

Krav til Tvungen TLS

Version: 1.4

23. April 2019

**TLP: WHITE**


Ihht. TrafikkLysProtokollen (Bits-TLP-TrafikkLysProtokollen)

Så lenge man følger regler for opphavsrett, kan informasjon merket **TLP: WHITE** distribueres uten restriksjoner.

# Innhold

[1 Innhold 2](#_Toc529799373)

[2 Dokumentinformasjon 3](#_Toc529799374)

[2.1 Dokumenthistorikk 3](#_Toc529799375)

[2.2 Referanser 3](#_Toc529799376)

[2.3 Definisjoner 3](#_Toc529799377)

[2.4 Forkortelse 3](#_Toc529799378)

[2.5 Nyeste versjon 3](#_Toc529799379)

[2.6 Formål 4](#_Toc529799380)

[2.7 Omfang og avgrensning 4](#_Toc529799381)

[3 Bakgrunn 5](#_Toc529799382)

[4 Registrering 6](#_Toc529799383)

[5 Krav 7](#_Toc529799384)

[5.1 Krav til Registrering 7](#_Toc529799385)

[5.2 Krav til oppsett av e-postserver 8](#_Toc529799386)

[5.3 Krav til bruk 8](#_Toc529799387)

[5.4 Publisering av Domeneliste for Tvungen TLS 8](#_Toc529799388)

[5.5 Eksempel - Domeneliste for Tvungen TLS 9](#_Toc529799389)

[6 Vedlegg 1 Samsvarserklæring 10](#_Toc529799390)

[7 Vedlegg 2 11](#_Toc529799391)

[8 Vedlegg 3 - Prosedyre for innmelding og deltakelse i Bits’ felles avtale for tvungen TLS. 12](#_Toc529799392)

# Dokumentinformasjon

## Dokumenthistorikk

|  |  |  |  |
| --- | --- | --- | --- |
| Versjon | Status | Dato | Redigert av |
| 1.0 | Korrekturlest satt til 1.0 | 2017-06-06 | N.Lailey |
| 1.1 | Nye krav 5.2.7 lagt til | 2017-06.08 | N.Lailey |
| 1.2 | Godkjent av Bits administrasjon | 07.12.2017 | N. Lailey |
| 1.3 | Godkjent av Bits administrasjon* Lagt til krav 5.1.6, 5.3.5
* Endret krav 5.2.4, 5.2.7
* Endret skjemaer og eksempler
 | 12.11.2018 | E. Bergersen |
| 1.4 | Godkjent av Bits administrasjonen med følgende endring:* Endret krav 5.3.1
* Publisert engelsk versjon
 | 23.04.2019 | Thomas Døderlein |

## Referanser

|  |  |
| --- | --- |
| Kortnavn | Tittel |
| Brev Datatilsynet | Brev av 24.10.2017 *Veiledning – sending av fødselsnr. mv på e-post* |
| Brev Politiet | Brev fra Politidirektoratet (POD) av 19.04.2016 *Behandling av sensitive personopplysninger – behov for sikker kommunikasjon.* |
| Personopplysningsloven | <https://lovdata.no/dokument/NL/lov/2018-06-15-38>  |

## Definisjoner

|  |  |
| --- | --- |
| **Begrep** | **Forklaring** |
| Avsender | Sluttbruker som sender e-post |
| Deltager | Virksomhet som har tilsluttet seg ordningen spesifisert i dette dokumentet |
| Domeneliste | Liste over domener som er tilsluttet ordningen publisert på bits.no/tls  |
| Mottaker | Sluttbruker som e-post er adressert til |
| Opportunistisk TLS | TLS benyttes for inn- og utgående e-post mot alle aktører som støtter bruk av TLS. For aktører som ikke støtter TLS blir epost sendt ukryptert |
| Organisasjon | Virksomhet eller etat. |
| Samsvarserklæring | Erklæring (punkt 5.7. i dette dokumentet) som sier at organisasjonen ønsker å tilslutte seg ordningen som er beskrevet i dette dokumentet, og dermed godtar forpliktelsene som følger av dette. |
|  TLS | Standard løsning som sørger for at e-post sendes på en sikker og kryptert måte mellom to domener |
| Trusted Root Certificate Authority | Offentlig godkjent rotsertifikat-utsteder. |
| Tvungen TLS |  Dersom systemet er innstilt på tvungen TLS mot domener blir inn/utgående e-post mot disse aktørene kun behandlet dersom TLS er benyttet.  |

