INFRASTRUCTURE DE CONFIANCE NATIONALE
AC SERVICES ADMINISTRATIFS
CONDITIONS GENERALES D'UTILISATION

État du document - Classification	Référence
En cours - Publique	2.16.492.1.1.1.1.5.3

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 certificats électroniques de signature, d'authentification et de cachet proposés par la Direction des Ressources Humaines et de la Formation de la Fonction Publique (Ci-après désignée « DRHFFP » ou « DRH ») ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les présentes CGU s'appliquent à tout Utilisateur, faisant partie des Services de l'Etat, sollicitant les certificats électroniques proposés par la DRH et utilisant lesdits certificats.

L'Utilisateur 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 ou AC** : désigne l'ensemble des systèmes informatiques qui permettent de créer et révoquer des certificats électroniques.
- **Autorité d'Enregistrement ou AE** : désigne la DRH.

Elle assure les fonctions suivantes :

- Réception des dossiers de demande de génération d'un certificat ;
- Réception des dossiers de demande de révocation d'un certificat ;
- Vérification de l'identité et de l'habilitation du futur porteur de certificats ;
- Remise au futur porteur des supports cryptographiques pour utiliser les certificats correspondants ;

  - Déclenchement de la génération des certificats ;
  - Traitement de la révocation des certificats ;
  - Déclenchement des fonctions d'archivage des données.
- **Conditions Générales d'Utilisations ou CGU :** désigne les présentes CGU.
- **Porteur** : désigne le Porteur de certificat, personne physique identifiée dans le certificat ;
- **Mandataire de certification** : il s'agit de la personne physique ayant reçu mandat d'un futur porteur pour gérer le cycle de vie du certificat.
- **Certificat** : désigne la Clé publique d'un utilisateur à laquelle sont associées d'autres informations. Elle correspond à la clé privée délivrée par l'autorité de certification.
- **Opérateur d'enregistrement** : désigne l'opérateur de la DRH en charge du traitement des dossiers de demande de certificats.
- **Processus d'enregistrement** : désigne le processus d'enregistrement qui consiste à créer et gérer le dossier de demande de certificat.
- **Utilisateur :** désigne le porteur ou le mandataire de certification.
- **Contrat** : ensemble contractuel constitué des présentes CGU, du dossier de demande de certificat ainsi que de la Politique de Certification afférentes figurant à l'adresse suivante : https://spp.gouv.mc/services-administratifs applicables à la date de conclusion du contrat.
- **Données à caractère personnel / Données personnelles / Informations nominatives** : toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée »). Est réputée être une « personne physique identifiable » toute personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- **Politique de Certification ou PC** : la PC de l'AC Services Administratifs désigne le document établissant les principes qui s'appliquent à l'AC, aux personnes morales, aux Mandataires de certification et aux porteurs intervenant dans l'ensemble du cycle de vie d'un certificat, (consultable à l'adresse suivante : https://spp.gouv.mc/services-administratifs
  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 Services Administratifs : 2.16.492.1.1.1.1.5.1

3 POINT DE CONTACT

Les demandes d'informations relatives à la délivrance des certificats électroniques proposés par la DRH peuvent être réalisées :

- Par courrier postal :

Direction des Ressources Humaines et de la Formation de la Fonction Publique
3° étage - Stade Louis II - Entrée H
1 avenue des Castelans
BP 672
98014 MONACO CEDEX

- Par e-mail : esign-services-administratifs@gouv.mc

4 TYPES DE CERTIFICAT ET USAGES

Les certificats délivrés par la DRH aux Services de l'Etat sont :

- Les certificats de signature, délivrés sur carte à puce et permettant la signature électronique d'une personne physique représentant une personne morale (dans ce cas, les acteurs des Services de l'Etat) ;
- Les certificats d'authentification, délivrés sur carte à puce afin et permettant de s'authentifier sur le portail de gestion des demandes de certificats électroniques.
- Les certificats cachets qui pourront être délivrés sur une carte à puce ou transmis par e-mail au porteur (cachet serveur).

