Jimma University

Jimma Institute of Technology

Faculty of Electrical and Computer Engineering

Masters of Science in Computer Engineering

Advanced computer and Network Security

Project one

Certificate Authorization for Ethiotelecom

Prepared by:

Misganaw Aguate & Fasika Tegegn

Submitted to: - Dr. Henock M. (PHD)

Abstract

In this paper we have try to show how we create security certificate for secure communication and data transmission between client and server or root organization to intermediate branch and intermediate branch to end user. For this project case we are going to assign the organization called **ethiotelecom,** its root CA is Addiss Ababa and its intermediate branch and end user are found in different region city and zone city. The scenario ii, first all servant organization including root CA create their private and public key, if the organization is intermediate branch or end user request root CA for signing certificate, root CA acccept requested information and sign on certificate then finally deliver signed certificate for each branch. The intermediate branch after getting signed certificate can have privilege for signing certificate requested certification by the corresponding end user. Remember that if the end user does not trust the intermediate one he/she can directly request to root CA. for the sake of implementation we used linux OS UBUNTU version and open SSL package on UBUNTU. Additionally this project also has testing certificate on web browser by connecting client PC and server. Since our test is based on windows OS, we create the certificate using windows CMD.

Table of contents

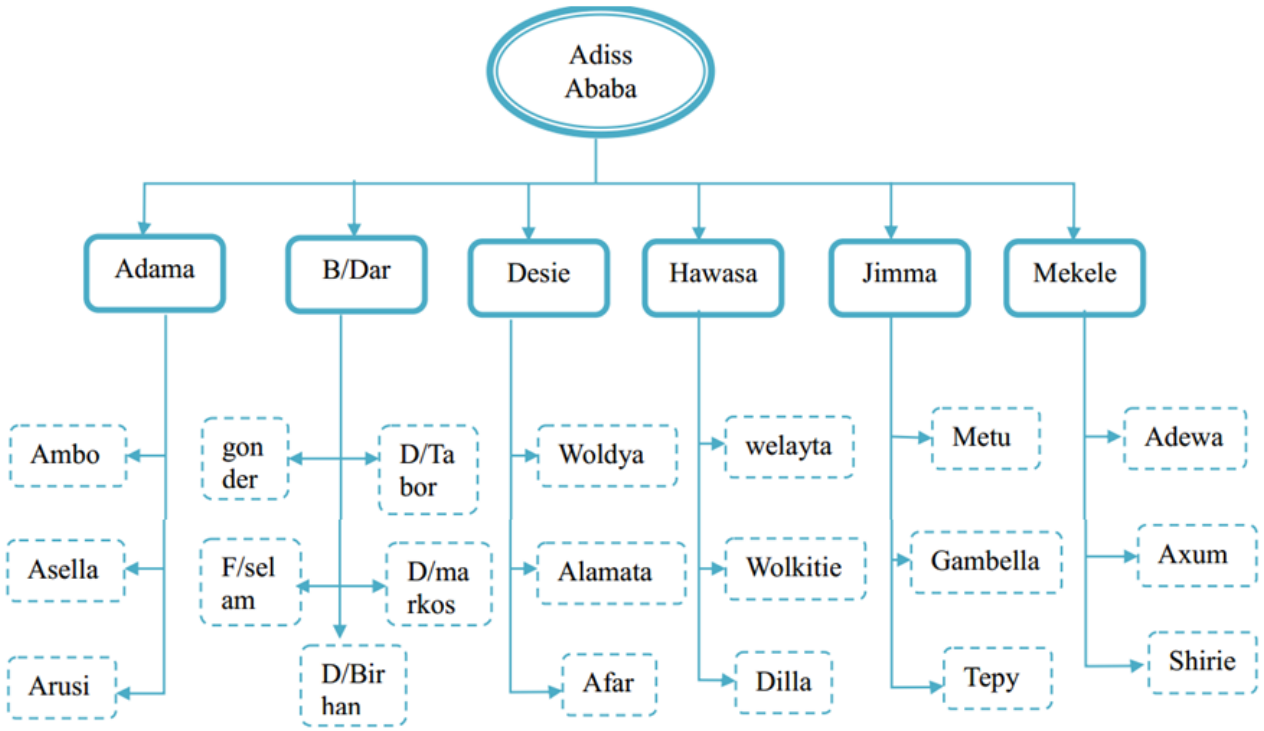
Contents **page**

Task covered

In this project we are covered the following core task

- creating private and public key of root CA
- root CA make self signed certificate for itself
- creating private and public key of intermediate CA
- intermediate CA request for signed certificate to root CA
- root CA sign the requested certificate and deliver authenticated certificate by using requested full information of intermediate CA or end user
- create private and public key of each end user
- end user request to intermediate CA for signed certificate
- intermediate CA sign certificate by using its private key and signed certificate that is delivered from root CA and deliver to corresponding end user
- testing signed certificate on web browser

As per our predefined description on the abstract the following sample organizational structure defines for ethiotelecom:



Root CA

The following snip hut indicates that root CA create its own self signed certificate called as addisCA.crt.

```
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -x509 -days 730 -key mkey/p
rk_addiss.pem -out addissCA.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Adiss Ababa
Locality Name (eg, city) []:Piasa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gevernmental Company
Organizational Unit Name (eg, section) []:www.etiotle.gov.et
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotele.gov.et
Email Address []:ethiotelecom@gmail.com
misganaw@misganaw-Vostro-15-3568:~$
```

Intermediate branch

Adama intermediate CA

This intermediate CA have signed certificate granted from root CA of Addiss Ababa. This intermediate CA has its own branch which is end user such as Ambo, Asella, Arusi and Woliso. This CA accept requested certificates from each of end user with extra information of end user then handle delivering signed certificate with respect to requested certificate. But if the end user does not trust this intermediate CA it can directly request to root CA which is in this case Addiss CA. for example **Ambo** end user is not request to Adama intermediate CA rather it request to **Addis root CA**.

Private and public key

The following snip shut indicates the private and public key of Adama intermediate CA before requesting root CA (Addiss) for signed certificate. This is **prk_adama.pem** and **pubk_adama.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out prk_adama.pem 2048
Generating RSA private key, 2048 bit long modulus
.............................+++
.........................................+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in prk_adama.pem -pubout -out pubk_a
dama.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$ writing RSA key
```

Requested Certificate

After having private and public key the intermediate CA (Adama) can request to Addiss CA for signed certification by adding some extra information that describe the identity of requester (Bahr Dar CA). In this case identity of Adama intermediate CA. Adama CA request using **req_adama.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key mkey/prk_adama.pem -ou
t req_adama.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Adama
Locality Name (eg, city) []:Adama
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelelcom
Organizational Unit Name (eg, section) []:Ethiotelecom_adama
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom.gov.et
Email Address []:ethiotelecom_adama@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321misgie
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to addiss root CA, if the required parameter by root CA from intermediate CA (Adama CA) is correct then root CA (Adiss CA) will grant signed certificate as follows. Here the delivered certificate is **adama_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_adama.cs
r -CA addissCA.crt -CAkey mkey/prk_addiss.pem -set_serial 01 -out adamaCA.crt
Signature ok
subject=/C=ET/ST=Adama/L=Adama/O=Ethiotelelcom/OU=Ethiotelecom_adama/CN=www.ethi
otelecom.gov.et/emailAddress=ethiotelecom_adama@gmail.com
Getting CA Private Key
misganaw@misganaw-Vostro-15-3568:~$
```

Adama end user

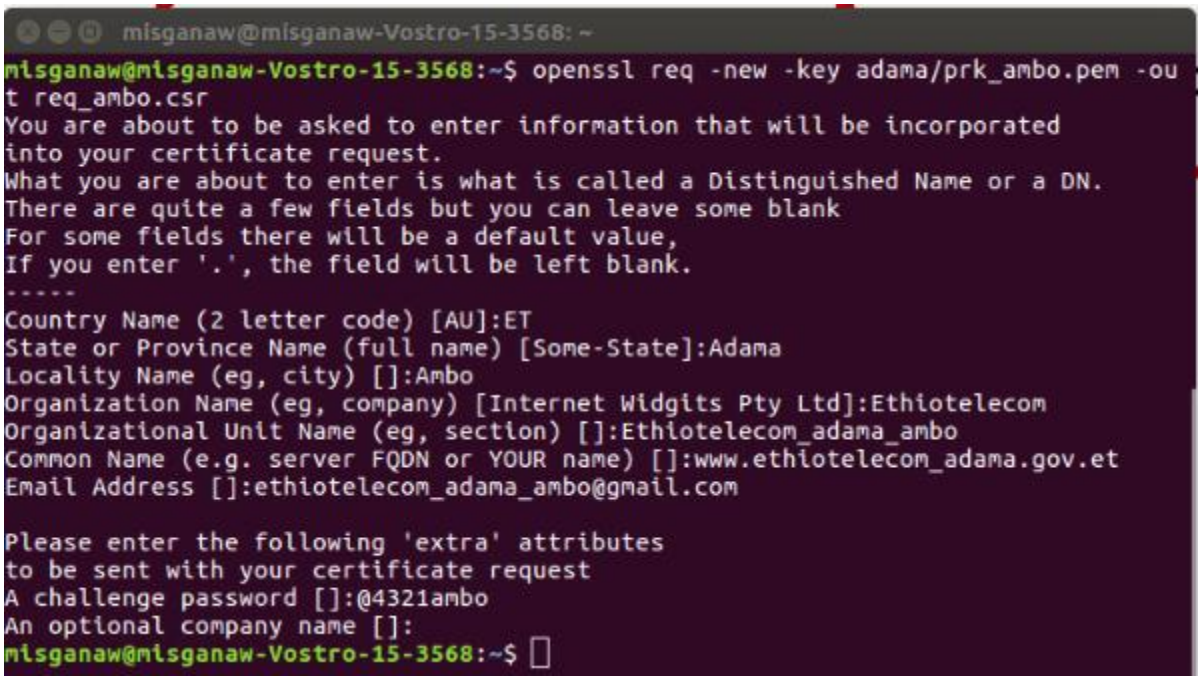
Ambo

Private and public key

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out adama/prk_ambo.pem 2048
Generating RSA private key, 2048 bit long modulus
.........................+++
.............................................................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in adama/prk_ambo.pem -pubout -
out adama/pubk_ambo.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

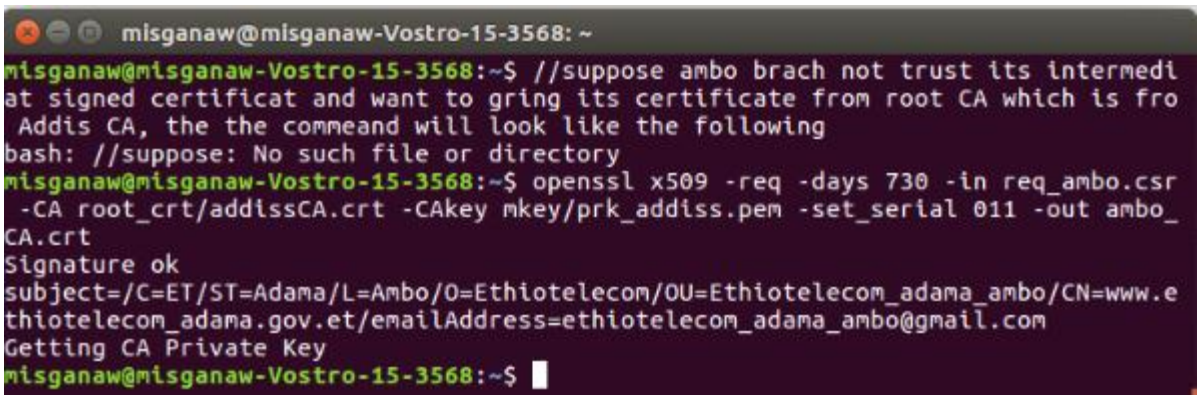
Requested Certificate

The uniqueness of this end user is that, he/she does not request the corresponding intermediate CA (Adama CA) because she/he does not trust his intermediate CA (Adama CA). so after having private and public key the end user (Ambo) can request to Addiss Ababa root CA for signed certification by adding some extra information that describe the identity of requester (Ambo). In this case identity of Ambo end user, Ambo request using **req_ambo.csr** as follows on snip shut.



