La signature numérique

Bruno Bonfils, <asyd@asyd.net>

2 Juillet 2008

Petits rappels 1/2

Petits rappels 1/2

- Principe des clés asymétriques :

Petits rappels 1/2

- Principe des clés asymétriques :
  - Deux clés différentes (une privée, une publique) (RSA, DSA)

Petits rappels 1/2

- Principe des clés asymétriques :
  - Deux clés différentes (une privée, une publique) (RSA, DSA)
  - Une clé chiffre, l'autre déchiffre

Petits rappels 1/2

- Principe des clés asymétriques :
  - Deux clés différentes (une privée, une publique) (RSA, DSA)
  - Une clé chiffre, l'autre déchiffre
  - En RSA, l'opération de signature n'existe pas en tant que tel, on chiffre un condensé

Petits rappels 2/2

Petits rappels 2/2

- Un condensé est une empreinte d'un document (l'empreinte a une taille fixe)

Petits rappels 2/2

- Un condensé est une empreinte d'un document (l'empreinte a une taille fixe)
  - Gestion des collisions : plusieurs documents peuvent avoir la même empreinte

Petits rappels 2/2

- Un condensé est une empreinte d'un document (l'empreinte a une taille fixe)
  - Gestion des collisions : plusieurs documents peuvent avoir la même empreinte
  - Néanmoins, une modification d'un octet du document d'origine donne un condensé totalement différent : difficulté d'obtenir un condensé unique pour un document en gardant le même contexte

Sommaire

Sommaire

- Contexte

Sommaire

- Contexte
- Approche fonctionnel

Sommaire

- Contexte
- Approche fonctionnel
- Les détails

Sommaire

- Contexte
- Approche fonctionnel
- Les détails
  - Obtention du certificat

Sommaire

- Contexte
- Approche fonctionnel
- Les détails
  - Obtention du certificat
  - Signature d’un document

Sommaire

- Contexte
- Approche fonctionnel
- Les détails
  - Obtention du certificat
  - Signature d’un document
  - Vérification d’une signature

Sommaire

- Contexte
- Approche fonctionnel
- Les détails
  - Obtention du certificat
  - Signature d’un document
  - Vérification d’une signature
- Aspects légaux et divers

Contexte légal

Contexte légal

- La signature numérique possède la même valeur légale que la signature manuscrite
  - Art. 1316-1. « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. (loi 2000 du 13 Mars 2000) »
  - Décret d'application du 30 Mars 2001

Approche fonctionnel

Approche fonctionnel

- Dématérialisation des marchés publics

Approche fonctionnel

- Dématérialisation des marchés publics
  - Nécessite un certificat émis par une autorité de confiance reconnue par l'administration

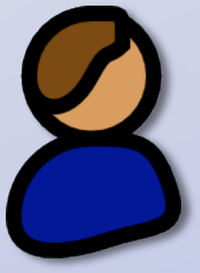
Approche fonctionnel

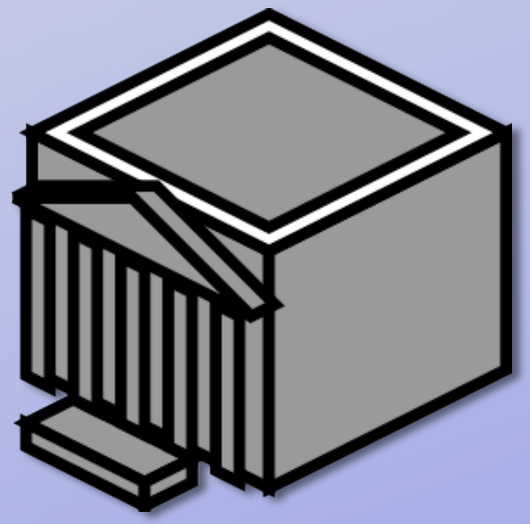
- Dématérialisation des marchés publics
  - Nécessite un certificat émis par une autorité de confiance reconnue par l'administration
- Retrait des dossiers

Approche fonctionnel

- Dématérialisation des marchés publics
  - Nécessite un certificat émis par une autorité de confiance reconnue par l'administration
- Retrait des dossiers
- Soumission de réponse signée

