Signature digitale

11/01/2024

Frédéric Paquay
mi.dpo@mi-is.be

Sommaire

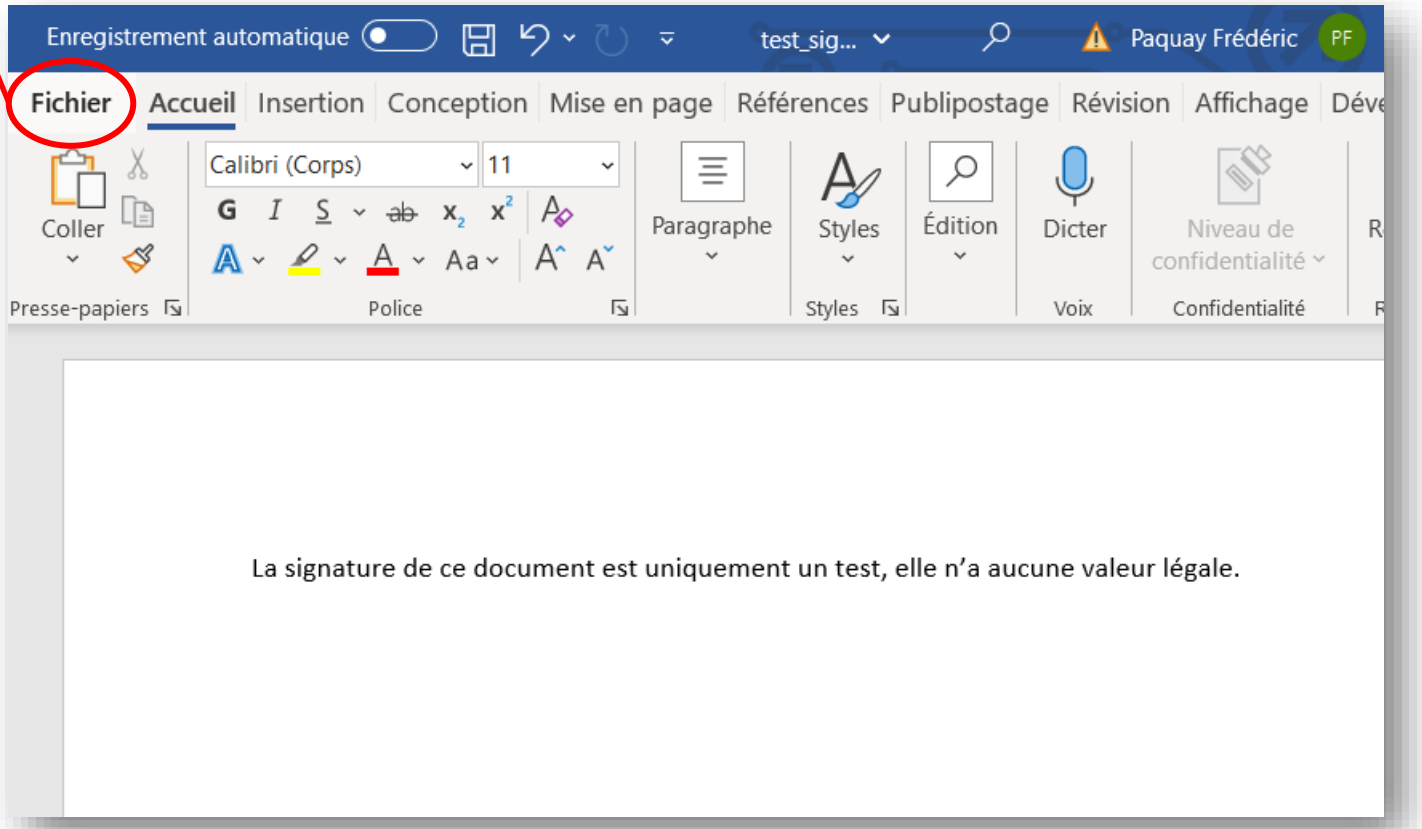
- Signature de PDF par Adobe Acrobat Reader
- Signature : principes
- Signature digitale : principes
- Qualités : normes européennes
- Limites d’une signature digitale
- Conclusion
- Annexe : configurer un horodatage dans Adobe Acrobat Reader

Signature de document PDF

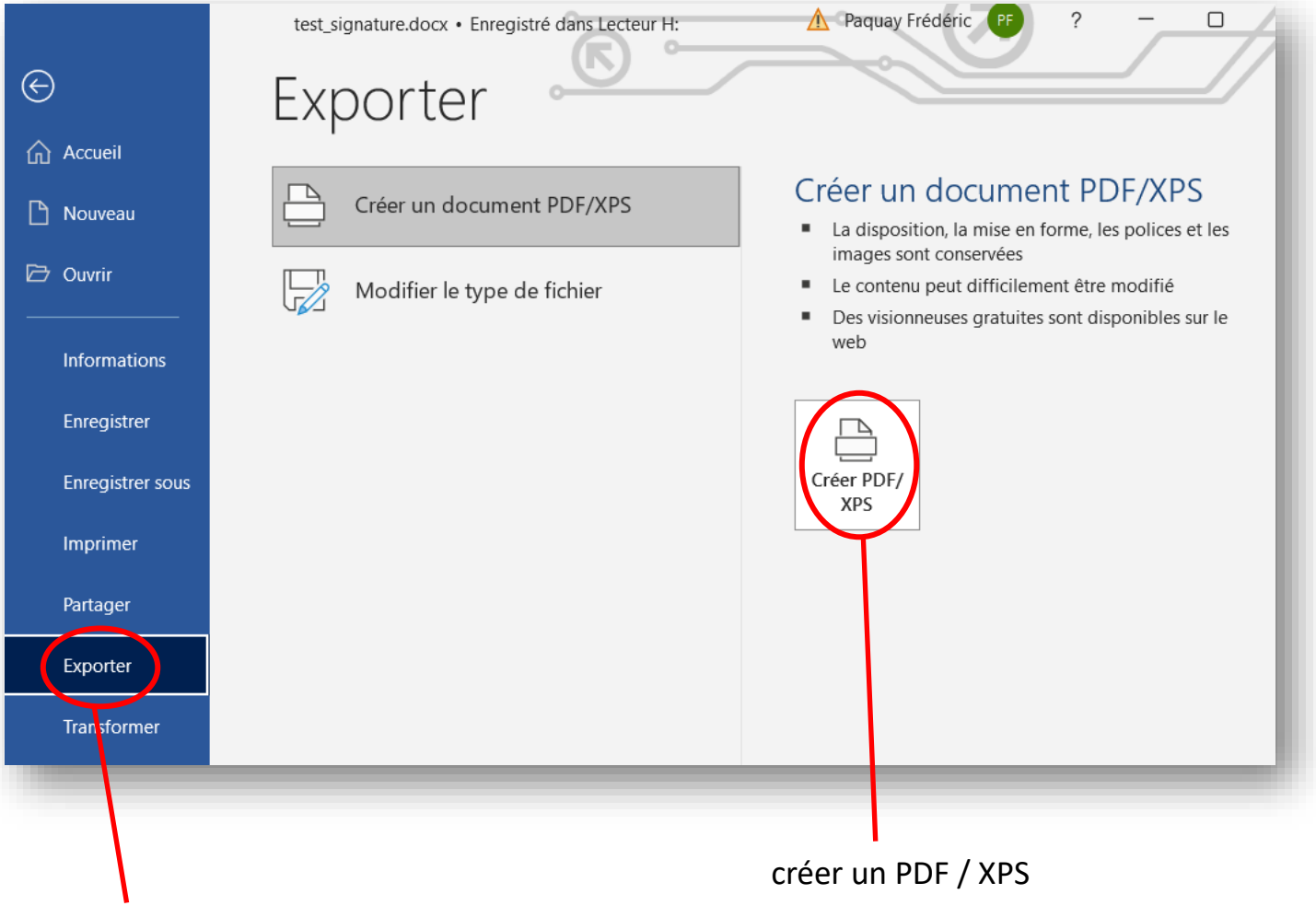
Signature de document PDF (1/10)

Préparer un document, à partir de Word par exemple, puis l'exporter en PDF.

le document fini, cliquer sur l'onglet « Fichier »



Signature de document PDF (2/10)

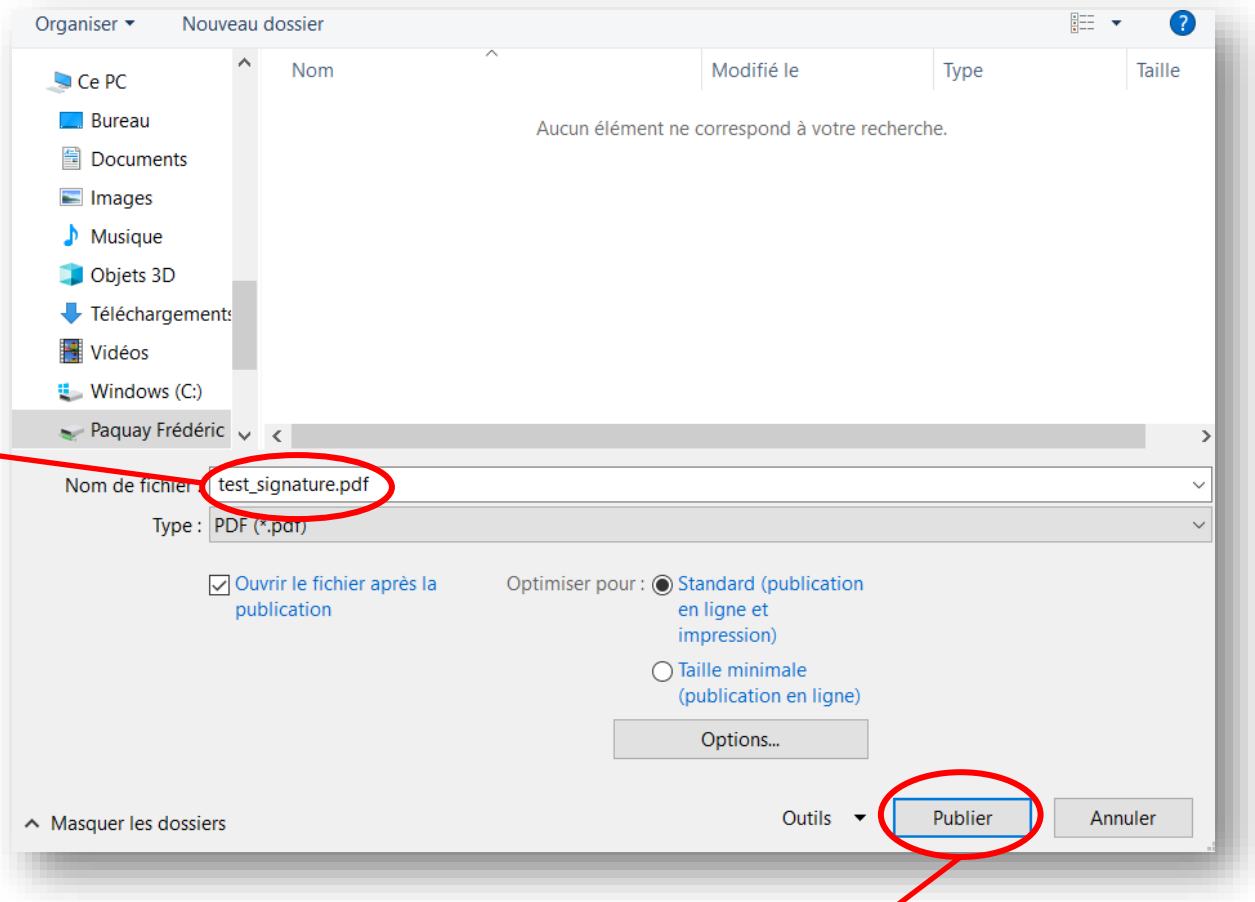


cliquer sur l'onglet « Exporter »

créer un PDF / XPS

Signature de document PDF (3/10)

choisir un nom de fichier



cliquer sur « Publier » pour l'enregistrer

Signature de document PDF (4/10)

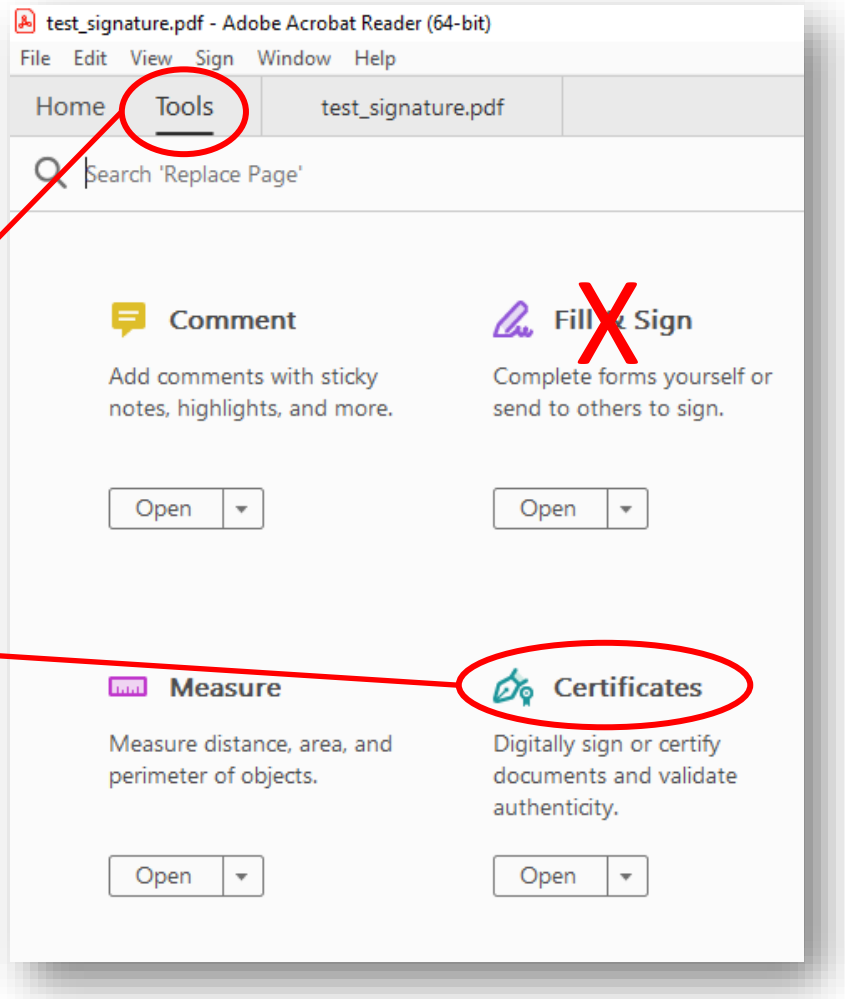
Adobe

Ouvrir le document avec Adobe Acrobat Reader.