Signed Certificate

Here suppose Ambo end user does not trust the certificate signed by his intermediate CA branch (Adama CA) and want to get certificate from root CA (Addiss Ababa). The following snip shut shows that Ambo end user brought signed certificate from root CA (Addiss Ababa CA) called as **ambo_CA.crt**



Asella

Private and public key

The following snip shut indicates the private and public key of Asella end user before requesting intermediate CA (Adama CA) for signed certificate. This is **prk_asella.pem** and **pubk_asella.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out adama/prk_asella.pem 204
8
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.....................................................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in adama/prk_asella.pem -pubout
 -out adama/pubk_asella.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested Certificate

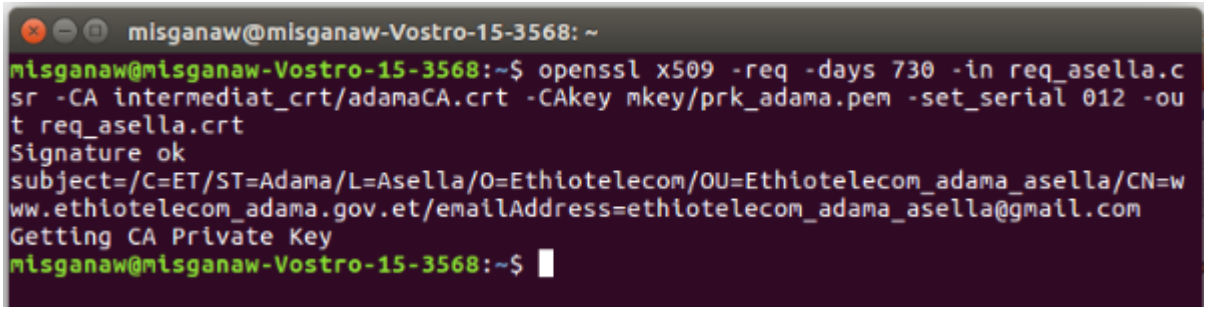
After having private and public key the end user (Asella) can request to Adama intermediate CA for signed certification by adding some extra information that describe the identity of requester (Asella). In this case identity of Asella end user, Asella request using **req_arusi.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key adama/prk_asella.pem -
out req_asella.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Adama
Locality Name (eg, city) []:Asella
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_adama_asella
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_adama.gov.et
Email Address []:ethiotelecom_adama_asella@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321asella
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to Adama intermediate CA, if the required parameter by intermediate CA from end user (Aella) is correct then intermediate CA (Adama CA) will grant signed certificate as follows. Here the delivered certificate is **asella_CA.crt**.



Arusi

Private and public key

The following snip shut indicates the private and public key of Arusi end user before requesting intermediate CA (Adama CA) for signed certificate. This is **prk_arusi.pem** and **pubk_arusi.pem** respectively.

Requested certificate

After having private and public key the end user (Arusi) can request to Adama intermediate CA for signed certification by adding some extra information that describe the identity of requester (Arusi). In this case identity of Arusi end user, Arusi request using **req_arusi.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key adama/prk_arusi.pem -o
ut req_arusi.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Adama
Locality Name (eg, city) []:Arusi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethitelecom_adama_asella
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_adama.gov.et
Email Address []:ethiotelecom_adama_arusi@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321arusi
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Singed certificate

After requesting for signed certification to Adama intermediate CA, if the required parameter by intermediate CA from end user (Arusi) is correct then intermediate CA (Adama CA) will grant signed certificate as follows. Here the delivered certificate is **arusi_CA.crt**.

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_arusi.cs
r -CA intermediat_crt/adamaCA.crt -CAkey mkey/prk_adama.pem -set_serial 013 -out
 req_arusi.crt
Signature ok
subject=/C=ET/ST=Adama/L=Arusi/O=Ethiotelecom/OU=Ethitelecom_adama_asella/CN=www
.ethiotelecom_adama.gov.et/emailAddress=ethiotelecom_adama_arusi@gmail.com
Getting CA Private Key
```

Woliso

Private and public key

The following snip shut indicates the private and public key of Woliso end user before requesting intermediate CA (Adma CA) for signed certificate. This is **prk_woliso.pem** and **pubk_woliso.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out prk_weliso.pem 2048
Generating RSA private key, 2048 bit long modulus
......+++
.....................................................................................
.................+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in prk_weliso.pem -pubout -out pubk_welis
o.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$ writing RSA key
```

Requested certificate

After having private and public key the end user (Woliso) can request to Bahr Dar intermediate CA for signed certification by adding some extra information that describe the identity of requester (Woliso). In this case identity of Woliso end user, Woliso request using **req_woliso.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key adama/prk_woliso.pem -
out req_woliso.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Adama
Locality Name (eg, city) []:Woliso
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_adama_woliso
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_adama.gov.et
Email Address []:ethiotelecom_adama_woliso@gmil.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321woliso
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Singed certificate

After requesting for signed certification to Adama intermediate CA, if the required parameter by intermediate CA from end user (Woliso) is correct then intermediate CA (Adama CA) will grant signed certificate as follows. Here the delivered certificate is **woliso_CA.crt**

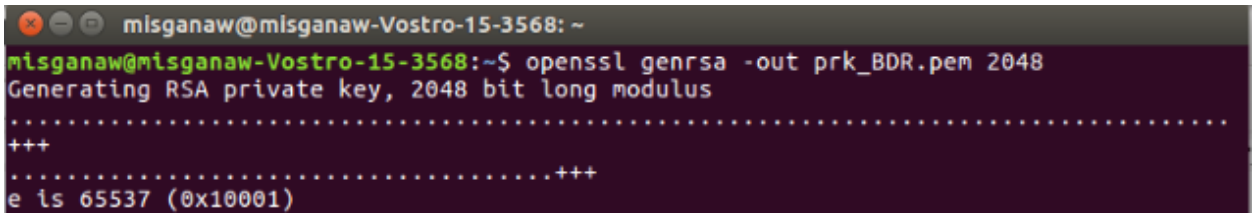
```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_woliso.c
sr -CA intermediat_crt/adamaCA.crt -CAkey mkey/prk_adama.pem -set_serial 014 -ou
t req_woliso.crt
Signature ok
subject=/C=ET/ST=Adama/L=Woliso/O=Ethiotelecom/OU=Ethiotelecom_adama_woliso/CN=w
ww.ethiotelecom_adama.gov.et/emailAddress=ethiotelecom_adama_woliso@gmil.com
Getting CA Private Key
```

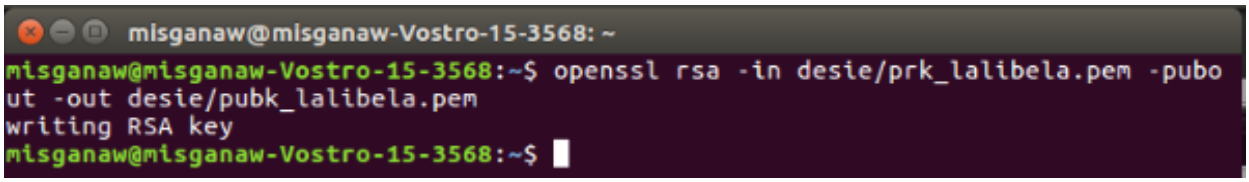
Bahr Dar intermediate CA

This intermediate CA have signed certificate granted from root CA of Addiss Ababa. This intermediate CA has its own branch which is end user such as Gonder, D/Tabor, F/selam, D/markos and D/Birhan . This CA accept requested certificates from each of end user with extra information of end user then handle delivering signed certificate with respect to requested certificate. But if the end user does not trust this intermediate CA it can directly request to root CA which is in this case Addiss CA. for example **Gonder** end user is not request to Adama intermediate CA rather it request to **Addis root CA**.

Private and public key

The following snip shut indicates the private and public key of Bahr Dar intermediate CA before requesting root CA (Addiss) for signed certificate. This is **prk_BDR.pem** and **pubk_BDR.pem** respectively.





Requested certificate

After having private and public key the intermediate CA (Bahr Dar) can request to Addiss CA for signed certification by adding some extra information that describe the identity of requester (Bahr Dar CA). In this case identity of Bahr Dar intermediate CA. Bahr Dar CA request using **req_BDR.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key mkey/prk_BDR.pem -out
req_BDR.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Bahir Dar
Locality Name (eg, city) []:Tana
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_bdr
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom.gov.et
Email Address []:ethiotelecom_bdr@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321misgie
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to addiss root CA, if the required parameter by root CA from intermediate CA (Bahr Dar CA) is correct then root CA (Adiss CA) will grant signed certificate as follows. Here the delivered certificate is **BDR_CA.crt**

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_BDR.csr
-CA addissCA.crt -CAkey mkey/prk_addiss.pem -set_serial 02 -out BDR_CA.crt
Signature ok
subject=/C=ET/ST=Bahir Dar/L=Tana/O=Ethiotelecom/OU=Ethiotelecom_bdr/CN=www.ethi
otelecom.gov.et/emailAddress=ethiotelecom_bdr@gmail.com
Getting CA Private Key
misganaw@misganaw-Vostro-15-3568:~$ clear
```

Bahr Dare end user

Gonder

Private and public key

The following snip shut indicates the private and public key of Gonder end user before requesting intermediate CA (Bahr Dar CA) for signed certificate. This is **prk_bonder.pem** and **pubk_gonder.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out BDR/prk_gonder.pem 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................
.....................................................+++
.....................................................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_lalibela.pem -pubo
ut -out desie/pubk_lalibela.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

The uniqueness of this end user is that, he/she does not request the corresponding intermediate CA (Bahr Dar CA) because she/he does not trust his intermediate CA (Bahr Dar CA). so after having private and public key the end user (Gonder) can request to Addiss Ababa root CA for signed certification by adding some extra information that describe the identity of requester (Gonder). In this case identity of Gonder end user, Gonder request using **req_gonder.csr** as follows on snip shut.

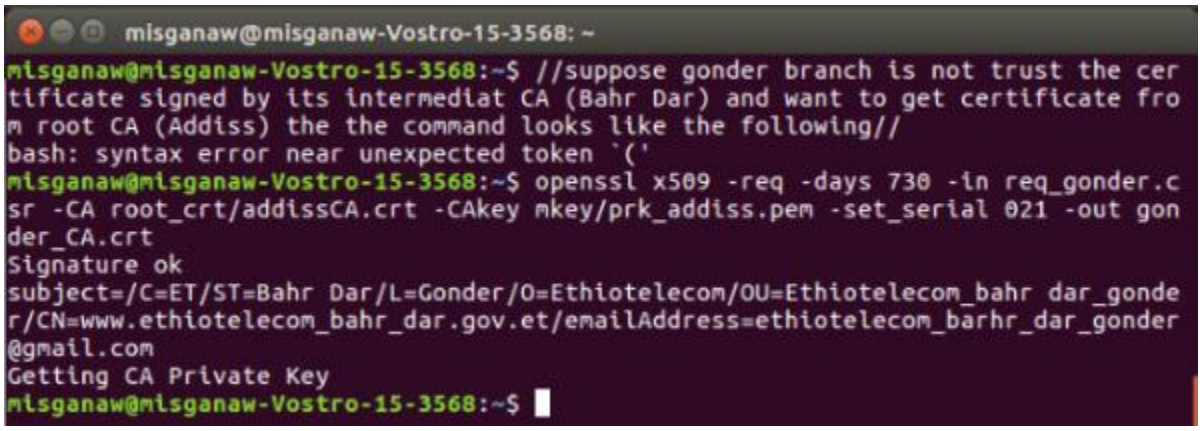
```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key BDR/prk_gonder.pem -ou
t req_gonder.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Bahr Dar
Locality Name (eg, city) []:Gonder
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_bahr dar_gonder
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_bahr_dar.gov.et
Email Address []:ethiotelecom_barhr_dar_gonder@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:#4321gonder
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

