HØRINGSNOTAT

Høring av forslag til nye eller reviderte forvaltningsstandarder			
Dato for utsendelse	23.01.17	Behandles i Standardiseringsrådet	22.03.17
Frist for høringssvar	**27.02.17**	Implementeres i referansekatalogen	April 2017

Grunnleggende datakommunikasjon
– *sikker datakommunikasjon fra offentlige nettsteder*

Innhold

Bakgrunn og historikk

Referansekatalogen for anbefalte og obligatoriske IT-standarder i offentlig sektor er publisert på Difi sitt nettsted[1]. Denne katalogen er organisert under *bruksområder*, og alle høringer omfatter *ett enkelt* av disse bruksområdene.

Beskrivelsene under bruksområdet omfatter en innledende beskrivelse (definisjon) av bruksområdet, krav til bruk av standarder på området, lenker til eventuelt veiledningsmateriell, mv. De endringene som foreslås kan gå på alle elementene i disse beskrivelsene, men vil normalt som et minimum omhandle krav til bruk av standarder.

Formål og målsetting med de foreslåtte endringene

Målsetningen med endringen er å øke tilliten til offentlige tjenester ved å tilby både autentisering av tjenesten og integritets- og konfidensialitetsbeskyttelse av informasjonen som sendes, og øke tilgjengeligheten for brukerne.

Autentisering av en tjeneste er avgjørende for å bekrefte at man utveksler data med korrekt tjeneste. Ved å ivareta integritetsbeskyttelse vet man at den samme informasjonen som ble sendt av avsender også når mottaker, det vil si at det ikke er gjort endringer i informasjonen under overføringen. Konfidensialitetsbeskyttelse gjør at uvedkommende ikke får innsyn i informasjonen som sendes. Søketjenester som Google gir fortrinn til nettsted som bruker sikker kommunikasjon. Enkelte nettlesere blokkerer nettsted som bruker sikker kommunikasjon feil. Anbefalingen vil derfor også bidra til bedre tilgjengelighet.

Utredningen har identifisert fire sentrale behov hos offentlige virksomheter. Behovene som utredningen regner som de mest sentrale er: Tillit, tilgjengelighet, brukervennlighet og effektivisering. I tillegg har vi i utredningen også identifisert eksterne føringer (Betalingstjenester på nett hos statlige virksomheter via PCI DSS) med krav til kryptering.

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

Det foreslås å anbefale at følgende standard og retningslinjer benyttes innen bruksområdet:

- RFC 7230 – HTTP/1.1: Denne standarden erstatter RFC 2616 som nå er foreldet.
- RFC 2818 – HTTP Over TLS: Et notat som beskriver hvordan TLS benyttes for å sikre HTTP tilkoblinger over internett og bør supplere RFC 7230. TLS protokollen finnes i flere versjoner.
- RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2: Denne standarden beskriver kommunikasjonssikkerhet over internett.

For at kommunikasjonen skal sikres i nødvendig og tilstrekkelig grad, er det viktig at standardene implementeres korrekt. NSM forvalter en veileder som omhandler implementasjon av HTTP over TLS. Difi og NSM anbefaler at NSMs veileder «HTTP over TLS»[2] følges så langt det er hensiktsmessig og ikke i konflikt med annet regelverk.

Prosess og deltakelse

Notatet «Utredning av behov for HTTPS i offentlig sektor – Tillit, tilgjengelighet, brukervennlighet og effektivisering» ble utarbeidet av Nasjonal sikkerhetsmyndighet (NSM) og Difi høsten 2016.

Historikk

Underområdet «Protokoll for overføring av informasjon på web» ble lagt inn fra NOSIP i referansekatalogen i 2012.

