e i g

Hes·so

PKI : Public Key Infrastructure

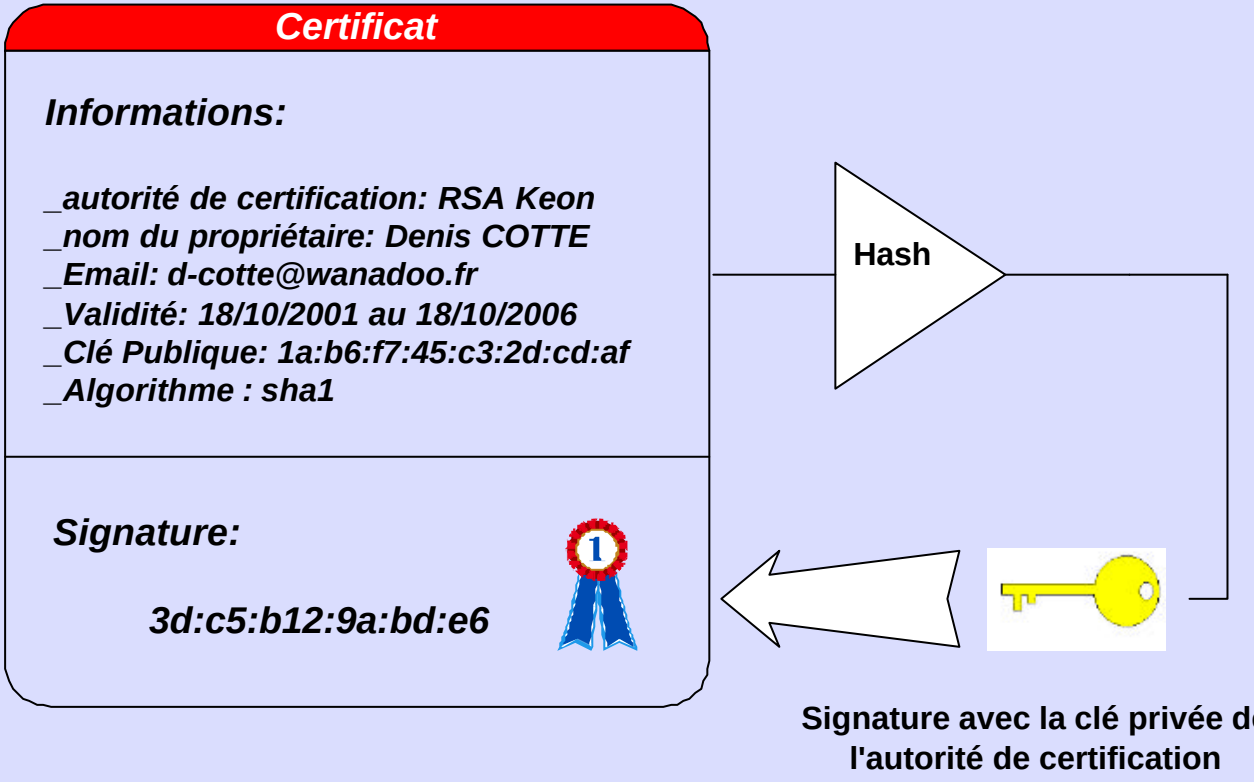
Diplômant	:	Denis Cotte
Professeur responsable	:	Gérald Litzistorf
Collaboration avec	:	Sylvain Maret e-Xpert solutions

Sommaire

- PKI : Infrastructure à clé publique
- Enrollment : Procédure d'inscription
- Protocole OCSP
- Server Apache
- Conclusion

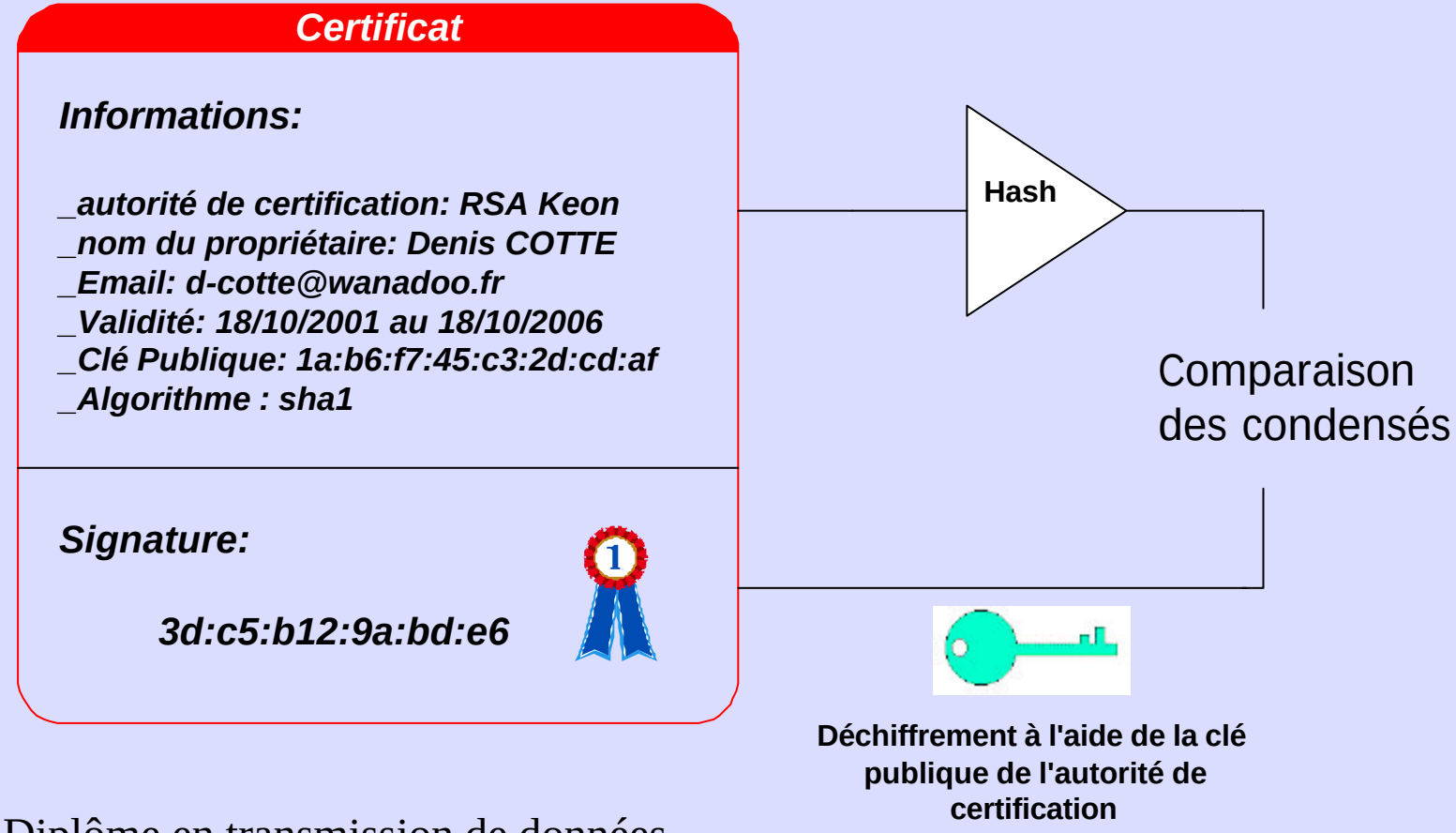
PKI : Certificats numérique

- Constitution



PKI : Vérifier un certificat

- Comparaison des condensés



PKI : Format DER et PEM

2 formats pour représenter un certificat numérique

- DER: *Distinguished Encoding Rules*

Utilisation des règles d'encodage DER sur la notation ASN1 (utilisée dans les RFCs)

ASN1:

```
Certificate  ::=  SEQUENCE  {
    tbsCertificate       TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signature            BIT STRING
}
```