## Forkortelse

|  |  |
| --- | --- |
| **Forkortelse** | **Forklaring** |
| TLS | Transport Layer Security |

## Nyeste versjon

Nyeste versjon av dette dokumentet er tilgjengelig her: <https://bits.no/tls>

## Formål

Formålet er å lage en standardisert løsning som en erstatning for bilaterale avtaler der partene basert på en samsvarserklæring (Vedlegg 1 til dette dokumentet) forplikter seg til å innrette sine systemer på en slik måte at brukerne som sender e-post fra en av virksomhetene på listen kun får sendt e-post som benytter TLS til de øvrige virksomhetene på listen.

## Omfang og avgrensning

Løsningen skal ivareta behov for å implementere tvungen TLS mellom forhåndsdefinerte aktører. Bits oppretter en webside der alle aktører som deltar i ordningen er angitt. Medlemmer er selv ansvarlig for å oppdatere sine egne lister på bakgrunn av masterlisten og implementere TLS mot alle aktører på listen.

TLS er en standard krypteringsløsning som sørger for en sikker, kryptert transport av e-post over internett mellom to domener.

TLS utgjør ingen ende til ende (sluttbruker til sluttbruker) kryptering, men ivaretar behov for sikring under transport over internett.

# Bakgrunn

Bakgrunnen er brev fra Politidirektoratet (POD) sendt den 19.04.2016 med tittelen "*Behandling av sensitive personopplysninger – behov for sikker kommunikasjon".* Her går det frem at politiet har behov for å benytte TLS ved kommunikasjon mot aktører der det kan være behov for å utveksle sensitive personopplysninger.

Den 24.10.2016 mottok en rekke virksomheter, deriblant banker, brev fra Datatilsynet med overskriften "*Veiledning – sending av fødselsnummer mv på e-post ".* Her stillesdet også krav til bruk av kryptering dersom personopplysninger (fødselsnummer) sendes på e-post.

Vi ser også at i tillegg til kommunikasjon med politiet, vil blant annet bankenes kommunikasjon med hverandre, Finanstilsynet og UD kunne inneholde personopplysninger.

Dette kan løses ved at bankene hver for seg inngår bilaterale avtaler med alle organisasjoner de har behov for å utveksle sikret e-post med. Imidlertid vil dette raskt innebære et svært stort antall likelydende bilaterale avtaler. Bits foreslår derfor å lage en felles løsning som ivaretar kravene til sikring av e-post som kan inneholde personopplysninger.

Bits har opprettet en webside www.bits.no/tls der organisasjoner som ønsker å delta i ordningen, registrerer seg med domenenavn og opplysninger som fremgår av skjemaet i vedlegg 2 til dette dokumentet.

Alle som registrerer seg forplikter seg til å innrette sine systemer i henhold til kravene i dette dokumentet. Listen på Bits sin webside representerer en masterliste. Påmeldte organisasjoner skal sjekke masterlisten over registrerte virksomheter minimum kvartalsvis, og oppdatere sin egen liste i henhold til denne, slik at alle registrerte organisasjoner skal benytte tvungen TLS mot alle andre organisasjoner på listen maksimalt tre måneder etter registrering.

# Registrering

For å registrere seg i ordningen må IT-ansvarlig sende en epost til tls@bits.no med skjemaene i vedlegg 1 og 2 vedlagt i utfylt stand. Vedlegg 3 til dette dokumentet gir en enkel oppskrift for innmelding.

# Krav

Dette kapittelet inneholder kravene til Bits, aktørene og konfigurasjonen i aktørenes systemer, ordnet tematisk.

