**The following steps are necessary to set up TLS encrypted email communication:**

1. **Buy a certificate** (should be possible for min 25 € per year).
   The required steps to generate a private and public key for your email gateway will be described in detail by the certificate vendors, e.g. www.geotrust.com "Install SSL Certificate".
   **Example certificate Authorities:**
   Deutsche Telekom AG http://www.telesec.de
   Entrust.net http://www.entrust.net
   Equifax http://www.geotrust.com
   GTE CyberTrust http://www.verizonbusiness.com
   GlobalSign http://www.globalsign.com
   TC TrustCenter http://www.trustcenter.de
   Thawte http://www.thawte.com
   VeriSign http://www.verisign.com

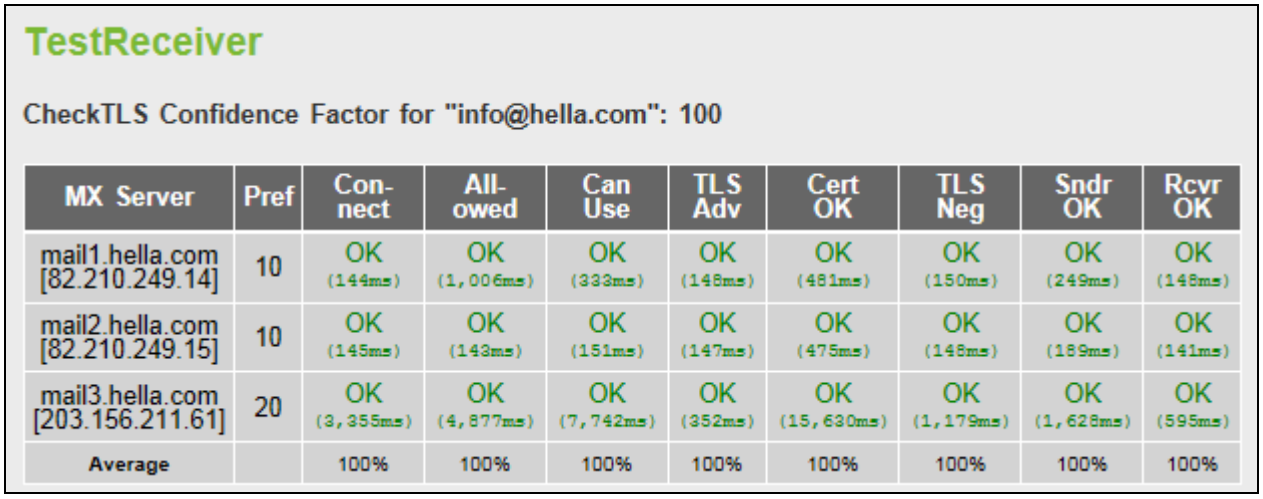
2. **Import the purchased certificate to your mail server or mail gateway**
   as described in detail by your chosen certificate vendor, e.g. www.geotrust.com "Install SSL Certificate".

3. **Change settings at your email gateway** (if you don't run an own email gateway, your provider has to do it) for incoming and outgoing emails for the domain hella.com:
   - Outgoing emails:
     - Target domain: hella.com
     - TLS mode: Required – Verify (or "mandatory TLS")
   - Incoming emails:
     - For source / origin domain: hella.com
     - TLS mode: Required – Verify (or "mandatory TLS")

4. Inform Hella that emails that you are now ready to send and receive emails using mandatory TLS. For this, please fill the request document at www.hella.com/securemail and send it to securemail@hella.com)

**Testing whether your email server is able to receive emails in TLS mode:**

On the website www.checktls.com you can check whether your mail gateway accepts to receive TLS encrypted e-mails. To start testing, enter your email address.
If TLS is accepted, you will see it in the response protocol ("TLS Adv", "TLS Neg", see screenshot below):



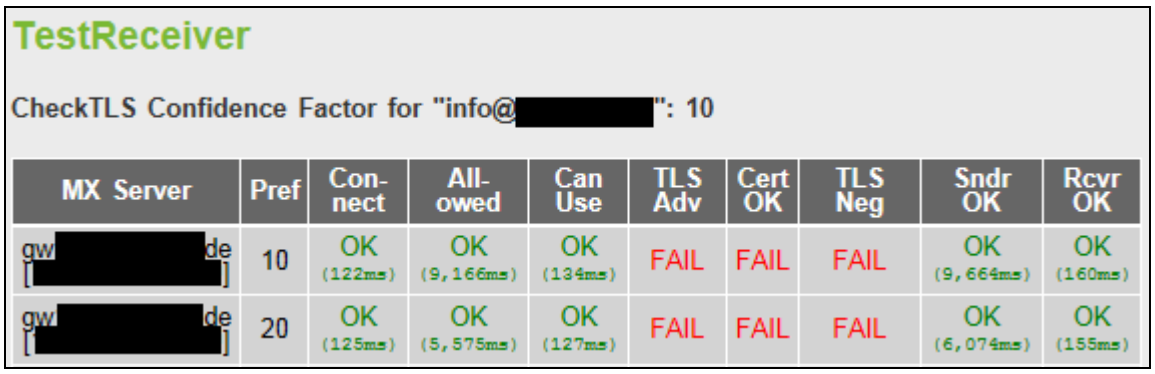
TestReceiver

CheckTLS Confidence Factor for "info@hella.com": 100

| MX Server | Pref | Con-nect | All-owed | Can Use | TLS Adv | Cert OK | TLS Neg | Sndr OK | Rcvr OK |
|---|---|---|---|---|---|---|---|---|---|
| mail1.hella.com [82.210.249.14] | 10 | OK (144ms) | OK (1,006ms) | OK (333ms) | OK (148ms) | OK (481ms) | OK (150ms) | OK (249ms) | OK (148ms) |
| mail2.hella.com [82.210.249.15] | 10 | OK (145ms) | OK (143ms) | OK (151ms) | OK (147ms) | OK (475ms) | OK (148ms) | OK (189ms) | OK (141ms) |
| mail3.hella.com [203.156.211.61] | 20 | OK (3,355ms) | OK (4,877ms) | OK (7,742ms) | OK (352ms) | OK (15,630ms) | OK (1,179ms) | OK (1,628ms) | OK (595ms) |
| Average | | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |

In case your mail gateway already accepts TLS-encrypted communication, you only need to do step 3 and 4.

If your domain does not support receiving TLS encrypted email, it will look like the following:



TestReceiver

CheckTLS Confidence Factor for "info@[redacted]": 10

| MX Server | Pref | Con-nect | All-owed | Can Use | TLS Adv | Cert OK | TLS Neg | Sndr OK | Rcvr OK |
|---|---|---|---|---|---|---|---|---|---|
| gw[redacted]de [redacted] | 10 | OK (122ms) | OK (9,166ms) | OK (134ms) | FAIL | FAIL | FAIL | OK (9,664ms) | OK (160ms) |
| gw[redacted]de [redacted] | 20 | OK (125ms) | OK (5,575ms) | OK (127ms) | FAIL | FAIL | FAIL | OK (6,074ms) | OK (155ms) |