**Nasjonal sikkerhetsmyndighet**

| Vår saksbehandler | Vår dato | Vår referanse |
|---|---|---|
| | 2016-05-25 | A03 - S:16/01408-2 |
| | Deres dato | Deres referanse |
| | 2016-04-01 | 16/2346 - ROKO |
| | Antall vedlegg | Side |
| | | 1 av 3 |

Til
Justis- og beredskapsdepartementet

# Oppdrag NSM - sikker tilkobling; HTTPS

Nasjonal sikkerhetsmyndighet viser til brev fra Justis- og beredskapsdepartementet av 1. april 2016 der NSM bes å vurdere bruk av sikker tilkobling for statlige webtjenester innen 6. mai 2016 (med innvilget fristutsettelse til 31. mai 2016). NSM vil i dette brevet vurdere hensiktsmessigheten av å innføre krav om sikker tilkobling for statlige webtjenester ved bruk av *Hypertext Transfer Protocol Secure* (HTTPS). Brevet omtaler også de nasjoner NSM er kjent med som har innført tilsvarende krav eller anbefalinger.

NSM har utarbeidet en rapport om bruk av HTTPS i for offentlige tjenester. Rapporten er vedlagt dette svaret i sin helhet og utdyper emnet ytterligere.

## Vurdering av hensiktsmessigheten av å innføre krav om sikker tilkobling til statlige webtjenester

### NSMs anbefaling

NSM mener at alle offentlige tjenester på web alltid skal benytte HTTPS. Dette vil gi både autentisering av tjenesten og integritets- og konfidensialitetsbeskyttelse av informasjonen som overføres.

For at HTTPS skal sikre kommunikasjonen må HTTPS benyttes på en sikker måte. Flere statlige webtjenester har ifølge NRK[1] implementert HTTPS med feil eller mangelfullt oppsett slik at sikker kommunikasjon ikke oppnås. NSM anbefaler at tiltrodde sertifikater benyttes sammen med moderne kryptografiske protokoller og mekanismer, og at systemet konfigureres korrekt. NSMs anbefalte implementering er beskrevet i vedlagt rapport kapittel 5 og bør inkluderes hvis et krav om å innføre sikker tilkobling innføres.

NSM anbefaler at andre private og kommersielle aktører også benytter HTTPS for deres tjenester.

[1] NRKs oversikt over offentlige domener som bruker HTTPS, https://nrkbeta.no/https-norge/

**Postadresse**
Postboks 814
1306 SANDVIKA

**Sivil telefon/telefaks**
+47 67 86 40 00/+47 67 86 40 09
**E-postadresse**
post@nsm.stat.no

**Militær telefon/telefaks**
515 40 00/515 40 09
**Internetadresse (URL)**
www.nsm.stat.no

### Nærmere redegjørelse

Ved bruk av HTTP overføres webtrafikk ukryptert mellom en webtjener og en klient. Dette gjør at man verken er sikker på hvem man snakker med eller om informasjonen er korrekt. HTTPS er overføring av webtrafikk over en sikker forbindelse.

NSM anbefalte i Sikkerhetsfaglig råd at krypteringsløsninger benyttes for å sikre offentlige nettsteder. Anbefalingen er beskrevet i tiltak 35:

*Alle statlige og kommunale nettsteder bør innføre krypteringsløsninger for bedre sikring av offentlige nettsteder. Dette vil øke sikkerheten i all kommunikasjon mellom innbyggerne og offentlige nettsteder.*

Offentlige tjenester krever en høy grad av tillitt fra brukeren av tjenesten. For tjenesteleverandøren er det viktig at brukeren kan stole på den informasjonen de mottar fra den tjenesten de etterspør og at kun involverte parter har tilgang til informasjonen som utveksles. Avlesning eller manipulering av data vil kunne ha både omdømmemessige, økonomiske og strafferettslige konsekvenser, og i ytterste fall innebære fare for liv og helse. 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 datagrunnlaget under overføringen. Ved å innføre HTTPS kan offentlige tjenestetilbydere tilby både autentisering av tjenesten og integritetsbeskyttelse av informasjonen som sendes slik at tillitten til tjenesten opprettholdes.