Here suppose Gonder end user does not trust the certificate signed by his intermediate CA branch (Bahr Dar CA) and want to get certificate from root CA (Addiss Ababa). The following

snip shut shows that Gonder end user brought signed certificate from root CA (Addiss Ababa) called as **gonder_CA.crt**



Debre Tabor

Private and public key

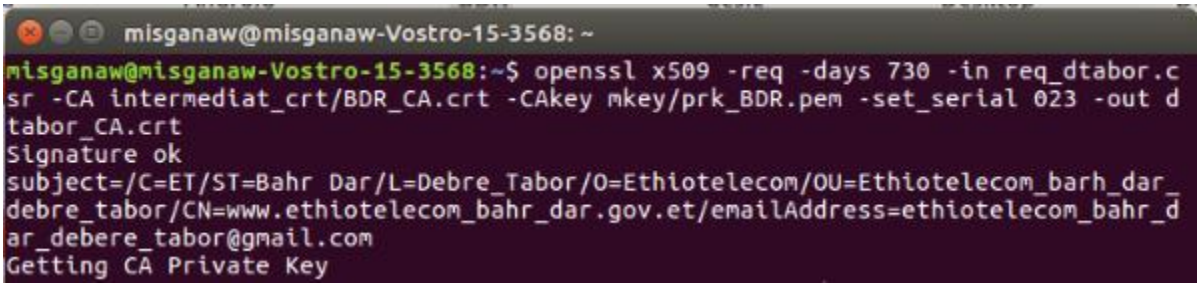
The following snip shut indicates the private and public key of D/Tabor end user before requesting intermediate CA (Bahr Dar CA) for signed certificate. This is **prk_dtabor.pem** and **pubk_dtabor.pem** respectively.

Requested certificate

After having private and public key the end user (D/Tabor) can request to Bahr Dar intermediate CA for signed certification by adding some extra information that describe the identity of requester (D/Tabor). In this case identity of D/Tabor end user, D/Tabor request using **req_dtabor.csr** as follows on snip shut.

Signed certificate

After requesting for signed certification to Bahr Dar intermediate CA, if the required parameter by intermediate CA from end user (D/Tabor) is correct then intermediate CA (Bahr Dar CA) will grant signed certificate as follows. Here the delivered certificate is **dtabor_CA.crt**



Finote Selam

Private and public key

The following snip shut indicates the private and public key of F/Selam end user before requesting intermediate CA (Bahr Dar CA) for signed certificate. This is **prk_fselam.pem** and **pubk_fselam.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~

misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out BDR/prk_fselam.pem 2048
Generating RSA private key, 2048 bit long modulus
.................................+++
.....................+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_lalibela.pem -pubo
ut -out desie/pubk_lalibela.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (F/Selam) can request to Bahr Dar intermediate CA for signed certification by adding some extra information that describe the identity of requester (F/Selam). In this case identity of F/Selam end user, F/Selam request using **req_fselam.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key BDR/prk_fselam.pem -ou
t req_fselam.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Bahr Dar
Locality Name (eg, city) []:Finote Selam
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_bahr_dar_debre_tabor
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_bahr_dar.gov.et
Email Address []:ethiotelecom_bahr_dar_f_selam@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321f_selam
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to Bahr Dar intermediate CA, if the required parameter by intermediate CA from end user (F/Selam) is correct then intermediate CA (Bahr Dar CA) will grant signed certificate as follows. Here the delivered certificate is **fselam_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_fselam.c
sr -CA intermediat_crt/BDR_CA.crt -CAkey mkey/prk_BDR.pem -set_serial 023 -out f
selam_CA.crt
Signature ok
subject=/C=ET/ST=Bahr Dar/L=Finote Selam/O=Ethiotelecom/OU=Ethiotelecom_bahr_dar
_debre_tabor/CN=www.ethiotelecom_bahr_dar.gov.et/emailAddress=ethiotelecom_bahr_
dar_f_selam@gmail.com
Getting CA Private Key
```

Debre Markos

Private and public key

The following snip shut indicates the private and public key of D/Markos end user before requesting intermediate CA (Bahr Dar CA) for signed certificate. This is **prk_dmarkos.pem** and **pubk_dmarkos.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out BDR/prk_dmarkos.pem 2048
Generating RSA private key, 2048 bit long modulus
..............................+++
.....................+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_lalibela.pem -pubo
ut -out desie/pubk_lalibela.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (D/Markos) can request to Bahr Dar intermediate CA for signed certification by adding some extra information that describe the identity of requester (D/Markos). In this case identity of D/Markos end user, D/Markos request using **req_dmarkos.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key BDR/prk_dmarkos.pem -o
ut req_dmarkos.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Bahr Dar
Locality Name (eg, city) []:Debre Markos
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_bahr_dar_debre_markos
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_bahr_dare.gov.et
Email Address []:ethiotelecom_bahr_dar_dmarkos@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321dmarkos
An optional company name []:
```

Signed certificate

After requesting for signed certification to Bahr Dar intermediate CA, if the required parameter by intermediate CA from end user (D/Markos) is correct then intermediate CA (Bahr Dar CA) will grant signed certificate as follows. Here the delivered certificate is **dmarkos_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_dmarkos.
csr -CA intermediat_crt/BDR_CA.crt -CAkey mkey/prk_BDR.pem -set_serial 024 -out
dmarkos_CA.crt
Signature ok
subject=/C=ET/ST=Bahr Dar/L=Debre Markos/O=Ethiotelecom/OU=Ethiotelecom_bahr_dar
_debre_markos/CN=www.ethiotelecom_bahr_dare.gov.et/emailAddress=ethiotelecom_bah
r_dar_dmarkos@gmail.com
Getting CA Private Key
```

Debre Birhan

Private and public key

The following snip shut indicates the private and public key of D/Birhan end user before requesting intermediate CA (Bahr Dar CA) for signed certificate. This is **prk_dbirhan.pem** and **pubk_dbirhan.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out BDR/prk_dbirhan.pem 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.....................................................+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_lalibela.pem -pubo
ut -out desie/pubk_lalibela.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (D/Birhan) can request to Bahr Dar intermediate CA for signed certification by adding some extra information that describe the identity of requester (D/Birhan). In this case identity of D/Birhan end user, D/Birhan request using **req_dbirhan.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key BDR/prk_dbirhan.pem -o
ut req_dbirhan.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Bahr Dar
Locality Name (eg, city) []:Debre Birhan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_bahr_dar_debere_birhan
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_bahr_dar.gov.et
Email Address []:ethiotelecom_bahr_dar_debere_birhan@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321dbirhan
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to Bahr Dar intermediate CA, if the required parameter by intermediate CA from end user (D/Birhan) is correct then intermediate CA (Bahr Dar CA) will grant signed certificate as follows. Here the delivered certificate is **dbirhan_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_dbirhan.
csr -CA intermediat_crt/BDR_CA.crt -CAkey mkey/prk_BDR.pem -set_serial 025 -out
dbirhan_CA.crt
Signature ok
subject=/C=ET/ST=Bahr Dar/L=Debre Birhan/O=Ethiotelecom/OU=Ethiotelecom_bahr_dar
_debere_birhan/CN=www.ethiotelecom_bahr_dar.gov.et/emailAddress=ethiotelecom_bah
r_dar_debere_birhan@gmail.com
Getting CA Private Key
misganaw@misganaw-Vostro-15-3568:~$
```

Desie intermediate CA

This intermediate CA have signed certificate (**desie_CA.crt**) granted from root CA of Addiss Ababa. This intermediate CA has its own branch which is end user such as Afar, Alamata, Lalibela and Woldya. This CA accept requested certificates from each of end user with extra information of end user then handle delivering signed certificate with respect to requested certificate.

Private and public key

The following snip shut indicates the private and public key of Desie intermediate CA before requesting root CA (Addiss) for signed certificate. This is **prk_desie.pem** and **pubk_desie.pem** respectively.

Requested certificate

After having private and public key the intermediate CA (Desie) can request to Addiss CA for signed certification by adding some extra information that describe the identity of requester (Desie CA). In this case identity of Desie intermediate CA, Desie CA request using **req_desie.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key mkey/prk_desie.pem -ou
t req_dessie.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Desie
Locality Name (eg, city) []:Desie
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_desie
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom.gov.et
Email Address []:ethioteelecom_desie@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321misgie
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to addiss root CA, if the required parameter by root CA from intermediate CA (Desie CA) is correct then root CA (Adiss CA) will grant signed certificate as follows. Here the delivered certificate is **desie_CA.crt**

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_dessie.c
sr -CA addissCA.crt -CAkey mkey/prk_addiss.pem -set_serial 03 -out desie_CA.crt
Signature ok
subject=/C=ET/ST=Desie/L=Desie/O=Ethiotelecom/OU=Ethiotelecom_desie/CN=www.ethio
telecom.gov.et/emailAddress=ethioteelecom_desie@gmail.com
Getting CA Private Key
misganaw@misganaw-Vostro-15-3568:~$
```

Desie end user

Afar

Private and public key

The following snip shut indicates the private and public key of Afar end user before requesting intermediate CA (Desie CA) for signed certificate. This is **prk_afar.pem** and **pubk_afar.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out desie/prk_afar.pem 2048
Generating RSA private key, 2048 bit long modulus
.................+++
.....................................................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_afar.pem -pubout -
out desie/pubk_afar.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Afar) can request to Desie intermediate CA for signed certification by adding some extra information that describe the identity of requester (AFAR). In this case identity of Afar end user, Afar request using **req_afar.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key desie/prk_afar.pem -ou
t req_afar.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Desie
Locality Name (eg, city) []:Semera
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_Desie_Semara
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_desie.gov.et
Email Address []:ethiotelecom_desie_semer@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321semera
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

After requesting for signed certification to Desie intermediate CA, if the required parameter by intermediate CA from end user (Afar) is correct then intermediate CA (Desie CA) will grant signed certificate as follows. Here the delivered certificate is **afar_CA.crt**

