

FreeIPA

Let's Encrypt SSL FreeIPA

FreeIPA Kerberos

```
$ sudo kinit admin
Password for admin@COMPUTINGFORGEEKS.COM:

$ sudo klist
Ticket cache: KCM:0
Default principal: admin@COMPUTINGFORGEEKS.COM

Valid starting          Expires                Service principal
08/02/2021 17:42:38    08/03/2021 17:42:31  krbtgt/COMPUTINGFORGEEKS.COM@COMPUTINGFORGEEKS.COM
```

EPEL Cerbot

RHEL Certbot EPEL Certbot Let's Encrypt HTTPS

epel-release

```
$ sudo yum install epel-release
Last metadata expiration check: 1 day, 15:05:30 ago on Tue 27 Jul 2021 10:11:28 PM EAT.
Dependencies resolved.
```

```
=====
Package                               Architecture
Version                               Repository                               Size
=====
Installing:
  epel-release                         noarch
10.el8                                extras                                  8-22 k
```

Transaction Summary

```
=====
=====
Install 1 Package

Total download size: 22 k
Installed size: 32 k
Is this ok [y/N]: y
Downloading Packages:
epel-release-8-
10.el8.noarch.rpm
182 kB/s | 22 kB 00:00
-----
-----
Total
67 kB/s | 22 kB 00:00

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing
:
1/1

Installing      : epel-release-8-
10.el8.noarch
1/1
Running scriptlet: epel-release-8-
10.el8.noarch
1/1
Verifying       : epel-release-8-
10.el8.noarch
1/1

Installed:
epel-release-8-10.el8.noarch

Complete!
```

certbot

```
sudo yum install certbot python3-certbot-apache
```

```
Last metadata expiration check: 0:10:00 ago on Thu 29 Jul 2021 01:17:18 PM EAT.
```

```
Dependencies resolved.
```

```
=====
=====
Package                                Architecture
Version                                Repository                                Size
=====
=====
Installing:
 certbot                                noarch                                1.14.0-
1. el8                                epel                                51 k
 python3-certbot-apache                noarch                                1.14.0-
1. el8                                epel                                143 k
Installing dependencies:
 python3-acme                          noarch                                1.14.0-
1. el8                                epel                                88 k
 python3-certbot                      noarch                                1.14.0-
1. el8                                epel                                391 k
 python3-configargparse               noarch                                0.14.0-
6. el8                                epel                                36 k
 python3-josepy                       noarch                                1.8.0-
1. el8                                epel                                102 k
 python3-parsedatetime                noarch                                2.5-
1. el8                                epel                                79 k
 python3-pyOpenSSL                   noarch                                19.0.0-
1. el8                                appstream                            102 k
 python3-pyrfc3339                   noarch                                1.1-
1. el8                                epel                                19 k
 python3-requests-toolbelt           noarch                                0.9.1-
4. el8                                epel                                91 k
 python3-zope-component               noarch                                4.3.0-
8. el8                                epel                                313 k
 python3-zope-event                  noarch                                4.2.0-
12. el8                               epel                                210 k
 python3-zope-interface              x86_64                                4.6.0-
1. el8                                epel                                158 k
Installing weak dependencies:
 python-josepy-doc                   noarch                                1.8.0-
1. el8                                epel                                22 k
```

Transaction Summary

=====
=====
Install 14 Packages

Total download size: 1.8 M

Installed size: 6.9 M

Is this ok [y/N]: y

certbot

```
$ certbot --version
```

```
certbot 1.14.0
```

Let's Encrypt SSL

FreeIPA

Let's Encrypt SSL

FreeIPA

```
sudo cp -r /var/lib/ipa/certs{,.bak}  
sudo cp -r /var/lib/ipa/private{,.bak}
```

git vim nano

```
sudo yum -y install vim nano
```

1 Let's Encrypt FreeIPA

Let's Encrypt CA

```
sudo su -  
mkdir freeipa-certs  
cd freeipa-certs
```

Let's Encrypt CA

```
CERTS=("isrgrootx1.pem" "isrg-root-x2.pem" "lets-encrypt-r3.pem" "lets-encrypt-e1.pem" "lets-encrypt-r4.pem" "lets-encrypt-e2.pem")
for CERT in "${CERTS[@]}"
do
    curl -o $CERT "https://letsencrypt.org/certs/$CERT"
done
```

Let's Encrypt CA

FreeIPA

```
CERTS=("isrgrootx1.pem" "isrg-root-x2.pem" "lets-encrypt-r3.pem" "lets-encrypt-e1.pem" "lets-encrypt-r4.pem" "lets-encrypt-e2.pem")
for CERT in "${CERTS[@]}"
do
    ipa-cacert-manage install $CERT
done
```

```
Installing CA certificate, please wait
Verified CN=ISRG Root X1,O=Internet Security Research Group,C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
Installing CA certificate, please wait
Verified CN=ISRG Root X2,O=Internet Security Research Group,C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
Installing CA certificate, please wait
Verified CN=R3,O=Let's Encrypt,C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
Installing CA certificate, please wait
Verified CN=E1,O=Let's Encrypt,C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
Installing CA certificate, please wait
Verified CN=R4,O=Let's Encrypt,C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
Installing CA certificate, please wait
Verified CN=E2,O=Let's Encrypt,C=US
CA certificate successfully installed
```

