

Requirements for forced TLS scheme

Version: 1.4

23rd of April 2019

**TLP: WHITE**


Acc. To the Norwegian defined Traffic-Light-Protocol (Bits-TLP Traffic-Light-Protocol)

As long as copyright is respected, information marked **TLP: WHITE** may be distributed without restrictions.

# Content

[1 Content 2](#_Toc6916839)

[2 Document information 3](#_Toc6916840)

[2.1 Document history 3](#_Toc6916841)

[2.2 References 3](#_Toc6916842)

[2.3 Definitions 3](#_Toc6916843)

[2.4 Abbreviation 3](#_Toc6916844)

[2.5 Latest version 4](#_Toc6916845)

[2.6 Purpose 5](#_Toc6916846)

[2.7 Scope and delimitation 5](#_Toc6916847)

[3 Background 6](#_Toc6916848)

[4 Registration 6](#_Toc6916849)

[5 Requirements 7](#_Toc6916850)

[5.1 Requirements for Registration 7](#_Toc6916851)

[5.2 E-mail server setup requirements 7](#_Toc6916852)

[5.3 Requirements for use 8](#_Toc6916853)

[5.4 Publishing of the Domain List for Forced TLS 8](#_Toc6916854)

[5.5 Example - Forced TLS Domain List 8](#_Toc6916855)

[6 Appendix 1 Declaration of conformity 9](#_Toc6916856)

[7 Appendix 2 10](#_Toc6916857)

[8 Appendix 3 - Procedure for registration and participation in Bits' joint agreement for forced TLS. 11](#_Toc6916858)

# Document information

## Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Status | Dato | Redigert av |
| 1.0 | Proofreading set to 1.0 | 2017-06-06 | N.Lailey |
| 1.1 | New requirements 5.2.7 added | 2017-06.08 | N.Lailey |
| 1.2 | Approved by Bits administration | 07.12.2017 | N. Lailey |
| 1.3 | Approved by Bit's administration* Added requirements 5.1.6, 5.3.5
* Amended requirements 5.2.4, 5.2.7
* Modified forms and examples
 | 12.11.2018 | E. Bergersen |
| 1.4 | Approved by Bits administration with the following change:* Changed requirement 5.3.1
* Published English version
 | 23.04.2019 | Thomas Døderlein |
|  |  |  |  |
|  |  |  |  |

## References

|  |  |
| --- | --- |
| Short | Description |
| Letter from the Norwegian Data Protection Authority | Letter of the 24th of October 2017 Guidance - sending of social security no. etc. by e-mail |
| Letter from the police | Letter from the Police Directorate (POD) of 19.04.2016 “Treatment of sensitive personal information - need for secure communication”. |
| The Personal Data Act | <https://lovdata.no/dokument/NL/lov/2018-06-15-38>  |

## Definitions

|  |  |
| --- | --- |
| **Term** | **Description** |
| Sender | End user sending email |
| Participant | Business that has joined the scheme specified in this document |
| Domain List | List of domains that are connected to the scheme published on bits.no/tls |
| Recipient | End user to whom email is addressed |
| Opportunistic TLS | TLS is used for incoming and outgoing e-mail against all actors who support the use of TLS. For operators who do not support TLS, email is sent unencrypte |
| Organization | Business or agency. |
| Declaration of compliance | Statement (section 5.7 of this document) that states that the organization wishes to adhere to the scheme described in this document and thereby accepts the obligations arising therefrom. |
|  TLS | Standard solution that ensures that emails are sent in a secure and encrypted manner between two domains |
| Trusted Root Certificate Authority | Publicly approved root certificate issuer. |
| Forced TLS |  If the system is set to forced TLS against domains, in / outgoing e-mail against these operators is only processed if TLS is used. |

## Abbreviation

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| TLS | Transport Layer Security |

## Latest version

The latest version of this document is available here: https://bits.no/tls

## Purpose

The purpose is to create a standardized solution as a substitute for bilateral agreements where the parties, based on a Declaration of Conformity (Appendix 1 to this document), undertake to align their systems in such a way that users sending e-mail from one of the companies on the list will send e-mails that use TLS to the other businesses on the list..

