freeIPA
identity | policy | audit

FreeIPA 3.3 Training Series

Blending FreeIPA in a Certificate Infrastructure

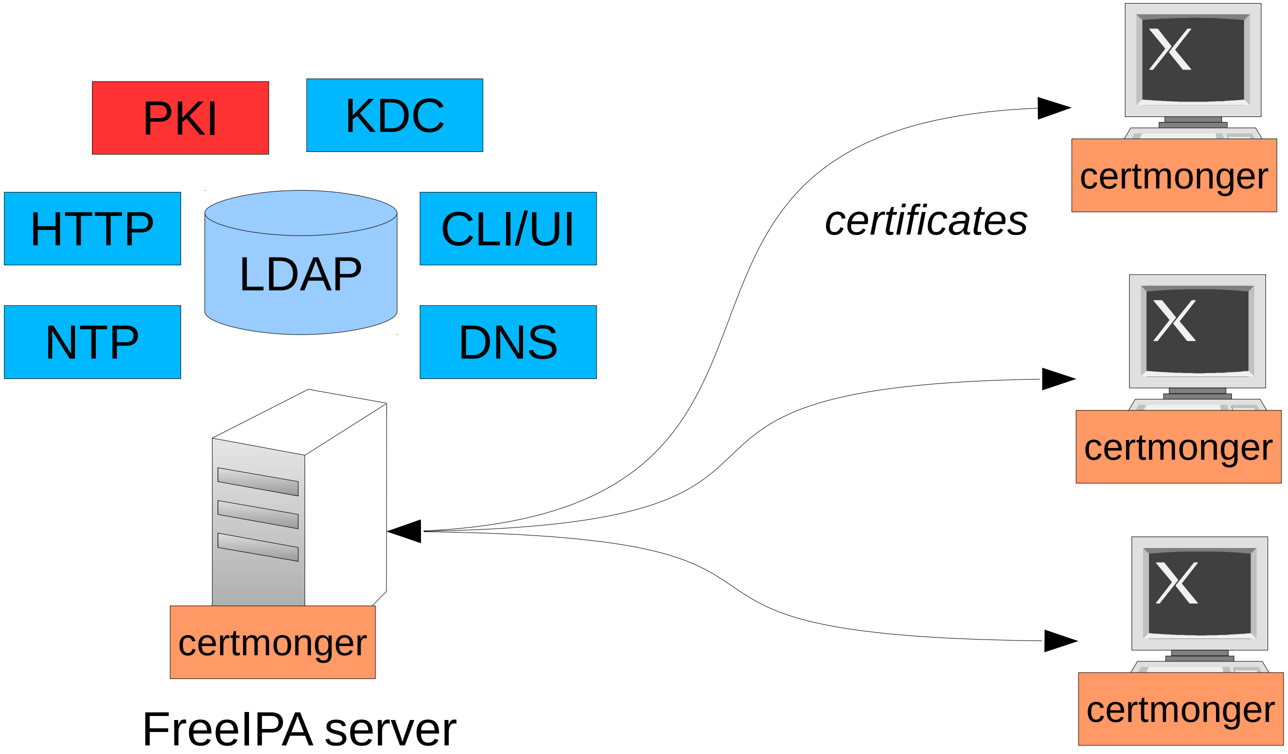
Jan Cholasta

2014-02-18

FreeIPA and PKI (1)

- Some services require certificates for secure communication
- FreeIPA includes CA to issue certificates
  - FreeIPA server certificates
  - Certificates for hosts and services in the FreeIPA domain
- Dogtag certificate system
  - Manages PKI
  - Provides CA for FreeIPA

FreeIPA and PKI (2)



FreeIPA and PKI (3)

- The FreeIPA CA needs to be trusted by all clients
  - So that FreeIPA services can be authenticated
- CA certificate is provided to clients
  - Done during client install

FreeIPA CA variants (1)

