

INFRASTRUCTURE DE CONFIANCE NATIONALE
AC TECHNIQUE
CONDITIONS GENERALES D'UTILISATION DES CERTIFICATS
D'HORODATAGE

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
1.1	04/03/2022	Version modifiée

Table des matières

1	OBJET	2
2	DEFINITIONS	2
3	POINT DE CONTACT	4
4	TYPES DE CERTIFICAT ET USAGES	4
5	LIMITE D'USAGE	4
6	CONDITIONS D'OBTENTION ET D'UTILISATION DU CERTIFICAT	4
6.1	Demande de Certificat et Justificatifs à fournir	4
6.2	remise du Certificat et acceptation	5
6.3	Utilisation d'ES CertificatS	5
6.4	Renouvellement des certificats.....	6
6.5	Révocation.....	6
7	OBLIGATIONS	6
8	RESPONSABILITE	7
9	LIMITES DE GARANTIES ET DE RESPONSABILITES	8
10	CONSERVATION DES DONNEES	8
11	PROPRIETE INTELLECTUELLE.....	9
12	PROTECTION DES DONNEES A CARACTERE PERSONNEL	9
13	LOI APPLICABLE, REGLEMENT DES LITIGES	9
14	INDEPENDANCE des parties et non-discrimination	9

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 certificats électroniques d'horodatage délivrés par le Gouvernement Princier (Ci-après désignée « Gouvernement ») ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les présentes CGU s'appliquent à tout Demandeur sollicitant les certificats électroniques d'horodatage proposés par le Gouvernement et utilisant lesdits certificats.

Le Responsable du Certificat 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 :

Abonné – Entité ayant besoin de faire horodater des données par une Autorité d'Horodatage et qui a accepté les conditions d'utilisation de ses services. Cette notion est valable pour les hypothèses où la contremarque de temps est demandée directement à l'AH.

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) - Entité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la marque de temps.

Contremarque de temps ou jeton de temps - 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) - 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.

Demandeur : Le Demandeur est la personne physique qui effectue une demande auprès d'une Autorité d'Enregistrement pour obtenir un certificat de personne physique ou de cachet.

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.

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 et 33 du [RGSP].

Infrastructure de Confiance Nationale ou ICN - L'ICN est l'ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance mise en œuvre par l'AMSN pour le compte du Gouvernement princier. L'AC TECHNIQUE est une des autorités rattachées à l'ICN.

Officier de sécurité de l'ICN - Personne qui a pour mission, sous les ordres de son autorité d'emploi, de fixer les règles et les consignes de sécurité à mettre en œuvre relatives aux personnes et aux informations ou supports protégés et d'en vérifier l'exécution.

Jeton d'horodatage - Voir contremarque de temps.

Liste de Certificats Révoqués (LCR) – Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

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.

- La PH de l'AC Technique : 2.16.492.1.1.1.1.6.11.2

Politique de Certification ou PC : la PC de l'AC TECHNIQUE désigne le document établissant les principes qui s'appliquent à l'AC, aux personnes morales, aux Représentants légaux, aux Mandataires de certification et aux porteurs intervenant dans l'ensemble du cycle de vie d'un certificat, (consultable à l'adresse suivante : <https://mconnect.gouv.mc/technique>)

Les identifiants des PC applicables pour les présentes CGU sont :

- La PC de l'AC Racine : 2.16.492.1.1.1.1.1.1. ;
- La PC de l'AC TECHNIQUE : 2.16.492.1.1.1.1.6.1.

Responsable du Certificat de la personne morale ou RC : La notion de Responsable de Certificat ne s'applique qu'aux certificats finaux de personnes morales. Le Responsable du Certificat est la personne physique nommée et mandatée par le Responsable Légal de la personne morale pour gérer tout ou partie des certificats de cachet de cette dernière.

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

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 (Rec. ITU-R TF.536-1 [TF.536-1]).

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 de contremarque de temps - Entité (personne ou système) qui fait confiance à une Contremarque de temps émise sous une Politique d'horodatage donnée par une Autorité d'horodatage donnée.

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

4 TYPES DE CERTIFICAT ET USAGES

L'horodatage électronique est un service de confiance qui permet d'attester que des données sous forme électronique existaient bien à un instant donné.

Ce service consiste à associer à une représentation sans équivoque des données concernées, un instant dans le temps suivant une précision prédéfinie par rapport au temps universel.

Le service d'horodatage électronique est sollicité par des Abonnés souhaitant obtenir un certificat d'horodatage, et qui ont en charge la fourniture, à leurs utilisateurs de contremarques de temps

L'AC TECHNIQUE émet différents profils de certificats <PROFIL>, chacun identifié par un OID spécifique. Les usages sont explicites dans le gabarit du certificat.

Les types de Certificats et usages sont décrits dans la PC dont l'Identifiant Objet (OID) est 2.16.492.1.1.1.1.6.11.2

Les services d'horodatage et d'authentification (via MConnect) sont disponibles en 24/7, 365 jours par an, sauf cas de force majeure qui sera dans ce cas annoncé sur le site mconnect.gouv.mc.

