**Mandrill**

[Mandrill](http://mandrill.com/) is a [transactional email](http://blog.mailchimp.com/what-is-transactional-email/?pid=compojoom&source=website) product from the people who brought you [MailChimp](http://mailchimp.com/?pid=compojoom&source=website). Mandrill is designed to help applications or websites that need to send transactional email like password resets, order confirmations, and welcome messages. Technically, though, you can send any legal, non-spam emails through Mandrill.Mandrill offers advanced tracking, easy-to-understand reports & email templates.

Mandrill is a recipient-based system.

With Mandrill, you can send emails through the [Mandrill API](https://mandrillapp.com/api/docs/) or [SMTP integration](https://mandrill.zendesk.com/hc/en-us/categories/200277207-SMTP-Integration). If you're already sending transactional emails for your website through SMTP, you can typically change your SMTP credentials to Mandrill's and begin sending immediately. With the Mandrill API, you can send emails, get information about your account, and view or parse reporting data in your own app or system.

**Mailchimp is primarily a bulk email service.**

Bulk email services send campaigns to multiple recipients at once, usually for marketing purposes. You can also create certain types of transactional messages in Mailchimp, like order notifications.

**Mandrill is a transactional email service.**

Transactional email services send email to one recipient, triggered by the recipient's action or inaction.

**Mailchimp**

Mailchimp is subscriber-based system. MailChimp is a web-based email marketing service. It helps you design email newsletters, share them on social networks, integrate with services you already use, and track your results

**SPF**

Sender Policy Framework (SPF) is a method of fighting spam. As more time passes, this protocol will be used as one of the standard methods of fighting spam on the Internet. An SPF record is a TXT record that is part of a domain's DNS zone file. The TXT record specifies a list of authorized host names/IP addresses that mail can originate from for a given domain name. Once this entry is placed within the DNS zone, no further configuration is necessary to take advantage of servers that incorporate SPF checking into their anti-spam systems. This SPF record is added the same way as a regular A, MX, or CNAME record.

**DKIM**

DKIM (Domain Keys Identified Mail) is an email authentication technique that allows the receiver to check that an email was indeed send and authorized by the owner of that domain. This is done by giving the email a digital signature. This [DKIM signature](https://www.dmarcanalyzer.com/dkim-signature/) is a header that is added to the message and is secured with encryption.

Once receiver (or receiving system) determines that an email is signed with a valid [DKIM signature](https://www.dmarcanalyzer.com/dkim-signature/), it’s certain that parts of the email among which the message body and attachments have not been modified. Usually, DKIM signatures are not visible to end-users, the validation is done on a server level.

Implementing the DKIM standard will improve email deliverability. If you use DKIM record together with DMARC (and even SPF) you can also protect your domain against malicious emails sent on behalf of your domains. Though, in practice these goals are achieved more effective if you use DKIM record together with DMARC (and even SPF). DMARC and DMARC Analyzer use both [SPF](https://www.dmarcanalyzer.com/spf/) and DKIM. Together they provide synergy and the best result for email security and deliverability.

DKIM attaches a new domain name identifier to a message and uses cryptographic techniques to validate authorization for its presence.

In,Cryptography A message authentication code (often called MAC) is a block of a few bytes that is used to authenticate a message. In other words message came from the started sender and its not been changed the mac value protects the both integrity and authenticity by allowing verifiers. The receiver can check this block and be sure that the message hasn't been modified by the third party.The abbreviation MAC can also be used for describing algorithms that can create an authentication code and verify its correctness.

**Setup your own postfix/sendmail mail server**

The easy way to install postfix and other programs which are needed for the testing email is the mailutils package by typing below command.

sudo apt-get install mailuils

Installing mailuils will also enable Postfix to be installed, as well as a few other programs needed for Postfix to function.

(or)

You can directly install postfix by using below command.

sudo su

Install postfix

yum install postfix -y

stop send mail (Default setting on Amazon Linux)

cd /etc/init.d

send mail stop

service send mail stop

Start postfix

cd /etc/init.d

postfix start

service postfix status

Switch MTA from sendmail to postfix

alternatives --set <name> <path>

alternatives --set mta /usr/sbin/sendmail.postfix

Configure postfix

nano /etc/postfix/main.cf

then in the file make sure all the lines that start with mydestination are commented out, like this:

#mydestination etc.

Then add your own:

mydestination =

myhostname = [insertyourhostname].[insertyourdomainname].com

myorigin = $mydomain

relayhost = $mydomain

inet\_interfaces = loopback-only

Reload postfix

cd /etc/init.d

service postfix reload

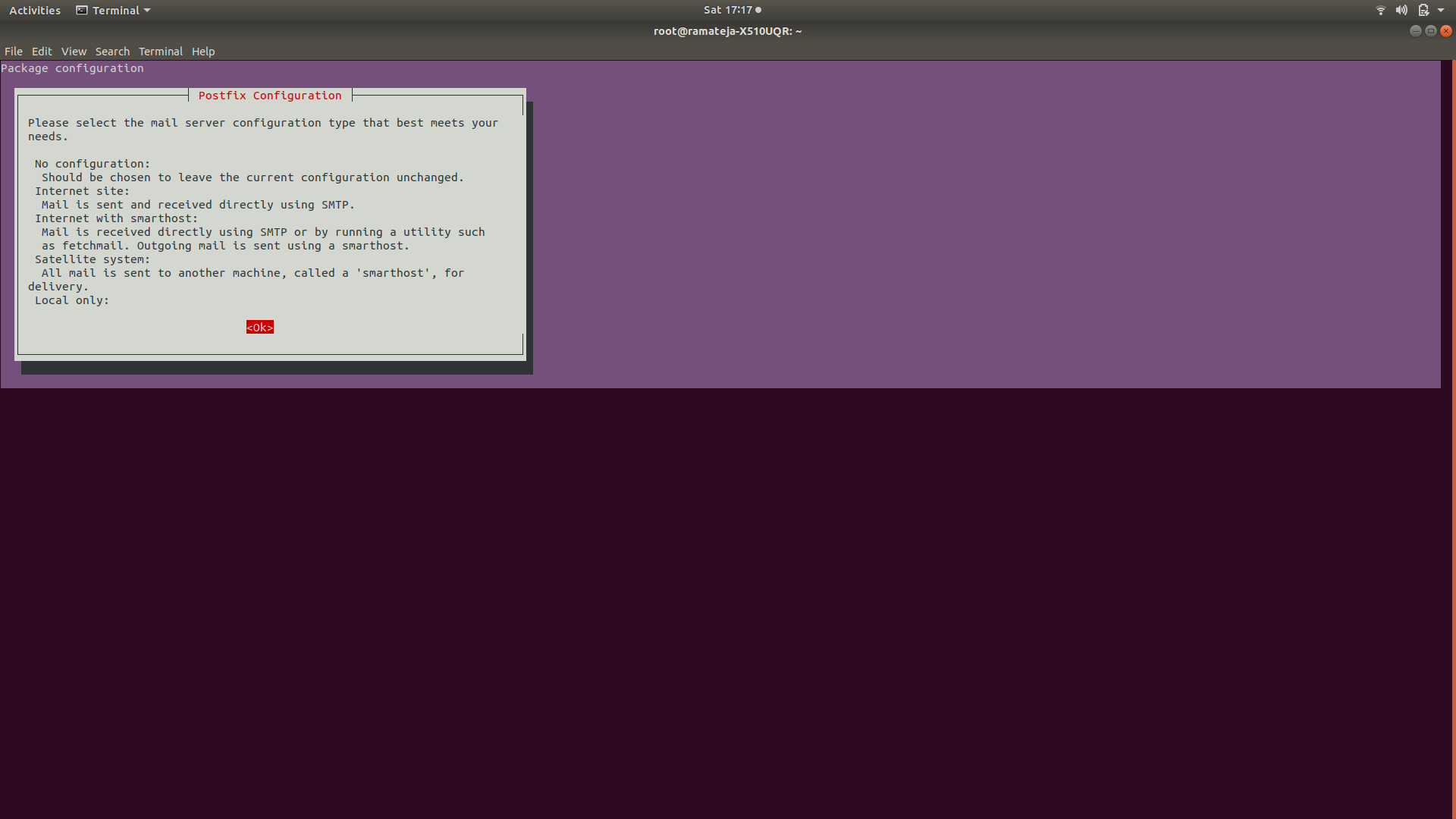
sudo yum install mailx

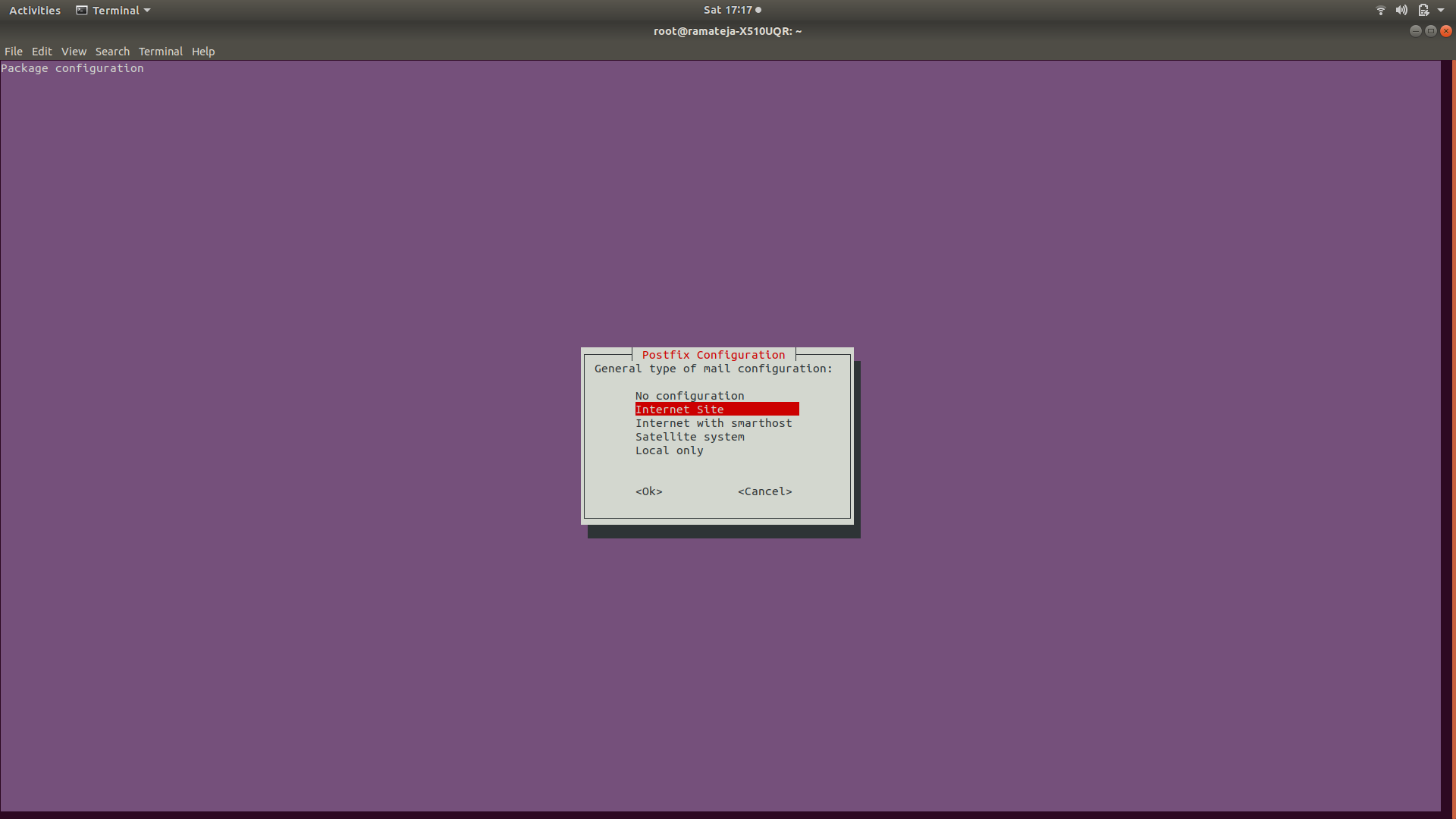
$ mail you@yourExistingEmailProvider

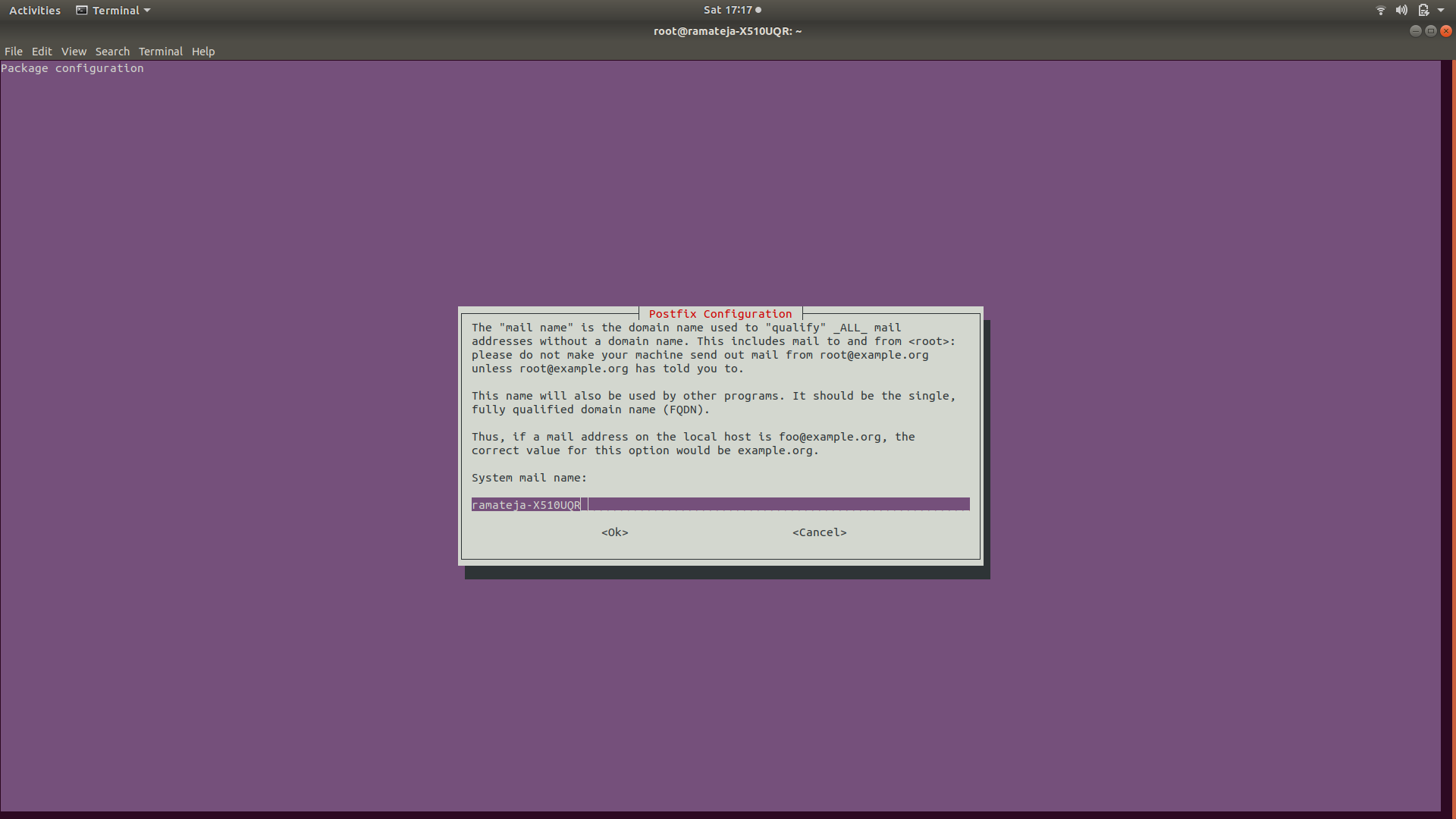
Subject: Test

This is a test email from my brand new email server!

.



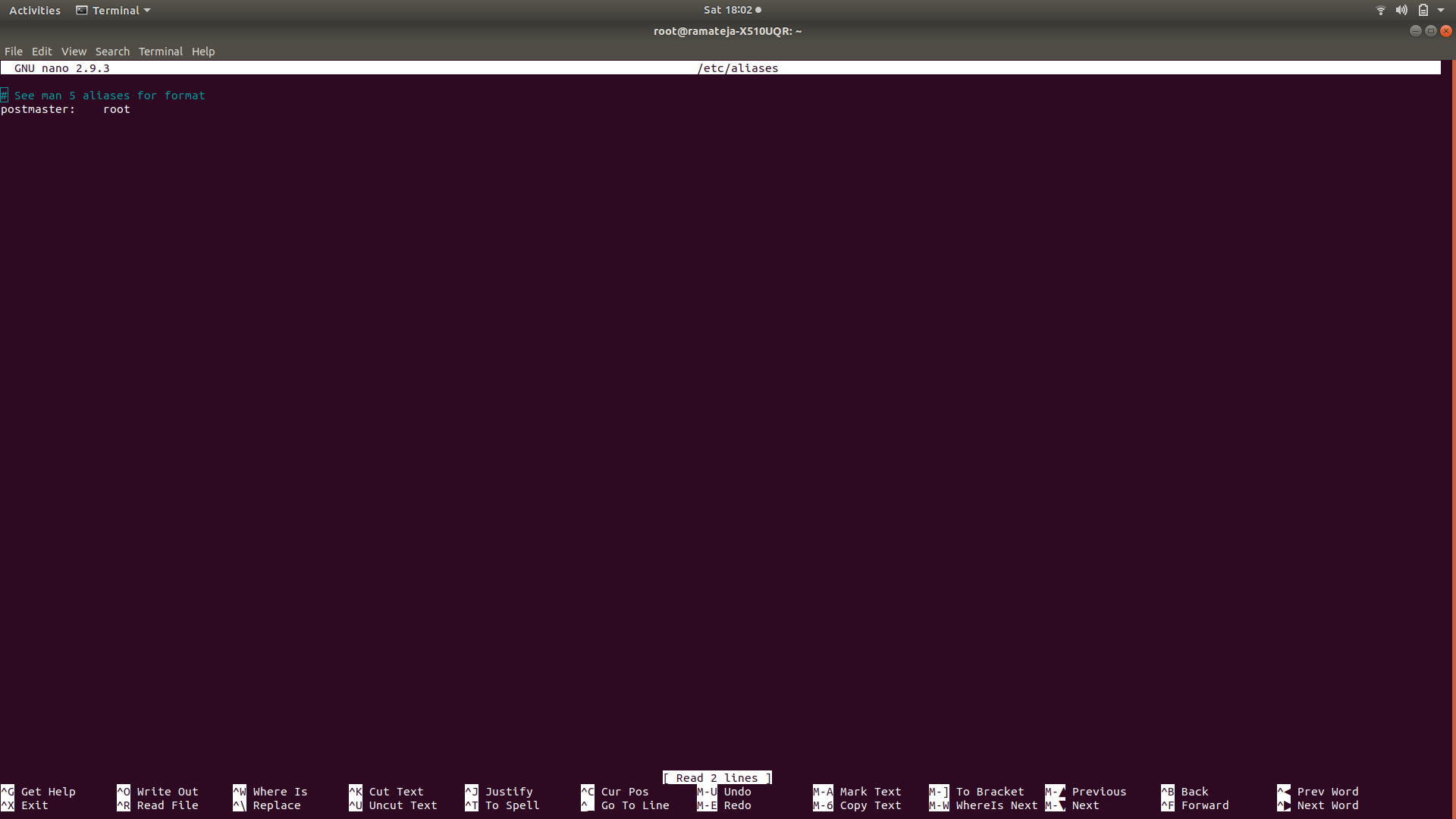




# 

# 

# 



# 

# 

# **KIM Core tokens for cinephilias.blogspot.com**

Generated at Sat Sep 28 04:59:09 2019 for selector *1569671949.blogspot*

You can bookmark this page and all your keys will be kept here (for at least a month, probably forever).

## **Private key**

This is the private key that needs to be entered into your DKIM signer. It must be kept secret - anyone with access to it can stamp tokens pretending to be you.

