Les infrastructures de clés publiques (PKI, IGC, ICP)

JDLL
14 Octobre 2006
Lyon

Bruno Bonfils
<asyd@asyd.net>

Plan

- L'utilisation des certificats
- Le rôle d'un certificat
- Les autorités de confiance
- Le principe de confiance
- La structure d'un certificat
- Une PKI
- Un générateur de PKI libre, EJBCA

L'utilisation des certificats 1/2

- Utilisation courante
  - HTTPs, POP3s, IMAPs, etc.
  - Email (S/MIME) (chiffrement et signature)
  - Signature d'objets (paquets, librairies, etc..)
- D'autres utilisations
  - Tunnel VPN
  - Non répudiation (désaveu impossible)

L'utilisation des certificats 2/2

- Des applications utilisateurs
  - Mozilla, Thunderbird, Kmail, etc.
- De nombreux services peuvent utiliser des certificats
  - Apache
    - chiffrement, authentification utilisateur
  - OpenSSH (patch requis)
    - authentification utilisateur
  - Postfix, OpenLDAP, etc.

Le rôle d'un certificat

- Chiffrement
  - clé privée
  - clé publique
- Carte d'idendité électronique
  - nom (de la personne ou de la machine)
  - l'émetteur
- Lors d'une communication basée sur SSL/TLS, l'idendité du client peut également être assurée (authentification)

Les autorités de confiance

- Publient un certificat racine qui peut être inclus dans des applications
- L'inclusion d'une autorité de confiance implique de faire confiance à tous les certificats qu'elle émet
- Quelques exemples
  - Thawte, Verisign, etc..

Le principe de confiance 1/2

- L'inclusion d'un certificat racine n'est pas une chose mineure, elle doit faire l'objet d'une attention particulière
- L'ETSI fournit quelques recommandations
  - Existence légale (entreprise)
  - Solidité financière
  - Service juridique

Le principe de confiance 2/2

- Les applications se doivent de fournir un document sur leurs politiques d'acceptation des certificats racines
- Quelques exemples de politiques importantes
  - Debian (package ca-certificates)
  - Mozilla et dérivés (navigateur Web, client mail)

La structure d'un certificat 1/2

- Les informations obligatoires
  - L'identifiant du destinataire du certificat
  - L'identifiant de l'émetteur
  - Une date de validité (début et fin)
  - Un numéro de série
- Un identifiant est composé d'attribut
  - CN, O, OU, C, etc.
  - Mapping possible avec annuaire LDAP

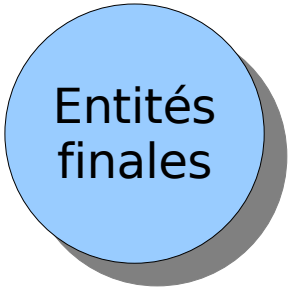
La structure d'un certificat 2/2

- Le standard X509v3 définit les extensions suivantes
  - Contrainte CA (autorise à signer d'autres certificats)
  - Une liste d'utilisation du certificat
    - Digital Signature, time stamping
    - Non repudiation
    - Client, server authentication
  - URI du répondeur OCSP, de la CRL
  - Des noms alternatifs

Une PKI

- Appellations : PKI, ICP, IGC
- C'est un ensemble comportant de multiples acteurs (entités)
- Une infrastructure technique
- Des documents décrivant la politique
  - CP, PC (Politique de certification)
  - Cheminement du certificat
    - émission
    - utilisation