Les types de Certificats et usages sont décrits dans la PC de l'AC Services Administratifs.

5 LIMITE D'USAGE

Les Porteurs doivent respecter strictement les usages autorisés des bi-clés et des Certificats. Dans le cas d'une utilisation frauduleuse, leur 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 Porteur et du Certificat associé est strictement limitée au service défini par l'identifiant de sa PC.

Le Porteur reconnait 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 de l'AC Services Administratifs.

6 CONDITIONS D'OBTENTION ET D'UTILISATION DU CERTIFICAT

6.1 DEMANDE DE CERTIFICAT ET JUSTIFICATIFS A FOURNIR

Une demande de Certificat doit être faite auprès de l'AE DRH grâce à un dossier d'enregistrement.

Le Processus d'enregistrement consiste à créer et gérer le dossier de demande de Certificat.

L'enregistrement nécessite une prise de rendez-vous préalable avec un Opérateur d'enregistrement.

Les modalités de prise de rendez-vous auprès de la DRH ainsi que les formulaires de demande de Certificats en vigueur sont disponibles depuis la page suivante : https://spp.gouv.mc/services-administratifs

Tout futur porteur transmet les formulaires dûment complétés à la DRH via l'e-mail suivant : esign-services-administratifs@gouv.mc

Réception des formulaires PDFs par e-mail par l'Opérateur d'Enregistrement

Un agent de la DRH vérifie quotidiennement les demandes reçues sur l'adresse e-mail esign-services-administratifs@gouv.mc

Il vérifie la complétude des formulaires joints.

Les formulaires sont remplis directement sur le PDF afin que l'agent puisse aisément saisir les données dans l'outil du guichet en ligne.

Si un formulaire est incomplet ou absent il retourne la demande de compléments à l'expéditeur (par retour d'e-mail).

La durée d'archivage est de 7 ans après la date d'expiration du certificat. La durée de vie d'un certificat étant de 3 ans, la durée d'archivage maximale est de 10 ans.

6.2 TRAITEMENT DE LA DEMANDE

Vérification et validation de l'identité du porteur

- Le porteur présente son formulaire (papier) signé (avec la case CGUs cochée)
- La DRH valide l'identité du porteur en vérifiant :
    - la pièce d'identité du porteur (carte d'identité, passeport ou carte de séjour)
    - la légitimité du demandeur en consultant le registre des personnes habilitées à la signature électronique

En complément, la DRH peut vérifier le matricule du demandeur dans son outil métier (Site central) en le comparant avec le matricule indiqué dans le formulaire

- La DRH valide l'identité et la légitimité du porteur et est prête à produire la carte à puce contenant le certificat électronique de signature ou de cachet

Production de la carte

- La DRH produit la carte à puce contenant le certificat électronique

6.3 DELIVRANCE DES CERTIFICATS

- Délivrance des certificats par l'opérateur d'enregistrement en face à face au porteur
- Acceptation tacite du certificat par l'utilisateur (validation par l'utilisateur des certificats électroniques) *

*Le porteur dispose de 7 jours francs à compter de la remise pour vérifier le contenu des certificats qui lui ont été délivrés.

Pour cela, il est possible de lire ses certificats en utilisant un lecteur USB ainsi que le driver Safenet disponible au téléchargement sur le Centre Logiciel de tout poste d'un fonctionnaire ou agent de l'Etat.

Si le porteur revient vers l'AE et indique une erreur dans son ou ses certificats, l'opérateur générera un nouveau certificat.

- Signature du document de remise des certificats. Ce document est archivé dans le dossier porteur.