Adobe

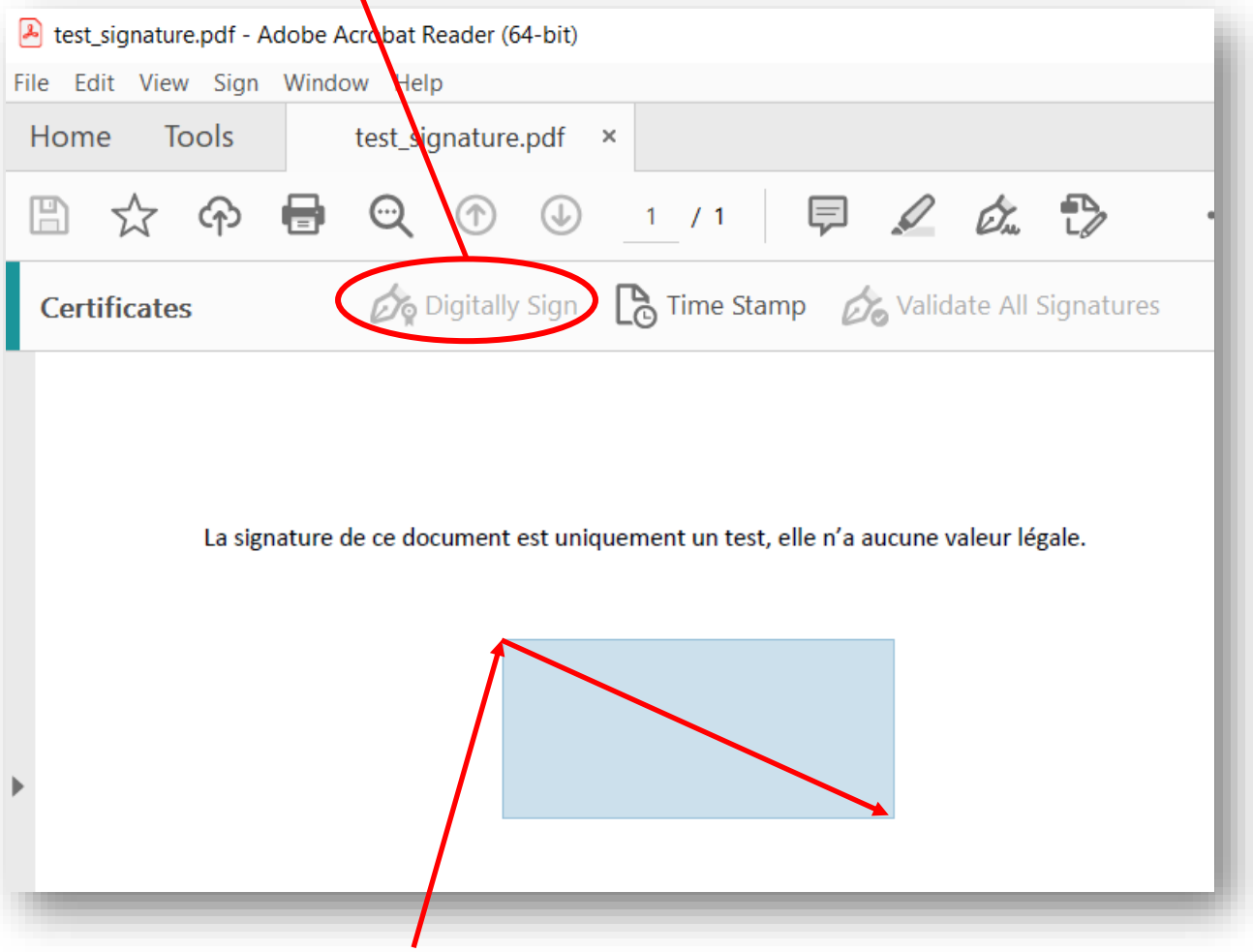
cliquer sur l'onglet « Tools » ou « Outils »

cliquer sur « Certificates », <u>pas</u> sur « Fill & Sign »



Signature de document PDF (5/10)

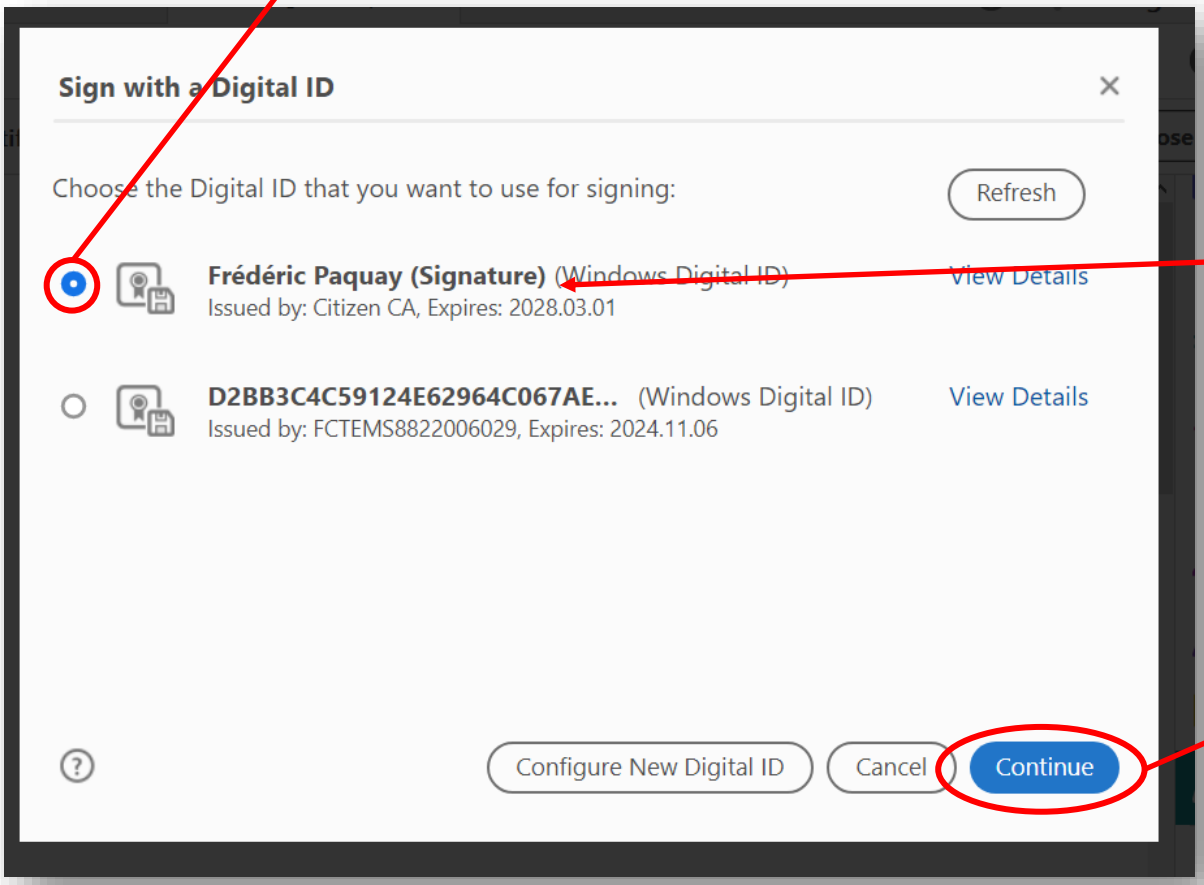
cliquer sur « Digitally Sign »



avec la souris (clic gauche), sélectionner une zone pour la signature

Signature de document PDF (6/10)

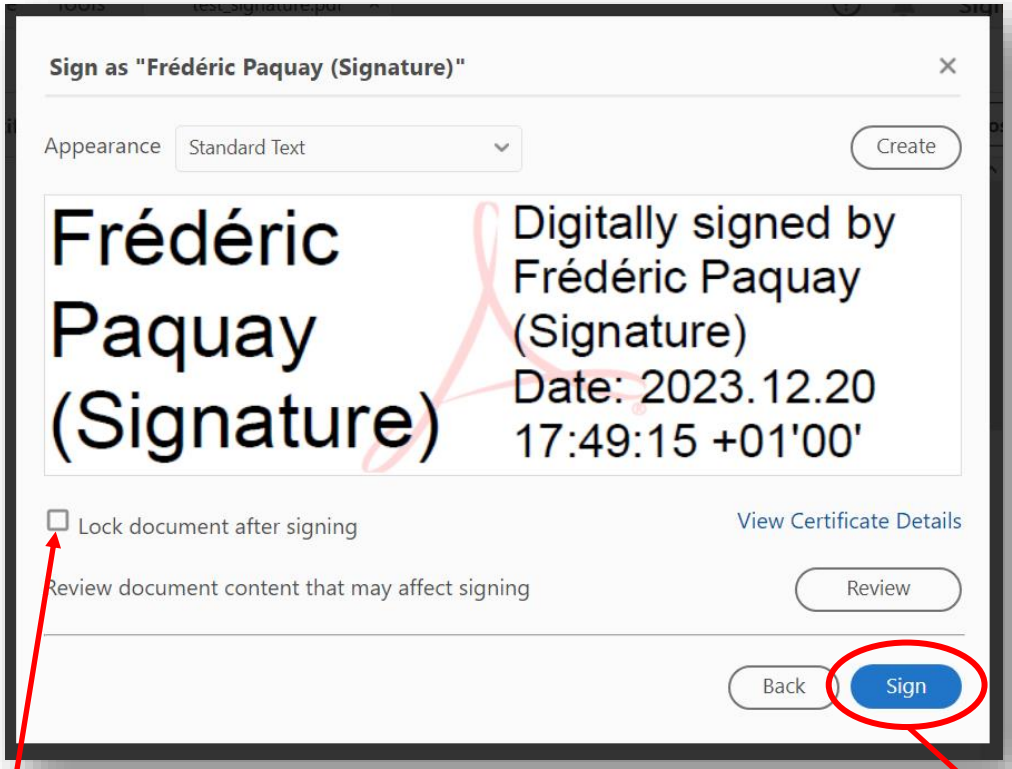
choisir la signature eID : ***prénom nom*** **(Signature)**



choisir **(Signature)** et pas **(Authentification)**

continuer à l'étape suivante

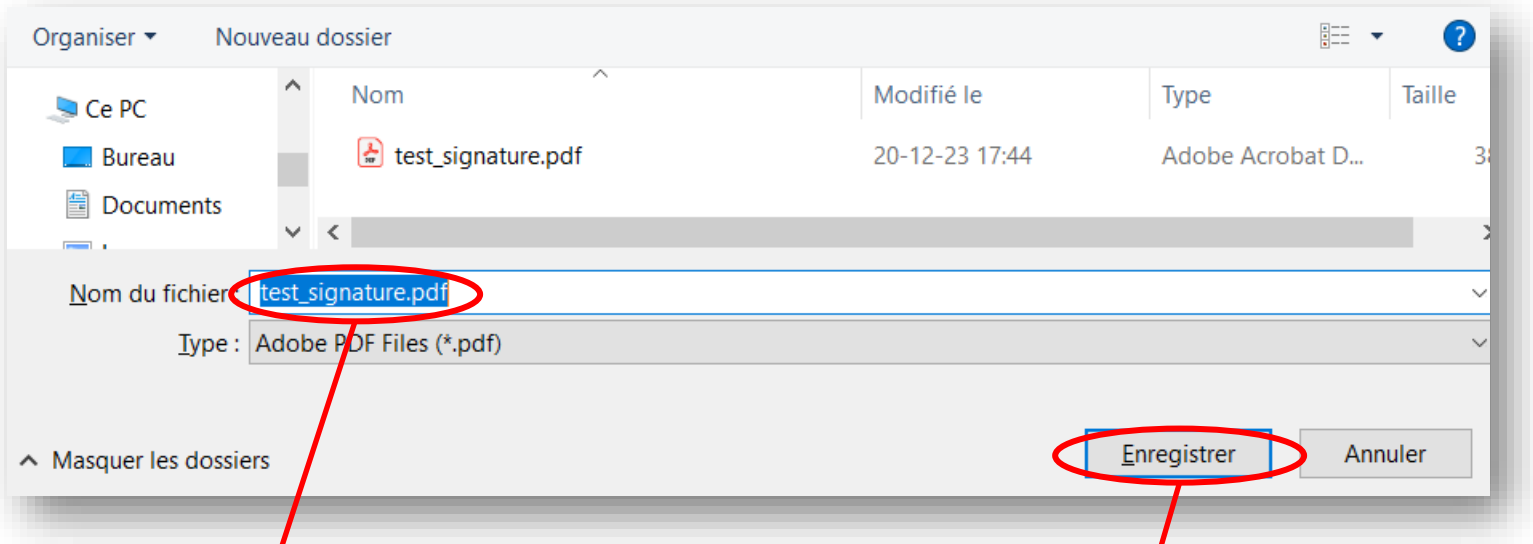
Signature de document PDF (7/10)



ne **pas cocher** cette case sinon d'autres personnes ne pourront plus signer le document.

confirmer

Signature de document PDF (8/10)



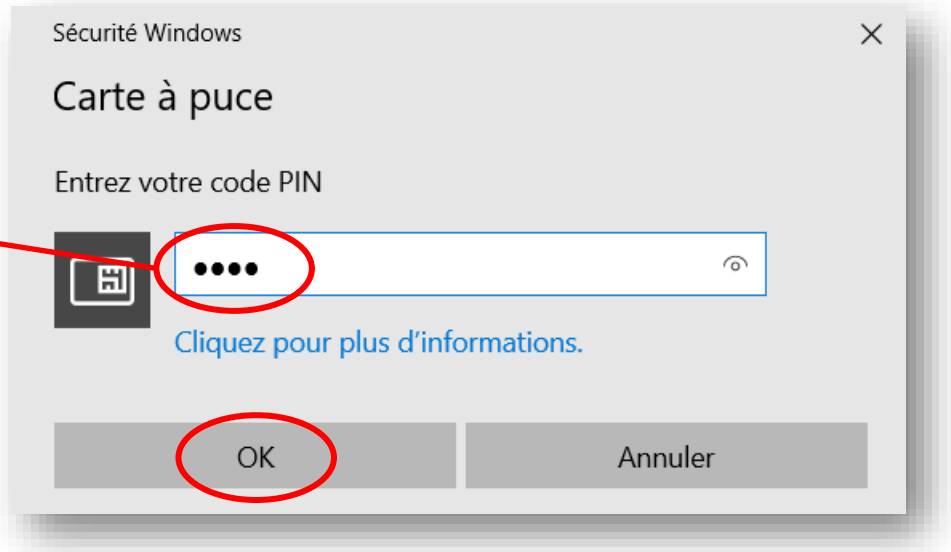
choisir un fichier de destination,
qui peut être identique à l'original.

enregistrer

Signature de document PDF (9/10)

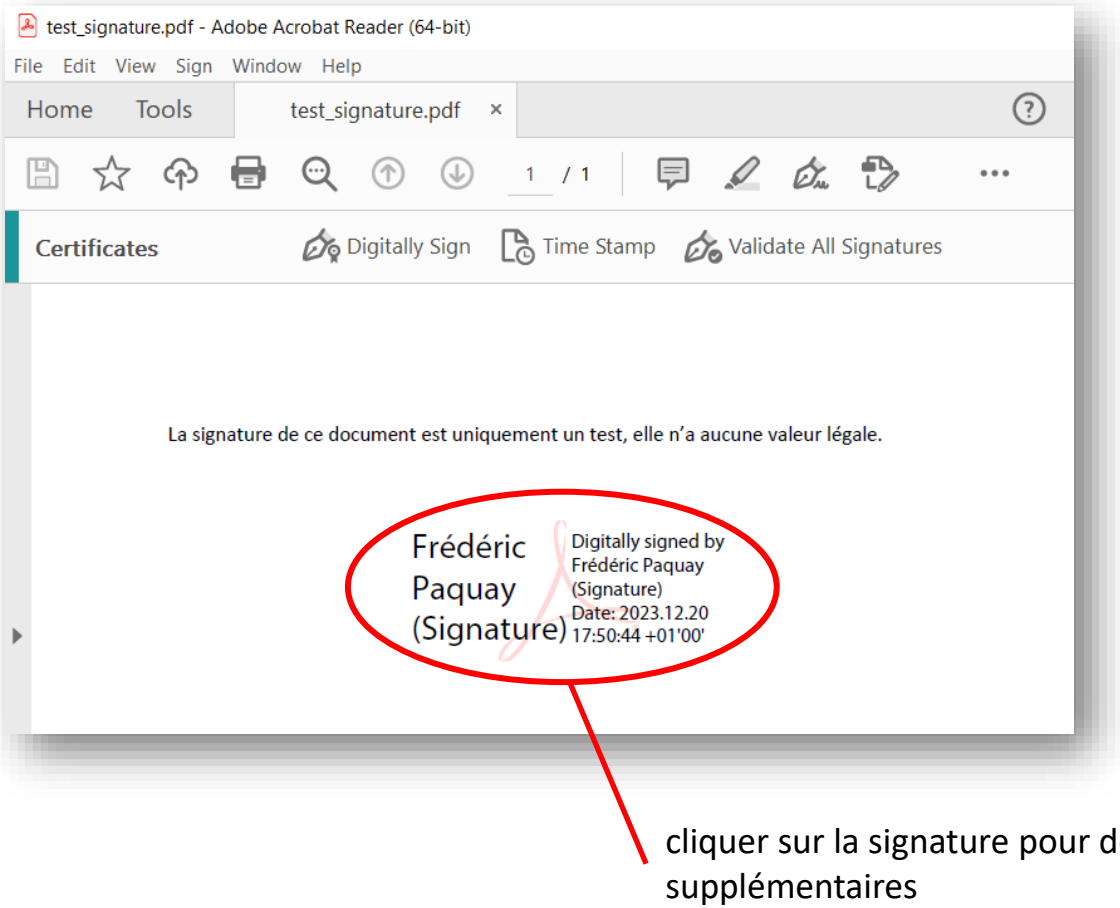
La carte d'identité doit être **insérée dans le lecteur** avant cette étape, sinon une erreur sera signalée.

insérer le code PIN
de la carte d'identité



Signature de document PDF (10/10)

Le document est signé !



