Dogtag Certificate System

Kashyap Chamarthy
<kashyap@redhat.com>

Outline

1/ Intro

2/ Subsystems involved

3/ Configuration overview

4/ Storing Keys and Certs

5/ High Availability

6/ Security

7/ What's ahead

8/ Quick Demo

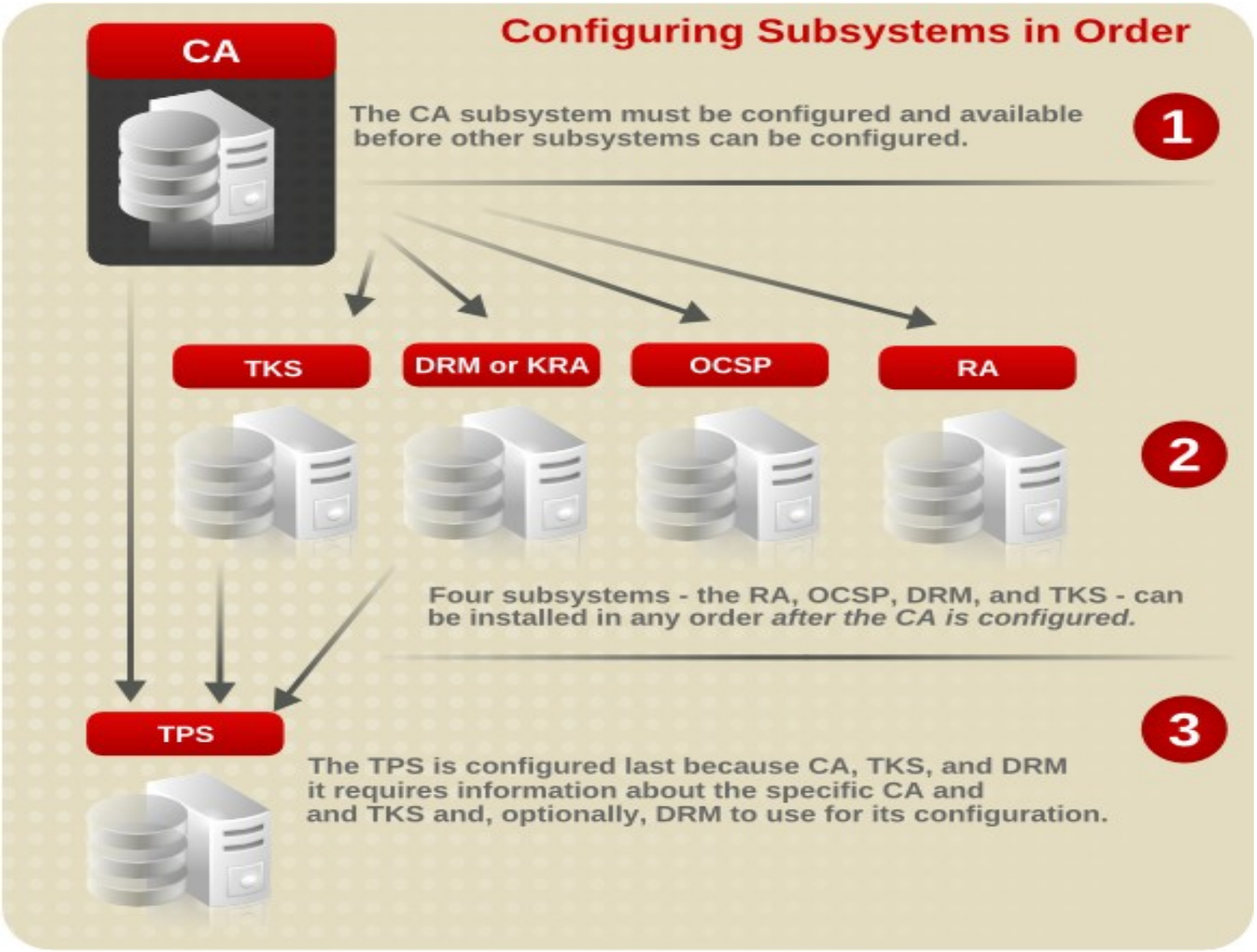
What Dogtag

- An enterprise class open-source PKI infrastructure
- Highly Configurable
- Scalable
- Supports Hardware Security Modules(HSMs)
- Secure (SELinux; ACLs ; Audit Logging)
- Completely GPL