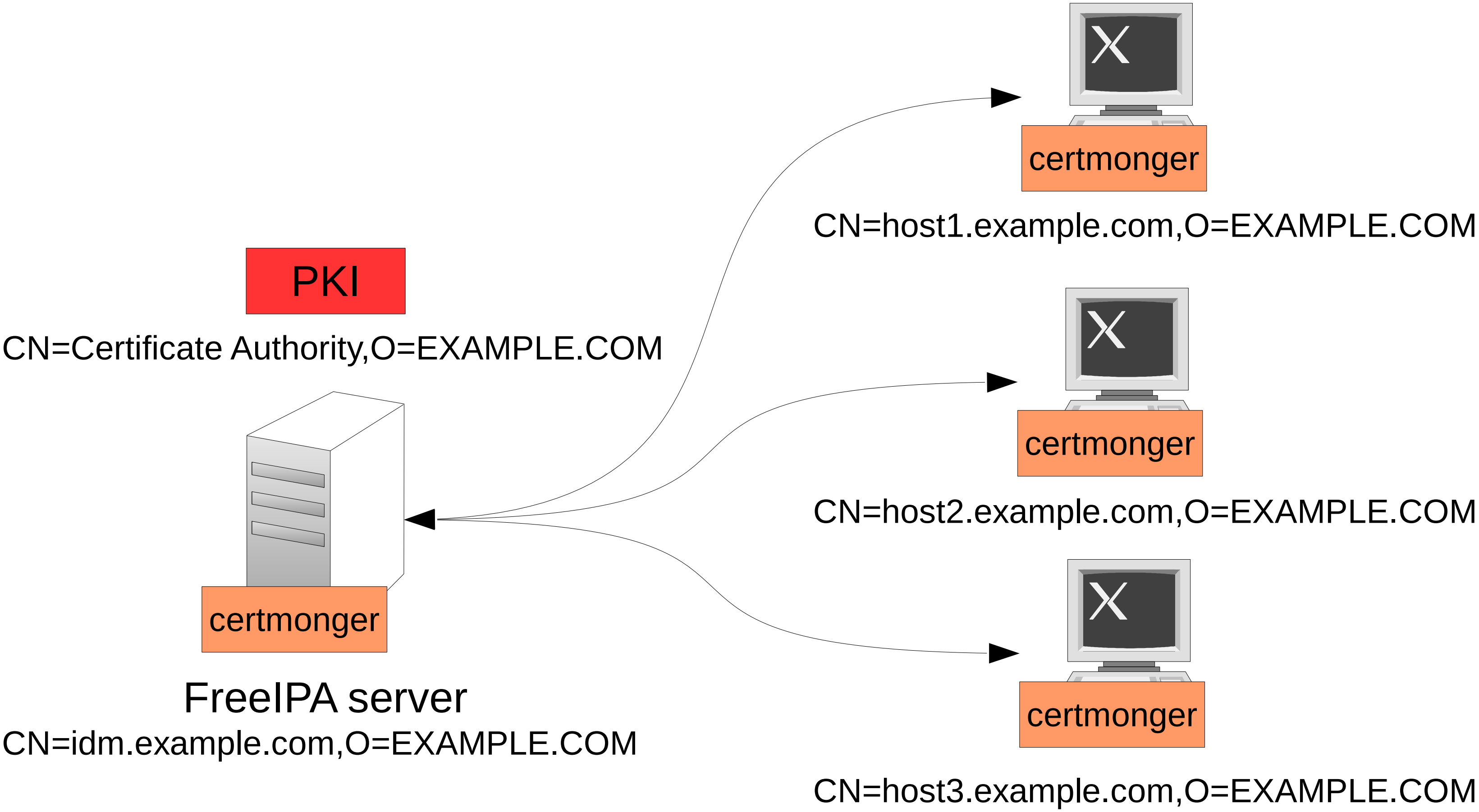
- FreeIPA with managed CA (“CA-ful”)
  - FreeIPA manages the CA
    - Dogtag
  - Two available install options
    - Self-signed – FreeIPA CA is the root CA
    - Externally signed – FreeIPA CA is subordinate of external CA
  - Automatic provisioning and renewal of FreeIPA service certificates

