INFRASTRUCTURE DE CONFIANCE NATIONALE
AC TECHNIQUE

CONDITIONS GENERALES D'UTILISATION DES JETONS DE TEMPS

État du document - Classification	Référence
En cours - Publique	2.16.492.1.1.1.1.6.3

Version	Date	Description
1.0	4/11/2021	Version applicable

1 OBJET

Les présentes Conditions Générales d'Utilisation (ou « Conditions Générales d'Utilisation du certificat », ci-après désignées « CGU ») ont pour objet de préciser les modalités de délivrance et d'utilisation des jetons de temps, aussi appelés contremarques de temps délivrés par le Prestataire de services d'horodatage (PSHE) du Gouvernement Princier (Ci-après désignée « Gouvernement ») ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Le PSHE est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps.

Les présentes CGU s'appliquent à tout partenaire autorisé sollicitant les jetons de temps proposés par le PSHE et utilisant lesdits jetons.

Le partenaire autorisé confirme avoir lu et compris l'intégralité des présentes CGU avant toute utilisation de Certificat et s'engage à les respecter.

2 DEFINITIONS

Les mots et expressions ci-après commençant par une lettre majuscule, au singulier ou au pluriel, sont employés dans les présentes avec la signification suivante :

Autorité de Certification (AC) - Entité émettant des Certificats après vérification de l'identité de la personne ou du représentant du système applicatif, ou de la procédure ayant mené à son identification. L'AC est responsable de l'ensemble des composantes matérielles, humaines et organisationnelles utilisées dans le processus de création et de gestion des Certificats.

Autorité d'Horodatage (AH) - Autorité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage de la DSN sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la marque de temps. Il s'agit de la DSN (Direction des Services Numériques) dans le cadre de la présente PH.

L'AH est une entité subordonnée au PSHE et ne dispose pas nécessairement de la personnalité juridique.

Contremarque de temps - Donnée 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) - Échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

Nota - Pour la plupart des usages, le temps UTC est équivalent au temps solaire au méridien principal (0°). De manière plus précise, le temps UTC est un compromis entre le temps atomique particulièrement stable (Temps Atomique International -TAI) et le temps solaire dérivé de la rotation irrégulière de la terre lié au temps moyen sidéral de Greenwich (GMST) par une relation de convention.

Horodatage électronique : des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ;

Horodatage électronique qualifié, un horodatage électronique qui satisfait aux exigences fixées à l'article 32 du [RGSP].

Jeton d'horodatage - Voir contremarque de temps.

Module d'horodatage - Produit de sécurité comportant une ressource cryptographique et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, 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.

Opérateur de Service d'Horodatage (OSH) - Opérateur assurant les prestations techniques nécessaires au processus d'horodatage. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques. Il est en charge de la sécurité des personnels, des locaux et, plus généralement, du bon respect des procédures, toutes choses indispensables pour garantir un niveau de fiabilité.

Responsable du service demandeur – responsable de l'entité demandant à l'AH la fourniture de service d'horodatage et ayant explicitement ou implicitement accepté les termes et conditions de cette fourniture

Politique d'Horodatage (PH) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps (partenaires autorisés).

Prestataire de services d'horodatage (PSHE) –Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

Service d'horodatage - Ensemble des prestations nécessaires à la génération et à la gestion de contremarques de temps.

Service demandeur (ou Porteur dans le présent document) - Entité demandant à l'AH la fourniture de service d'horodatage et ayant explicitement ou implicitement accepté les termes et conditions de cette fourniture.

Système d'horodatage - Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

Unité d'Horodatage (UH) - Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

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

Nota - 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).

Utilisateur final - Personne physique ou morale identifiée ou non qui reçoit par l'intermédiaire du service demandeur un jeton d'horodatage correspondant à la fourniture d'un service d'horodatage par l'AH.

3 POINT DE CONTACT

Les demandes d'informations relatives à la délivrance des Certificats d'Horodatage délivrés par la Direction des Services Numériques peuvent être réalisées :

- Par courrier postal : auprès de la Direction des Services Numériques (DSN) dont le siège est situé au 23 avenue Albert II, MC 98000 MONACO.
- Par e-mail à l'adresse suivante : service-horodatage@gouv.mc

Les demandes d'informations relatives à la délivrance des jetons de temps par le PSHE du Gouvernement représenté par la Direction des Services Numériques peuvent être réalisées :

- Par courrier postal : auprès de la Direction des Services Numériques (DSN) dont le siège est situé au 23 avenue Albert II, MC 98000 MONACO.
- Par e-mail à l'adresse suivante : identitenumerique@gouv.mc

4 USAGES DES JETONS

Un jeton d'horodatage est une structure signée numériquement et qui contient en particulier :

- l'identifiant de la Politique d'Horodatage sous laquelle le jeton d'horodatage a été généré ;
- 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 la contremarque de temps (certificat qui identifie aussi l'AH).

