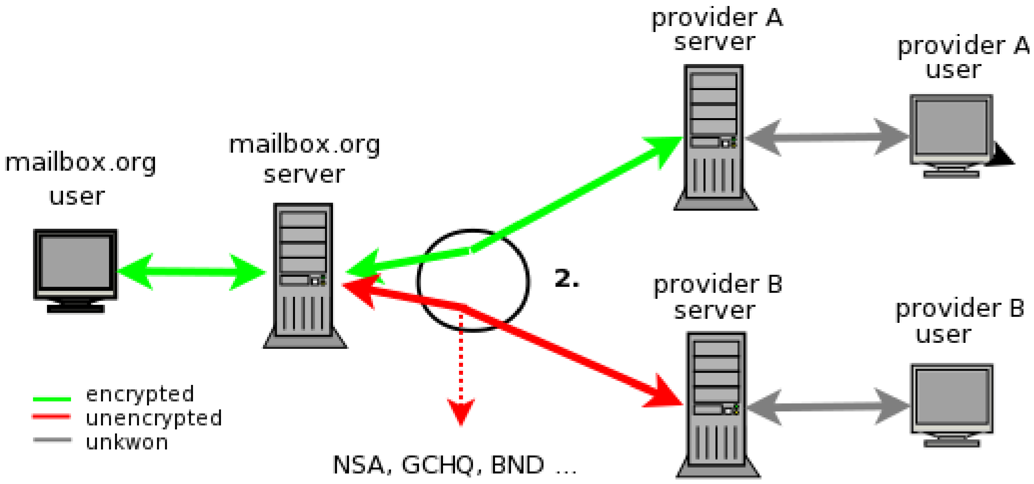
SSL-TLS encryption at mailbox.org

**SSL-encrypted or not? – Get a definite answer by entering a recipient's e-mail address.
Graphical symbols indicate the transport security level used by an external e-mail provider.**

The diagram below illustrates the transmission pathways of an e-mail sent by a mailbox.org customer to somebody else who is using the e-mail service of another provider:



Any connection our customers make using their mail clients to the mailbox.org servers will always use the most up-to-date and secure encryption standard available (1).

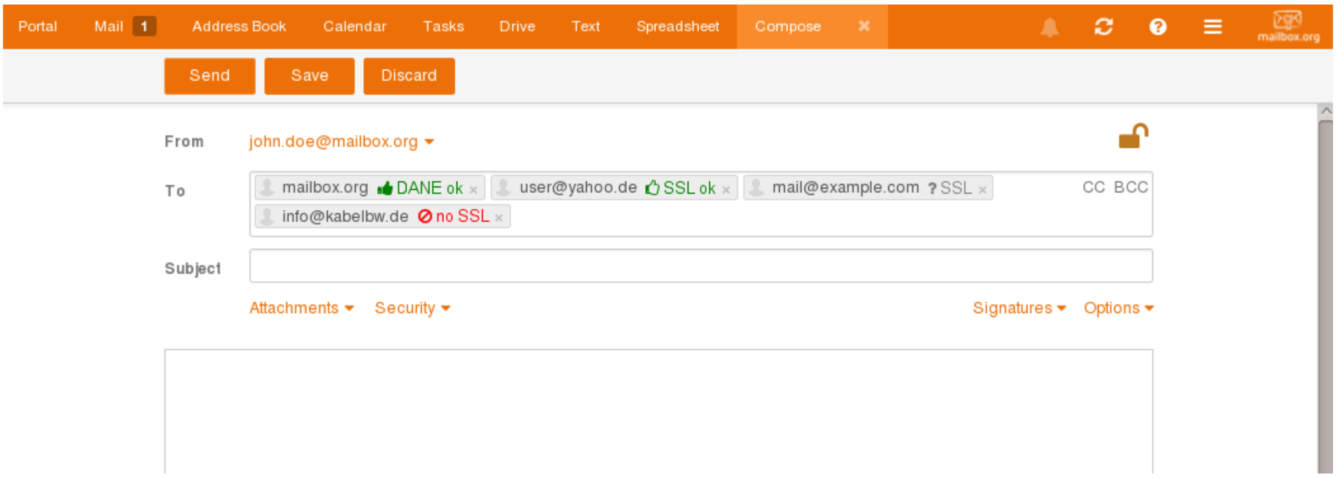
For the connections that our servers make to those of other providers, we are offering the same secure connection from our side, and many providers operate at the same level and allow a properly encrypted connection to be made for receiving the e-mail. However, there are still some providers who are unable to make use of encryption for this (2).

