Politique d'horodatage et Déclaration des pratiques d'horodatage (PH/DPH)

De l'Autorité d'Horodatage

Adria DigiTrust

Objet :	**Politique d'horodatage et Déclaration des pratiques d'horodatage (PH/DPH) De l'Autorité d'Horodatage « Adria DigiTrust »**
OID	1.2.504.1.2.2.1.5

Diffusion	**Externe**	**Interne**
	- **Personnes physique et morales Utilisateurs du service d'horodatage électronique de la plateforme Adria DigiTrust.** - **Applications Métiers faisant recours à la plateforme Adria DigiTrust pour le service d'horodatage électronique**	- **Personnel Adria DigiTrust**

Date	**Version**	**Rédacteur**	**Evolutions**
15/11/2024	**1.0**	**Adria Digitrust**	**Création du document**

Date	**Version**	**Validation**
15/11/2024	**1.0**	**Rachid BEKKAR/DG**

Sommaire

1. Introduction

Pour assurer la sécurité des échanges de données au format numérique, entre les entreprises et leurs clients, ainsi qu'entre l'administration et les usagers, Adria DigiTrust s'est dotée d'une infrastructure pour l'horodatage électronique.

En effet, Adria DigiTrust est un Prestataire de Services de Confiance Numérique (PSCo) proposant un service d'horodatage électronique selon la loi n° 43-20 relative aux services de confiance pour les transactions électroniques

Le présent document vise à être conforme aux référentiels suivants :

- Référentiels de la DGSSI d'exigences relatifs aux services de confiance qualifiés et aux prestataires fournissant ces services :
  - *Ref_Serv_Conf_NonQual* Exigences de conformité des prestataires fournissant un service d'horodatage électronique simple
  - *[Ref_PSCo_AG]* Exigences générales de conformité des prestataires fournissant des services de confiance autre que qualifiés
- Référentiels ETSI EN 319 421 et EN 319 401 ETSI EN 319-422 ;
- Normes IETF RFC 3161 et RFC 5816 ;

Cette conformité permet à Adria DigiTrust de viser l'agrément de service d'horodatage électronique par la DGSSI comme service d'horodatage électronique qualifié au sens de la loi n° 43-20.

Le service d'Horodatage électronique d'Adria DigiTrust peut être utilisé par ses clients :

- Inclus dans l'offre de signature électronique d'Adria DigiTrust, pour fournir des dates fiables, donnant ainsi une bonne assurance sur la qualité des dates associées aux transactions de signature électronique ;
- Directement, en tant que service à part entière.

Le Service d'Horodatage d'Adria DigiTrust est utilisé également pour assurer les opérations d'archivage des transactions réalisées sur les plateformes de confiance numérique d'Adria DigiTrust, ainsi que les applications métier utilisatrices de ses clients.

1.1.Présentation générale

Le présent document fait partie d'un ensemble documentaire des politiques de certification et des déclarations des pratiques de certification du prestataire de services de confiance numérique Adria DigiTrust, et concerne la politique d'horodatage et Déclaration des pratiques d'horodatage de l'Autorité déléguée d'horodatage (AH), et spécifie l'ensemble des engagements pris par la TSA Adria DigiTrust et spécifie l'ensemble des politiques et pratiques appropriées à la fourniture du service d'horodatage.

L'objectif de ce document PH/DPH est de définir les engagements pris par Adria DigiTrust, en tant que TSA, pour la délivrance et la gestion de contremarques de temps, de décrire les procédures techniques et organisationnelles mises en œuvre pour le respect de ces engagements, et enfin de définir les obligations des autres partenaires. En particulier, cette PH/DPH décrit les moyens mis en œuvre pour atteindre les objectifs de sécurité du service d'horodatage électronique, comme ceux de création des contremarques de temps et de maintien de l'exactitude des horloges.

Cette PH/DPH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge de l'utilisateur du service d'horodatage.

Les clauses principales de cette PH/DPH sont synthétisées dans les Conditions Générales d'Utilisation du service d'horodatage électronique (CGU), que les clients et utilisateurs doivent s'engager à respecter.

1.2.Acronymes et Terminologie

1.2.1.Acronymes

Les acronymes utilisés dans la présente PH/DPH sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
TSA	Time-Stamping Authority (Autorité d'Horodatage)
TSU	Time-Stamping Unit (Unité d'Horodatage)
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
PKI	Public Key Infrastructure

PH	Politique d'Horodatage
DPH	Déclaration des Pratiques d'horodatage
PGSSI	Politique générale de sécurité des systèmes d'information
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés
LAR	Liste des certificats d'Autorités Révoqués
LCR	Liste des Certificats Révoqués
OID	Object Identifier (identifiant d'objet)
PP	Profil de Protection
PSCo	Prestataire de service de confiance au sens de la Loi n° 43-20
UTC	Coordinated Universal Time
RFC	Request For Comments
http	Hypertext transfer protocol
URL	Uniform Resource Locator
SHA	Secure Hash Algorithm
CGU	Conditions Générales d'utilisation les CGUs sont publiées dans le site web de Adria DigiTrust

1.2.2.Terminologie

- **Abonné :** Appelé aussi **Client.** Entité ayant contractualisé avec Adria DigiTrust pour pouvoir demander des contremarques de temps émises par son autorité d'horodatage (TSA) pour faire horodater des données. Pour ce faire, Le client a accepté les conditions d'utilisation des services d'Adria DigiTrust.

- **Utilisateur final :** Abonné ou utilisateur de contremarques de temps émises par l'autorité d'horodatage (TSA).
- **Autorité Administrative (AA)** : Autorité responsable d'une PKI et/ou d'une TSA et possédant un pouvoir décisionnaire au sein de celles-ci.
- **Autorité de Certification (AC)** : Au sein d'un PSCo, une entité a en charge l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification.
- **Autorité d'Horodatage (TSA)** – Entité fournissant un service d'horodatage électronique sur la base d'une ou plusieurs TSU, conformément à une politique d'horodatage.
- **Unité d'Horodatage (TSU)** : désigne une Unité d'horodatage conformément à l'ETSI 319 421 à savoir un ensemble de matériels (incluant une horloge interne) et de logiciels gérés comme une seule unité assurant la création de jetons d'horodatage et qui est caractérisé par :
  - Une clé unique de signature de jetons d'horodatage ;
  - Un identifiant accordé par une Autorité de Certification (certificat obtenu auprès de l'AC).
- **Contremarque de temps** : Appelée aussi **Jeton d'horodatage**. Donnée signée 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.
- **Coordinated Universal Time (UTC)** : Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].
- **UTC(k)** : Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde. (Rec. ITU-R TF.536-1 [TF.536-1]).
  NB : Une liste des laboratoires UTC(k) est indiquée dans la section 1 de la Circulaire T publiée par le BIPM et est disponible sur le site web du BIPM (www.bipm.org).
- **Horodatage** : Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.
- **Politique d'horodatage (PH)** : Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une TSA se conforme dans la mise en place et la fourniture de ses prestations et indiquant les exigences de sécurité satisfaites. Une PH identifie également les obligations et exigences portant sur les autres intervenants, notamment les Abonnés et les Utilisateurs de contremarques de temps. La PH identifie aussi les pratiques (organisation, procédures opérationnelles, moyens techniques et

humains) que la TSA applique dans le cadre de la fourniture de ses services d'horodatage pour respecter les exigences qui lui incombe.