## Scope and delimitation

The solution must meet the need to implement forced TLS between predefined actors. Bits creates a web page where all participating actors in the scheme are specified. Members are responsible for updating their own lists based on the master list and implementing TLS against all actors in the list.

TLS is a standard encryption solution that ensures a secure, encrypted transport of e-mail over the Internet between two domains.

TLS is no end to end (end-user to end-user) encryption but safeguards the need for security during transport over the internet.

# Background

The background is a letter from the Norwegian Police Directorate (POD) sent on 19.04.2016 entitled "Treatment of sensitive personal information - need for secure communication". Here it is stated that the police need to use TLS when communicating with actors where there may be a need to exchange sensitive personal information.

On October 24, 2016, several companies, including banks, received letters from the Norwegian Data Protection Authority, entitled "Guidance - sending a national ID number, etc. by e-mail". Here, there are also requirements for the use of encryption if personal information (national identity number) is sent by e-mail.

We also anticipate that in addition to communication with the police, the banks' communication with each other, the Financial Supervisory Authority and the Ministry of Foreign Affairs, may include personal information.

This can be solved by the banks individually entering into bilateral agreements with all the organizations they need to exchange secured e-mail with. However, this will quickly involve a very large number of identical bilateral agreements. Bits therefore proposes to create a common solution that meets the requirements for securing e-mail that may contain personal information.

Bits has created a website www.bits.no/tls where organizations that wish to participate in the scheme register with domain names and information that appears in the form in appendix 2 to this document.

Anyone registering undertakes to arrange their systems in accordance with the requirements of this document. The list on Bits’ website represents a master list. Registered organizations should check the master list of registered businesses at least quarterly and update their own listing accordingly, so that all registered organizations will use forced TLS against all other organizations on the list for a maximum of three months after registration.

# Registration

In order to register in the scheme, the IT manager must send an e-mail to tls@bits.no with the forms in appendices 1 and 2 enclosed in the completed condition. Appendix 3 to this document provides a simple recipe for enrolment.

# Requirements

This chapter contains the requirements from Bits, the actors and the configuration of the participants systems, arranged thematically

## Requirements for Registration

| **#** | **Status** | **Krav** |
| --- | --- | --- |
|  | M | The business must have an e-mail solution that supports Forced TLS. |
|  | M | TLS Encryption must be based on Trusted Root Certificate Authority |
|  | M | By registering, the participant confirms that they undertake to comply with the requirements specified in this requirement document. |
|  | M | Participant must register on bits.no/tls with the information that appears in the form in appendix 2 to this document. |
|  | M | By registering as a participant, the Organization subscribes to the Declaration of Conformity in Appendix 1. |
|  | M | By registering as a participant, the Organization allows technical contact information to be shared with other participants in Forced TLS Schemes. |

## E-mail server setup requirements

| **#** | **Status** | **Requirements** |
| --- | --- | --- |
|  | M | Upon listing on the Forced TLS Domain List, it is a requirement that the participant has already configured their e-mail server to communicate with opportunistic TLS. |
|  | M | Attendees should immediately configure their e-mail server so that e-mail for organizations domains listed on the Forced TLS Domain List is always sent with forced TLS. |
|  | M | The e-mail server must be configured in such a way that the end user who is the sender, cannot choose to send e-mail without forced TLS. |
|  | C | The e-mail server must be configured so that incoming e-mail without TLS from an organization on the Domain List for the Forced TLS, are immediately rejected.**Note**: Few systems currently support this requirement. Therefore, the requirement applies only to those who have the ability to configure this. |
|  | M | The e-mail server must be configured so that the end user receives an error message if the outgoing e-mail is rejected by the recipient. |
|  | M | The E-mail server change routines should include a point of testing that enforced TLS domain list configuration is maintained, after server changes or server switch |
|  | M | The e-mail server must at least support TLS Version 1.2Note: The e-mail server can support older versions of TLS but should always prioritize TLS version 1.2. By prioritizing version 1.2, it is ensured that this version for all participants in the forced TLS scheme. |
|  | M | E-mail server must validate recipient's certificate. Hostname must be validated against the certificate name's common name. |
|  |  |  |