Des notifications sont réalisées sur le site de référence mconnect.gouv.mc en cas de problèmes susceptibles de porter atteinte à l'intégrité et la disponibilité du service.

5 LIMITE D'USAGE

Le RC doit respecter strictement les usages autorisés des bi-clés et des Certificats. Dans le cas d'une utilisation frauduleuse, sa responsabilité peut être engagée.

L'usage autorisé de la bi-clé et du Certificat associé est précisé dans le Certificat lui-même.

L'utilisation de la clé privée du RC et du Certificat associé est strictement limitée au service défini par l'identifiant de sa PC.

Le RC reconnaît être informé qu'une utilisation frauduleuse ou non conforme aux présentes CGU ainsi qu'à l'usage autorisé de la bi-clé et du Certificat est un motif légitime de révocation par l'AC.

L'usage des Certificats est limité aux usages décrits dans la PC.

6 CONDITIONS D'OBTENTION ET D'UTILISATION DU CERTIFICAT

6.1 DEMANDE DE CERTIFICAT ET JUSTIFICATIFS A FOURNIR

6.1.1 *La demande de certificat*

Une demande de Certificat d'horodatage, doit être faite auprès de l'AC Technique du Gouvernement Princier grâce à un dossier d'enregistrement.

Le service d'enregistrement proposé par l'AC est disponible, sur rendez-vous, pendant les heures d'ouverture de la DIRECTION DES SERVICES NUMÉRIQUES.

6.1.2 *Déroulé du processus d'enrôlement et de production des Certificats électroniques*

- Réception du formulaire de demande de certificat d'horodatage (avec acceptation des présentes CGUs) par l'Opérateur d'Enregistrement (DSN)
- Vérification de l'identité (pièce d'identité : carte d'identité, passeport ou carte de séjour) et de l'habilitation du Demandeur à solliciter un Certificat d'Horodatage
- Génération du certificat d'horodatage par l'Opérateur d'Enregistrement

Le service d'émission des certificats qualifiés a été évalué par un organisme accrédité par le Comité Français d'Accréditation (COFRAC). Ce service est conforme à la PC publiée.

6.2 REMISE DU CERTIFICAT ET ACCEPTATION

6.2.1 *Déroulé du processus de délivrance du certificat d'horodatage*

Le processus de remise du certificat d'horodatage se déroule comme suit :

- Délivrance du certificat d'horodatage (renvoi par e-mail au RC)
- Délivrance d'un document de remise et signature par le RC ou le Mandataire et l'Opérateur d'Enregistrement et archivage par l'Opérateur d'Enregistrement
- Archivage du dossier

Afin de s'assurer de la qualité du certificat délivré par l'AC technique, le RC prend connaissance des attributs du certificat et vérifie l'exactitude des champs. (Émetteur, AC, dates de validité, objet, Key usage = digitalsignature (Signature numérique) et Extended Key Usage = Time stamping))

6.3 UTILISATION DES CERTIFICATS

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

6.4 RENOUELEMENT DES CERTIFICATS

Les Certificats électroniques ont une durée de vie maximale de trois (3) ans.

Le renouvellement du certificat aura lieu tous les ans (1).

La procédure sera identique à celle d'une 1^{ère} demande.

6.5 REVOCATION

Les causes possibles d'une révocation sont décrites dans la PC.

Lors de la délivrance des certificats, l'opérateur d'enregistrement de l'AC technique transmet un code de révocation au RC.

Ce code de révocation est transmis par e-mail lors de la délivrance du certificat.

En cas de compromission du certificat ou pour toute autre raison justifiant une révocation, le RC doit contacter par email (service-horodatage@gouv.mc) l'Opérateur d'Enregistrement (24/7), qui l'authentifie et procède à la révocation du certificat.

L'authentification est réalisée par l'Opérateur d'Enregistrement soit :

- Via le code de révocation (fourni lors de la délivrance)
- Ou en posant les questions personnelles renseignées dans le formulaire de demande de certificat d'horodatage.

Il confirme ensuite au RC la bonne exécution de la révocation.

La demande de révocation du Certificat peut également être réalisée par le Mandataire de Certification ou le Représentant Légal, qui seront alors authentifiés par l'Opérateur d'Enregistrement grâce aux questions personnelles renseignées lors du dépôt du dossier d'enregistrement.

Le Responsable d'AC, le Responsable du C2SC ou une autorité judiciaire, peuvent également saisir par courrier officiel l'Opérateur d'Enregistrement de l'AE ou l'Officier de Sécurité de l'ICN, pour effectuer l'opération de révocation.

- Consultation de l'état d'un Certificat :

Le Responsable du Certificat peut à tout moment vérifier l'état de ses Certificats en consultant les LCR (Liste des Certificats Révoqués) disponibles, ou en interrogeant le service en ligne d'état des certificats (OCSP) qui intègre une réponse « certificat révoqué » après la date de fin de vie du certificat. Les certificats révoqués restent présents dans la LCR même après leur date d'expiration d'origine. En cas de cessation définitive d'activité de l'AC, une dernière LCR sera émise avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s.

