CERTIGNA
Groupe Tessi

CERTIGNA HORODATAGE

Application Programing Interface

Mars 2023

Sommaire

1. CERTIGNA – EXPERT DE LA CONFIANCE NUMERIQUE

Créée en 2005 et basée à Villeneuve d'Ascq, CERTIGNA se positionne en tant que prestataire de service de confiance (PSCO) et apporte un espace de confiance sur Internet avec des solutions d'authentification, de chiffrement, de signature et d'horodatage électronique.

Depuis juillet 2017, CERTIGNA est devenue filiale du **Groupe Tessi**, N°1 français du flux documentaire.

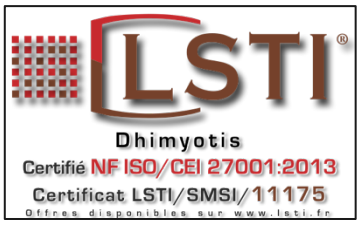
Composée d'experts reconnus, **CERTIGNA se concentre sur deux axes : la sécurité des échanges sur Internet et la dématérialisation des documents.**

1.1. Nos qualifications

En 2008, **CERTIGNA** devient le **premier PSCO français certifié** sur les normes européennes de l'ETSI relatives à l'authentification et à la signature électronique.

CERTIGNA devient « Opérateur de certification » et « Autorité de certification », et commercialise dès lors des certificats numériques certifiés.

En 2016, les certificats délivrés par CERTIGNA sont reconnus **« Qualifiés »** au sens du Règlement européen **eIDAS**, en complément de leur qualification **RGS** et de leur certification ETSI.



En 2017, CERTIGNA obtient la certification ISO/CEI 27001 de l'ensemble de ses solutions, prestations et activités attestant de la capacité du groupe à garantir un management rigoureux et vertueux de la sécurité de ses services.

CERTIGNA est **qualifiée** par l'**ANSSI** concernant :

- La délivrance de certificats de signature électronique
- La délivrance de certificats de cachet électronique
- La délivrance de certificats d'authentification de site web
- **La délivrance de Services d'Horodatage électronique**

Fort de ses certifications et références, **CERTIGNA s'est imposée comme le prestataire de services de confiance français qui accompagne actuellement plus de 25 000 clients** (Ministères, Collectivités, Entreprises, Banques, ...).

En découvrir plus en vidéo : https://www.youtube.com/watch?v=zxq2GMtJxIo

2. PRESENTATION DU SERVICE CERTIGNA HORODATAGE

2.1. Rappel : Qu'est-ce que l'horodatage ?

L'horodatage électronique **donne une date et une heure certaine** aux documents utilisés dans le cadre des échanges électroniques en vue d'en **garantir l'existence à une date donnée, ainsi que l'intégrité, prouvant ainsi qu'il n'a subi aucune modification depuis ladite date.**

L'horodatage des documents sert de preuve irréfutable concernant :

- **La non-altération du document numérique** c'est-à-dire que le document numérique n'a pas été modifié depuis son horodatage.
- **Le respect des délais légaux** : la date de l'horodatage faisant foi comme le cachet de la Poste. (ex : preuve qu'une réponse à un appel d'offres a été effectuée dans les délais impartis).
- **L'accusé de réception** après envoi des documents. (lettre recommandée électronique)
- **La traçabilité** des actions.

Lors de l'horodatage de données numériques, **un jeton d'horodatage (timestamp) est délivré par un Prestataire de Service d'Horodatage Electronique (CERTIGNA)**. Ce jeton d'horodatage scelle les données numériques en y apposant une datation à la seconde près permettant d'en garantir son intégrité et son antériorité. Ceci peut être utilisé comme **un élément de preuve**.

2.2. Principe de l'horodatage

Concrètement, lors de l'horodatage d'un document numérique :

1/ Une empreinte numérique des données / du fichier numérique est créé.

2/ Cette empreinte est scellée via un jeton d'horodatage délivré par CERTIGNA en respectant les protocoles juridiques et les techniques normalisées pour sceller les données électroniques.

3/ Le jeton d'horodatage scelle les données avec une datation à la seconde près pour en garantir leur integrité et leur antériorité. Le jeton prend la forme de données numériques délivrées par l'association de l'empreinte numérique des données horodatées avec une heure provenant d'une source de temps fiable signée par CERTIGNA.

Le jeton d'horodatage contient notamment

- **L'identifiant de la Politique d'Horodatage** (PH) sous laquelle le jeton d'horodatage de temps a été généré. Ce document décrit les engagements de CERTIGNA quant à son service d'horodatage ;
- **La valeur de hachage et l'algorithme de hachage de la donnée** qui a été **horodatée** ;
- **La date et le temps UTC** ;
- **L'identifiant du certificat de l'Unité d'Horodatage** (UH) qui a généré le jeton d'horodatage (qui contient aussi le nom de l'Autorité d'Horodatage).

Les utilisateurs finaux peuvent sur besoins**, vérifier la validité des certificats d'horodatage** (chaîne de certification, liste des certificats révoqués...).

2.3. Pourquoi choisir CERTIGNA Horodatage ?

Prestataire de service de confiance, **reconnu au niveau français et européen** CERTIGNA est plus particulièrement **Prestataire de Service d'Hordatage Électronique.**

CERTIGNA est à la fois **l'Autorité de Certification qui délivre les certificats utilisés pour son service horodatage et l'Autorité d'horodatage qui délivre les jetons d'horodatage**.

Le service d'horodatage de CERTIIGNA bénéficie de nombreuses qualifications et certifications nationales et européennes. Les jetons d'horodatage ainsi délivrés par CERTIGNA sont :

CERTIGNA met en œuvre les moyens humains et techniques nécessaires pour assumer la sécurité et la conformité de son service d'horodatage. Pour cela, CERTIGNA s'appuie sur une infrastructure redondée et l'emploi de plusieurs unités d'horodatage et sources de temps afin de garantir la disponibilité de son service d'horodatage et la précision de l'heure délivrée dans ses jetons.

3. INFORMATIONS TECHNIQUES DU SERVICE

La présente partie décrit l'API du service d'horodatage que CERTIGNA met à votre disposition dans le but d'apposer une date certaine à vos données ou fichiers numériques.

Vous pourrez y retrouver les fonctions, leur syntaxe, la liste des paramètres (en entrée et en sortie) ainsi que leurs codes retours.

3.1. Prérequis nécessaires

L'usage du service CERTIGNA Horodatage nécessite que vous disposiez des informations / éléments suivants :

- Un compte administrateur.
- Un compte utilisateur (credentiel) permettant d'accéder au service d'horodatage. Vous pouvez créer autant de compte utilisateurs (credentiels) que nécessaire.
- Des jetons d'horodatage acquis via **notre site Internet**.

Pour ce faire :

1/ **Connectez-vous** sur notre **site internet Certigna Horodatage**.