```
misganaw@misganaw-Vostro-15-3568: ~

misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_afar.csr
 -CA intermediat_crt/desie_CA.crt -CAkey mkey/prk_desie.pem -set_serial 031 -out
 afar_CA.crt
Signature ok
subject=/C=ET/ST=Desie/L=Semera/O=Ethiotelecom/OU=Ethiotelecom_Desie_Semara/CN=w
ww.ethiotelecom_desie.gov.et/emailAddress=ethiotelecom_desie_semer@gmail.com
Getting CA Private Key
```

Alamata

Private and public key

The following snip shut indicates the private and public key of Alamata end user before requesting intermediate CA (Desie CA) for signed certificate. This is **prk_alamata.pem** and **pubk_alamata.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out desie/prk_alamata.pem 20
48
Generating RSA private key, 2048 bit long modulus
.....................................................................
.............+++
.+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_lalibela.pem -pubo
ut -out desie/pubk_lalibela.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Alamata) can request to Desie intermediate CA for signed certification by adding some extra information that describe the identity of requester (Alamata). In this case identity of Alamata end user, Alamata request using **req_alamata.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key desie/prk_alamata.pem
-out req_alamata.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Desie
Locality Name (eg, city) []:Alamata
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_desie_alamata
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_desie.gov.et
Email Address []:ethiotelecom_desie_alamata@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321alamata
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

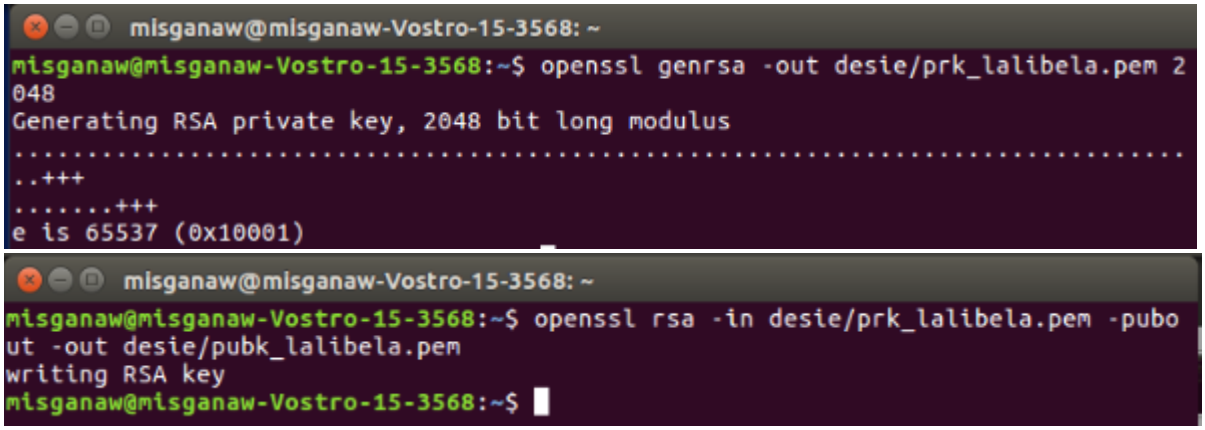
After requesting for signed certification to Desie intermediate CA, if the required parameter by intermediate CA from end user (Alamata) is correct then intermediate CA (Desie CA) will grant signed certificate as follows. Here the delivered certificate is **alamata_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_alamata.
csr -CA intermediat_crt/desie_CA.crt -CAkey mkey/prk_desie.pem -set_serial 031 -
out alamata_CA.crt
Signature ok
subject=/C=ET/ST=Desie/L=Alamata/O=Ethiotelecom/OU=Ethiotelecom_desie_alamata/CN
=www.ethiotelecom_desie.gov.et/emailAddress=ethiotelecom_desie_alamata@gmail.com
Getting CA Private Key
```

Lalibella

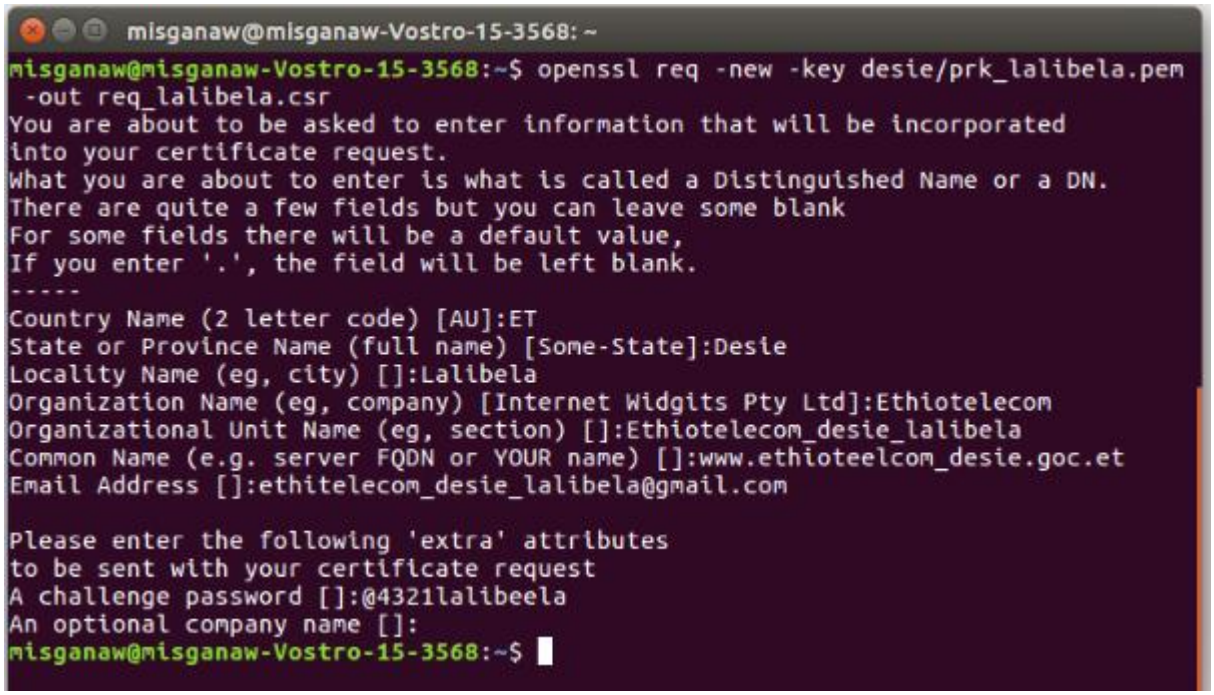
Private and public key

The following snip shut indicates the private and public key of Lalibela end user before requesting intermediate CA (Desie CA) for signed certificate. This is **prk_lalibela.pem** and **pubk_lalibela.pem** respectively.



Requested certificate

After having private and public key the end user (Lalibela) can request to Desie intermediate CA for signed certification by adding some extra information that describe the identity of requester (Lalibela). In this case identity of Lalibela end user, Lalibela request using **req_lalibela.csr** as follows on snip shut.



Signed certificate

After requesting for signed certification to Desie intermediate CA, if the required parameter by intermediate CA from end user (Lalibela) is correct then intermediate CA (Desie CA) will grant signed certificate as follows. Here the delivered certificate is **lalibela_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_lalibela
.csr -CA intermediat_crt/desie_CA.crt -CAkey mkey/prk_desie.pem -set_serial 031
-out lalibela_CA.crt
Signature ok
subject=/C=ET/ST=Desie/L=Lalibela/O=Ethiotelecom/OU=Ethiotelecom_desie_lalibela/
CN=www.ethioteelcom_desie.goc.et/emailAddress=ethitelecom_desie_lalibela@gmail.c
om
Getting CA Private Key
```

Woldya

Private and public key

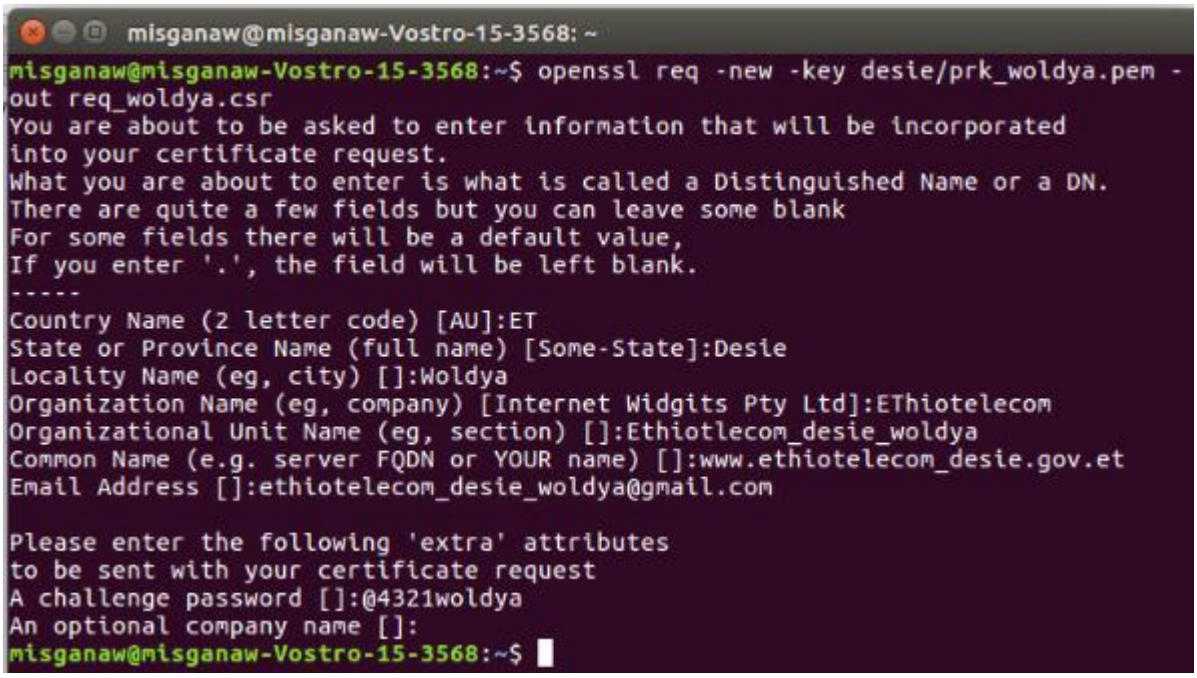
The following snip shut indicates the private and public key of Woldya end user before requesting intermediate CA (Desie CA) for signed certificate. This is **prk_woldya.pem** and **pubk_woldya.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out desie/prk_woldya.pem 204
8
Generating RSA private key, 2048 bit long modulus
.......+++
.....................................................................+++
e is 65537 (0x10001)
```

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in desie/prk_woldya.pem -pubout
 -out desie/pubk_woldy.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Woldya) can request to Desie intermediate CA for signed certification by adding some extra information that describe the identity of requester (Woldya). In this case identity of Woldya end user, Woldya request using **req_woldya.csr** as follows on snip shut.



Signed certificate

After requesting for signed certification to Desie intermediate CA, if the required parameter by intermediate CA from end user (Woldya) is correct then intermediate CA (Desie CA) will grant signed certificate as follows. Here the delivered certificate is **woldya_CA.crt**

Hawassa intermediate CA

This intermediate CA have signed certificate (**hawassa_CA.crt**) granted from root CA of Addiss Ababa. This intermediate CA has its own branch which is end user such as Dilla, Wolkitie and Welayta. This CA accept requested certificates from each of end user with extra information of end user then handle delivering signed certificate with respect to requested certificate.