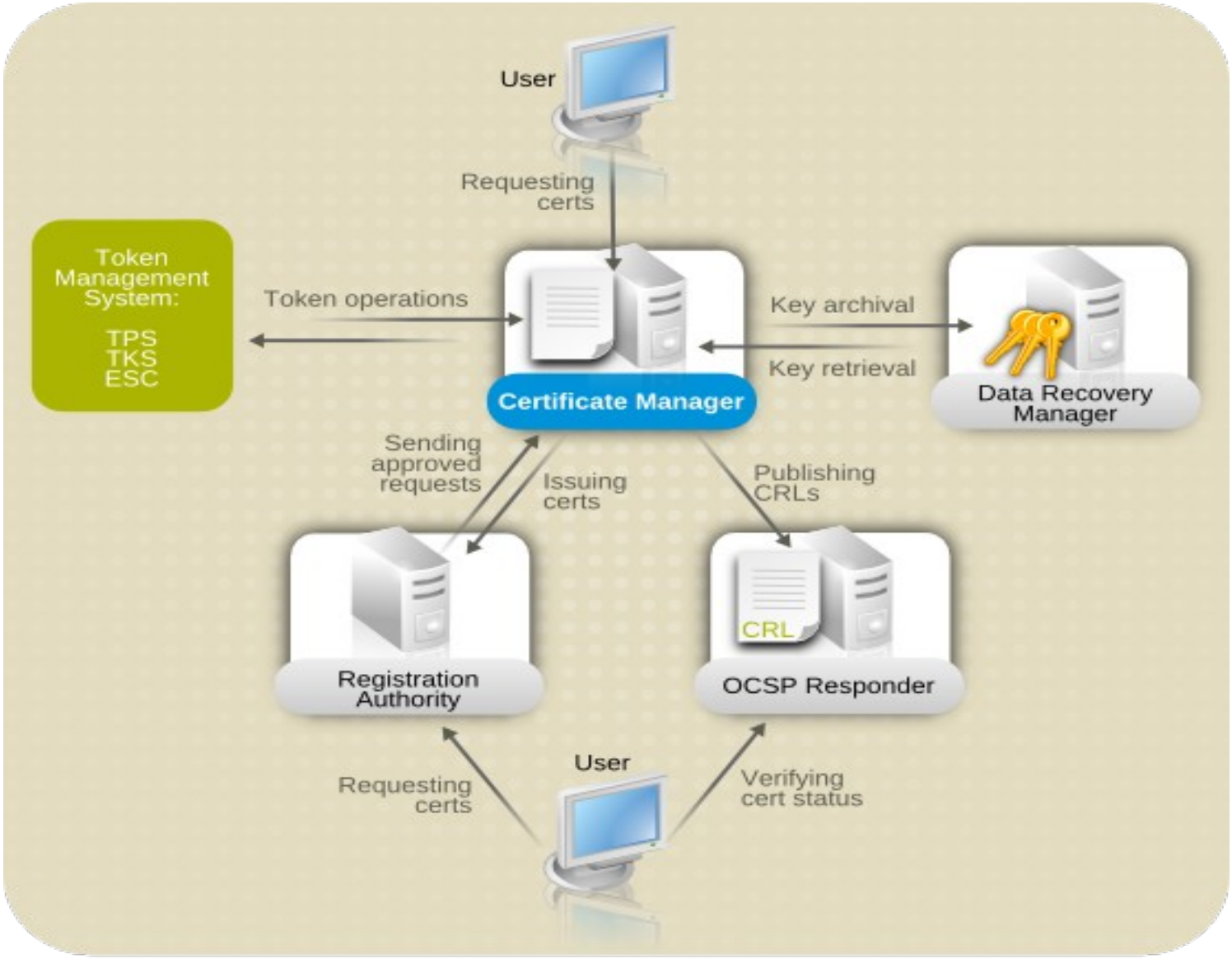
Subsystems

- Certificate Authority(CA)
  - Issue; Revoke; Renew;Publish CRL
- Key Recovery Authority (or DRM)
- OCSP Responder
- Registration Authority (RA)
- Token Key Service(TKS)
- Token Processing System(TPS)

Configuration Overview



Non-TMS Env.


User
Requesting certs
Token Management System:
TPS
TKS
ESC
Token operations
Certificate Manager
Key archival
Key retrieval
Data Recovery Manager
Sending approved requests
Issuing certs
Publishing CRLs
CRL
Registration Authority
OCSP Responder
User
Requesting certs
Verifying cert status