La signature numérique
Vue d'ensemble 1/3



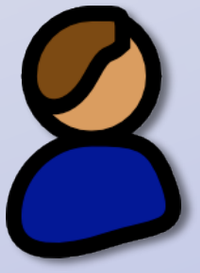


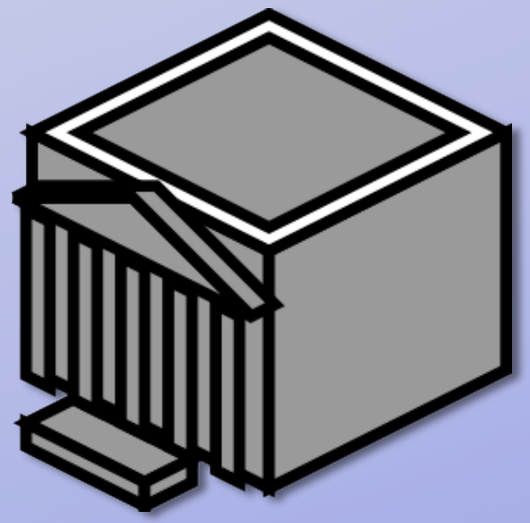
Administration

Obtention d'un certificat

La signature numérique
Vue d'ensemble 1/3

Demande de certificat



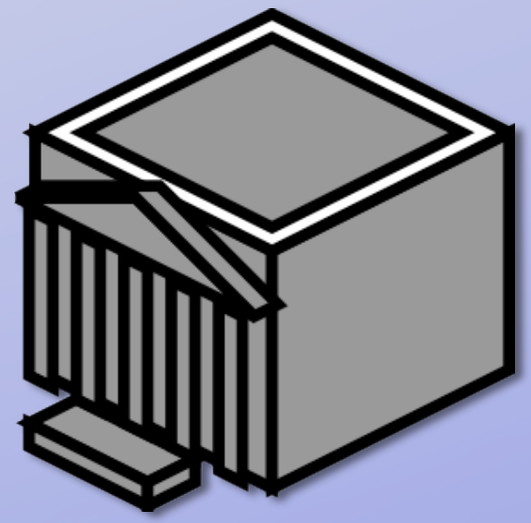


Administration

Obtention d'un certificat

La signature numérique
Vue d'ensemble 1/3

Demande de certificat

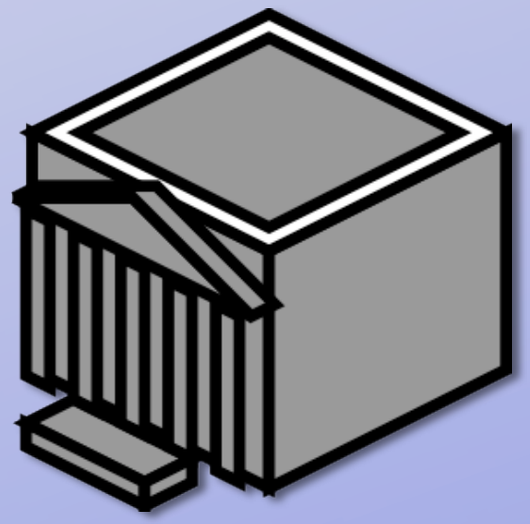


Administration

Certificat

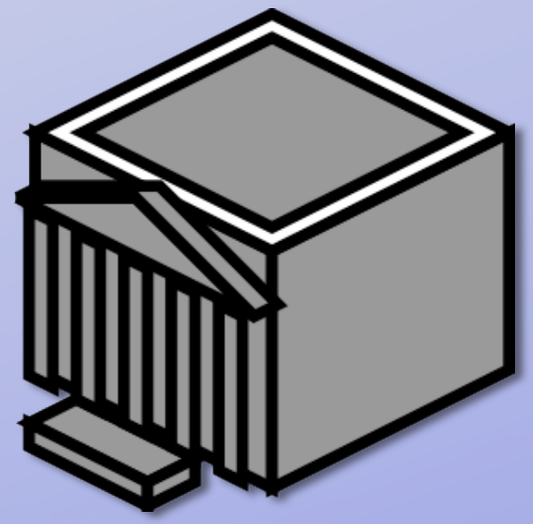
Obtention d'un certificat

La signature numérique
Vue d'ensemble 2/3



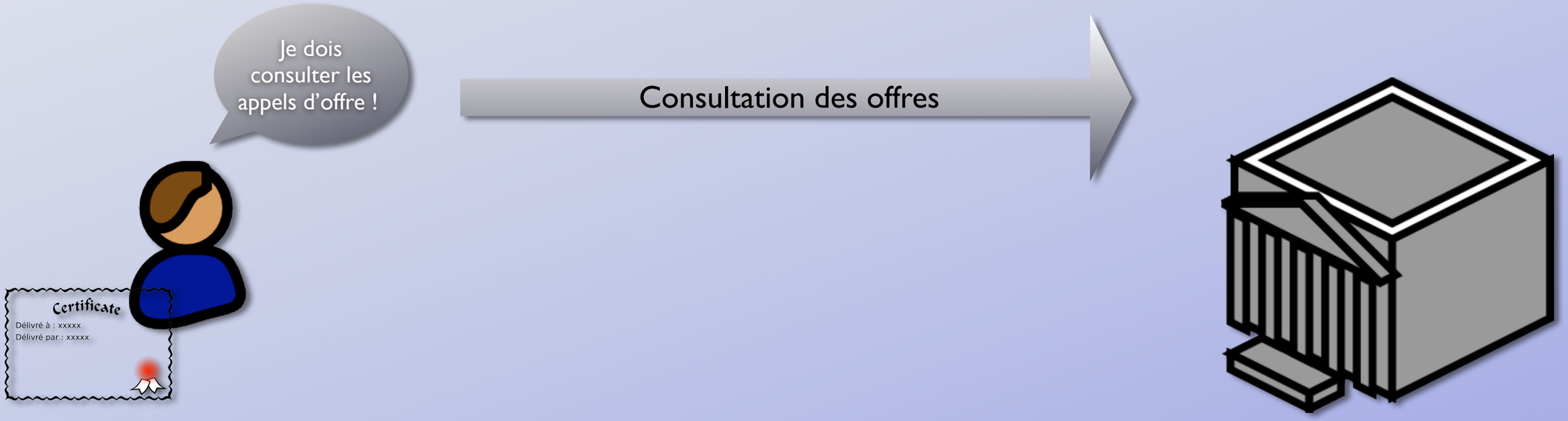
Signature d'un document

La signature numérique
Vue d'ensemble 2/3



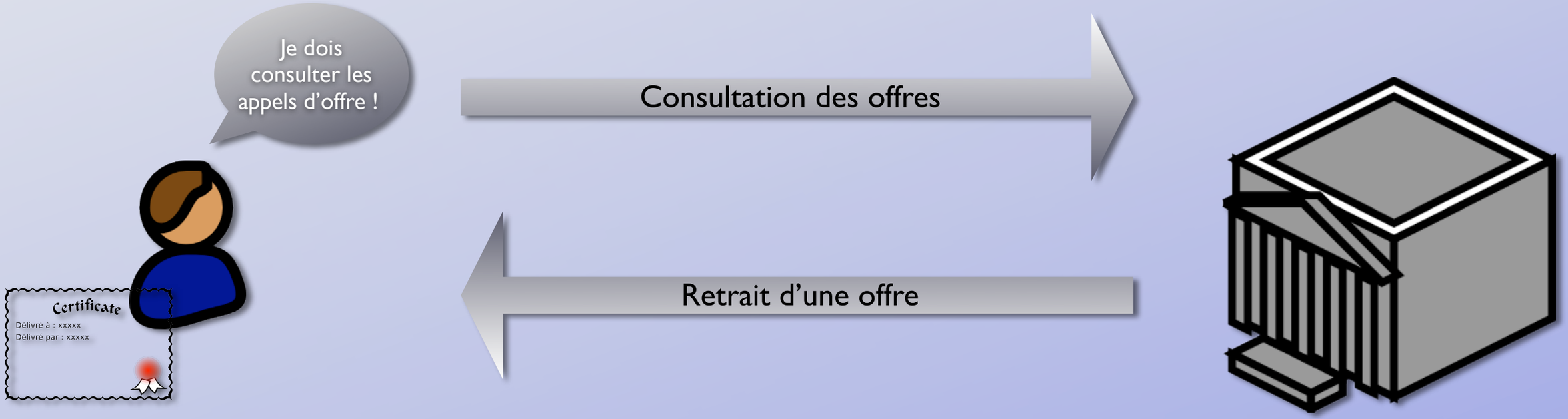
Signature d'un document

La signature numérique
Vue d'ensemble 2/3



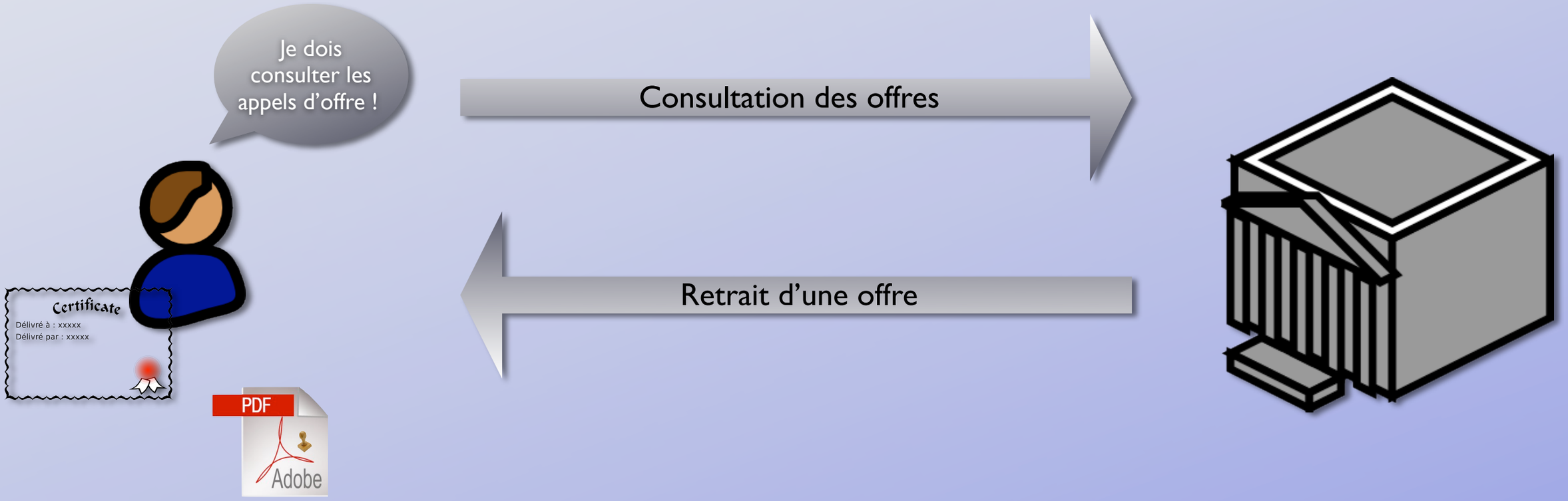
Signature d'un document

La signature numérique
Vue d'ensemble 2/3



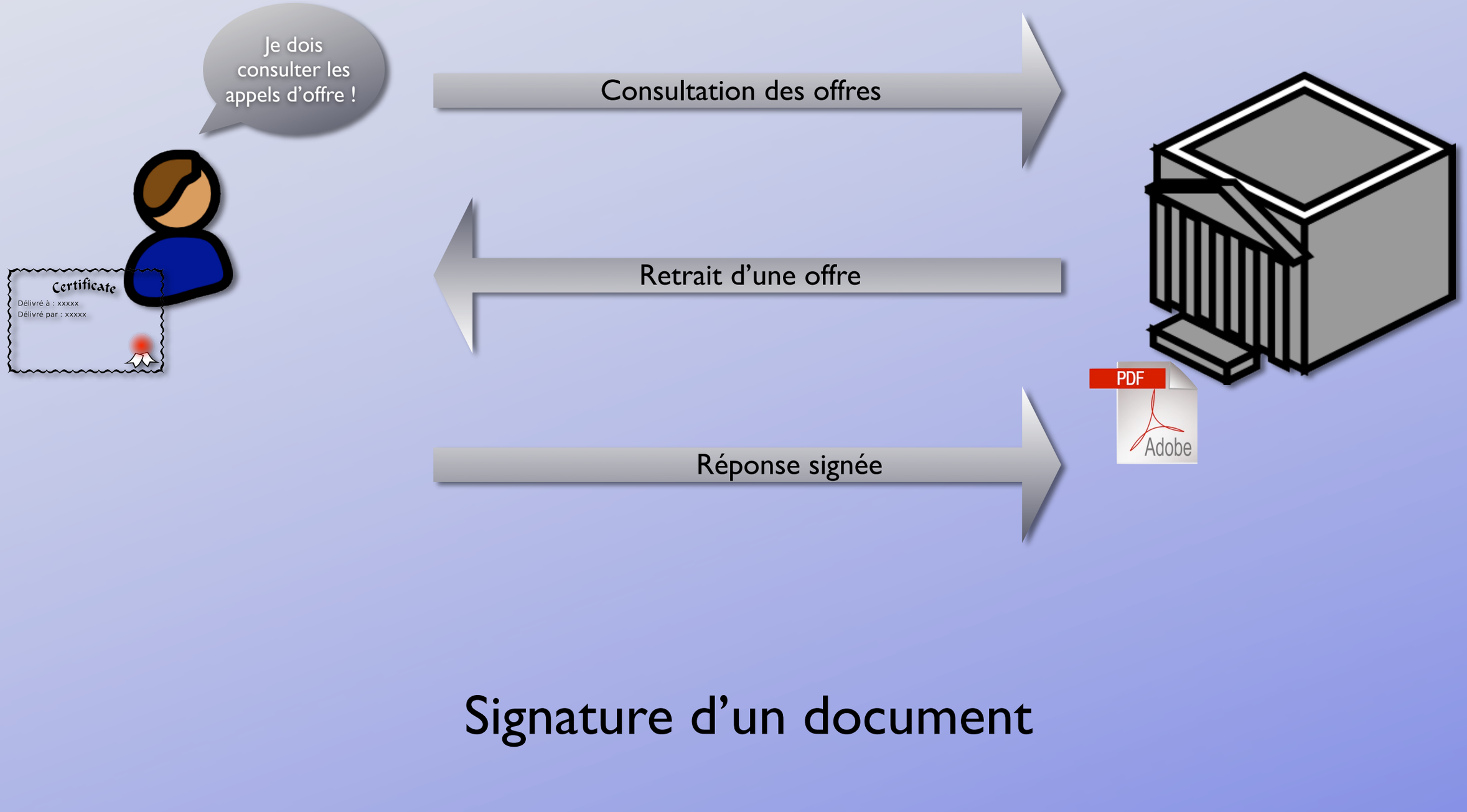
Signature d'un document

La signature numérique
Vue d'ensemble 2/3



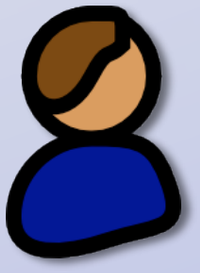
Signature d'un document

La signature numérique
Vue d'ensemble 2/3



Signature d'un document

La signature numérique
Vue d'ensemble 3/3



Dans le cas d'un PDF, le lecteur vérifie généralement lui même la signature et permet d'afficher les informations contenues dans celle-ci. Dans les autres cas il est nécessaire d'utiliser un outil tiers.

Vérification d'une signature

La signature numérique
Vue d'ensemble 3/3

Dans le cas d'un PDF, le lecteur vérifie généralement lui même la signature et permet d'afficher les informations contenues dans celle-ci. Dans les autres cas il est nécessaire d'utiliser un outil tiers.

Vérification d'une signature

La signature numérique

La signature numérique

- Les détails

La signature numérique

- Les détails
- Obtention d'un certificat

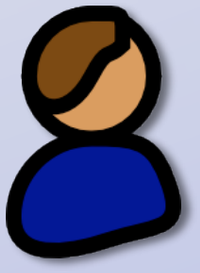
La signature numérique

- Les détails
  - Obtention d'un certificat
  - Signature d'un document

La signature numérique

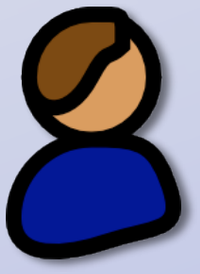
- Les détails
  - Obtention d'un certificat
  - Signature d'un document
  - Vérification d'une signature

Obtention d'un certificat



Obtention d'un certificat

1. Obtention d'un token

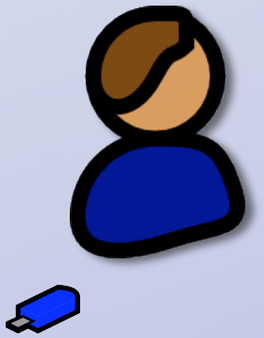


Token matériel

Les tokens matériel permettent de sécurisé les accès aux différents contenus (privé et public) en fonction d'une politique donnée. Par exemple, blocage au bout de 3 codes PIN invalides.

Obtention d'un certificat

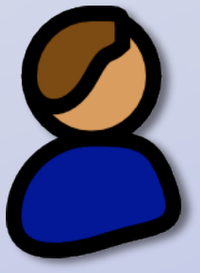
1. Obtention d'un token
2. Formulaire



Nom	Bonfils
Prénom	Bruno
Type de certificat	Signature

Obtention d'un certificat

1. Obtention d'un token
2. Formulaire
3. Génération d'une biclé par le token



Nom	Bonfils
Prénom	Bruno
Type de certificat	Signature

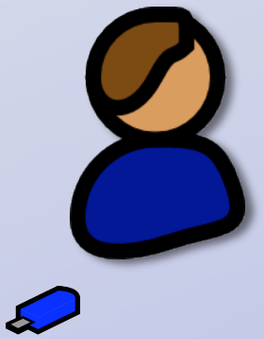
Clé privée

La clé privée ne sort jamais du token !

Clé publique

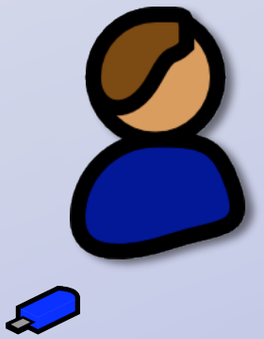
Obtention d'un certificat

1. Obtention d'un token
2. Formulaire
3. Génération d'une biclé par le token



Nom	Bonfils
Prénom	Bruno
Type de certificat	Signature

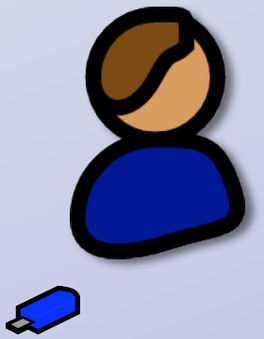
Obtention d'un certificat



Nom	Bonfils
Prénom	Bruno
Type de certificat	Signature

1. Obtention d'un token
2. Formulaire
3. Génération d'une biclé par le token
4. Envoi à l'autorité de confiance

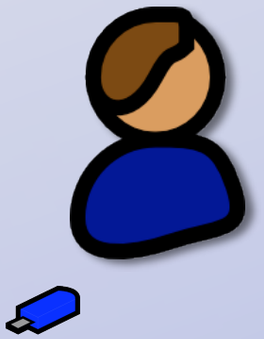
Obtention d'un certificat



CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Obtention d'un token
2. Formulaire
3. Génération d'une biclé par le token
4. Envoi à l'autorité de confiance
5. Consolidation des données

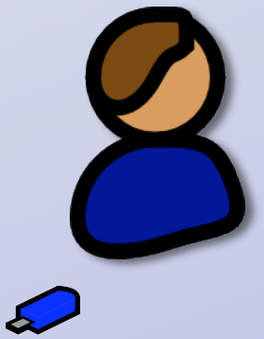
Obtention d'un certificat



CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

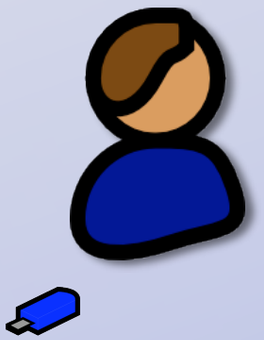
1. Obtention d'un token
2. Formulaire
3. Génération d'une biclé par le token
4. Envoi à l'autorité de confiance
5. Consolidation des données
6. Génération du certificat

