FreeIPA Project Update
Version 4.4 and beyond

Fraser Tweedale
Software Engineer
2017-01-17

What is **Identity Management**?

- Define users, hosts, services, access policies
- **Authentication** and **authorisation** mechanisms
- Increase **security** and **productivity**
- Reduce **cost** and **risk**

freeIPA

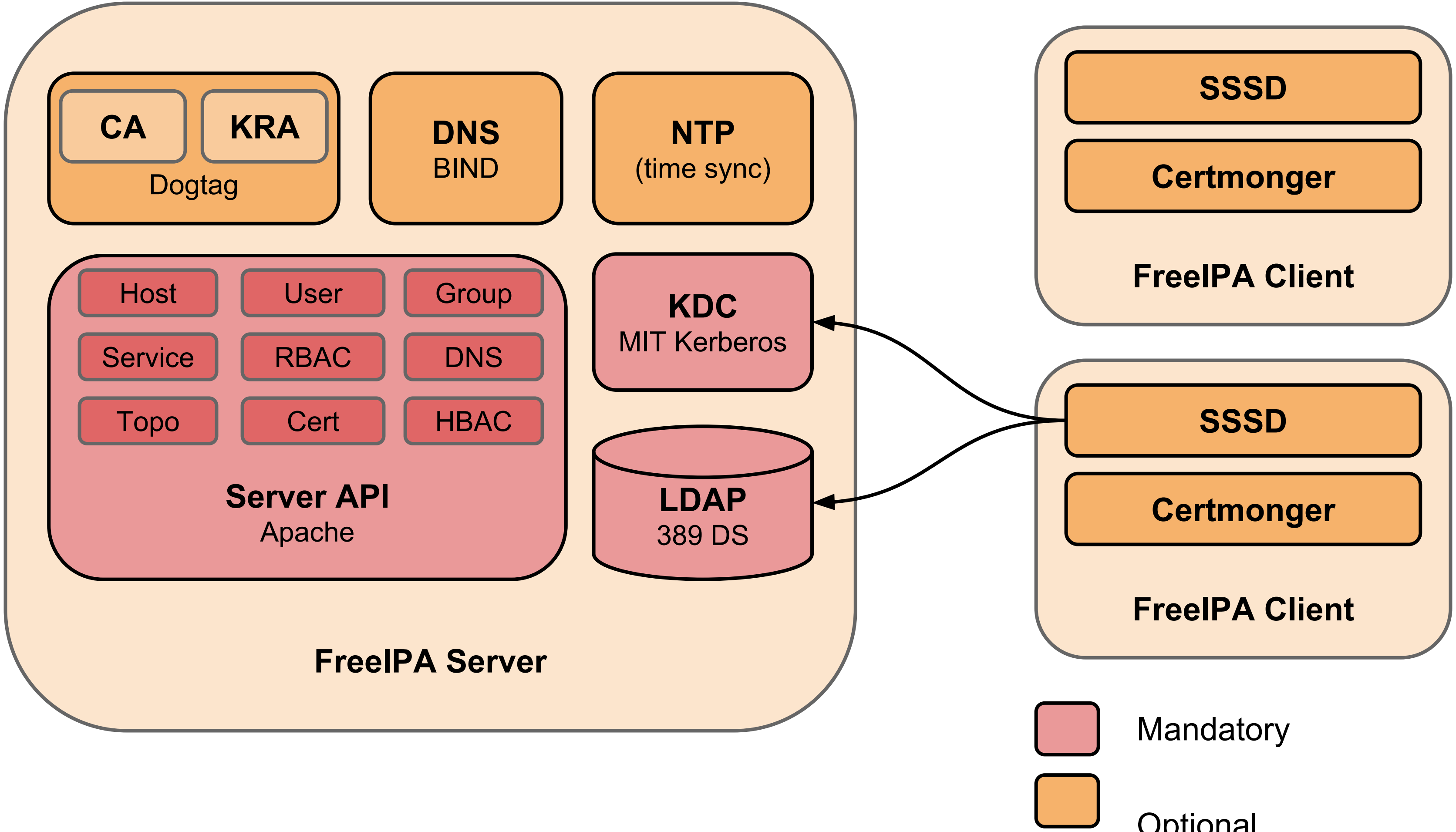
Open Source Identity Management Solution

- LDAP, Kerberos, CA, DNS, admin tools, client
  - Integrate with Active Directory via **trusts**
- Simple management via web UI and CLI
- Available in Fedora, Ubuntu, RHEL, CentOS
- Client component: SSSD

389 directory server

Dogtag Certificate System

sssd


CA
KRA
Dogtag
DNS
BIND
NTP
(time sync)
Host
User
Group
Service
RBAC
DNS
Topo
Cert
HBAC
Server API
Apache
KDC
MIT Kerberos
LDAP
389 DS
FreeIPA Server
SSSD
Certmonger
FreeIPA Client
SSSD
Certmonger
FreeIPA Client
Mandatory
Optional

Release history (recent)

- **v4.2**: July 2015
- **v4.3**: December 2015
- **v4.4**: July 2016
- **v4.5**: (March 2017)

Highlights of v4.2, v4.3, v4.4

Sub-CAs

- **Story**: support sub-CAs for specific purposes
- Before: all certs issued by a single CA (**bad!**)
- Now: simple creation and administration of sub-CAs

```
ftweedal% ipa ca-add linux.conf.au \
    --subject CN=lca2017,O=IPA.LOCAL
--------------------------
Created CA "linux.conf.au"
--------------------------
  Name: linux.conf.au
  Authority ID:
6eeb0b37-e824-4cad-9724-04265a7723a0
  Subject DN: CN=lca2017,O=IPA.LOCAL
  Issuer DN: CN=Certificate
Authority,O=IPA.LOCAL 201701121820
  Certificate:
MIIDhDCCAmygAwIBAgIBFDANBgkqhkiG9w0BA...
```

Kerberos *Authentication Indicator*

- **Story: require 2FA** for important services
- Kerberos tickets indicate whether 2FA was used
- Configure service to reject non-2FA tickets
- Only FreeIPA has this! (so far…)

Also worth a mention...

- Kerberos HTTP **KDC proxy**
- Custom **certificate profiles**
- Password vault
- Kerberos **principal aliases**
- **Smart card login** for AD users
- Topology management

What's in the pipeline?

Network-bound encryption

- **Story**: secure, automatic decryption of LUKS volumes
  - or other secrets
- **Tang**: two-party secret recovery protocol
  - *McCallum-Relyea* algorithm (based on DH)
- **Clevis**: client-side secret management
  - *n*-of-*m* splitting via *Shamir's Secret Sharing*

User session recording

- **Story**: record privileged sessions to satisfy audit / legal requirement
- Record all I/O passing through TTY
- Events stored and indexed by ElasticSearch
- Session replay; correlation with `auditd`

Also in the pipeline...

- Kerberos **PKINIT** with Smart Card
- SSSD ***secrets as a service***
- Harden FreeIPA→Dogtag communications

Resources

- https://www.freeipa.org/
- freeipa-users@redhat.com
- #freeipa
- **STICKERS**