- **Déclaration des pratiques d'horodatage (DPH)** : identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que la TSA applique dans le cadre de la fourniture du service d'horodatage et qu'elle s'est engagée à respecter dans la PH/DPH.
- **Service d'horodatage** : Ensemble des prestations nécessaires à la génération et à la gestion de Contremarques de temps.
- **Système d'horodatage** : Ensemble des Unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir le Services d'horodatage.
- **Certificat électronique :** Fichier liant une bi-clé à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans un certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre un identifiant de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une période donnée précisée dans celui-ci.
- **Certificat Cachet Serveur :** Il s'agit d'un certificat de serveur de signature pour les personnes morales. Il permet à des applications Métier de signer d'importants volumes de documents en simultané pour garantir leur intégrité et leur authenticité.
- **Infrastructure de gestion de clés (IGC ou PKI)** : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une PKI peut être composée d'une autorité de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, d'une entité de séquestration des clés, etc.
- **Modules cryptographiques (HSM)** : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle HSM évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.
- **Profil de protection (PP)** : Document public qui définit, pour une catégorie de produits, un ensemble d'exigences et d'objectifs de sécurité, indépendants de leur technologie et de leur implémentation, qui satisfont les besoins de sécurité communs à un groupe d'utilisateurs.
- **Liste des certificats révoqués (CRL)** : Liste des numéros de certificats émis par une AC qui doivent être considérées comme non valides bien de n'ayant pas encore atteint

leur fin de validité. La liste CRL ne contient pas les numéros de certificats révoqués au-delà de la fin de leur période de validité.

- **Liste des certificats d'AC révoqués (LAR)** : Liste des certificats révoqués contenant seulement des numéros de série de certificats d'AC.
- **Applications métier utilisatrices** : Services applicatifs en ligne liées par voie contractuelle avec la plateforme Adria DigiTrust pour exploitation des contremarques de temps émises par l'Autorité d'hrodatage (TSA) pour des besoins de signature.
- **Service de signature :** Service mis à disposition par la plateforme Adria DigiTrust et permettant aux porteurs de certificats électroniques de signer électroniquement. L'utilisation par le porteur de la Clé privée associée au Certificat électronique se fait moyennant un code secret qui est communiqué.
- **Transaction de signature :** Opération identifié par un ID (id_Transaction) gérée au niveau du Service de signature, pendant laquelle le porteur de certificat électronique communique le secret de la clé privé de son certificat pour signer électroniquement les documents liés à cette transaction.

1.3.Identification de la PH/DPH (OID)

La présente PH/DPH est enregistré par un numéro d'identifiant d'objet (OID) qui est : 1.2.504.1.2.2.1.5
Cet identifiant est également inclus dans les conditions générales d'Utilisation (CGU) à destination des clients

1.4.Gestion de la PH/DPH

La PH/DPH n'est accessible, pour création ou modification, qu'au seul personnel autorisé par l'AA de Adria Digitrust, et ce à travers des contrôles d'accès appropriés.

La mise à jour de la PH/DPH est un processus impliquant toutes les parties prenantes et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur le lieu de publication sur internet https://pki.adria-digitrust.com/cp.html. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du point de contact.

La nouvelle version de la PH/DPH avec son nouveau OID entre en vigueur dès qu'elle est publiée sur le lieu de publication cité précédemment.

1.5.Publication de la PH/DPH

La PH/DPH est diffusée à l'ensemble des parties concernées par le service d'horodatage afin de permettre à chaque partie de prendre connaissance des principes que la PH/DPH s'engage à respecter dans le cadre de la délivrance du service.

La PH/DPH est mise à disposition de l'ensemble des parties prenantes via le lien de publication sur Internet suivant : https://pki.adria-digitrust.com

Le site de publication comporte également :

- Les Conditions Générales d'Utilisation (CGU) à destination des utilisateurs ;
- Les certificats des unités d'horodatage (TSU) et leur chaîne de certification ;
- La liste des certificats révoqués (LAR / LCR) ;
- Les attestations de conformité des services Adria DigiTrust obtenues

1.6.Délais de publication

Les informations sont publiées dès leur approbation par l'AA, avant l'ouverture du service ou de l'évolution impliquant la modification des informations publiées. De cette sorte, les informations publiées sont toujours à jour par rapport au service disponible.

1.7.Point de contact

Toute demande d'information concernant la présente PH/DPH peut se faire auprès du :

- Nom et Prénom : Contact Adria DigiTrust
- Email : contact@adria-digitrust.com

Adria Digitrust peut également être contacté au travers du formulaire de contact disponible sur son site internet : https://adria-digitrust.com

2. Dispositions Générales

2.1.Obligations de l'Autorité d'Horodatage (TSA)

La TSA d'Adria Digitrust a les obligations suivantes :

- Génère et signe les contremarques de temps conformément à la présente PH et aux CGU associées.
- Garantir la conformité pour tout acteur intervenant dans la gestion des contremarques de temps par rapport aux exigences et aux procédures prescrites dans cette PH/DPH.
- Remplir tous ses engagements tels que stipulés dans ses Conditions Générales d'Utilisation (CGU).

- Mettre à la disposition des abonnés et utilisateurs du service d'horodatage l'ensemble des informations nécessaires à la vérification des contremarques de temps.
- Respecter les conditions de disponibilité du service d'horodatage convenues contractuellement avec les abonnés.
- Maintenir une information sur la compromission des bi-clés des certificats des unités TSU..

2.2.Obligations de l'abonné

Un abonné (appelé aussi client) est une personne morale ou personne physique ou application métier ayant besoin de faire horodater des données par la TSA d'Adria DigiTrust et qui a accepté les conditions d'utilisation de ce service d'horodatage.