Questions

Est-il possible de signer avec autre chose que l'eID ?

OUI en théorie **MAIS** en pratique, peu d'alternatives immédiates, à part **It's me** avec facturation à la signature (https://www.itsme-id.com/en-BE/business/services/sign).

Peut-on signer autre chose qu'un PDF ?

OUI car n'importe quel fichier ou document peut être signé **MAIS** les PDF sont de loin les plus utilisés. Il est aussi facilement possible de signer un document **Word** ou **Excel** avec Microsoft Office.

Peut-on utiliser autre chose qu'Adobe Acrobat Reader ?

OUI MAIS il n'existe pas beaucoup d'alternatives sur le marché (ex : Foxit payant) car la signature digitale est moins utilisée dans la plupart des autres pays européens, qui n'ont souvent pas d'outil de signature généralisé comme l'eID.

Questions

Comment signer un ensemble de documents ?

Chaque document devrait être signé individuellement. Le geste qui applique une signature, digitale (ex : introduction d'un code PIN) ou non, ne devrait pas être automatisé ou répété de manière automatique.

It's me propose néanmoins la possibilité de signer plusieurs documents en une fois.

https://www.itsme-id.com/content-assets/53388/1670876179-communique-de-presse-itsme-13-12-2022.pdf

Obligation : chaque document doit toujours être présenté avant la signature.

réglementation eIDAS, Annexe II

2. Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

Signature

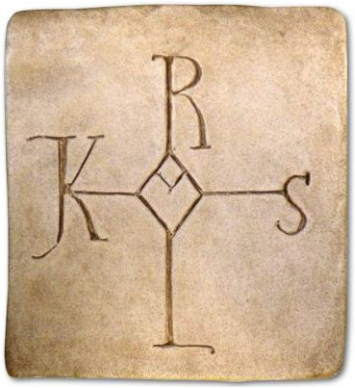
Signature

Définition :

Toute **marque** distinctive et personnelle **manuscrite**, permettant d'individualiser, sans doute possible, son **auteur** et traduisant la **volonté** non équivoque de consentir à un **acte**.

https://www.larousse.fr/dictionnaires/francais/signature/72699

Conditions nécessaires pour une signature valide :

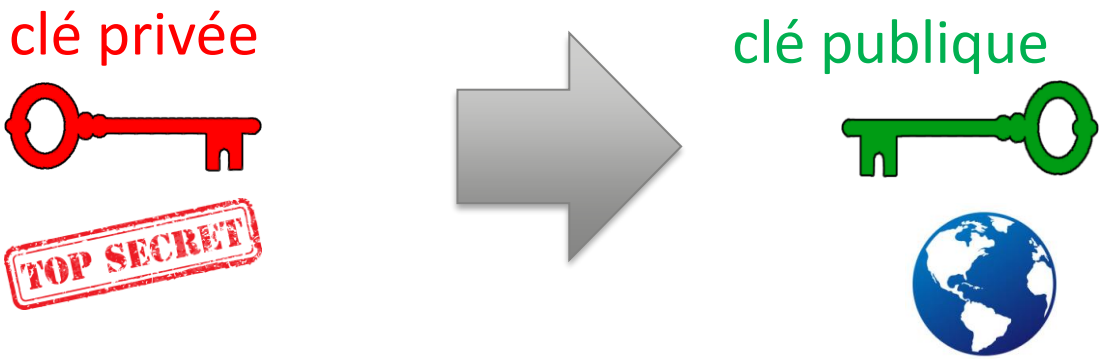


- la **marque distinctive** ne peut pas être utilisée par une autre personne,
- l'auteur doit être **authentifié** (identification prouvée),
- la description de l'acte et la signature sont consignées dans un **document** écrit **non modifiable** pour préserver la volonté non équivoque.

La signature garantit la **non-répudiation** de la volonté de l'auteur : pas de contestation ou de rétractation possible.

Signature digitale

Signature digitale : marques distinctives



Clé privée :

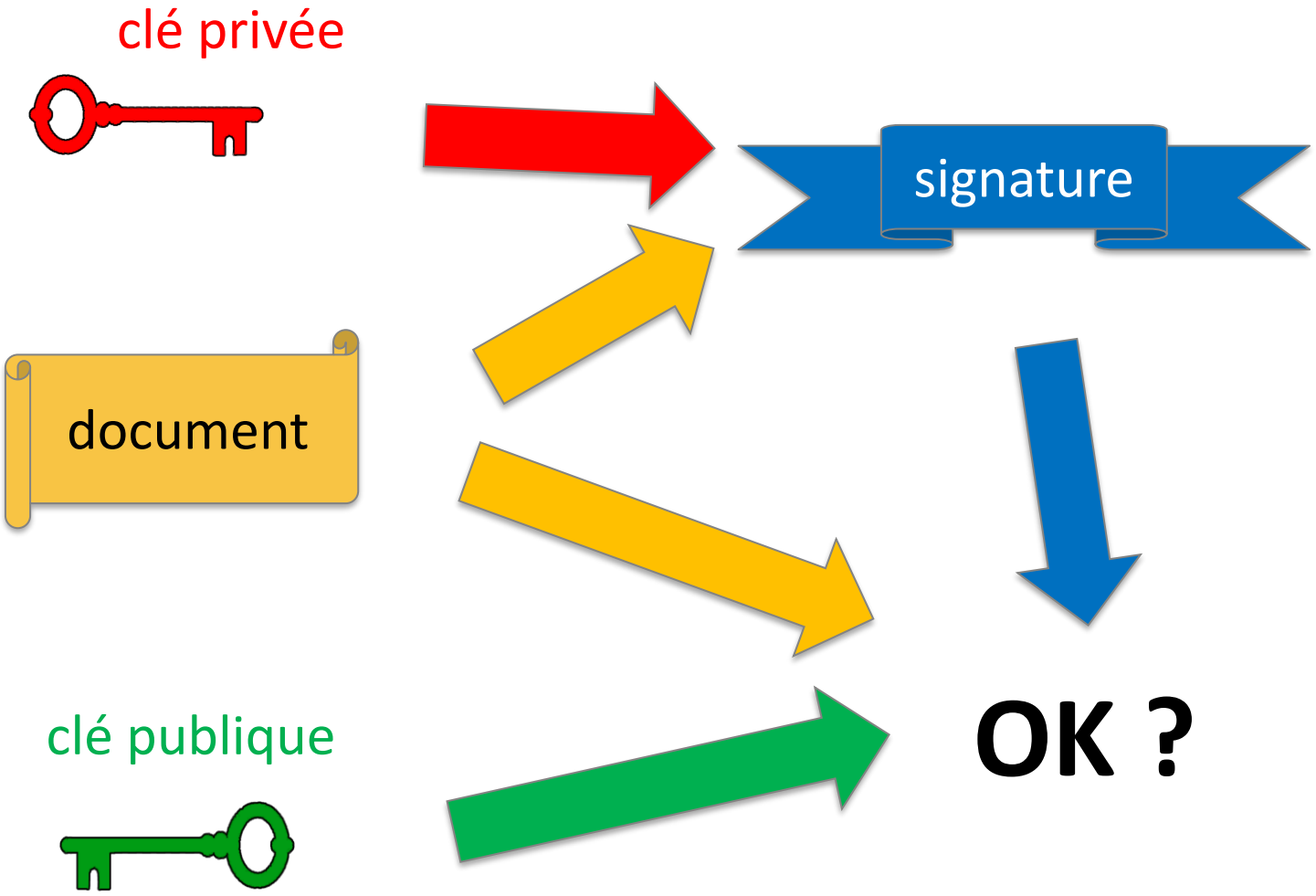
Données **secrètes** pour signer.

Clé publique :

- **Unique** et calculée à partir de la clé privée.
- **Impossible** de calculer la clé privée.
- Utilisée pour **vérifier** la signature.
- Publique = doit être accessible à tout le monde.

Signature digitale : signer - vérifier

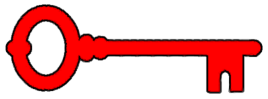
Algorithme de signature : **RSA** (1977) ou **ECDSA** (1992).



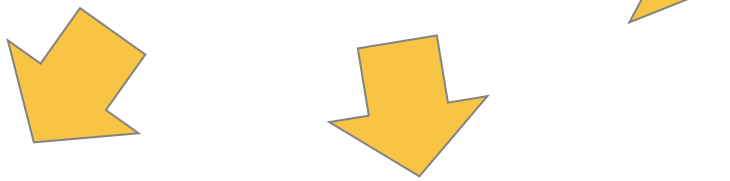
Signature digitale : marque distinctive

Protection de la clé privée

fichier
*.p12, *.jks
trop peu sécurisé



utilisation protégée par code PIN ou mot de passe



carte à puce

petit volume
de signatures

clé USB
cryptographique

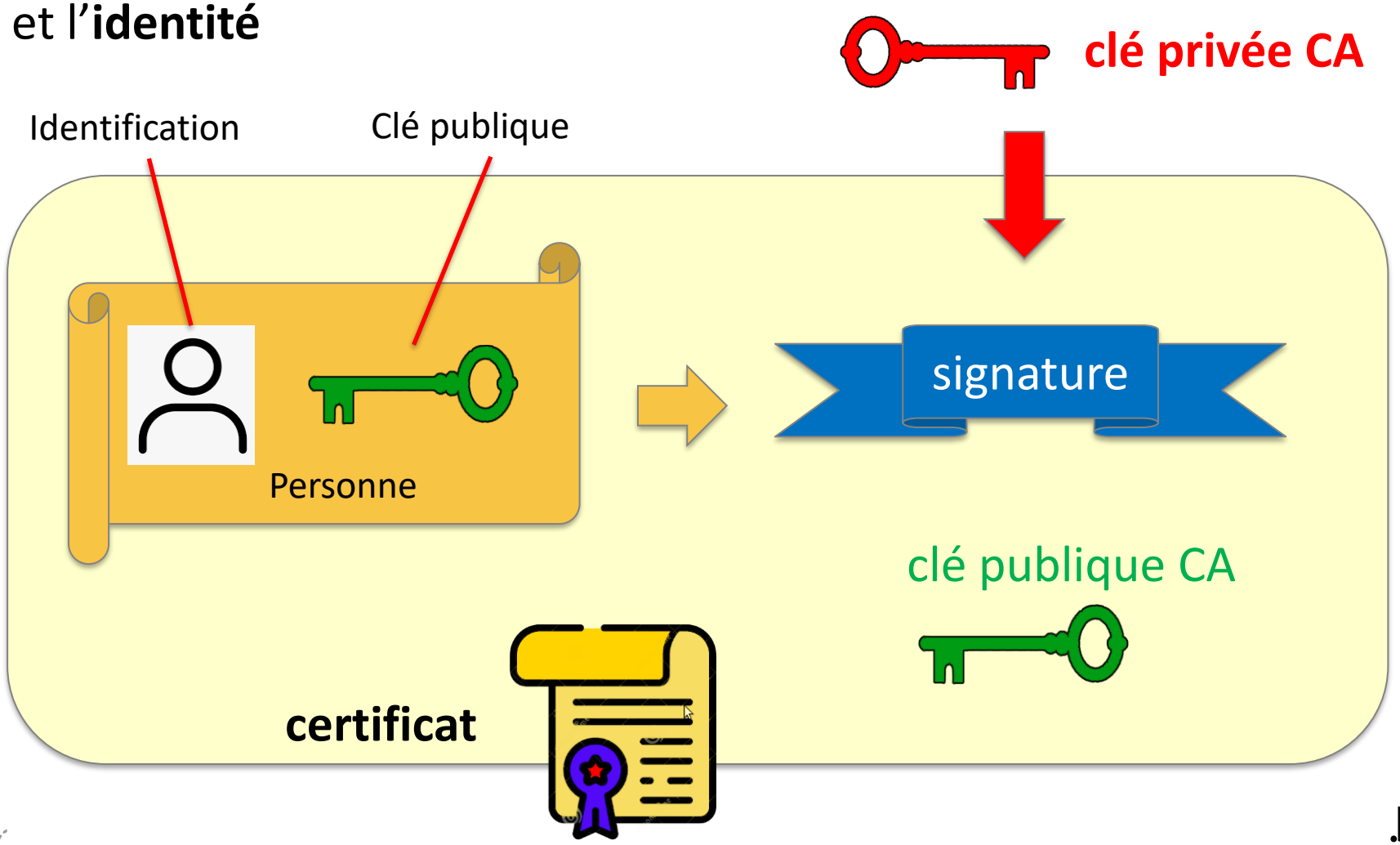
PME, petite
institution

HSM

gros volume
de signatures

Signature digitale : authentification

Certificat : lien entre la **clé publique** et l'**identité**



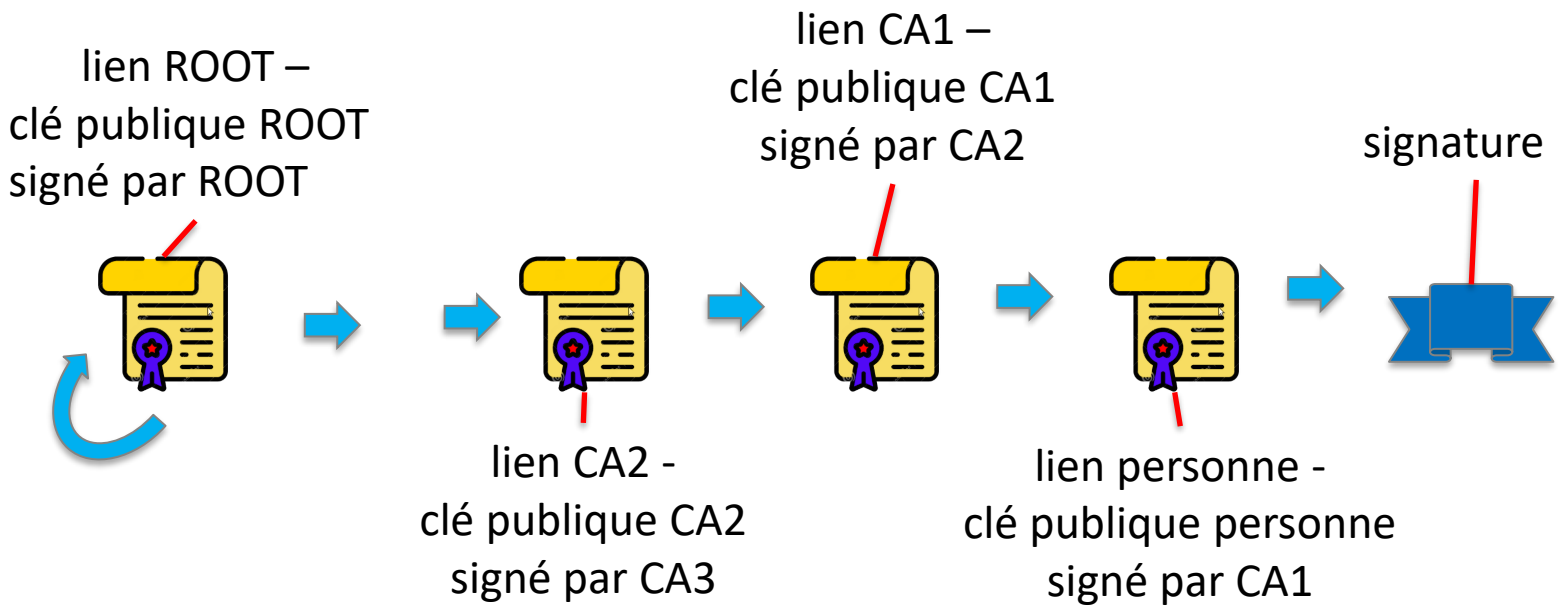
Signature digitale : authentification

Certificat : lien entre la **clé publique** et l'**identité**

- signature d'une **autorité de certification (CA)** de confiance pour valider ce lien
- toujours une **durée de validité**
- peut être **révoqué** (compromis, corrompu, invalide) avant échéance (ex. : données d'identité non conformes à la réalité, décès de la personne, vol ou perte de la clé privée / eID)