Architecture d'une PKI

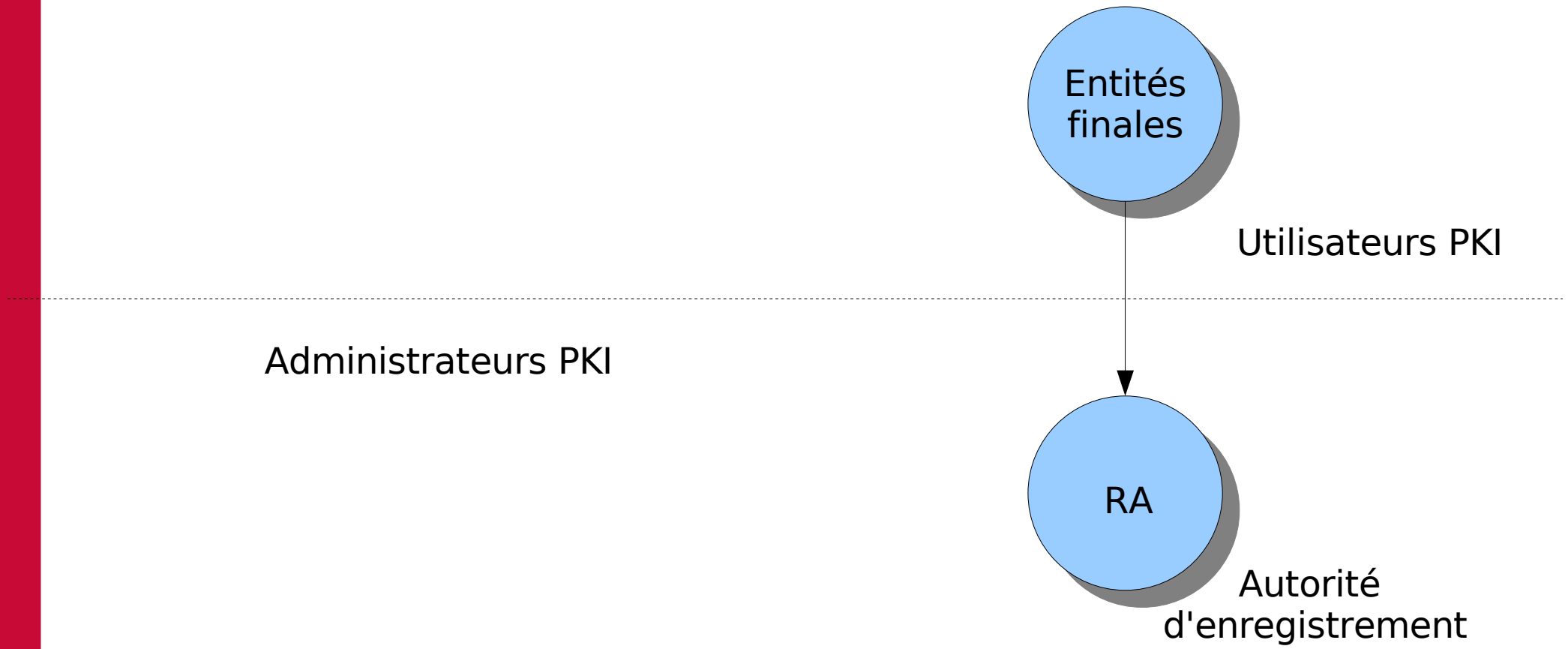


Utilisateurs PKI

Administrateurs PKI