L'abonné a l'obligation d'émettre une requête utilisant un algorithme de hashage supporté par la TSA d'Adria DigiTrust (SHA256, SHA384 ou SHA512).

L'abonné doit, au moment de l'obtention d'une contremarque de temps, vérifier que le certificat de l'unité d'horodatage TSU n'est pas révoqué.

L'abonné doit respecter ses engagements énoncés dans les CGU.

2.3.Obligations de l'utilisateur

Pour faire confiance à une contremarque de temps, l'utilisateur devra :

- Comparer le hash des données horodatées avec le hash présent dans la contremarque de temps;
- Vérifier la signature d'une contremarque de temps à l'aide du certificat de l'unité d'horodatage TSU;
- Vérifier la validité du certificat d'horodatage. Cette vérification est réalisée en s'appuyant sur la chaîne de certification et la liste de certificats révoqués (LCR) émis par l'autorité de certification (AC).

2.4.Obligations de l'AC fournissant les certificats des unités d'horodatage TSU

Les certificats des unités TSU doivent être délivrés par l'AC «**Adria DigiTrust Corporate**» selon la Politique de Certification dont l'OID est 1.2.504.1.2.2.1.2.

En particulier, l'AC est responsable de la publication des certificats et des informations de révocation permettant de vérifier le certificat des unités d'horodatage TSU.

La chaîne de certification complète des certificats des unités d'horodatage TSU est la suivante :

- AC Racine : « **Adria DigiTrust Root CA** »
  - AC déléguée : « **Adria DigiTrust Corporate** »
    - Certificat TSU

2.5.Déclarations des pratiques d'horodatage

La TSA d'Adria DigiTrust garantit qu'elle possède la fiabilité nécessaire pour fournir le service d'horodatage. En particulier :

a) La TSA a effectué une analyse de risques afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.
b) La TSA dispose de procédures internes utilisées pour adresser toutes les exigences identifiées dans cette PH/DPH.
c) La PH/DPH identifie les obligations de toutes les organisations externes participant à la fourniture du service d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux unités TSU.
d) La TSA met à la disposition des abonnés et des utilisateurs de contremarques de temps les éléments publics de ses procédures opérationnelles dans sa PH/DPH, et, s'il y a lieu, toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la PH/DPH.
e) La TSA dispose d'une organisation adéquate pour la vérification de l'harmonie entre les procédures opérationnelles exposées dans la PH/DPH et les engagements pris dans la PH/DPH.
f) Le responsable opérationnel de la TSA garantit que les pratiques sont correctement mises en œuvre
g) La TSA définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la PH/DPH.
h) La TSA doit informer au préalable les abonnés pour tout changement qu'elle a l'intention de faire dans sa PH/DPH et, après l'approbation, immédiatement mettre à la disposition des abonnés et des utilisateurs de contremarques de temps la PH/DPH mise à jour.
i) Si la TSA a été évaluée comme conforme à la présente PH/DPH et si une modification envisagée à l'initiative de la TSA pouvait entraîner une non-conformité avec ladite PH/DPH, alors l'AA soumettra cette modification à l'organisme évaluateur indépendant pour avis.

2.6.Conditions générales d'Utilisation

Compte tenu de la complexité de lecture de la PH/DPH pour des utilisateurs non spécialistes du domaine, la TSA Adria DigiTrust fournit également des conditions générales d'utilisation (CGU) correspondant aux "*TSA Disclosure Statement*" de la norme ETSI 319 401.

Les CGU ne sont pas destinées à remplacer la présente PH/DPH, mais visent à permettre aux abonnés et utilisateurs non techniciens des contremarques de temps de comprendre facilement les informations essentielles qu'ils doivent connaître.
Les CGU intègrent, à minima, es informations suivantes :

- La PH/DPH applicable ;
- Les limites sur l'utilisation du service d'horodatage ;
- Les obligations de l'abonné ;
- Les obligations des utilisateurs des contremarques de temps ;
- La période pendant laquelle les journaux d'événements sont conservés ;
- Les limites de responsabilité ;
- Le système légal applicable ;
- Les procédures pour le règlement des plaintes et des conflits ;
- Le schéma d'évaluation de la conformité de cette PH/DPH ;
- Les coordonnées du point de contact de la TSA ;
- La période minimum, hors cas de révocation, durant laquelle les contremarques de temps seront vérifiables ;
- L'exactitude du temps dans les contremarques de temps par rapport au temps UTC ;
- Les dispositions permettant de valider la chaîne de certificat lié aux certificats des unités TSU ;
- Le nom du pays dans lequel l'Autorité d'horodatage est établie.

Les CGU du service d'horodatage sont mises à disposition des abonnés en annexe de leur contrat de service avec Adria Digitrut.

Les CGU du service d'horodatage sont mises à disposition des utilisateurs des contremarques de temps sur le site web d'Adria DigiTrust (cf. paragraphe 1.5)

2.7.Conformité avec les exigences légales

La TSA Adria DigiTrust garantit la conformité avec les exigences légales.

La TSA Adria DigiTrust a mis en place les mesures techniques et organisationnelles nécessaires pour garantir un niveau approprié de protection des données à caractère personnel, conformément à la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
Conformément à la législation et réglementation en vigueur, les informations personnelles remises par les abonnés à la TSA ne doivent pas être divulguées ni transférées à un tiers sauf

dans les cas suivants : consentement préalable de l'abonné, décision judiciaire ou autre exigence légale.

La divulgation des informations confidentielles n'est effectuée qu'aux autorités judiciaires ou administratives habilitées officiellement et exclusivement sur leur demande expresse en conformité avec la législation marocaine

3. Exigences opérationnelles

3.1.Gestion des requêtes de contremarques de temps

La TSA Adria DigiTrust émet une contremarque de temps en réponse à une demande contenant l'empreinte numérique de la donnée à horodater.
L'émission d'une contremarque de temps s'effectue en temps réel et ne dépasse pas quelques secondes, afin de préserver l'ergonomie des applications métier utilisant le service d'horodatage.

La TSA Adria DigiTrust reçoit des requêtes provenant des plateformes de confiance numérique d'Adria DgiTrust, ainsi que les applications métier utilisatrices de ses clients pour pour les besoins suivants :

- Horodatage des transactions de signature et de cachetage électronique
- Horodatage des éléments de traçabilité.
- L'horodatage des données et documents

La TSA Adria DigiTrust assure la conservation des contremarques de temps générées.