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgQDc82csHyvhUc6giMau3mt6sCuDkdIUn5+6m71it3GGsys6dL+A

npM45m5KUxieJRHrRGwRFUfYvKnrcf2NFw41ejgXP7IECKjys9eG/QNst5nIOCAc

6uLfhDGMx8e9CUaMoL5nVJCh6v5WdYsavNhJVzdgbejE7+YkywowMaYB1QIDAQAB

AoGAMzDxpndSY1Hg3bDS15EQtcw7SLBwS/bvuvx6VHTMCLlaOqDx/Yq/8V7yDqZR

/dH45NllcE/N5ZlQhQxUAmxlDfCcqCOqMzL/Hs4620vKX5e0XiXvMAAWZjkVY9BZ

9hD7kZBvtg2qx61i8yFdTAC3KQf9kSoBnkA/BtJ4gWwavcECQQDwlRjBPbryK5vN

3+60VTGCWuVJkigcThdQ2HPduF7d1J10tZ0JZPBNwsZKdbscDn0mCjwblghgTYoq

nF7Z+THbAkEA6xw8zXQrdjbm/loqYWcX1a9G1pdMOHzv3Rl8oLk0+2aPvsLQRcLw

D25E1UsZhkx3O5XsWqOGTuZx3jb9xlciDwJBAMpwCxZ/xREF1OKVbZzcmv5fUdRo

Ycv/gesLV+PXwivTPnL4Zx2CjBpCrOv2yO1A29nofs+PnZi7ZmmYjs/HukUCQQC8

qeYowCX4MMpgJR6JFt9Le+GOZc6mLauVctRNbRGVA5Ip886JjIpy93uI5UDQQiAT

0pTdjwdB3S5WsS4nsNgFAkEA38ZJTfUT48OW7e40FHHT+xZOPYrbtZcXON49h5OF

RKp1gnBYbxNgMyZBKeVIqlh+nWLh3+H0SfelxlwXI+G7Ag==

-----END RSA PRIVATE KEY-----

## **Public key**

This is the public key that needs to be published via DNS before you start using the tokens to send mail.