Forslag til endringer i referansekatalogen

Gjeldende tittel på bruksområdet:
Grunnleggende datakommunikasjon – Protokoll for overføring av informasjon på web

Lenke til bruksområdet i referansekatalogen:
https://www.difi.no/artikkel/2015/11/grunnleggende-datakommunikasjon-0

Tekstlig endring i beskrivelsen av bruksområdet

Navn på bruksområdet

Navnet på bruksområdet forblir «Grunnleggende datakommunikasjon», men navnet på underområdet endres *fra* «Protokoll for overføring av informasjon på web» *til* «Sikker datakommunikasjon fra offentlige nettsteder»

Innledende beskrivelse

Dagens beskrivelse er:

Offentlige kommunikasjonstjenester bør ha støtte for HTTP 1.1 [RFC 2616]. Dette er en grunnleggende protokoll for overføring av informasjon på web. Støtte for denne protokollen er en forutsetning for å lage nettjenester for brukere. Støtte for betyr at virksomheten skal kunne ha en mulighet for å bruke protokollen http, ikke at dere alltid skal benytte http. Andre protokoller kan benyttes/brukes der dere ønsker eller har behov for det

Denne foreslås endret til:

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].

[2] NSM veileder i HTTPS over TLS, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/https.pdf

HTTP/1.1 er en grunnleggende protokoll for overføring av informasjon på web. Støtte for denne protokollen er en forutsetning for å lage nettjenester for brukere. Denne protokollen bør settes opp med bruk av TLS, vanligvis omtalt som HTTPS, slik at informasjonen overføres gjennom en sikker forbindelse.

Støtte for betyr at virksomheten skal kunne ha en mulighet for å bruke protokollen HTTP, ikke at dere alltid skal benytte HTTP. Andre protokoller kan benyttes/brukes der dere ønsker eller har behov for det.

Krav til bruk av standarder

RFC 7230 – Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing (Juni 2014)
RFC 2818 – HTTP Over TLS (Mai 2000)
RFC 5246 – The Transport Layer Security (TLS) Protocol – Version 1.2 (August 2008)

Disse standardene revideres enkeltvis av IETF og Difi vil oppdatere anbefalingen med gjeldende versjon av hver standard når dette skjer, Dersom en revisjon medfører større endringer vil Difi vurdere behovet for å revidere hele anbefalingen. Revisjoner som medfører større endringer vil behandles av Standardiseringsrådet.

Når gjelder kravene fra

Anbefalingen vil publiseres i referansekatalogen i april 2017.

Hvordan tilfredsstille kravene

Nettsted som brukes av virksomheter i offentlig sektor bør etablere en teknisk løsning som bruker HTTP over TLS for alle deler av nettstedet.

Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet en veiledning for å etablere HTTP over TLS:
«Hypertext Transport Protocol Secure – Hvordan autentisere nettsteder og konfidensialitets- og integritetsbeskytte webtrafikk»
IT-veiledning for ugraderte systemer nr. 15 (U-15)

Veilederen forvaltes av Nasjonal sikkerhetsmyndighet og gir en sikkerhetsfaglig vurdering av hvordan HTTPS bør implementeres. For at kommunikasjonen skal sikres i nødvendig og tilstrekkelig grad, er det viktig at standardene implementeres korrekt. Veilederen NSM forvalter omhandler implementasjon av HTTP over TLS. Difi anbefaler at NSMs veileder «HTTP over TLS» følges så langt det er hensiktsmessig og ikke i konflikt med annet regelverk for å ivareta sikker implementasjon og vurdering av kompenserende tiltak for kjente sårbarheter.

Relevante standarder

RFC 6066 – Transport Layer Security (TLS) Extensions: Extension Definitions (2011)
RFC 6797 – HTTP Strict Transport Security (HSTS) (2012)
RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)
RFC 7469 – Public Key Pinning Extension for HTTP (2015)

Vurderinger om *anbefalte* versus *obligatoriske* standarder

Denne anbefalingen omfatter et sett med standarder og er i det vesentligste en anbefaling som dekker hvordan disse standardene bør brukes. De enkelte standardene oppdateres relativt ofte for å følge utviklingen i teknologi og marked. Enkelte virksomheter som følge av anskaffelser og oppgraderinger velge nyere versjoner av standardene som er anbefalt. Det vil derfor ikke være hensiktsmessig å gjøre samtlige standarder i denne anbefalingen obligatoriske.

