Direktoratet for e-helse

Høringsuttalelse

Tittel: Høringsuttalelse, Forslag om å gjøre HTTPS som obligatorisk standard for offentlig forvaltning

Høringsbrev og – notat fra Digitaliseringsdirektoratet datert 27.05.2020, ref. 20/00581-2

Frist: 14.08.2020

Direktoratet for e-helse

Innledning

Direktoratet for e-helse viser til invitasjon om innspill på forslag om å gjøre HTTPS til en obligatorisk standard for offentlig sektor datert 27.5.2020.

Sammendrag

Direktorat for e-helse støtter tiltaket og ser det som hensiktsmessig å gjøre HTTPS obligatorisk for bruk i hele offentlig sektor.

Vår viktigste tilleggskommentar er at sikkerhetsegenskapene som man oppnår gjennom bruk av HTTPS er avhengig av kvaliteten på sertifikatene som tas i bruk. Standarden bør derfor også beskrive krav til sertifikater.

Vurdering av forslaget fra Digitaliseringsdirektoratet

I helse- og omsorgstjenesten foregår det aller meste av den eksterne kommunikasjonen mellom helseaktørene på Helsenettet. Helsenettet er en sikker digital arena for alle aktører i helse- og omsorgstjenesten, hvor du kan kommunisere og utveksle personopplysninger og pasientinformasjon på en trygg og lovlig måte. Aktørene er gjennom medlemsvilkårene forpliktet til å følge Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som angir helse- og omsorgstjenestens felles krav til informasjonssikkerhet og personvern.

I Normen er det en forutsetning at ekstern kommunikasjon av person- og helseopplysninger er sikret for konfidensialitet, integritet og tilgjengelighet. I tillegg er sikker autentisering viktig for å verifisere at kommunikasjonsparten faktisk er den som den utgir seg for å være. I Normen er det laget et eget faktaark[1] om kommunikasjon over åpne nett (nettverk som en dataansvarlig ikke har kontroll over selv) som legger til grunn Nasjonal sikkerhetsmyndighets sin veileder Sikring av kommunikasjon med Transport Layer Security (TLS).

Vi anser at HTTPS-standarden vil komme til anvendelse for helseaktørenes eksterne kommunikasjon både innad i Helsenettet og ut mot andre aktører og innbyggere.

Direktoratet for e-helse har ikke oversikt over bruk av HTTPS i helse- og omsorgstjenesten og kan derfor ikke kommentere hvilke konsekvenser innføringen av denne standarden som obligatorisk vil ha, men vi tror at nytten av å gjøre HTTPS til en obligatorisk standard er større enn kostnaden. På bakgrunn av at helse- og omsorgstjenesten er svært opptatt av å sikre konfidensialitet og integritet i ekstern kommunikasjon, tror vi at utbredelsen av HTTPS er langt større enn 1/3 av tjenestene som eksponeres innad og ut av helse- og omsorgstjenesten.

Obligatorisk standard bør også kunne peke på anbefalte og frarådede internasjonale standarder
I utredningen kommer det frem at Digdir ser det uhensiktsmessig å ta inn internasjonale standarder (eksempel: RFC 6844). En av grunnene som trekkes frem er ukjent utbredelse av en standard. Vi mener at den obligatoriske standarden også kan inneholde anbefalinger (bør-krav) til ikke-obligatoriske internasjonale standarder. Utredningen inneholder også fraråding av bruk av

[1] https://ehelse.no/normen/faktaark/faktaark-24-kommunikasjon-over-apne-nett

internasjonale standarder (eksempel HPKP RFC7469). Direktoratet mener også at slike frarådinger er viktig del av en offentlig standard og frarådinger om bruk av RFC7469 bør derfor inkluderes i HTTPS standarden.

Bør HTTPS standarden i tillegg anbefales for bruk innen intern kommunikasjon og lukkede tjenester over åpne nett?
Digdir legger opp til at standarden kun skal gjelde for ekstern kommunikasjon. Basert på erfaring fra helsesektoren bør også bruk av HTTPS anbefales for både intern kommunikasjon over åpne nett og lukkede tjenester over åpne nett som mangler annen transportsikring.

Krav til sertifikater
Generelt kunne HTTPS-standarden vært tydeligere på hvilke sikkerhetsegenskaper som ønskes å oppnå ved ta i bruk standarden og hvilke krav til sertifikater dette gir. TLS kan implementeres og legge til rette for tre viktige egenskaper som påvirker sikkerheten og tilliten til en tjeneste:

- Autentisitet – Bruk av offentlige sertifikater (asymmetrisk krypto), som er en forutsetning for effektiv implementasjon av TLS, kan benyttes for å autentisere nettstedet som tilbyr tjenesten.
- Konfidensialitet – En kryptert forbindelse basert på TLS-protokollen sikrer at uvedkommende ikke kan lese innholdet i kommunikasjonen.
- Integritet – Integritetsmekanismer kan legges på for å hindre uautorisert og uoppdaget manipulasjon av datastrømmen.

For å oppnå disse egenskapene er man helt avhengig av kvaliteten på sertifikatene som tas i bruk. Ved bruk av HTTPS er det derfor viktig med sertifikater man stoler på og standarden bør si noe om minimumskrav til sertifikater som tas i bruk for å realisere HTTPS for offentlige nettsteder og nettjenester.

Krav til SSL/TLS sertifikater
Innenfor nettleserbasert kommunikasjon har det vært tradisjon for at bransjen selv regulerer dette gjennom CAB CA/Browser forum. Høyeste tillitsnivå er Extended Validation (EV) som også sikrer en kobling mellom domene og juridisk person og dermed kan benyttes for autentisering av virksomheten som eier domenet. I tillegg regulerer eIDAS tillitstjenester for utstedelse av nettstedssertifikater. Disse kan være kvalifiserte (QWAC) eller ikke-kvalifiserte. eIDAS peker ikke på tekniske standarder som må følges, men QWAC-sertifikater utstedes etter de samme kravene som et SSL/TLS EV-sertifikat. I tillegg må utsteder av QWAC være en Qualified Trust Service Provider (QTSP) og tilfredsstille kravene til QTSP i henhold til ETSI EN 319 403. QWAC-sertifikater er nesten dobbelt så dyre som SSL/TLS EV-sertifikater. Dette er komplisert for den enkelte offentlige aktør å forholde seg til, og ved å innføre HTTPS som en obligatorisk standard bør en derfor også gi råd for valg av nettstedssertifikater.

Krav til sertifikater ved maskin-til-maskin kommunikasjon
Ved kommunikasjon over HTTPS mellom applikasjoner hos ulike virksomheter benyttes HTTPS til autentisering, integritets- og konfidensialitetsbeskyttelse av kommunikasjonen. Utredningen behandler ikke krav til autentisering. For autentisering har normal praksis vært å benytte virksomhetssertifikater (ikke SSL/TLS-sertifikater). Digdir har tidligere regulert krav til slike sertifikater

ved hjelp av egne forskrifter og vist til kravspesifikasjon til PKI i offentlig sektor[2], men i dag peker de på eIDAS for dette. Men det er uklart hvordan man skal benytte eIDAS for virksomhetssertifikater. Dersom HTTPS skal være en obligatorisk standard for slik kommunikasjon bør Digdir komme med krav eller råd om autentisering og krav til sertifikater ved bruk av HTTPS.

[2] https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/