ASSEMBLÉE
DE LA
POLYNÉSIE FRANÇAISE

Commission du logement,
des affaires foncières, de l'économie
numérique, de la communication
et de l'artisanat

N° 88-2020

Papeete, le 16 SEP. 2020

RAPPORT

relatif à un projet de délibération relative à l'accomplissement de certaines formalités contractuelles par voie électronique et au coffre-fort numérique,

présenté au nom de la commission du logement, des affaires foncières, de l'économie numérique, de la communication et de l'artisanat,

par Mesdames les représentantes Monette HARUA et Joëlle FREBAULT

Monsieur le Président,
Mesdames, Messieurs les représentants,

Par lettre n° 4295/PR du 17 juillet 2020, le Président de la Polynésie française a transmis aux fins d'examen par l'assemblée de la Polynésie française, un projet de délibération relative à l'accomplissement de certaines formalités contractuelles par voie électronique et au coffre-fort numérique.

En Polynésie française, le cadre législatif et règlementaire de la dématérialisation est constitué de deux textes majeurs :

— La loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices ;

— La loi du pays n° 2017-31 du 2 novembre 2017 relative à l'accomplissement de certains formalités contractuelles par voie électronique et au coffre-fort numérique.

La loi du pays n° 2017-31 du 2 novembre 2017 vient compléter le code civil, tel qu'applicable en Polynésie française, de dispositions encadrant les formalités contractuelles par voie électronique[1], la possibilité de conclure un contrat par voie électronique étant déjà applicables.

Par ailleurs, elle introduit dans l'ordonnancement juridique polynésien, la possibilité de recourir au service de coffre-fort numérique qui permet d'archiver dans un espace sécurisé en ligne, des documents dématérialisés importants, énonçant la possibilité de conclure un contrat par voie électronique dans ce cadre.

La présente délibération vient préciser les exigences réglementaires découlant des principes instaurés par la loi du pays n° 2017-31 en matière de dématérialisation des échanges entre particuliers. Elle réunit, en les adaptant, les mesures réglementaires issues de différents décrets et arrêtés nationaux encadrant ce domaine.

[1] Échange d'informations préalables visant à permettre l'exécution de l'obligation d'information précontractuelle et envoi ou remise d'un écrit par voie électronique.

Le choix a été fait de ne pas suivre les évolutions intervenues en France et en Europe suite à l'entrée en vigueur du Règlement européen n° 910/2014 du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*, dit Règlement e-IDAS[2], compte tenu de son application récente et des évolutions qu'il connaitra sans doute prochainement face à l'évolution exponentielle des technologies et du marché.

Le projet de délibération est structuré autour de 6 titres :

— Le titre I regroupe les dispositions relatives à la signature électronique (*articles 1 à 7*) ;

— Le titre II aborde l'horodatage électronique (*articles 8 à 13*) ;

— Le titre III précise les règles applicables à l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat (*articles 14 à 16*) ;

— Le titre IV, au sein de l'article 17, permet d'évaluer et de certifier la sécurité offerte par les produits et les systèmes des technologies de l'information (*TIC*) ;

— Le titre V qui instaure au sein de l'article 18, une équivalence entre services de confiance qualifiés utilisés par l'administration et les particuliers ;

— Le titre VI énonce au sein d'un article unique l'abrogation de deux décrets nationaux, l'un relatif à la signature électronique et l'autre, à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des TIC.

I- L'instauration de présomptions de fiabilité et de conformité

La signature électronique d'un document garantit l'identité de son signataire et l'intégrité du document signé tandis que l'horodatage est un procédé qui fait foi dans le domaine des échanges électroniques permettant de garantir qu'un message existait à un instant donné.

Présomption de fiabilité de la signature et de l'horodatage électroniques

La délibération accorde à la signature et à l'horodatage électroniques une présomption de fiabilité (*articles 2 et 9*), sous réserve de respecter les exigences posées par la délibération.

Ainsi, la signature électronique est présumée fiable, jusqu'à preuve du contraire, lorsqu'elle est sécurisée, c'est-à-dire :

1. qu'elle est établie grâce à un dispositif sécurisé de création de signature électronique certifié conforme aux exigences sont listées à l'article 3
2. et que sa vérification repose sur l'utilisation d'un certificat électronique qualifié dont les exigences sont énumérées au I de l'article 5, délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II de l'article 5.

Un procédé d'horodatage est présumé fiable si le prestataire de services d'horodatage électronique qui met en œuvre ce procédé et le module d'horodatage utilisé satisfont respectivement aux exigences des articles 10 et 11.

Présomption de conformité des produits et systèmes des technologies de l'information

Peuvent être certifiés conformes aux exigences visées par la délibération :

– le dispositif de création de signature électronique (*matériel ou un logiciel destiné à mettre en application les données de création de signature électronique*) ;

– le dispositif de vérification de signature électronique (*matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique*) ;

[2] Electronic identification and trust services.