### **Bind 9 Format**

This is the public key in a format for use in a bind 9 zone file

1569671949.blogspot.\_domainkey.cinephilias.blogspot.com. IN TXT (

"v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDc82csHyvhUc6giMau3mt6sCuD"

"kdIUn5+6m71it3GGsys6dL+AnpM45m5KUxieJRHrRGwRFUfYvKnrcf2NFw41ejgX"

"P7IECKjys9eG/QNst5nIOCAc6uLfhDGMx8e9CUaMoL5nVJCh6v5WdYsavNhJVzdg"

"bejE7+YkywowMaYB1QIDAQAB")

**Create your own SPF:**

Step 1: Gather IP addresses that are used to send email

Step 2: Make a list of your sending domains

Step 3: Create your SPF record

Example: v=spf1 mx include:\\_spf.example.com -all

v=spf1: Sets the SPF version that is used.

mx: Allows the domain’s MX details to send email.

include:\_spf.example.com: Includes example mail servers as authorized servers.

-all: Indicates that servers that are not listed previously are not authorized to send email

Step 4: Publish your SPF to DNS

Step 5: Test

**How to check mx record :**

MX record example:

owner-name ttl class rr pref name

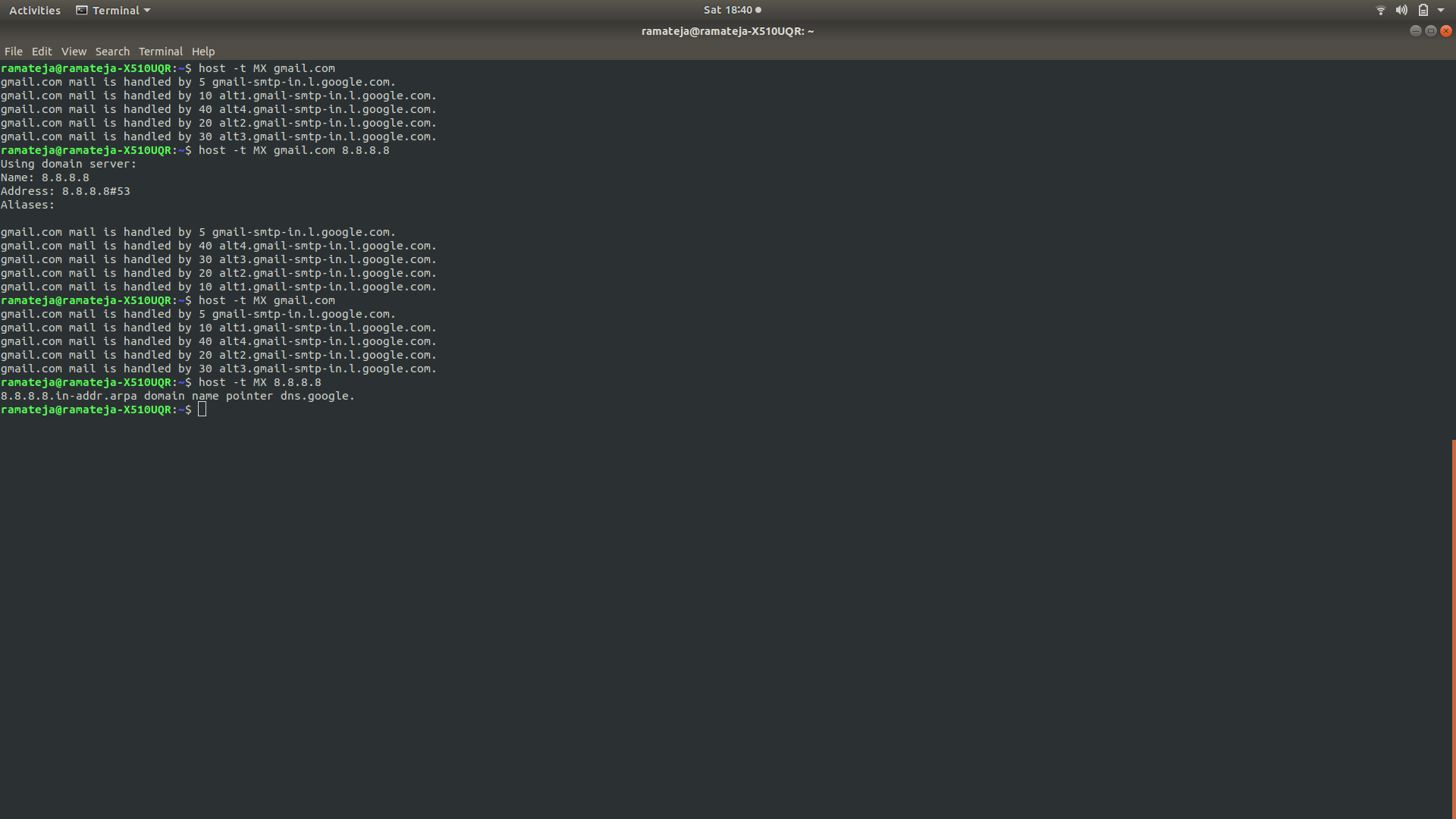
example.com. 3w IN MX 10 mail.example.com.

Back-up mail servers (higher pref values) are usually configured to simply forward mail over a prolonged period (multiple days or even weeks) to the primary mail server.

To check MX record:

host -t MX example.com

For example if we want to check the mx records of gmail   
 host -t MX gmail.com



**DKIM:**

1.Choose a DKIM selector :A DKIM selector is a string used to to point to a specific DKIM public key record in your DNS

2.Generate a public-private key pair by using ssh-keygen

3.Publish the selector and public key by creating a DKIM TXT record.

DKIM key example:

dk1024.\_domainkey.returnpath.com. 600 IN TXT "v=DKIM1\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLlSyQMNWVLNLvyY/neDgaL2oqQE8T5illKqCgDtFHc8eHVAU+nlcaGmrKmDMw9dbgiGk1ocgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAGoi/UyPmqfcPibytH81NFtTMAxUeM4Op8A6iHkvAMj5qLf4YRNsTkKAV