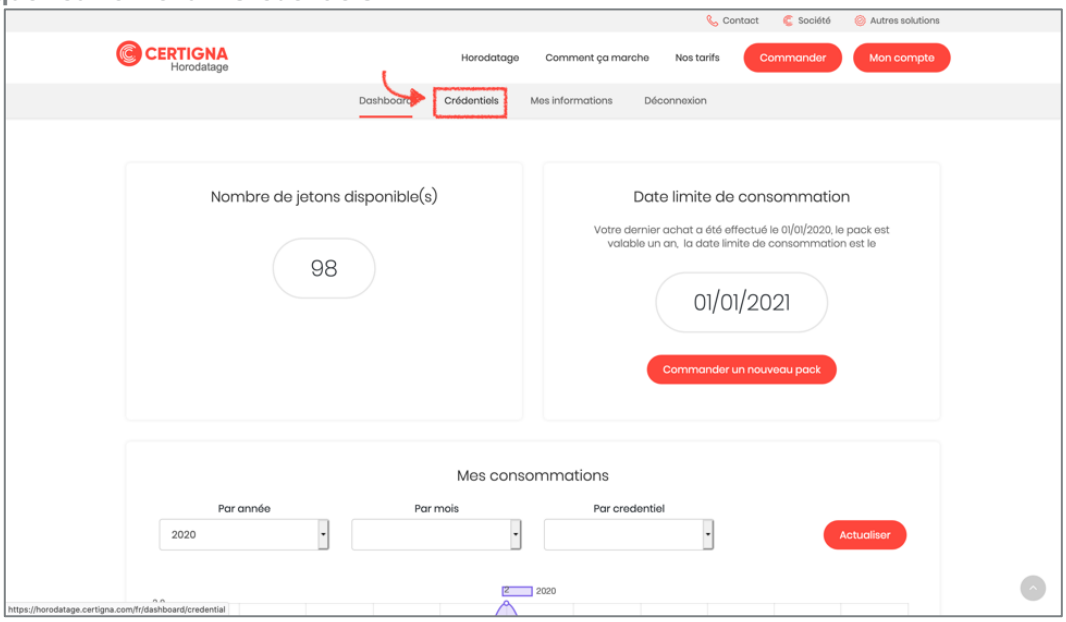
2/ **Procédez à la création d'un compte Administrateur** en cliquant sur le bouton « **Mon Compte** ».

3/ **Faites l'acquisition** d'un **pack de jetons d'horodatage**

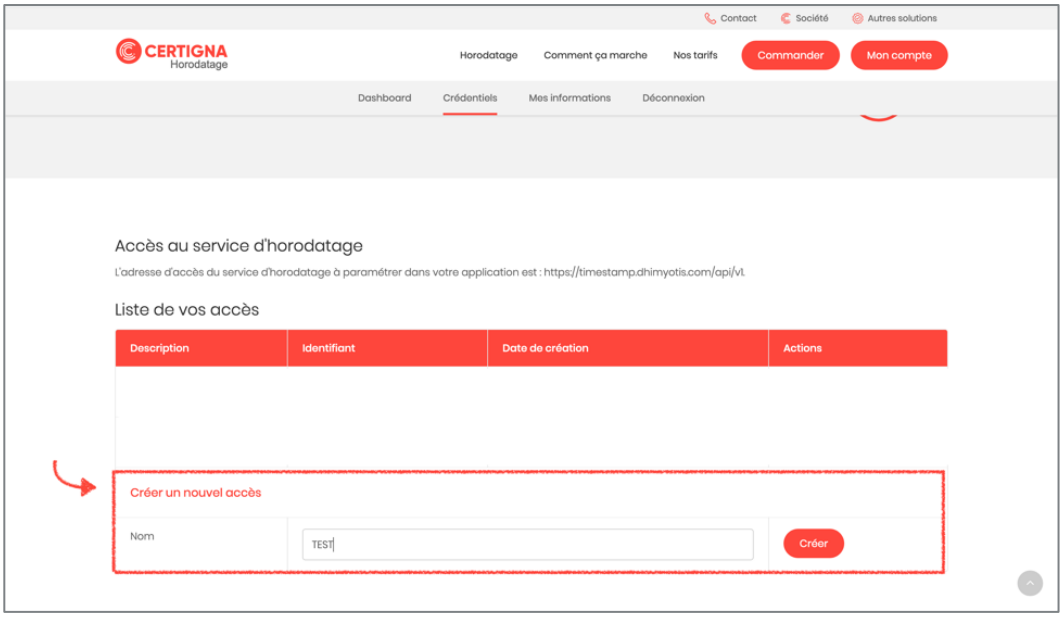
4/ **Procédez à la création d'un compte utilisateur** (crédentiel) – à partir de votre espace personnel et en cliquant sur le menu « **Crédentiels** ». Ce compte utilisateur vous permettra de vous authentifier sur le service Certigna Horodatage.

Comment créer un compte utilisateur (crédentiel) ?

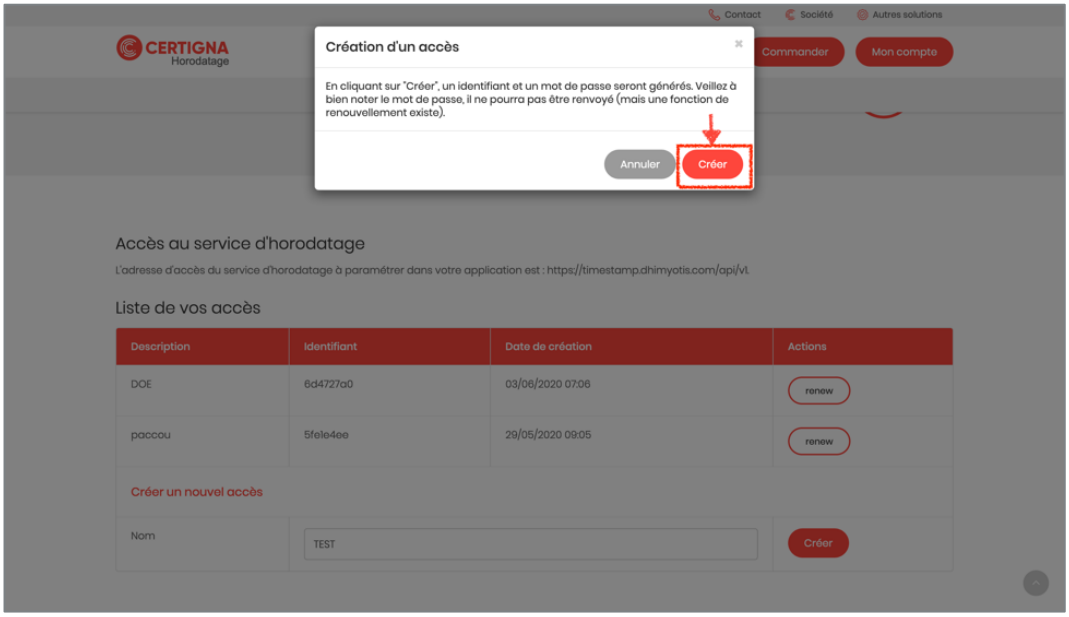
1/ Cliquez sur le menu « **Crédentiels** »



2/ Créez un **nouvel accès au service d'horodatage**



3/ **Confirmez** la création de votre compte utilisateur



4/ **Conservez** bien les informations « **identifiant** » et « **Mot de passe** »

Lorsque vous disposez de jetons d'horodatage et d'un compte crédentiel vous pouvez accéder au service **Certigna Horodatage**.

3.2. Description de l'API CERTIGNA Horodatage

L'API est de type **REST**. Il convient donc **utiliser la méthode POST**.

Nous proposons deux fonctionnalités distinctes dans cette API :

- **L'Horodatage d'un Hash** (une empreinte numérique)
- **L'Horodatage de PDF**

3.3. Accès au service

Le service est disponible à l'url suivante : **https://timestamp.dhimyotis.com/api/v1/**

Pour vous connecter au service, **vous devez utiliser un compte utilisateur** (credentiel - cf partie 3.1).

En effet, votre compte admin ne pourra pas être utilisé pour un accès au service, il est dédié à l'administration de votre compte.

L'authentification de l'appelant est de type ***Basic***.
L'identifiant et le mot de passe (du compte) sont fournis dans le header de la requête http.