## Krav til Registrering

| **#** | **Status** | **Krav** |
| --- | --- | --- |
|  | M | Virksomheten må ha en e-postløsning som støtter Tvungen TLS. |
|  | M | TLS kryptering skal være basert på offentlig godkjent rotsertifikat-utsteder (Trusted Root Certificate Authority) |
|  | M | Ved å registrere seg bekrefter deltager at de forplikter seg til å etterleve kravene som er spesifisert i dette kravdokumentet. |
|  | M | Deltager må registrere seg på [bits.no/tls](https://bits.no/tls) med opplysningene som fremgår av skjemaet i vedlegg 2 til dette dokumentet. |
|  | M | Ved å registrere seg som deltaker tilslutter Organisasjonen seg samsvarserklæringen i vedlegg 1. |
|  | M | Ved å registrere seg som deltaker tillater Organisasjonen at teknisk kontaktopplysninger kan deles med andre deltakere i ordninger for Tvungen TLS. |

## Krav til oppsett av e-postserver

| **#** | **Status** | **Krav** |
| --- | --- | --- |
|  | M | Ved oppføring på *Domenelisten for Tvungen TLS* er det et krav at deltaker allerede har konfigurert sin e-postserver til å kommunisere med opportunistisk TLS.  |
|  | M | Deltager skal umiddelbart konfigurere sin e-postserver slik at e-poster til domener hos organisasjon som er oppført på *Domeneliste for Tvungen TLS*, alltid blir sendt med tvungen TLS.  |
|  | M | E-postserveren skal konfigureres på en slik måte at sluttbruker som er avsender ikke kan velge å sende e-post uten tvungen TLS. |
|  | C | E-postserveren skal konfigureres slik at innkommende e-post uten TLS fra en organisasjon på *Domeneliste for Tvungen TLS*, blir umiddelbart avvist.**Notat:** Få systemer har i dag støtte for dette kravet. Derfor gjelder kravet kun for de som har mulighet til å konfigurere dette. |
|  | M | E-postserveren skal konfigureres slik at sluttbruker får feilmelding dersom utgående epost blir avvist av mottaker. |
|  | M | Endringsrutiner for e-postserver skal inneholde et punkt med test av at konfigurering av Domeneliste for Tvungen TLS er opprettholdt etter endringer i eller bytte av server  |
|  | M | Epostserver skal minimum støtte TLS Versjon 1.2**Notat:** E-postserveren kan støtte eldre versjoner av TLS, men skal alltid prioritere TLS versjon 1.2. Ved at alle prioriterer versjon 1.2 er man sikret at denne versjonen for alle deltakerne i ordningen for Tvungen TLS. |
|  | M | Epostserver skal validere mottakers sertifikat. Hostname skal valideres mot sertifikatatets common name. |

## Krav til bruk

| **#** | **Status** | **Krav** |
| --- | --- | --- |
|  | M | Deltager skal minimum kvartalsvis oppdatere listen over domener de benytter tvungen TLS til, slik at den er i samsvar med domenelisten.  |
|  | M | Det skal opprettes en generisk epostadresse til en administrator for ordningen, som kan varsles ved behov. |
|  | M | Ved endringer i kontaktinformasjon til administrator skal varsel sendes til tls@bits.no  |
|  | O | Sluttbrukere som er avsender av epost kan benytte leverings – og lesebekreftelse slik at de raskt blir klar over e-poster som ikke blir mottatt. |
|  | O | Deltaker kan forespørre Bits om en liste over domene med tekniske kontaktpersoner. |

## Publisering av Domeneliste for Tvungen TLS

| **#** | **Status** | **Krav** |
| --- | --- | --- |
|  | M | Domeneliste for Tvungen TLS skal publiseres på [www.bits.no/tls](http://www.bits.no/tls). |

## Eksempel - Domeneliste for Tvungen TLS

Listen vil bli laget på dette formatet og publisert på [www.bits.no/tls](http://www.bits.no/tls) .