DKIM selector (s=): dk1024-2012

The domain (d=): returnpath.com

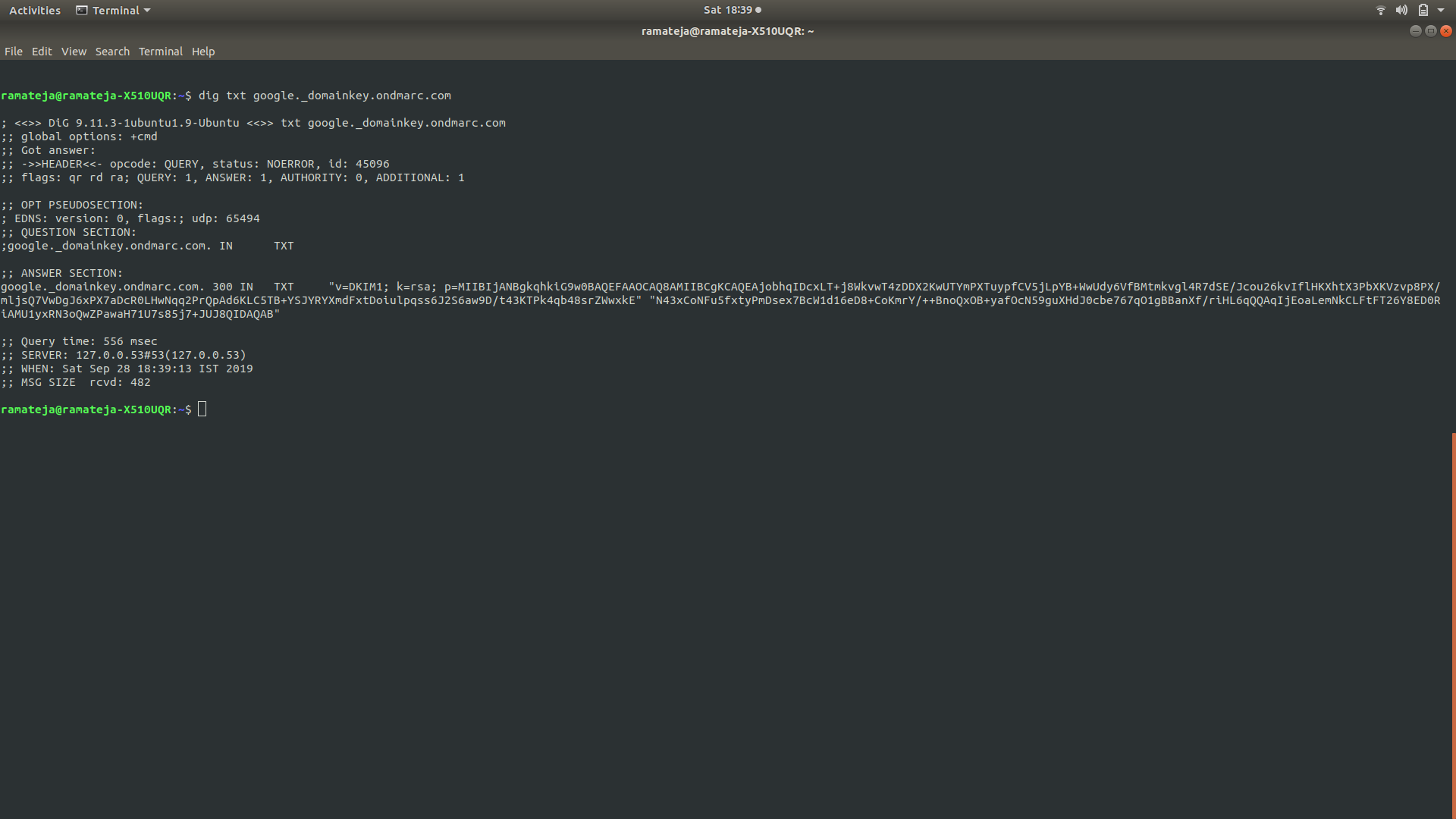
The version (v=): DKIM1

The public key (p=): MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLlSyQMNWVLNLvyY/neDgaL2oqQE8T5illKqCgDtFHc8eHVAU+nlcaGmrKmDMw9dbgiGk1ocgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAGoi/UyPmqfcPibytH81NFtTMAxUeM4Op8A6iHkvAMj5qLf4YRNsTkKAV

To check DKIM record:  
 dig txt selector.\_domainkey.domain

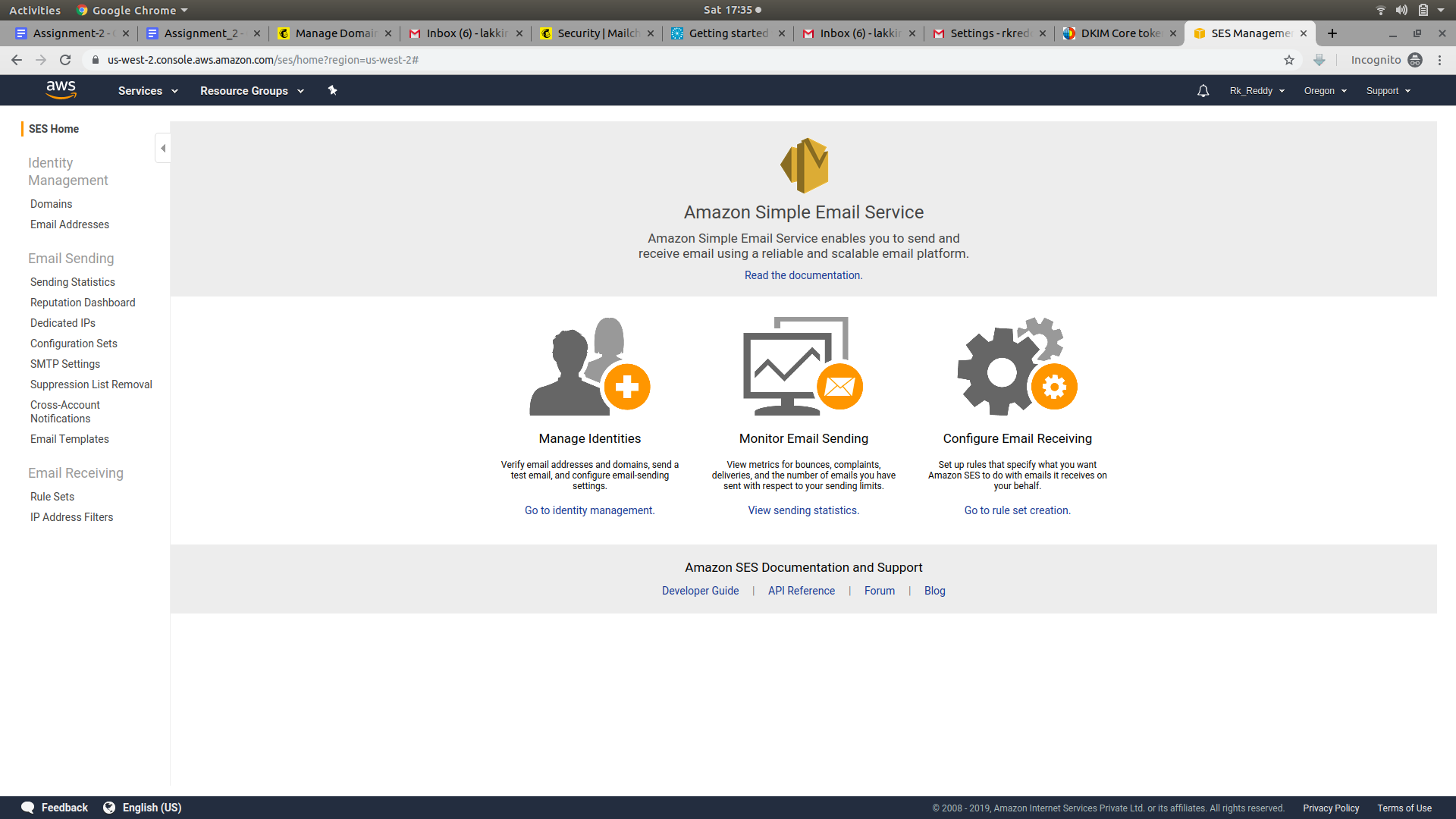
Here i checked the DKIM key of a domain using dig command:

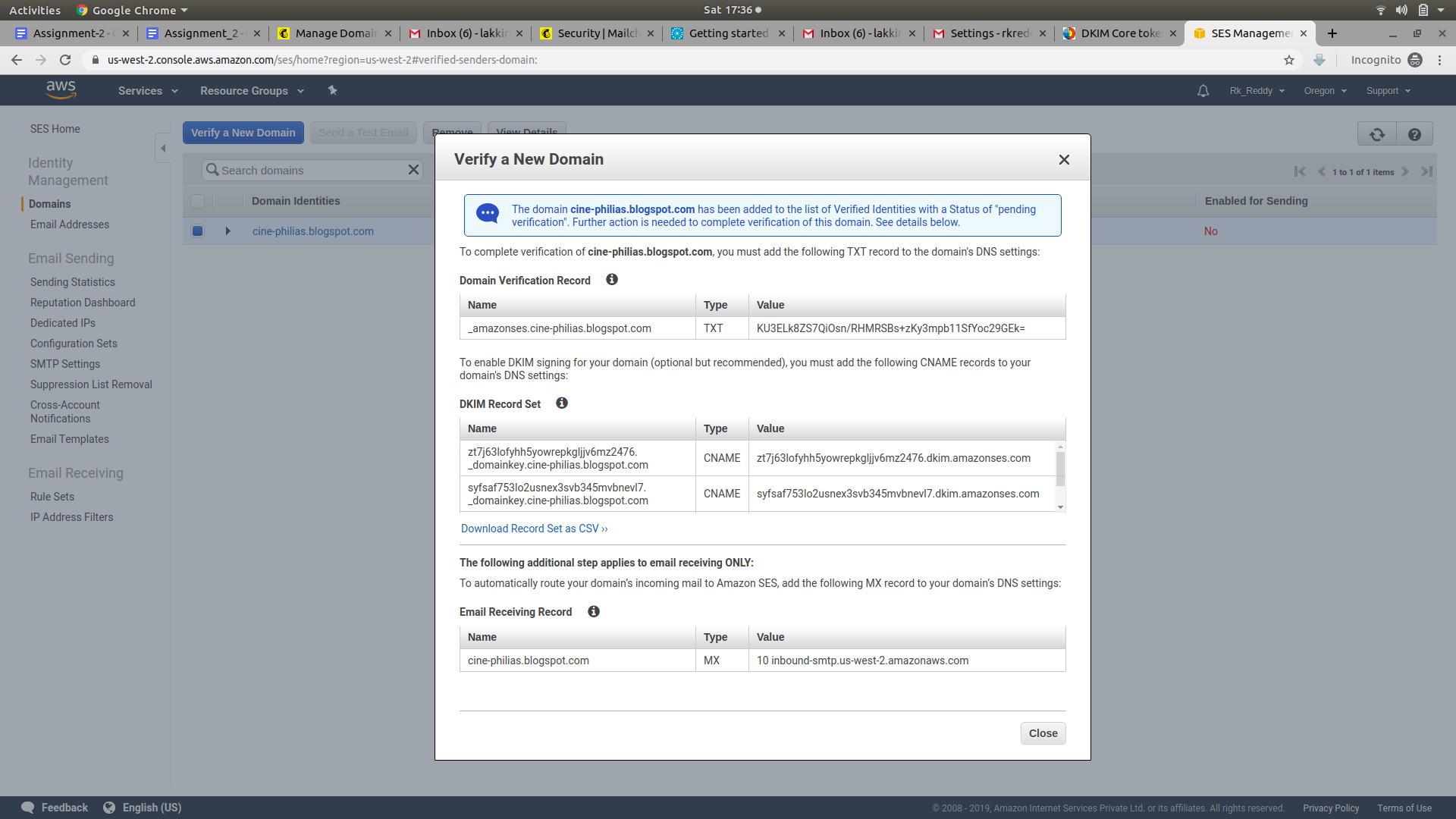
dig txt google.\_domiankey.ondmarc.com

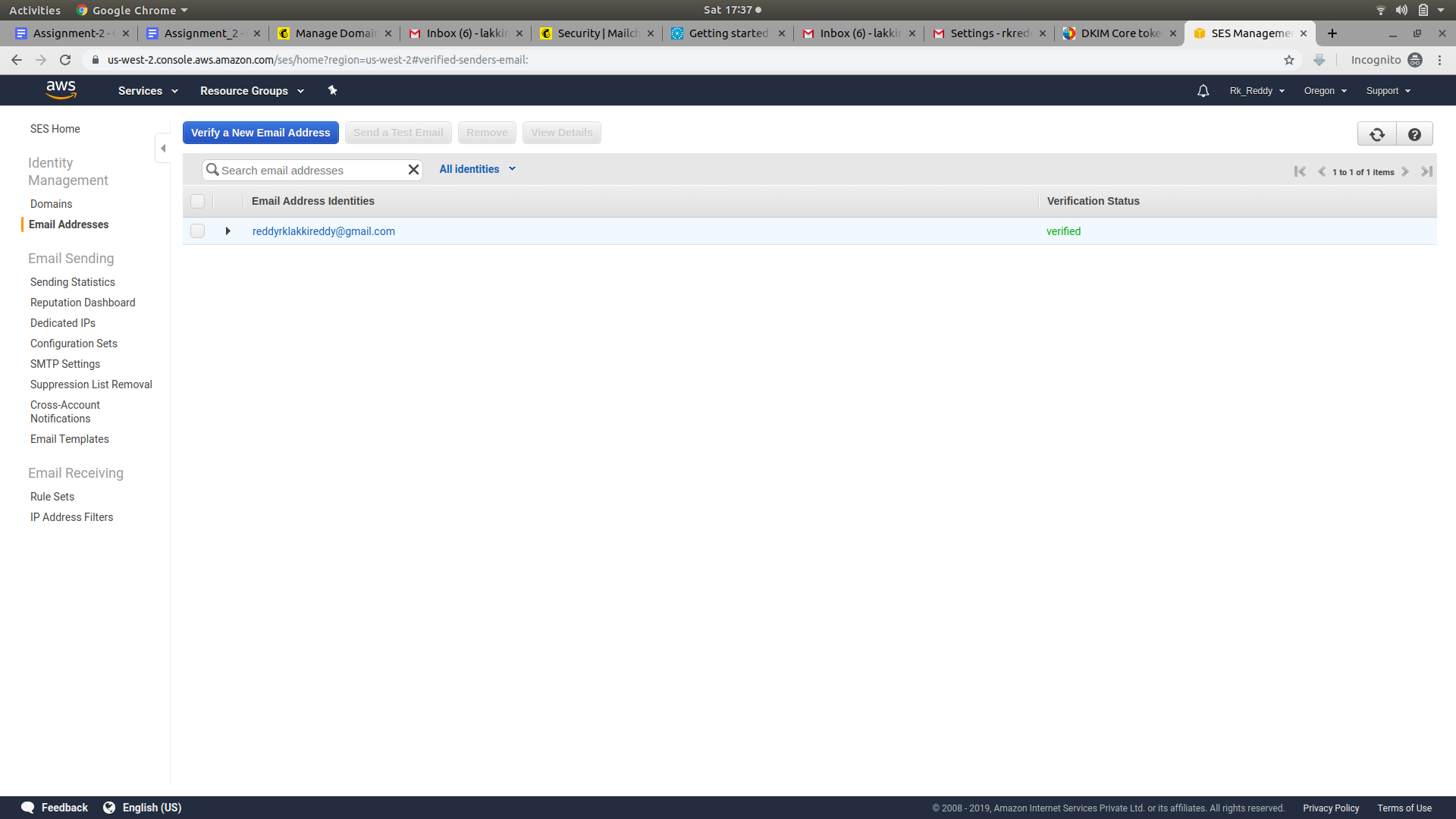


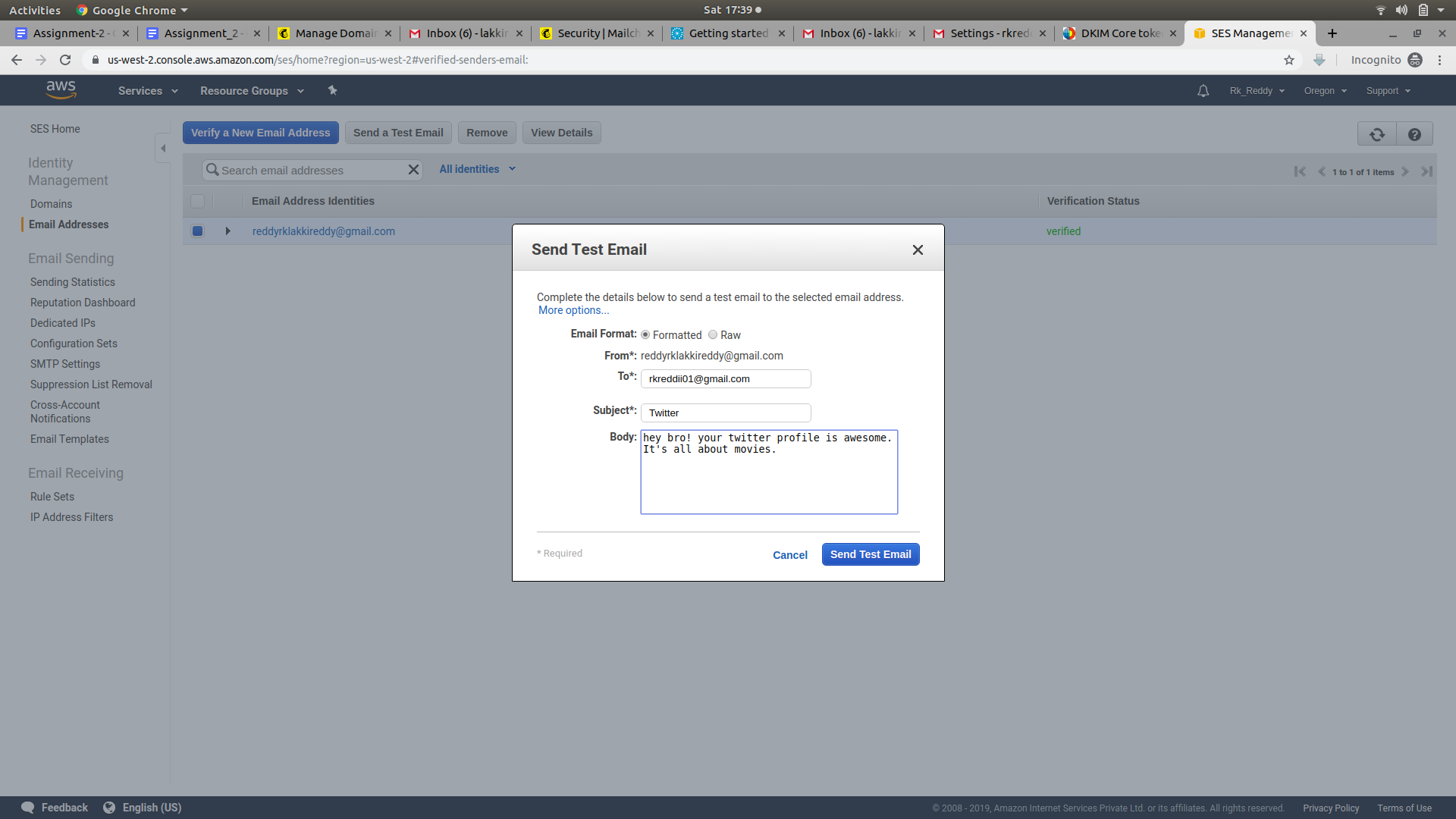