3.4. Horodatage d'une empreinte numérique (Hash)

En fonction de vos besoins, vous pouvez horodater un hash selon deux méthodes :

1- Utilisation du protocole RFC 3161

Cette méthode nécessite l'envoi d'une requête d'horodatage de type : ***application/timestamp-query***

Pour plus d'information sur le protocole **RFC 3161** : **https://www.ietf.org/rfc/rfc3161.txt**

La requête retourne une réponse de type ***application/timestamp-reply***

2- Utilisation d'un envoi de formulaire

Cette méthode nécessite l'envoi d'une requête d'horodatage de type :

***application/x-www-form-urlencoded*.**

La requête retourne en réponse **un jeton d'horodatage**.

Les paramètres de la requête sont :

Paramètre	Description	Type	Valeur
certReq	le paramètre indique si le jeton d'horodatage contient ou non le certificat de l'UH (Unité d'horodatage).	boolean	True ou false
hashAlgorithm	libellé de l'algorithme utilisé pour calculer l'empreinte (hash) du message	*string*	*SHA256*, *SHA384* ou *SHA512*
hashedMessage	valeur de l'empreinte du message (exprimée en hexadécimal)	string	empreinte du message **Regex : ^([0-9A-F]{2})*$**

Voici un exemple d'appel avec curl pour générer un jeton d'horodatage

```
https://timestamp.dhimyotis.com/api/v1/

curl        --user "username:password"   \
--data "certReq=true"                      \
--data "hashAlgorithm=SHA256"              \
--data "hashedMessage=1A2B…..FF"           \
--output out.tsr                           \
```

3- Vérification d'un jeton généré par Certigna

La librairie OpenSSL fournit une commande 'ts' (pour time stamp). La commande' ts' est une application client et serveur de base de l'autorité d'horodatage (TSA) telle que spécifiée dans la RFC 3161.

La commande 'ts' a trois fonctions principales : créer une requête d'horodatage basée sur un fichier de données, créer une réponse d'horodatage basée sur une requête, vérifier si une réponse correspond à une requête particulière ou à un fichier de données. Nous vous renvoyons sur la documentation en ligne d'OpenSSL pour en découvrir plus sur les différentes fonctions et options de la commande 'ts'.

Les exemples 1 et 2 vous indiquent en particulier comment vérifier un jeton généré par Certigna.

Exemple 1 : commande pour vérifier un jeton généré avec le protocole RFC 3161

openssl ts -verify -CAfile *trusted_certs.pem* -data *file_to_hash* -in *response.tsr*

Exemple 2 : commande pour vérifier un jeton généré avec l'envoi de formulaire

openssl ts -verify -CAfile *trusted_certs.pem* -data *file_to_hash* -in *response.tsr* -token_in

Exemple 3 : commande pour visualiser le contenu d'un jeton généré avec l'envoi de formulaire

openssl ts -reply -in *response.tsr* -text -token_in

Réponse :

```
TST info:
Version: 1
Policy OID: 1.2.250.1.177.2.9.1.1
Hash Algorithm: sha256
Message data:
    0000 - 2d 5a 74 ba c0 56 c9 01-a6 8e 32 65 93 33 6e 21   -Zt..V....2e.3n!
    0010 - fe f6 2b aa 1f 81 f8 8c-d1 21 93 21 00 9d d9 0c   ..+.....!.!....
Serial number: 0x01ABCD8870C449A1B165D5C9569D0B1F
Time stamp: Mar  7 16:42:29 2023 GMT
Accuracy: 0x01 seconds, unspecified millis, unspecified micros
Ordering: no
Nonce: 0x66356264636135632D343131662D343064652D613564652D623134316431373530383938
TSA: DirName:/C=FR/O=DHIMYOTIS/organizationIdentifier=NTRFR-48146308100036/OU=0002
48146308100036/CN=DHIMYOTIS - TSU15/serialNumber=T249921842
Extensions:
qcStatements:
    0.0.....^..
```

3.5. Horodatage d'un document PDF

Afin d'horodater un document PDF il est nécessaire d'envoyer un formulaire contenant le fichier à horodater.

Il convient ici de transmettre une requête de **type** ***multipart/form-data***

La requête retourne en réponse **le fichier PDF horodaté**

Les paramètres de la requête sont :

Paramètre	Description	Type	Valeur
file	Contenu du fichier PDF à horodater	Selon paramètre *Content-Type*	Selon paramètre *Content-Transfer-Encoding*

Voici un exemple d'appel avec curl pour horodater un PDF

```
https://timestamp.dhimyotis.com/api/v1/

curl                --user "username:password"   \
--form file=@in.pdf                              \
--output out.pdf                                 \
```

3.6. Principaux codes retour

Les principaux codes retour de l'API sont :

200 => **Succès**. La réponse est de type ***application/timestamp-reply*** ou ***application/pdf*** dans le cas du PDF horodaté.

En cas d'erreur

Code erreur	Description
400	Requête incorrecte ou non supportée
401	Echec de l'authentification (identifiant inconnu ou mot de passe incorrect)
402	Crédits épuisés (il faut acquérir de nouveaux crédits – hors abonnement)
403	Interdit (accès à une ressource non autorisée)
404	Ressource non trouvée
405	Méthode non autorisée
415	Format de requête non supporté pour une méthode et une ressource données.
501	Erreur interne du serveur

4. EXEMPLE D'USAGES DU SERVICE D'HORODATAGE

4.1. Horodater un document PDF avec Adobe Acrobat Reader

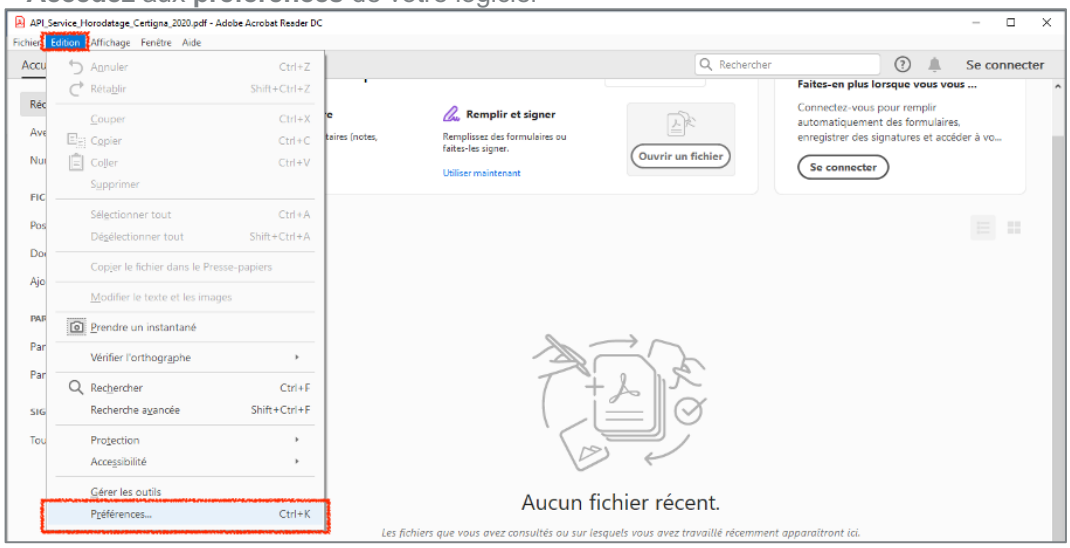
Grâce au service **CERTIGNA Horodatage** vous **pouvez simplement** en quelques clics **horodater un document PDF**.

Comment procéder ?