- PEM: *Privacy Enhanced Mail*

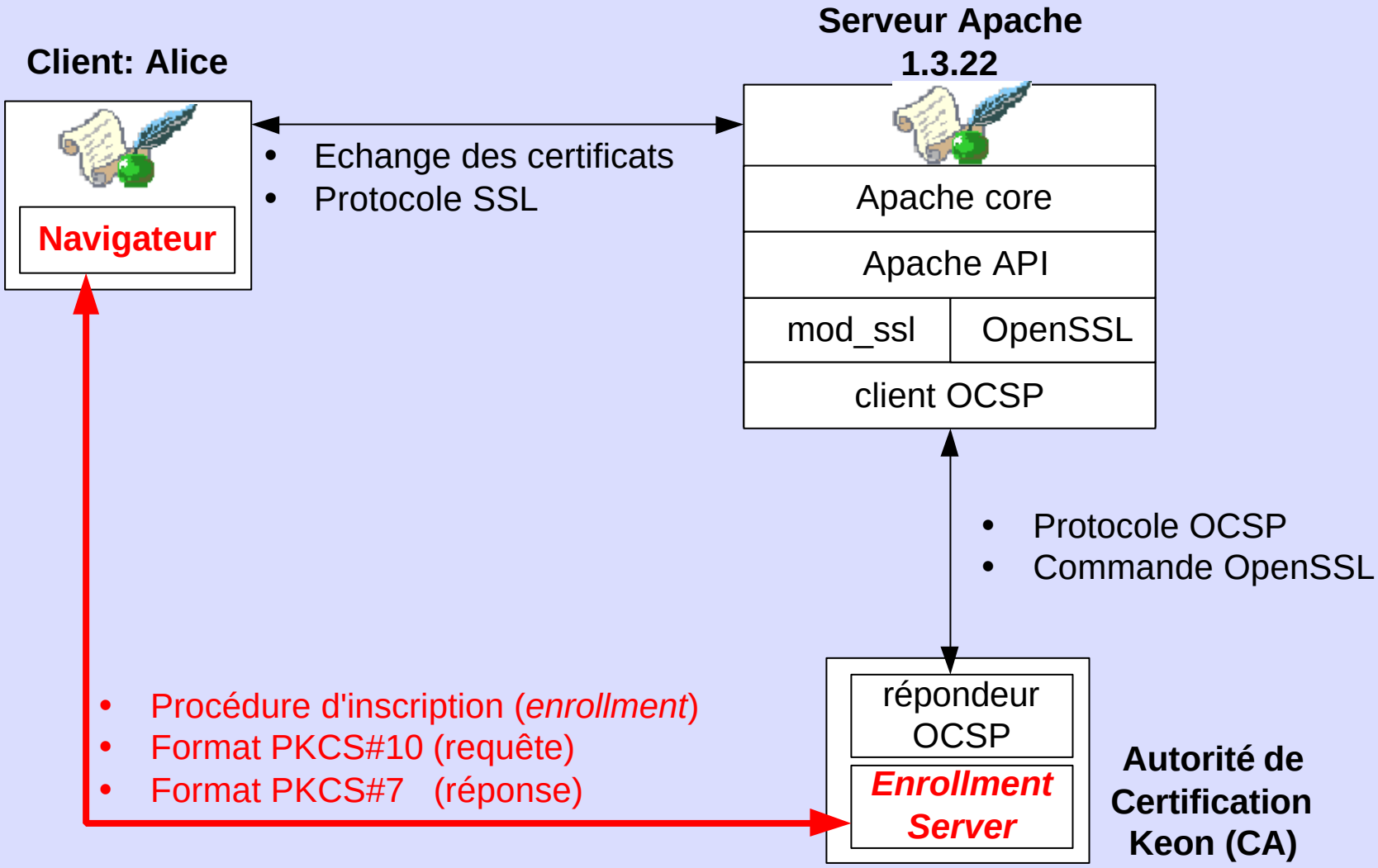
Utilisation de l'encodage **base64** pour passer au format à PEM.

```
-----BEGIN CERTIFICATE-----
MIIDDzCCAnigAwIBAgIQQCGkq2tbn5cBywZjDwhu0DANBgkqhkiG9w0BAQUFADCB
gjELMAkGA1UEBhMCQ0gxDDAKBgNVBAgTA2d2YTEPMA0GA1UEBxMGZ2VuZXZlMQww
...
mPQSr7GBdiIad3n9e4DOrwDOZ59MQ65Vh9NyNCUq2NhGd6vkPYgMJ08UD0wTqzh7
JfxrKZ7K3T80mgiLvB+0QYKUZvlQY3ot6d1Jd9qwbc+FL6ykA2qnIJ2zvQGqghfo
4saPp8qkCrOYOj5ruR398J4YKA==
-----END CERTIFICATE-----
```

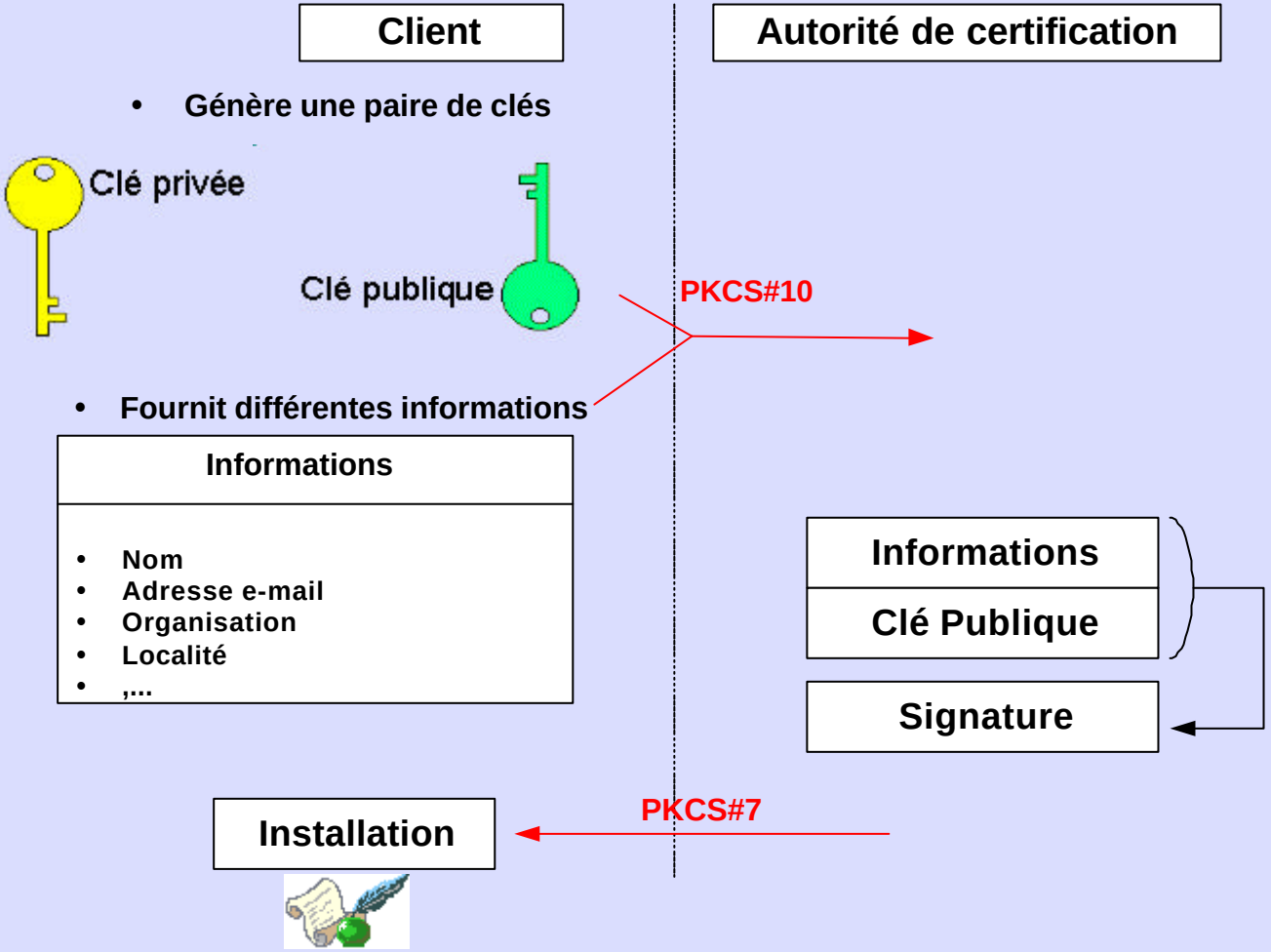
Sommaire

- PKI : Infrastructure à clé publique
- Enrollment : Procédure d'inscription
- Protocole OCSP
- Server Apache
- Conclusion