Signature d’un document



Signature client

Signature d'un document

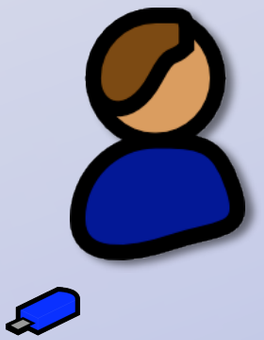


Signature client

Signature d'un document

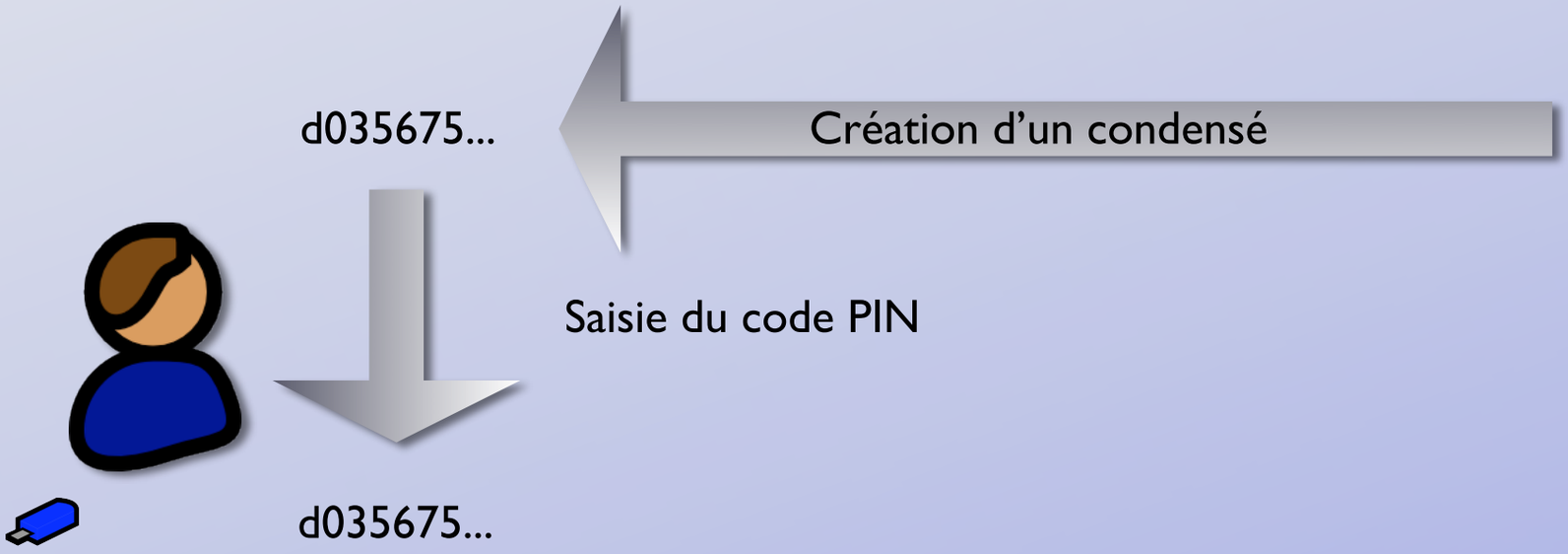
d035675...

Création d'un condensé



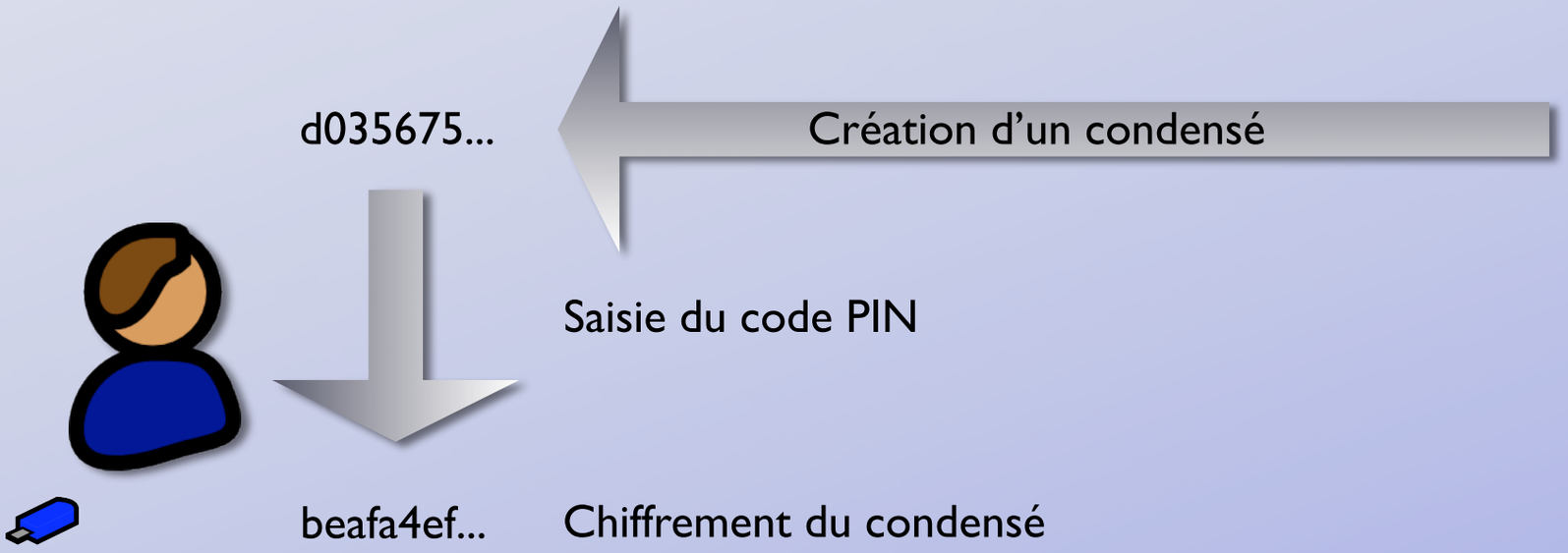
Signature client

Signature d'un document



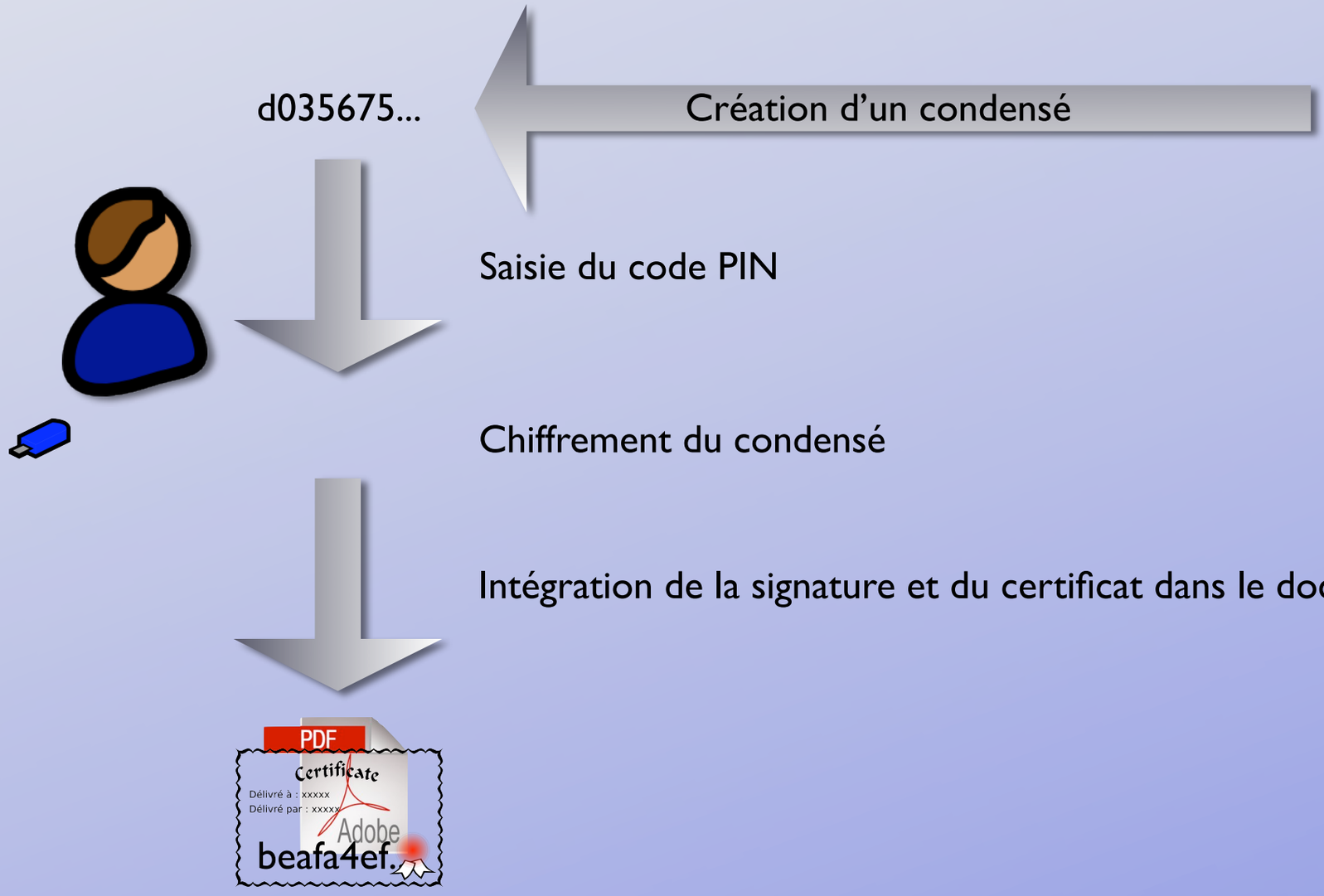
Signature client

Signature d'un document



Signature client

Signature d'un document

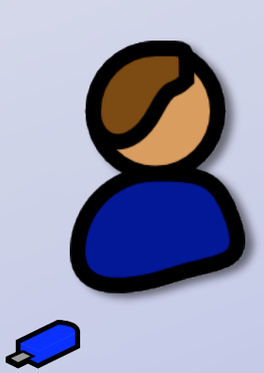


Signature client

Signature d'un document

d035675...

Création d'un condensé



Saisie du code PIN

Chiffrement du condensé

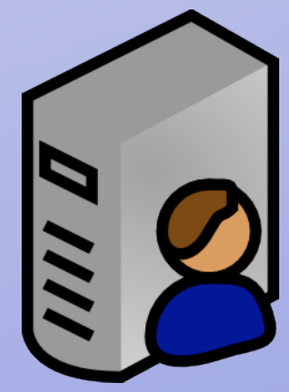
Intégration de la signature et du certificat dans le document

Émission du document signé

Signature client

Signature d'un document

Serveur de signature



Serveur OCSP

Serveur d'horodatage

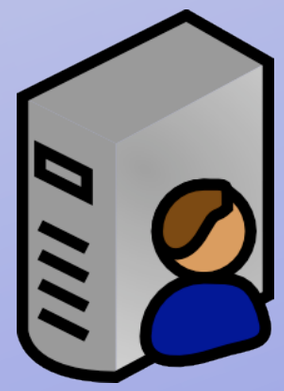
Signature serveur

Signature d’un document

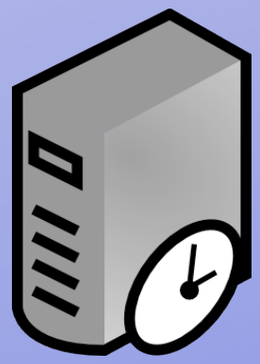
Envoi d’un document

Serveur de signature

Co/Contre signature



Serveur OCSP



Serveur d’horodatage

Signature serveur

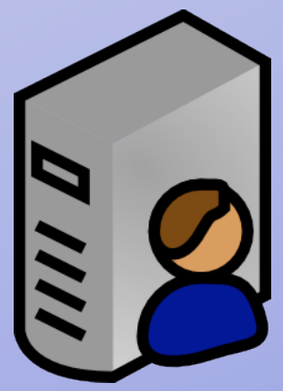
Signature d’un document

Envoi d’un document

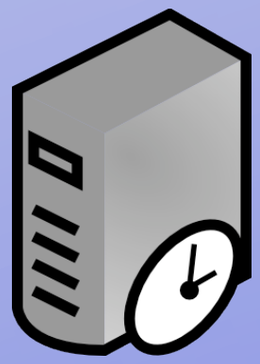
Serveur de signature

13cb43c..