La durée de vie attendue des clés privées de signature utilisées pour signer le jeton d'horodatage est une durée de vie maximale de trois (3) ans.

La fonction de hachage utilisée pour constituer l'objet horodaté est SHA 256.

Les usages des jetons sont décrits dans la PH (Politique d'Horodatage) dont l'Identifiant Objet (OID) est 2.16.492.1.1.1.1.6.1.

5 LIMITE D'USAGE

L'usage des jetons est limité aux usages décrits dans la PH.

6 CONDITIONS D'OBTENTION ET D'UTILISATION DU JETON

6.1 DEMANDE DE JETON

6.1.1 *La demande de jeton de temps*

Une demande de jeton de temps se fait auprès du Prestataire de services d'horodatage (PSHE) du Gouvernement Princier selon le protocole de la [RFC 3161] auprès de l'adresse https://time.mconnect.mc.

6.1.2 *Déroulé du processus de génération du jeton*

Le partenaire autorisé accède à https://time.mconnect.mc et il sollicite l'obtention d'un jeton d'horodatage depuis l'application pour laquelle il souhaite le jeton.

La plateforme délivre le jeton.

6.2 UTILISATION DES JETONS

Le Jeton ne sert qu'aux usages définis à l'article 4 des présentes CGU.

7 OBLIGATIONS

Obligations des services demandeurs :

Le service demandeur s'engage à vérifier le certificat d'horodatage issu de la chaîne de certification de l'AC Racine du Gouvernement Princier, utilisé pour émettre les jetons.

Le service demandeur s'engage également à vérifier que les données sur lesquelles portent le scellement d'horodatage sont bien celles transmises pour horodatage.

Obligations des utilisateurs finaux :

Les utilisateurs finaux doivent être déclarés et autorisés par l'Etat.

Les utilisateurs finaux doivent respecter le protocole de la [RFC 3161].

Il leur est cependant recommandé de valider les jetons d'horodatage reçus.

L'utilisateur final a l'obligation de prendre toutes les mesures propres à assurer la sécurité de ses postes informatiques sur lesquels sont utilisés les jetons d'horodatage.

Tout utilisateur final d'une contremarque de temps (partenaire autorisé) fournie par le service demandeur peut vérifier l'état révoqué ou non d'un Certificat en vérifiant la liste de Certificats révoqués indiquée par le point de distribution présent dans le Certificat. Dans le cas où le Certificat viendrait à être révoqué, il incombe au destinataire du document signé de déterminer s'il est raisonnable d'accorder sa confiance au Certificat. La responsabilité de la DSN ne pourra en aucun cas être engagée en cas de révocation du Certificat.

8 RESPONSABILITE

Les jetons ne doivent pas être utilisés de façon abusive ou malveillante.

De manière générale, l'utilisateur s'engage à utiliser les jetons :

- Dans le respect des lois, de la règlementation monégasque, et des droits de tiers ;
- De manière loyale et conformément à leurs usages ;
- Sous sa responsabilité exclusive.

Les contremarques de temps fournies respectant la PH applicable doivent être une structure TimeStampToken conforme au [RFC3161].

Afin de s'assurer de la qualité du jeton de temps, l'utilisateur final prend connaissance des attributs du certificat et vérifie l'exactitude des champs ci-dessous :

Champ	**Exigences**
Generation time	*Date de l'horodatage*
messageImprint	SHA-256
policy	2.16.492.1.1.1.1.6.1
serial number	Numéro de série de la contremarque
accuracy	Si la synchronisation avec le temps UTC est différente de 1 seconde, ce champ doit être présent et doit préciser l'exactitude de la synchronisation. Si la synchronisation est de 1 seconde, il peut être omis.
gentimeaccuracy	absent
messageimprint	Empreinte des données et OID de l'algorithme utilisé
ordering	Ce champ doit être absent ou bien contenir la valeur false.
tsa	Si ce champ est présent, il doit être identique au champ subject du certificat de l'UH ayant signé la contremarque de temps.
extensions	Des extensions peuvent être incluses par l'AH, mais aucune ne doit être marquée comme critique.
nonce	Valeur incluse si présente dans la requête

Le Porteur reconnaît et accepte que la responsabilité de la DSN ne peut être engagée au titre du service de fourniture de jetons de temps, notamment en cas d'altération, de toute utilisation illicite ou préjudiciable au Porteur ou à un tiers du réseau par un tiers.