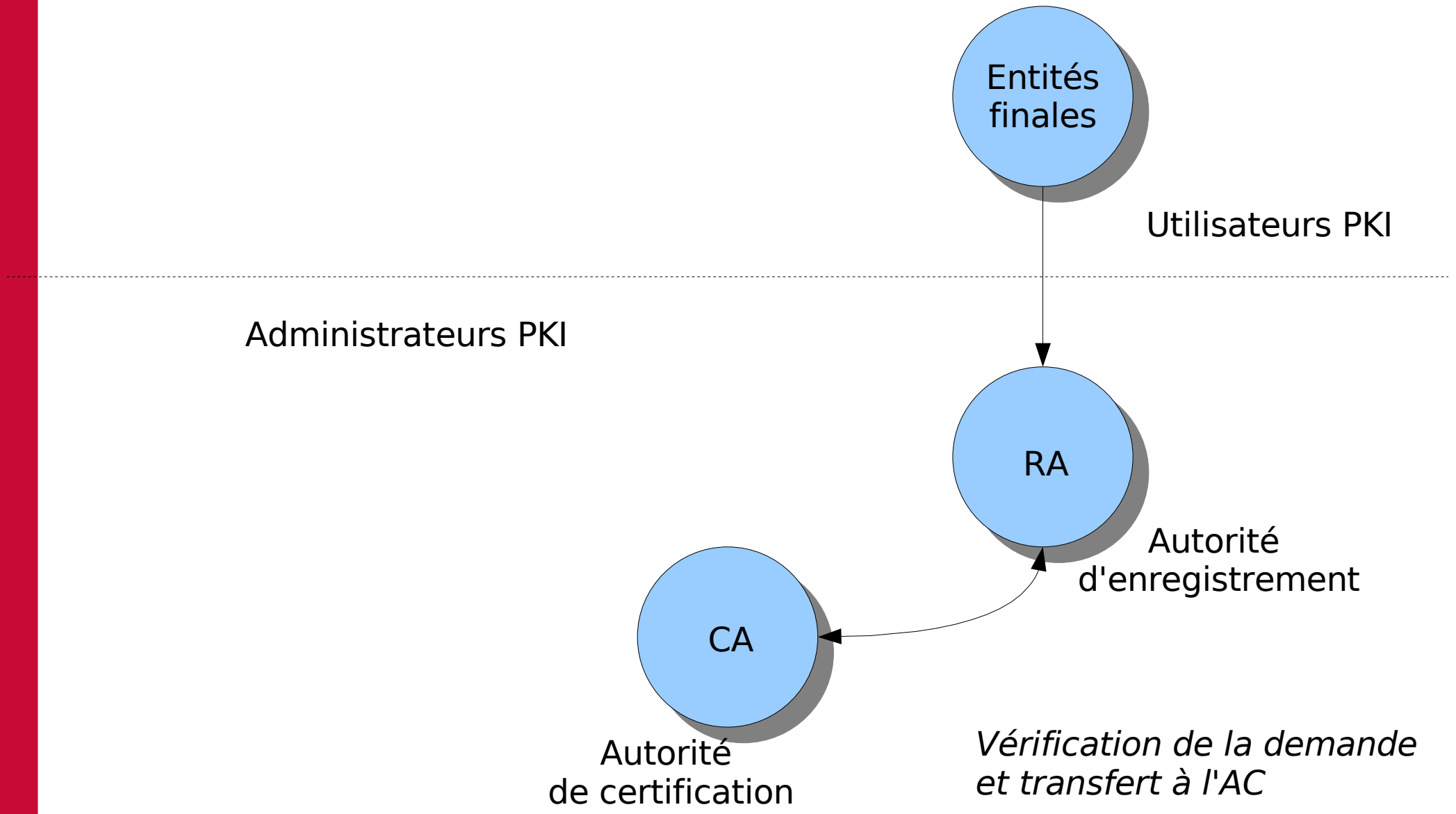
Création d'une nouvelle entité
(exemple : nouveau partenaire)