Co/Contre signature



Serveur OCSP



Serveur d’horodatage

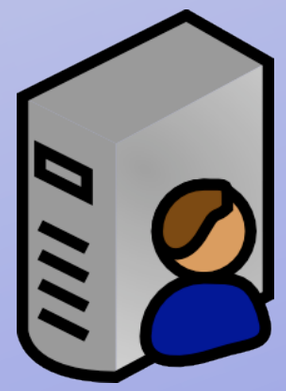
Signature serveur

Signature d’un document

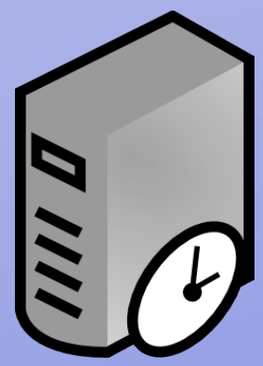
Envoi d’un document

Serveur de signature

Co/Contre signature



Serveur OCSP



Serveur d’horodatage

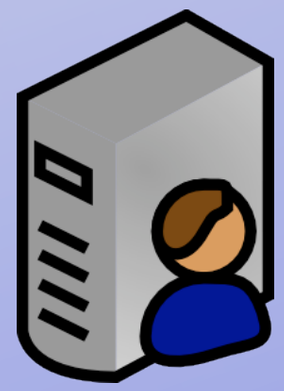
Signature serveur

Signature d’un document

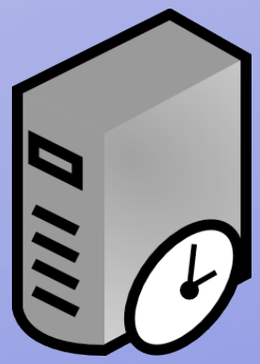
Envoi d’un document

Serveur de signature

Co/Contre signature



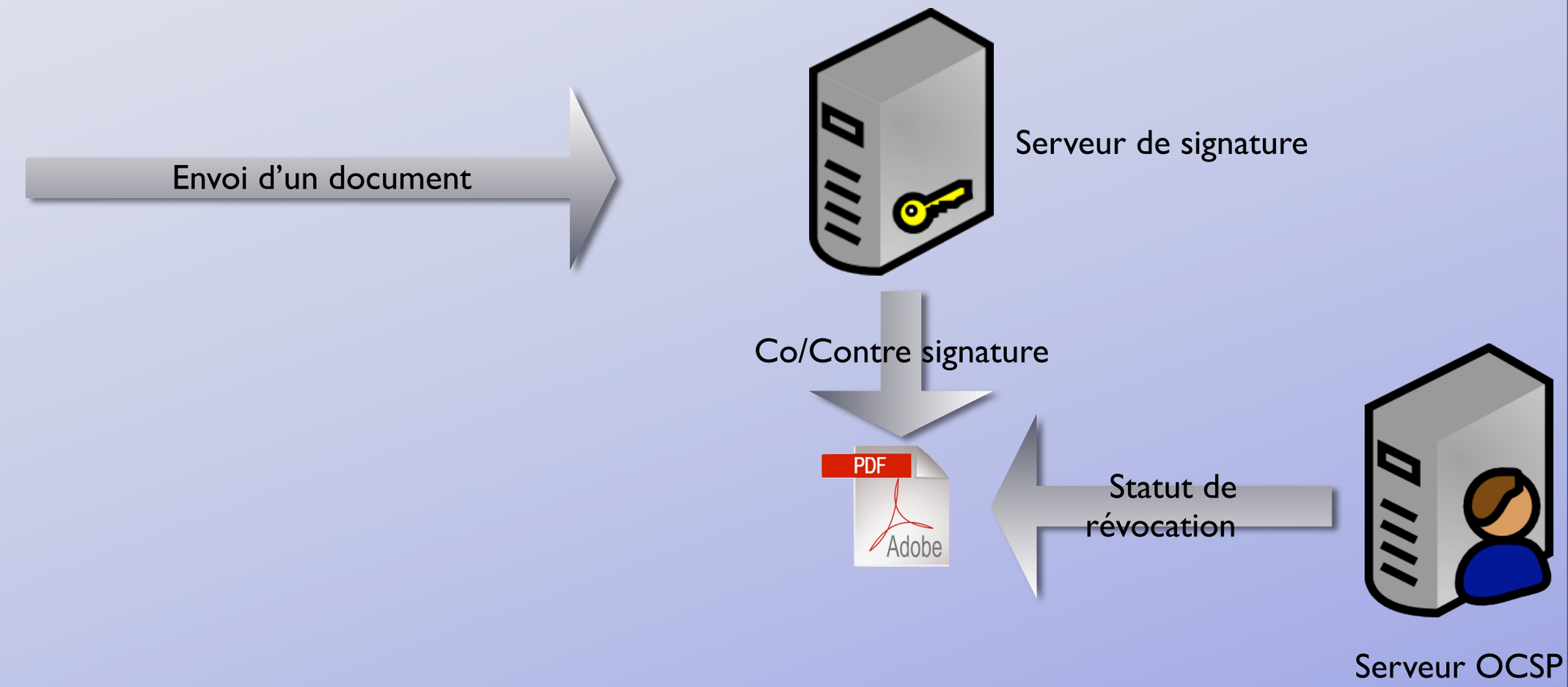
Serveur OCSP



Serveur d’horodatage

Signature serveur

Signature d'un document



Signature serveur

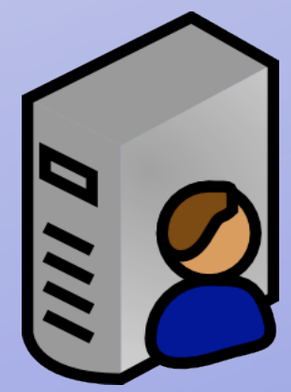
Signature d'un document

Envoi d'un document

Serveur de signature

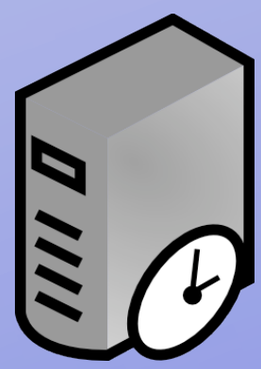
Co/Contre signature

Statut de révocation



Serveur OCSP

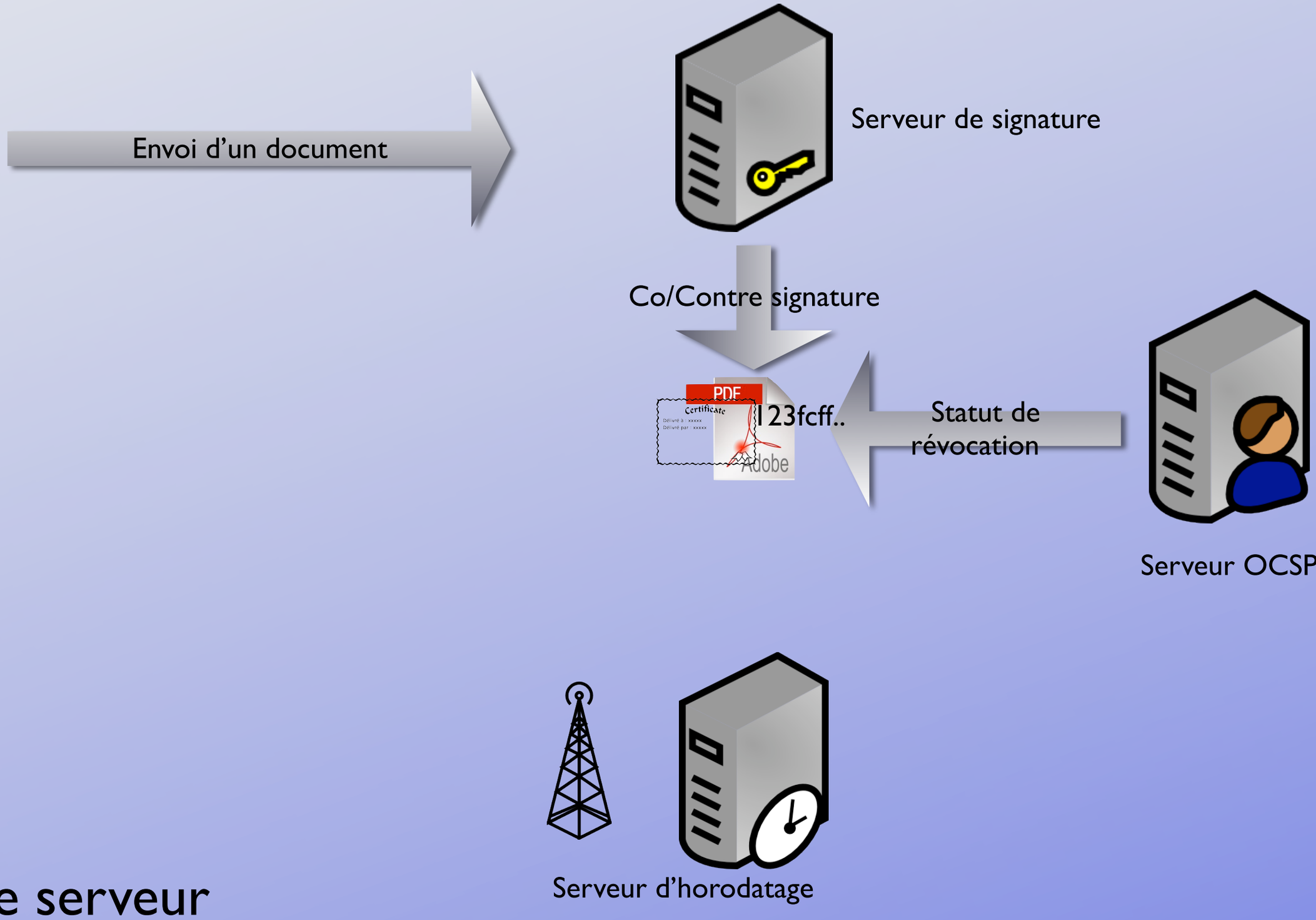
123fcff..