I de tilfeller det skal utveksles sensitive data mellom en tjenesteleverandør og en mottaker må konfidensialitetsbeskyttelse implementeres for at ingen uvedkommende får innsyn i informasjonen som sendes. Ved å benytte HTTPS gis slik beskyttelse av informasjonen i overføringen mellom sender og mottaker.

Utover de sikkerhetsmessige fordelene nevnt over vil gevinster og konsekvensene av et slikt krav kunne variere stort for de ulike tjenestetilbyderne. Momenter som tjenestens innhold, konfigurasjon og sluttbruker vil kunne påvirke omfanget av en implementasjon, men NSM mener at fordelene av et slikt krav veier opp mot de konsekvenser det vil kunne medføre. Kapittel 6 i rapporten adresserer de momentene NSM anser som de viktigste.

NSM ti viktige tiltak mot dataangrep S-02[2] sikrer endepunktene i kommunikasjonen (webtjener og klient) mens HTTPS sikrer selve overføringen av data. Fra et sikkerhetsperspektiv bør derfor disse tiltakene anbefales i kombinasjon med HTTPS for å øke sikkerheten. Tiltakene i S-02 vil dermed ikke kunne erstatte innføring av HTTPS eller motsatt. Følges derimot tiltakene i S-02, spesielt tiltak en og to, vil implementasjonen av HTTPS basert på NSMs anbefalte implementering antas å være mindre krevende og kostnadsdrivende. Dette er også gjeldende for sluttbruker av tjenesten. Dette er nærmere beskrevet i vedlagt rapport, kapittel 6.

## Tilsvarende anbefalinger fra andre nasjoner

NSM er kjent med at amerikanske og tyske myndigheter har innført krav om bruk av HTTPS i offentlig forvaltning. I USA kravstilte Office of Management and Budget i memorandum av 8.

[2] NSM S-02 Sjekkliste: Ti viktige tiltak mot dataangrep
https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf

juni 2015[3] at alle føderale tjenester skal har benytte HTTPS innen utgangen av 2016. Tyskland har gjennom *Act to Strengthen the security of Federal Information Technology* av 14. august 2009[4] og *Mindestandard des BSI für den Einsatz des SSL/TLS-Protocols ducrh Dundesbehören*[5] av 21. november 2014 anbefalt bruk av HTTPS for offentlige webtjenester. Tyskland stiller i tillegg krav til implementasjon av HTTPS, som i stor grad korresponderer med de anbefalingene NSM her gir.

Offentlig bruk av HTTPS er også omtalt av andre myndigheter. Nederlandske myndigheter har i brev datert 4.januar 2016 publisert sitt syn på kryptering[6] der viktigheten av kryptering for å ivareta konfidensialitet og integritet presiseres. Deres National Cyber Security Centre anbefaler også bruk av HTTPS, spesielt for sider som behandler sensitive data, og rådgir også hvordan HTTPS bør konfigureres. Deres konfigurasjonsråd er tilsvarende de NSM her gir. Svenske myndigheter anbefaler i sin veiledning for *Robust elektronisk kommunikasjon* utgitt av Post- og telestyrelsen at trafikk mellom webserver og eksterne klienters weblesere bør beskyttes mot manipulasjon og innsyn[7]

NSM er også kjent med at enkelttjenester krever sikker tilkobling. Eksempelvis har EUs fellesregister (Union registry)[8], som inkluderer det norske kvoteregisteret, per 15. oktober 2015 kravstilt bruk av HTTPS for tilkobling til registeret.

Hans Christian Pretorius
Avdelingsdirektør

Bente Hoff
Seksjonssjef

[3] M-15-13 HTTPS-Only Standard directive,
https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf
[4] Tysklands Act to Strengthen the Security of Federal Information,
Technologyhttps://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=1
[5] Bundesamt für Sicherheit in der Informationstechnik,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile&v=3
[6] Government of the Netherlands Cabinet's view on encryption,
https://www.government.nl/binaries/government/documents/letters/2016/01/04/cabinet%E2%80%99s-view-on-encryption/nl-cabinet-encryption-position.pdf
[7] Robust elektronisk kommunikasjon utgitt av Post- og telestyrelsen,
http://www.pts.se/upload/Documents/SE/PTSFS_20072_allmanna_rad_god_funktion_teknisk%20sakerhet.pdf
8 European Commission Climate Action,
https://ets-registry.webgate.ec.europa.eu/euregistry/EU/index.xhtml