3.2.Fichier d'audit

Afin d'assurer la traçabilité de son service, La TSA Adria DigiTrust enregistre et conserve des traces dans des fichiers d'audit.
En particulier, sont conservées :

- L'ensemble des traces des demandes reçues par le service et des réponses retournées ;
- L'ensemble des traces pertinentes relatives à l'administration du service d'horodatage ;
- L'ensemble des traces pertinentes relatives au fonctionnement du service d'horodatage ;
- L'ensemble des traces pertinentes concernant les événements liés au cycle de vie des clés desUH et au cycle de vie des certificats associés ;

- L'ensemble des traces pertinentes concernant la synchronisation des horloges et serveurs de temps utilisés par l'unité TSU, y compris la perte de synchronisation ou le recalibrage/la resynchronisation des horloges.

La confidentialité des fichiers d'audit est assurée par une gestion des accès physiques, systèmes et réseaux appropriée.
L'intégrité et la protection contre la suppression sont assurées.

Les journaux du service d'horodatage sont conservés pendant un minimum de 7 ans, conformément aux exigences des référentiels de la DGSSI.

3.3.Gestion de la durée de vie de la clé privée

La TSA Adria DigiTrust garantit que les clés privées de signature des unités TSU ne sont pas utilisées au-delà de la fin de leur cycle de vie.

En particulier :

- Des procédures opérationnelles et techniques sont mises en place pour assurer le renouvellement de la paire de clés lorsque la fin de la période d'utilisation d'une clé privée d'une TSU est atteinte.
- La TSA Adria DigiTrust détruit la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

La durée de vie des clés privées de signature des UH est définie dans le chapitre 5 de la présente PH/DPH.

3.4.Synchronisation de l'horloge

La TSA Adria DigiTrust garantit une synchronisation de ses horloges d'horodatage avec UTC, avec la précision de l'ordre de la seconde. Cette précision est obtenue par la mise en œuvre de serveurs de temps synchronisés.
Ces derniers sont synchronisés sur,àminima, une source de temps référencée UTC(k).

Le mécanisme de synchronisation garantit les points suivants :

- Le calibrage de chaque horloge d'unité TSU est maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée ;
- Les horloges des unités TSU doivent être protégées contre les menaces relatives à leur environnement, pouvant entraîner une désynchronisation avec le temps UTC, en dehors de l'exactitude déclarée ;
- La TSA Adria DigiTrust garantit que, si son horloge interne ne respecte plus l'exactitude déclarée, alors l'anomalie est automatiquement détectée ;

- Si l'horloge d'une unité TSU est détectée comme étant en dehors de l'exactitude annoncée, les contremarques de temps ne sont plus générées ;
- La TSA Adria DigiTrust garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé. Le changement prend en compte le fait que le saut de seconde est effectué durant la dernière minute du jour où il est programmé. Un enregistrement du temps exact (selon l'exactitude déclarée) au moment de ce changement est effectué.

3.5.Exigences du contenu d'une contremarque de temps

Les contremarques de temps sont générées dans un environnement sûr et contiennent les informations suivantes :

- L'identifiant de l'unité TSU fourni à travers le DN du certificat de l'unité TSU ;
- L'identifiant (OID) de la PH/DPH appliquée ;
- Optionnellement, un identifiant unique de la contremarque ;
- Un temps, correspondant au moment de génération de la contremarque, synchronisé avec le temps de référence UTC(k) ;
- L'empreinte et l'algorithme d'empreinte de la donnée horodatée.

La contremarque de temps est signée par l'unité TSU avec sa clé privée, réservée à cet usage. Les contremarques de temps sont conformes à la norme IETF RFC 3161.

Le détail du format des contremarques de temps est donné dans le chapitre 6 de la présente PH/DPH.

3.6.Compromission de la TSA

La TSA Adria DigiTrust garantit, en cas d'événements affectant la sécurité des services d'horodatage (y compris la compromission de la clé privée de signature d'une unité TSU ou la perte de calibrage détectée, pouvant affecter les contremarques de temps émises)qu'une information appropriée soit mise à la disposition des abonnés et des utilisateurs de contremarques de temps.
Cette notification sera effectuée par une publication (voir paragraphe 1.5 de la présente PH/DPH).
Les dispositions suivantes sont prises en compte en cas de compromission :

- Le plan de secours (PCA/PRA) de la TSA Adria DigiTrust traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité TSU ou la perte de calibrage de l'horloge d'une unité TSU, qui pourrait affecter des contremarques de temps émises.
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité TSU, qui pourrait affecter des contremarques de temps émises, la TSA Adria DigiTrust met à la disposition de tous les utilisateurs de contremarques de temps

une description de la compromission qui est survenue. Cette notification se fait parune publication sur le site web indiqué au paragraphe 1.5 de la présente PH/DPH ;

- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité TSU, qui pourrait affecter des contremarques de temps émises, la TSA Adria DigiTrust prendra les mesures nécessaires pour que les contremarques de temps de cette unité TSU ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation. Ces dispositions prennent la forme d'une suspension de l'activité de l'unité TSU et en cas de compromission avérée, de son décommissionnement ;
- En cas d'un événement majeur dans le fonctionnement de la TSA Adria DigiTrust ou d'une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, la TSA Adria DigiTrust mettra à la disposition des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité du service d'horodatage ;
- La TSA Adria DigiTrust préviendra directement et sans délai l'autorité nationale DGSSI.

3.7.Fin d'activité de la TSA

L'AC déléguée Cachet Serveur n'autorise pas la délivrance d'un nouveau certificat Cachet Serveur suite au changement de la bi-clé.

En cas de cessation d'activité d'autorité d'horodatage, le PSCo Adria DigiTrust doit s'assurer que l'impact sur les utilisateurs soit réduit au maximum et doit assurer la maintenance continue des informations nécessaires pour vérifier la justesse des contremarques de temps.

À ce titre, le PSCo Adria DigiTrust a mis en œuvre un plan de cessation d'activité détaillant l'ensemble des actions à exécuter :

- Le PSCo Adria DigiTrust notifiera l'autorité nationale DGSSI de son plan cessation d'activité ;
- Le PSCo Adria DigiTrust rendra disponible sur son site web (voir paragraphe 1.5 de la présente PH/DPH) l'information concernant sa cessation d'activité ;
- Le PSCo Adria DigiTrust abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des contremarques de temps ;
- Le PSCo Adria DigiTrust maintiendra les obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable. En cas de cessation totale de ses activités, le PSCo Adria DigiTrust transférera à un organisme fiable ses éléments pour la même durée de conservation cible ;

- Le PSCo Adria DigiTrust maintiendra ou transférera à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
- Le PSCo Adria DigiTrust détruira de façon définitive les clés privées de telle façon que celles-ci ne puissent être recouvrées ;
- L'ensemble des certificats des unités TSU seront révoqués.