Vi ber om tilbakemelding kun på de foreslåtte endringene beskrevet over.
Eventuelle ønsker om andre endringer eller justeringer i referansekatalogen, eller ønske om nye krav eller bruksområder, kan fortløpende meldes til Difi/Standardiseringssekretariatet, på e-post til standard@difi.no.

Spørsmål og ønsker til høringssvarene

Vi ber særlig om tilbakemeldinger og kommentarer på følgende:

1. Bruker din virksomhet standardene i dag?

2. Hva er virksomhetenes erfaringer/synspunkt på de foreslåtte standardene, både når det gjelder kostnader ved å ta dem i bruk, standardenes egnethet på bruksområdet og behov for kompetanse? Difi anbefaler veiledningsmateriell fra NSM i dette forslaget for å tilfredsstille kravene Difi foreslår, har deres virksomhet innspill til det, og til annet nyttig veiledningsmateriell?

3. Er det andre standarder på bruksområdene som burde vært vurdert?

4. Bør de foreslåtte standardene gjøres anbefalte, obligatoriske eller ikke pekes på i det hele tatt?

Høringsfristen er 27.02.2017. Høringsuttalelser merkes med saksnummer 17/00158, og sendes postmottak@difi.no eller Difi, postboks 8115 Dep, 0032 Oslo.

Konsekvensvurderinger

Gevinster

Denne anbefalingen vil bidra til å øke tilgjengeligheten til informasjon publisert på nettstedene til virksomheter i offentlig sektor. Den vil også bidra til å øke tilliten til digitale tjenester i forvaltningen.

Kostnader for forvaltningen

Kostnaden ved å implementere HTTPS vil variere. Anskaffelse- og vedlikeholdskostnader av sertifikater ansees ikke å være kostnadsdrivende. For eksisterende tjenester vil det påløpe kostnader relatert til implementering av og vedlikehold av selve tjenesten. Med dette menes for eksempel å konfigurere nettverksutstyr, endre tjenestekonfigurasjon, tilpasse innhold og eventuell anskaffelse av maskinvarebasert nøkkelmodul.

For utviklere / offentlige leverandører av spesialprogramvare som omfattes av anbefalingene, vil anbefalingene kunne bety at eldre programvare må fornyes.

Andre konsekvenser

Sikringsmekanismene som anbefales i utredningen, kan også brukes på e-post (for eksempel START-TLS) og VPN. Ved å se underliggende teknologier i sammenheng får man en ekstragevinst fordi en del av teknologi-investeringene da kun gjøres en gang for løsningene. Ett eksempel er sertifikater. Ved å implementere teknologiene i sammenheng, vil virksomhetene redusere sine kostnader. Å etterleve anbefalingene i NSM sin veileder er derfor også en måte å redusere kostnader.

Enkelte av mekanismene som brukes i denne anbefalingen forventes å bli innarbeidet i løsningene som bruker standarden HTTP/2 (RFC 7540), og denne anbefalingen vil bidra til at virksomheter i offentlig sektor opparbeider kompetanse som vil redusere kostnadene ved innføring av HTTP/2.

Utfyllende informasjon

Se vedlegg «Utredning av behov for – HTTPS i offentlig sektor – Tillit, tilgjengelighet, brukervennlighet og effektivisering» for teknisk gjennomgang og nyttig bakgrunnsforståelse.

Vedlegg

- Utredning av behov for – HTTPS i offentlig sektor – Tillit, tilgjengelighet, brukervennlighet og effektivisering

---

20.01.17
Høringsnotatet er utarbeidet av Difi / Avdeling Digitalisering / Seksjon Datadeling og informasjons-sikkerhet v/ Håkon Styri, i egenskap av kompetansesenter for bruksområde *Grunnleggende datakommunikasjon*.

Eventuelle spørsmål rettes på e-post til Difi/Standardiseringssekretariatet, til standard@difi.no.