Date **2016-07-07**
Author **Finansinspektionen, IT**
Version **1.0**

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Secure Email Communication - TLS encryption

Introduction

Transport Layer Security (TLS) allows encrypted SMTP conversations over the Internet. SMTP servers and clients normally communicate in clear text over the Internet, but with TLS the communication is encrypted between two SMTP servers.

Finansinspektionen and TLS

Finansinspektionen encourage a wider use of TLS encryption. The external mail gateways at Finansinspektionen are configured to offer TLS for all sending servers by default. This means that any party can use TLS towards Finansinspektionen at any time without any configuration on the Finans-inspektionen side.

For a more controlled and reliable TLS communication Finansinspektionen recommend to setup enforce TLS. Enforce TLS will encrypt the mail and only deliver if all settings are correct and the CA-signed certificate is fully validated. This setting require specific configuration and verification on both sides.

If enforce TLS is not configured the mail gateway will try to send encrypted but the mail might go through unencrypted if something is not fully correct.

To set up enforce TLS with Finansinspektionen the following external mail gateways (MX records) should be used:

FQDN	IP address	Certificate details
post.fi.se	193.15.242.199	CN=post.fi.se
post1.fi.se	193.15.242.200	CN=post1.fi.se

All server certificates are signed by DigiCert CA.

Requirements for enforced TLS

All the following requirements must be fulfilled to use enforced TLS between Finansinspektionen and your organization:

- All Secure Email communication with the Finansinspektionen must be done through enforced and verified TLS.
- The ciphers used for the TLS session must be chosen from the list of approved algorithms supplied below.
- The Certificate Authority (CA) used to sign the TLS certificate must be from the list of approved CA's below.
- If a TLS encrypted channel cannot be established, the sender must be notified with a non-delivery report (NDR) according to RFC2821.

Minimal requirement for ciphers:

```
AES128-SHA
```

Recommended minimal level/strength for ciphers:

```
AES256-SHA256
```

The following ciphers must not be used due to their weak nature

```
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
```

Approved CA´s:
A list of approved CA's can be found here:

http://mxr.mozilla.org/mozilla/source/security/nss/lib/ckfw/builtins/certdata.txt

Recommended Configuration Procedure

Since several steps are performed prior to establishing an enforced TLS session (see section below, "Technical Overview") it is imperative that the certain types of operational changes are performed in a controlled way.

Ensure that all verification steps passes before:

1. Changing MX resource records.
2. Changing content of the Common Name (CN) field in the certificate.
3. Not replacing an expired certificate in due time.

Technical Overview

Due to the SMTP protocol and the implementation of SMTP TLS, encryption can only be enforced on outgoing mail; hence it is vital that both ends follow the same "protocol":

If mail to an encryption-enforced domain is to be delivered and encryption cannot be established, (due to lack of support for TLS, expired certificate etc.)

mail must be held in queue at the sending side until a SMTP TLS connection can be established, if this is done on all sending parties, all mail will be sent encrypted.

Delivery of email to a domain where mail is protected with enforced TLS depends on several different key elements.

First a DNS MX lookup is performed by the sending Mail Transport Agent (MTA), the DNS system returns a list of Mail Exchanger resource records that are willing to accept and deliver mail for the domain in question.

Before delivering mail, several operations are performed when enforced TLS is enabled:

1. The signing Certificate Authority (CA) is verified against a local list of trusted issuers.
2. Certificate must be valid, e.g. the "Not After" date must not have been reached.
3. The fully qualified domain name (FQDN) of the Mail Exchanger resource records must match the Common Name (CN) field in the certificate.

Nota Bene

If any of the above tests fails, the mail **MUST** not be delivered and instead be kept in the mail queue until either the all of the above tests passes or a will wait in the mail queue for a site dependent number (usually 5 to 7) of days, and after expiration of this time in the mail queue, a Non Delivery Report (NDR) must be sent to original sender.

Questionnaire

To setup enforce TLS with Finansinspektionen the following questions should be answered and returned via e-mail to admin@fi.se.

1. Company Information

Company name	
Organization number	
Street address	
Postcode	
Country	

2. Administrative Contact Information

Name	
E-mail	
Title/role	
Telephone number	
Department	

3. Technical Contact Information

Name	
E-mail	
Title/role	
Telephone number	
Department	

4. Domains[1]:

5. Date and time for implementation[2]:

6. CA used for the TLS certificate[3]:

7. Certificate details[4]:

[1] *Please provide a list with all domains Finansinspektionen should establish enforced TLS with*
[2] *Date and time when Finansinspektionen should implement enforce TLS*
[3] *Name of the Certificate Authority issuing the TLS certificate*
[4] *yourhost.domain.cc., IP: 1.2.3.4 CN=yourhost.domain.cc Valid until YY:MM:DD*