The ipa-cacert-manage command was successful

IPA

```
$ sudo ipa-certupdate
Systemwide CA database updated.
Systemwide CA database updated.
The ipa-certupdate command was successful
```

Let's Encrypt

http80

```
sudo systemctl stop httpd
```

Certbot Let's Encrypt

```
EMAIL="your-email-address"
DOMAIN="idm.example.com"
sudo certbot certonly --standalone --preferred-challenges http --agree-tos -n -d $DOMAIN -m
$EMAIL
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Requesting a certificate for idm.example.com
Performing the following challenges:
http-01 challenge for idm.example.com
Waiting for verification...
Cleaning up challenges
```

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/idm.example.com/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/idm.example.com/privkey.pem
Your certificate will expire on 2021-10-27. To obtain a new or tweaked version of this certificate in the future, simply run certbot again. To non-interactively renew *all* of your certificates, run "certbot renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>
Donating to EFF: <https://eff.org/donate-le>

/etc/letsencrypt/live/idm.example.com

```
$ ls /etc/letsencrypt/live/idm.example.com  
cert.pem chain.pem fullchain.pem privkey.pem README
```

httpd

```
sudo systemctl restart httpd
```

Let's Encrypt SSL FreeIPA Web UI

```
DOMAIN="idm.example.com" # Set correct IdM hostname  
sudo ipa-server-certinstall -w -d /etc/letsencrypt/live/$DOMAIN/privkey.pem  
/etc/letsencrypt/live/$DOMAIN/cert.pem --pin=' '
```

Directory Manager password:

Please restart ipa services after installing certificate (ipactl restart)
The ipa-server-certinstall command was successful

FreeIPA

```
$ sudo ipactl restart  
Restarting Directory Service  
Restarting krb5kdc Service  
Restarting kadmind Service  
Restarting httpd Service  
Restarting ipa-custodia Service  
Restarting pki-tomcatd Service  
Restarting ipa-otpd Service  
ipa: INFO: The ipactl command was successful
```

