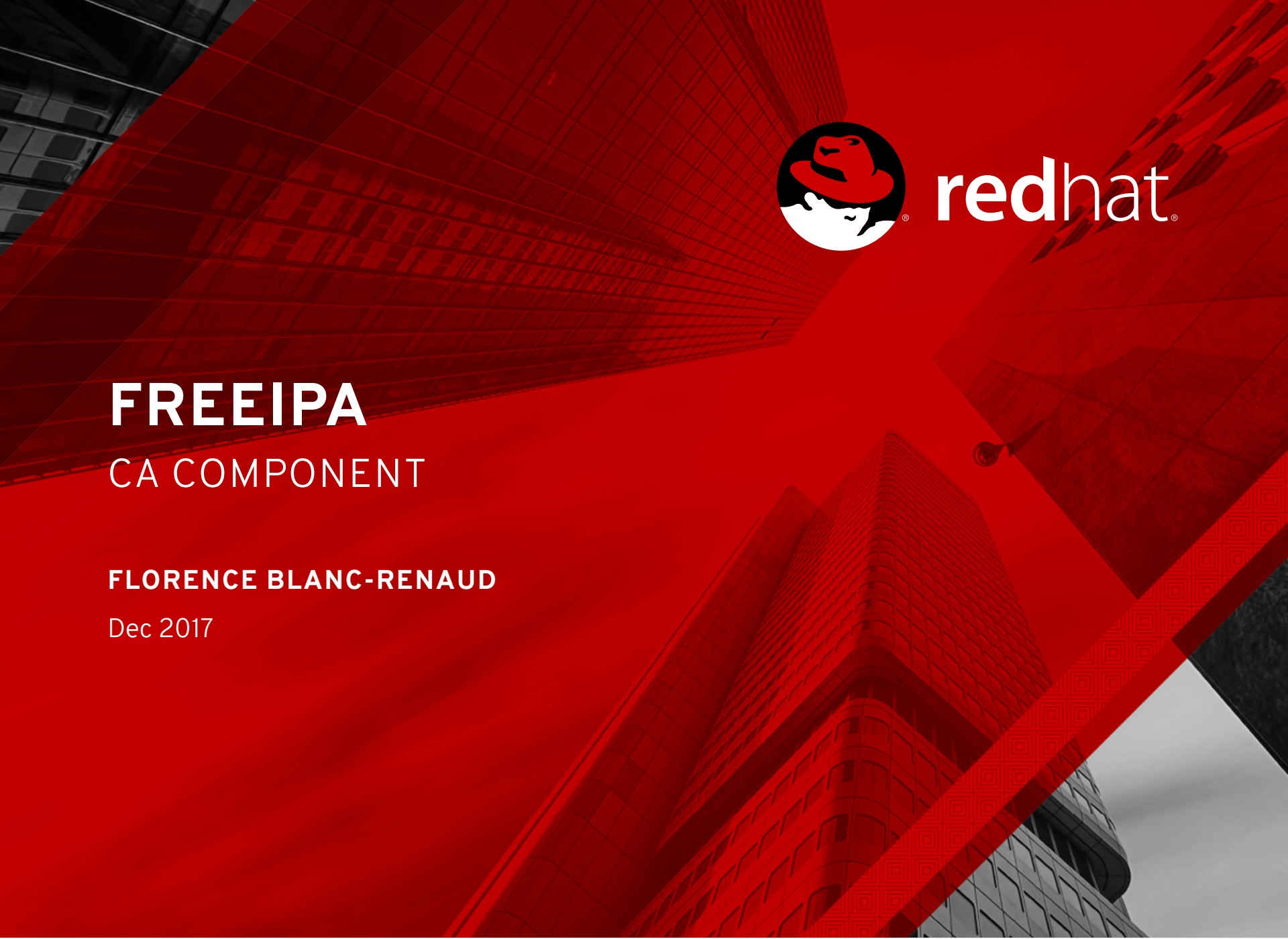


FREEIPA

CA COMPONENT

FLORENCE BLANC-RENAUD

Dec 2017

DEPLOYMENT OPTIONS

CA-LESS

- LDAP and HTTP require a server certificate
- PKINIT support (optional)