Private and public key

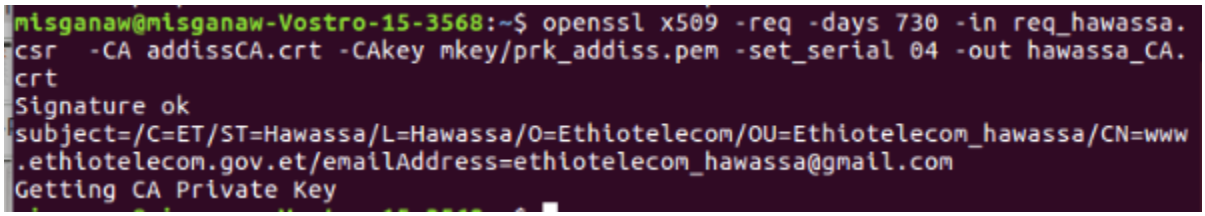
The following snip shut indicates the private and public key of Desie intermediate CA before requesting root CA (Addiss) for signed certificate. This is **prk_hawassa.pem** and **pubk_hawassa.pem** respectively.

Requested certificate

After having private and public key the intermediate CA (Hawassa) can request to Addiss CA for signed certification by adding some extra information that describe the identity of requester (Hawassa CA). In this case identity of Hawassa intermediate CA, Hawassa CA request using **req_hawassa.csr** as follows on snip shut.

Signed certificate

After requesting for signed certification to addiss root CA, if the required parameter by root CA from intermediate CA (Hawassa CA) is correct then root CA (Adiss CA) will grant signed certificate as follows. Here the delivered certificate is **hawassa_CA.crt**



Hawassa end user

Dilla

Private and public key

The following snip shut indicates the private and public key of Dilla end user before requesting intermediate CA (Hawassa CA) for signed certificate. This is **prk_dilla.pem** and **pubk_dilla.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out hawassa/prk_dilla.pem 20
48
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.........................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in hawassa/prk_dilla.pem -pubou
t -out hawassa/pubk_dilla.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Dilla) can request to Hawassa intermediate CA for signed certification by adding some extra information that describe the identity of requester (Dilla). In this case identity of Dilla end user, Dilla request using **req_dilla.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key hawassa/prk_dilla.pem
-out req_dilla.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Hawassa
Locality Name (eg, city) []:Dilla
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_hawassa_dilla
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_hawassa.gov.et
Email Address []:ethiotelecom_hawassa_dilla@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321dilla
An optional company name []:
```

Signed certificate

After requesting for signed certification to Hawassa intermediate CA, if the required parameter by intermediate CA from end user (Dilla) is correct then intermediate CA (Hawassa CA) will grant signed certificate as follows. Here the delivered certificate is **dilla_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_dilla.cs
r -CA intermediat_crt/hawassa_CA.crt -CAkey mkey/prk_hawassa.pem -set_serial 043
 -out dilla_CA.crt
Signature ok
subject=/C=ET/ST=Hawassa/L=Dilla/O=Ethiotelecom/OU=Ethiotelecom_hawassa_dilla/CN
=www.ethiotelecom_hawassa.gov.et/emailAddress=ethiotelecom_hawassa_dilla@gmail.c
om
Getting CA Private Key
```

Wolkitie

Private and public key

The following snip shut indicates the private and public key of Wolkitie end user before requesting intermediate CA (Hawassa CA) for signed certificate. This is **prk_wolkitie.pem** and **pubk_wolkitie.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out hawassa/prk_wolkitie.pem
 2048
Generating RSA private key, 2048 bit long modulus
.....................................+++
.....................................................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in hawassa/prk_wolkitie.pem -pu
bout -out hawassa/pubk_wolkitie.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Wolkitie) can request to Hawassa intermediate CA for signed certification by adding some extra information that describe the identity of requester (Wolkitie). In this case identity of Wolkitie end user, Wolkitie request using **req_wolkitie.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key hawassa/prk_wolkitie.p
em -out req_wolkite.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Hawassa
Locality Name (eg, city) []:Wolkitie
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_hawassa_wolkitie
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_hawassa.gov.et
Email Address []:ethiotelecom_hawassa_wolkitie@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321wolkitie
An optional company name []:
```

Signed certificate

After requesting for signed certification to Hawassa intermediate CA, if the required parameter by intermediate CA from end user (Wolkitie) is correct then intermediate CA (Hawassa CA) will grant signed certificate as follows. Here the delivered certificate is **wolkitie_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_wolkite.
csr -CA intermediat_crt/hawassa_CA.crt -CAkey mkey/prk_hawassa.pem -set_serial 0
42 -out wolkitie_CA.crt
Signature ok
subject=/C=ET/ST=Hawassa/L=Wolkitie/O=Ethiotelecom/OU=Ethiotelecom_hawassa_wolki
tie/CN=www.ethiotelecom_hawassa.gov.et/emailAddress=ethiotelecom_hawassa_wolkiti
e@gmail.com
Getting CA Private Key
```

Welayta

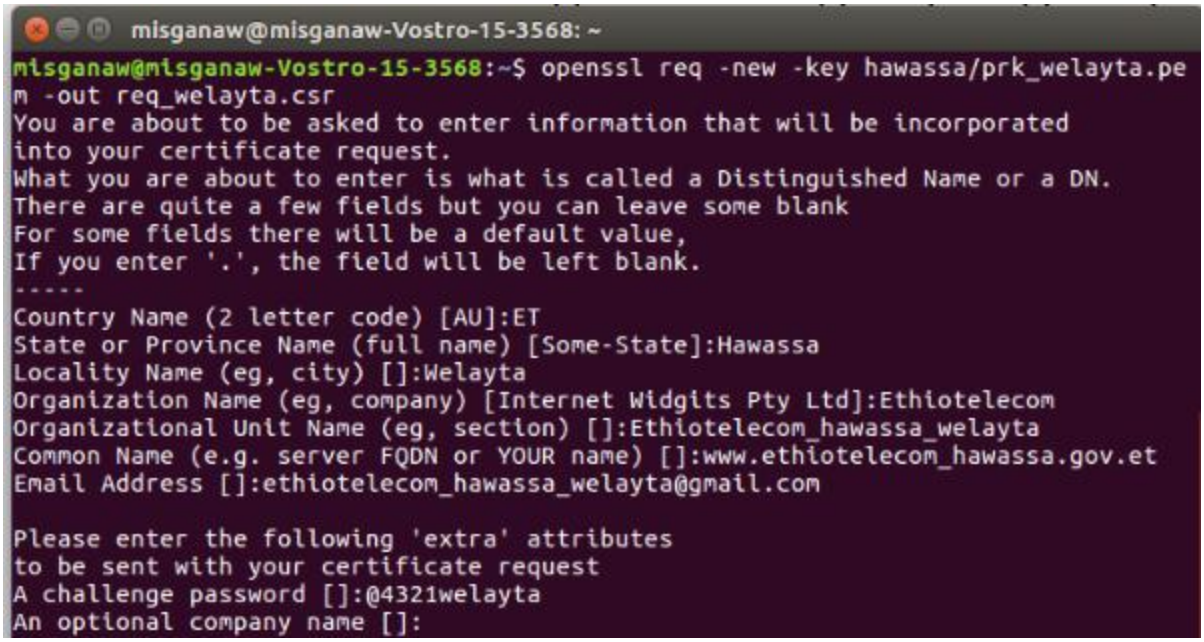
Private and public key

The following snip shut indicates the private and public key of Welayta end user before requesting intermediate CA (Hawassa CA) for signed certificate. This is **prk_welayta.pem** and **pubk_welayta.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out hawassa/prk_welayta.pem
2048
Generating RSA private key, 2048 bit long modulus
.....................................+++
.....................................................................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in hawassa/prk_welayta.pem -pub
out -out hawassa/pubk_welayta.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

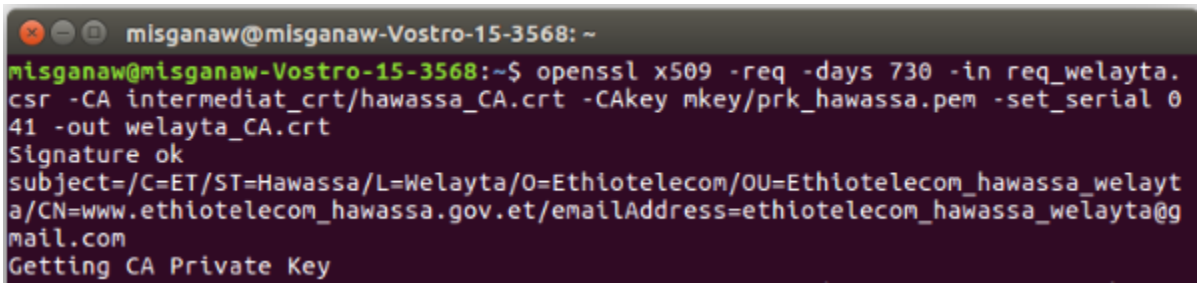
Requested certificate

After having private and public key the end user (Welayta) can request to Hawassa intermediate CA for signed certification by adding some extra information that describe the identity of requester (Welayta). In this case identity of Welayta end user, Welayta request using **req_welayta.csr** as follows on snip shut.



Signed certificate

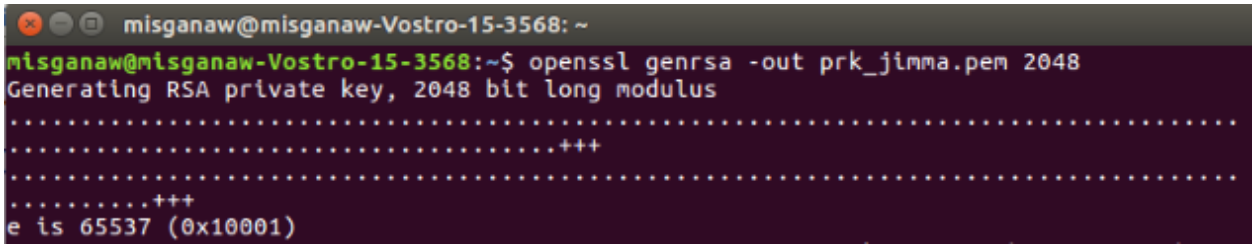
After requesting for signed certification to Hawassa intermediate CA, if the required parameter by intermediate CA from end user (Welayta) is correct then intermediate CA (Hawassa CA) will grant signed certificate as follows. Here the delivered certificate is **welayta_CA.crt**

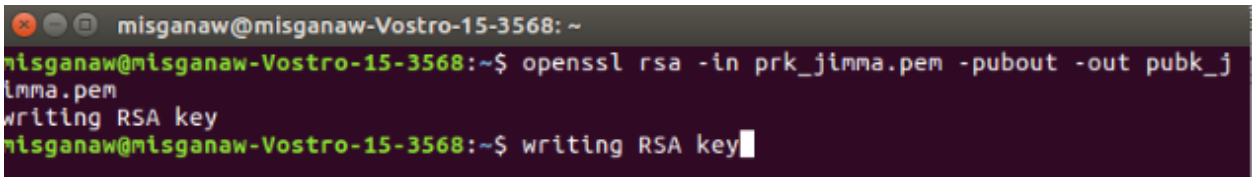


Jimma intermediate CA

Private and public key

The following snip shut indicates the private and public key of Jimma intermediate CA before requesting root CA (Addiss) for signed certificate. This is **prk_jimma.pem** and **pubk_jimma.pem** respectively.