Le plan de cessation d'activité est tenu à jour. Il est revu annuellement et lors de tout changement majeur.

4. Exigences physiques et environnementales, procédurales et organisationnelles

La plateforme de la TSA Adria DigitTrust est hébergée dans le même site que la PKI du PSCo Adria DigiTrust et respecte les mêmes exigences.

4.1.Sécurité physique

4.1.1.Situation géographique

Le site d'exploitation de la TSA Adria DigitTrust respecte les règlements et normes de sécurité en vigueur et son installation tient compte des exigences du métier du prestataire de services de confiance numérique. Les résultats de l'analyse de risque ont été pris en compte par le prestataire d'hébergement de la plateforme Adria DigiTrust.

4.1.2.Accès physique

Les accès au site d'exploitation de la TSA Adria DigitTrust sont limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout événement de sécurité fait l'objet d'un enregistrement et d'un traitement.

4.1.3.Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de climatisation sont mis en œuvre par le prestataire d'hébergement de la plateforme Adria DigiTrust afin d'assurer la continuité des services délivrés.
Les matériels utilisés pour la réalisation des services sont exploités dans le respect des conditions définies par leurs fournisseurs et/ou constructeurs.

4.1.4.Vulnérabilité aux dégâts des eaux

Les systèmes du prestataire d'hébergement de la plateforme Adria DigiTrust sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

4.1.5.Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par le prestataire d'hébergement de la plateforme Adria DigiTrust permettent de respecter les exigences et les engagements pris par la TSA Adria DigitTrust dans la présente PH/DPH, en matière de disponibilité de ses fonctions.

4.1.6.Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) correspondant au service d'horodatage sont traités et conservés dans une enceinte sécurisée accessible aux seules personnes autorisées.

4.1.7.Mise hors service des supports

En fin de vie, Les supports seront soit détruits, soit réinitialisés en vue d'une réutilisation.

4.1.8.Sauvegardes hors site

Le PSCo Adria DigiTrust, en se basant sur les compétences de son prestataire d'hébergement, réalise des sauvegardes hors site permettant une reprise rapide des services de la TSA Adria DigitTrust après la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services.

4.2.Mesures de sécurité procédurales

4.2.1.Sécurité des systèmes

La TSA Adria DigitTrust garantit que les composants du système d'horodatage sont sûrs et correctement opérés, avec un risque minimal d'échec. En particulier :

- L'intégrité des composants du système d'horodatage et l'information sont protégés contre les virus, les logiciels malveillants et non autorisés.
- Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances soient réduits au minimum.
- Les supports employés dans le système d'horodatage sont manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence.

4.2.2.Manipulation et sécurité des supports

Tous les supports doivent être traités de manière sécurisée, conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles doivent être retirés de manière sécuritaire quand ils ne sont plus utiles.

4.2.3.Planification de système

Les charges doivent être surveillées, et des projections de charge futures doivent être réalisées pour garantir la disponibilité des capacités de traitement et de stockage adéquates.

4.2.4.Rapport d'incident et réponse

La TSA Adria DigitTrust agira d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents seront signalés dès que possible après leur survenance.

4.3.Mesures de sécurité vis-à-vis du personnel

4.3.1.Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de la TSA Adria DigitTrust est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Le personnel de la TSA Adria DigitTrust possède :

- La connaissance de la technologie de l'horodatage ;
- La connaissance de technologie de la signature numérique ;
- La connaissance des mécanismes de calibrage et de synchronisation des horloges des unités d'horodatage avec le temps UTC ;
- Pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité ;
- L'expérience avec la sécurité de l'information et l'évaluation des risques.

Toute personne intervenant dans les procédures de la TSA Adria DigitTrust est informée de ses responsabilités relatives au service d'horodatage et des procédures liées à la sécurité du système et au contrôle du personnel.

4.3.2.Rôles de confiance

Le personnel doit avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.
Les rôles de confiance de la TSA Adria DigitTrust sont classés en trois groupes :

- Les personnels d'exploitation, dont la responsabilité est le maintien des systèmes qui supportent la TSA en conditions opérationnelles de fonctionnement ;
- Les personnels d'administration, dont la responsabilité est l'administration technique des composantes de la TSA ;
- Les personnels de « sécurité », dont la responsabilité est de réaliser les opérations de vérification et de contrôle de la bonne application des mesures et de la cohérence de fonctionnement de la composante de la TSA.

4.3.3.Procédures de vérification des antécédents

L'AA de la TSA Adria DigitTrust met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification repose sur un contrôle des antécédents de la personne. Il est notamment vérifié

que chaque individu n'a pas fait l'objet de condamnations judiciaires incompatibles avec ses attributions.
Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches. Ces vérifications sont effectuées avant l'affectation à un rôle de confiance et revues régulièrement (au moins tous les trois ans).

4.3.4.Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.
Le personnel a pris connaissance et compris les implications des opérations dont il a la responsabilité.

4.3.5.Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

4.3.6.Sanctions en cas d'actions non autorisées

L'AA de la TSA Adria DigitTrust décide des sanctions à appliquer en cas d'une action non autorisée de la part d'un personnel.

4.3.7.Exigences vis-à-vis du personnel des prestataires externes

L'AA de la TSA Adria DigiTrust doit conclure un contrat avec le prestataire externe, stipulant que son personnel doit respecter les dispositions du présent chapitre.Documentation fournie au personnel
La documentation adéquate, dont doit disposer le personnel en fonction de son besoin d'en connaître pour l'exécution de sa mission, est composée des documents suivants :

- La PH/DPH,
- La politique de gestion de preuve d'Adria DigiTrust
- Les PC/DPC des ACs d'Adria DigiTrust
- Les procédures internes,
- Les manuels d'exploitation,
- Les documents techniques relatifs aux matériels et logiciels utilisés.