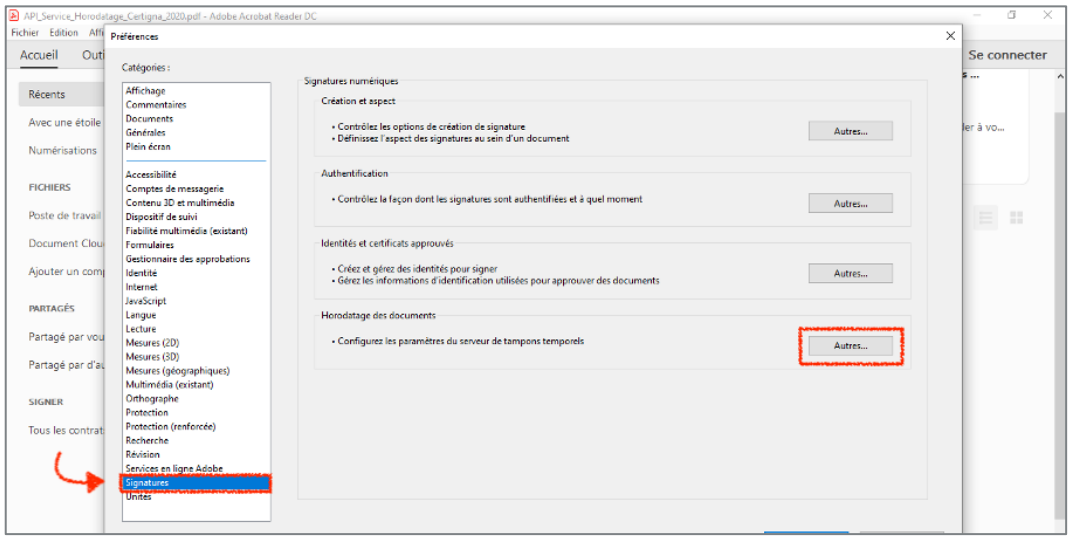
Vous devez configurer votre logiciel Adobe Acrobat. Cette manipulation est à réaliser une seule fois

4.1.1. Configuration Windows

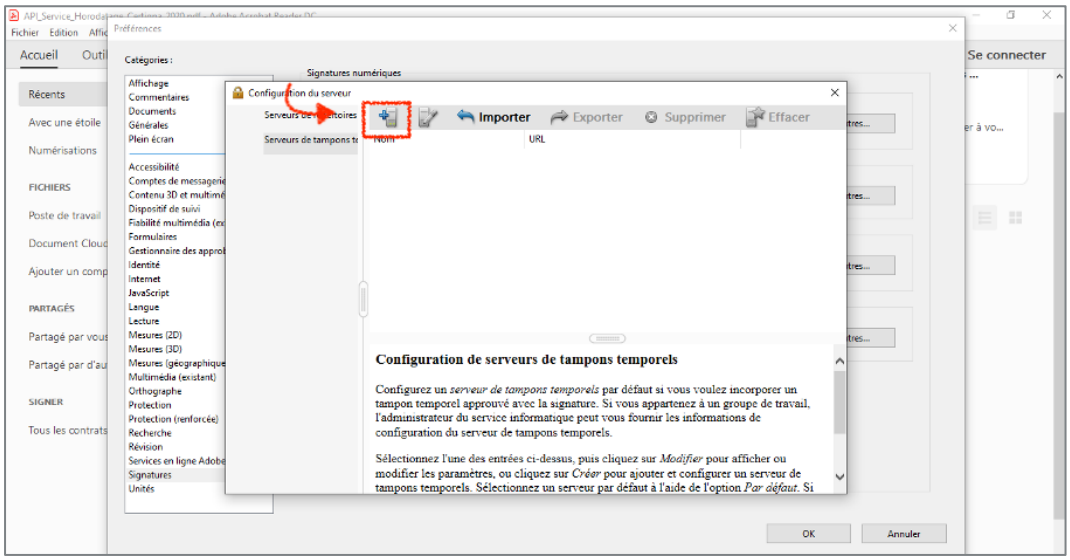
1- **Accédez** aux **préférences** de votre logiciel



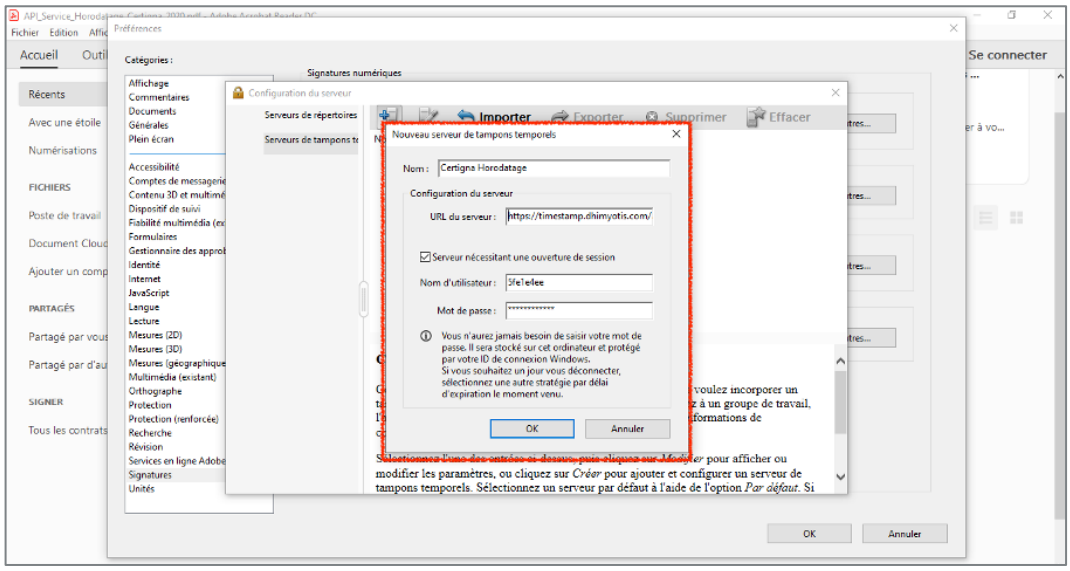
2- **Sélectionnez** la catégorie « signatures » et configurez les paramètres du serveur de tampons temporels.



3- **Ajoutez** un nouveau serveur de tampon temporel



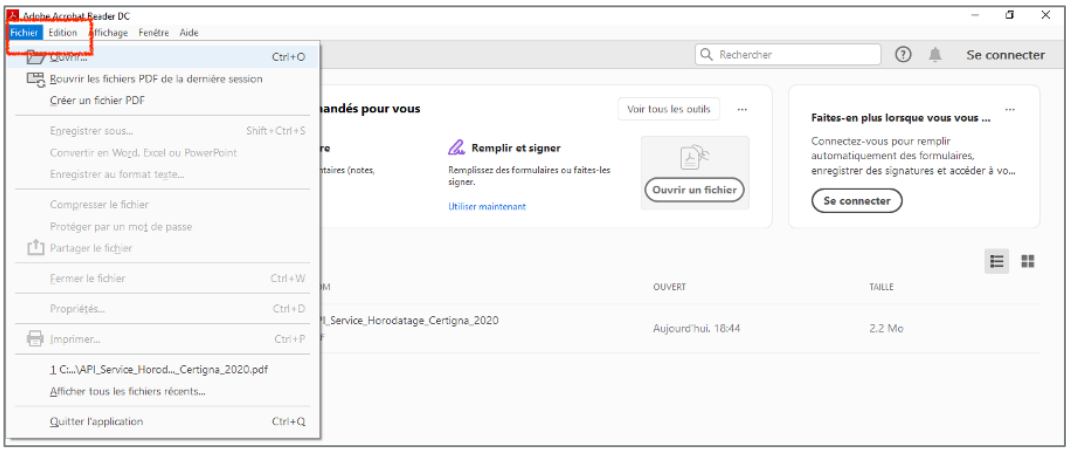
4- **Vous devez saisir ici 3 informations :**
L'url permettant d'accéder au service d'horodatage ;
L'identifiant du compte crédentiel précédemment créé
Le mot de passe associé à ce crédentiel.