| **Selskapsnavn**  | **Organisasjonsnummer** | **Domene med tvungen TLS** | **Dato innmeldt** | **Støtte for krav 5.2.4** |
| --- | --- | --- | --- | --- |
| Bits AS | 916960190 | bits.no | 2017-02-01 | Nei |
| Finans Norge |  | fno.no | 2017-02-01 | Ja |
|  |  |  |  |  |

# Vedlegg 1 Samsvarserklæring

Samsvarserklæringen signeres av IT-ansvarlig i organisasjonen

Organisasjonen \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, med organisasjonsnummer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

vil for domene \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ kun motta e-post sikret

med TLS fra selskaper oppført i Domeneliste for Tvungen TLS.

Kontaktperson for organisasjonen ved oppdatering av Domeneliste for Tvungen TLS er

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ med e-postadresse \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Jeg forplikter organisasjonen til kun å sende TLS-sikret e-post til domener oppført i Domeneliste for Tvungen TLS i samsvar med kravene i dette dokumentet. Jeg godtar at tekniske kontaktpersoner kan deles med andre deltakere i ordningen for Tvungen TLS.

Dato, \_\_ \_\_ / \_\_ \_\_ - \_\_ \_\_ \_\_ \_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn Signatur

# Vedlegg 2

Opplysninger om virksomheten. Vedlegges samsvarserklæring og sendes til:

|  |  |
| --- | --- |
| **Org.nr** |  |
| **Administrator navn** |  |
| **Administrator e-post** |  |
| **Teknisk kontakt e-post** |  |
| **Teknisk kontakt telefon** |  |
| **Dato for innmelding** |  |
| **Domene(r) for tvungen TLS** |  |
| **Støtte for krav 5.2.4** |  |

# Vedlegg 3 - Prosedyre for innmelding og deltakelse i Bits’ felles avtale for tvungen TLS.

Dette dokumentet inneholder en forenklet «oppskrift» for innmelding og deltakelse i ordningen, og er et vedlegg til dokumentet *Krav til tvungen TLS*. For fullstendig beskrivelse av kravene se *Krav til tvungen TLS.* Virksomheten er ansvarlig for å påse at alle kravene i dokumentet *Krav til Tvungen TLS* er oppfylt.

**Før innmelding**

1. Kontroller at din virksomhet har et epostsystem som støtter styring av TLS (Tvungen/obligatorisk og Opportunistisk) på domenenivå.
2. Gå inn på [www.bits.no/tls](http://www.bits.no/tls). Her finner du *Domeneliste* for deltakere i ordningen.
3. Konfigurer egen epostserver slik at dere senter epost med tvungen/obligatorisk TLS til alle domenene på *Domenelisten.*
4. Konfigurer egen epostserver slik at opportunistisk TLS benyttes ved *mottak* av epost.

**Ved innmelding**

1. Når skritt 1-4 er gjennomført, send skjemaet i vedlegg 1 til tls@bits.no ,
2. Motta tilbakemelding om at din virksomhets domene(r) er lagt til listen.
3. Sørg for å innføre prosedyre i eget driftsmiljø slik at domenelisten blir kontrollert minimum kvartalsvis, og epostserver konfigurert i henhold til denne. Oppdater øvrig dokumentasjon og rutinebeskrivelser i henhold til *Krav til tvungen TLS*

**Tre måneder etter innmelding**

1. Kontroller *Domenelisten* på [www.bits.no/tls](http://www.bits.no/tls) og konfigurer egen domeneliste i henhold til denne
2. Konfigurer også innkommende epost til tvungen TLS for alle domener på domenelisten.

**Minimum en gang hvert kvartal**

1. Kontroller *Domenelisten* på [www.bits.no/tls](http://www.bits.no/tls) og se til at egen epostserver er konfigurert slik at din virksomhet benytter tvungen TLS ved utveksling av epost til alle domener på listen.

**Ved feilmelding**

Ved feil som oppstår der epost til deltakere i ordningen feiler grunnet at mottaker ikke kan motta epost med tvungen TLS. Kontakt tls@bits.no