4.4.Procédures de constitution des données d'audit

La TSA Adria DigitTrust enregistre les informations appropriées concernant le fonctionnement du service d'horodatage, en particulier :

a) Les enregistrements d'audit relatifs à l'administration des services d'horodatage :
   - ✓ Gestion des opérateurs d'administration.
   - ✓ Connexion / déconnexion des opérateurs d'administration (même en cas d'échec).
   - ✓ Configuration technique ou métier.

b) Les enregistrements d'audit relatifs au fonctionnement du service d'horodatage :
   - ✓ Démarrage et arrêt des services.
   - ✓ Traitement d'une demande de jeton.
   - ✓ Défaillance / indisponibilité du service.

c) Les enregistrements d'audit concernant les événements touchant au cycle de vie des clés et certificats des unités TSU :
   - ✓ Génération de clés.
   - ✓ Demande de certificat.
   - ✓ Génération du certificat.
   - ✓ Import du certificat.
   - ✓ Désinstallation d'un certificat.
   - ✓ Destruction de la clé privée.

d) Les enregistrements d'audit concernant les événements touchant à une synchronisation de l'horloge des unités TSU, y compris les événements touchant à la détection de perte de synchronisation :
   - ✓ Déclaration des sources de temps.
   - ✓ Pertes d'accès à une source de temps.
   - ✓ Détection de perte de synchronisation.
   - ✓ Resynchronisation de l'horloge saut de seconde.

Chacun de ces événements comprend au minimum les données suivantes :

- Type de l'événement Auteur (personne physique, système).
- Date et heure.
- Résultat de l'événement (échec ou réussite).

L'intégrité, la protection contre la suppression et la confidentialité des enregistrements d'audit sont assurés par une gestion d'accès physique, système et réseau appropriée. Les traces techniques sont conservées sans purge sur les équipements du système d'horodatage. Une procédure de sauvegarde quotidienne permet d'exporter ces traces, protégées en intégrité (calcul d'empreinte) et confidentialité (chiffrement), vers des systèmes de conservation sur le long terme.

Les journaux du service d'horodatage sont conservés pendant 7 ans au minimum après l'expiration du certificat d'horodatage actif.

4.5.Continuité d'activité

Au-delà de la continuité d'activité assurée au niveau de l'hébergement, la TSA Adria DigitTrust met en place son propre plan de continuité d'activité concernant les données et les secrets du système.
Les composantes du système d'horodatage disposent d'une sauvegarde hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).
Les fonctions de sauvegarde et de restauration sont effectuées par des administrateurs autorisés conformément aux mesures de sécurité procédurales.
Les sauvegardes hors sites sont réalisées dans un environnement sécurisé en accès physique et logique, et sécurisé contre les risques d'incendie et d'inondation

4.6.Gestion des incidents

La TSA Adria DigitTrust garantit, dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité TSU ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps.

En particulier :

- la TSA Adria DigitTrust traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité TSU ou la perte de calibrage de l'horloge d'une unité TSU, qui pourrait affecter des contremarques de temps émises dans le cadre d'un plan de secours
- Dans le cas d'une compromission, réelle ou suspectée, la TSA Adria DigitTrust mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue.
- Dans le cas d'une perte de calibrage d'une unité TSU, qui pourrait affecter des contremarques de temps émises, la TSA Adria DigitTrust prendra les mesures nécessaires pour que les contremarques de temps de cette unité TSU ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.
- Dans le cas d'une perte de connexion prolongés avec les serveurs de temps, la TSA Adria DigitTrust prendra les mesures nécessaires pour que les contremarques de temps de cette unité TSU ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.
- Dans le cas d'un événement majeur dans le fonctionnement de la TSA Adria DigitTrust ou d'une perte de calibrage qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, la TSA Adria DigitTrust mettra à la disposition de tous ses abonnés et utilisateurs de contremarques de temps toute information pouvant être

utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité du service d'horodatage.

- la TSA Adria DigitTrust prévient directement et sans délai l'autorité nationale DGSSI.

5. Mesures de sécurité techniques

Le présent chapitre contient les exigences de sécurité techniques, en particulier relatives à l'exactitude du temps et à la cryptographie. En particulier, des mesures de contrôles appropriées sont mises en place pour toutes clés cryptographiques ou les modules cryptographiques tout au long de leur cycle de vie.

5.1.Exactitude temps

Les unités TSU de la TSA Adria DigitTrust fournissent une exactitude de l'ordre de la seconde.

5.2.Génération des bi-clés

La génération des clés de signature des unités TSU de la TSA Adria DigitTrust est signée par l'autorité Adria DigiTrust Corporate et effectuée dans un module cryptographique (HSM) :

- Certifié au niveau EAL4+ des critères communs.
- Disposant d'une attestation de conformité de la part de l'autorité nationale DGSSI, au sens de la loi 43-20.

La TSA Adria DigitTrust garantit que toutes les clés cryptographiques sont produites dans des circonstances contrôlées.
Cette génération est réalisée par des personnes en rôle de confiance, et sous contrôle double, c'est-à-dire que deux personnes en rôle de confiance sont requises pour toute opération de création de clés.

Les clés cryptographiques ne sont pas importées dans différents modules cryptographiques, sauf à des fins éventuelles de sauvegarde.
En tout état de cause, une clé privée ne pourra être associée qu'à un et un seul certificat. Seule une clé cryptographique peut être active à un instant t.

La bi-clé de l'unité d'horodatage est transmise à la plateforme Adria DigiTrust de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Le certificat sera par la suite publié dans toutes les contremarques générées pour la signature des demandes d'horodatage, dans les magasins de certificats des applications utilisatrices Adria DigiTrust.

Cependant, le secret du certificat restera directement contrôlé par le service d'horodatage Adria DigiTrust et sera contrôlé par le responsable de TSU. Pour les opérations de signature des demandes d'horodatage, Adria DigiTrust met à disposition un espace sécurisé dédié aux transactions d'horodatages. Ce dernier peut ainsi effectuer les opérations de signature des jetons d'horodatage en activant à distance la clé privée du TSU à l'aide de son propre secret, tout en passant par une authentification forte sur le portail Adria DigiTrust.

5.3.Certification des clés de l'unité TSU

Les clés publiques de vérification des unités TSU sont mises à disposition des utilisateurs au travers d'un certificat d'unité TSU rendu public sur le site de publication (voir paragraphe 1.5 de la présente PH/DPH).

Pour l'émission des certificats, la TSA Adria DigitTrust fait appel à l'AC « Adria DigiTrust Corporate» selon la Politique de Certification dont l'OID est 1.2.504.1.2.2.1.2.
La TSA Adria DigitTrust garantit que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'unité TSU sont égaux à ceux générés par l'Unité TSU.

5.4.Protection des clés privées des unités TSU

La TSA Adria DigitTrust garantit que des clés privées des unités TSU restent confidentielles et conservent leur intégrité.
En particulier, la TSA Adria DigitTrust garantit que toutes les clés cryptographiques sont produites dans des circonstances contrôlées.

5.5.Exigences de sauvegarde des clés des unités TSU

Les clés privées des unités TSU font l'objet de copies de secours dans un espace sécurisé respectant les exigences de la DGSSI et les normes ETSI EN relative au service d'horodatage.