FreeIPA CA variants (2)

- FreeIPA with unmanaged CA (“CA-less”)
  - CA is outside of FreeIPA
    - Can be anything
  - User is in charge of providing and renewing FreeIPA service certificates

FreeIPA Self-Signed CA

FreeIPA Self-Signed CA


PKI
CN=Certificate Authority,O=EXAMPLE.COM
certmonger
FreeIPA server
CN=idm.example.com,O=EXAMPLE.COM
certmonger
CN=host1.example.com,O=EXAMPLE.COM
certmonger
CN=host2.example.com,O=EXAMPLE.COM
certmonger
CN=host3.example.com,O=EXAMPLE.COM

FreeIPA Self-Signed CA Install (1)

- Default install mode
- To install first master, run ipa-server-install without any special options:

```
ipa-server-install
```

FreeIPA Self-Signed CA Install (2)

- To prepare replica, run ipa-replica-prepare without any special options:

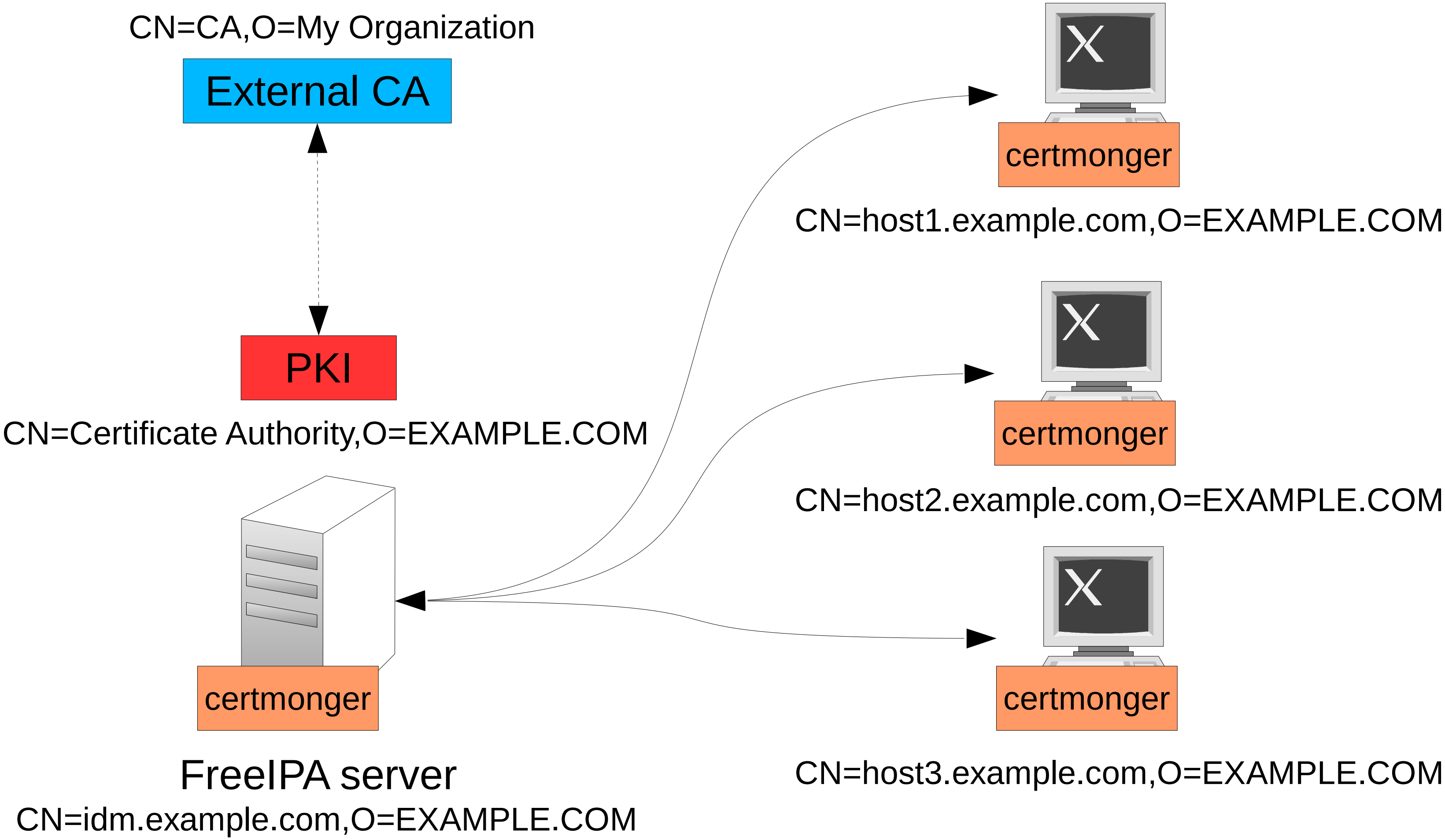
```
ipa-replica-prepare replica.example.com
```

