene er tatt inn i annet europeisk regelverk - som RTS (Regulatory Technical Standard) for nytt betalingstjenestedirektiv (PDS2). En slik sertifikattype bør være relevant å nevne også i denne anbefalingen.»

Difi er enige i at anbefalingen bør inneholde et punkt om at det skal benyttes sertifikater fra en tiltrodd leverandør. Når det gjelder valg av hvilken type sertifikater som skal benyttes mener Difi at dette skal være en risikobasert vurdering. Difi mener det er hensiktsmessig å blant annet bruke veiledning fra NSM når denne risikovurderingen gjennomføres. Når det gjelder QWAC-sertifikater er det viktig å avklare hvordan dagens nettlesere vil behandle slike sertifikater,

Buypass AS uttaler også at det er ønskelig at RFC 6844 (DNS Certification Authority Authorization) benyttes. Difi vurderer også dette som et relevant innspill, men vil behandle denne kommentaren under forslag D som gjelder DNSSEC.

Oppdatert forslag til anbefaling – Saksframlegg A – HTTPS

Den følgende utgaven av teksten er oppdatert etter behandling av høringssvar.

«Det anbefales at offentlige kommunikasjonstjenester har støtte for HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230] og TLS 1.3 [RFC 8846].

Dersom en tjeneste får en forespørsel med bruk at HTTP uten bruk av sikker overføring med bruk av TLS skal tjenesten svare ved omdirigering til samme URL med bruk HTTP over TLS.

Det anbefales også at HTTP Strict Transport Security (RFC 6797) blir brukt, men dersom den ansvarlige for nettstedet har behov for å logge omdirigeringer er dette tilstrekkelig begrunnelse for å ikke bruke RFC 6797 i perioden hvor det logges.»

Det er viktig at nettstedet settes opp korrekt, og det vises i den forbindelse til veiledning fra Nasjonal sikkerhetsmyndighet (NSM): *HTTP over TLS: Hvordan autentisere nettsteder og konfidensialitets- og integritetsbeskytte webtrafikk*. IT-veiledning for ugraderte systemer nr. 15 (U-15) og veiledningen *Sikring av kommunikasjon med TLS: Beskrivelse av grunnleggende tiltak for sikring av kommunikasjon over usikre nett ved hjelp av TLS*. IT-veiledning for ugradert nr. 14 (U-14).

Vær oppmerksom på at selv om TLS 1.2 ikke lenger er anbefalt så er det nødvendig å beholde støtten for denne versjonen fordi det er mange brukere som har programvare som ikke er oppdatert med den nyeste versjonen av TLS.