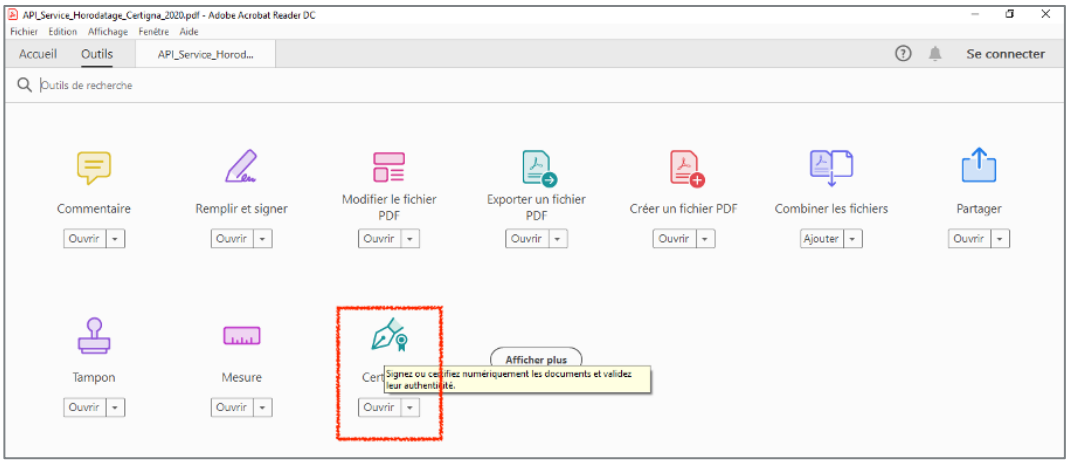
Vous pouvez maintenant horodater le PDF de votre choix !

CERTIGNA
Horodatage

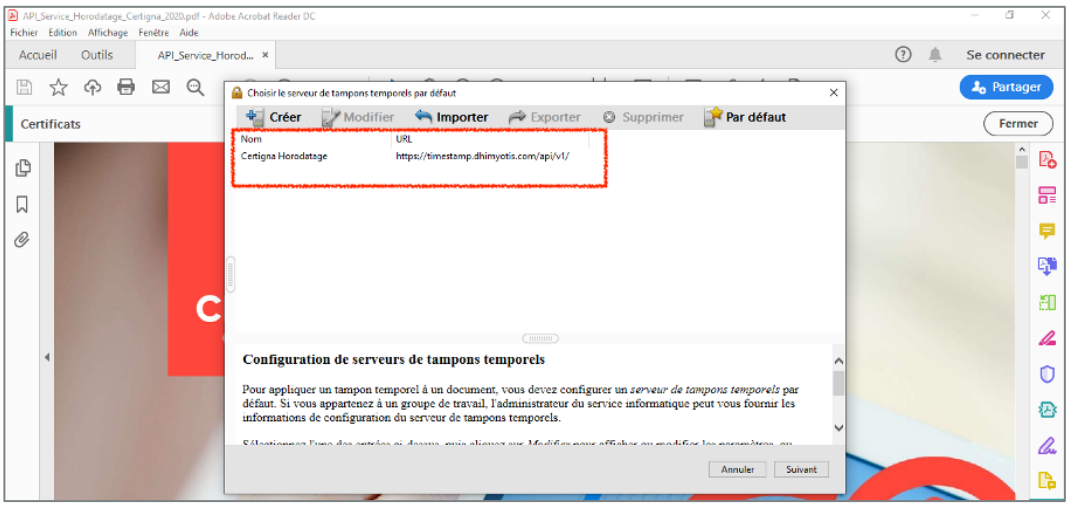
5- **Sélectionnez** le fichier à horodater



