freeIPA Certificate Renewal Deep Dive

Fraser Tweedale
ftweedal@redhat.com

November 1, 2017
Overview
Certificate renewal - why?

- Renew certificates that are approaching expiry
- Change the particulars of certificate (e.g. SAN)
- Re-issue CA certificate from different CA
Components involved

- FreeIPA (ipa cert-request)
- Dogtag
- Certmonger
- possibly an external CA
Scenarios

1. Renewal of CA certificate
   ▶ self-signed / externally signed

2. Renewal of Dogtag system certificate
   ▶ subsystem / HTTP / audit signing / OCSP

3. Renewal of IPA system certificate
   ▶ HTTP / LDAP / PKINIT / RA Agent

4. Lightweight (sub-)CA certificate
Why do we have so many issues with renewal?

- easy for topology to be misconfigured
- no monitoring / health check to detect misconfiguration
- just one expired cert can lead to total failure
- complex architecture
Certificates in play
Dogtag system certificates - /etc/pki/pki-tomcat/alias

caSigningCert cert-pki-ca Main CA signing certificate.

subsystemCert cert-pki-ca Used by Dogtag CA program to authenticate to LDAP and other subsystems. Issued by main CA.

Server-Cert cert-pki-ca TLS server certificate for Dogtag website and HTTP APIs. Issued by main CA.

auditSigningCert cert-pki-ca Used to sign audit logs. Issued by main CA.

ocspSigningCert cert-pki-ca Used to sign OCSP responses. Issued by main CA.

caSigningCert cert-pki-ca <UUID> Lightweight CA certificates (and keys)

May also contain:

- KRA subsystem and transport certs (and keys)
- External CA certs: (when Dogtag CA is signed by external CA)
IPA RA Agent certificate

- Credential used to perform privileged operations in Dogtag
- (IPA < 4.5): /etc/httpd/alias, nickname ipaCert
- (IPA ≥ 4.5): /var/lib/ipa/ra-agent.{pem,key}
IPA service certificates

- HTTP: /etc/httpd/alias, nickname Server-Cert
- LDAP: /etc/dirsrv/slapd-DOMAIN-TLD, nickname Server-Cert
- KDC: /var/kerberos/krb5kdc/kdc.{crt,key}
IPA cert management programs

ipa-cacert-manage  Renew IPA CA cert, install 3rd-party CA cert
ipa-certupdate    Update local certificate DBs with certs from LDAP
ipa-server-certinstall Install new HTTP, LDAP or KDC certificate
Certmonger
Certmonger overview

- Tracking requests monitor certificates
- When close to expiry (28 days), attempt to renew the cert
- Request config specifies a Certmonger CA
- Certmonger CA config specifies a renewal helper to invoke
- If helper succeeds, new cert replaces existing cert
- Post-renewal scripts may perform additional tasks
Renewal - IPA service certs

- **CA: IPA**
- helper invokes `ipa cert-request` command
  - needs valid *HTTP* cert
- `ipa cert-request` validates request and forwards to Dogtag
  - needs valid *IPA RA* cert
- **post-renewal**: restart `dirsrv` / `httpd`
Renewal - Dogtag system cert

- CA: dogtag-ipa-ca-renew-agent
- if server **is not** renewal master, check LDAP for updated cert
  - cn=<nickname>,cn=ca_renewal,cn=ipa,cn=etc,{basedn}
  - if updated cert present, install in NSSDB
- if server **is** renewal master:
  - invoke dogtag-ipa-renew-agent with RA Agent credential
  - store issued cert in LDAP
- **post-renewal**: restart Dogtag
Renewal - Dogtag CA signing cert (self-signed)

- CA: dogtag-IPA-ca-renew-agent
- same as Dogtag system cert, with extra step:
  - add updated cert to cn=certificates,cn=ipa,cn=etc,{basedn}
Renewal - Dogtag CA signing cert (externally-signed)

- CA: dogtag-IPA-ca-renew-agent
- if server **is not** renewal master, check LDAP for updated cert
- if server **is** renewal master:
  - write CSR to /var/lib/ipa/ca.csr
  - exit with message to use ipa-cacert-manage renew
Renewal - Lightweight CA signing cert

- CA: dogtag-ipa-ca-renew-agent
- same as Dogtag system cert, except:
  - cert *not* stored in cn=ca_renewal,cn=ipa,cn=etc,{basedn}
  - update `authoritySerial` attribute in Dogtag LWCA entry
Specific problem scenarios
CA renewal master configuration

- There must be exactly **one renewal master** in the topology
- Problems:
  - renewal master offline / decommissioned
  - no (or multiple) renewal master configured
- **Indicator**: Certmonger request stuck in CA_WORKING
- **Diagnosis**: check caRenewalMaster configuration
- **Resolution**: fix caRenewalMaster configuration
CA renewal master configuration

dn: cn=CA,cn=f27-1.ipa.local,cn=masters,cn=ipa,cn=etc,dc=ipa,dc=local
objectClass: ipaConfigObject
ipaConfigString: caRenewalMaster <-- one and only one of these
ipaConfigString: enabledService
ipaConfigString: startOrder 50
...

dn: cn=CA,cn=f27-2.ipa.local,cn=masters,cn=ipa,cn=etc,dc=ipa,dc=local
objectClass: ipaConfigObject
ipaConfigString: enabledService
ipaConfigString: startOrder 50
...
Missing external CA certificate(s) in trust store(s)

- e.g. CA cert was re-chained; LDAP/HTTP cert changed to externally signed
- Resolution
  - run `ipa-certupdate` on affected IPA server(s)
LDAP cert auth problems - RA Agent

dn: uid=ipara,ou=people,o=ipaca
uid: ipara
description: 2;7;CN=Certificate Authority,o=IPA.LOCAL;CN=IPA RA,o=IPA.LOCAL
userCertificate:: MIIDfz... # the current cert; base64-encoded DER

▶ Indicators:
  ▶ All IPA cert management commands failing (e.g. ipa cert-show 1)
  ▶ Basic Dogtag functionality working (https://<server>:8443)

▶ Resolution: ldapmodify
  ▶ Update the userCertificate attribute
  ▶ Update the description: 2;<serial>;<issuer-dn>;<subject-dn>
LDAP cert auth problems - subsystemCert cert-pki-ca

dn: uid=pkidbuser,ou=people,o=ipaca
uid: pkidbuser
description: 2;4;CN=Certificate Authority,O=IPA.LOCAL;CN=CA Subsystem,O=IPA.LOCAL
seeAlso: CN=CA Subsystem,O=IPA.LOCAL 201710111026
userCertificate:: MIIDhT...
...

- Indicators:
  - TLS handshake errors in /var/log/pki/pki-tomcat/ca/alias
  - Basic Dogtag functionality unavailable (direct use)

- Resolution: same as previous slide
Missing tracking requests

- `ipa-server-upgrade` should add missing tracking requests
- for lightweight CAs: `ipa-certupdate` will add tracking requests
Expired cert(s)

- If a cert involved in renewal has expired...
- reset clock to a time when all relevant certs are valid
  - be careful of notBefore
Questions?
What's next?

- IPA v3 renewal overview
- Publish the info to... Wiki? Blogs? Mojo?
- What else do you need?
- Email me / mailing list any time!