Signature digitale : authentification

Chaîne de certificats

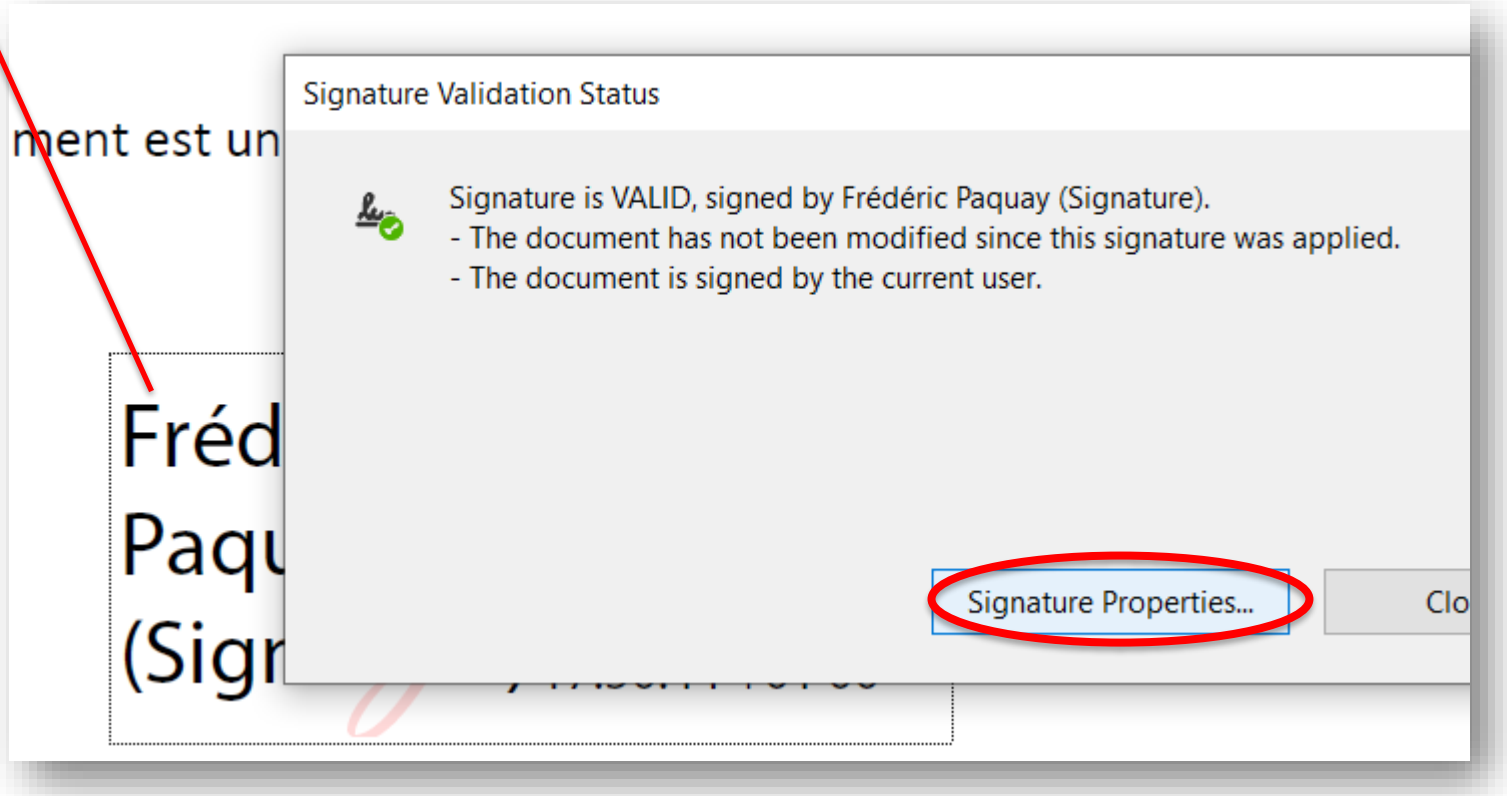


- une autorité de certification (CA) utilise une signature qui doit être validée (lien clé publique – identité) par une **autorité de certification supérieure**
- l'autorité de certification racine (root) s'auto-certifie
- plusieurs niveaux pour **limiter les risques** si un certificat est compromis

Signature digitale : certificat eID

Ouvrir avec **Adobe Acrobat Reader** un PDF signé

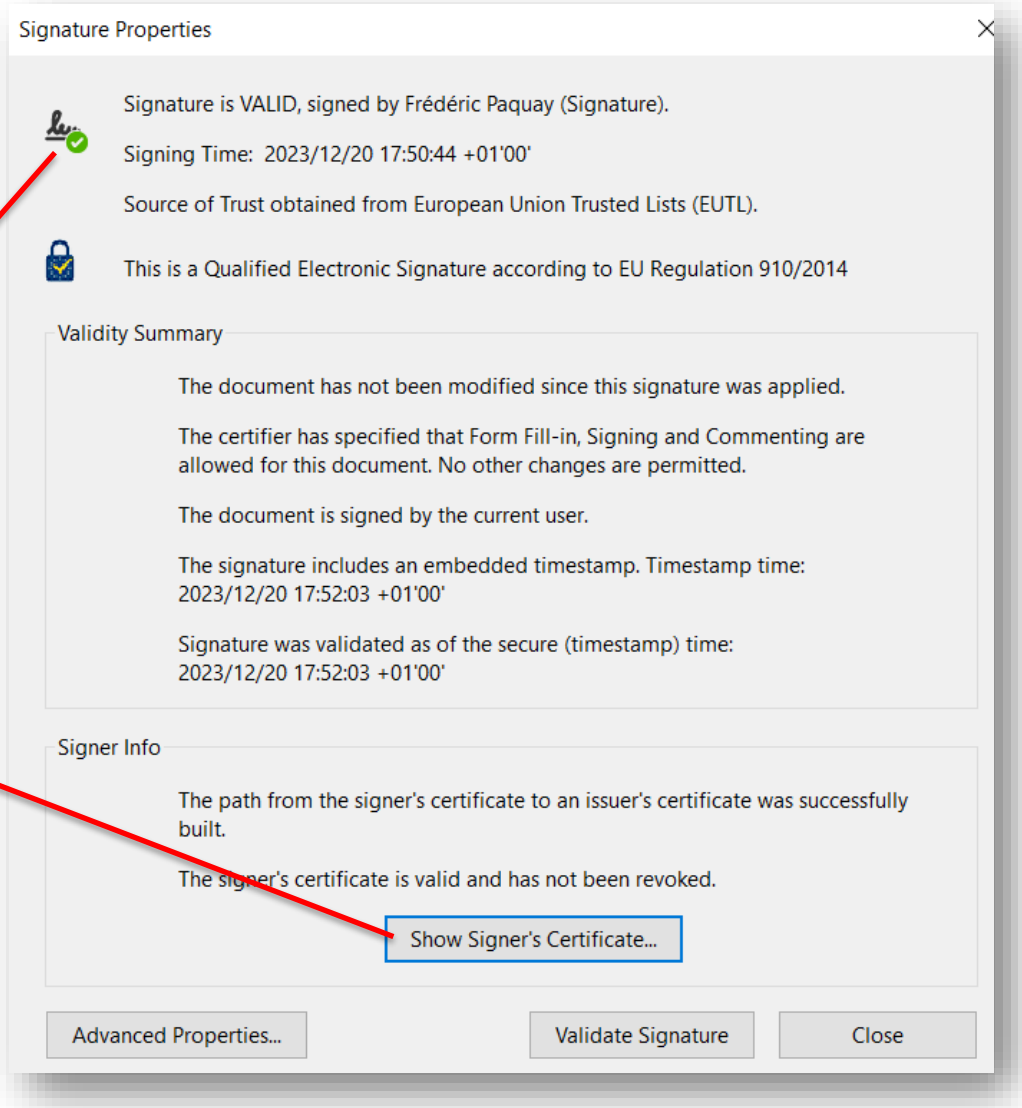
Cliquer sur la signature dans le PDF signé



Signature digitale : certificat eID

Signature valide

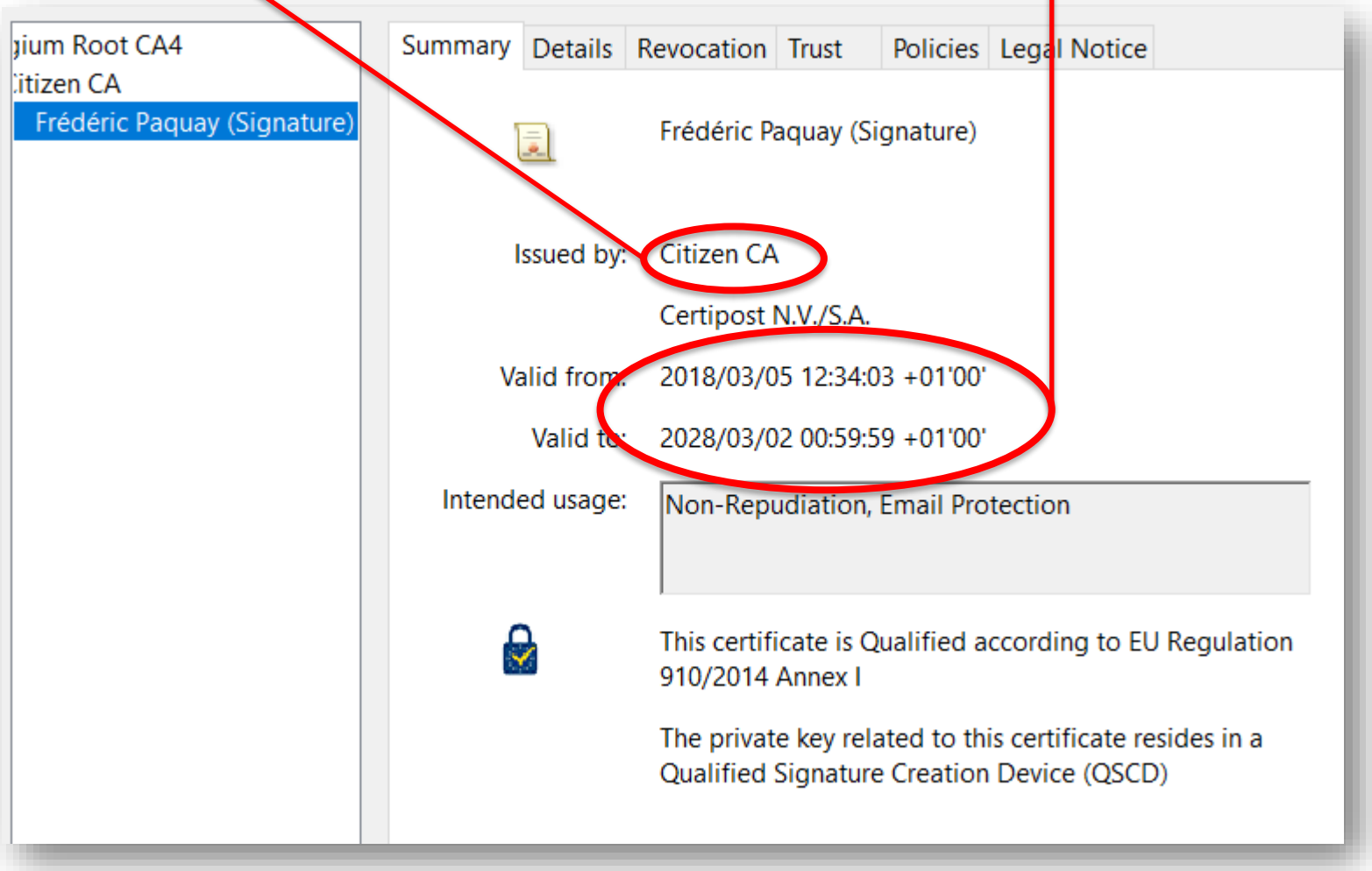
Cliquer ici pour voir le certificat de signature



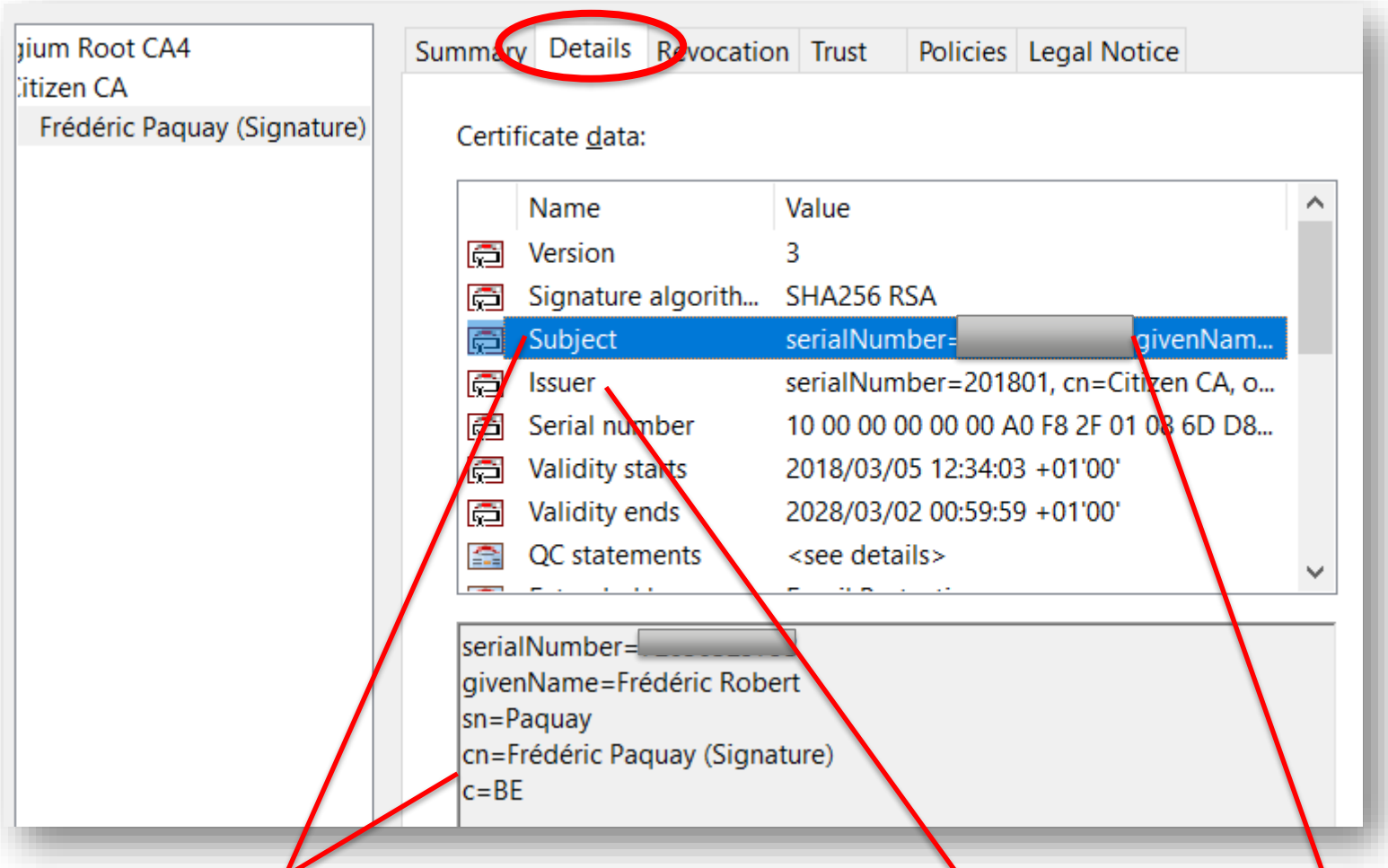
Signature digitale : certificat eID

Autorité de certification (CA)