- et le module d'horodatage (*dispositif, matériel ou logiciel, comportant un module cryptographique et une horloge interne synchronisée avec une ou plusieurs sources de temps, et destiné à mettre en application les données nécessaires à la production d'une contremarque de temps, dont les données de signature de la contremarque de temps*).

La certification de conformité de ces trois dispositifs est délivrée par les autorités nationales et selon les procédures décrites par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits des technologies de l'information.

Quant au certificat électronique, qui est un document attestant du lien entre les données de vérification de signature électronique et le signataire, il ne peut être regardé comme qualifié que s'il est conforme aux exigences posées par la délibération et s'il est délivré par un prestataire de service de certification électronique.

La délibération prévoit qu'un arrêté pris en conseil des ministres fixera la liste de référence des produits et des systèmes des technologies de l'information certifiés par référence aux listes dressées par les autorités nationales.

La délivrance d'un certificat électronique et d'un module d'horodatage par des prestataires reconnus qualifiés entraîne pour eux une présomption de conformité aux exigences posées par la délibération.

La délibération prévoit qu'un arrêté en conseil des ministres viendra fixer les spécifications techniques et la liste de référence des prestataires de services de certification électronique et d'horodatage électronique par référence à la liste dressée par les autorités nationales. Il a en effet été jugé souhaitable que les procédures sur la base desquelles la reconnaissance des prestataires et des certificats qualifiés est faite soient reconnues par l'*European Telecommunications Standards Institute (ETSI)*. Cet institut européen des normes de télécommunications, est l'organisme de normalisation européen du domaine des télécommunications.

Un travail de fond a été mené par la direction générale de l'économie numérique sur l'identification et la sélection de ces prestataires de services (*près de 700 solutions d'authentification de serveur, de cachet électronique, de chiffrement, de signature électronique et d'horodatage ont été vérifiés*).

II- Les principes encadrant l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat

En complément de l'article L. 1369-8 intégré par la délibération n° 2017-31 du 2 novembre 2017 dans le code civil applicable en Polynésie française, les articles 14 à 16 de la délibération :

- précisent l'obligation imposée à l'expéditeur d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat de recueillir au préalable le consentement du destinataire ;
- instaurent une présomption de garantie de l'identité du destinataire dès indication de son adresse électronique à l'expéditeur ;
- instaurent une présomption de fiabilité des date et heures d'expédition et d'acceptation, de refus ou d'absence de prise de connaissance par le destinataire, de la lettre recommandée lorsque le procédé électronique employé satisfait aux exigences posées par la délibération en matière d'horodatage.

III- L'instauration d'une équivalence entre services de confiance qualifiés

Il est proposé à l'article 18 de fixer une équivalence avec les procédés d'horodatage électronique qualifiés prévus par le référentiel général de sécurité (*RGS*) instauré par la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices.

Le RGS fixe en effet les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité, d'intégrité et d'horodatage. Il sera donc modifié afin de prévoir une telle équivalence.

L'arrêté d'application de la délibération fixera notamment la norme AFNOR NF Z42-020 qui permettra d'apporter une présomption de conformité au respect des exigences prévues par la loi du pays n° 2017-31 du 2 novembre 2017 relative à l'accomplissement de certains formalités contractuelles par voie électronique et au coffre-fort numérique.

*****

Examiné en commission le 18 septembre 2020, le projet de délibération relative à l'accomplissement de certaines formalités contractuelles par voie électronique et au coffre-fort numérique a recueilli un vote favorable unanime des membres de la commission.

En conséquence, la commission du logement, des affaires foncières, de l'économie numérique, de la communication et de l'artisanat propose à l'assemblée de la Polynésie française d'adopter le projet de délibération ci-joint.

LES RAPPORTEURES

Monette HARUA **Joëlle FREBAULT**

ASSEMBLÉE
DE LA
POLYNÉSIE FRANÇAISE

NOR : ADN2021038DL-4

DÉLIBÉRATION N° /APF

DU

---

relative à l'accomplissement de certaines formalités contractuelles par voie électronique et au coffre-fort numérique

---

L'ASSEMBLÉE DE LA POLYNÉSIE FRANÇAISE

Vu la loi organique n° 2004-192 du 27 février 2004 modifiée portant statut d'autonomie de la Polynésie française, ensemble la loi n° 2004-193 du 27 février 2004 modifiée complétant le statut d'autonomie de la Polynésie française ;

Vu la loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique ;

Vu le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Vu le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

Vu le décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat ;

Vu la loi du pays n° 2017-31 du 2 novembre 2017 relative à l'accomplissement de certaines formalités contractuelles par voie électronique et au coffre-fort numérique ;

Vu l'arrêté n° 1073 CM du 17 juillet 2020 soumettant un projet de délibération à l'assemblée de la Polynésie française ;

Vu la lettre n° /2020/APF/SG du portant convocation en séance des représentants à l'assemblée de la Polynésie française ;