Serveur d'horodatage

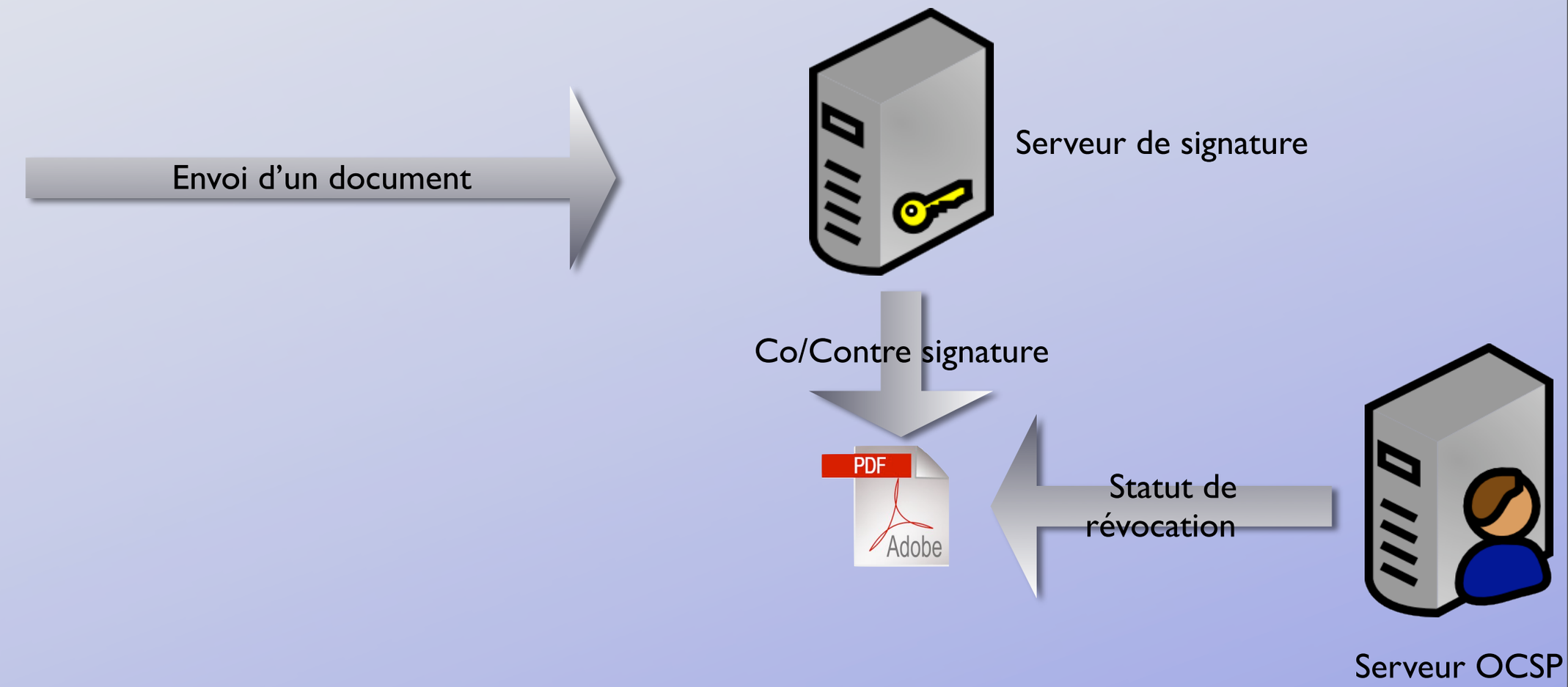
Signature serveur

Signature d'un document



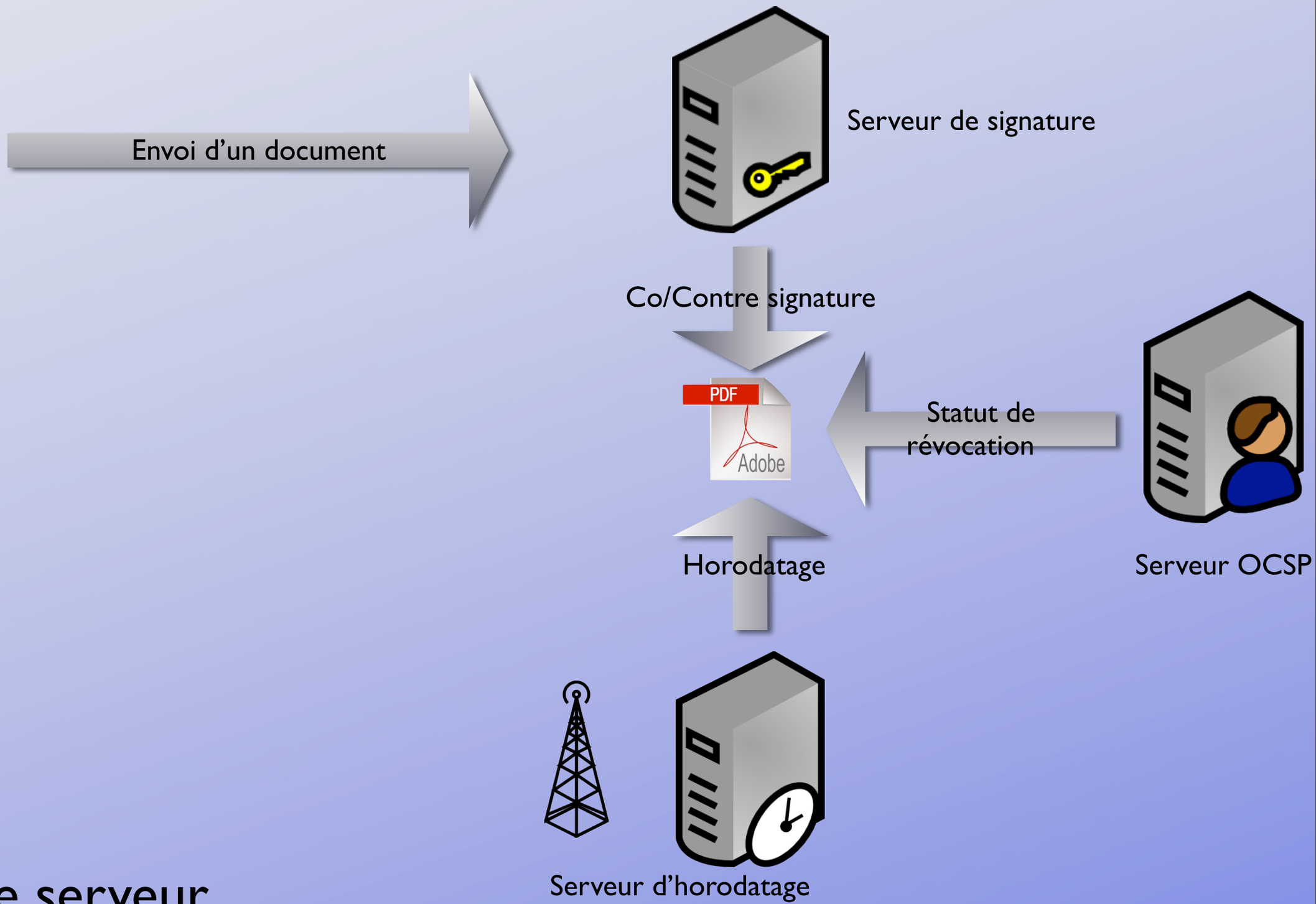
Signature serveur

Signature d'un document



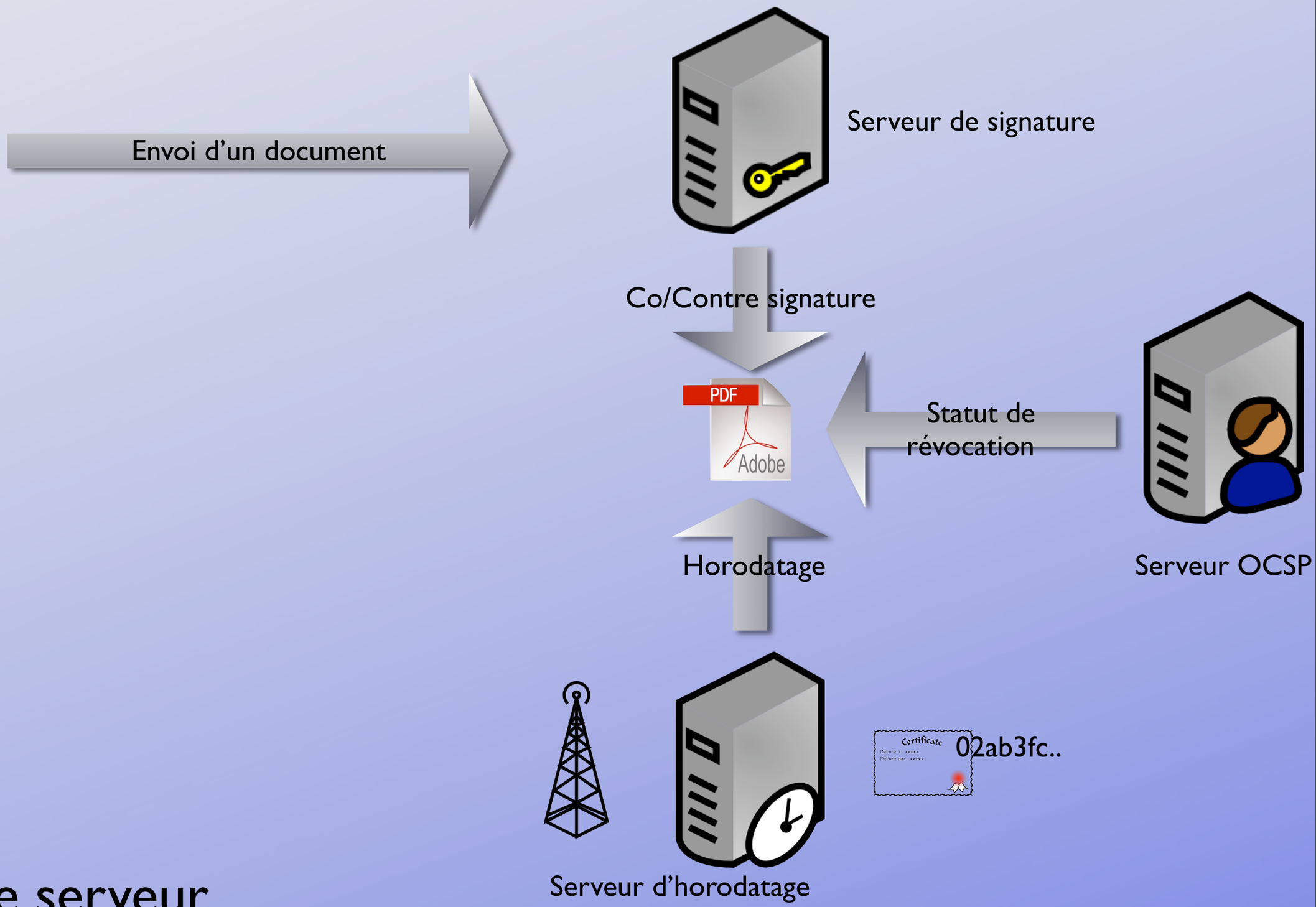
Signature serveur

Signature d'un document



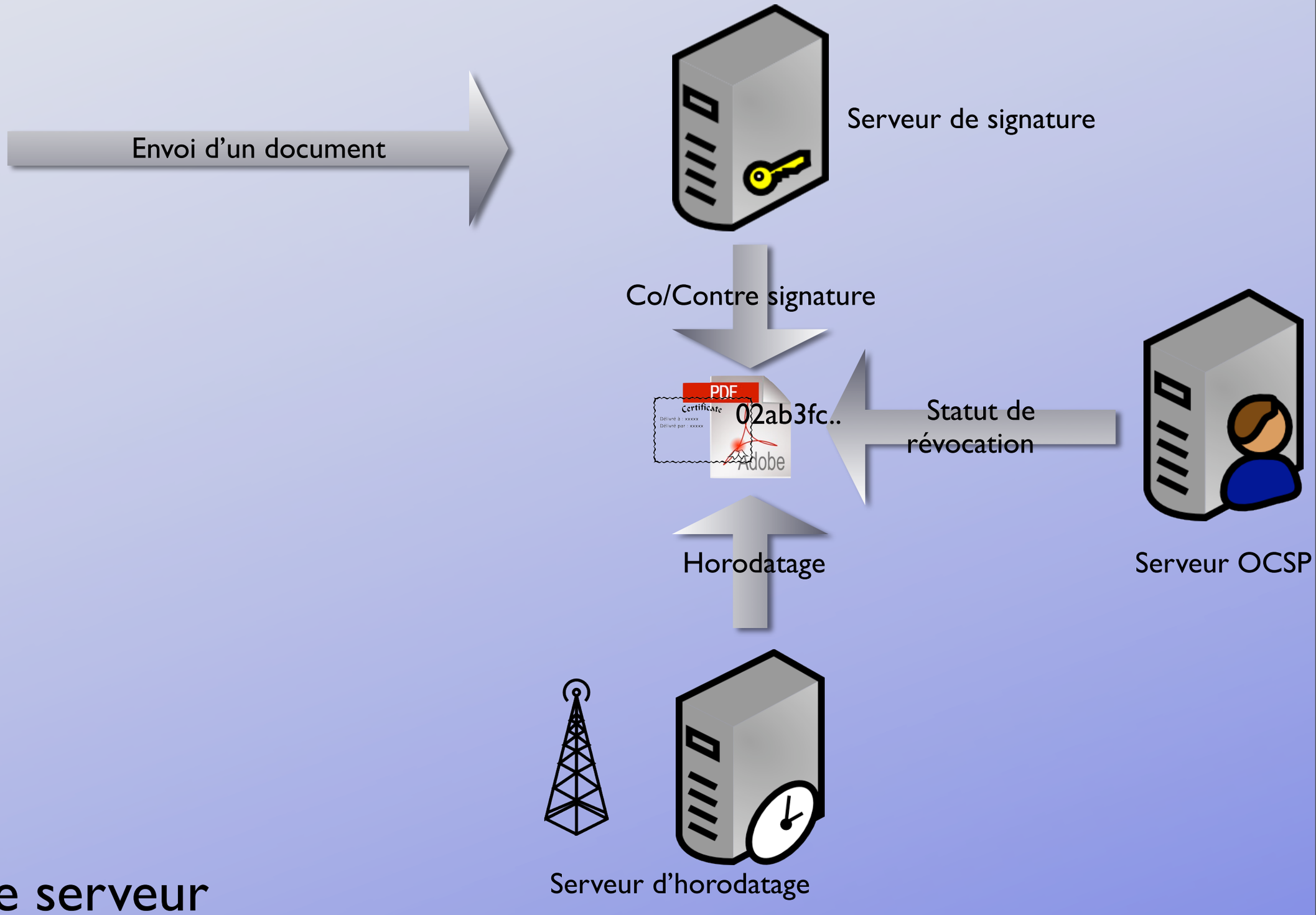
Signature serveur

Signature d'un document



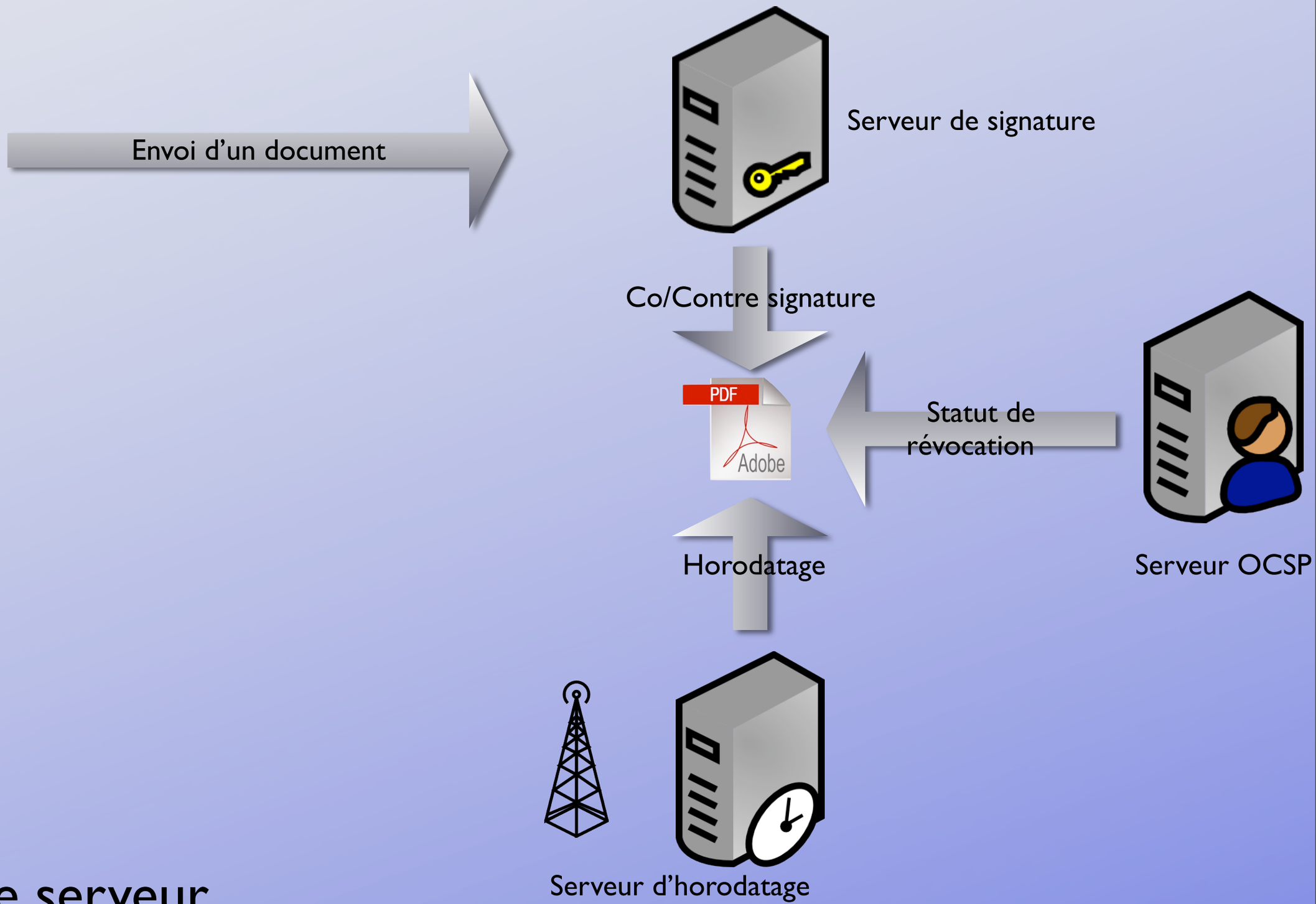
Signature serveur

Signature d’un document



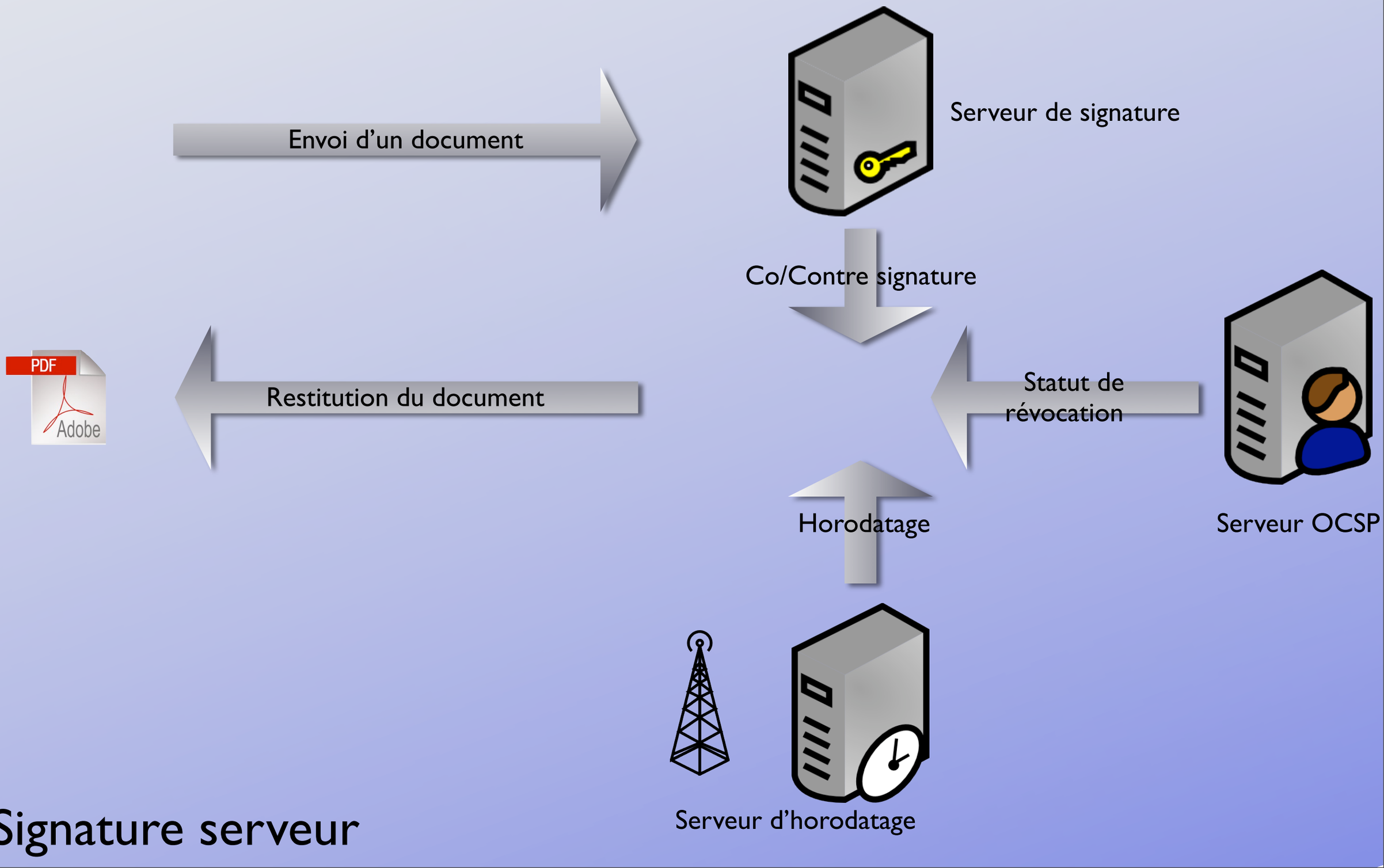
Signature serveur

Signature d'un document



Signature serveur

Signature d'un document



Signature serveur

Vérification d’une signature

Vérification d'une signature

Création d'un condensé
et extraction de la signature

Vérification d'une signature

Création d'un condensé
et extraction de la signature

d035675...

beafa4ef...

Vérification d'une signature

Création d'un condensé
et extraction de la signature

d035675...

Déchiffrement de la signature

d035675...

Vérification d'une signature

Création d'un condensé
et extraction de la signature

d035675...

Déchiffrement de la signature

d035675...

Comparaison des condensés

Vérification d'une signature

Création d'un condensé
et extraction de la signature

Déchiffrement de la signature

Comparaison des condensés