Durée de validité



Signature digitale : certificat eID

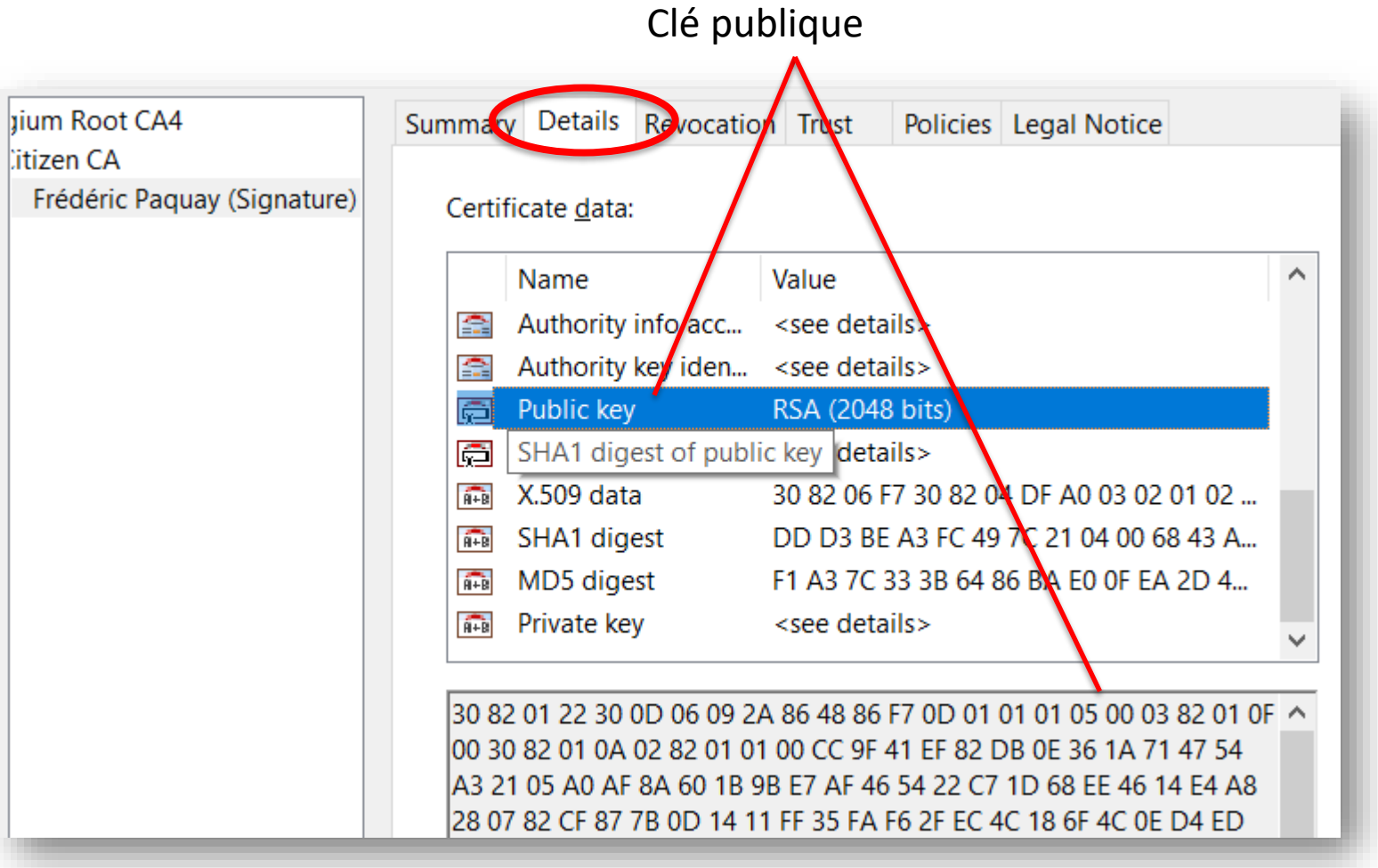


Identification de la personne

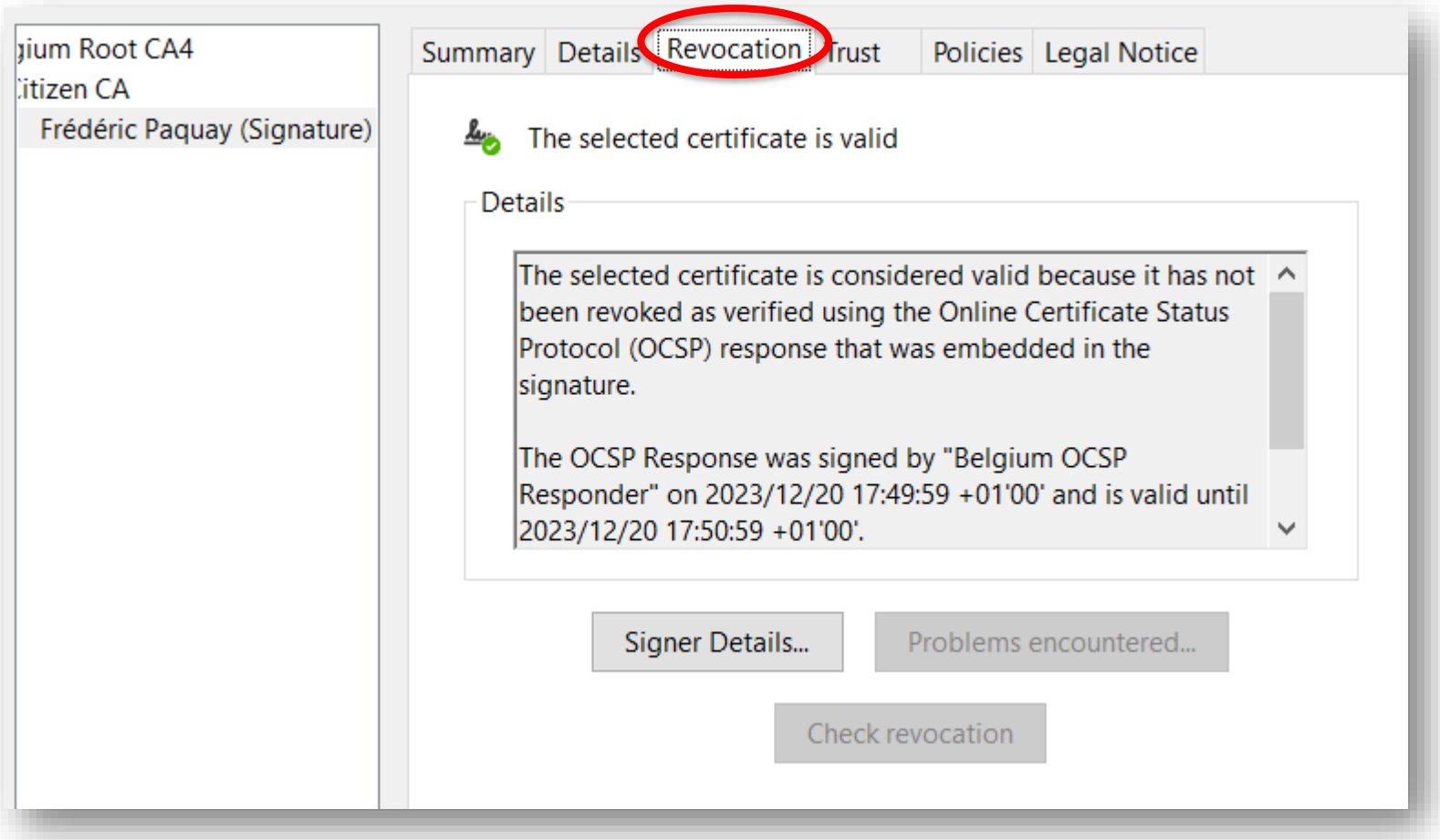
Identification CA

Numéro national

Signature digitale : certificat eID



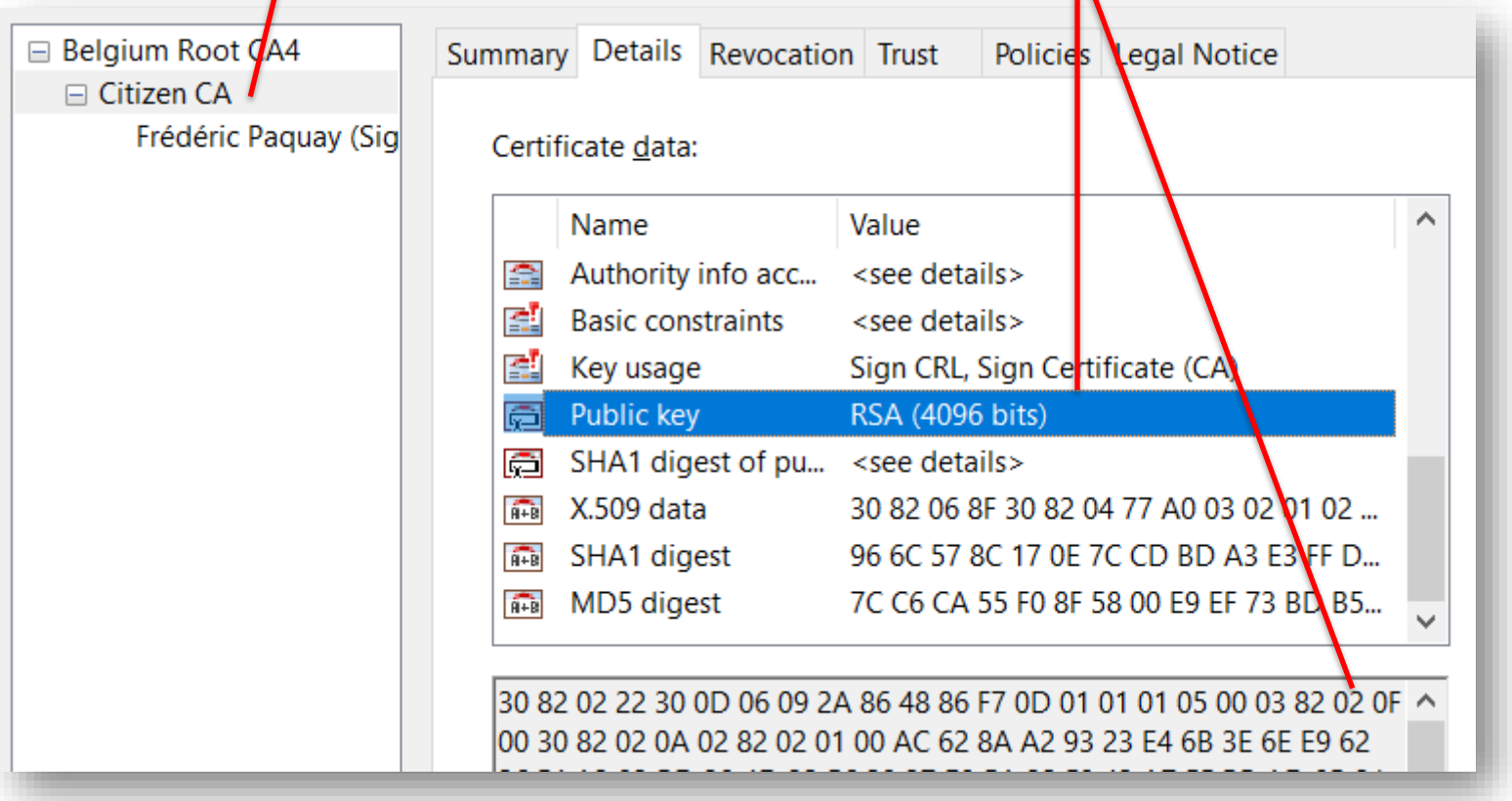
Signature digitale : certificat eID



Signature digitale : certificat eID

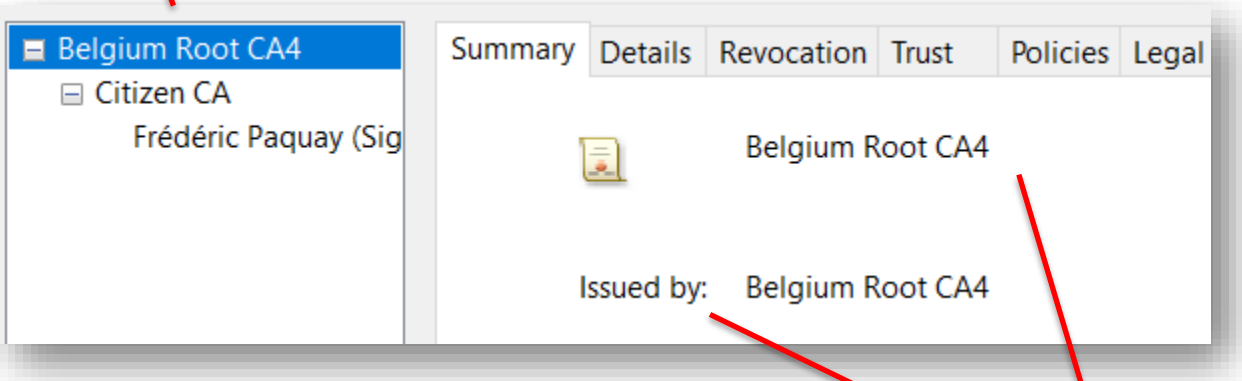
Informations sur CA

Clé publique du CA



Signature digitale : chaine de certificats eID

Chaîne de certificats



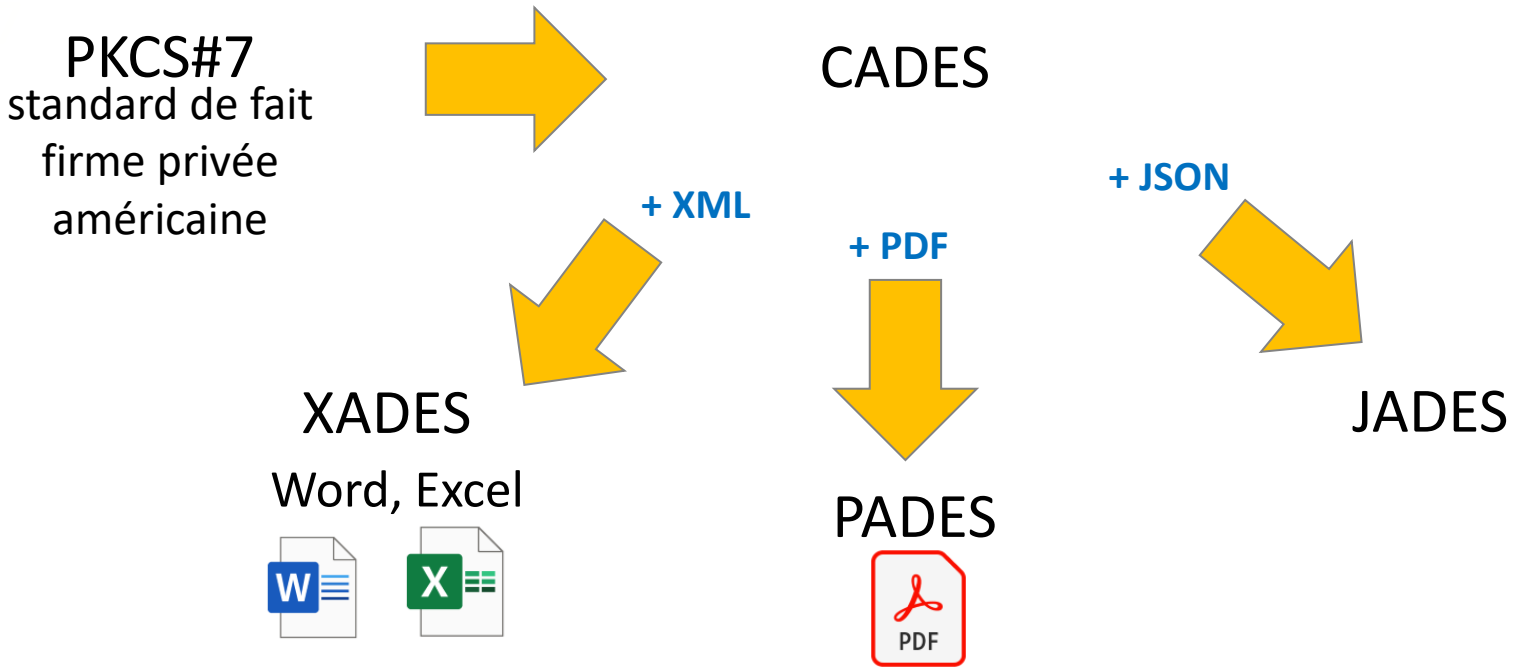
Certificat ROOT autosigné

Signature digitale : document

Modification du document détectée

Signature d'une empreinte du document (algorithme **SHA256**) qui est différente dès que le document est modifié.