- To install replica, run ipa-replica-install without any special options:

```
ipa-replica-install replica-info-replica.example.com.gpg
```

FreeIPA Externally Signed CA

FreeIPA Externally Signed CA



CN=CA,O=My Organization

External CA

PKI

CN=Certificate Authority,O=EXAMPLE.COM

certmonger

FreeIPA server

CN=idm.example.com,O=EXAMPLE.COM

certmonger

CN=host1.example.com,O=EXAMPLE.COM

certmonger

CN=host2.example.com,O=EXAMPLE.COM

certmonger

CN=host3.example.com,O=EXAMPLE.COM

FreeIPA Externally Signed CA Install (1)

- To install first master:
  - Run ipa-server-install to get FreeIPA CA certificate request:

    ```
    ipa-server-install --external-ca
    ```

    - This will produce a certificate request in /root/ipa.csr
  - Get the certificate request signed by the external CA
    - User is in charge of requesting the certificate
  - Run ipa-server-install to complete the installation:

    ```
    ipa-server-install --external_cert_file /path/to/ipa
    .pem --external_ca_file /path/to/ca.pem
    ```

    - The ca.pem file contains the external CA certificate chain

FreeIPA Externally Signed CA Install (2)

- To prepare replica, run ipa-replica-prepare without any special options:

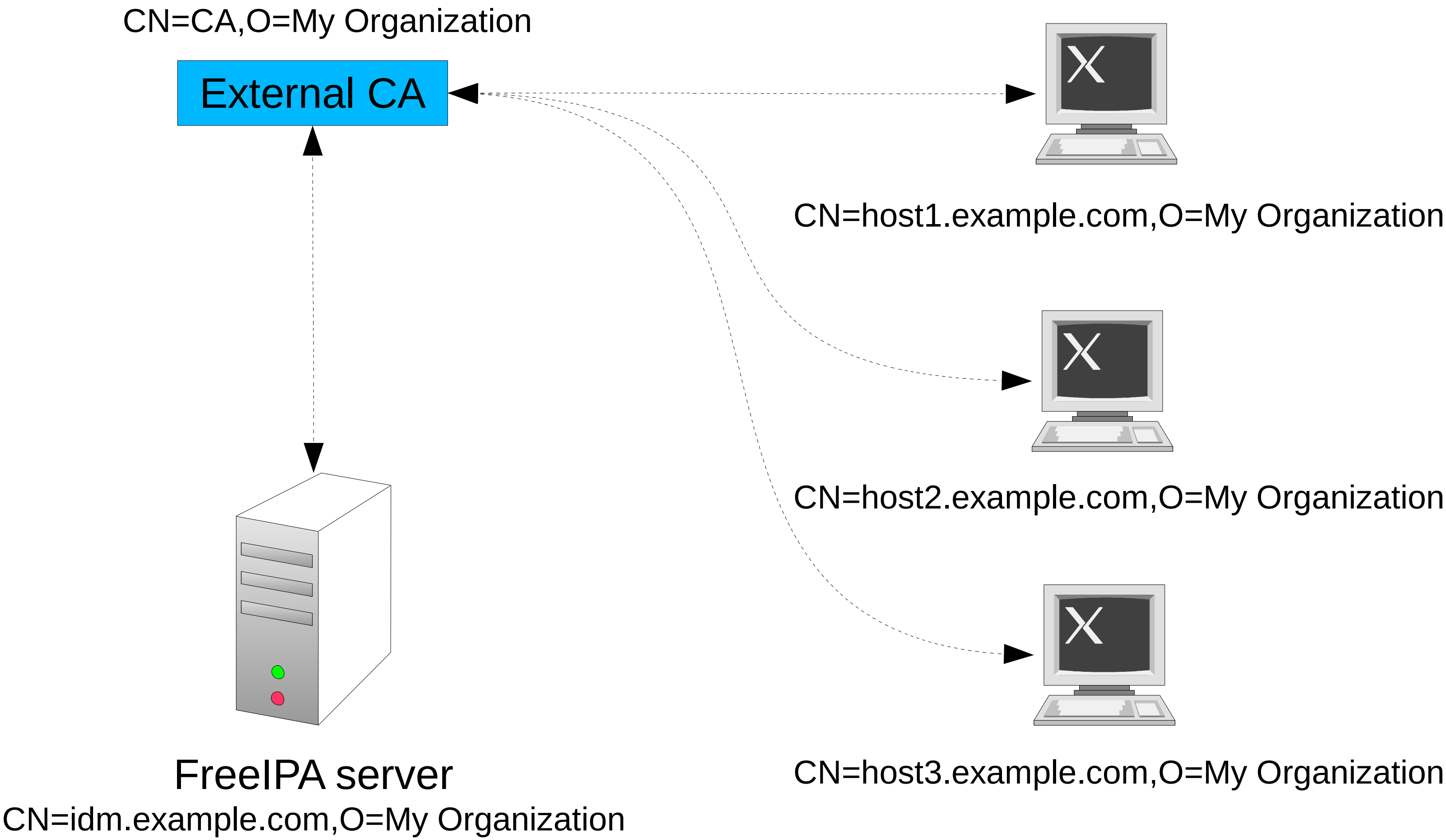
```
ipa-replica-prepare replica.example.com
```

- To install replica, run ipa-replica-install without any special options:

```
ipa-replica-install replica-info-replica.example.com.gpg
```

FreeIPA CA-less

FreeIPA CA-less (1)


CN=CA,O=My Organization
External CA
CN=host1.example.com,O=My Organization
CN=host2.example.com,O=My Organization
CN=host3.example.com,O=My Organization
FreeIPA server
CN=idm.example.com,O=My Organization

FreeIPA CA-less (2)

- User is in charge of renewing certificates
  - Certmonger is not automatically configured during install
- Certmonger has support for other CAs besides FreeIPA
  - It can be manually configured to handle certificate renewal on supported CAs

Preparation of server certificates

- In CA-less install, user is in charge of providing FreeIPA server certificates
  - Usually the user will request certificates from their company's CA
- FreeIPA expects a PKCS#12 file with the certificate and private key and a PEM file containing the CA certificate chain
  - Different certificate and private key may be used for HTTP and LDAP
  - The CA must be the same for all servers

FreeIPA CA-less install (1)

- To install first master:
  1. Prepare certificates for the server
  2. Run ipa-server-install:

```
ipa-server-install --dirsrv_pkcs12 server.p12 --http
_pkcs12 server.p12 --root-ca-file ca.pem
```

FreeIPA CA-less install (2)

- To prepare replica:

  1. Prepare certificates for the server
  2. Run ipa-replica-prepare:

```
ipa-replica-prepare replica.example.com --dirsrv_pkc
s12 replica.p12 --http_pkcs12 replica.p12
```

- To install replica, run ipa-replica-install without any special options:

```
ipa-replica-install replica-info-replica.example.com.gpg
```

freeIPA

identity | policy | audit