d035675...

d035675...

Vérification d'une signature

Création d'un condensé
et extraction de la signature

Déchiffrement de la signature

Comparaison des condensés

d035675... = d035675...

Signature vérifiée

Co/Contre Signature

Co/Contre Signature

Co/Contre Signature

Données

Co/Contre Signature

- Co-signature : signatures de même niveau

Co/Contre Signature

- Co-signature : signatures de même niveau

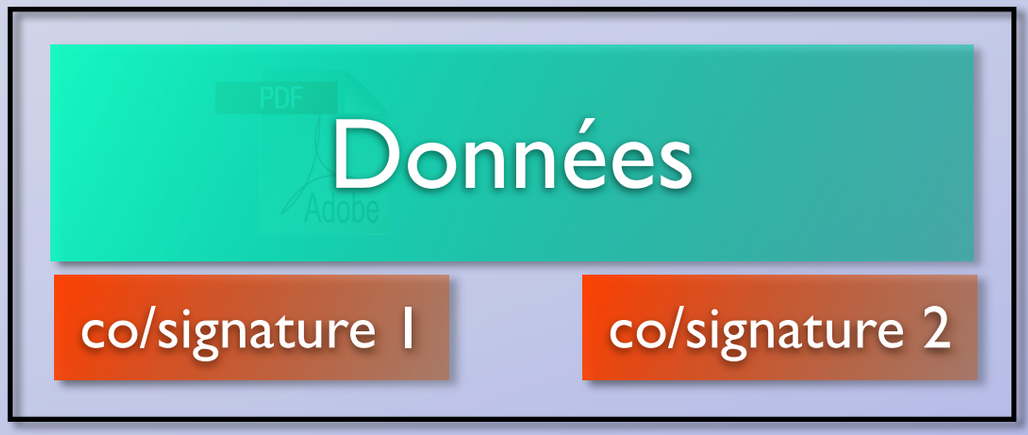
Co/Contre Signature

- Co-signature : signatures de même niveau

Co/Contre Signature

- Co-signature : signatures de même niveau
- Contre-signature : signature englobant d'autres signatures

Co/Contre Signature



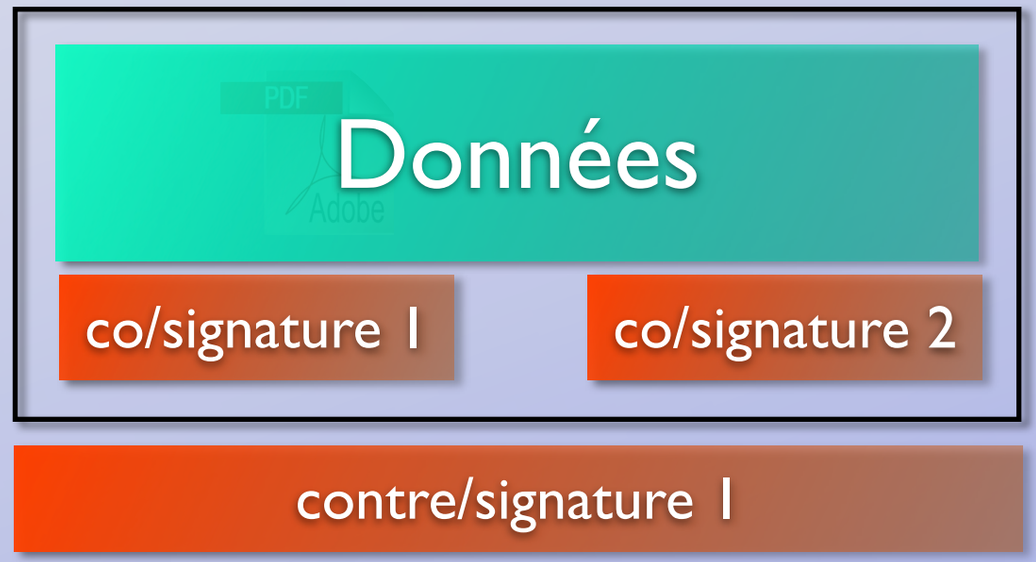
- Co-signature : signatures de même niveau

- Contre-signature : signature englobant d'autres signatures

Co/Contre Signature

- Co-signature : signatures de même niveau

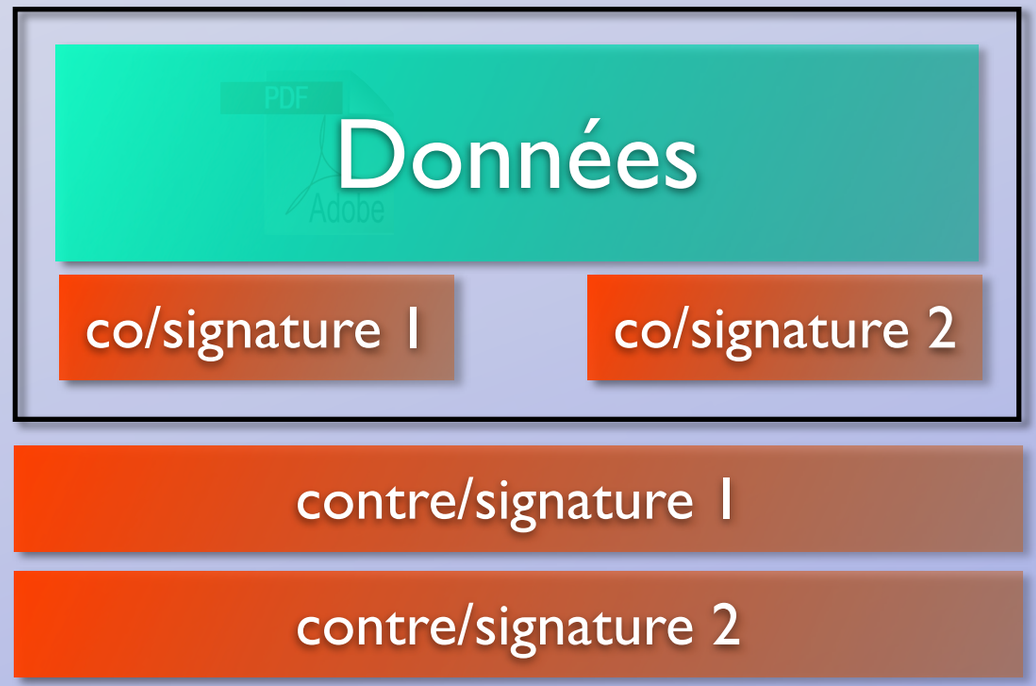
- Contre-signature : signature englobant d'autres signatures



Co/Contre Signature

- Co-signature : signatures de même niveau

- Contre-signature : signature englobant d'autres signatures



Les formats

Les formats

- Certains formats de document permettent l'intégration d'une signature (PDF, ODF), et d'afficher des informations (PDF)