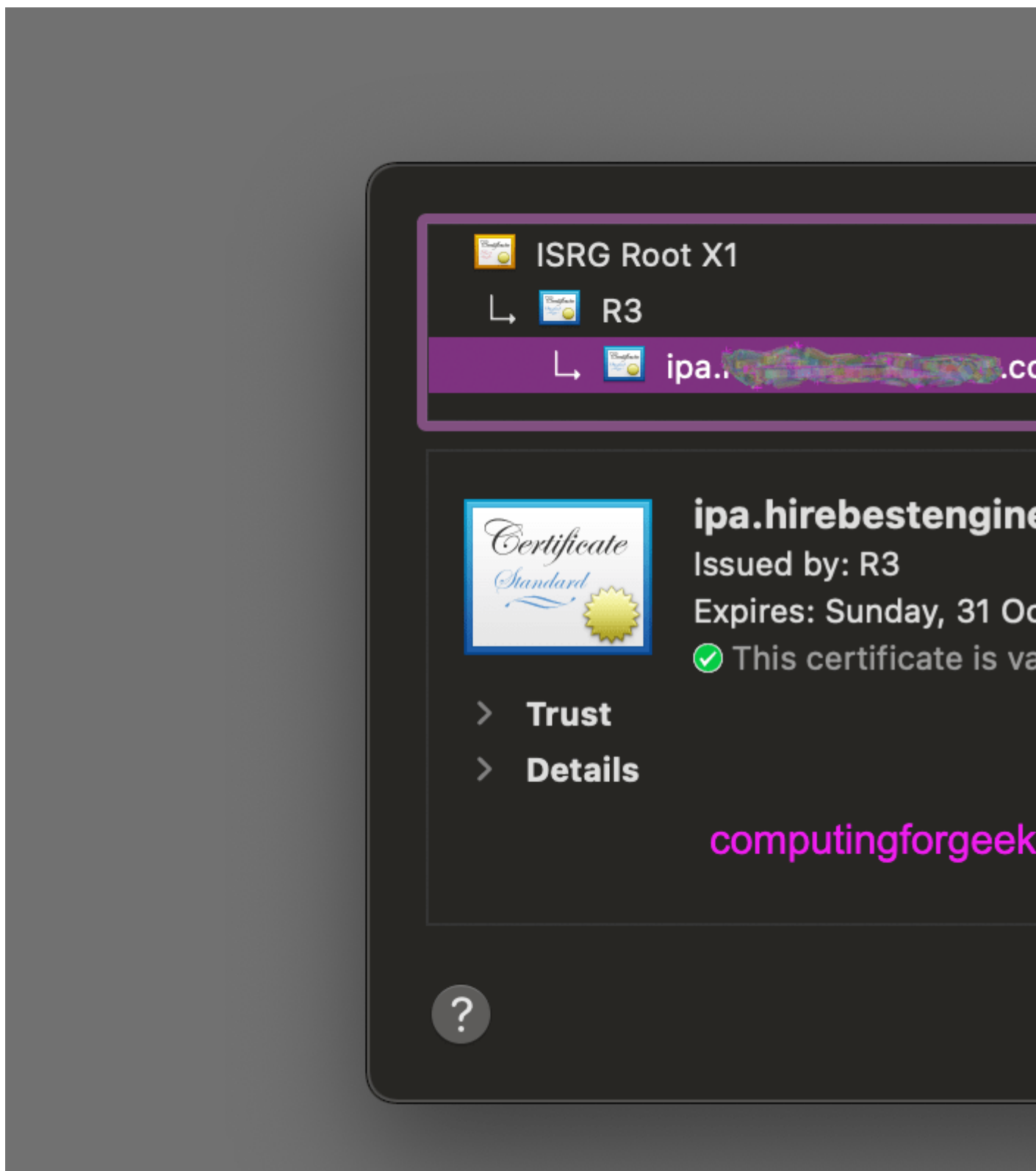
SSL

OpenSSL

```
$ openssl s_client -showcerts -verify 5 -connect $(hostname -f):443
```

```
verify depth is 5
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = idm.example.com
verify return:1
---
Certificate chain
 0 s: CN = idm.example.com
   i: C = US, O = Let's Encrypt, CN = R3
-----BEGIN CERTIFICATE-----
```

Web



2 bash Let's Encrypt FreeIPA

Let's Encrypt FreeIPA Let's Encrypt

```
$ git clone https://github.com/freeipa/freeipa-letsencrypt.git
Cloning into 'freeipa-letsencrypt'...
remote: Enumerating objects: 71, done.
```

```
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 71 (delta 6), reused 13 (delta 4), pack-reused 48
Unpacking objects: 100% (71/71), 18.71 KiB | 299.00 KiB/s, done.
```

```
cd freeipa-letsencrypt
```

```
renew-le.sh EMAIL
```

```
$ vim renew-le.sh
EMAIL="input-your-email-address"
```

```
setup-le.sh    FreeIPA    FQDN
```

```
FQDN=$(hostname -f)
```

```
FQDN
```

```
$ hostname -f
idm.example.com
```

setup-le.sh

```
sudo bash setup-le.sh
```

- Let's Encrypt CA FreeIPA
- FreeIPA

```
...
Installing CA certificate, please wait
Verified CN=R4, O=Let's Encrypt, C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
--2021-07-29 14:46:06-- https://letsencrypt.org/certs/lets-encrypt-e2.pem
Resolving letsencrypt.org (letsencrypt.org)... 34.194.149.67, 68.183.23.220,
2a05:d014:275:cb01:8909:43f0:2069:7b77, ...
Connecting to letsencrypt.org (letsencrypt.org)|34.194.149.67|:443... connected.
GnuTLS: Resource temporarily unavailable, try again.
GnuTLS: Resource temporarily unavailable, try again.
```

```
GnuTLS: Resource temporarily unavailable, try again.
HTTP request sent, awaiting response... 200 OK
Length: 1021 [application/x-pem-file]
Saving to: '/etc/ssl/idm.example.com/lets-encrypt-e2.pem'

/etc/ssl/idm.example.com/lets-
100%[=====>]
1021  --.-KB/s    in 0s

2021-07-29 14:46:06 (13.3 MB/s) - '/etc/ssl/idm.example.com/lets-encrypt-e2.pem' saved
[1021/1021]

Installing CA certificate, please wait
Verified CN=E2,O=Let's Encrypt,C=US
CA certificate successfully installed
The ipa-cacert-manage command was successful
```

httpd

```
sudo systemctl restart httpd
```

ipa-certupdate

```
$ sudo ipa-certupdate
Systemwide CA database updated.
Systemwide CA database updated.
The ipa-certupdate command was successful
```

FreeIPA Let's Encrypt

SSL FreeIPA s

```
DOMAIN="idm.example.com" # Set correct IdM hostname
sudo ipa-server-certinstall -w -d /etc/letsencrypt/live/$DOMAIN/privkey.pem
/etc/letsencrypt/live/$DOMAIN/cert.pem --pin=''
```

Directory Manager password:

The ipa-server-certinstall command was successful

FreeIPA

```
sudo ipactl restart
```

FreeIPA

Let's Encrypt SSL

FreeIPA

SSL

Revision #1

Created 25 July 2022 04:57:59 by

Updated 25 July 2022 05:11:41 by