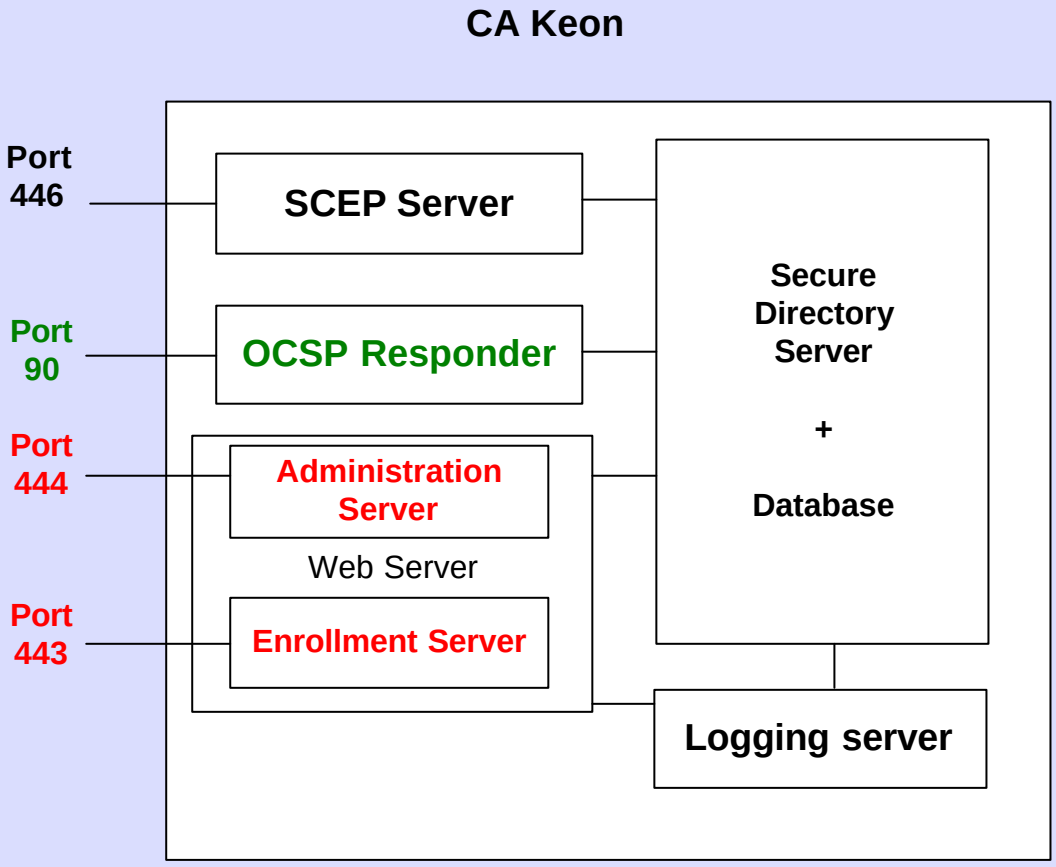
Enrollment : Architecture



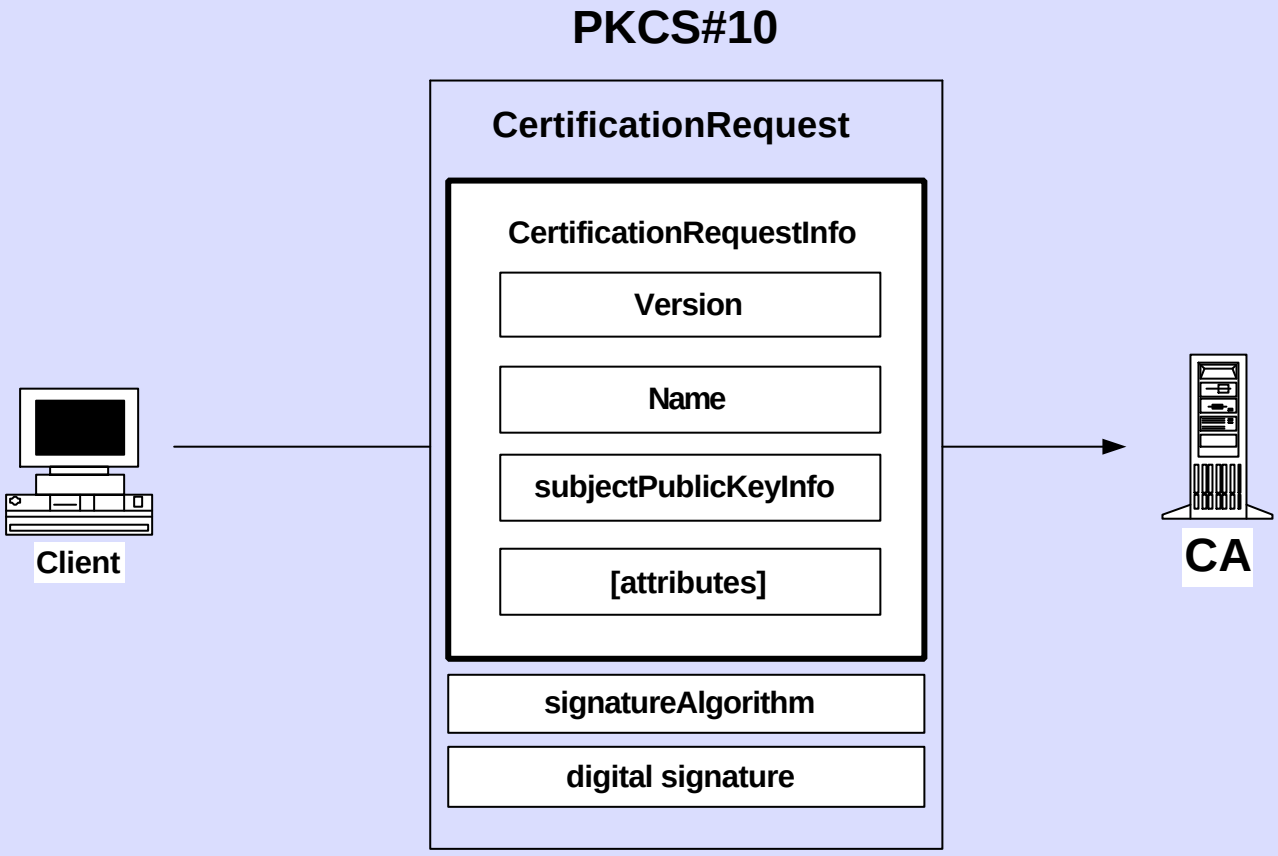
Enrollment : Principe



Enrollment : Architecture CA Keon



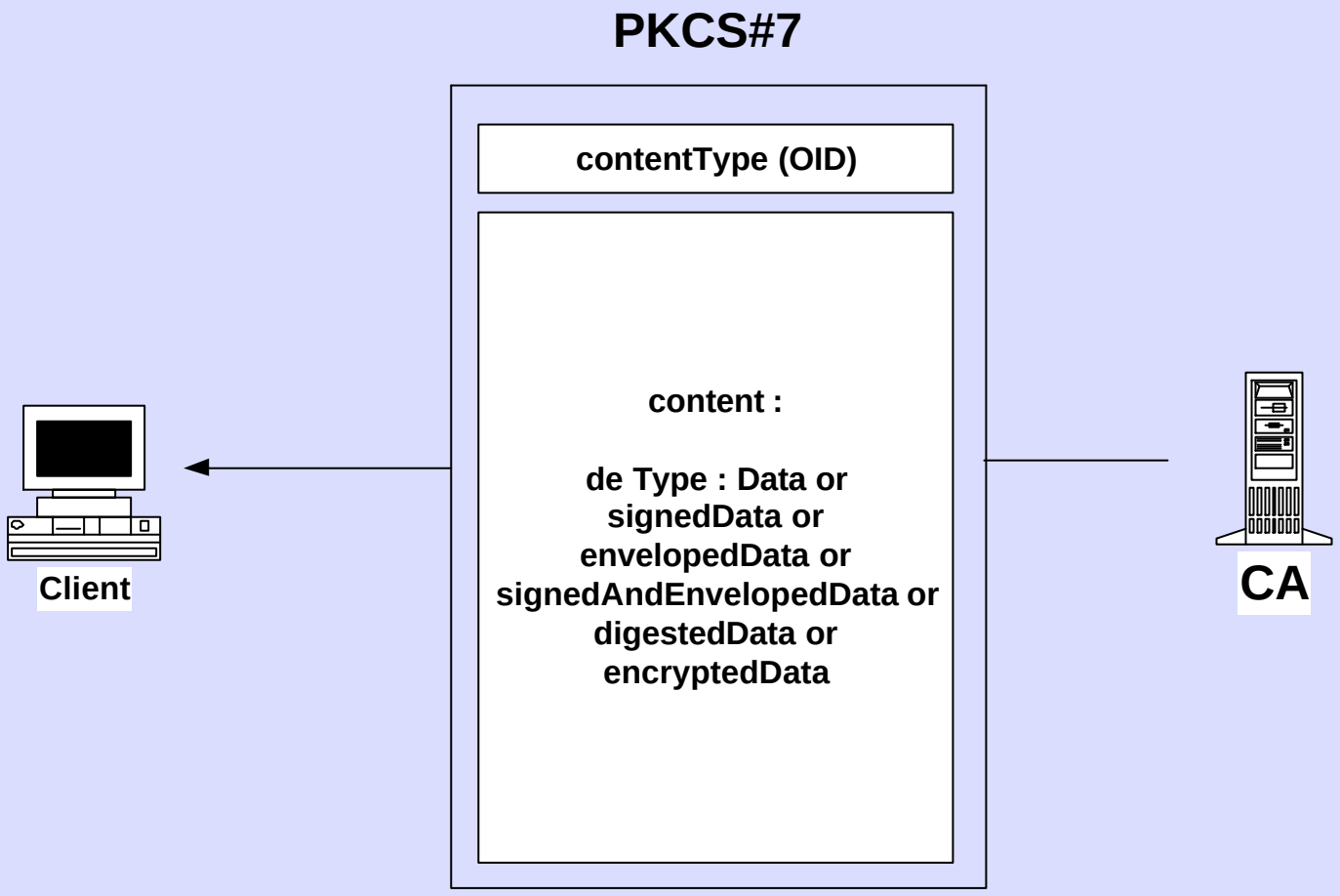
Enrollment : requête PKCS#10



Enrollment : PKCS#10 avec *OpenSSL*

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CH, ST=GVA, L=Geneve, O=eig, CN=cot2/Email=d-cotte@wanadoo.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:aa:f0:7a:56:4b:01:89:d3:12:9f:a0:05:70:30:
                    66:46:72:30:9d:ac:44:52:6d:1d:e7:0a:41:a7:2c:
                    52:60:e4:2e:36:1a:6d:77:f7:e5:ca:85:d8:2e:db:
                    fa:3f:c4:7c:83:5e:f2:4f:ae:fc:18:bf:71:64:e7:
                    8c:36:0b:dc:37
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: md5WithRSAEncryption
        40:f3:47:7a:90:9d:f6:66:35:3e:0b:2a:22:1f:a4:b3:8b:33:
        1e:d2:aa:11:02:89:70:3a:59:39:0e:87:bf:04:e3:e5:14:fe:
        05:6d:dc:03:f3:ba:65:73:01:2e:20:c8:4c:c6:4f:fc:ed:8a:
        e7:22:ae:96:51:eb:1e:0e:d4:96
-----BEGIN CERTIFICATE REQUEST-----
MIIBJjCB0QIBADBsMQswCQYDVQQGEwJDSDEMMAoGA1UECBMDR1ZBMQ8wDQYDVQQH
EwZHZW5ldmUxDDAKBgNVBAoTA2VpZzENMAsGA1UEAxMEY290MjEhMB8GCSqGSIb3
DQEJARYSZC1jb3R0ZUB3YW5hZG9vLmZyMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
AKrwelZLAYnTEp+gBXAwZkZyMJ2sRFJtHecKQacsUmDkLjYabXf35cqF2C7b+j/E
fINe8k+u/Bi/cWTnjDYL3DcCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA0EAQPNHepCd
9mY1PgsqIh+ks4szHtKqEQKJcDpZOQ6HvwTj5RT+BW3cA/O6ZXMBLiDITMZP/O2K
5yKullHrHg7Ulg==
-----END CERTIFICATE REQUEST-----
```

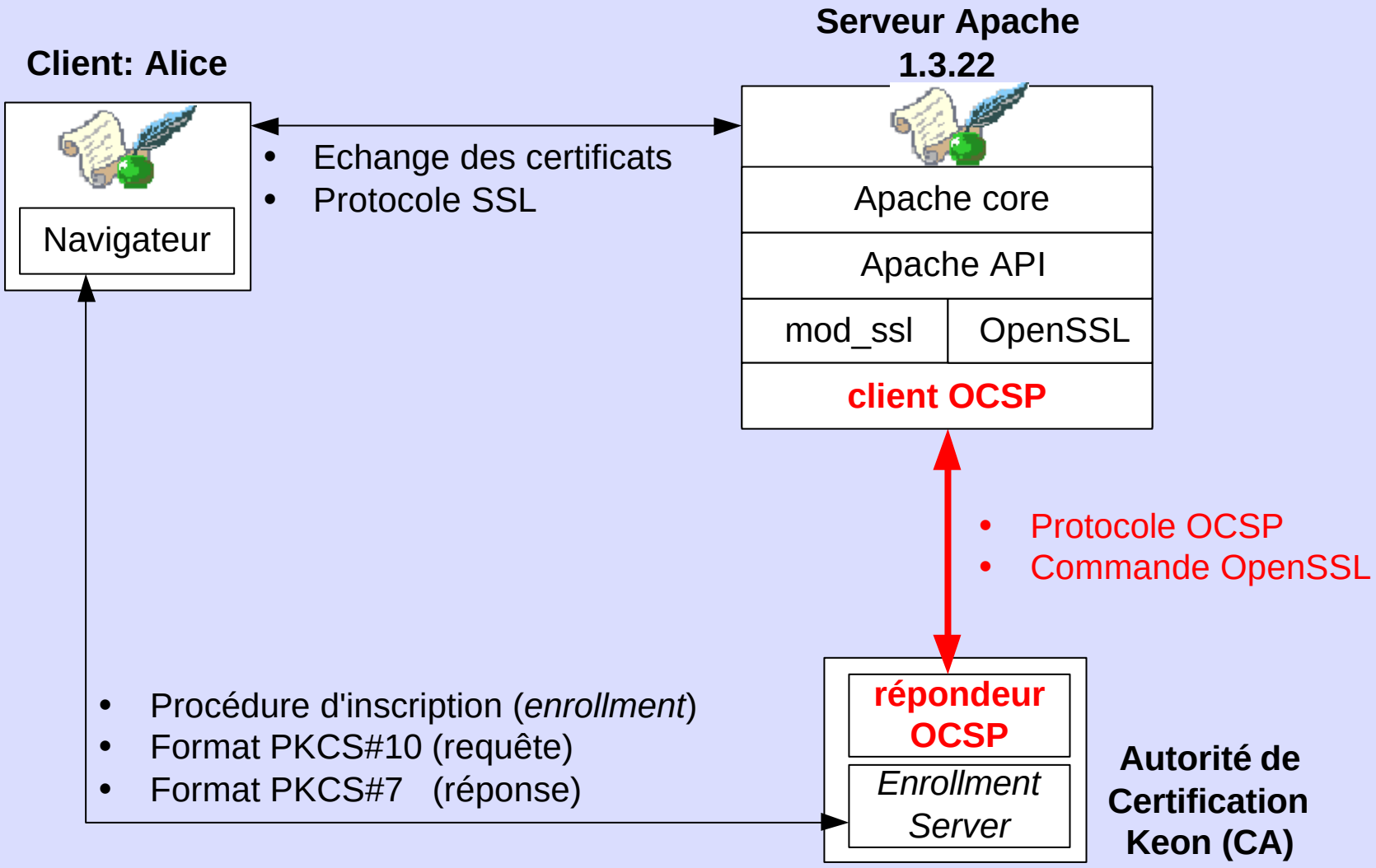
Enrollment : Réponse PKCS#7



Sommaire

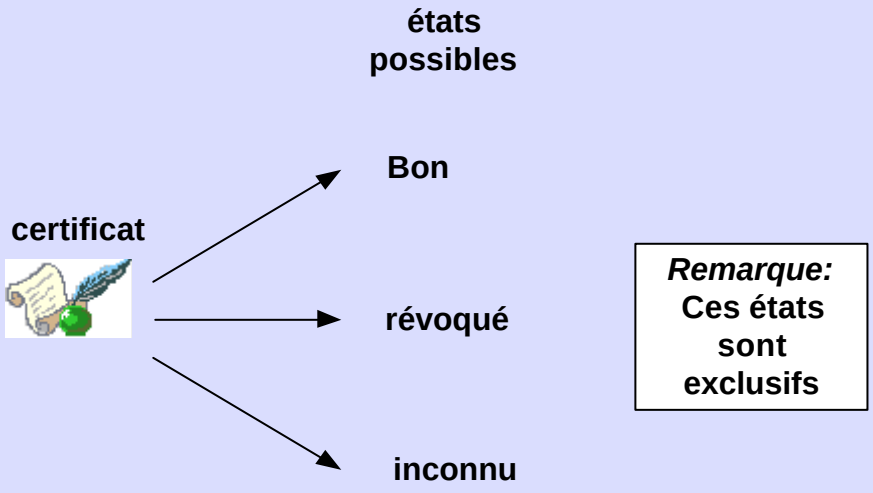
- PKI : Infrastructure à clé publique
- Enrollment : Procédure d'inscription
- Protocole OCSP
- Server Apache