**Configure SES with postfix mail server**

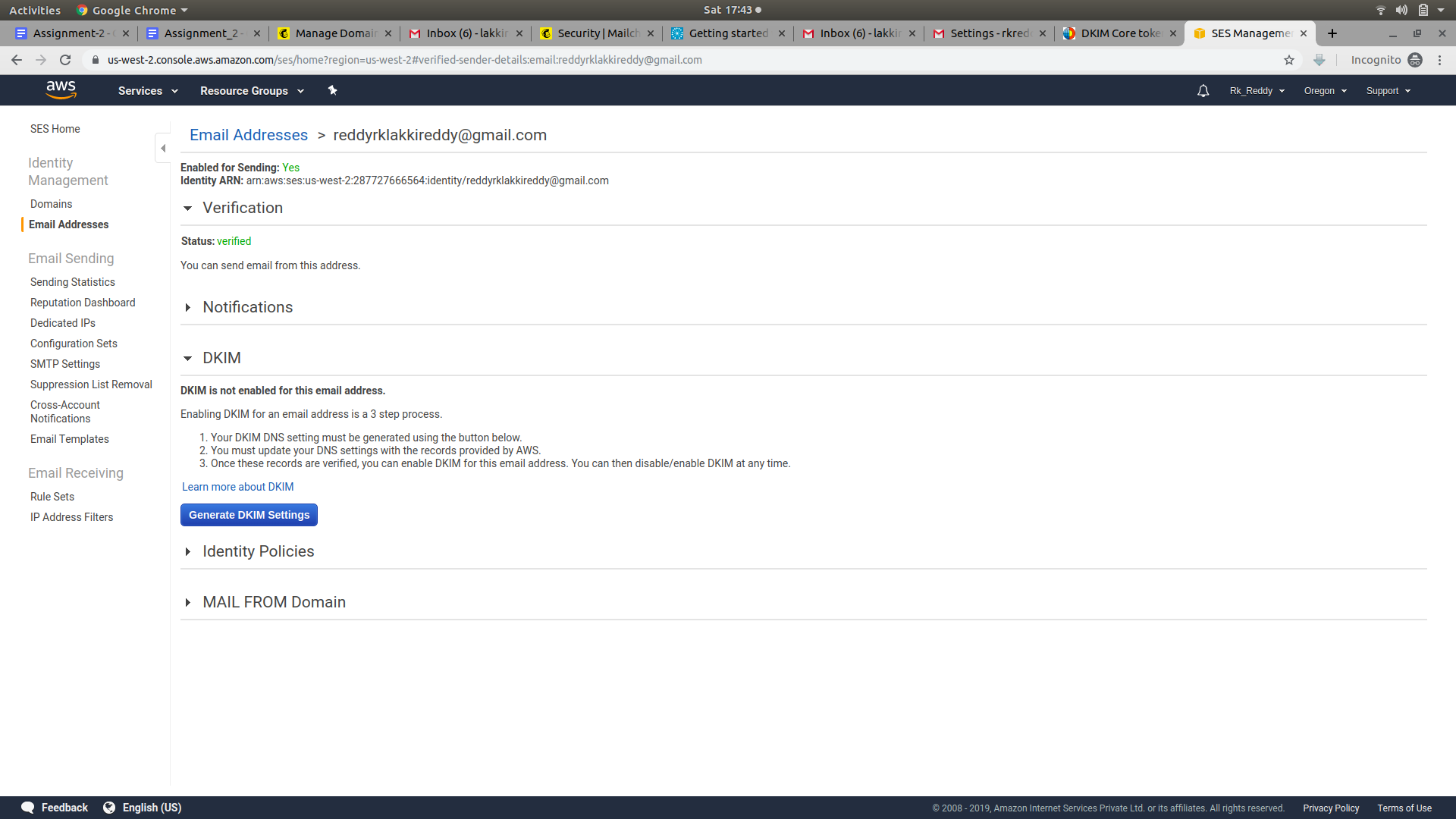
Postfix is an alternative to the widely used Sendmail Message Transfer Agent (MTA)