Normes européennes ETSI



Signature digitale

- **Marque distinctive** : **clé privée** protégée pour signer et **clé publique** pour vérifier la signature.
- **Authentification** : **certificat** qui lie la clé publique et donc la signature à une personne physique ou morale.
- **Document signé non modifiable** : signature d'une empreinte du document, formalisée par des **standards européens** (CADES, XADES, PADES, JADES).

Signature digitale : qualité

Signature digitale : qualité

Le règlement européenne **eIDAS** (EU 910/2014) fixe plusieurs niveaux de qualité, valables dans tous les états membres.

Signature de **personne physique** ou **morale** (**cachet** ou ***seal***).

Signature digitale : qualité

Règlement eIDAS transposé dans la législation belge par le **Digital Act**, loi du 21 juillet 2016

- **Pas d'obligation** d'utiliser une signature digitale, sauf disposition contraire.
- **Cachet = signature de la personne physique** qui représente la personne morale.
- Vérification de la signature avant de la présumer valide.
- Archivage électronique

Signature digitale : qualité

Simple

- Données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer. (eIDAS, art. 3.10)
- Preuve juridique qui ne peut pas être refusée d'office. (eIDAS, art. 25.1)

Ex : image signature,
signature sur écran tactile, …

Scan & Fax : PAS une signature digitale

- Copie digitale d'une signature manuscrite ≠ signature digitale
- Le document de référence est la signature manuscrite.

Signature digitale : qualité

Avancé - Advanced

- Signature liée au signataire de manière univoque.
- Identification du signataire.
- Contrôle exclusif des données de création de signature.
- Détection d'une modification du document signé.
- Validité suffisante pour certaines demandes administratives, selon les dispositions légales.
- Preuve de non-conformité à charge de l'utilisateur (eIDAS art. 13).

Dans la pratique, un **module cryptographique** (carte à puce, HSM, …) est souvent exigé pour signer.

Ex : signature AATL approuvée par Adobe

Signature digitale : qualité

Qualifié - Qualified

- Reprend les qualités de la signature avancée.
- Géré par un **prestataire de service de confiance qualifié** : preuve de respect des obligations à sa charge, statut officiel (trusted list) par organisme de contrôle (SPF Economie), audit tous les 2 ans à leur frais, personnel qualifié et formé, normes internationales de sécurité à respecter, garantie de fiabilité du système, ressources financières suffisantes, plan d'arrêt à prévoir pour maintenir certains services, validité des certificats disponible 24/7, … **beaucoup de contraintes** !
- Preuve de conformité à charge du prestataire.
- **Certificat qualifié** (mention QEC) valide et identifiant la personne.
- Dispositif de création de signature qualifiée (QSCD), certifié et présent dans une liste officielle.
- Présentation du document avant signature.

→ Signature qualifiée **équivalente** à une **signature manuscrite** reconnue dans tous les états membres, cachet supposé intègre et exact.

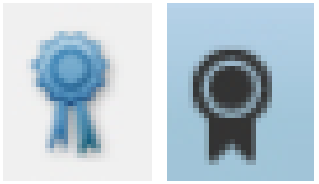
Signature digitale : qualité

Qualifié - Qualified

- Outils disponibles pour le grand public en Belgique :
  - **eID** (gratuit)
  - **It’s me** (payant)
- D’autres solutions professionnelles existent mais sont **complexes** et **onéreuses**.

Signature PDF dans Adobe Acrobat Reader

Signature digitale : qualité



certificat issu de CA qualifié

≠

signature qualifiée

Pour une signature qualifiée, il ne suffit pas que l'autorité de certification (CA) soit qualifiée, il y a des exigences supplémentaires.

Signature digitale : qualité

Défini par la réglementation eIDAS, de la plus forte à la moins forte :

- **qualifié**, équivalent à une **signature manuscrite** (ex : eID, It's me)
- **avancé**, fiable, souvent équivalent techniquement à une signature qualifiée (ex : AATL reconnu par Adobe)
- **simple**, facile mais peu fiable (ex : signature manuelle sur écran tactile, image de signature)

Article 25

Effets juridiques des signatures électroniques

1. L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

2. L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.

3. Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres.

Signature digitale : extensions

Signature digitale : extension horodatage

Horodatage (timestamp)

- **Signature** par un **service d'horodatage** réputé fiable.
- Preuve d'existence à un moment donné.
- **Nécessaire si obligation légale de datation.**

Horodatage qualifié = signature qualifiée par service certifié d'horodatage.

Ex : http://tss.eidpki.belgium.be/

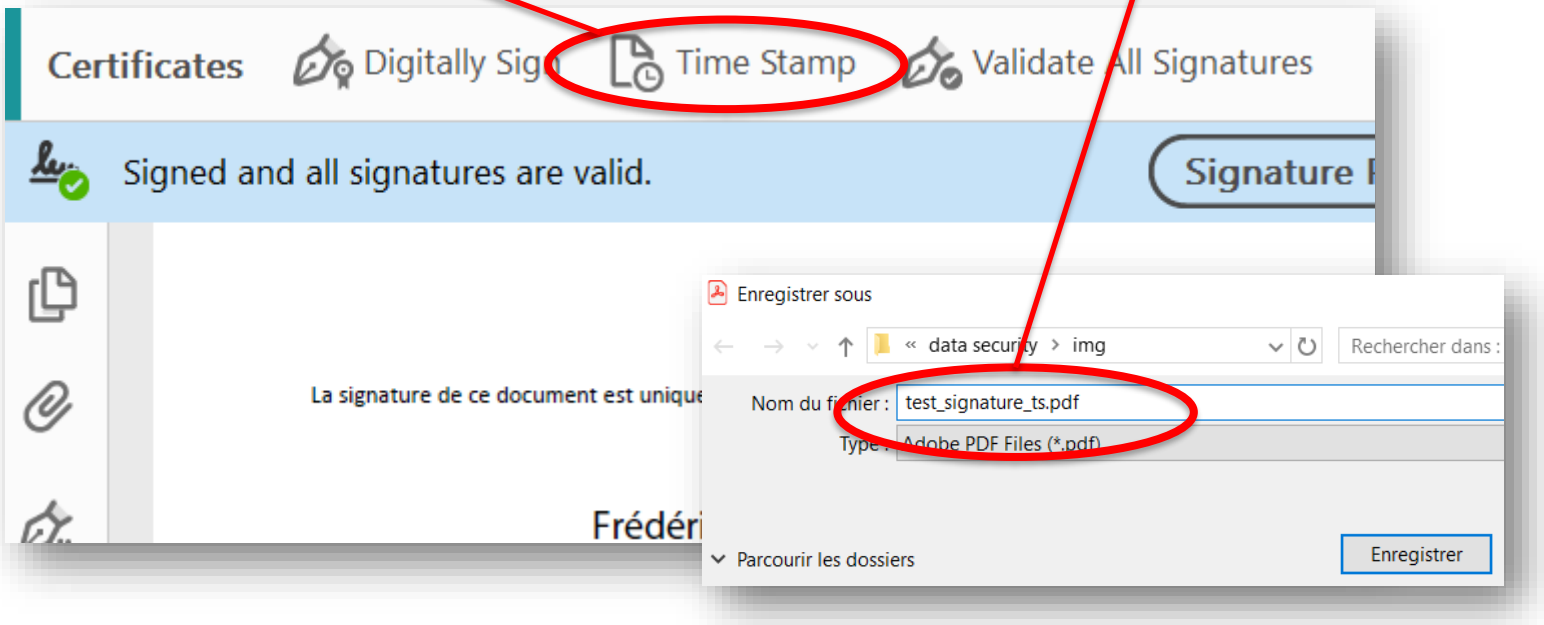
Signature digitale : extension horodatage

Ajout d'un horodatage (timestamp)

Adobe Acrobat Reader doit être configuré avant de pouvoir ajouter un horodatage (voir annexe en fin de présentation).

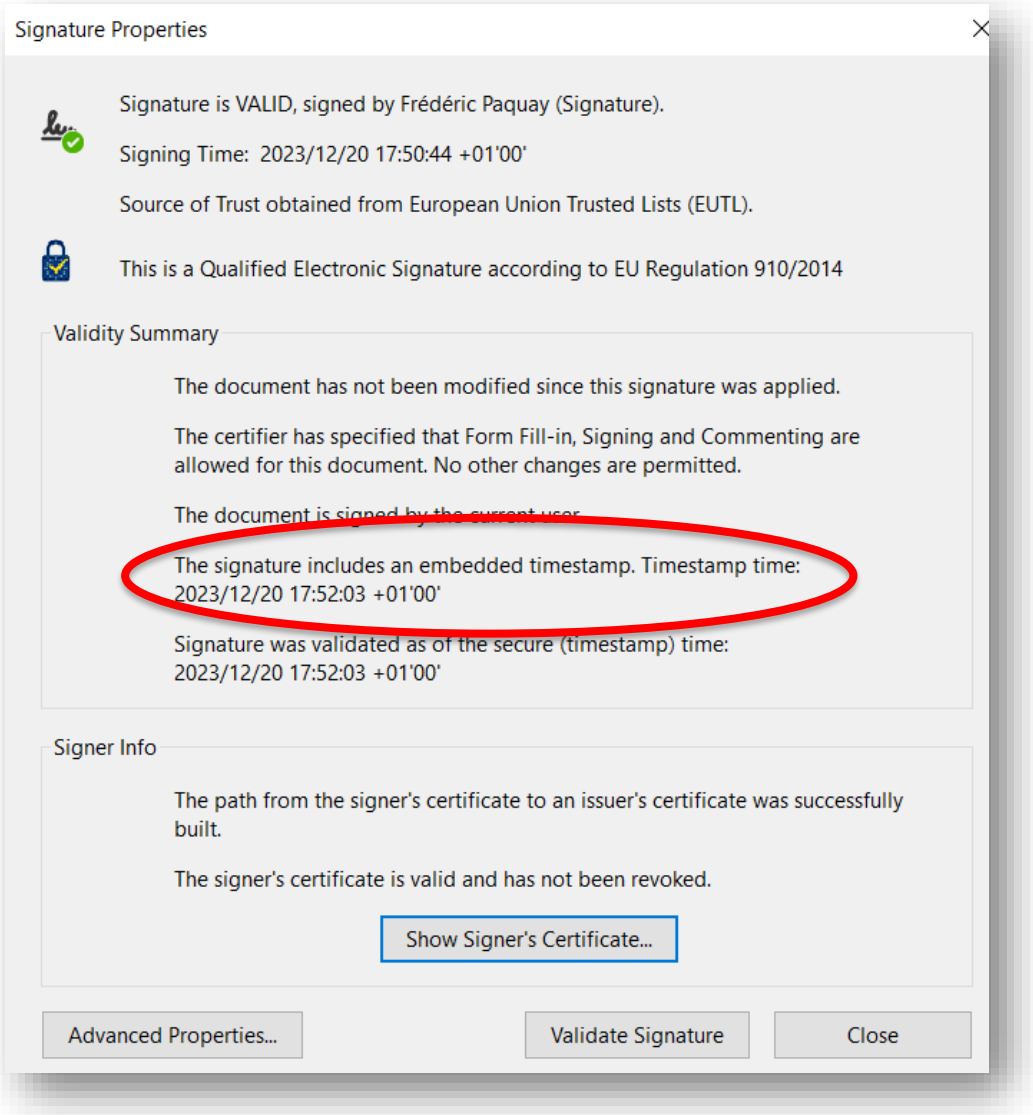
Cliquer sur « Time Stamp »

Sauvegarde du fichier horodaté



Signature digitale : extension horodatage

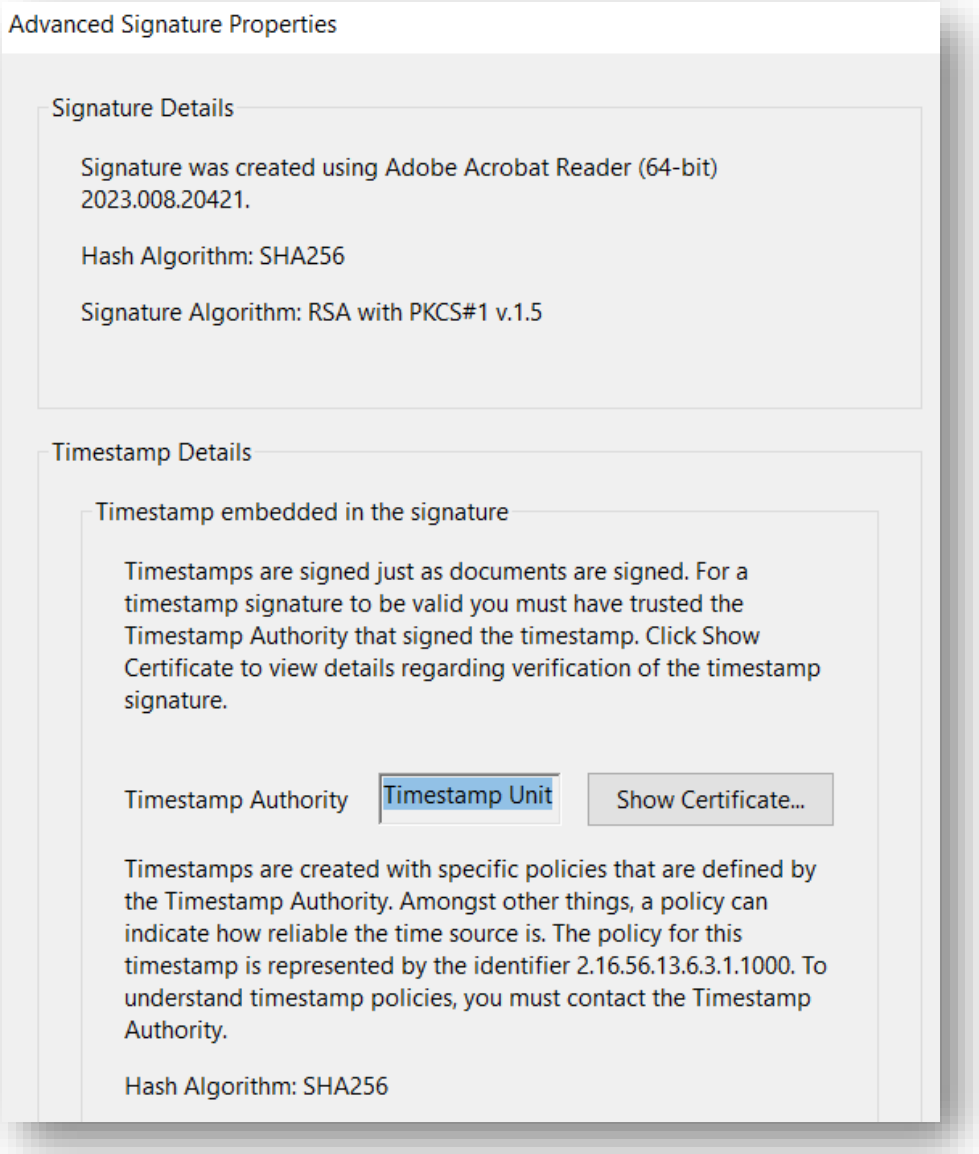
Vérification horodatage (timestamp)



Plus d'informations en cliquant sur « Advanced Properties… »

Signature digitale : extension horodatage

Vérification horodatage (timestamp)



Signature digitale : extension validation

Validité des certificats

Le certificat de signature et ses supérieurs dans la chaîne doivent être valides, au moins lors de la signature :

- **non expiré** → signature horodatée nécessaire
- **non révoqué**, vérifié par
  - **CRL** : liste de révocation des certificats,
  - **OCSP** : vérification en ligne pour un certificat.