6- Dans le menu Outils d'Adobe Acrobat, **Sélectionnez « certificats »**

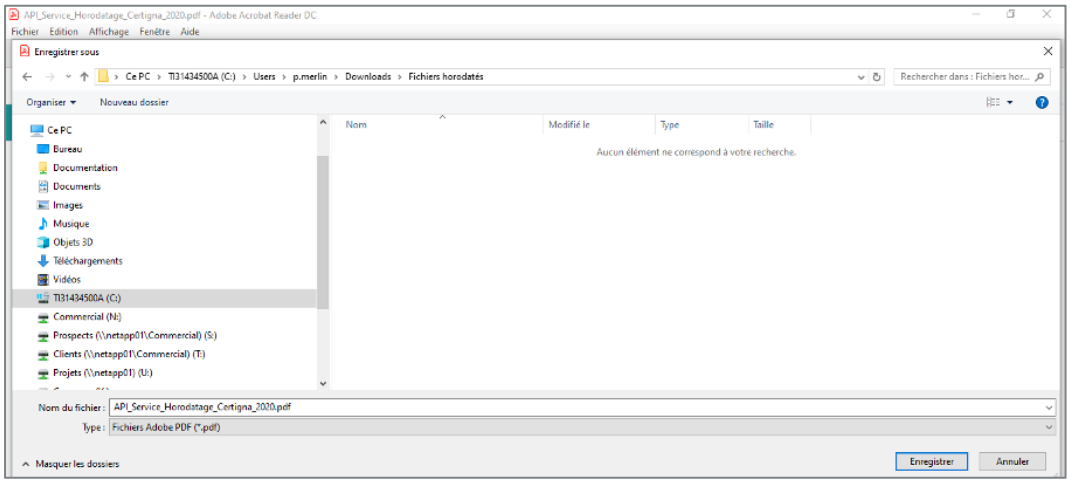


7- **Sélectionnez** le **serveur de tampon temporel CERTIGNA**

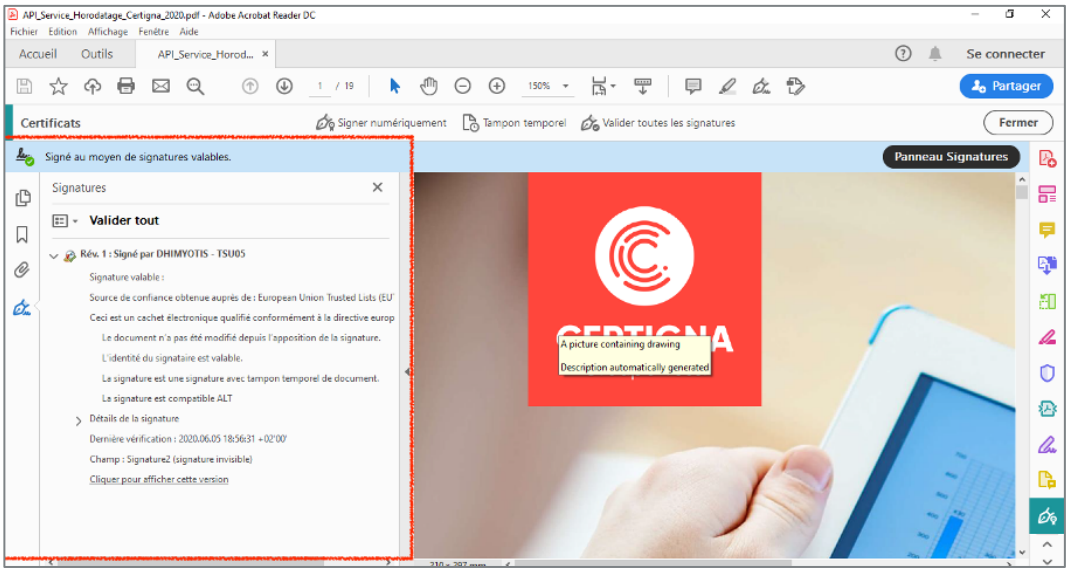


CERTIGNA
Horodatage

8- Enregistrez le nouveau fichier sous un autre nom

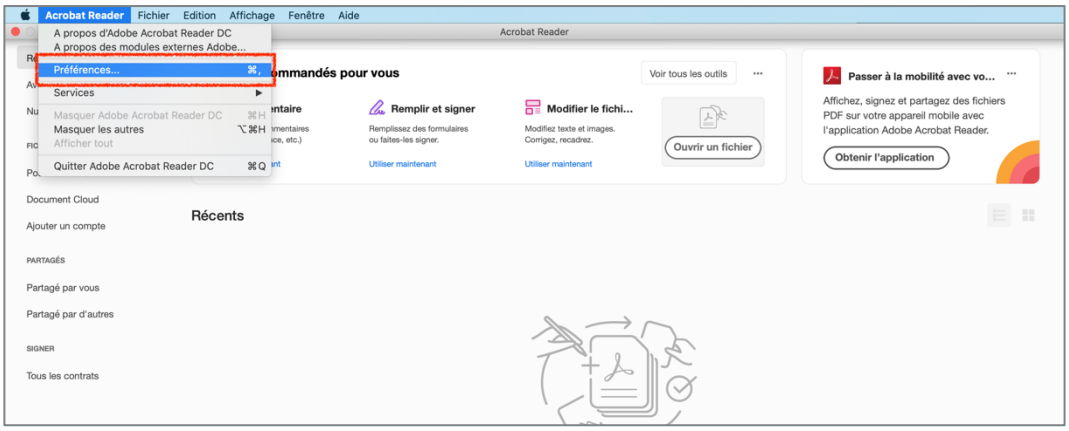


Félicitations ! Votre PDF est Horodaté !

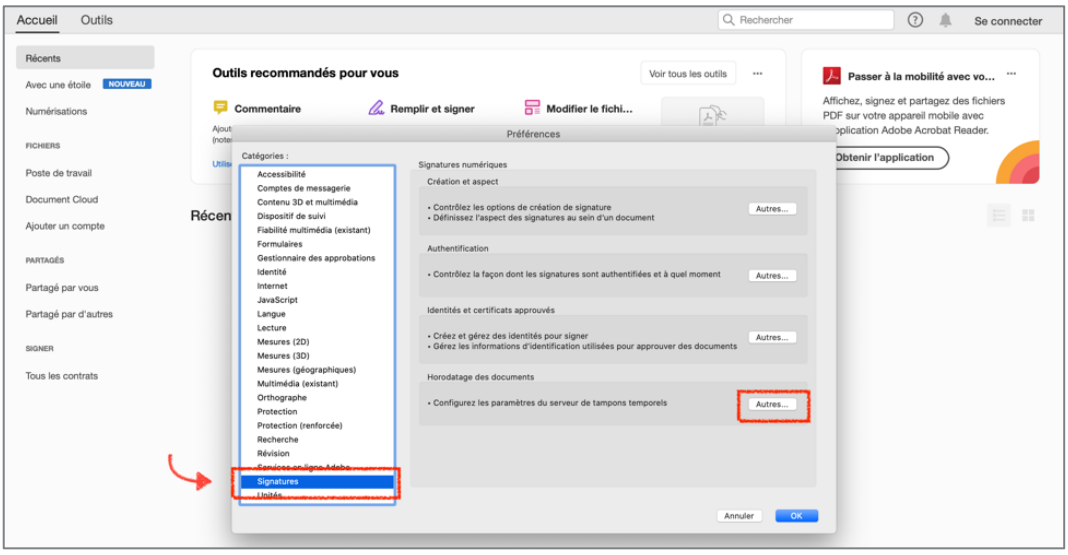


4.1.2. Configuration Mac

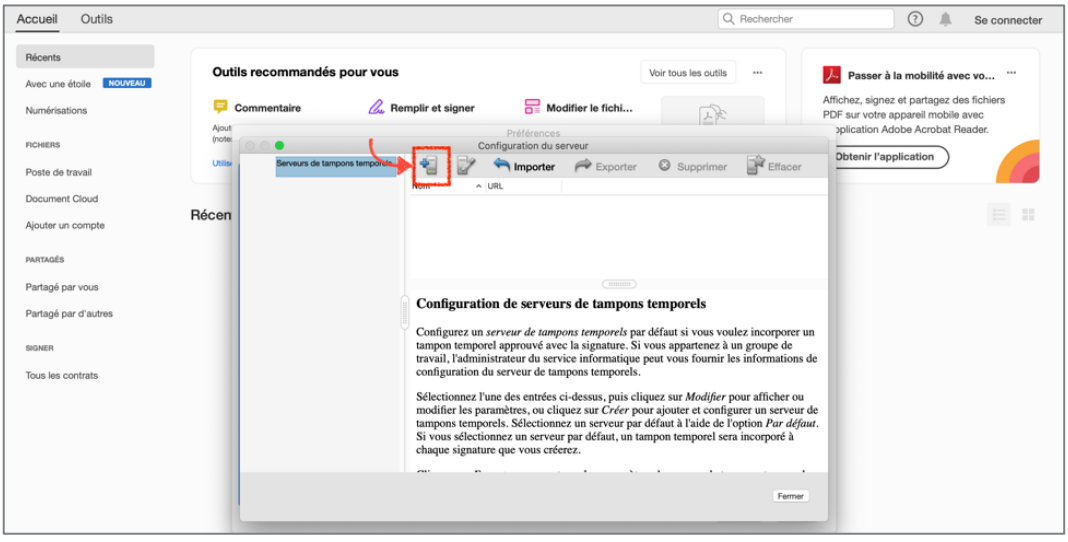
1- **Accédez** aux **préférences** de votre logiciel



2- **Sélectionnez** la catégorie « signatures » et configurez les paramètres du serveur de tampons temporels.