Architecture d'une PKI

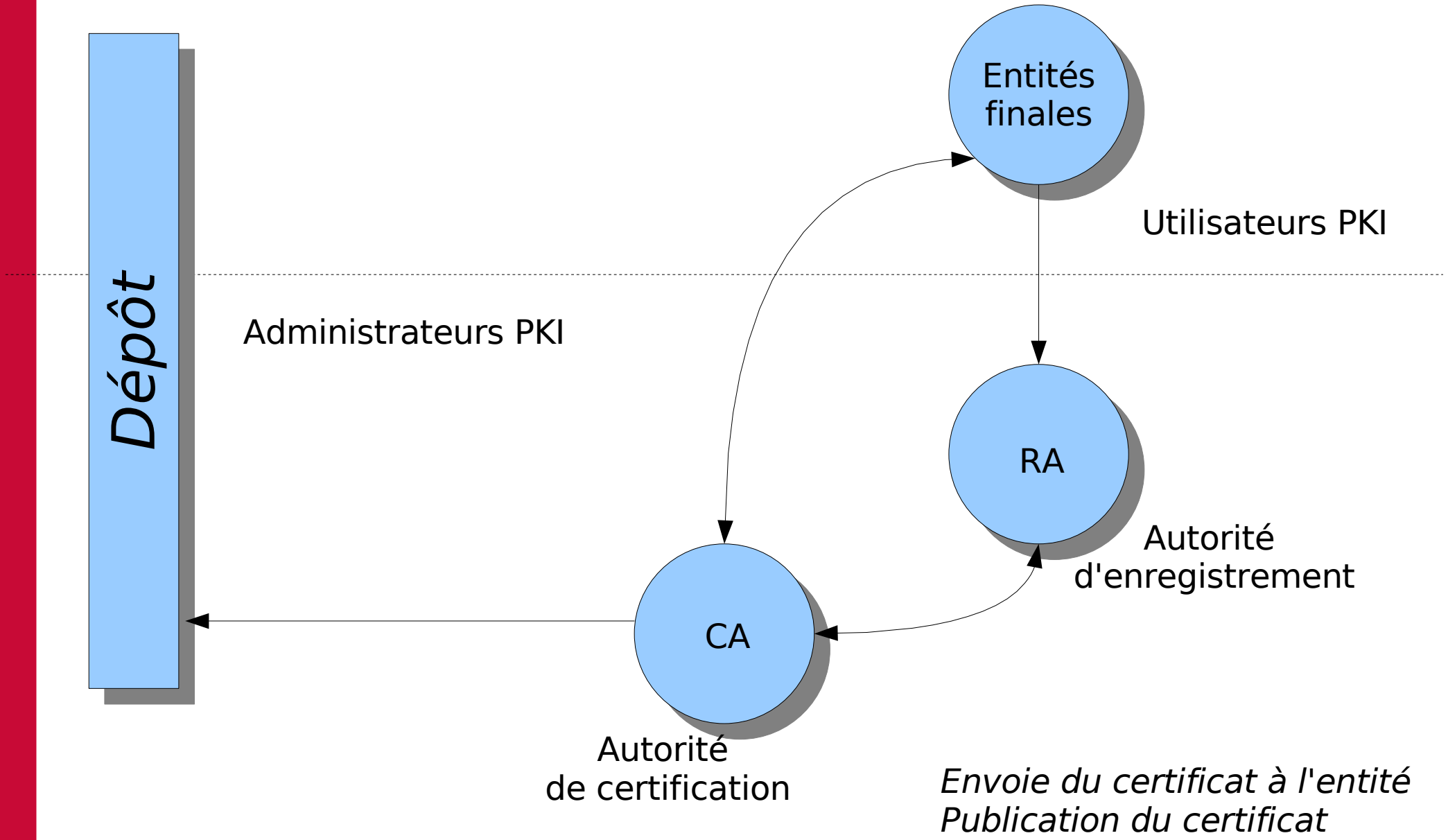


Émission d'une demande de certificat

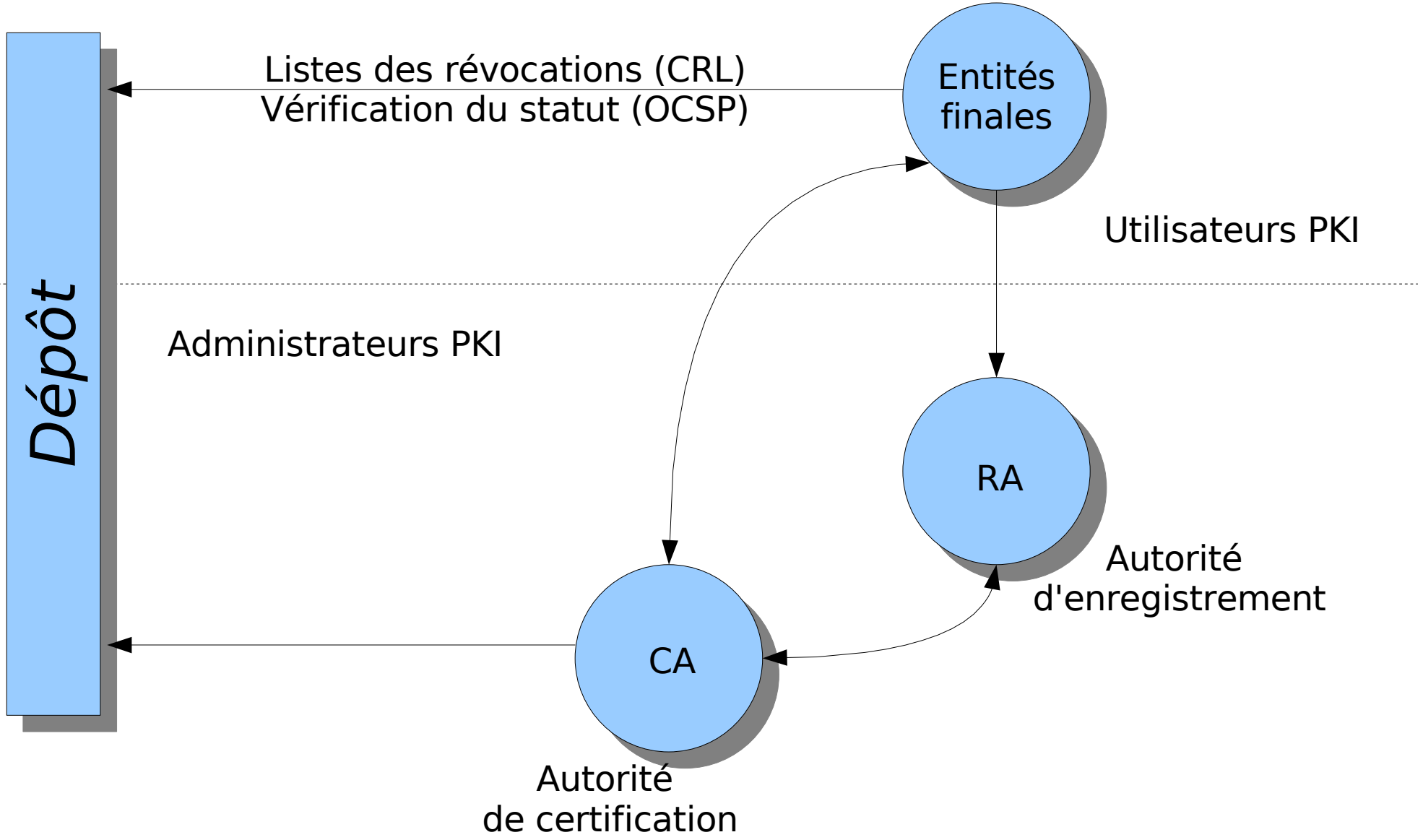
Architecture d'une PKI



Architecture d'une PKI



Architecture d'une PKI



Les acteurs d'une PKI

- Des entités finales (des utilisateurs, des services)
  - possesseur de un ou plusieurs certificats
- Des autorités d'enregistrement
  - Valident et génèrent les demandes de certificats
- Des autorités de certification
  - Définition des politiques (CP / PC)
  - Création des certificats

L'infrastructure technique

- Une interface utilisateur, administrateur
  - généralement Web
  - peut être CLI
- Publication (dépôt)
  - des certificats (LDAP)
  - des révocations, statuts (CRL, OCSP)
- Des interfaces d'enrôlements
  - Navigateur web
  - Equipements VPN (SCEP)