Adobe Acrobat Reader dans une version récente fait appel systématiquement à OCSP

Signature digitale : extensions

Ajout dans la signature :

- 🕐 **Horodatage** (timestamp) : configuration dans Adobe avec le service http://tss.eidpki.belgium.be/
- ✔ Vérification de la **validité des certificats** (OCSP ou CRL) : utilisé par Adobe

Normes ETSI EN 319 142 (profils de signature) :

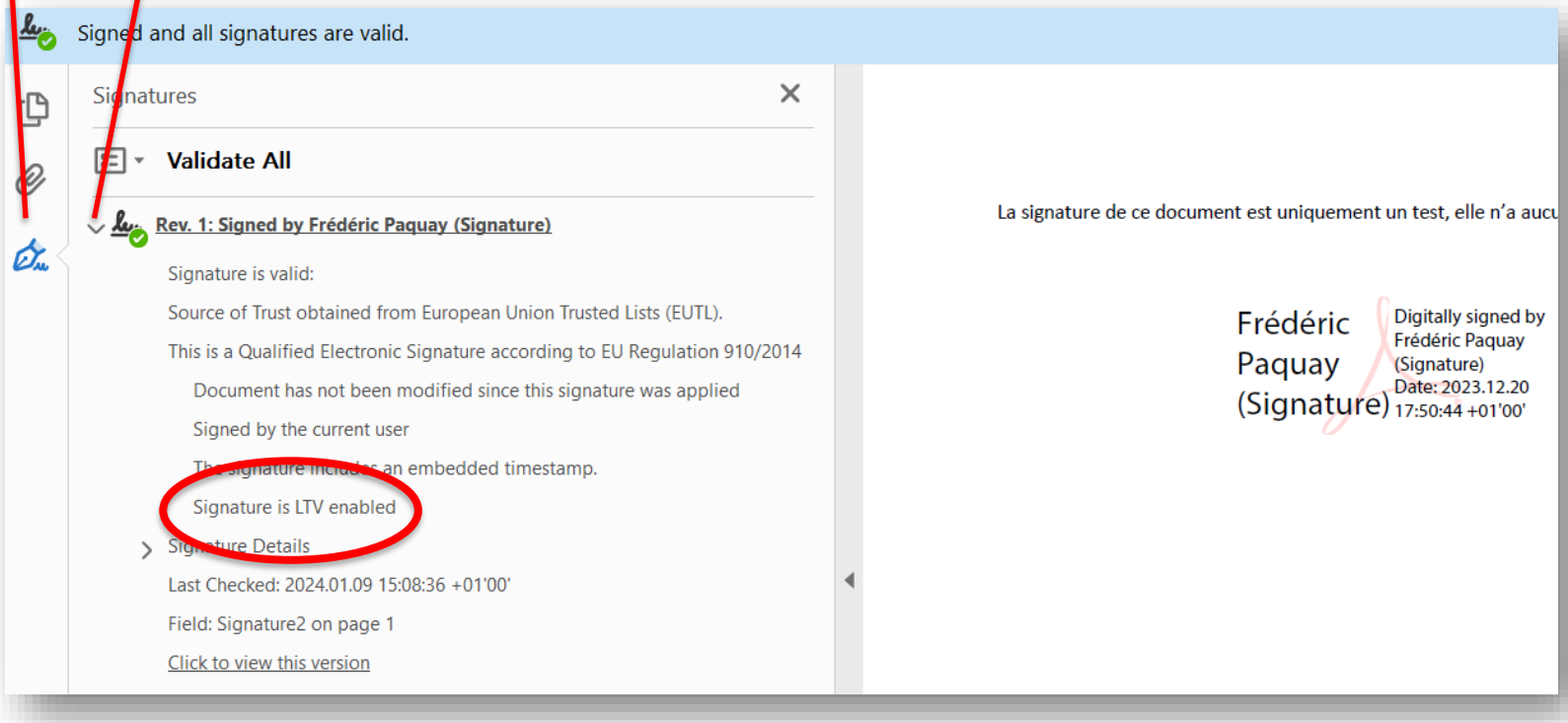
- **B :** signature basique à **court terme** (1 an)
- **T :** ajout d'un horodatage à la signature
- **LT :** ajout d'un horodatage et des données de validité des certificats
- **LTA/LTV :** signature LT **resignée périodiquement** par horodatage pour une **conservation à long terme**.

Signature digitale : extensions

Vérification du **profil** de signature par **Adobe Acrobat Reader**.

1. Ouvrir le panneau de signature

2. Ouvrir la signature

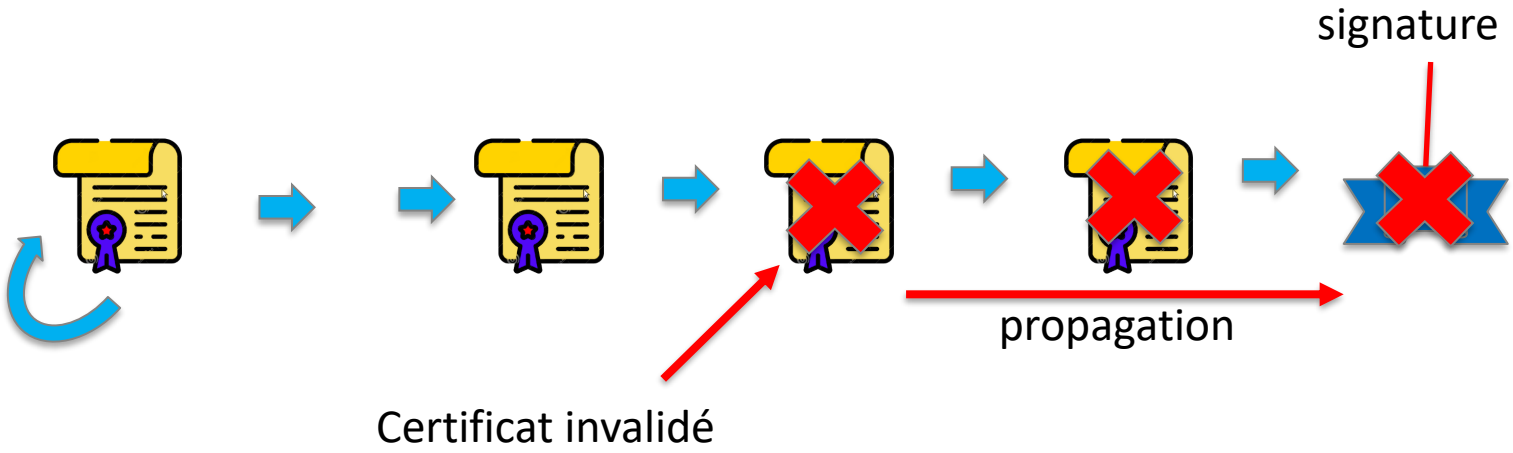


Signature digitale : limites

Signature digitale : limite connue

Validité certificat

Un certificat est invalide si expiration de la **date** de validité ou **révocation**, cela entraine l'**invalidation des dépendances**.

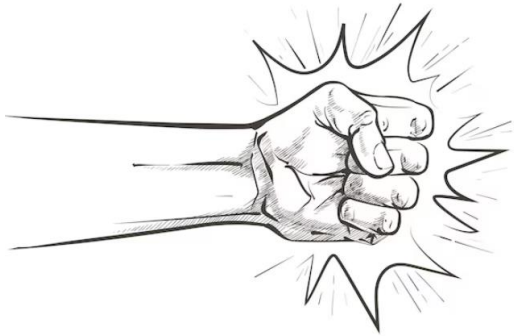


La **signature** correspondante à ce certificat n'est **plus valide**, sauf si elle a été étendue **avant** l'invalidation du certificat. Il faut **resigner** (horodater) périodiquement le document pour maintenir la validité de la signature.

Signature digitale : limite connue

Taille de la clé

Les algorithmes de signature sont réputés fiable mais la taille de la clé doit être suffisante pour éviter les **attaques par force brute** (essai de toutes les possibilités).

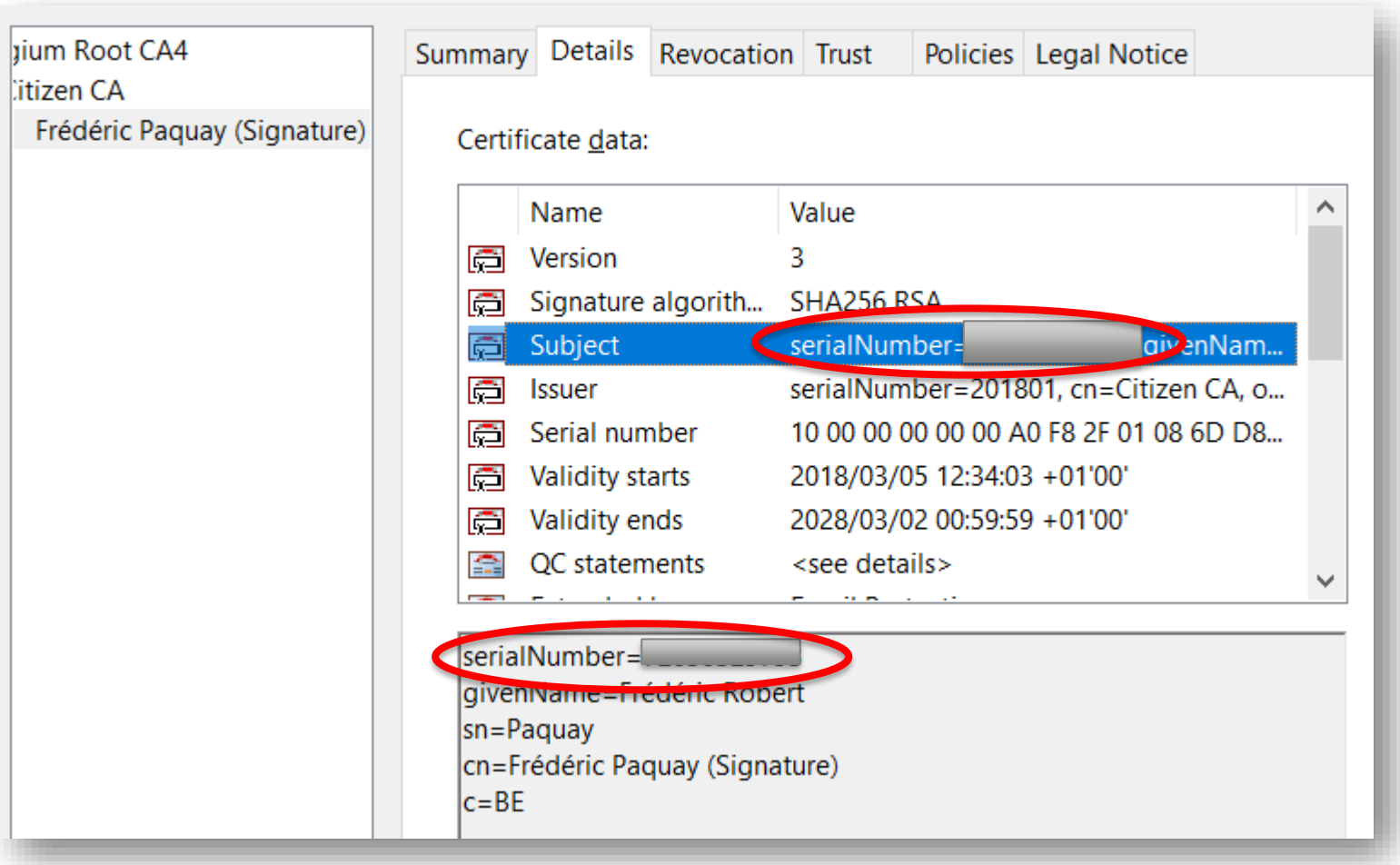


Taille de clé recommandée :

- **RSA** : 2048 bits, 3072 bits à partir de 2030
- **ECDSA** : 224 bits, 256 bits à partir de 2030

Signature digitale : limite connue

Numéro national visible dans le certificat eID.



Signature digitale : limite connue

Environnement technique

L'utilisation de méthode de signature est soumise à des **contraintes techniques**.

Carte à puce (eID) :

- Lecteur de carte et pilote (driver) adapté.
- Application développée pour utiliser ce matériel.
- Pas directement utilisable depuis un navigateur internet.
- Peu développé pour les smartphones et tablettes.

Méthode distante (It's me) :

- Connexion internet nécessaire lors de la signature.
- Disponibilité du service distant.

Signature digitale : limite connue

Opacité technique

Volontairement ou par erreur, une application pourrait signer autre chose que le document affiché. Vérifier si la signature est appliquée au bon document ne peut se faire qu'**après la signature**.

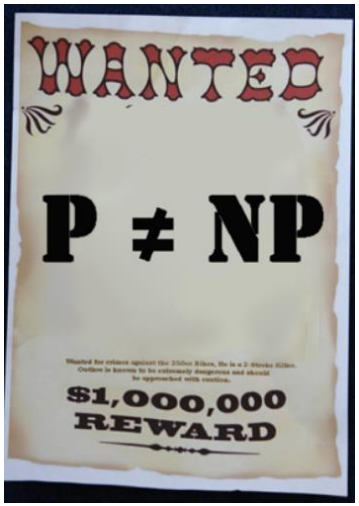
Signature digitale : limite inconnue

Algorithmes de signature

Pour les algorithmes actuels, il n'y a aucune preuve mathématique que la signature digitale est complexe à falsifier.

C'est lié au problème : P = NP ?

1.000.000 $ si vous trouvez la solution (prix du millénaire Clays) !



Signature digitale : limite inconnue

Matériel de sécurité

Les fabricants de matériel cryptographique (carte à puce, HSM) utilisent des méthodes de protection pour interdire l'accès au circuits électroniques et à leur contenu.

Méthodes d'intrusion :

- Ouverture du matériel
- Rayon X
- Analyse des entrées/sorties (résultats en fonction des entrées, temps de calcul)

Les méthodes de protections sont gardées secrètes. Sont-elles suffisantes à terme ?

Signature digitale : limite inconnue

Ordinateur quantique

Calcul en parallèle avec des **bits quantiques** (qbit) qui possèdent simultanément la valeur 0 et 1. Il existe un algorithme de factorisation pour craquer le RSA et le ECDSA.

Les machines existent mais ont trop peu de qbits et sont déjà trop **instables**.

« Je crois pouvoir dire que personne ne comprend la mécanique quantique.» **Richard Feynman**

Signature digitale : limites

Connues :

- **Validité** limitée du **certificat** (resignature périodique).
- **Taille minimale** nécessaire pour la **clé**.
- **Numéro national visible** dans le certificat eID.
- **Environnement technique** pas toujours adéquat (ex : utilisation de l'eID avec un smartphone ou un navigateur).
- **Opacité technique** sur le contenu à signer.

Inconnues :

- **Algorithmes :** aucune preuve mathématique de fiabilité !
- **Matériel de sécurité (eID) :** fiabilité inconnue à long terme.
- **Ordinateur quantique :** risque peut-être exagéré.

Conclusion

Une signature digitale légale doit nécessairement être **qualifiée**, sauf disposition contraire dans un document législatif. Par contre, une signature non qualifiée ne peut pas être rejetée d'office comme preuve.

➡ **signature qualifiée pas toujours nécessaire**

La preuve du **consentement à un acte** ne dépend pas que d'une signature, elle dépend aussi d'un **contexte** : courrier échangé, preuve de présence, enregistrement audio ou vidéo, témoignage assermenté, …

➡ **signature pas toujours nécessaire**

Risque : sujet à interprétation !

Merci !