6.4 RECEPTION ET GENERATION DU CODE PIN ET DU CODE DE REVOCATION

- Dès la génération des certificats électroniques sur la carte à puce, trois actions se produisent :
    - un courrier papier contenant le code d'accès est immédiatement imprimé par l'opérateur d'enregistrement
    - un e-mail automatique contenant une URL d'activation est envoyé au porteur
    - un e-mail automatique contenant son code de révocation est également envoyé
- Le code d'accès aussi appelé code d'activation permet au porteur de générer son code PIN à 6 chiffres en cliquant sur l'URL indiquée dans l'e-mail qu'il a reçu. Un document PDF contenant le code PIN est alors généré, le porteur doit le conserver précieusement. (Il n'est pas possible de choisir ni de modifier son code PIN).

Informations importantes sur le code d'activation et le code PIN :

Tant que le porteur n'a pas activé le lien, l'opérateur d'après-vente peut renvoyer l'e-mail (uniquement à l'adresse e-mail qui est contenue dans le certificat).

Une fois que le porteur a saisi le code d'activation après avoir cliqué sur le lien, le porteur accède au lien de téléchargement du PDF contenant son code PIN. Il ne peut cliquer de nouveau sur le lien qui génère le PDF que pendant les 24h suivantes.

Si le porteur, muni de sa carte, saisit le code d'activation mais pas le code PIN comme il convient de le faire, il y a échec après 5 tentatives. Dans ce cas-là, l'opérateur d'enregistrement devra régénérer un certificat électronique sur une nouvelle carte à puce.

L'agent doit donc bien expliciter le processus d'activation et la distinction entre le code d'activation et le code PIN.

6.5 UTILISATION DU CERTIFICAT

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

Le Certificat contient :

- Le nom et le Prénom du Porteur ;
- Le numéro de série du Certificat ;
- Le numéro d'immatriculation dans le l'outil de référentiel du RCI ;
- Le rôle du Porteur au sein de l'Etat ;
- Le Nom du Service de l'Etat;
- Le pays ;
- L'Adresse e-mail professionnelle du Porteur.

6.6 GESTION DU CODE PIN ASSOCIE A LA CARTE A PUCE

Le Porteur s'engage à conserver le support quel qu'il soit et le code PIN associé sous son contrôle exclusif de manière à préserver l'intégrité et la confidentialité de sa clé privée.

En conséquence, le code PIN ne doit jamais être conservé en clair ni se trouver à proximité de la carte à puce.

Le code PIN ne doit jamais être divulgué sous aucun prétexte. Dans le cas du non-respect de cette obligation le Porteur assumerait l'entière responsabilité des conséquences induites sans recours possible contre la DRH.

6.7 RENOUVELLEMENT DES CERTIFICATS

Le Certificat est valable trois (3) ans.

Le Porteur et le Mandataire de certification sont avertis par l'AE de l'expiration proche de son Certificat par courriel 45, 30 et 15 jours avant l'expiration.

La procédure de traitement d'une demande de nouveau Certificat suit le même processus que lors du processus initial.

En cas de modifications apportées au corpus documentaire entre la délivrance du premier Certificat et celui lié au renouvellement, le Porteur en est informé et pourra les consulter sur le site dédié. En particulier, si les CGU ont changé, celles-ci sont communiquées au Porteur qui doit les accepter.

Dans tous les cas, les CGU doivent être lues et acceptées.

6.8 REVOCATION

Les causes possibles d'une révocation sont décrites dans la PC de l'AC Services Administratifs.

La demande de révocation doit être formulée dès connaissance de l'évènement correspondant.

Toute personne à l'origine d'une demande de révocation est authentifiée selon un processus propre à son statut notamment :

- le Porteur à l'aide de son code de révocation fourni au moment de la demande de Certificat, d'éléments présents dans le dossier d'enregistrement.
- Le Mandataire de certification à l'aide de son code de révocation fourni au moment de la demande de Certificat, d'éléments présents dans le dossier d'enregistrement.

- le Mandataire de certification sur la base d'une signature manuscrite par comparaison avec la signature présente dans son dossier d'enregistrement ;
- le porteur sur la base d'une signature manuscrite à l'aide d'un carton de signature.

