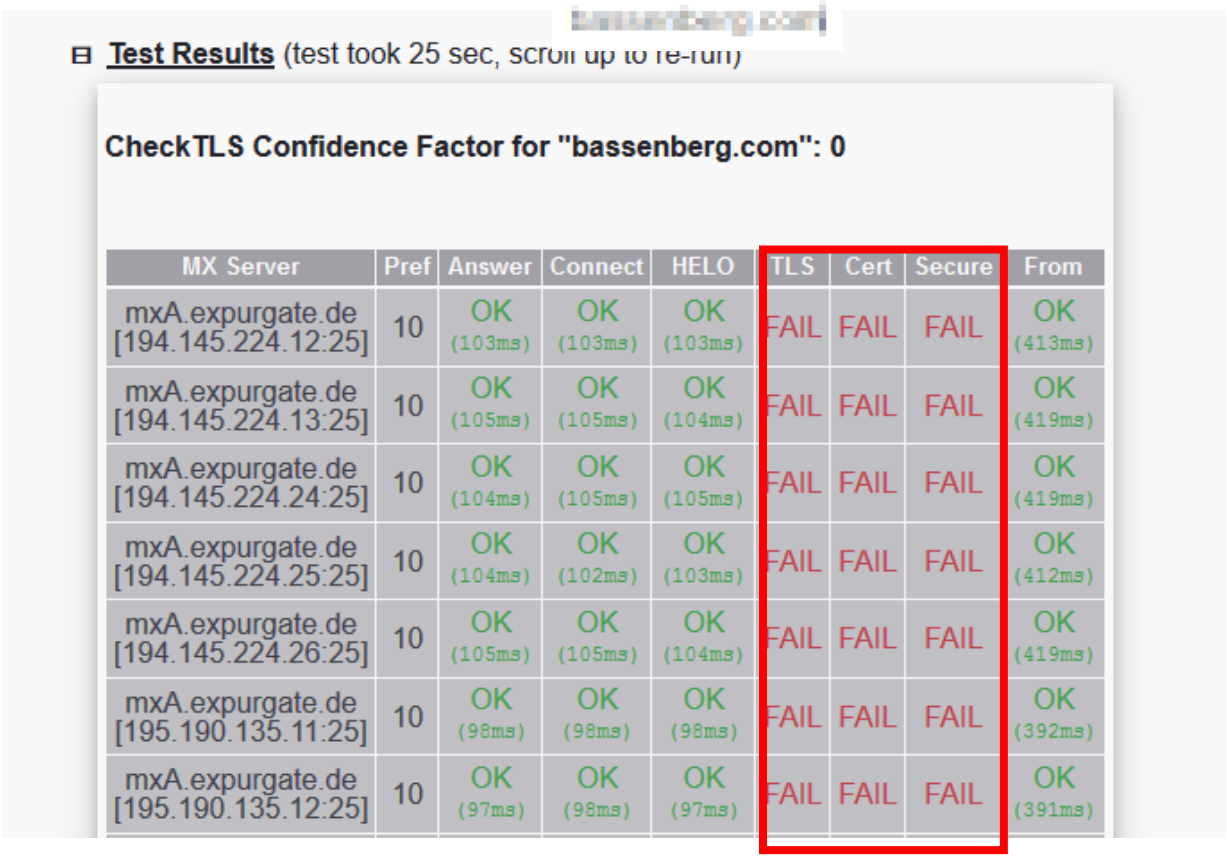
Detailinformationen zu den Ergebnissen von CheckTLS

Nach Durchführung der TLS-Überprüfung über https://www.checktls.com/TestReceiver haben Sie ein Ergebnis erhalten, das üblicherweise positiv sein sollte. Sofern Sie jedoch eine der drei auf der Infoseite von IT.Niedersachsen dargestellten negativen Ergebnisse erhalten haben, zeigen wir Ihnen auf den folgenden Seiten detaillierte Erläuterungen zu den Ergebnissen:

Ergebnis 1: Kein TLS

Die folgende Tabelle zeigt den Status der Überprüfung. Ist eine der Spalten rot, so findet die Übertragung unverschlüsselt statt.