SPP Intégration sociale, Lutte contre la Pauvreté, Economie sociale et Politique des Grandes Villes

Centre administratif Botanique
Finance Tower
Boulevard du Jardin Botanique 50 boîte 165
1000 Bruxelles

POD MAATSCHAPPELIJKE INTEGRATIE
BETER SAMEN LEVEN
SPP INTÉGRATION SOCIALE
MIEUX VIVRE ENSEMBLE

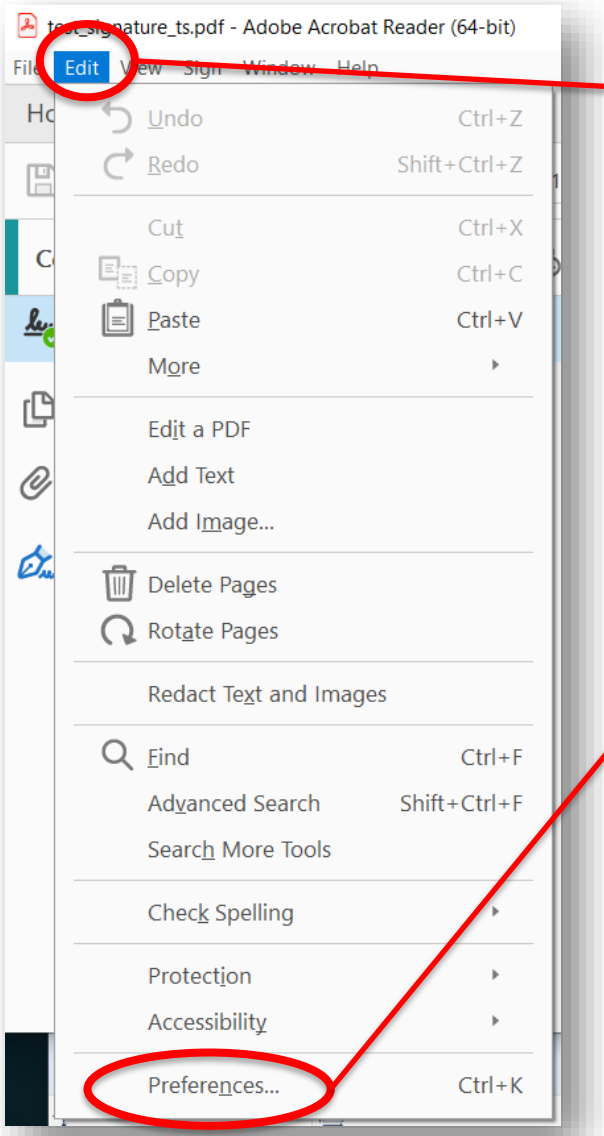
Contactez-nous

lundi au vendredi de 8h30 à 12h30 et de 13h à 16h30 (vendredi jusque 16h) via

+32 2 508 85 86 ou +32 508 8430
question@mi-is.be mi.dpo@mi-is.be
www.mi-is.be

Suivez-nous

Annexe : configurer un horodatage dans Adobe

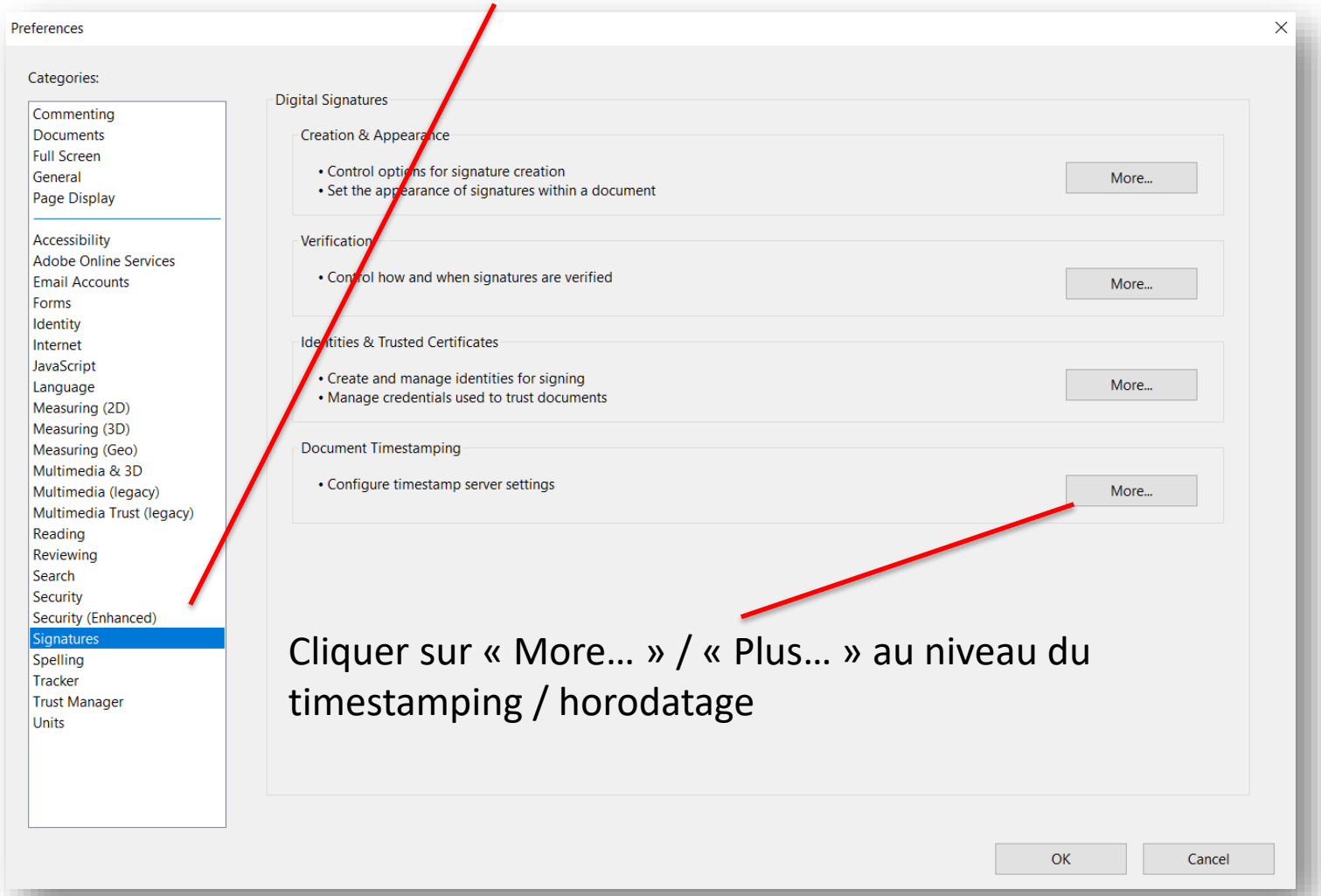


Cliquer sur « Edit »

Cliquer sur « Preferences »

Annexe : configurer un horodatage dans Adobe

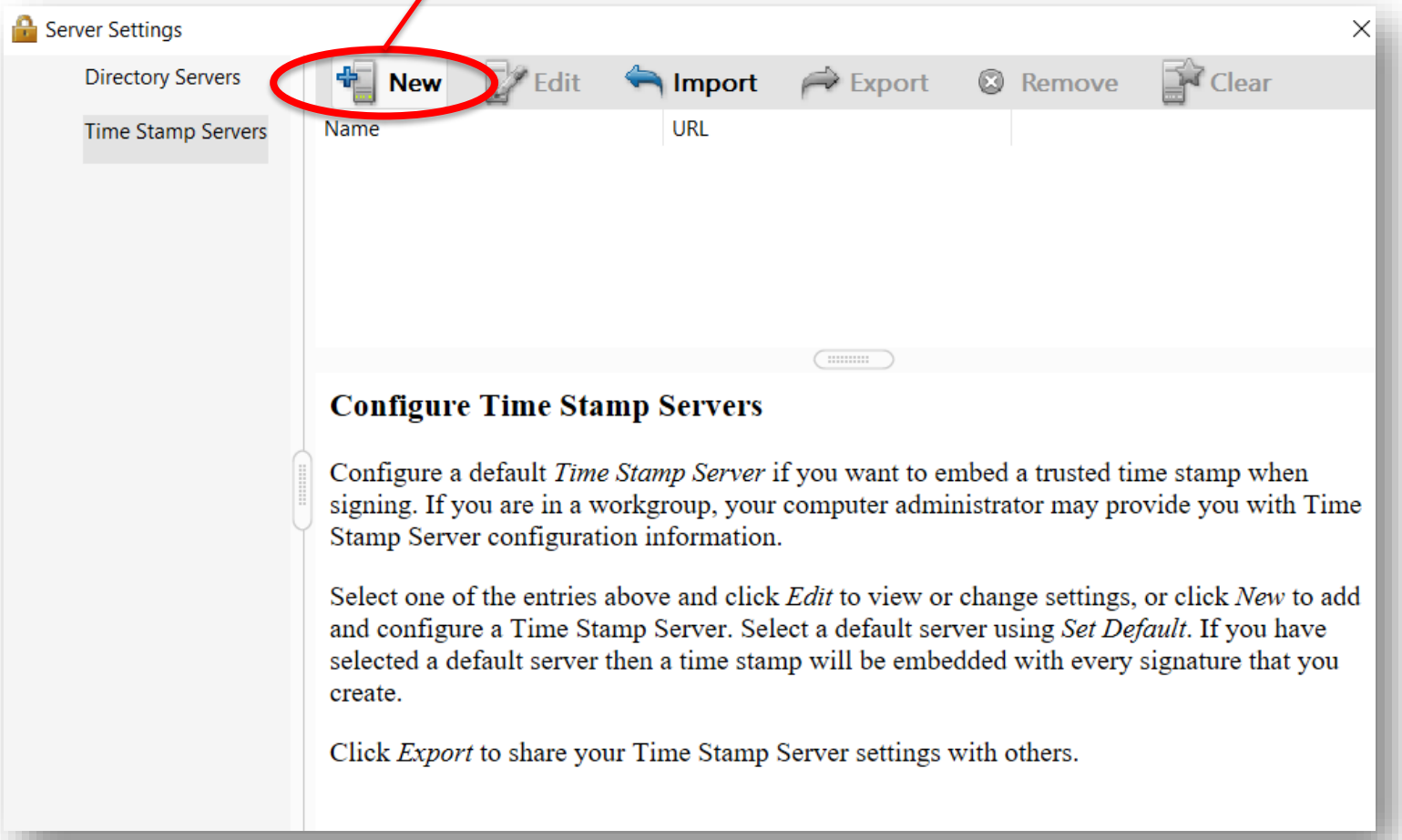
Choisir « Signatures » à gauche



Cliquer sur « More… » / « Plus… » au niveau du timestamping / horodatage

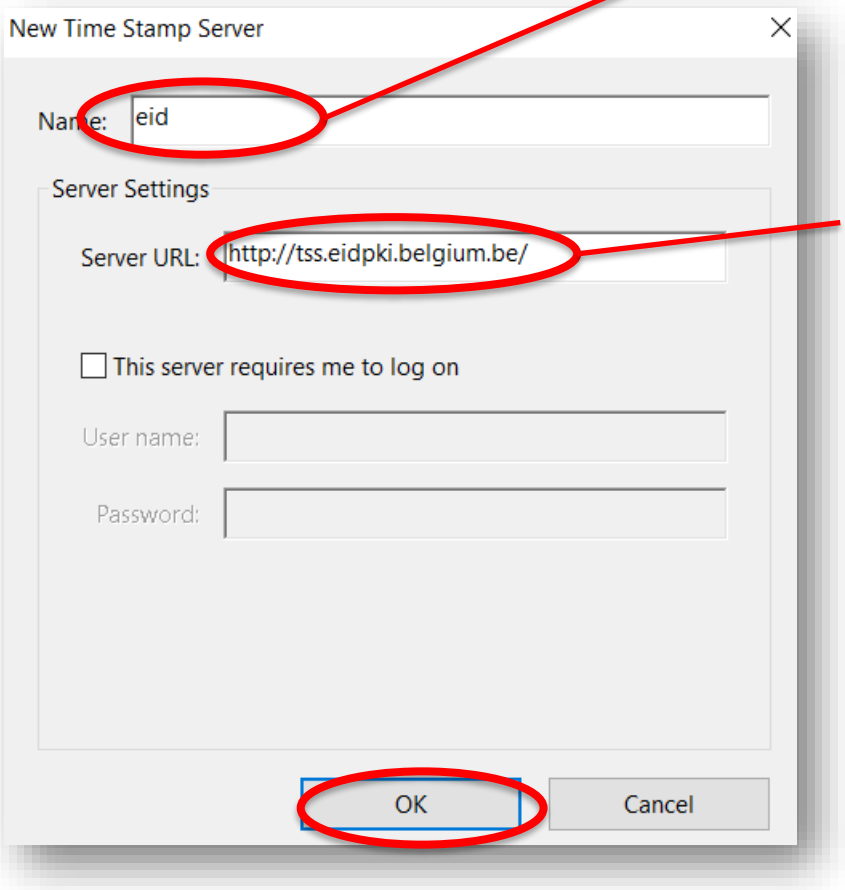
Annexe : configurer un horodatage dans Adobe

Cliquer sur « New »



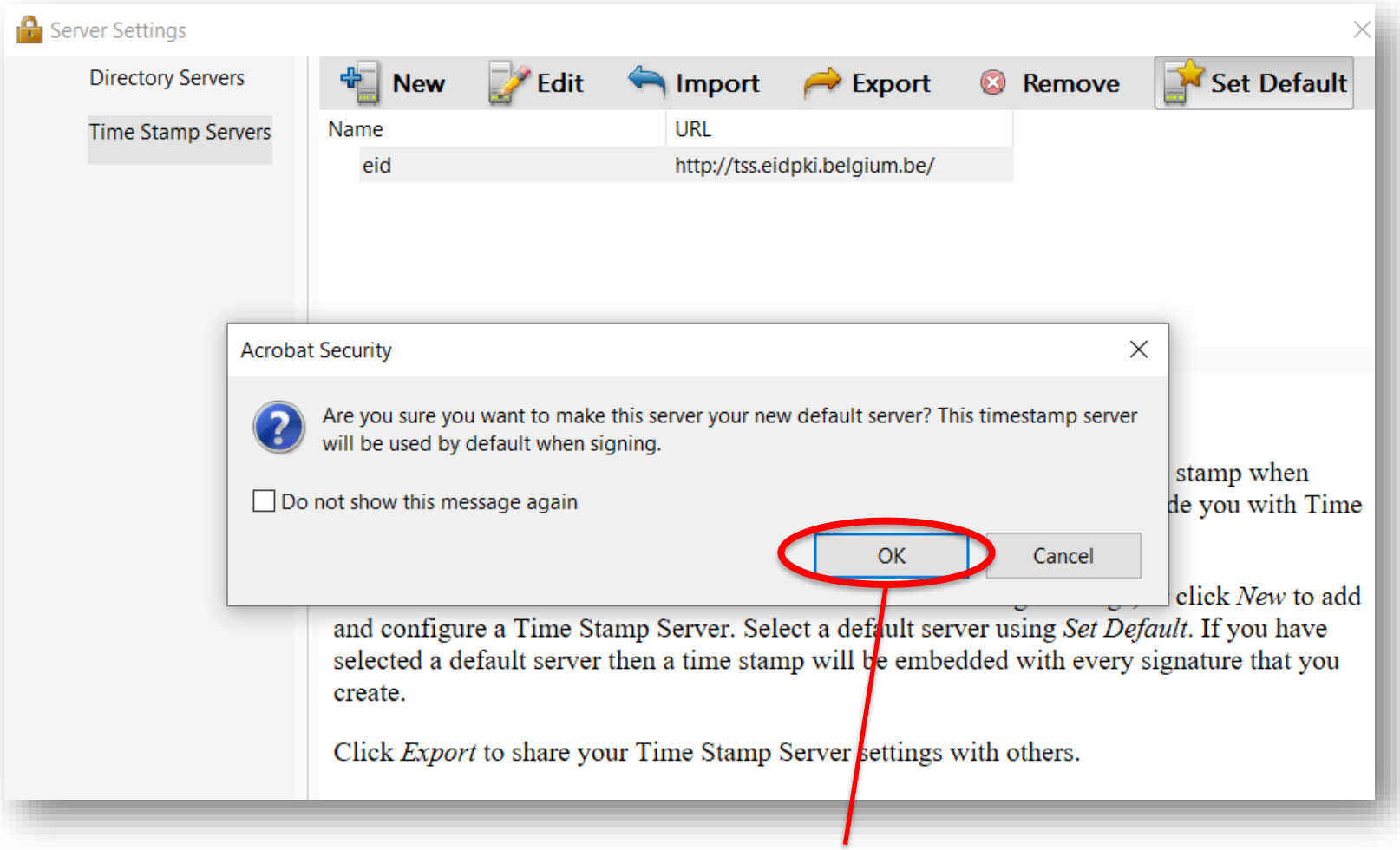
Annexe : configurer un horodatage dans Adobe

Attribuer un nom de votre choix



URL vers le service d'horodatage :
http://tss.eidpki.belgium.be

Annexe : configurer un horodatage dans Adobe



Cliquer « OK » pour ajouter un horodatage aux signatures