Le Porteur assume l'entière responsabilité des conséquences résultant de ses fautes, erreurs ou omissions.

Le Porteur garantit à l'Administration qu'il est propriétaire des documents qu'il horodate grâce au Service.

L'Administration n'est pas responsable de la légalité et de la conformité des documents signés grâce à son Service.

L'Administration n'est pas responsable si le jeton d'horodatage d'un document ne respecte pas les conditions d'horodatage pour ce type de document.

Le Porteur est seul responsable du cycle de vie des documents qu'il horodate : de leur établissement jusqu'au terme de la conservation.

Le Porteur du jeton s'interdit toute utilisation ou tentative d'utilisation du jeton de temps à des fins autres que celles prévues par les présentes et par le jeton lui-même

Les termes des présentes CGU peuvent également être amendés à tout moment, sans préavis, en fonction des modifications opérées par la DSN, de l'évolution de la législation ou de tout autre motif jugé nécessaire. Il appartient au Porteur de s'informer desdites conditions.

9 LIMITES DE GARANTIES ET DE RESPONSABILITES

En aucun cas la DSN en tant que responsable de l'AC technique n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre les utilisateurs finaux des contremarques de temps (partenaires autorisés) et les destinataires des documents horodatés.

La DSN en tant que responsable de l'AC technique n'assume aucun engagement ni responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, ni quant aux retards, l'altération ou autres erreurs pouvant se produire dans la transmission de toute communication électronique.

La responsabilité de la DSN en tant que responsable de l'AC technique ne peut être engagée en cas de compromission de la clé privée. La DSN en tant que responsable de l'AC technique ne se voit pas confier la conservation et/ou la protection de la clé privée du Certificat.

10 CONSERVATION DES DONNEES

Des données sont conservées lors de la création du dossier d'enregistrement dès la demande de fourniture de Certificat.

Les informations à caractère personnel sont les informations nominatives du responsable du service demandeur mentionnés au sein du dossier d'enregistrement.

Ces données sont conservées pendant dix (10) ans. La durée d'archivage est de sept (7) ans après la date d'expiration du Certificat (la durée de vie d'un Certificat étant de trois (3) ans).

La conservation est réalisée dans le respect et avec le niveau de protection adapté aux données à caractère personnel dont la gestion fait l'objet du paragraphe 12.

11 PROPRIETE INTELLECTUELLE

Les marques et/ou logos dont est titulaire la DSN en tant que responsable de l'AC technique, apparaissant sur tous supports, sont des marques protégées par les dispositions légales applicables à Monaco.

Toute représentation ou reproduction totale ou partielle sans autorisation expresse et préalable de l'Administration est interdite et constitue une infraction pénalement sanctionnée par les Cours et Tribunaux monégasques.

12 PROTECTION DES DONNEES A CARACTERE PERSONNEL

La DSN exploite un traitement d'informations nominatives qui s'inscrit dans le cadre de la finalité suivante : « Fourniture des services de confiance pour l'identité numérique » dont la délibération a été prononcée le 2 juin 2021 avec un avis favorable :

Délibération n° 2021-112 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « Fourniture des services de confiance pour l'identité numérique » dénommé « MConnect et MConnect Mobile » exploité par la Direction des Services Numériques et présenté par le Ministre d'État.

13 LOI APPLICABLE, REGLEMENT DES LITIGES

Les parties conviennent de manière expresse que seule la législation et la règlementation monégasque sont applicables.

Elles s'engagent à rechercher un accord amiable en cas de litige. A l'initiative de la partie demandeuse, une réunion sera organisée. Tout accord de règlement du litige devra être consigné par écrit sur un document signé par un représentant accrédité des deux parties.

En cas de litige relatif à l'interprétation, la formation ou l'exécution du Contrat et faute d'être parvenues à un accord amiable, les parties donnent compétence expresse et exclusive aux tribunaux compétents de la Principauté de Monaco.