⊟ **Test Results** (test took 25 sec, scroll up to re-run)

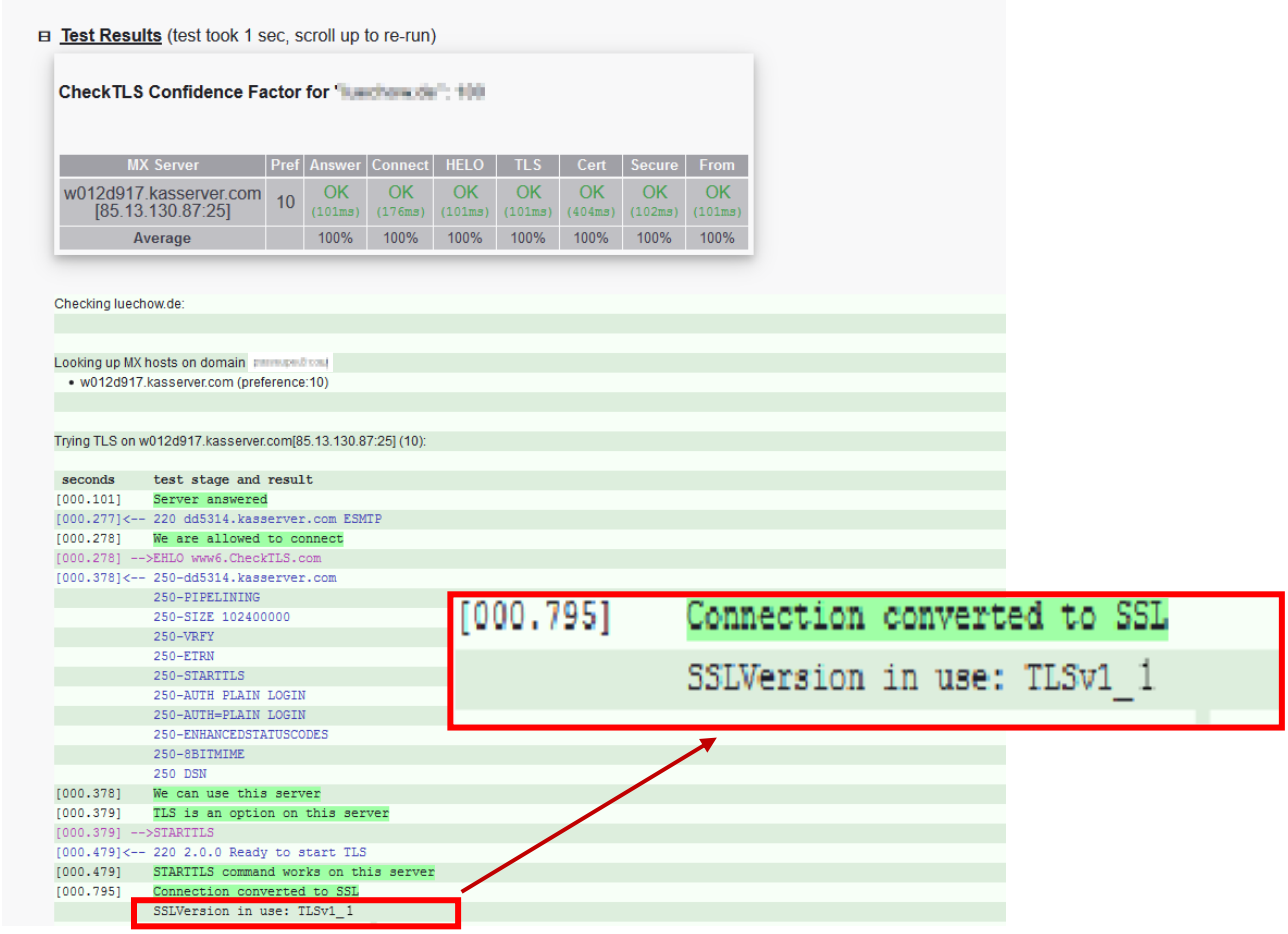
CheckTLS Confidence Factor for "bassenberg.com": 0

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
mxA.expurgate.de [194.145.224.12:25]	10	OK (103ms)	OK (103ms)	OK (103ms)	FAIL	FAIL	FAIL	OK (413ms)
mxA.expurgate.de [194.145.224.13:25]	10	OK (105ms)	OK (105ms)	OK (104ms)	FAIL	FAIL	FAIL	OK (419ms)
mxA.expurgate.de [194.145.224.24:25]	10	OK (104ms)	OK (105ms)	OK (105ms)	FAIL	FAIL	FAIL	OK (419ms)
mxA.expurgate.de [194.145.224.25:25]	10	OK (104ms)	OK (102ms)	OK (103ms)	FAIL	FAIL	FAIL	OK (412ms)
mxA.expurgate.de [194.145.224.26:25]	10	OK (105ms)	OK (105ms)	OK (104ms)	FAIL	FAIL	FAIL	OK (419ms)
mxA.expurgate.de [195.190.135.11:25]	10	OK (98ms)	OK (98ms)	OK (98ms)	FAIL	FAIL	FAIL	OK (392ms)
mxA.expurgate.de [195.190.135.12:25]	10	OK (97ms)	OK (98ms)	OK (97ms)	FAIL	FAIL	FAIL	OK (391ms)

Die Mailserver der Landesverwaltung verwenden nur TLS 1.2 oder übermitteln die E-Mails unverschlüsselt. TLS 1.0 und 1.1 werden aus Sicherheitsgründen nicht verwendet.