The following guidelines are implemented by default for **the sending of e-mail**:

1. If a provider has a TLSA/DANE record with the fingerprint of the SSL certificate made public via DNSSEC, then encryption with this certificate will be enforced for transmission security (e.g., Provider A in the diagram). In this scenario, customers of mailbox.org can rest assured that their e-mail is transmitted through a secure channel to the provider of the recipient.
2. The above holds even when e-mails are sent to providers like Gmail or Yahoo, as the mailbox.org servers will always enforce TLS-encryption by default. If our servers have previously connected to servers of other providers using SSL/TLS, then this fact will be remembered for future connections. mailbox.org users can be sure that an encrypted connection will always be required with any server that has supported such connection in the past.
3. There are some providers who previously could not and still cannot support encrypted connections using SSL/TLS. E-mails to these providers will then be sent unencrypted.

When composing an e-mail in the mailbox.org Office, the level of transmission security is made transparent so that our users will instantly know if their e-mail will be sent securely to the chosen recipients. Next to every recipient a symbol is displayed that indicates the transmission security achievable for their e-mail address and hence, their provider.

mailbox.org classifies other providers into three main categories: No encryption, SSL-enabled, and SSL-enabled plus DANE/DNSSEC-verified. If the receiving server does not support encryption at all, you will be notified by a red symbol and the status message "no SSL" next to the e-mail address of your recipient when composing an e-mail in the mailbox.org browser interface. If SSL encryption is available, users will see a green thumbs-up symbol and the message "SSL ok". Finally, if the receiving system supports the highest security level with SSL and verification via DANE and DNSSEC, then the user will get a green thumbs-up symbol plus the status message "DANE ok". There may be servers out there that we do not have any information about yet – this will be indicated by the message "SSL ?" in grey font.

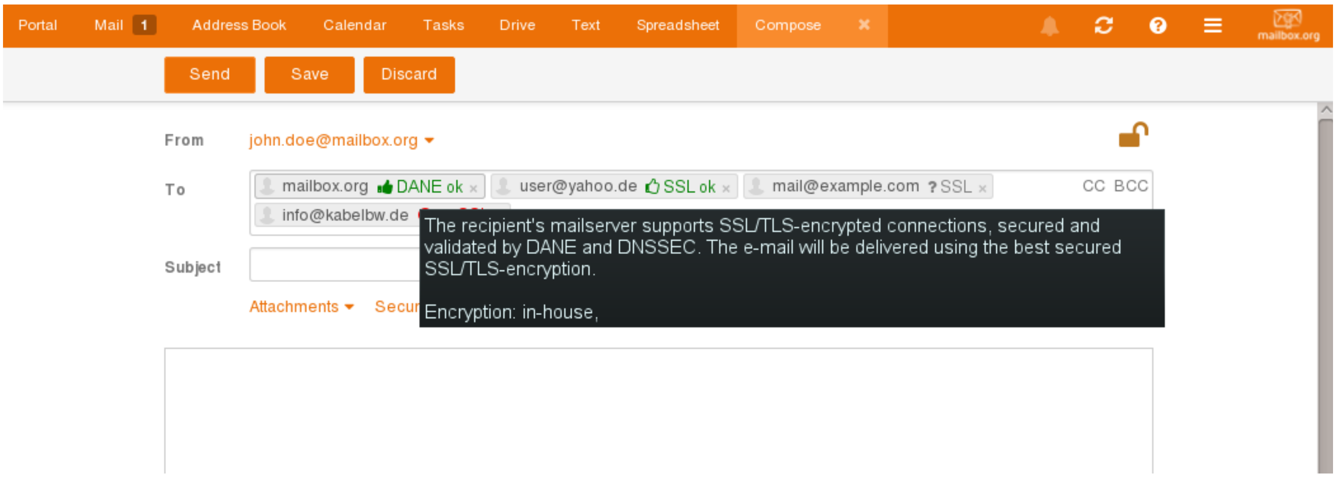


From john.doe@mailbox.org

To mailbox.org DANE ok × user@yahoo.de SSL ok × mail@example.com ? SSL × info@kabelbw.de no SSL ×

Subject

Move the mouse pointer over each symbol to get more details about the particular cipher algorithms and TLS version employed.



From john.doe@mailbox.org

To mailbox.org DANE ok × user@yahoo.de SSL ok × mail@example.com ? SSL × info@kabelbw.de

Subject

The recipient's mailserver supports SSL/TLS-encrypted connections, secured and validated by DANE and DNSSEC. The e-mail will be delivered using the best secured SSL/TLS-encryption.