Requested certificate

After having private and public key the intermediate CA (Jimma) can request to Addiss CA for signed certification by adding some extra information that describe the identity of requester (Jimma CA). In this case identity of Jimma intermediate CA, Jimma CA request using **req_jimma.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key mkey/prk_jimma.pem -ou
t req_jimma.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Jimma
Locality Name (eg, city) []:Jimma
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelcom_jimma
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom.gov.et
Email Address []:ethioteleecom_jimma@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321jimma
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$ clear
```

Signed certificate

After requesting for signed certification to addiss root CA, if the required parameter by root CA from intermediate CA (Jimma CA) is correct then root CA (Adiss CA) will grant signed certificate as follows. Here the delivered certificate is **jimma_CA.crt**

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_jimma.cs
r  -CA addissCA.crt -CAkey mkey/prk_addiss.pem -set_serial 04 -out jimma_CA.crt
Signature ok
subject=/C=ET/ST=Jimma/L=Jimma/O=Ethiotelecom/OU=Ethiotelcom_jimma/CN=www.ethiot
elecom.gov.et/emailAddress=ethioteleecom_jimma@gmail.com
Getting CA Private Key
misganaw@misganaw-Vostro-15-3568:~$
```

Jimma end user

Gambella

Private and public key

The following snip shut indicates the private and public key of Gambella end user before requesting intermediate CA (Jimma CA) for signed certificate. This is **prk_gambella.pem** and **pubk_tepy.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out jimma/prk_gambella.pem 2
048
Generating RSA private key, 2048 bit long modulus
.....................................+++
.............................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in jimma/prk_gambella.pem -pubo
ut -out jimma/pubk_gambella.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Gambella) can request to Jimma intermediate CA for signed certification by adding some extra information that describe the identity of requester (Gambella). In this case identity of Gambella end user, Gambella request using **req_gambella.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key jimma/prk_gambella.pem
 -out req_gambella.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:JImma
Locality Name (eg, city) []:Gambella
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_jimma_gambella
Common Name (e.g. server FQDN or YOUR name) []:www.ethitelcom_jimma.gov.et
Email Address []:ethiotelecom_jimma_gambella

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321gambella
An optional company name []:
```

Signed certificate

After requesting for signed certification to Jimma intermediate CA, if the required parameter by intermediate CA from end user (Gambella) is correct then intermediate CA (Jimma CA) will grant signed certificate as follows. Here the delivered certificate is **gambella_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_gambella
.csr -CA intermediat_crt/jimma_CA.crt -CAkey mkey/prk_jimma.pem -set_serial 042
-out gambella_CA.crt
Signature ok
subject=/C=ET/ST=JImma/L=Gambella/O=Ethiotelecom/OU=Ethiotelecom_jimma_gambella/
CN=www.ethitelcom_jimma.gov.et/emailAddress=ethiotelecom_jimma_gambella
Getting CA Private Key
```

Metu

Private and public key

The following snip shut indicates the private and public key of Metu end user before requesting intermediate CA (Jimma CA) for signed certificate. This is **prk_metu.pem** and **pubk_metu.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out jimma/prk_metu.pem 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................................
.....................................................+++
.....................+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in jimma/prk_metu.pem -pubout -
out jimma/pubk_metu.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Metu) can request to Jimma intermediate CA for signed certification by adding some extra information that describe the identity of requester (Metu). In this case identity of Metu end user, Metu request using **req_metu.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key jimma/prk_metu.pem -ou
t req_metu.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:JImma
Locality Name (eg, city) []:Metu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_jimma_metu
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_jimma.gov.et
Email Address []:ethiotelecom_jimma_metu@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321metu
An optional company name []:
```

Signed certificate

After requesting for signed certification to Jimma intermediate CA, if the required parameter by intermediate CA from end user (Metu) is correct then intermediate CA (Jimma CA) will grant signed certificate as follows. Here the delivered certificate is **metu_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_metu.csr
 -CA intermediat_crt/jimma_CA.crt -CAkey mkey/prk_jimma.pem -set_serial 041 -out
 metu_CA.crt
Signature ok
subject=/C=ET/ST=JImma/L=Metu/O=Ethiotelecom/OU=Ethiotelecom_jimma_metu/CN=www.e
thiotelecom_jimma.gov.et/emailAddress=ethiotelecom_jimma_metu@gmail.com
Getting CA Private Key
```

Tepy

Private and public key

The following snip shut indicates the private and public key of Tepy end user before requesting intermediate CA (Jimma CA) for signed certificate. This is **prk_tepy.pem** and **pubk_tepy.pem** respectively.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl genrsa -out jimma/prk_tepy.pem 2048
Generating RSA private key, 2048 bit long modulus
.................................+++
..........+++
e is 65537 (0x10001)
misganaw@misganaw-Vostro-15-3568:~$ openssl rsa -in jimma/prk_tepy.pem -pubout -
out jimma/pubk_tepy.pem
writing RSA key
misganaw@misganaw-Vostro-15-3568:~$
```

Requested certificate

After having private and public key the end user (Tepy) can request to Jimma intermediate CA for signed certification by adding some extra information that describe the identity of requester (Tepy). In this case identity of Tepy end user, Tepy request using **req_tepy.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key jimma/prk_tepy.pem -ou
t req_tepy.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:JImma
Locality Name (eg, city) []:Tepy
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_jimma_tepy
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_jimma.gov.et
Email Address []:ethiotelecom_jimma_tepy@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321tepy
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

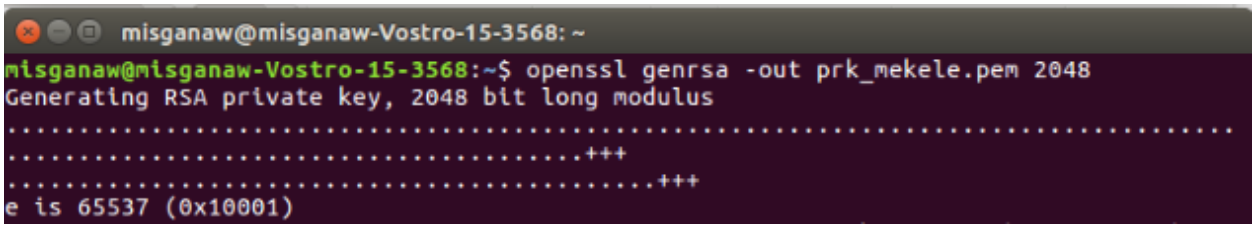
After requesting for signed certification to Jimma intermediate CA, if the required parameter by intermediate CA from end user (Tepy) is correct then intermediate CA (Jimma CA) will grant signed certificate as follows. Here the delivered certificate is **tepy_CA.crt**

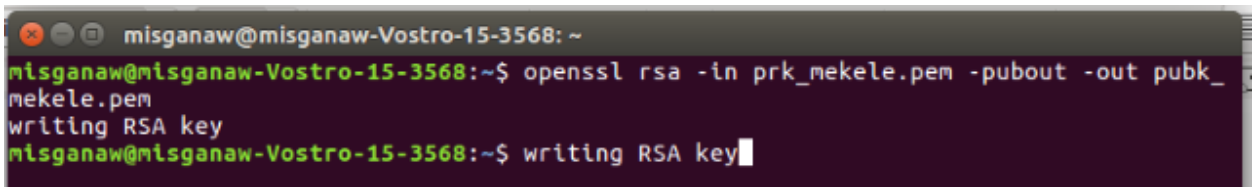
```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_tepy.csr
 -CA intermediat_crt/jimma_CA.crt -CAkey mkey/prk_jimma.pem -set_serial 041 -out
 tepy_CA.crt
Signature ok
subject=/C=ET/ST=JImma/L=Tepy/O=Ethiotelecom/OU=Ethiotelecom_jimma_tepy/CN=www.e
thiotelecom_jimma.gov.et/emailAddress=ethiotelecom_jimma_tepy@gmail.com
Getting CA Private Key
```

Mekele intermediate CA

Private and public key

The following snip shut indicates the private and public key of Mekele intermediate CA before requesting root CA (Addiss) for signed certificate. This is **prk_mekele.pem** and **pubk_mekele.pem** respectively.



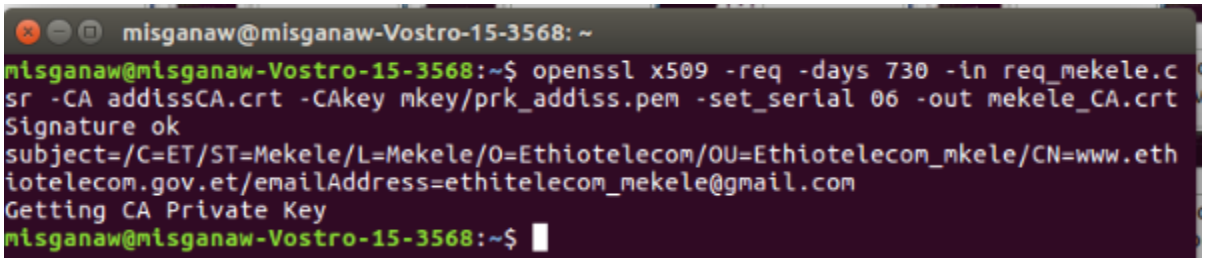


Requested certificate

After having private and public key the intermediate CA (Mekele) can request to Addiss CA for signed certification by adding some extra information that describe the identity of requester (Mekele CA). In this case identity of Mekele intermediate CA, Mekele CA request using **req_mekele.csr** as follows on snip shut.

Signed certificate

After requesting for signed certification to addiss root CA, if the required parameter by root CA from intermediate CA (Mekele CA) is correct then root CA (Adiss CA) will grant signed certificate as follows. Here the delivered certificate is **mekele_CA.crt**



Mekele end user

Adewa

Private and public key

The following snip shut indicates the private and public key of Adewa end user before requesting intermediate CA (Mekele CA) for signed certificate. This is **prk_adewa.pem** and **pubk_adewa.pem** respectively.

Requested certificate

After having private and public key the end user (Adewa) can request to Mekele intermediate CA for signed certification by adding some extra information that describe the identity of requester (Adawa). In this case identity of Adawa end user, Adawa CA request using **req_adawa.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key mekele/prk_adewa.pem -
out req_adawa.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Mekele
Locality Name (eg, city) []:Adawa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethiotelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_mekele_adawa
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_mekele.gov.et
Email Address []:ethiotelecom_mekele_adewa@gmailcom

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321adewa
An optional company name []:
misganaw@misganaw-Vostro-15-3568:~$
```