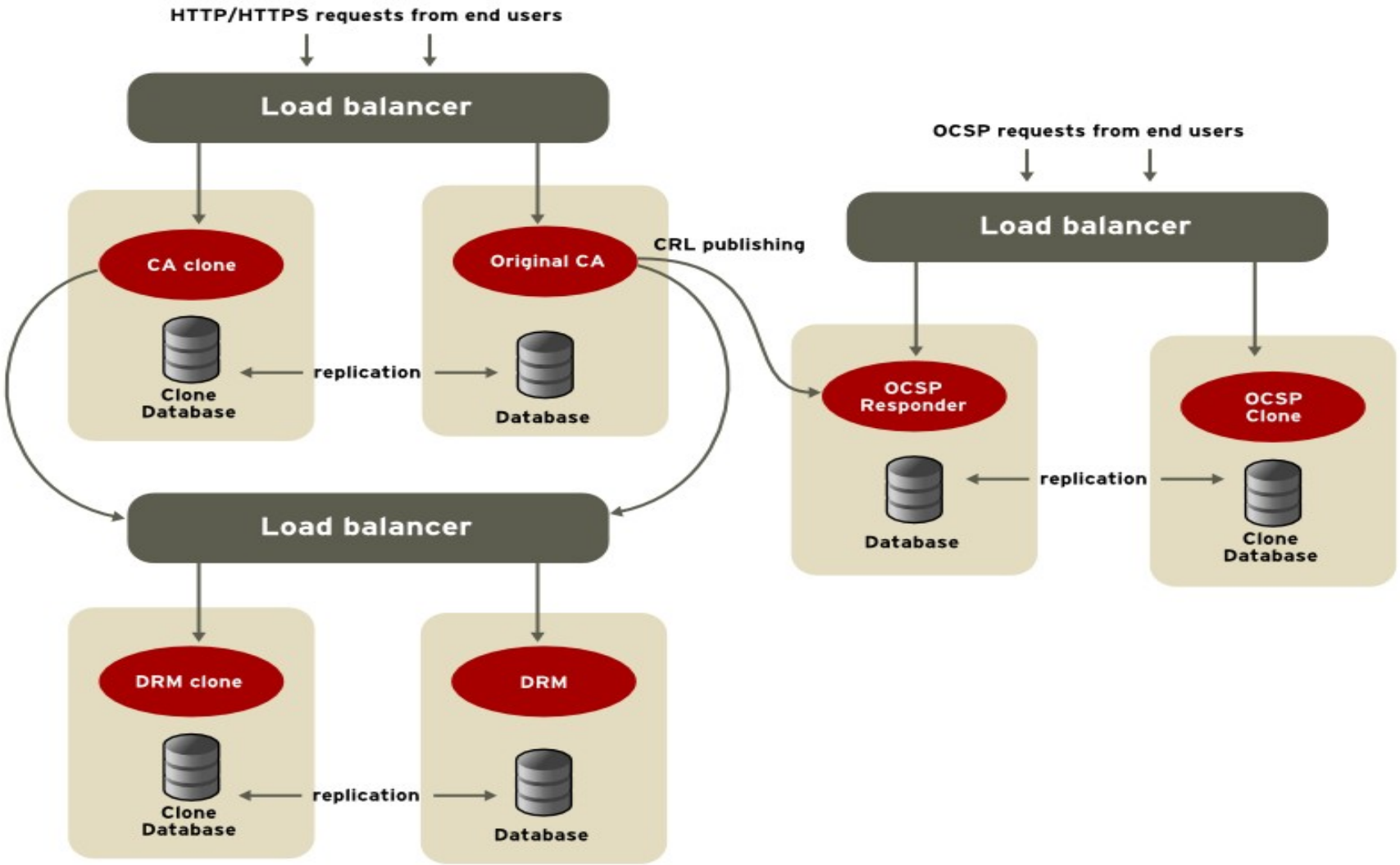
Storing keys and Certs

- Internal Tokens
  - Or software tokens – mozilla nss db files
  - Auto-generated when a subsystem instance is created
- External Tokens
  - HSMs
    - ncipher
    - Safenet Luna

Interafaces

- **End-Entity:** Enrollment/Renewal; Revocation; Retrieval
- **Agent:** Approve Requests; Search; Revoke; Update CRL
- **Admin:** Manage Users/Groups; ACLs; Log Config using a console

High availability



Security for subsystems

- Logging
  - Debug ; Transactions; Errors
- Auditing
  - Audit log for all events; Signed;
- Authentication, Authorization and ACLs
  - AUTH: User/Passwd; SSL auth; LDAP auth.
- SELinux
  - Specific context for subsystem files, dir, ports, and processes.

Tools

- **pkicreate, pkiremove, pkisilent**
- **PKCS10Client, PKCS12Export**
- **OCSPClient**
- **sslget**
- **revoker**
- **tpsclient**
- **AtoB ; BtoA** and many others

Ex: Instance Creation(CA)

- # **pkicreate** -pki_instance_root=**/var/lib** \
  -pki_instance_name=**pki-ca** \
  -subsystem_type=**ca** -agent_secure_port=**9443** \
  -ee_secure_port=**9444** \
  -ee_secure_client_auth_port=**9446** \
  -admin_secure_port=**9445** \
  -unsecure_port=**9180** \
  -tomcat_server_port=**9701** \
  -user=pkiuser -group=**pkiuser** \
  -redirect conf=**/etc/pki-ca** -redirect logs=**/var/log/pki-ca**
  -verbose

What's coming next

- REST based interface design
- More tighter Integration of other subsystems(DRM, OCSP) with freeIPA(Identity, Policy, Audit) project
- Reworking/Simplification of 'pkicreate' and 'pkisilent' tools
- More code simplification and cleanups all over

Resources

- http://pki.fedoraproject.org/
- http://pki.fedoraproject.org/wiki/Dogtag_Future_Dir
- http://freeipa.org
- Mailing Lists
  - http://pki.fedoraproject.org/wiki/PKI_Mailing_Lists
- IRC(on freenode) -- #dogtag-pki , #freeipa

Short demo

?