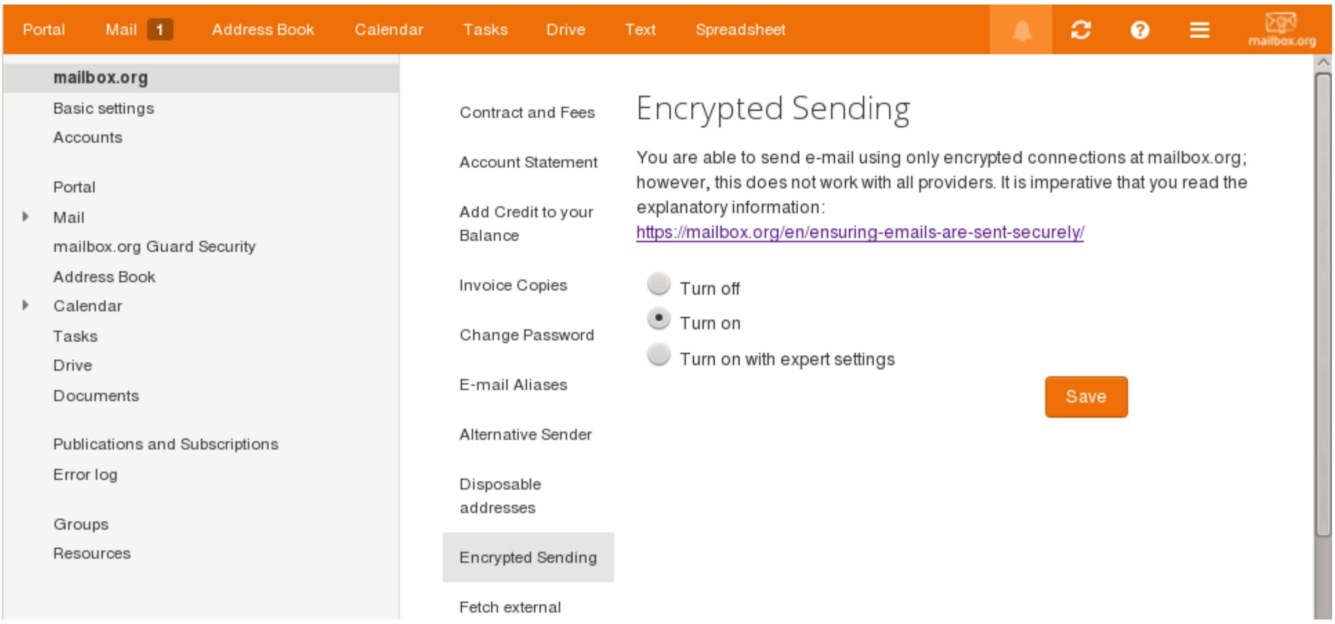
Encryption: in-house,

@secure.mailbox.org – make no compromises

At mailbox.org, each user can also have an address in the format *me@secure.mailbox.org* in addition to their normal e-mail address. Using that address will force the communicating mailserver nodes to enable secure transmission for BOTH the sending and the receiving of e-mail or abandon the communication if this cannot be achieved. When communicating with your secure.mailbox.org address, no compromises will be made when it co

mes to transmission security, as encryption is always required here. If, for any reason, a secure connection cannot be established, the e-mail will NOT be transmitted.

The aliases ...**@secure.mailbox.org** can be enabled in the configuration settings: **mailbox.org Encrypted Sending**:



Encrypted Sending

You are able to send e-mail using only encrypted connections at mailbox.org; however, this does not work with all providers. It is imperative that you read the explanatory information: https://mailbox.org/en/ensuring-emails-are-sent-securely/

○ Turn off
● Turn on
○ Turn on with expert settings

After enabling secure sending, the alias address ...**@secure.mailbox.org** can now be selected as a sender when composing e-mail. If you do this, then our mail servers will only send the message on if the e-mail provider of your recipient(s) actually supports the secure transmission of the data. If the provider at the other end does not support encryption, then the e-mail won"t be sent at all (an error message would be shown in this case to let you know).

The reasoning behind this mechanism is simple: TLS-encryption can only fulfil its purpose if secure transmission can be guaranteed for both ends of the communication. If it was not, then a recipient could simply reply to an e-mail which contains the previous message as a quote, and an intercepting agent could retrieve both messages in plain text, even if the first was originally encrypted during transmission.

For this reason, any e-mails sent to the special alias adresses ...**@secure.mailbox.org** will only be accepted if the incoming connection is encrypted. Consequently, the provider of your communication partner must support encrypted sending, otherwise no e-mail will be received at the alias address. In that case, the e-mail could not be delivered and would be returned to the sender.

Related Articles

- Can I trust the staff at mailbox.org
- An introduction to mailbox.org Guard
- Is there going to be transport encryption for my e-mail
- Fingerprints of our SSL Certificates
- HowTo: YubiKey NEO as PGP smartcard