Signed certificate

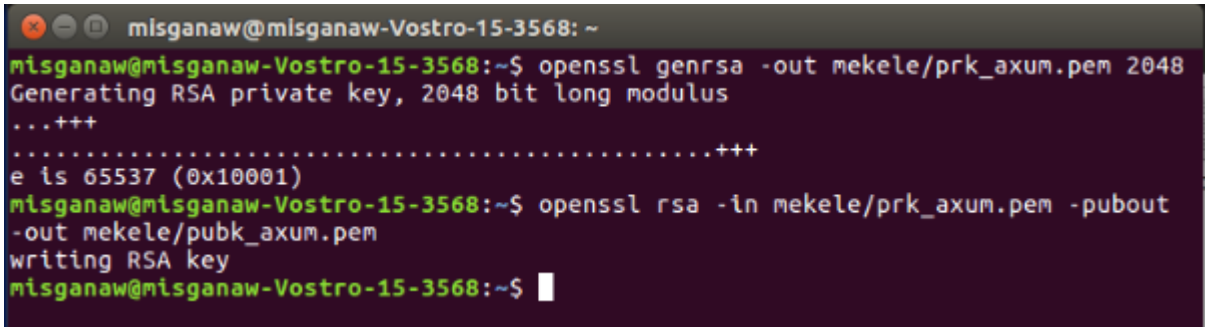
After requesting for signed certification to Mekele intermediate CA, if the required parameter by intermediate CA from end user (Adewa) is correct then intermediate CA (Mekele CA) will grant signed certificate as follows. Here the delivered certificate is **adewa_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_adawa.cs
r -CA intermediat_crt/mekele_CA.crt -CAkey mkey/prk_mekele.pem -set_serial 063 -
out adewa_CA.crt
Signature ok
subject=/C=ET/ST=Mekele/L=Adawa/O=Ethiotelecom/OU=Ethiotelecom_mekele_adawa/CN=w
ww.ethiotelecom_mekele.gov.et/emailAddress=ethiotelecom_mekele_adewa@gmailcom
Getting CA Private Key
```

Axum

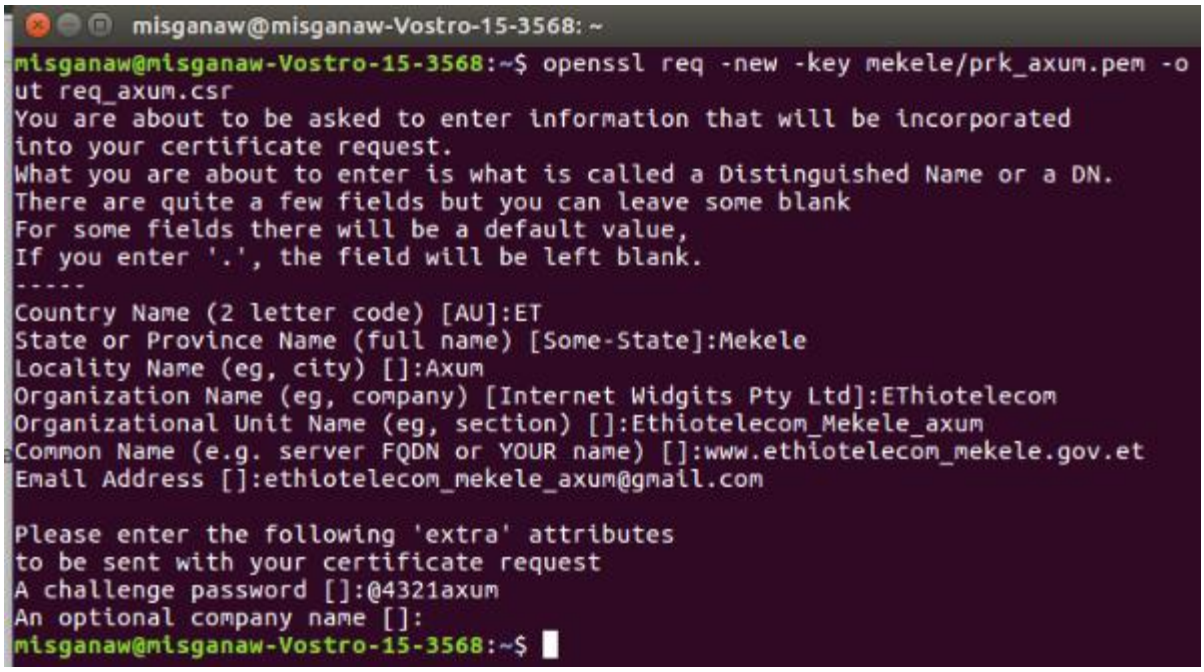
Private and public key

The following snip shut indicates the private and public key of Axum end user before requesting intermediate CA (Mekele CA) for signed certificate. This is **prk_axum.pem** and **pubk_axum.pem** respectively.



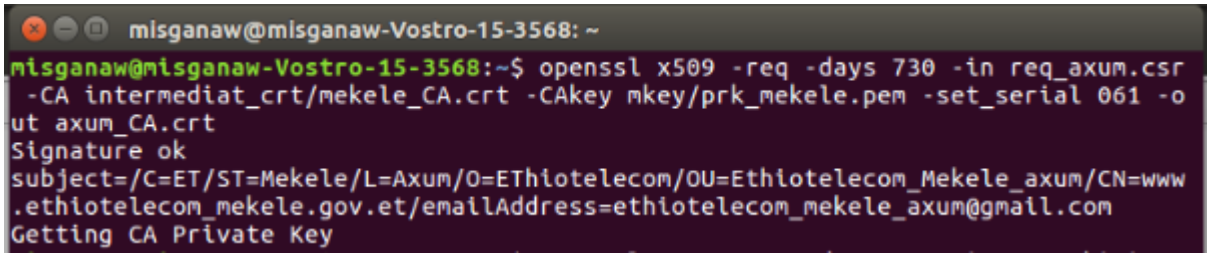
Requested certificate

After having private and public key the end user (Axum) can request to Mekele intermediate CA for signed certification by adding some extra information that describe the identity of requester (Axum). In this case identity of Axum end user, Axum request using **req_shirie.csr** as follows on snip shut.



Signed certificate

After requesting for signed certification to Mekele intermediate CA, if the required parameter by intermediate CA from end user (Axum) is correct then intermediate CA (Mekele CA) will grant signed certificate as follows. Here the delivered certificate is **axum_CA.crt**



Shirie

Private and public key

The following snip shut indicates the private and public key of Shirie end user before requesting intermediate CA (Mekele CA) for signed certificate. This is **prk_shirie.pem** and **pubk_shirie.pem** respectively.

Requested certificate

After having private and public key the end user (Shirie) can request to Mekele intermediate CA for signed certification by adding some extra information that describe the identity of requester (Shirie). In this case identity of Shirie end user, Shirie request using **req_shirie.csr** as follows on snip shut.

```
misganaw@misganaw-Vostro-15-3568: ~
misganaw@misganaw-Vostro-15-3568:~$ openssl req -new -key mekele/prk_shirie.pem
-out req_shirie.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Mekele
Locality Name (eg, city) []:Shirie
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Ethitelecom
Organizational Unit Name (eg, section) []:Ethiotelecom_mekele_shire
Common Name (e.g. server FQDN or YOUR name) []:www.ethiotelecom_mekele.gov.et
Email Address []:ethiotelecom_mekele_shirie@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:@4321shirie
An optional company name []:
```

Signed certificate

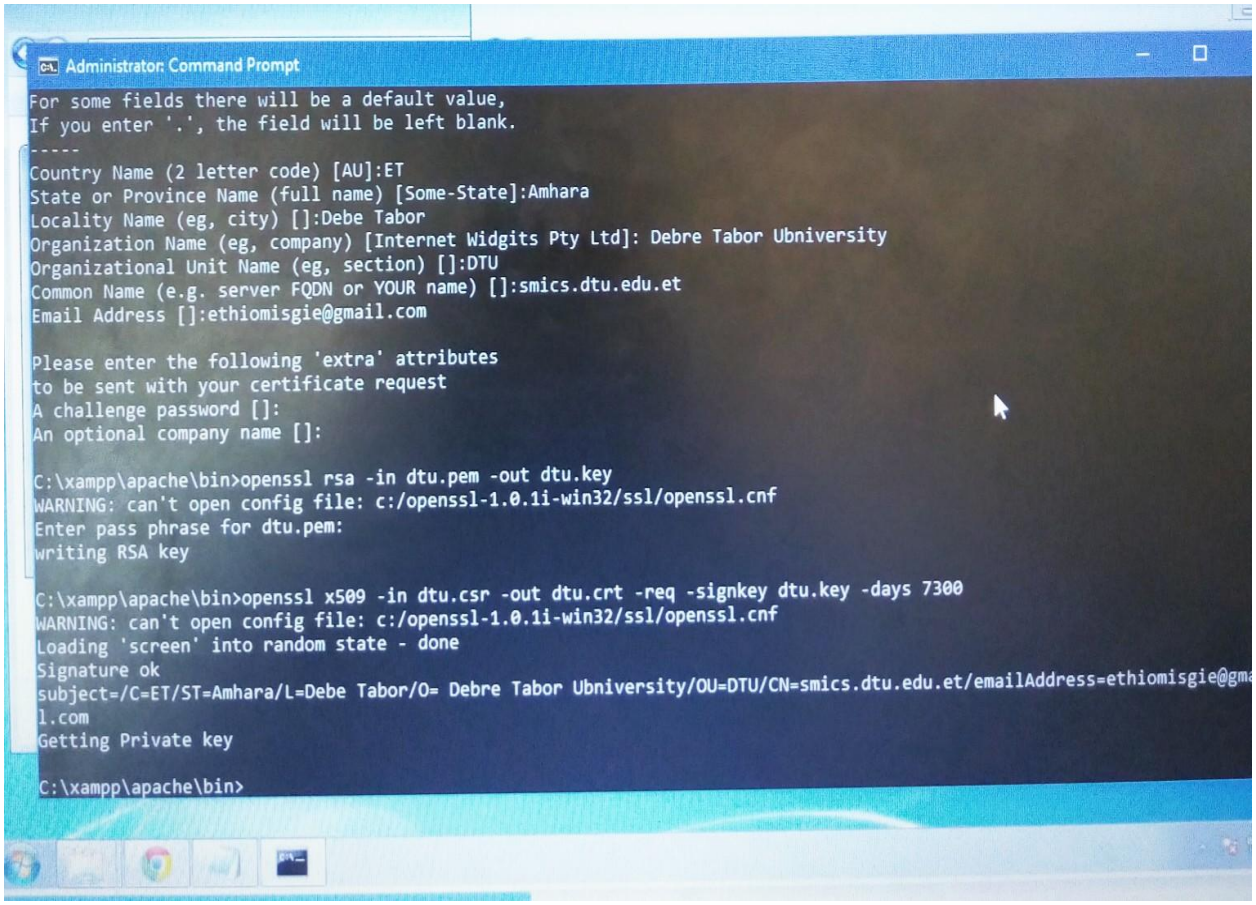
After requesting for signed certification to Mekele intermediate CA, if the required parameter by intermediate CA from end user (Shirie) is correct then intermediate CA (Mekele CA) will grant signed certificate as follows. Here the delivered certificate is **shirie_CA.crt**