7 OBLIGATIONS

Conditions Générales d'Utilisation

Le RC a l'obligation de prendre toutes les mesures propres à assurer la sécurité de ses postes informatiques sur lesquels sont utilisés les supports et le certificat d'horodatage.

Le RC s'engage à générer puis stocker le certificat dans un HSM correspondant à la catégorie déclarée lors du dépôt du formulaire de demande de certificat afin d'en préserver l'intégrité et la confidentialité de sa clé privée.

La connaissance de la compromission avérée ou soupçonnée des données confidentielles, du non-respect des présentes conditions générales, du décès du RC, ou de la modification des données contenues dans le Certificat, par le RC ou par la DSN, emporte obligation, à leur charge, de demander dans les meilleurs délais la révocation du Certificat associé.

Le RC s'engage à ne plus utiliser un Certificat suite à l'expiration de celui-ci, à une demande de révocation ou à la notification de la révocation du Certificat, quelle qu'en soit la cause.

Le RC s'engage à vérifier l'usage indiqué dans le Certificat.

Obligations de l'AC :

En cas de demande de révocation par le Porteur, respectivement le RC, la DSN révoque le Certificat dans un délai inférieur à vingt-quatre (24) heures à compter d'une sollicitation par le demandeur.

Les conditions de fin de relation avec l'AC TECHNIQUE sont publiées au paragraphe 4.11 de la PC.

Obligations de l'AH :

- S'assure que toutes les exigences détaillées dans les chapitres qui suivent sont mises en place ;
- Garantit l'application des procédures découlant de la présente politique, que les fonctionnalités de l'AH soient sous-traitées auprès de sociétés externes ou non ;
- S'assure que les moyens mis en œuvre, répondent complètement aux exigences de la PH ;
- S'engage à respecter la confidentialité des éléments précisés de la PH. Concernant la génération des jetons d'horodatage, l'AH s'assure que le Service d'horodatage :
 - Respecte et répond aux exigences de la PH ;
 - ⊖ Accepte les audits périodiques de contrôle de conformité à la PH.

8 RESPONSABILITE

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

De manière générale, le Responsable du Certificat s'engage à utiliser les Certificats :

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

Afin de s'assurer de la conformité du certificat délivré par l'AC technique, le Responsable du Certificat prend connaissance des attributs du certificat et vérifie l'exactitude des champs suivants :

- Émetteur
- AC
- dates de validité
- objet
- Key usage = digitalsignature
- Extended Key Usage = timestamping

Le Responsable du Certificat reconnaît et accepte que la responsabilité de la DSN ne peut être engagée au titre de son activité de délivrance de certificats, notamment en cas d'altération, de toute utilisation illicite ou préjudiciable au Responsable du Certificat ou à un tiers du réseau par un tiers.

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

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 certificat d'horodatage d'un document ne respecte pas les conditions d'horodatage pour ce type de document.

Le Responsable du Certificat s'interdit toute utilisation ou tentative d'utilisation du Certificat des fonctionnalités et des usages autorisés des bi-clés à des fins autres que celles prévues par les présentes et par le Certificat 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 Responsable du Certificat 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 le RC, l'AH, les Abonnés et les utilisateurs des contremarques de temps.

La DSN en tant que responsable de l'AC technique n'assume aucun engagement ni responsabilité quant à la forme, la suffisance, l'exactitude, l'authenticité, ou l'effet juridique des documents remis lors de la demande de Certificat.

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.

Les parties conviennent expressément, qu'en aucune façon, la responsabilité de la DSN en tant que responsable de l'AC technique ne pourra être engagée dès lors que le Responsable du Certificat n'aura pas effectué de demande de révocation de Certificat conformément aux stipulations des présentes.

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.

Les logs techniques sont conservés dans un espace sécurisé pour une durée d'un an, puis sont effacés.

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 réglementation monégasque sont applicables.

Elles s'engagent à rechercher un accord amiable en cas de litige. A l'initiative de la partie demanderesse, 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.

14 INDEPENDANCE DES PARTIES ET NON-DISCRIMINATION

L'organisation mise en place par l'AC est dédiée à ses activités et garantit l'étanchéité des rôles. Elle permet de préserver l'impartialité des opérations et assure que les activités de confiance fournies sont pratiquées de façon équivalente pour l'ensemble des bénéficiaires ayant accepté les conditions générales d'utilisation du service et respectant les obligations qui leur incombent.

Conditions Générales d'Utilisation

Dans toute la mesure du possible, l'AC met en œuvre des approches appropriées pour rendre son service accessible à toute personne y compris en situation de handicap, en prenant en compte au cas par cas les spécificités de chaque demandeur.

D'une manière générale, les services fournis par l'AC tels que, notamment, la génération de certificats, la gestion des révocations et le statut des certificats sont exercés de façon indépendante et ne sont donc soumis à aucune pression éventuelle.