- Conclusion

OCSP : Architecture

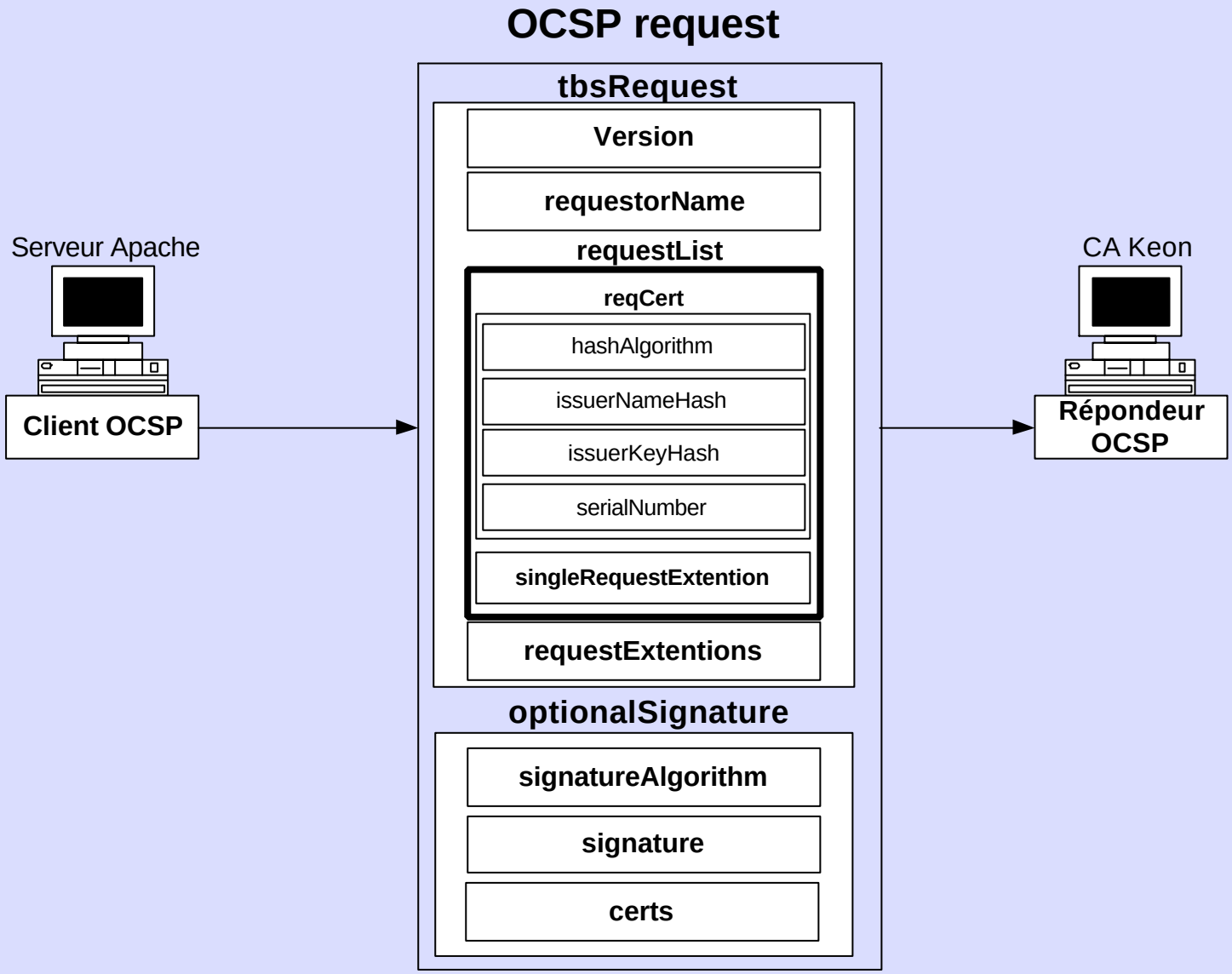


OCSP : Principe

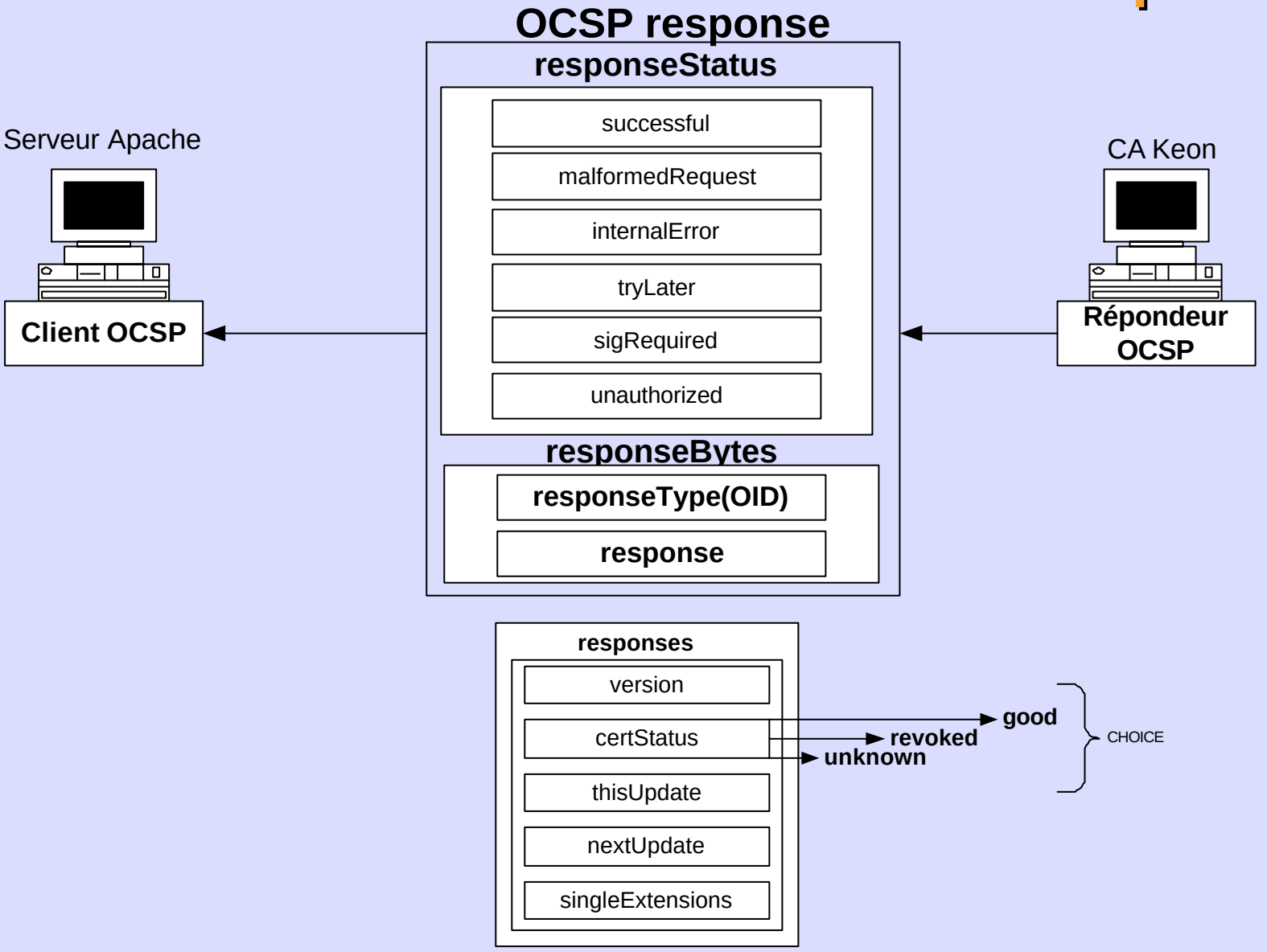
- OCSP : *Online Certificate Status Protocol*
- Vérifie l'état d'un certificat.
- Mécanisme Requête/Réponse.



OCSP : Constitution d'une Requête

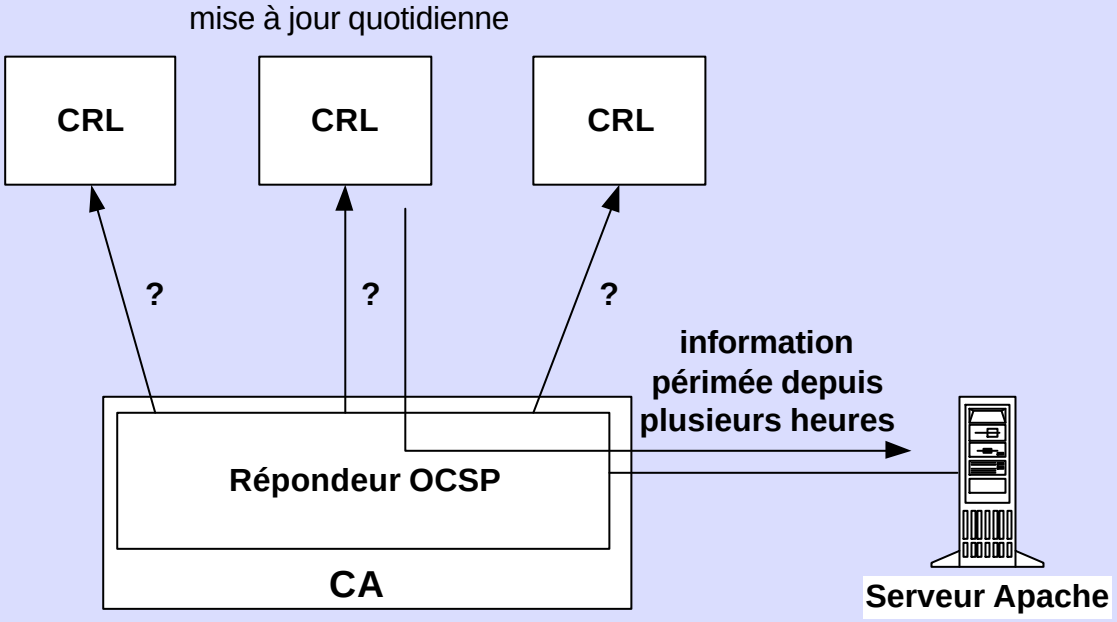


OCSP : Constitution d'une Réponse

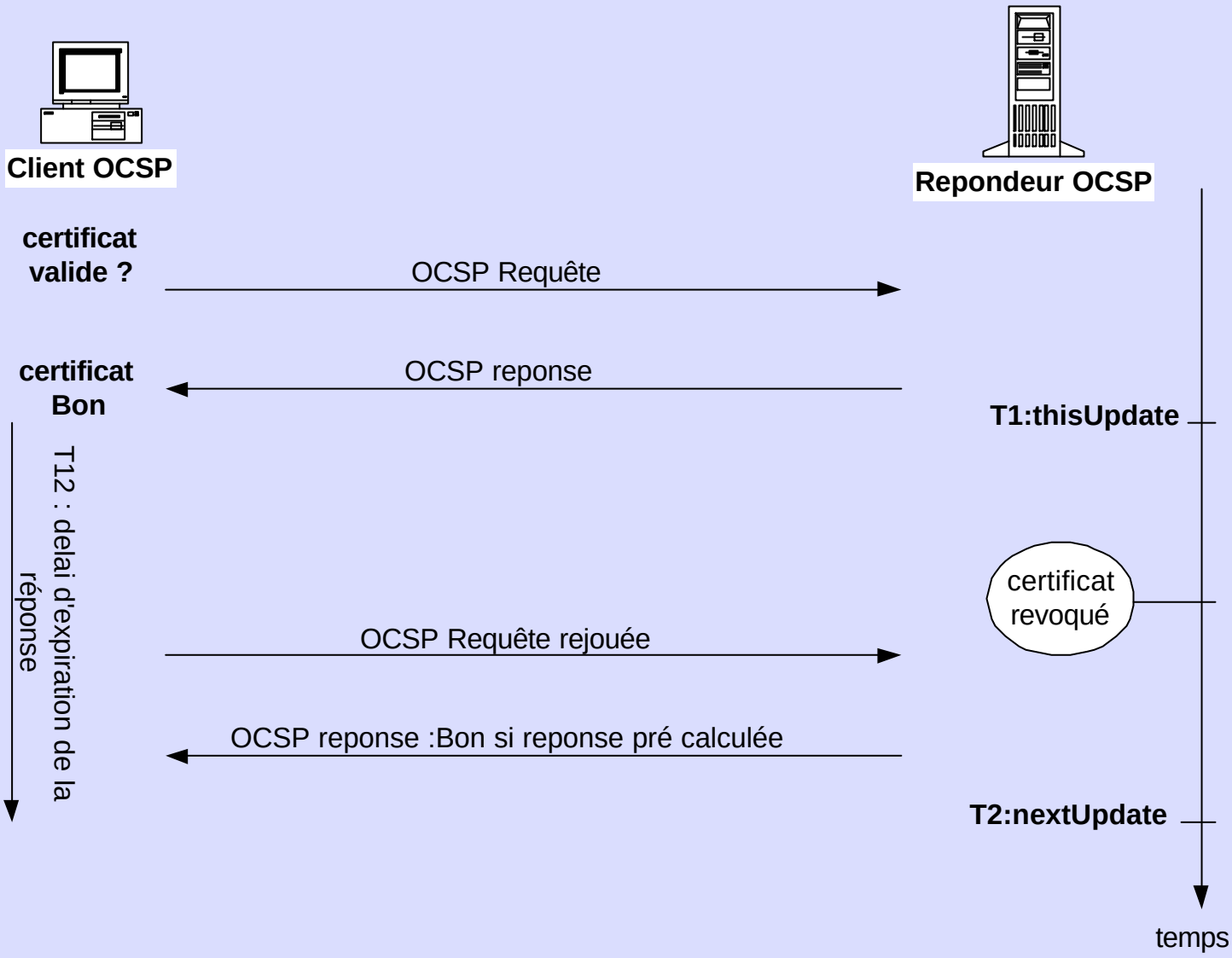


Remarques

- Utilisation des *CRLs* comme sources d'informations.



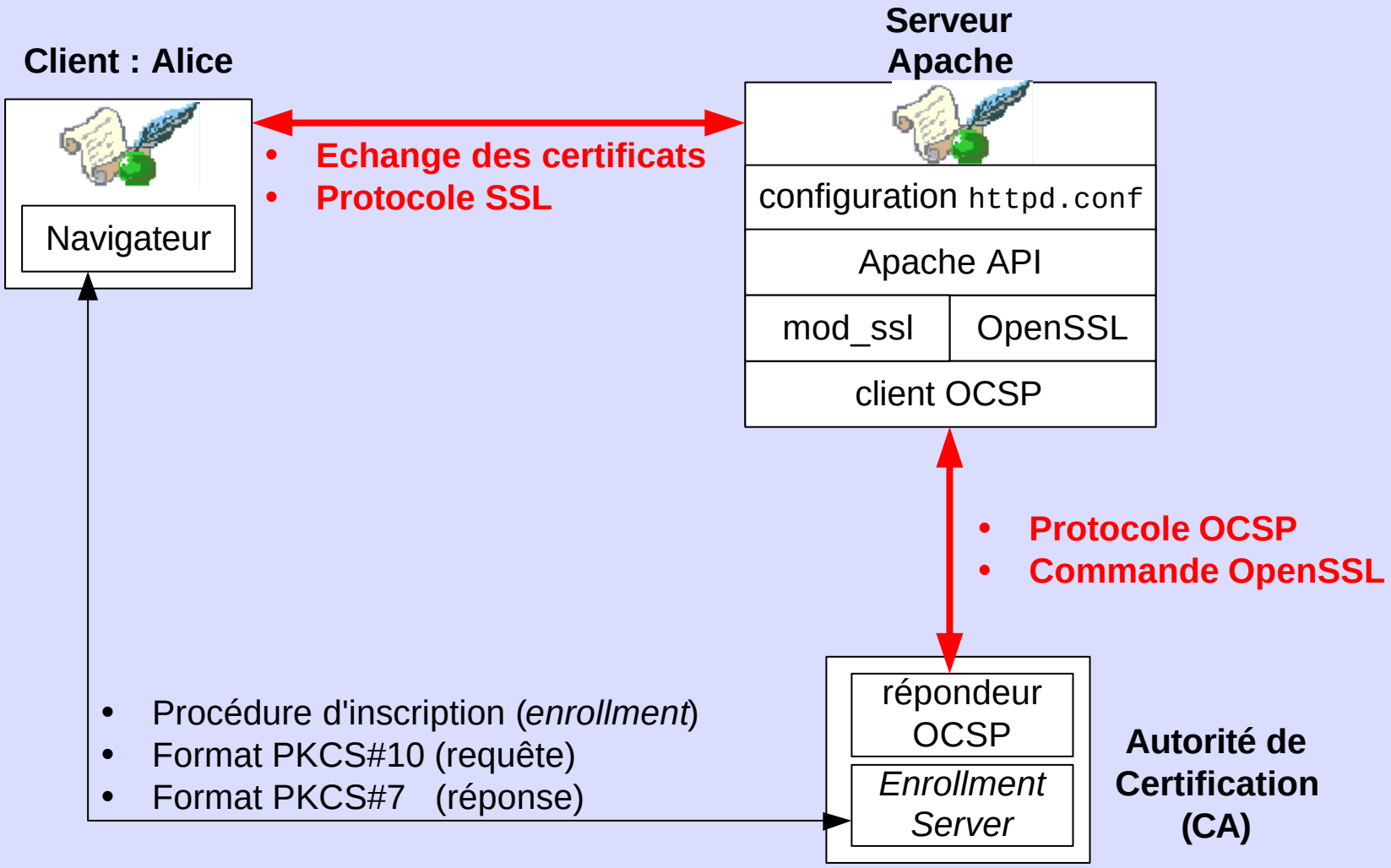
- Les réponses OCSP pré calculées



Sommaire

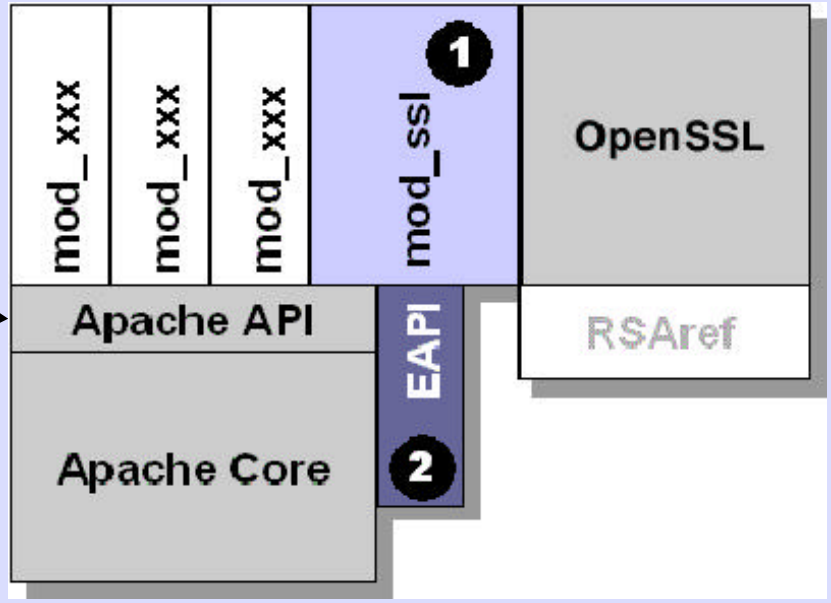