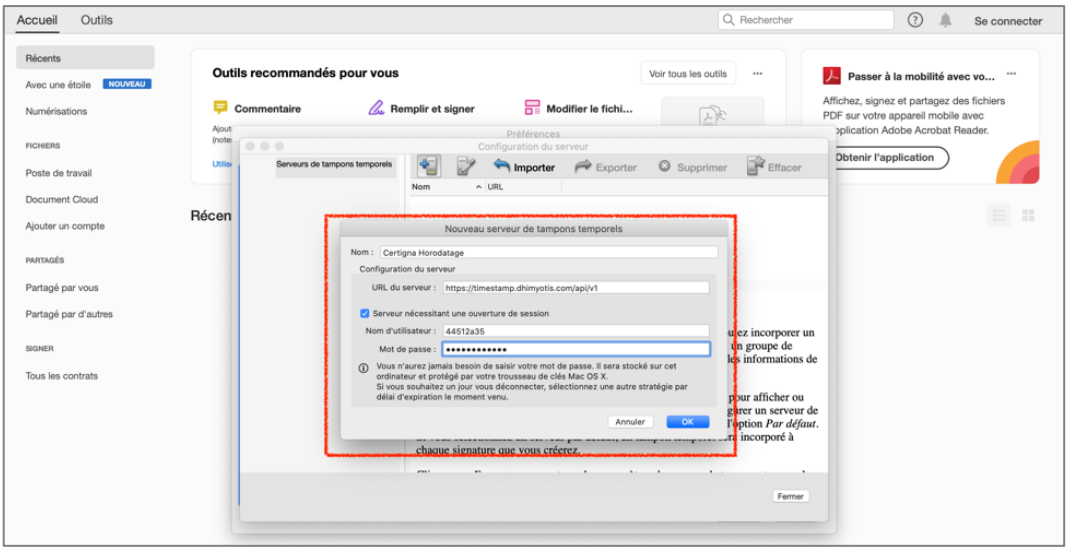


3- **Ajoutez un nouveau serveur de tampon temporel**



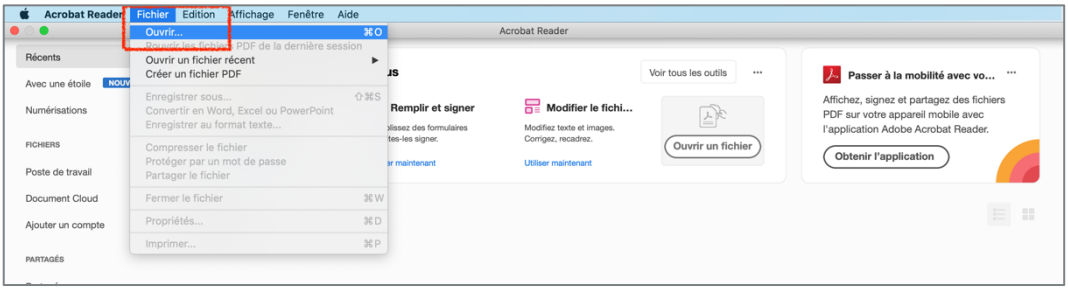
4- Vous devez saisir ici 3 informations :

- **L'url** permettant d'accéder au service d'horodatage ;
- **L'identifiant** du compte crédentiel précédemment créé
- **Le mot de passe** associé à ce crédentiel.

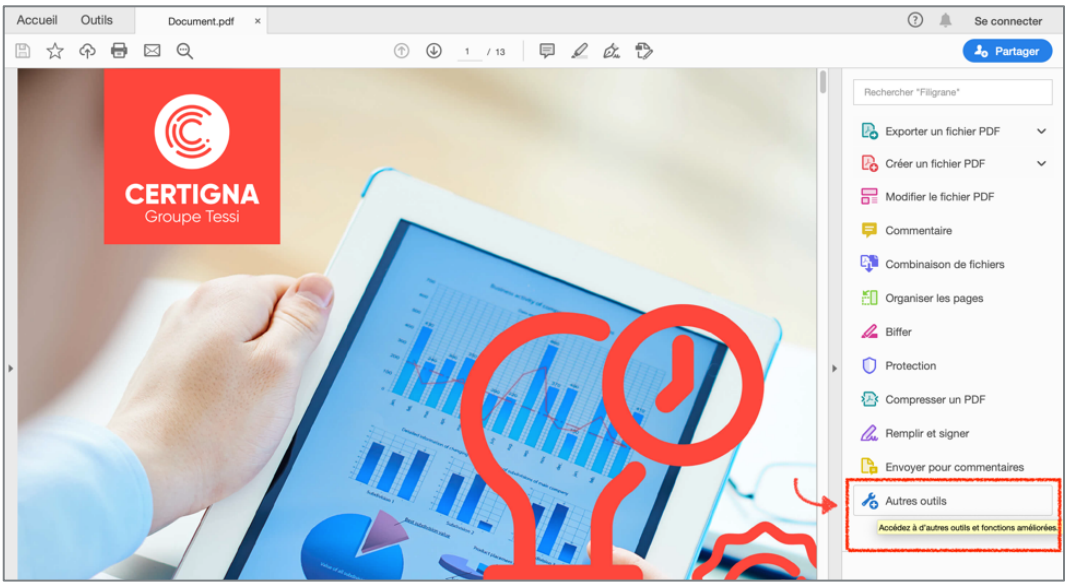


Vous pouvez maintenant horodater le PDF de votre choix !

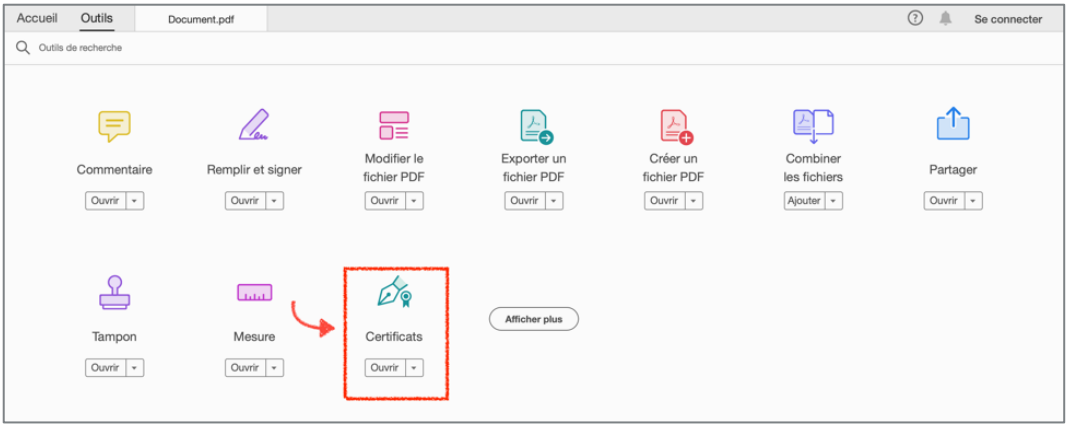
5- Sélectionnez le fichier à horodater



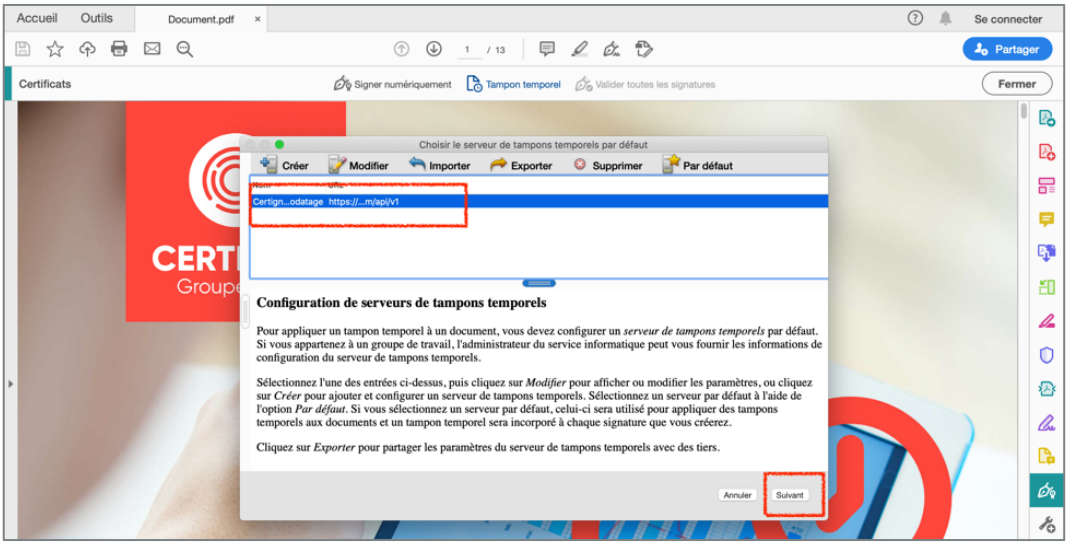
6- Cliquez sur le menu **« Autres outils »**