Ergebnis 2: Nur TLS Version 1.1 oder schwächer

Die folgenden Bilder zeigen eine korrekte Verschlüsselung an, allerdings wird eine veraltete TLS-Version verwendet.



Test Results (test took 1 sec, scroll up to re-run)

CheckTLS Confidence Factor for '[redacted]': 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
w012d917.kasserver.com [85.13.130.87:25]	10	OK (101ms)	OK (176ms)	OK (101ms)	OK (101ms)	OK (404ms)	OK (102ms)	OK (101ms)
Average		100%	100%	100%	100%	100%	100%	100%

```
Checking luechow.de:

Looking up MX hosts on domain [redacted]
  • w012d917.kasserver.com (preference:10)

Trying TLS on w012d917.kasserver.com[85.13.130.87:25] (10):

 seconds      test stage and result
[000.101]     Server answered
[000.277]<-- 220 dd5314.kasserver.com ESMTP
[000.278]     We are allowed to connect
[000.278] -->EHLO www6.CheckTLS.com
[000.378]<-- 250-dd5314.kasserver.com
             250-PIPELINING
             250-SIZE 102400000
             250-VRFY
             250-ETRN
             250-STARTTLS
             250-AUTH PLAIN LOGIN
             250-AUTH=PLAIN LOGIN
             250-ENHANCEDSTATUSCODES
             250-8BITMIME
             250 DSN
[000.378]     We can use this server
[000.379]     TLS is an option on this server
[000.379] -->STARTTLS
[000.479]<-- 220 2.0.0 Ready to start TLS
[000.479]     STARTTLS command works on this server
[000.795]     Connection converted to SSL
              SSLVersion in use: TLSv1_1
```

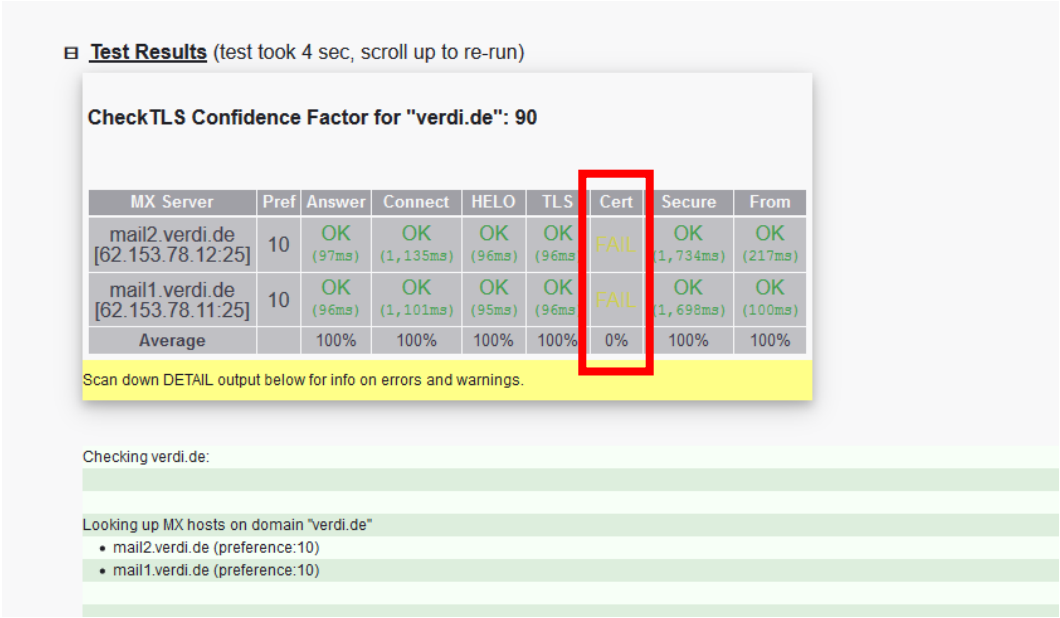

Ergebnis 3: Nicht gültiges Zertifikat

Um TLS zu verwenden, überprüft der sendende Mailserver das Zertifikat des empfangenden Mailservers. Eine zertifikatsbasierte Verschlüsselung wird nur dann aktiviert, wenn das Zertifikat des empfangenden Servers gültig ist.

Ein Zertifikat ist **nicht gültig**, wenn:

- es abgelaufen ist.
- einen ungültigen Vertrauenspfad (z.B. unvollständig, ungültige Zertifikate enthalten) hat.