Les formats

- Certains formats de document permettent l'intégration d'une signature (PDF, ODF), et d'afficher des informations (PDF)
- Pour les autres types de données, il est nécessaire d'utiliser un autre fichier contenant les informations de la signature, par exemple XAdES

La signature numérique

En savoir plus :
XAdES, les formes de signature

XAdES

XAdES

- Schéma XML, défini par le W3C

XAdES

- Schéma XML, défini par le W3C
- Sur-couche à xmldsig (XML Digital Signature)

XAdES

- Schéma XML, défini par le W3C
- Sur-couche à xmldsig (XML Digital Signature)
- En version 1.3.2, différents .. :

XAdES

- Schéma XML, défini par le W3C
- Sur-couche à xmldsig (XML Digital Signature)
- En version 1.3.2, différents .. :
  - XAdES-T (horodatage)

XAdES

- Schéma XML, défini par le W3C
- Sur-couche à xmldsig (XML Digital Signature)
- En version 1.3.2, différents .. :
  - XAdES-T (horodatage)
  - XAdES-C (Statut de non révocation)

La signature enveloppée

Fichier XML à signer, par exemple un FDF, résultat d'un formulaire PDF

La signature enveloppée

Fichier XML à signer, par exemple un FDF, résultat d'un formulaire PDF

```
<staff>
    <people>
        <member>asyd</member>
        <member>fanf</member>
    </people>
</staff>
```

La signature enveloppée

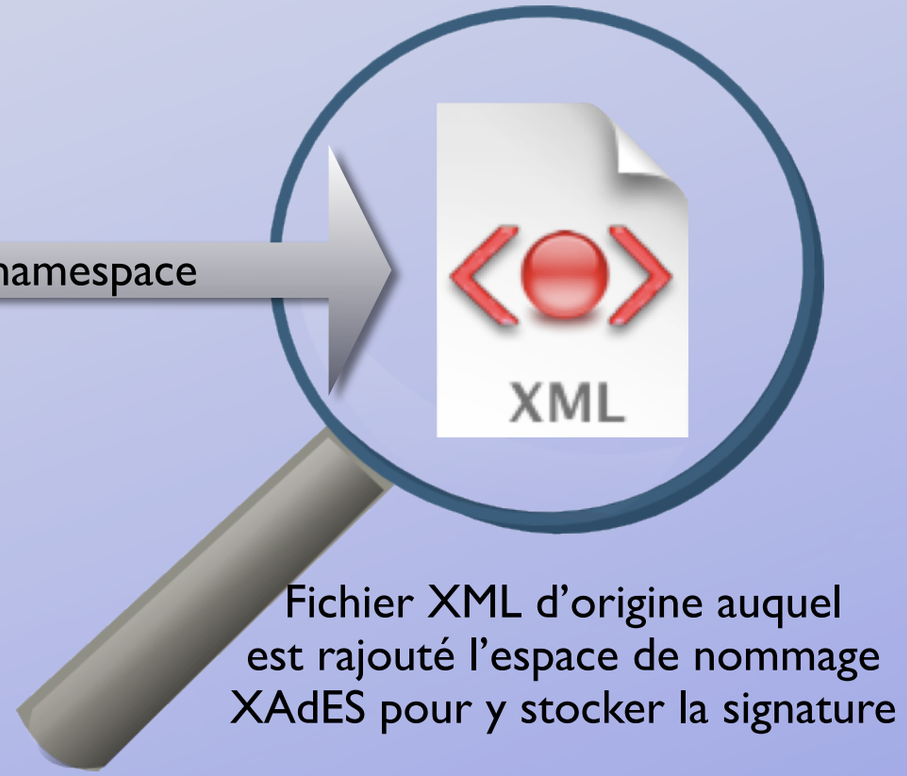
Création de la signature et ajout du namespace

Fichier XML à signer, par exemple un FDF, résultat d'un formulaire PDF

Fichier XML d'origine auquel est rajouté l'espace de nommage XAdES pour y stocker la signature

La signature enveloppée

Création de la signature et ajout du namespace



Fichier XML à signer, par exemple un FDF, résultat d'un formulaire PDF

Fichier XML d'origine auquel est rajouté l'espace de nommage XAdES pour y stocker la signature

La signature enveloppée

Création de la signature et ajout du namespace

Fichier XML à signer, par exemple un FDF, résultat d'un formulaire PDF

Fichier XML d'origine auquel est rajouté l'espace de nommage XAdES pour y stocker la signature

```
<staff>
    <people>
        <member>asyd</member>
        <member>fanf</member>
    </people>
    <digitalSignature>
        <signature>ZGdzZGFmZ2FzMnIya2Nkc2EK..</signature>
    </digitalSignature>
</staff>
```

La signature enveloppante

Données à signer

La signature enveloppante

Création du fichier XAdES et signature du document

Données à signer

La signature enveloppante

Création du fichier XAdES et signature du document

Données à signer

La signature enveloppante

Création du fichier XAdES et signature du document

Données à signer

Fichier XAdES contenant les donnés d'origine encodées en base64, et les informations de la signature

Contexte

- La signature numérique possède la même valeur légale que la signature manuscrite
  - Art. 1316-1. « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, **sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.** (loi 2000 du 13 Mars 2000) »
  - Décret d'application du 30 Mars 2001

Les aspects légaux

Les aspects légaux

- En Europe, seul le format XAdES à une valeur probante (ETSI)

Les aspects légaux

- En Europe, seul le format XAdES à une valeur probante (ETSI)
  - La signature PDF n'est PAS reconnue

Les aspects légaux

- En Europe, seul le format XAdES à une valeur probante (ETSI)
  - La signature PDF n'est PAS reconnue
- Pour une utilisation « réelle » la gestion des certificats doit être conforme à la PRIS (Politique de référencement intersectorielle de sécurité)

Les aspects légaux

- En Europe, seul le format XAdES à une valeur probante (ETSI)
  - La signature PDF n'est PAS reconnue
- Pour une utilisation « réelle » la gestion des certificats doit être conforme à la PRIS (Politique de référencement intersectorielle de sécurité)
- Attention, pas encore de jurisprudence !

Quelques exemples d’utilisation

Quelques exemples d'utilisation

- Dématérialisation des marchés publics

Quelques exemples d'utilisation

- Dématérialisation des marchés publics
- En Belgique, les citoyens disposent d'une carte d'identité numérique, permettant - à terme - de signer des documents administratifs

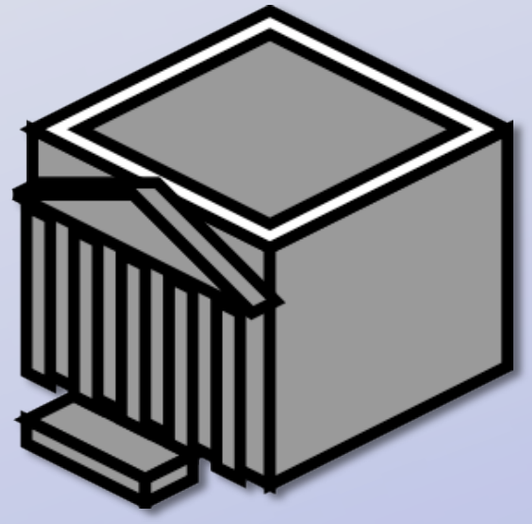
Merci de votre attention !

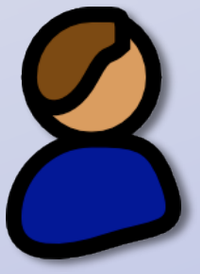
Retrouver cette présentation sur http://asyd.net/talks/

Le chiffrement

- Les différences entre un certificat de signature et un certificat de chiffrement

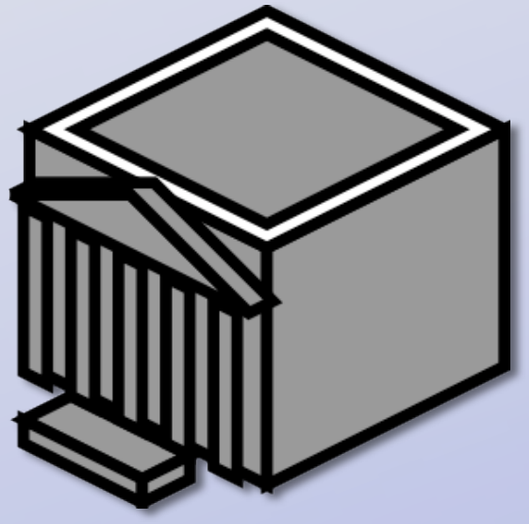
Obtention d'un certificat



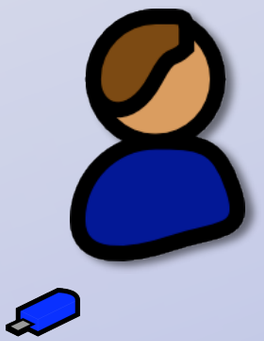


Token matériel

Obtention d'un certificat

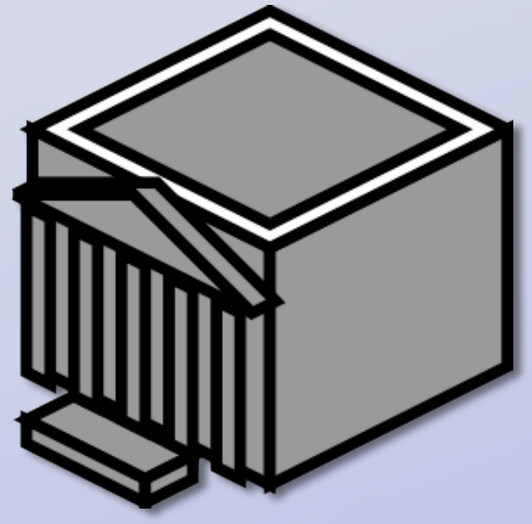


1. Formulaire

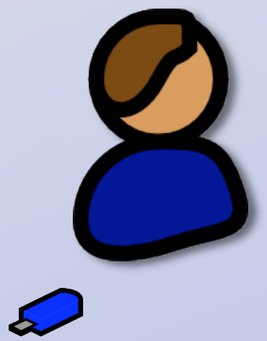


Nom	Bonfils
Prénom	Bruno
Type de certificat	Signature

Obtention d'un certificat

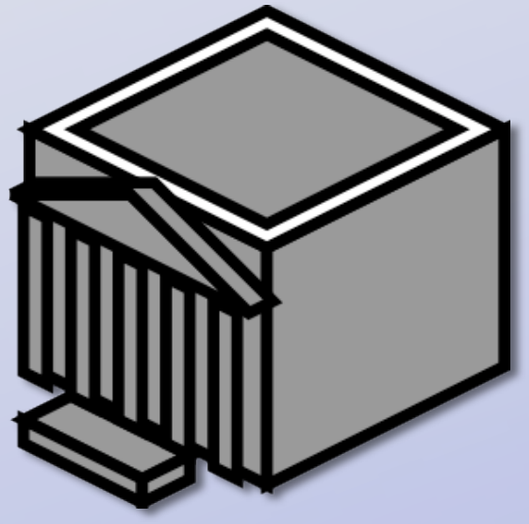


1. Formulaire
2. Consolidation des données

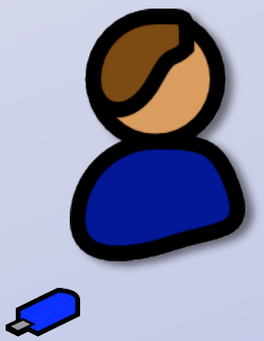


Nom	Bonfils
Prénom	Bruno
Type de certificat	Signature

Obtention d'un certificat

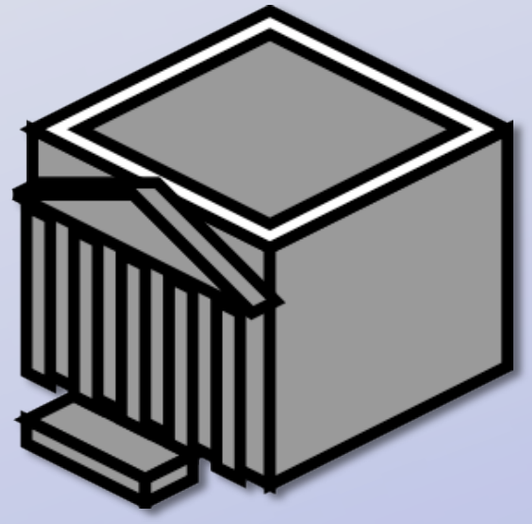


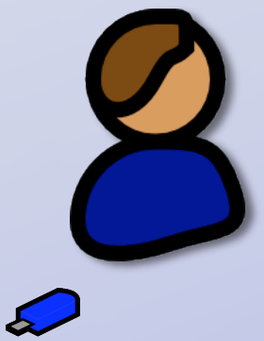
1. Formulaire
2. Consolidation des données



CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

Obtention d'un certificat

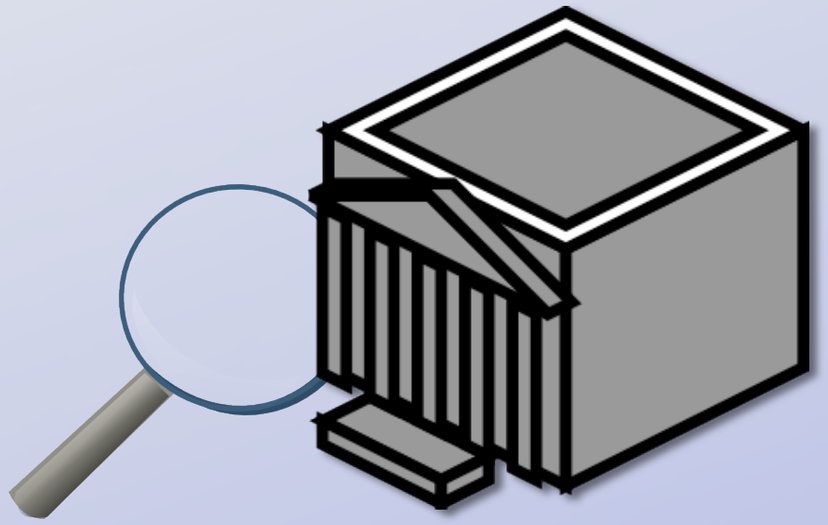


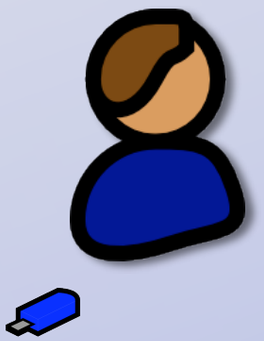


CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance

Obtention d'un certificat

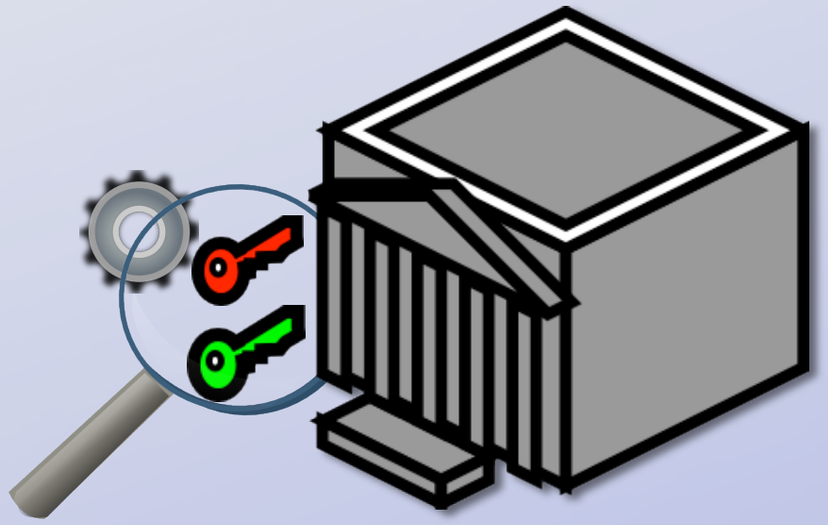


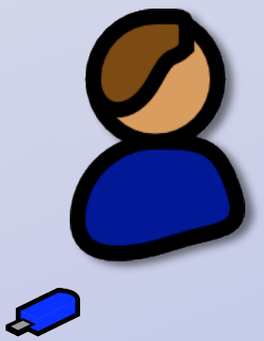


CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance

Obtention d'un certificat

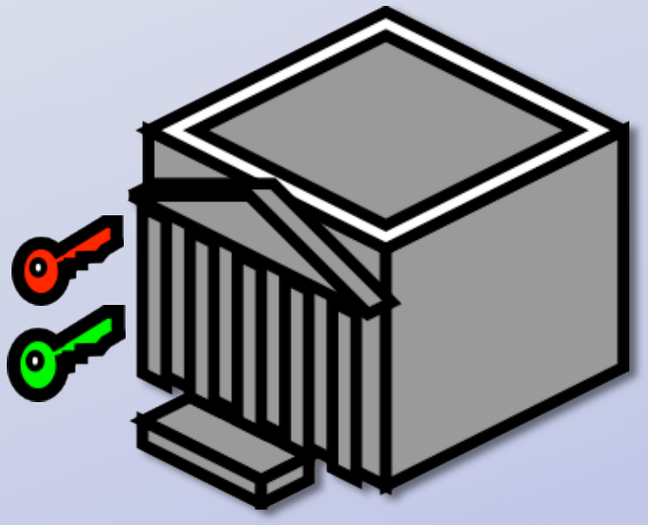


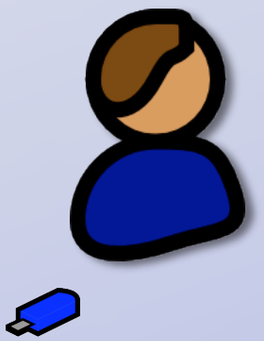


CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance

Obtention d'un certificat

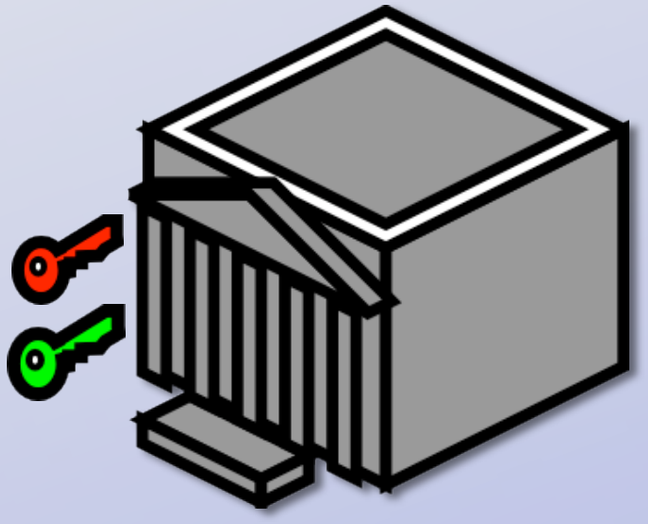


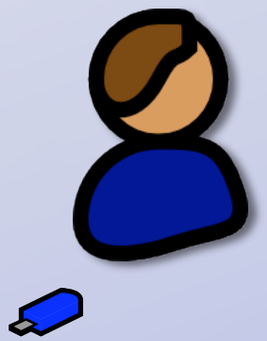


CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance
4. Archivage

Obtention d'un certificat



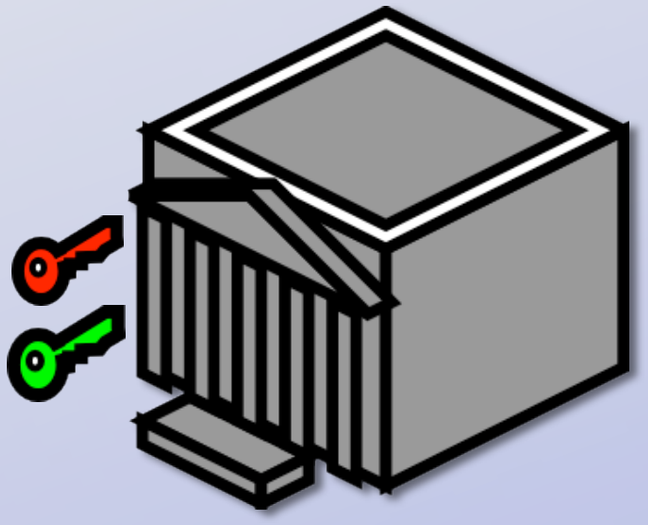


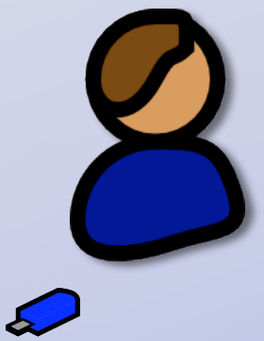
CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance
4. Archivage

La clé privée est archivée pour que l'utilisateur soit en mesure de restaurer ses données en cas de perte du token.

Obtention d'un certificat

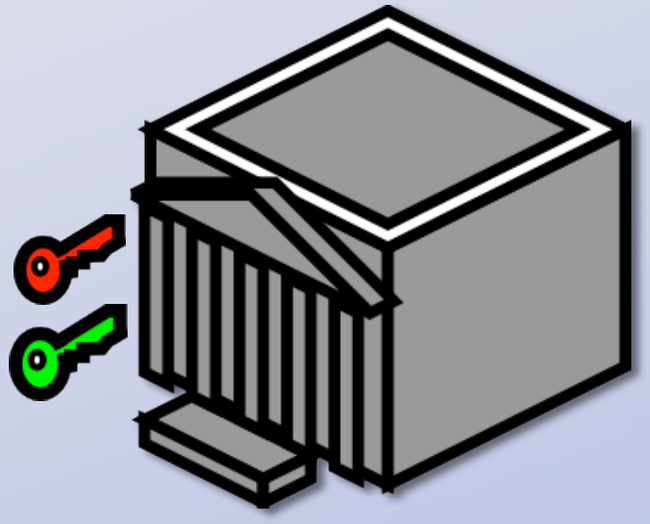


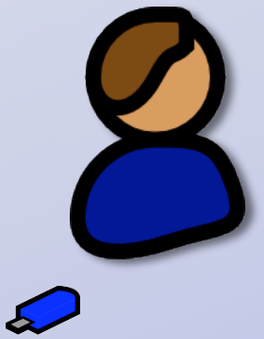


CN	Bruno Bonfils
OU	Staff
O	asyd dot net
C	FR
Profil de certificat	ENDUSER_SIGNATURE

1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance
4. Archivage

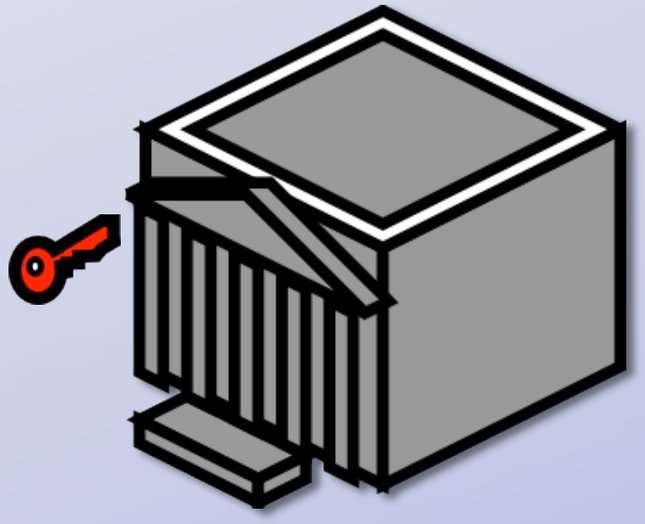
Obtention d'un certificat

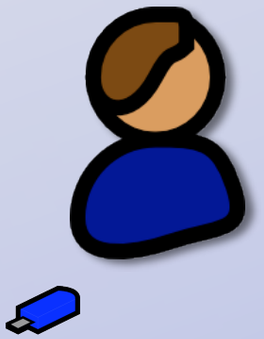




1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance
4. Archivage
5. Génération du certificat

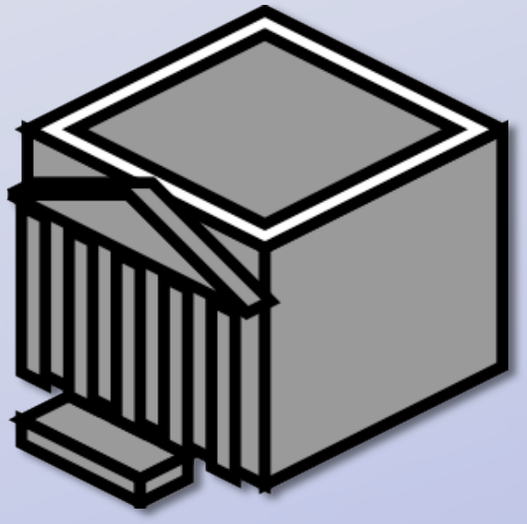
Obtention d'un certificat

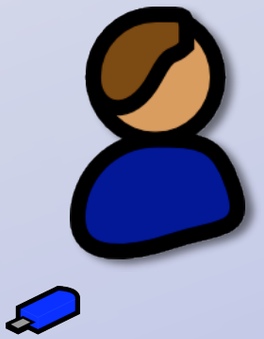




1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance
4. Archivage
5. Génération du certificat

Obtention d'un certificat





1. Formulaire
2. Consolidation des données
3. Génération d'une biclé par l'autorité de confiance
4. Archivage
5. Génération du certificat
6. Injection du certificat et de la clé privée dans le token de l'utilisateur