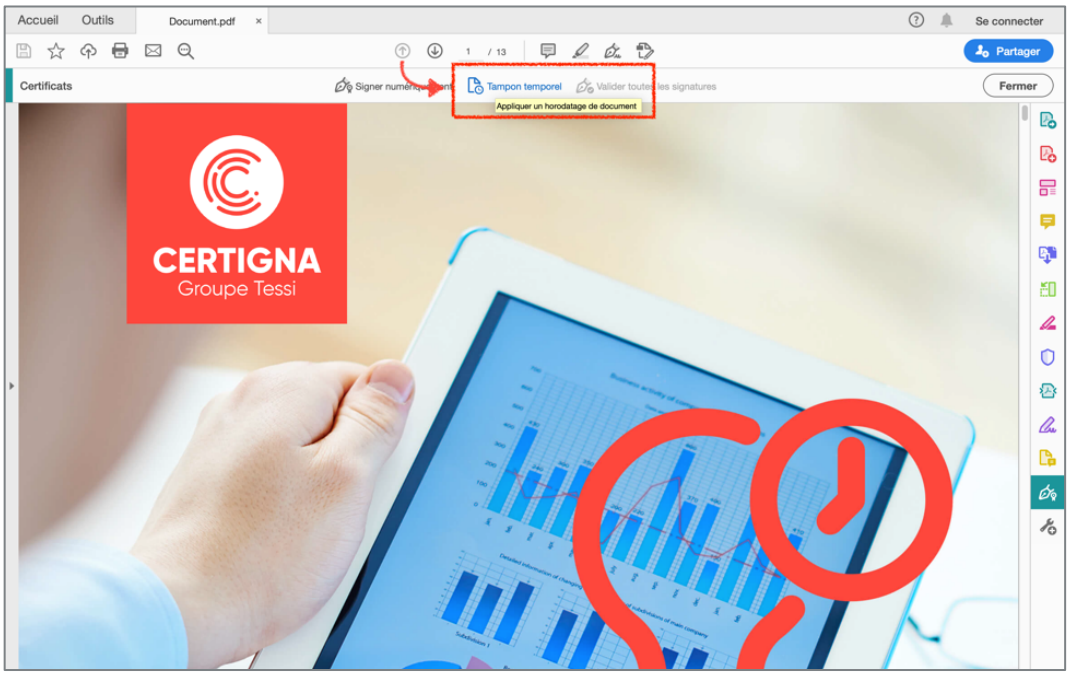
7- **Sélectionnez** l'item « **Certificats** »



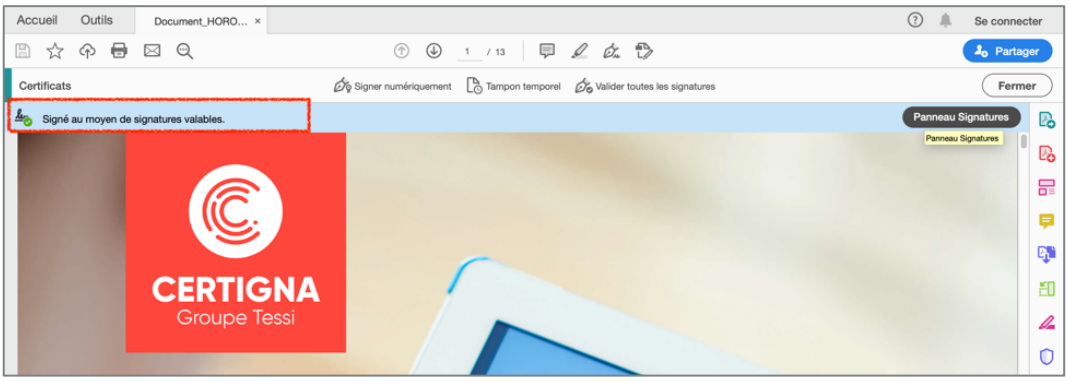
8- **Sélectionnez** le **serveur de tampon temporel CERTIGNA**

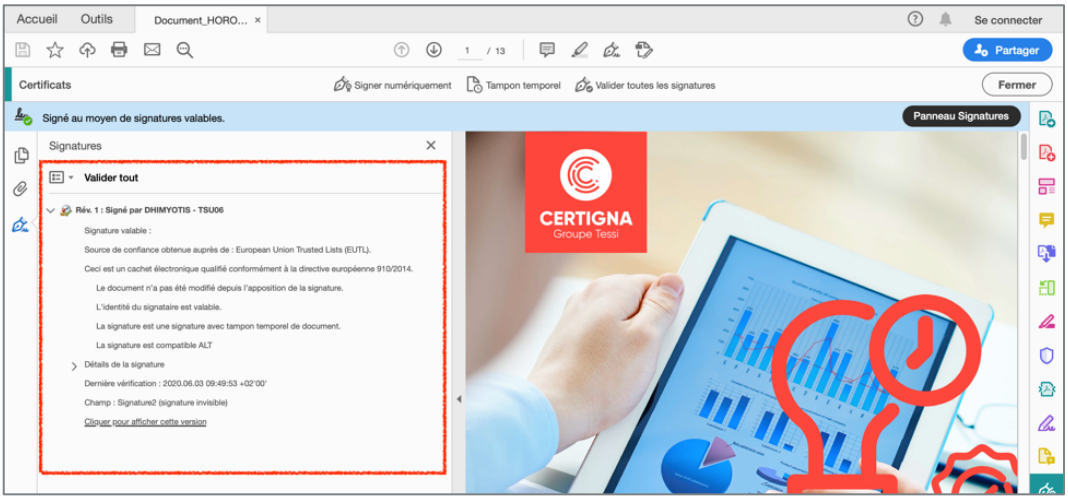


9- **Horodatez votre PDF** en sélectionnant **« Tampon Temporel »**



Félicitations ! Votre PDF est Horodaté !





5. INFORMATIONS COMPLEMENTAIRES

5.1. Lexique

Abréviation	Correspondance
PH	**P**olitique d'**H**orodatage
PSHE	**P**restataire de **S**ervice d'**H**orodatage **E**lectronique
TSA	Autorité d'Horodatage (**T**ime **S**tamping **A**uthority)
UH	**U**nité d'**H**orodatage
UTC	Temps Universel Coordonné (**U**niversal **T**ime **C**oordinated)

5.2. Définitions

Terme	Définition
Autorité d'Horodatage	Autorité en charge du service d'horodatage en conformité avec la Politique d'Horodatage et en s'appuyant sur une ou plusieurs unités d'horodatage
Jeton d'horodatage	Donnée signée électroniquement qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.
Empreinte Numérique	Ensemble de bits caractéristique d'un document numérique. L'empreinte est obtenue par une fonction de hachage. Toute modification du document numérique entraînera une empreinte différente qui révélera la modification par comparaison avec la première empreinte.
Fonction de Hachage	Fonction qui fait subir une succession de traitements à une donnée quelconque fournie en entrée pour en produire une empreinte numérique servant à identifier la donnée initiale.
Module d'Horodatage	Produit de sécurité comportant une ressource cryptographique et qui est dédié à la mise en œuvre des fonctions d'horodatage, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des contremarques de temps.
Politique d'Horodatage	Document public décrivant les règles définissant les exigences auxquelles un PSHE se conforme.
Système de la TSA	Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir le service d'horodatage.

CERTIGNA
Groupe Tessi

horodatage.certigna.com