5.6.Destruction des clés des unités TSU

La TSA Adria DigitTrust garantit que les clés de signature des unités TSU sont détruites à la fin de leur cycle de vie.

5.7.Algorithmes obligatoires

La TSA Adria DigitTrust accepte de générer des contremarques de temps pour les empreintes calculées avec les algorithmes suivants :

- SHA-256 ;
- SHA-384 ;
- SHA-512.

Les contremarques de temps sont signées selon les algorithmes et les longueurs de clé conformes à l'état de l'art.
Actuellement, les bi-clés des unités TSU sont de taille RSA de 2048 bits et l'algorithme de signature utilise une fonction de hachage SHA-256.

5.8.Vérification des contremarques de temps

La TSA Adria DigitTrust garantit que les utilisateurs de contremarques de temps ont accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps.
En particulier les certificats des unités TSU sont joints à la contremarque de temps. Ils sont également publiés sur le site web d'Adria DigiTrust (voir paragraphe 1.5 de la présente PH/DPH).

5.9.Durée de validité des certificats des unités TSU

La TSA Adria DigitTrust garantit que la durée de validité des certificats des unités TSU n'est pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée ;
- La fin de validité du certificat d'AC « Adria DigiTrust Corporate» qui l'a émis.

5.10. Durée d'utilisation des clés privées des unités TSU

La durée d'utilisation d'une clé privée des unités TSU sera au plus égale à la période de validité du certificat de clé publique correspondant.

Toutefois elle sera en pratique réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant un laps de temps suffisant.

En tout état de cause, la durée d'utilisation de la clé privée ne pourra dépasser 3 ans.

Dans la pratique, elle sera renouvelée de façon anticipée afin de garantir un recouvrement entre nouvelles et anciennes unités TSU.

Les clés privées ne peuvent être utilisées au-delà de leur période de validité. En particulier :

- Des mesures techniques et opérationnelles sont mises en œuvre de façon à mettre en place une nouvelle clé avant que la clé courante n'expire ;

- Les clés privées sont alors détruites, ainsi que toutes les copies de sauvegardes, afin que la clé ne puisse être restaurée.

5.11. Mesures de sécurité réseau

Les composantes accessibles de la TSA Adria DigitTrust sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).
Les autres composantes de la TSA Adria DigitTrust utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion.
Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseaux non utilisés sont coupés.
Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel la TSA Adria DigitTrust est hébergée refuse tout service, hormis ceux qui sont nécessaires au fonctionnement de la TSA Adria DigitTrust, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

5.12. Politique de sécurité de l'information

La TSA Adria DigiTrust dispose d'une politique générale de sécurité des systèmes d'information (PGSSI). Elle a pour objectif de préciser les enjeux de la sécurité des systèmes d'information, définir les principes et les règles de mise en œuvre au sein des différents acteurs de la TSA Adria DigiTrust, clarifier les responsabilités et organiser la gouvernance de la sécurité des systèmes d'information en tenant compte des évolutions de la structure.

L'organisation de la sécurité des SI repose sur le principe de la séparation des pouvoirs. Les fonctions de décision et de contrôle permanent sont placées sous la responsabilité du RSSI de Adria Digitrust et des responsables de la sécurité SI et se distinguent des fonctions de mise en application et la gestion opérationnelle de la plateforme (équipes métier et support).

La PGSSI d'Adria DigiTrust est documentée, implémentée, maintenue, révisée annuellement et approuvée par l'AA.

6. Profil des certificats et contremarques de temps

6.1. Format du certificat d'horodatage

Les certificats de signature des contremarques de temps respectent le gabarit suivant :

Champs de base

Champ	Valeur	Détail valeur	Commentaire
Version	V3	2	Certificat x509 v3
Numéro de série	Nombre entier		Nombre entier pour indiquer le numéro de série du certificat
Algorithme de signature du certificat	La valeur doit correspondre à l'OID de l'algorithme défini pour l'attribut « signatureAlgorithm »	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11	Identifiant de l'algorithme de signature
Emetteur	DN (Distinguished Name)	*CN= Adria DigiTrust Corporate* *O= Adria DigiTrust* *OI=IC:MA-003277827000016*	Identifiant de l'AC Corporate
Valide à partir de	T0		Date de début de validité
Valide jusqu'au	T0 + 3 ans		Date de fin de validité
Sujet	DN (Distinguished Name)	*SerialNumber= numéro de série attribué par l'AC* *CN= Adria DigiTrust TSU N* *O= Adria DigiTrust* *OI=IC:MA-003277827000016* *C= MA*	Identifiant de la TSU N
Algorithme et valeur de la clé publique de l'AC déléguée	RSA encryption OID=1.2.840.113549.1.1.1	Valeur sur 2048 bits	Identifiant de l'algorithme

Extensions

Champ	Valeur	Criticité	Commentaires
basic constraints	Type d'objet = pas une autorité de certification Contrainte de longueur de chemin d'accès = aucune	Extension critique	Indique qu'il ne s'agit pas d'un certificat d'AC
keyUsage	Digital Signature	Extension critique	Utilisation de la clé : - « non répudiation » selon le RFC 5280
Extended Key Usage:	Time Stamping	Extension critique	Utilisation de la clé : - « id-kp-timeStamping» selon le RFC 5280
cRL DistributionPoints	Nom du point de distribution : Nom complet : URI : http://pki.adria-digitrust.com/sources/AdriaDigiTrustCorporate.crl	Extension non critique	Point de distribution de la LCR
authorityInfo Access	Accès aux informations de l'autorité [1] : Méthode d'accès : Emetteur d'autorité (1.3.6.1.5.5.7.48.2) Adresse d'accès : URI : https://pki.adria-digitrust.com/sources/AdriaDigiTrustCorporate.crt Accès aux informations de l'autorité [2] : Méthode d'accès : Méthode d'accès OCSP (1.3.6.1.5.5.7.48.1) Adresse d'accès : URI : https://adt-ocsp.adria-digitrust.com	Extension non critique	Adresse du service OCSP
certification Policy	Identificateur de la politique : 1.2.504.1.2.2.1.5 Information de qualificateur de politique [1.1]: Qualificateur de pointeur CPS PKIX	Extension non critique	Identifiant de la PC de la TSA

	(1.3.6.1.5.5.7.2.1) Pointeur CPS : https://pki.adria-digitrust.com/cp.html		
authorityKey Identifier	Variable	Extension non critique	Identifiant de la clé publique de l'AC à utiliser pour vérifier la signature du certificat