- PKI : Infrastructure à clé publique
- Enrollment : Procédure d'inscription
- Protocole OCSP
- Server Apache
- Conclusion

Apache : Architecture



Apache: Architecture du module SSL

Utilisation de la librairie d'*OpenSSL*



Utilisation des fonctions de base d'Apache

Série de patchs additionnels à Apache (*Extended API*)

Apache : Configuration `httpd.conf`

HTTPS sur port 443

Active/Désactive SSL

Certificat du serveur Apache

Clé associée au certificat

Certificat du CA racine

Authentification Client

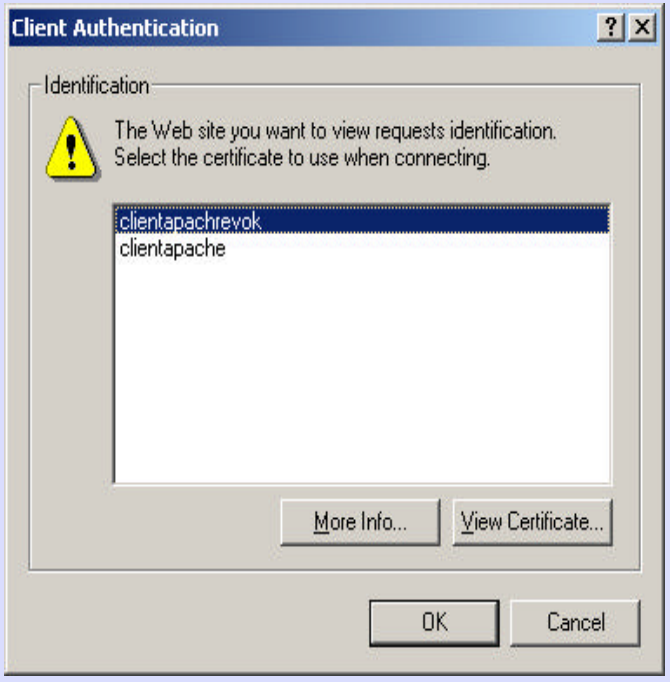
Profondeur de vérification