## Requirements for use

| **#** | **Status** | **Requirements** |
| --- | --- | --- |
|  | M | Participants must minimum update the list of domains quarterly for all forced TLS participants. |
|  | M | A generic e-mail address must be created for an administrator of the scheme, which can be notified as needed. |
|  | M | In case of changes to the contact information of the administrator, notification should be sent to tls@bits.no |
|  | O | End users who are e-mails senders can use delivery and read confirmation so that they can quickly become aware of e-mails that are not received. |
|  | O | Participant can request Bits for a list of domains with technical contact information. |

## Publishing of the Domain List for Forced TLS

| **#** | **Status** | **Requirements** |
| --- | --- | --- |
|  | M | Domain list for Forced TLS must be published at www.bits.no/tls |

## Example - Forced TLS Domain List

The list will be made in this format and published on www.bits.no/tls .

| **Company name**  | **Company Identification number** | **Domain with forced TLS** | **Date of enrolment** | **Requirement 5.2.4 supported?** |
| --- | --- | --- | --- | --- |
| Bits AS | 916960190 | bits.no | 2017-02-01 | Nei (translated=No) |
| Finans Norge |  | fno.no | 2017-02-01 | Ja (translated= Yes) |
|  |  |  |  |  |

DO NOT use the English term for yes/ no. The Norwegian term Ja / Nei is to be used

# Appendix 1 Declaration of conformity

#

The Declaration of Conformity is to be signed by the IT manager in the organization

Organization \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, with company ID number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will for the domain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ only receive TLS secured e-mails

with TLS from Companies listed in the Forced TLS Domain List.

Contact person for the organization when updating Domain List for Forced TLS is

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ with e-mail address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

I oblige the organization to only send TLS secured e-mail to the domains listed in the Forced TLS Domain List in accordance with the requirements of this document. I agree that technical contacts may be shared with other participants in the forced TLS scheme.

Date, \_\_ \_\_ / \_\_ \_\_ - \_\_ \_\_ \_\_ \_\_

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

Name Signature

# Appendix 2

Information about the business. Attached to the Declaration of Conformity and sent to:

|  |  |
| --- | --- |
| **Org.no.** |  |
| **Name of administrator** |  |
| **Administrator e-mail** |  |
| **Technical contact e-mail** |  |
| **Technical contact telephone number** |  |
| **Date of enrolment** |  |
| **Forced TLS Domain(s)**  |  |
| **Requirement 5.2.4 support** |  |

# Appendix 3 - Procedure for registration and participation in Bits' joint agreement for forced TLS.

This document contains a simplified "recipe" for enrollment and participation in the scheme and is an attachment to the Required TLS Requirements. For a complete description of the requirements, see Required TLS Requirements. The business is responsible for ensuring that all the requirements of the document Required TLS are met.

**Before enrolment**

1. Make sure your business has an e-mail system that supports TLS management (forced / mandatory and Opportunistic) at domain level.
2. Go to www.bits.no/tls. Here you will find Domain List for participants in the scheme.
3. Configure your own e-mail server so you can e-mail with forced / mandatory TLS to all domains on the Domain List.
4. Configure your own e-mail server so that opportunistic TLS is used when receiving e-mail.

**Upon registration**

1. Once steps 1-4 have been completed, send the form in appendix 1 to tls@bits.no,
2. Receive feedback that your business domain (s) have been added to the list.
3. Be sure to introduce procedure in your own operating environment so that the domain list is checked at least quarterly, and e-mail server configured accordingly. Update other documentation and routine descriptions according to Required TLS Requirements

**Three months after registration**

1. Check the Domain List at www.bits.no/tls and configure your own domain list according to this
2. Also configure incoming e-mail for forced TLS for all domains on the domain list.

**Minimum once every quarter**

1. Check the Domain List at www.bits.no/tls and make sure your own e-mail server is configured so that your business uses forced TLS when exchanging e-mail to all domains on the list.

**In case of error message**

For errors that occur where e-mail to participants in the scheme fails due to the recipient being unable to receive e-mail with forced TLS. Contact tls@bits.no