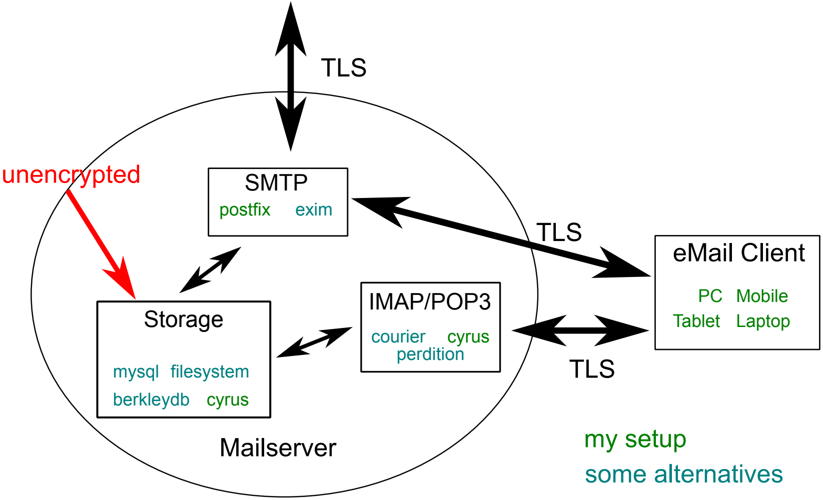
SECURE EMAIL STORAGE

with qpsmtpd + GPG

DOMINIK MEYER
byterazor@federationhq.de

LIGHTNINGTALK | 30C3

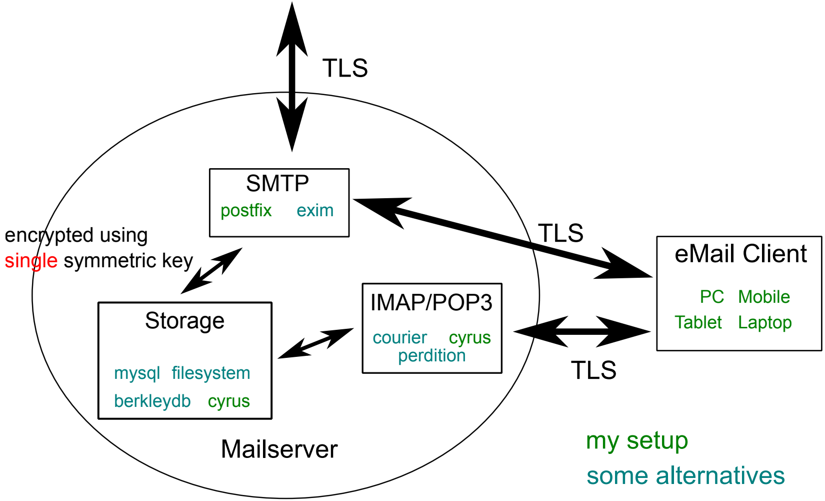
typical eMail System



my setup

some alternatives

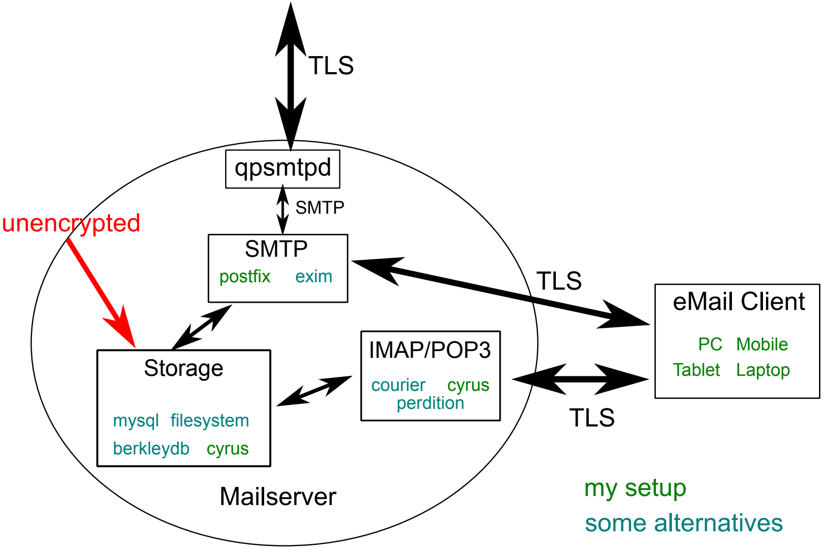
typical eMail System with secure storage



my setup

some alternatives

qpsmtpd

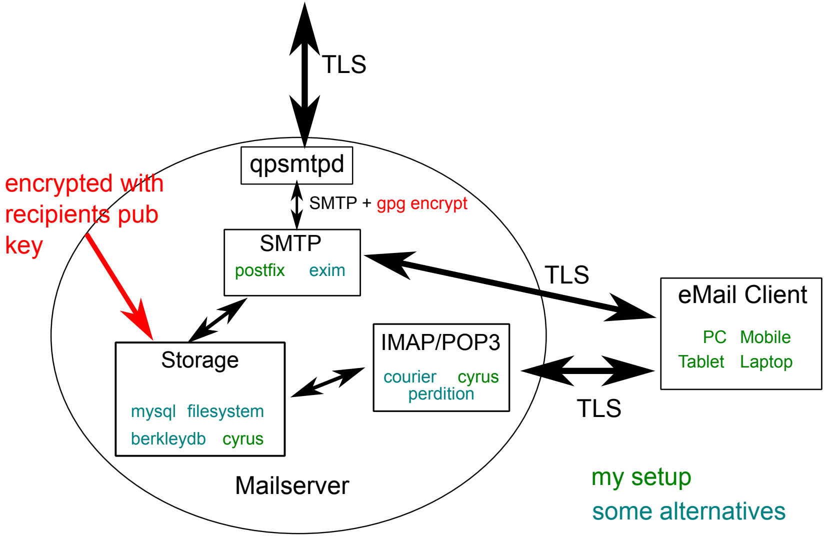


my setup

some alternatives

- easily extensible smtp server
- written in Perl + Plugin System in Perl
- good protection against spam + virusses
- Backends: qmail, postfix, exim, smtp

qpsmtp GPG Plugin



my setup

some alternatives

qpsmtp GPG Plugin

Overview

- written in Perl
- uses GnuPG to encrypt non encrypted incoming eMails
- PGP Mime standard
- uses recipients PGP key if locally available + trusted

Advantages

- can be used with standard eMail clients with PGP support
- linux: evolution, claws-mail, ...
- android: r2mail2
- even if eMail password is sniffed, emails can not be read
- decryption key is only available to recipient
- security not dependend on third party

Drawbacks

- Server side searches in body doesn’t work anymore
- attacker can add additional keys to keyring if server is not secure
- emails not readable if client doesn’t support PGP
- emails can be read before encryption
- recipients + subjects visible

Summary

- qpsmtpd + GPG Plugin ⇒ secure eMail storage
- http://byterazor.federationhq.de/blog/qpsmtpd-gpg.shtml
- inspired by: https://grepular.com/Automatically_Encrypting_all_Incoming_Email
- want to help improve plugin: mail me byterazor@federationhq.de