```
# httpd.conf
 .
<IfDefine SSL>
Listen 443
</IfDefine>
 .
<VirtualHost _default_:443>
SSLEngine on
 .
 .
SSLCertificateFile /usr/../ssl.crt/certificat_apache.crt
 .
 .
SSLCertificateKeyFile /usr/../ssl.key/certificat_apache.key

SSLCACertificateFile /usr/../ssl.crt/rootscepca.crt

SSLVerifyClient require

SSLVerifyDepth  4
 .
 .
```

Apache : L'authentification

Authentification Client avec les directives:

(*SSLVerifyClient*, *SSLVerifyDepth*, *SSLCACertificateFile*)

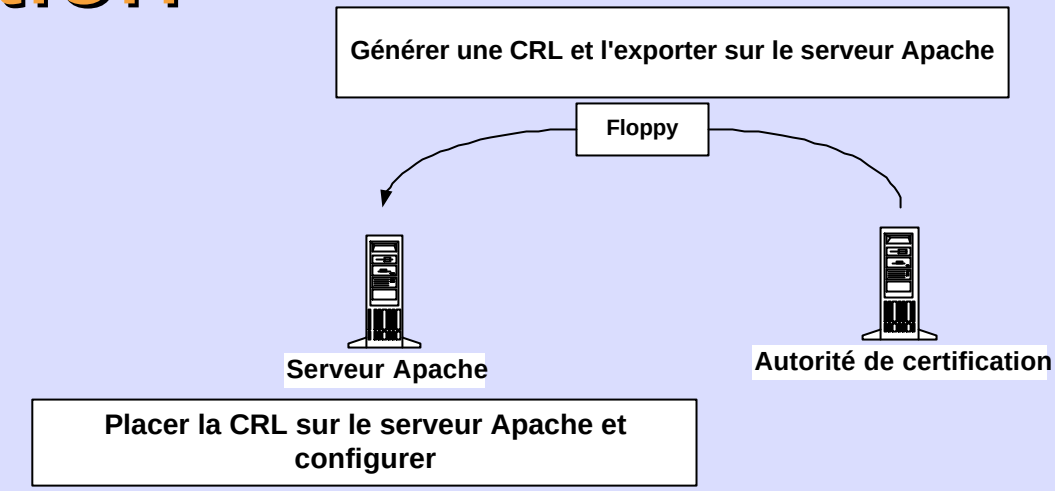


Authentification Serveur avec les directives:

(*SSLCertificateFile*, *SSLCertificateKeyFile*)

Apache : utilisation CRL

démo2



Fichier contenant la CRL

```
# httpd.conf
  .
  .
SSLCACertificateFile /usr/../ssl.crt/rootscepca.crt

SSLCARevocationFile /usr/../ssl.crl/rootscepcrl.crl

SSLVerifyClient require
  .
  .
```

Recherche le numéro de série du certificat dans la CRL.

Apache : Utilisation d' OCSP

```
Httpd.conf:
SSLOCSPVerify enable
#SSLCARevocationFile
```

Serveur Apache

Client OCSP

Autorité de certification

Répondeur OCSP

Certificat Client

SSL →

État = **?** → Requête OCSP

Réponse OCSP →

Valide

Revoqué,

Inconnu

→ Accès aux ressources du serveur Apache

→ Accès au serveur Apache refusé

Fonction OCSP avec *OpenSSL*

- Commande *OpenSSL:*

> Openssl ocsp –url http://129.194.187.55:90/ocsp.xuda -issuer rootscepca.crt –VAfile ocsproot.crt –cert clientapache.crt

- Réponse associée:

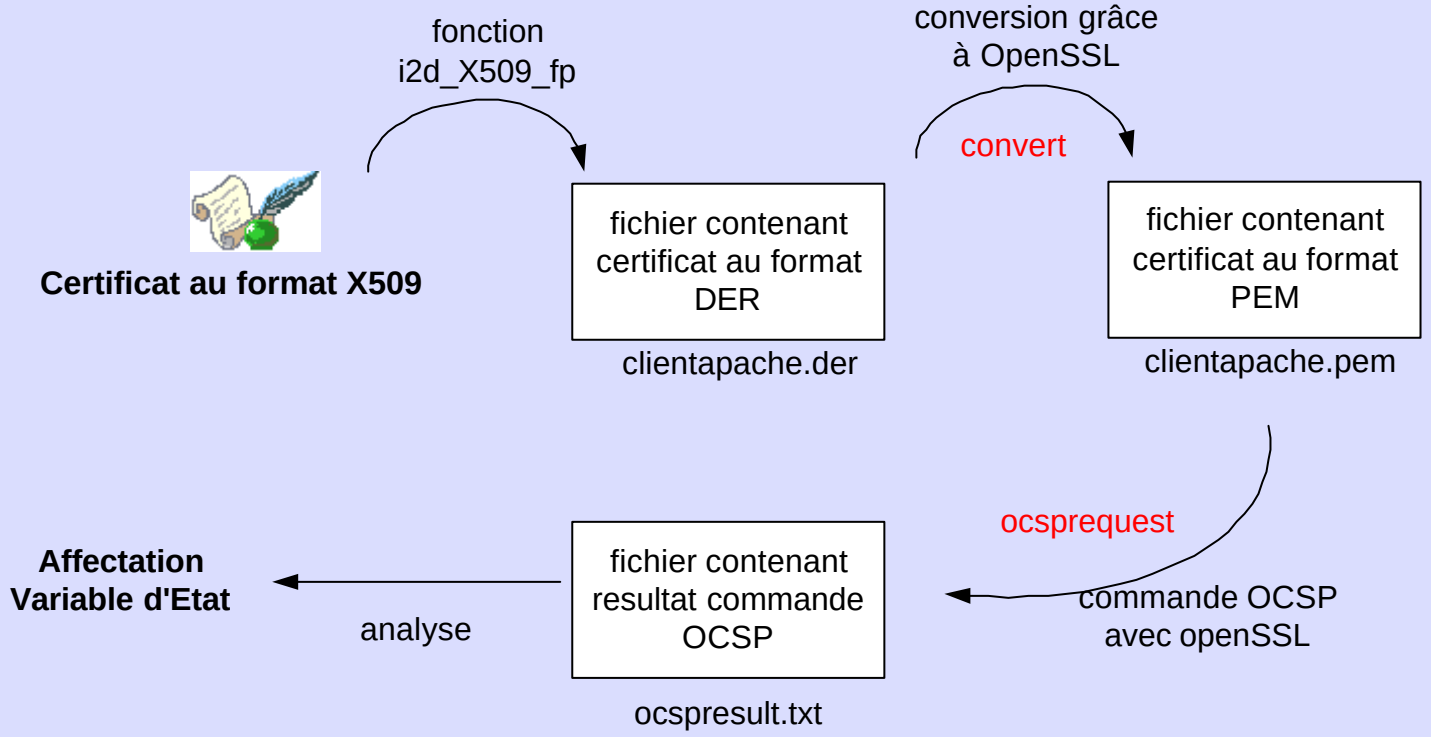
Response verify : OK

clientapache.crt : good

This UpDate : Oct 17 10 :12 :03 2001 GMT

Codage Client OCSP

- Récupérer le certificat du client lors de la phase d'authentification au format DER (fonction *i2d_X509_fp*)
- Convertir le certificat du format DER au format PEM. (*OpenSSL*)
- Envoyer la requête au répondeur OCSP. (*OpenSSL*)
- Lecture du fichier contenant la réponse OCSP.



Conclusion

- Procédure d'inscription (*enrollment*)
- Etude protocole OCSP
- Vérification par CRL
- Vérification par OCSP
- Possibilités d'optimisation

Planning du diplôme

Tâche	Descritption	
A	Installation + prise en main de la CA Keon	Points 1&2
B	Recherche d'Informations sur les protocoles de gestion des PKI	
C	Mise en pratique de la procédure d'inscription	
D	Etude du protocole OCSP; comparaison avec les CRLs	Point 3
E	Installation et configuration du Serveur Apache	Point 4
F	Etude du module SSL	
G	Implémentation Fonction OCSP	
H	Ecriture du mémoire