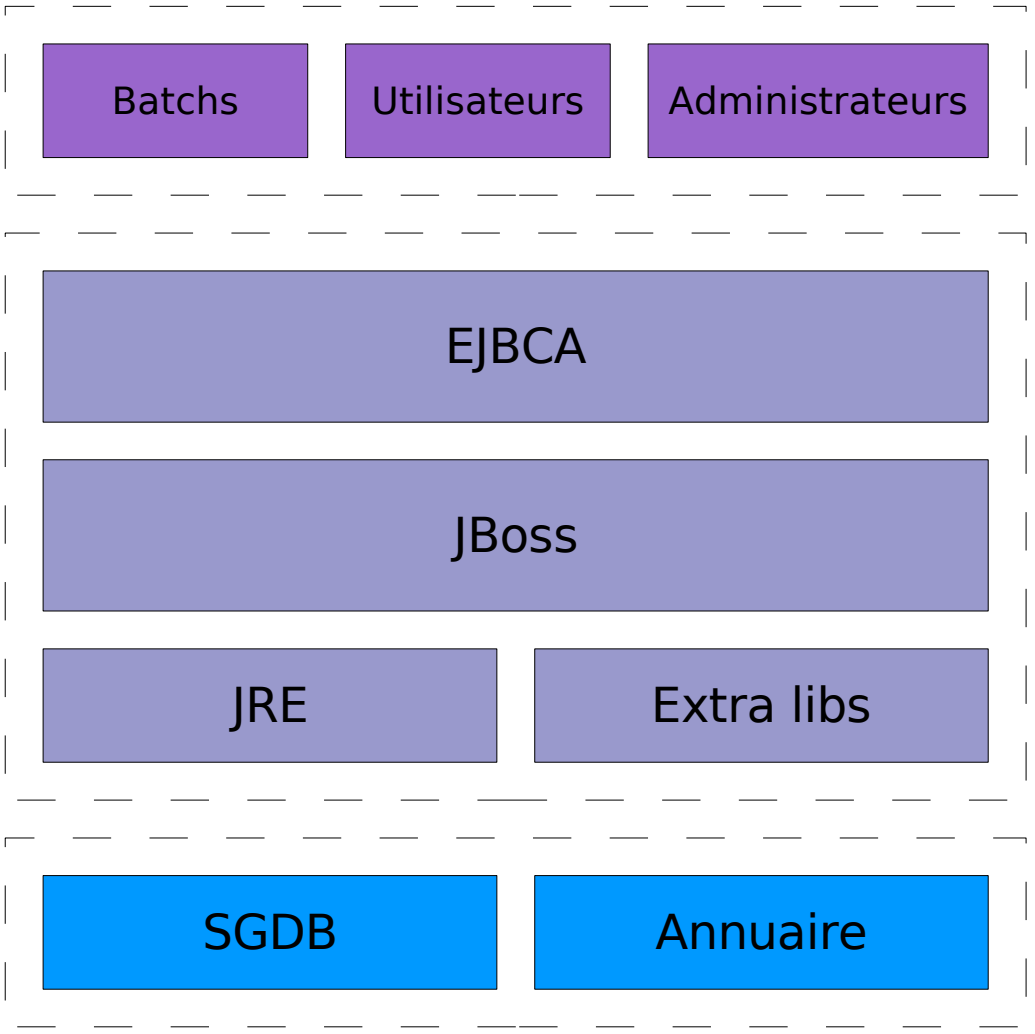
Exemple de PKI : EJBCA

- Générateur libre de PKI
- Indépendant de la plateforme
- Interopérable
- S'adapte aux politiques
- Peut gérer plusieurs certificats racines

EJBCA, à propos

- Application Java (1.4, 1.5) EJB
- Licence LGPL
- Edité par la société PrimeKey (Suède)
- Réactivité de développement
- Développement spécifique possible
- ~40 contributeurs
- Utilisée par de grand comptes

Architecture système



Architecture réseau

EJBCA

Home

CA Functions
- Basic Functions
- Edit Certificate Profiles
- Edit Publishers
- Edit Certificate Authorities

RA Functions
- Edit End Entity Profiles
- Add End Entity
- List/Edit End Entities

Log Functions
- View Log
- Log Configuration

System Functions
- System Configuration
- Edit Administrator Privileges

Public Web

My Preferences

- Fonctionnalités
  - Installation simple (15 minutes)
  - OCSP (Online Certificate Status Protocol)
    - Vérification des révocations
  - SCEP (Simple Certificate Enrollment Protocol)
    - IOS (Cisco)
    - NSOS (NetScreen)
    - OpenSCEP

EJBCA

Home

CA Functions
- Basic Functions
- Edit Certificate Profiles
- Edit Publishers
- Edit Certificate Authorities

RA Functions
- Edit End Entity Profiles
- Add End Entity
- List/Edit End Entities

Log Functions
- View Log
- Log Configuration

System Functions
- System Configuration
- Edit Administrator Privileges

Public Web

My Preferences

- Fonctionnalités
  - Supporte de nombreux SGBD via le mécanisme JDBC
    - MySQL
    - PostgreSQL
    - Mais aussi Oracle, Sybase, etc.
  - Permet la publication
    - Standard LDAP
    - Active Directory
    - Extensible via programmation

EJBCA

Home

CA Functions
- Basic Functions
- Edit Certificate Profiles
- Edit Publishers
- Edit Certificate Authorities

RA Functions
- Edit End Entity Profiles
- Add End Entity
- List/Edit End Entities

Log Functions
- View Log
- Log Configuration

System Functions
- System Configuration
- Edit Administrator Privileges

Public Web

My Preferences

- Fonctionnalités
  - Approbation possible
    - Plusieurs administrateurs sont nécessaires pour effectuer une opération
  - Supporte des équipement hardware tel que nCipher
    - Accélération hardware
    - Approbation multiples
  - Interface ligne de commande
    - Traitements par lots
    - Opérations d'administrations

La fonction CA

- Gestion des certificats racines
- Gestion des profils de certificats
  - Utilisation (keyUsage, Extended KeyUsage)
    - Certificat serveur
    - Signature de courrier (SMIME)
  - Profil de publication
  - Taille de clé
- Connaissances techniques requises