Ein Zertifikat kann zudem **gesperrt** worden sein („revoked“).
Ein Zertifikat ist **nicht valide** (resp. nicht validierbar), wenn es selbst erstellt und signiert worden ist („self signed“).



Test Results (test took 4 sec, scroll up to re-run)

CheckTLS Confidence Factor for "verdi.de": 90

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
mail2.verdi.de [62.153.78.12:25]	10	OK (97ms)	OK (1,135ms)	OK (96ms)	OK (96ms	FAIL	OK (1,734ms)	OK (217ms)
mail1.verdi.de [62.153.78.11:25]	10	OK (96ms)	OK (1,101ms)	OK (95ms)	OK (96ms	FAIL	OK (1,698ms)	OK (100ms)
Average		100%	100%	100%	100%	0%	100%	100%

Scan down DETAIL output below for info on errors and warnings.

Checking verdi.de:

Looking up MX hosts on domain "verdi.de"

- mail2.verdi.de (preference:10)
- mail1.verdi.de (preference:10)

Das folgende Bild zeigt die beispielhafte Ausgabe für ein selbst erstelltes Zertifikat. Es ist für den Absender nicht vertrauenswürdig.

```
seconds     test stage and result
[000.096]   Server answered
[001.230]<-- 220 verdi.de ESMTP mail service Fri, 25 Oct 2019 11:28:43 +0200
[001.231]   We are allowed to connect
[001.231] -->EHLO www6.CheckTLS.com
[001.326]<-- 250-mail1.verdi.de Hello www6.checktls.com [159.89.187.50], pleased to meet you
             250-ENHANCEDSTATUSCODES
             250-PIPELINING
             250-EXPN
             250-VERB
             250-8BITMIME
             250-SIZE 14336000
             250-DSN
             250-ETRN
             250-STARTTLS
             250-DELIVERBY
             250 HELP
[001.326]   We can use this server
[001.327]   TLS is an option on this server
[001.327] -->STARTTLS
[001.421]<-- 220 2.0.0 Ready to start TLS
[001.422]   STARTTLS command works on this server
[001.628]
             SSLVersion in use: TLSv1_2
             Cipher in use: ECDHE-RSA-AES256-GCM-SHA384
             Certificate 1 of 2 in chain: Cert VALIDATION ERROR(S): self signed certificate in certificate chain
             So email is encrypted but the recipient domain is not verified
             Cert Hostname VERIFIED (mail1.verdi.de = mail.verdi.de | DNS:mail.verdi.de | DNS:mail1.verdi.de | DNS:mail2.verdi.de | DNS:mail3.verdi.de | DNS:mail4.verdi.de | DNS:mail5.verdi.de | DNS:mail6.verdi.de)
             Not Valid Before: Apr 12 09:51:25 2019 GMT
             Not Valid After: Apr  9 09:51:25 2029 GMT
             subject= /C=DE/ST=Berlin/L=Berlin/O=ver.di - Vereinte Dienstleistungsgewerkschaft/OU=ver.di IT/CN=mail.verdi.de
             issuer= /CN=verdi-CA01-intern
             Certificate 2 of 2 in chain: Cert VALIDATION ERROR(S): self signed certificate in certificate chain
             So email is encrypted but the recipient domain is not verified
             Not Valid Before: Oct 15 14:21:37 2013 GMT
             Not Valid After: Mar 21 19:35:47 2042 GMT
             subject= /CN=verdi-CA01-intern
             issuer= /CN=verdi-CA01-intern
```


```
Certificate 1 of 2 in chain: Cert VALIDATION ERROR(S): self signed certificate in certificate chain
So email is encrypted but the recipient domain is not verified
Cert Hostname VERIFIED (mail1.verdi.de = mail.verdi.de | DNS:mail.verdi.de | DNS:mail1.verdi.de | DNS:mail2.verdi.de
Not Valid Before: Apr 12 09:51:25 2019 GMT
Not Valid After: Apr  9 09:51:25 2029 GMT
subject= /C=DE/ST=Berlin/L=Berlin/O=ver.di - Vereinte Dienstleistungsgewerkschaft/OU=ver.di IT/CN=mail.verdi.de
issuer= /CN=verdi-CA01-intern
Certificate 2 of 2 in chain: Cert VALIDATION ERROR(S): self signed certificate in certificate chain
So email is encrypted but the recipient domain is not verified
Not Valid Before: Oct 15 14:21:37 2013 GMT
Not Valid After: Mar 21 19:35:47 2042 GMT
subject= /CN=verdi-CA01-intern
issuer= /CN=verdi-CA01-intern
```