

FreeIPA XCA DogTag

•
•
• ()
• web-



XCA

- XCA:
 - FreeIPA XCA DogTag
 - OpenVPN XCA
- ..:
- astra-freeipa-server-crt - FreeIPA



:

- Astra Linux Special Edition .10015-01 (1.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12



FreeIPA /etc/ssl/freeipa . , XCA. . , .

- FreeIPA DogTag;
- : IPADOMAIN.RU;
- : SERVER.IPADOMAIN.RU;
- -: REPLICAPADOMAIN.RU.

, . , , DogTag.

, XCA . . XCA:

- «» «».
 - «Use this Certificate for signing» => «rootCA».
 - "[Default] HTTPS_server".
 - ""
- «» («»)
 - () "organizationName" (IPADOMAIN.RU).
 - "commonName" "" () "server.ipadomain.ru", "replica.ipadomain.ru" . .



, SSL , commonName, DNS-

- «» .
 - «» , serverKey.
 - «».
- .
- «» .
 - «» «» («»).
 - "Critical", "Subject Key identifier", "Authority key Identifier".
 - : «» => 5.
 - "X509v3 Subject Alternative Name" (DNS:....) .
 - ("")
- " " .
 - ("x509 v3 Key Usage") :
 - "Critical".
 - ("x509 v3 Key Usage") :
 - "Digital Signature";
 - "Non Repudiation";
 - "Key Encipherment";
 - "Data Encipherment";
 - "Key Agreement".
 - ("x509 v3 Extended Key Usage") :
 - "TLS Web Server Authentication";
 - "KDC Authentication" ("Signing KDC response").
 - :
 - "OCSP Signing" - OCSP;
 - "E-mail protection" - ca-agent.



.



XCA XCA "" - "" () , , .

- ■■■ ■■■■
 ○
 ○ , (,) . :
 , (,) . :

```
i issuerAltName=issuer:copy
subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:kdc_princ_name,
DNS:server.ipadomain.ru

[kdc_princ_name]
realm = EXP:0, GeneralString:IPADOMAIN.RU
principal_name = EXP:1, SEQUENCE:kdc_principal_seq

[kdc_principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:kdc_principals

[kdc_principals]
princ1 = GeneralString:krbtgt
princ2 = GeneralString:IPADOMAIN.RU
```

$$\vdots$$

- Astra Linux Specisl Edition x.7 :

 princ2 = GeneralString:IPADOMAIN.RU

- Astra Linux Special Edition Astra Linux Common Edition:

 princ2 = GeneralString:IPADOMAIN.RU@IPADOMAIN.RU

- "The certificate will be earlier valid than the signer. This is probably not what you want.", "

()

1. XCA .
2. , , XCA.
3. XCA , FreeIPA. :

```
i /etc/ssl/freeipa/ca.crt
```

4. XCA , FreeIPA. :

 /etc/ssl/freeipa/ca.key

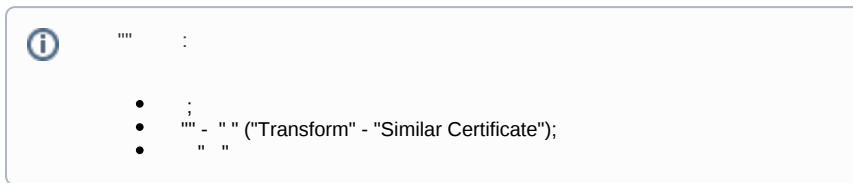
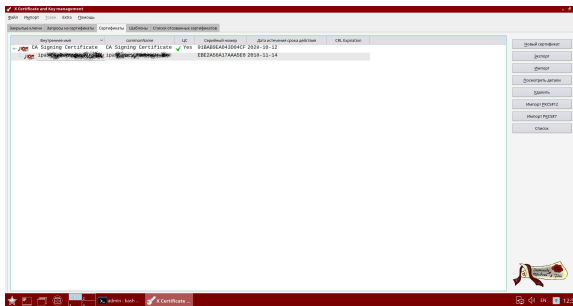
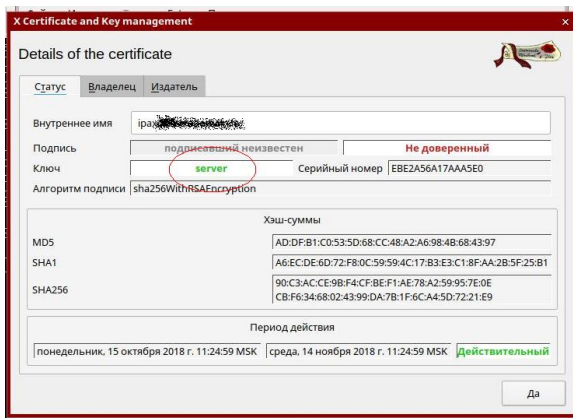
, . .

- ## 5. XCA FreeIPA:

```

i /etc/ssl/freeipa/server.crt
  /etc/ssl/freeipa/server.key

```



- , «» => « » => PKCS12 chain => «»
- => «»

astra-freeipa-server:

```
sudo apt install astra-freeipa-server
```

```
«astra-freeipa-server» -l <_> -lp <_>, :
```

```
sudo astra-freeipa-server -l /root/server.example.com.p12 -lp Password123
```

astra-freeipa-server :

```
astra-freeipa-server --help
```

web-

, web- , XCA, web- XCA. :

1. XCA "PEM (*.crt)";



/etc/ssl/freeipa/ca.crt

2. .
3. web- (web- FireFox):
 - a. ;
 - b. " ";
 - c. "" - " ";
 - d. " " "";
 - e. ;
 - f. "";
 - g. " -";
 - h. "";
 - i. web-.