Edit End Entity Profile

Profile : Certificat serveur PEM - Type simple

Back to End Entity Profiles

	Username	Required ☑ Modifyable ☑
	Password	Autogenerated ☐ Required ☑
	Batch generation (clear text pwd storage)	Use ☐ Default ☐ Required ☐
Select for Removal	Subject DN Fields	E, EmailAddress in DN [Add]
☐	E, EmailAddress in DN	Required ☑ See also configuration of Email field.
☐	CN, Common Name	Required ☑ Modifyable ☑
☐	O, Organization	asyd;GUSES;Solaris-FR Required ☑ Modifyable ☐
☐	C, Country	FR Required ☑ Modifyable ☐

La fonction RA

- Rôle
  - Gérer les demandes de certificats
  - Transférer les demandes de certificats
- Connaissances techniques non requises
- Valider la demande de certificat

La fonction RA

- Profil RA
  - Choix d'un profil de certificat
  - Champs du sujet (DN)
    - choix des attributs disponibles (obligatoire ou facultatif)
    - présélection de valeur
      - Contraintes : champ fixe, liste de choix
      - Domaine de l'adresse mail
  - Choix du format (ex : PEM, PKCS12)

EJBCA Administration

Add End Entity

End Entity Profile	Certificat serveur PEM - Type simple	Required
Username	apache-subversion	☑
Password	**********	☑
Confirm Password	**********	
Email	asyd @ asyd.net	☑
Subject DN Fields		
E, EmailAddress in DN	Use data from Email field : ☑	☑
CN, Common Name	subversion.asyd.net	☑
O, Organization	asyd	☑
C, Country	FR	☑
Certificate Profile	Certificat Serveur	☑
CA	AdminCA1	☑
Token	PEM file	☑
Send Notification	☑	

Add End Entity | Reset

EJBCA Administration

Username: apache-subv

Password: subversion

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUCAQAwXDERMA8GA1UEChMIYXN5ZC5uZXQxCzAJBgNVBAYTAkZSMRww
GgYJKoZIhvcNAQkBFg1hc3lkQGFzeWQubmV0MRwwGgYDVQQDExNzdWJ2ZXJzaW9u
LmFzeWQubmV0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC95DZ1A3KCQEDA
9tcatGhGPyaZwl2/4YNHKH7KS1cpleWEZCjYPxtnkj5H5O2TknVAYvKsNAeBLzCM
9pD7RRRdOFBl45C8j06Vn5ShnzB1Q3VaHjrI30yyRa3ywGL/YZiW69lRp3Y8q1Dh
5eyGbQPP+jIBy6gkL66OARazmJ/llwIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
UAAyjQrMkviGPkEC+bwR9FvBThiZ5fSp8cEtnkX5vr//hxcas8XqRU4OKBZN7EQj
ctnQKyea6Dh+jBA1CdfpMlBohEUozjpvTiELPEb6ChdBd30R5YYYeEkQ6xfPidw+
fJ5tOAB71YFrvLfolek5cwW2sKDSD85xJlzyxiWn4Q4=
-----END CERTIFICATE REQUEST-----
```

PEM Certificate

OK

View Certificate

Username	apache-subversion
Certificate nr	1 of 1
Certificate Version	X509 V.3
Certificate Serial Number	4D8C0A366AB73F34
Issuer DN	CN=Asyd Dot Net CA,O=asyd,C=FR
Valid from	5/15/06
Valid to	5/16/07
Subject DN	E=asyd@asyd.net,CN=subversion.asyd.net,O=asyd,C=FR
Subject Alternative Name	None
Public key	RSA (1024Bits)
Basic constraints	End Entity
Key usage	Digital Signature, Key encipherment
Extended Key Usage	Server Authentication
Signature Algorithm	SHA1WithRSAEncryption
Fingerprint SHA1	2C697A2FAB8DAA9FEF2A24EB629D6BEBB9B1E39A
Fingerprint MD5	8169E1679E12DA80FB78494EF65FE981
Revoked	No

Close

Republish

Revoke

Unspecified

Download to Internet Explorer
Download to Netscape
Download pem file

Démonstration EJBCA
Questions / réponses

Remerciements

- Linagora et L'équipe de EJBCA (spécialement Tomas et Philip)
- Yannick Quenec'hdu

En savoir plus

- Site RSA
- Site Linagora sur les PKI
- RFC, code source
- Wikipedia

LINAGORA