WITH AN EMBEDDED CA

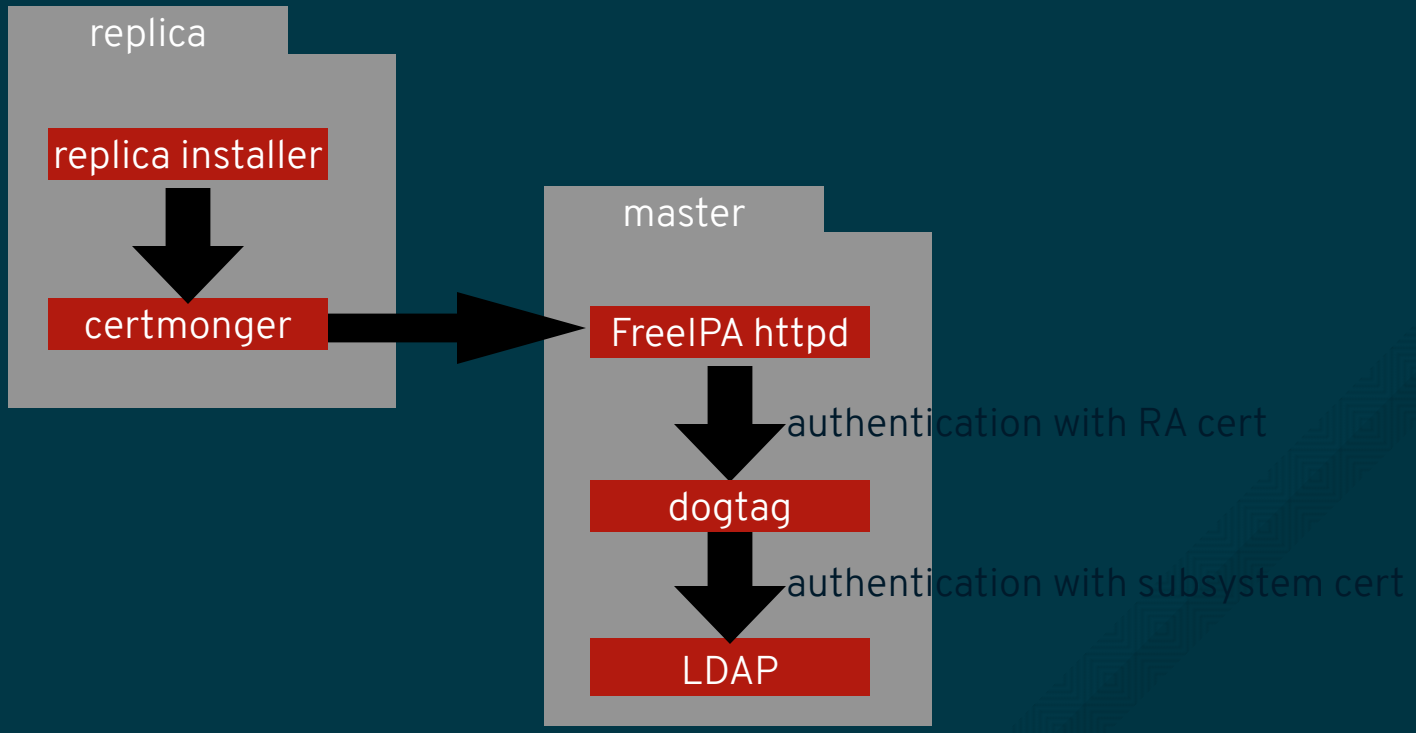
EXTERNALLY SIGNED

SELF SIGNED

- deliver certificates for LDAP, HTTP, PKINIT
- deliver certificates for users, hosts, services
- automatically renew the certificates used by FreeIPA (Dogtag, LDAP, HTTP...) with certmonger

REPLICA INSTALLATION

- replica needs to obtain HTTP and LDAP certificates (different from the master ones)
- certmonger already locally configured as IPA client



CERTIFICATE RENEWAL

- Some certificates are specific to each master/replica (HTTP, LDAP)
- Some certificates are identical on all the masters (dogtag certs):
  - only the renewal master can renew them
  - other replicas only download them
- Managed by different Certmonger CA (getcert list-cas):
  - IPA: HTTP, LDAP, KDC
  - dogtag-ipa-ca-renew-agent: ra agent, auditSigning, ocspSigning, subsystem, caSigning, server-cert PKI
  - (versions < 4.5) dogtag-ipa-renew-agent: server-cert PKI

ADDITIONAL INFORMATION

- Demystifying the certificate authority component in FreeIPA
- Using certmonger to track certificates
- Troubleshooting certmonger issues with FreeIPA