6.2. Profil des LCRs

Le gabarit des LCRs est le suivant :

Champs de base

Champ	Valeur	Commentaires
Version	V2	Version de la LCR utilisée (V2)
Signature	Sha512WithRSAEncryption OID: 1.2.840.113549.1.1.13	OID de l'algorithme de signature
Issuer	*CN= Adria DigiTrust Corporate* *O= Adria DigiTrust* *OI=IC:MA-003277827000016* *C=MA*	DN de l'AC qui a signé la LCR
ThisUpdate	Date et heure UTC	Date de génération de la LCR
NextUpdate	Date et heure UTC	Date au plus tard de la mise à jour de la LCR
RevokedCertificates	Liste de tuples: • UserCertificate (numéro de série) • RevocationDate (date de révovation)	Liste des numéros de série des certificats révoqués ainsi que leur date de révocation

Extensions

Champ	Valeur	Criticité	Commentaires

Numéro de LCR	Nombre entier	Extension non critique	Numéro croissant
Identifiant de la clé publique de l'Autorité (AuthorityKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique du certificat. Dérivé de la valeur de la clé publique du certificat.

6.3. Profil du répondeur OCSP

Le gabarit du répondeur OCSP est le suivant :

Champs de base

Champ	**Valeur**	**Détail valeur**	**Commentaire**
Version	V3	2	Certificat x509 v3
Numéro de série	Nombre entier		Nombre entier pour indiquer le numéro de série du certificat
Algorithme de signature du certificat	La valeur doit correspondre à l'OID de l'algorithme défini pour l'attribut « signatureAlgorithm »	Sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11	Identifiant de l'algorithme de signature
Emetteur	DN (Distinguished Name)	*CN= Adria DigiTrust Corporate* *O= Adria DigiTrust* *C=MA* *OI=IC:MA-003277827000016*	Identifiant de l'AC déléguée
Valide à partir de	T0		Date de début de validité
Valide jusqu'au	T0 + an	X ans est équivalant à 1 an maximum	Date de fin de validité
Sujet	DN (Distinguished Name)	*CN=* OCSP Responder Corporate *O= Adria DigiTrust* *OI=IC:MA-003277827000016*	Identifiant du répondeur OCSP

		C=MA	
Algorithme et valeur de la clé publique de l'AC déléguée	RSA encryption OID=1.2.840.113549.1.1.1	Valeur sur 2048 bits	Identifiant de l'algorithme

Extensions

Champ	**Valeur**	**Criticité**	**Commentaires**
Contraintes de base	Type d'objet = pas une autorité de certification Contrainte de longueur de chemin d'accès = aucune	Extension critique	Un certificat à utilisation finale pour signer les réponses OCSP
Utilisation de la clé	Signature numérique	Extension critique	Signature numérique « Digital Signature »
Identifiant de la clé publique du sujet (SubjectKey Identifier)	Variable	Extension non critique	Identifiant de la clé publique du certificat. Dérivé de la valeur de la clé publique du certificat.
Identifiant de la clé publique de l'Autorité (AuthorityKey Identifier)	Variable	Extension non critique	
Pas de vérification OCSP	Pas de vérification OCSP		
Usage étendu de la clef (EKU)	Signature OCSP (1.3.6.1.5.5.7.3.9)		Indique que ce certificat est utilisé pour la signature des réponses OCSP

6.4. Format des contremarques de temps

Les contremarques de temps respectent le gabarit suivant :

Champ	**Valeur**	**Commentaire**
version	1	Version du format
Policy	1.2.504.1.2.2.1.5	OID de la présente PH/DPH
messageImprint	Identiques aux valeurs inclues dans la demande	OID de l'algorithme de hash (empreinte) hash des données à horodater
serialNumber	Généré par la TSU	Identifiant unique de la contremarque de temps
genTime	Heure de la TSU au moment de la génération	Heure de la contremarque de temps
accuracy	1 seconde	Précision déclarée
ordering	False	Information d'ordonnancement
nonce	Identique à celui présent dans la demande si nonce était présent	Donnée anti-rejeu
tsa	Non présent dans la version actuelle du service. Les futures versions pourront intégrer le champ "subject" du certificat d'horodatage de la TSU	Identifiant de la TSU
extensions	Aucune extension supplémentaire	Extension supplémentaire optionnelle Aucune extension supplémentaire

7. Audit de conformité et autres évaluations

7.1. Fréquences et / ou circonstances des évaluations

LaTSA Adria DigitTrust fait l'objet d'audit de conformité interne périodique au moins une fois par an.

La TSA Adria DigitTrust peut faire l'objet également d'un contrôle de conformité par la DGSSI selon la règlementation en vigueur.

7.2. Identité des auditeurs

L'AA de la TSA Adria DigitTrust désigne les auditeurs de conformité qui doivent avoir les compétences nécessaires dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la présente PH/DPH

La DGSSI peut également accréditer les auditeurs de conformité externes pour réaliser des missions de contrôle de conformité des composants de la TSA Adria DigitTrust.

7.3. Relations entre auditeur et entités évaluées

Afin d'effectuer une évaluation juste et indépendante, les auditeurs chargés de l'audit de conformité de la TSA Adria DigitTrust sont :

- Soit des auditeurs internes de l'AA indépendants du service opérant dans la TSA Adria DigitTrust ;
- Soit des auditeurs externes commandités par l'AA ;
- Soit des auditeurs externes accrédités par la DGSSI.

7.4. Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante de la TSA Adria DigitTrust opère ses services en conformité avec la présente PH/DPH.

7.5. Actions prises suite aux conclusions des évaluations

A la constatation d'une non-conformité par rapport aux exigences de la PH/DPH de la TSA Adria DigitTrust, l'auditeur de conformité procède aux actions suivantes :

- Documenter la non-conformité ;
- Notifier l'entité concernée par la non-conformité ;
- L'entité responsable de la correction de la non-conformité détermine quelles sont les mesures à prendre en fonction des exigences de la présente PH/DPH, et les effectue sans délai avec l'approbation de l'AA.

Selon le degré de criticité de la non-conformité, et la rapidité avec laquelle elle peut être corrigée, l'AA peut décider de suspendre temporairement le fonctionnement de la TSA Adria DigitTrust, de révoquer le certificat de l'unité TSU, ou de prendre toute autre mesure qu'il juge opportune.

7.6. Communication des résultats

Le Rapport de la mission d'audit de Conformité, incluant l'état de réalisation des mesures correctives (réalisé, validé, en cours) est remis à l'AA.