En cas de perte du code de révocation :

- Le Porteur ou le Mandataire de certification peuvent contacter le service par téléphone.
- L'authentification de la personne par téléphone se fait par le biais des réponses aux 4 questions personnelles (parmi les 7) que le porteur aura renseignées lors du dépôt de son dossier d'enregistrement.
- En cas de demande réalisée en présentiel, l'authentification de la personne se fait par le biais de la présentation d'une pièce d'identité en cours de validité

A noter que le porteur ou le Mandataire de Certification peuvent, pour des raisons légitimes, demande la révocation du Certificat d'un porteur (licenciement, départ, départ en retraite, maladie, etc.).

Le traitement d'une demande de révocation par l'AC est tel que décrit dans la PC de l'AC Services Administratifs.

7 OBLIGATIONS

Obligations du Porteur et du Mandataire de certification :

Le Porteur a l'obligation de prendre toutes les mesures propres à assurer la sécurité de ses postes informatiques sur lesquels sont utilisés les supports (carte à puce). Lorsque la DRH fournit le support, ce dernier est conforme aux exigences de sécurité figurant aux chapitres afférents de la PC.

Le Porteur doit s'assurer d'utiliser une version toujours à jour de son logiciel Adobe Acrobat Reader DC.

Si une donnée communiquée par le Porteur ou le Mandataire de certification venait à évoluer (adresse e-mail…), celui-ci doit en informer l'AE sans délai afin de mettre à jour le dossier enregistré.

La connaissance de la compromission avérée ou soupçonnée des données confidentielles, du non-respect des présentes conditions générales, du décès du Porteur, ou de la modification des données contenues dans le Certificat, par le Porteur ou par la DRH, emporte obligation, à leur charge, de demander immédiatement et dans un délai inférieur à vingt-quatre (24) heures, la révocation du Certificat associé.

Le Porteur 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 Porteur ou le Mandataire de certification s'engage à vérifier l'usage indiqué dans le Certificat.

Tout destinataire d'un document signé par un Porteur 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 DRH ne pourra en aucun cas être engagée en cas de révocation du Certificat.

Obligations de l'AC :

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

8 RESPONSABILITE

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

De manière générale, l'Utilisateur s'engage à utiliser les Certificats :

- 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.

L'Utilisateur reconnaît et accepte que la responsabilité de la DRH ne peut être engagée au titre du service de certification, notamment en cas d'altération, de toute utilisation illicite ou préjudiciable à l'Utilisateur ou à un tiers du réseau par un tiers.

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

L'Utilisateur garantit à l'Administration qu'il est propriétaire des documents qu'il signe ou cachète 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 cachet ou la signature électronique d'un document ne respecte pas les conditions de signature ou de cachet pour ce type de document.

L'Utilisateur est seul responsable du cycle de vie des documents qu'il signe ou qu'il cachette : de leur établissement jusqu'au terme de la conservation.

L'Utilisateur 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 DRH, de l'évolution de la législation ou de tout autre motif jugé nécessaire. Il appartient à l'Utilisateur de s'informer desdites conditions.

9 LIMITES DE GARANTIES ET DE RESPONSABILITES

En aucun cas la DRH n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre les Utilisateurs desdits Certificats.

La DRH 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 DRH 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 DRH ne peut être engagée en cas de compromission de la clé privée. La DRH 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 DRH ne pourra être engagée dès lors que le Porteur 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 Porteur et du Mandataire de certification mentionnées 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.

La solution technique utilisée par la DRH pour la délivrance de certificats aux acteurs de l'Etat est la même que celle utilisée par la Direction de l'Expansion Economique pour la délivrance de certificats aux entreprises. Cette solution a fait l'objet d'une déclaration CCIN et d'une délibération favorable.

11 PROPRIETE INTELLECTUELLE

Les marques et/ou logos dont est titulaire la DRH, 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 solution technique utilisée par la DRH pour la délivrance de certificats aux acteurs de l'Etat est la même que celle utilisée par la Direction de l'Expansion Economique pour la délivrance de certificats aux entreprises. Cette solution a fait l'objet d'une déclaration CCIN et d'une délibération favorable.

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.