

<https://security.berkeley.edu/data-encryption-transit-guideline>

[12:13 PM] Ajith Kodithuwakku

<https://security.berkeley.edu/data-encryption-transit-guideline>

​

[12:14 PM] Ajith Kodithuwakku

It mainly depends on the risks you want to mitigate. If you can (reasonably) trust all the infra around the server, and if you do not need to protect this data from a corporate deep inspection proxy, you can trust the SSL/TLS encryption layer.

You should normally only add another encryption level in the following use cases:

you are at work behind a corporate proxy with deep packet inspection and the data is sensitive enough to require being hidden to the local network support team the data should never be on decrypted form on the server. This can be used if you cannot trust the server admin team An example of the latter use case is the exchange of S/MIME encrypted mails. You still use TLS to protect the communication (mainly the credentials) but only the final recipient will be able to read the message: the mail server admin only finds a crypted payload.