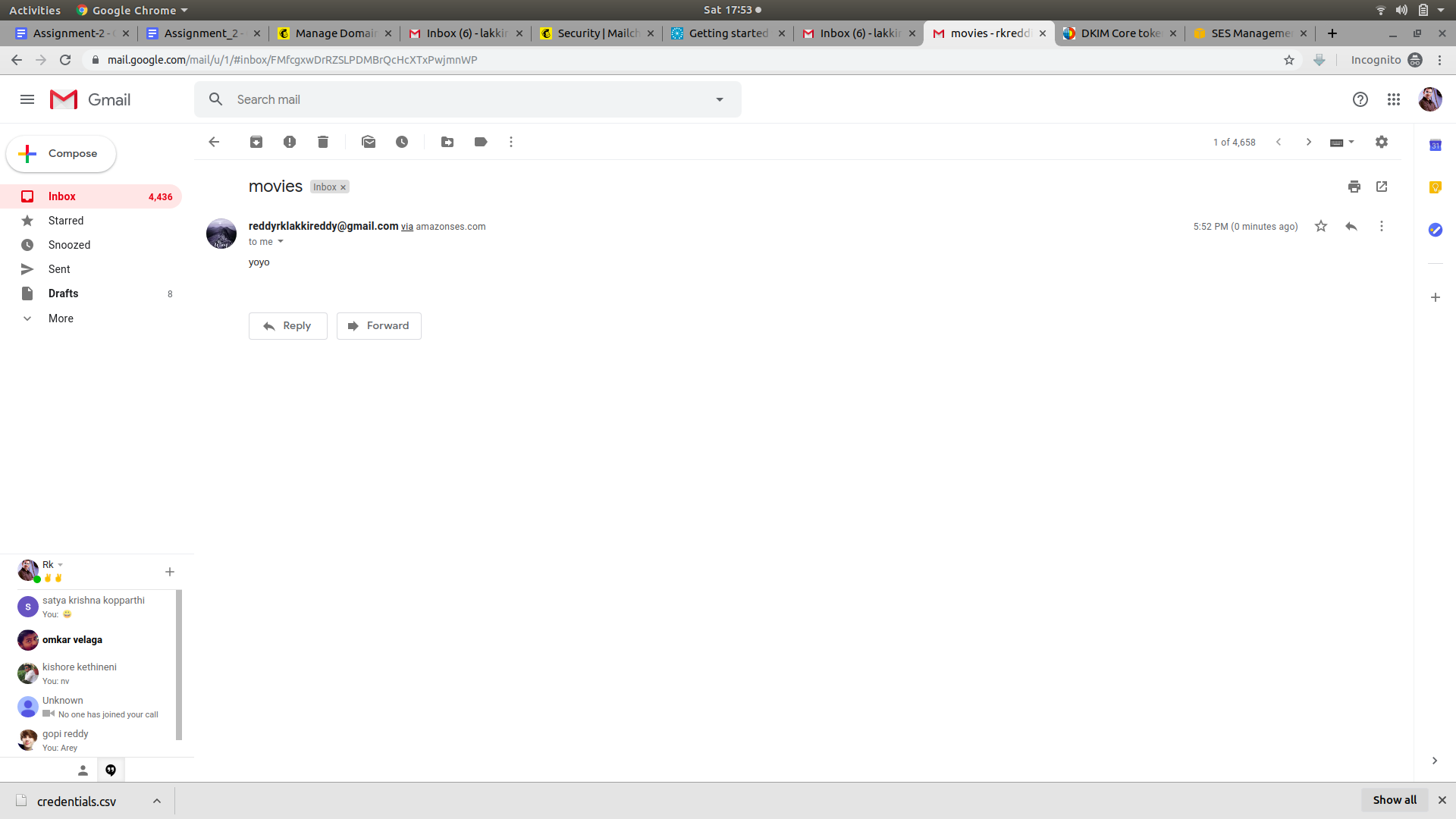


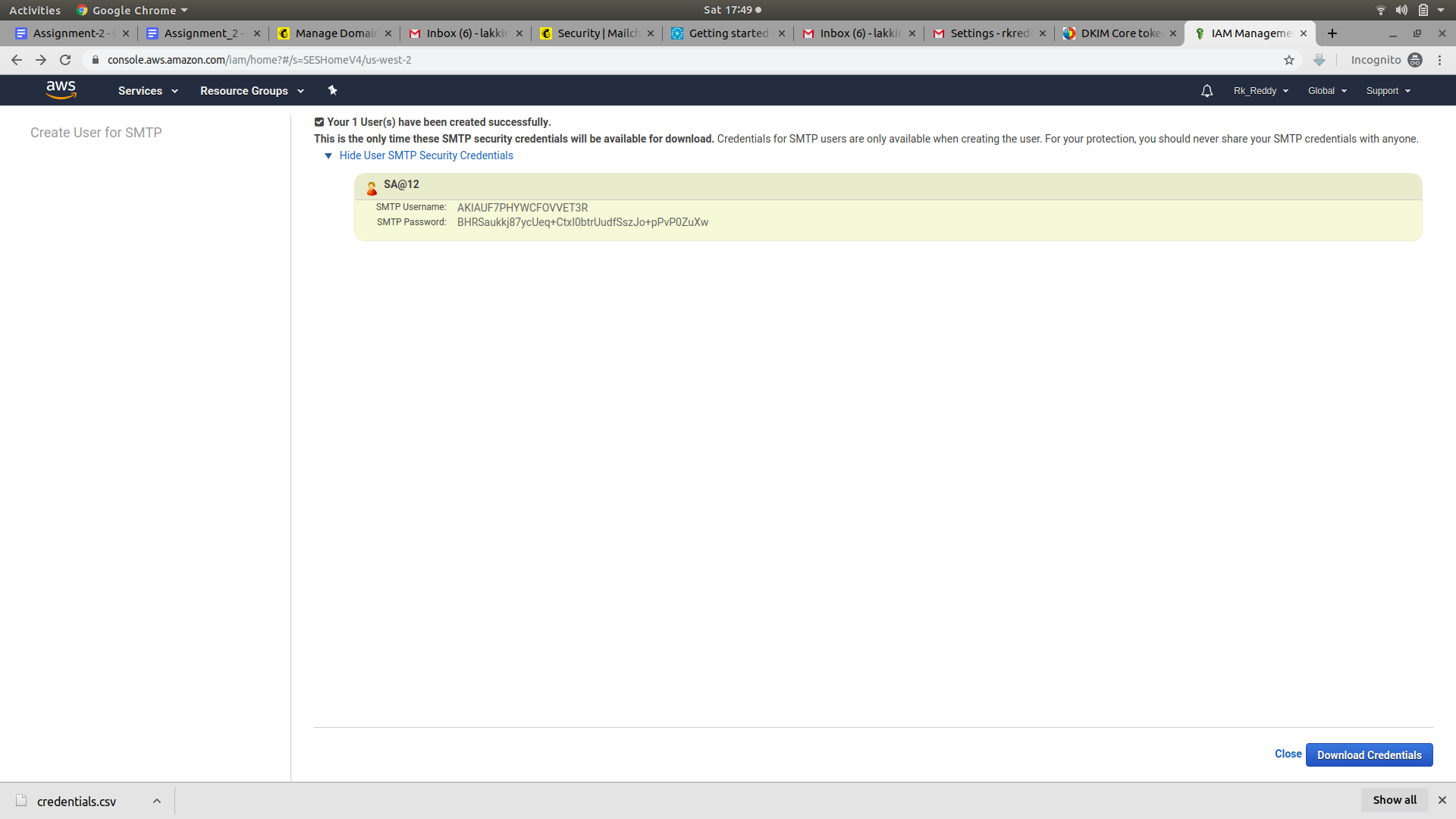












**Debug why mails going into spam folder**

