- Issue: Email message is recognized as spam by SpamAssassin. We use SpamAssassin to check if your mail might get blocked (please note: even if our internal SPAM check gives you a good SPAM score it does not mean that other SPAM filters might still block your mail!). Please visit the chapter Steps to Avoid Being Rejected by SPAM Filters or the chapter What to do? for more info on this subject.
- Issue: Reverse DNS of email mail server is not available or not pointing to Lucy. Some SPAM filters test, if a reverse DNS entry exists for an IP. A reverse DNS can only be set by your provider.
- Issue: No DKIM signature in email message. The DKIM feature attaches a new domain name identifier to a message and uses cryptographic techniques to validate authorization for its presence. The identifier is independent of any other identifier in the message, such in the author's From: field. DKIM is a way of 'signing' emails to prove they came from you. It is a form of email authentication that works via a digital signature and makes it easier to identify spoofed emails. The sending mail server signs the email with the private key, and the receiving mail server uses the public key in the domain's DNS information to verify the signature. One domain can have several DKIM keys publicly listed in DNS, but each matching private key is only on one mail server. When you send emails through the LUCY mail server and have this option enabled, they will be automatically signed. Please note, that it's just a notification. More than likely, your emails won't be blocked and you don't have to change anything. Please visit the chapter DKIM Background Info: for more info.
- Issue: No SPF record for sender e-mail domain or Lucy host doesn't match it. An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain. The purpose of an SPF record is to prevent spammers from sending messages with forged From addresses at your domain. Please note, that it's just a notification. More than likely, your emails won't be blocked and you don't have to change anything. Please visit Steps to Avoid Being Rejected by SPAM Filters for more info.
- Issue: SMTP server has been found in blacklists. A DNS-based Blackhole List (DNSBL) is an effort to stop email spamming. It is a "blacklist" of locations on the Internet reputed to send email spam. The locations consist of IP addresses which are most often used to publish the addresses of computers or networks linked to spamming; most mail server software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists. Please go to the according to blacklist webpage (https://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists) to get your server removed from the list.