```
misganaw@misganaw-Vostro-15-3568:~$ openssl x509 -req -days 730 -in req_shirie.c
sr -CA intermediat_crt/mekele_CA.crt -CAkey mkey/prk_mekele.pem -set_serial 062
-out shire_CA.crt
Signature ok
subject=/C=ET/ST=Mekele/L=Shirie/O=Ethitelecom/OU=Ethiotelecom_mekele_shire/CN=w
ww.ethiotelecom_mekele.gov.et/emailAddress=ethiotelecom_mekele_shirie@gmail.com
Getting CA Private Key
```

Tested self signed certificate

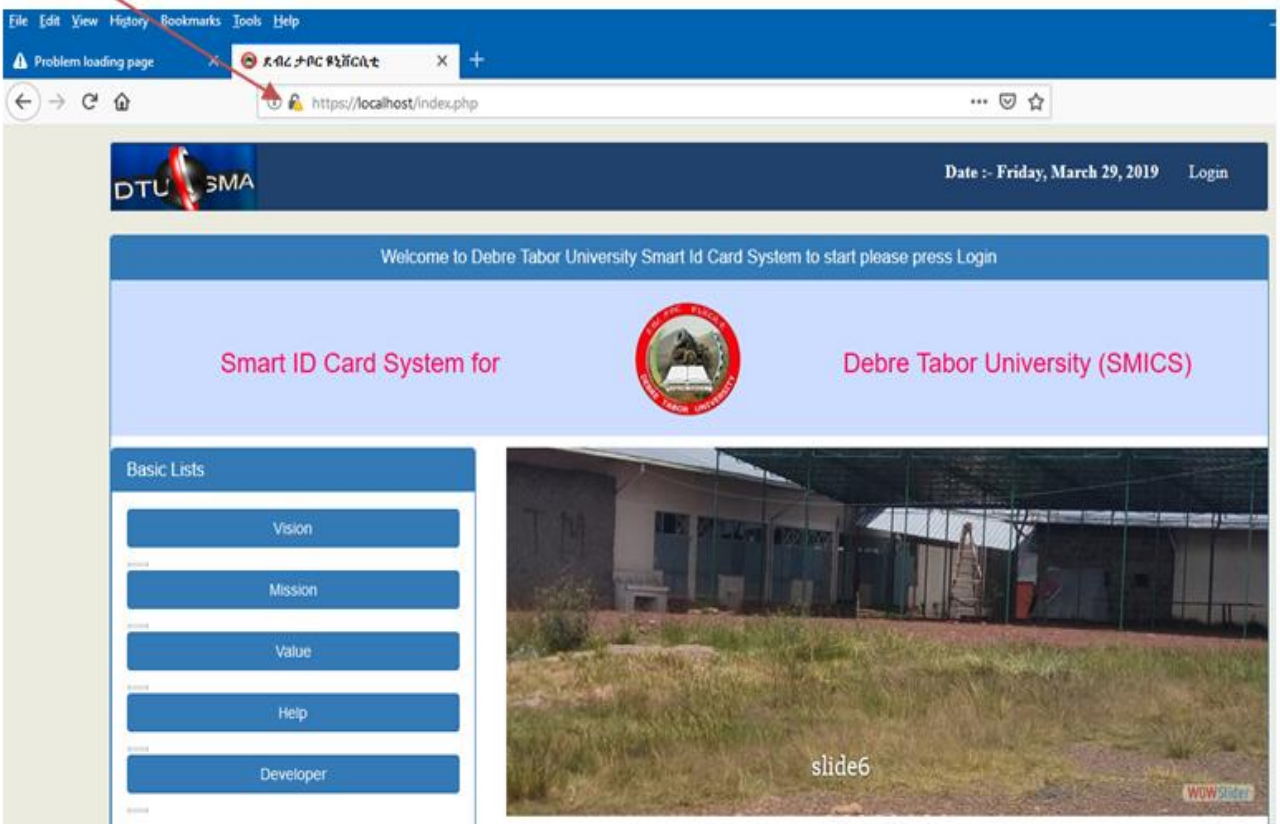
This is the final task to be covered as per our layout at the beginning of the paper. In this scenario we are going to test our self signed certificate created by windows CMD for XAMPP local server for windows.

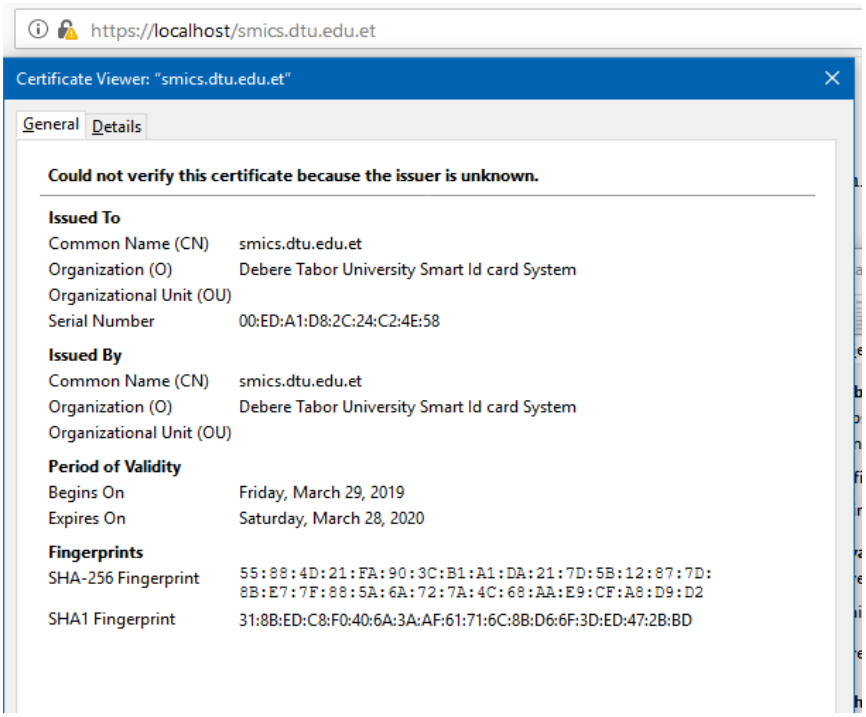
The following snip shut shows self signed certificate created on windows CMD for testing purpose. Remember that the is no difference, we can create this using linux command on UBUNTU.

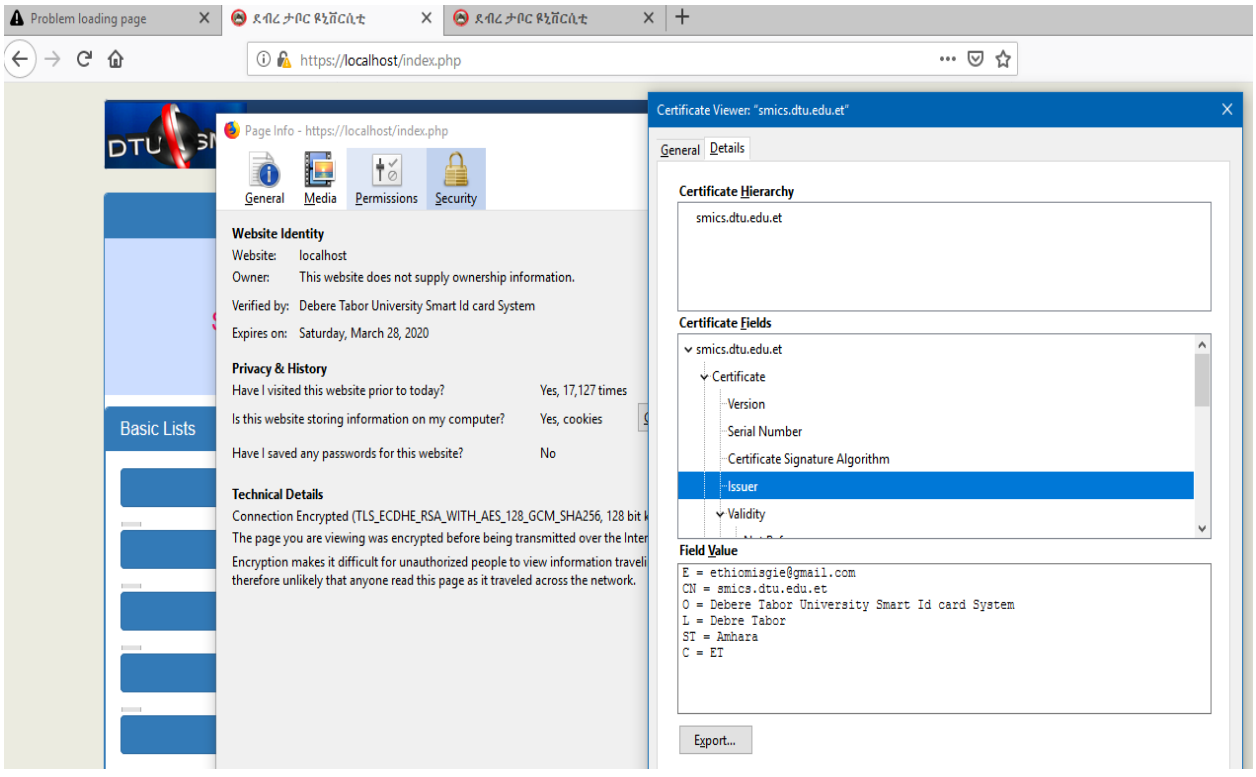

Administrator: Command Prompt
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ET
State or Province Name (full name) [Some-State]:Amhara
Locality Name (eg, city) []:Debe Tabor
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Debre Tabor Ubniversity
Organizational Unit Name (eg, section) []:DTU
Common Name (e.g. server FQDN or YOUR name) []:smics.dtu.edu.et
Email Address []:ethiomisgie@gmail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
C:\xampp\apache\bin>openssl rsa -in dtu.pem -out dtu.key
WARNING: can't open config file: c:/openssl-1.0.1i-win32/ssl/openssl.cnf
Enter pass phrase for dtu.pem:
writing RSA key
C:\xampp\apache\bin>openssl x509 -in dtu.csr -out dtu.crt -req -signkey dtu.key -days 7300
WARNING: can't open config file: c:/openssl-1.0.1i-win32/ssl/openssl.cnf
Loading 'screen' into random state - done
Signature ok
subject=/C=ET/ST=Amhara/L=Debe Tabor/O= Debre Tabor Ubniversity/OU=DTU/CN=smics.dtu.edu.et/emailAddress=ethiomisgie@gma
l.com
Getting Private key
C:\xampp\apache\bin>

The key icon indicates that our self signed certificate is working and there is orange triangle sign with key indicates that there is no third party for the certificate




https://localhost/smics.dtu.edu.et
Certificate Viewer: "smics.dtu.edu.et"
General Details
Could not verify this certificate because the issuer is unknown.
Issued To
Common Name (CN) smics.dtu.edu.et
Organization (O) Debere Tabor University Smart Id card System
Organizational Unit (OU)
Serial Number 00:ED:A1:D8:2C:24:C2:4E:58
Issued By
Common Name (CN) smics.dtu.edu.et
Organization (O) Debere Tabor University Smart Id card System
Organizational Unit (OU)
Period of Validity
Begins On Friday, March 29, 2019
Expires On Saturday, March 28, 2020
Fingerprints
SHA-256 Fingerprint 55:88:4D:21:FA:90:3C:B1:A1:DA:21:7D:5B:12:87:7D:8B:E7:7F:88:5A:6A:72:7A:4C:68:AA:E9:CF:A8:D9:D2
SHA1 Fingerprint 31:8B:ED:C8:F0:40:6A:3A:AF:61:71:6C:8B:D6:6F:3D:ED:47:2B:BD


Problem loading page
https://localhost/index.php
Page Info - https://localhost/index.php
General Media Permissions Security
Website Identity
Website: localhost
Owner: This website does not supply ownership information.
Verified by: Debere Tabor University Smart Id card System
Expires on: Saturday, March 28, 2020
Privacy & History
Have I visited this website prior to today? Yes, 17,127 times
Is this website storing information on my computer? Yes, cookies
Have I saved any passwords for this website? No
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit k
The page you are viewing was encrypted before being transmitted over the Inter
Encryption makes it difficult for unauthorized people to view information travel
therefore unlikely that anyone read this page as it traveled across the network.
Basic Lists
Certificate Viewer: "smics.dtu.edu.et"
General Details
Certificate Hierarchy
smics.dtu.edu.et
Certificate Fields
smics.dtu.edu.et
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Field Value
E = ethiomisgie@gmail.com
CN = smics.dtu.edu.et
O = Debere Tabor University Smart Id card System
L = Debre Tabor
ST = Amhara
C = ET
Export...