Vu le rapport n° du de la commission du logement, des affaires foncières, de l'économie numérique, de la communication et de l'artisanat ;

Dans sa séance du

A D O P T E :

TITRE I - DE LA SIGNATURE ÉLECTRONIQUE

Article 1er.- Au sens de la présente délibération, on entend par :

1. Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;

2. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :

   - être propre au signataire ;

   - être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

   - garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;

3. Signataire : toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique ;

4. Données de création de signature électronique : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;

5. Dispositif de création de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;

6. Dispositif sécurisé de création de signature électronique : un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 ;

7. Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;

8. Dispositif de vérification de signature électronique : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;

9. Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;

10. Certificat électronique qualifié : un certificat électronique répondant aux exigences définies à l'article 5 ;

11. Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;

12. Qualification des prestataires de services de certification électronique : l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Article 2.- La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

CHAPITRE I - DES DISPOSITIFS SÉCURISÉS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE

Article 3.- Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est certifié conforme à ces exigences dans les conditions prévues au II.

I. - Un dispositif sécurisé de création de signature électronique doit :

1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :

   a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;

   b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;

   c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

II. - Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I dans les conditions prévues au titre IV de la présente délibération.

CHAPITRE II - DES DISPOSITIFS DE VÉRIFICATION DE SIGNATURE ÉLECTRONIQUE

Article 4.- Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies au titre IV de la présente délibération, s'il répond aux exigences suivantes :

a) Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en œuvre le dispositif et qui est dénommée vérificateur ;

b) Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci et le résultat de cette vérification doit, sans subir d'altération, être porté à la connaissance du vérificateur ;

c) Le vérificateur doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;

d) Les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette vérification doit, sans subir d'altération, être porté à la connaissance du vérificateur ;

e) L'identité du signataire doit, sans subir d'altération, être portée à la connaissance du vérificateur ;

f) Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement portée à la connaissance du vérificateur ;

g) Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.

CHAPITRE III - DES CERTIFICATS ÉLECTRONIQUES QUALIFIÉS ET DES PRESTATAIRES DE SERVICES DE CERTIFICATION ÉLECTRONIQUE

Article 5.- Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II.

I. - Un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) L'identité du prestataire de services de certification électronique ainsi que l'État dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

II. - Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :

a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;

b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;

c) Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;

d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;

e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;

f) Appliquer des procédures de sécurité appropriées ;

g) Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;

h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;

i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;

j) Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;

k) Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique ;

l) Utiliser des systèmes de conservation des certificats électroniques garantissant que :

- l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;

- l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;

- toute modification de nature à compromettre la sécurité du système peut être détectée ;

m) Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;

n) S'assurer au moment de la délivrance du certificat électronique :

- que les informations qu'il contient sont exactes ;

- que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;

o) Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un certificat électronique :

- des modalités et des conditions d'utilisation du certificat ;

- du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique mentionnée à l'article 7 ;

- des modalités de contestation et de règlement des litiges ;

p) Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au o qui leur sont utiles.

Un arrêté pris en Conseil des Ministres fixe la liste des spécifications techniques relatives aux prestataires de services de certification en vue de la reconnaissance de leur qualification.

Article 6.- Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 5 peuvent demander à être reconnus comme qualifiés.

Cette qualification, qui vaut présomption de conformité auxdites exigences, correspond à la qualification délivrée par les autorités de métropole en application du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

Un arrêté pris en Conseil des Ministres précise les modalités d'application du présent article et fixe la liste de référence des prestataires de services de certificat électronique qualifiés par référence à la liste dressée par les autorités nationales dans le cadre de la mise en œuvre du décret mentionné au précédent alinéa.

Article 7.- Au titre de la déclaration de fourniture de prestations de cryptologie effectuée conformément aux dispositions de l'article 31 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, le prestataire de services de certification électronique doit, quand il entend délivrer des certificats électroniques qualifiés, l'indiquer.

TITRE II - DE L'HORODATAGE ÉLECTRONIQUE

Article 8.- Au sens de la présente délibération, on entend par :

1° Source de temps fiable : ensemble de moyens permettant de fournir une date reconnue comme fiable selon les normes internationales en vigueur ;

2° Procédé d'horodatage électronique : mécanisme associant une représentation d'une donnée à un temps particulier et attestant de l'existence de la représentation de cette donnée à cet instant au moyen d'une contremarque de temps ;

3° Contremarque de temps : donnée sous forme électronique liant une représentation d'une donnée à un temps particulier et attestant de l'existence de la représentation de cette donnée à cet instant. La contremarque de temps comporte un cachet du prestataire de services d'horodatage électronique établi à l'aide des données de signature de la contremarque de temps ;

4° Prestataire de services d'horodatage électronique : personne en charge de la production et de la délivrance de contremarques de temps ;

5° Cachet d'une contremarque de temps : donnée sous forme électronique permettant d'identifier le prestataire de services d'horodatage électronique qui la délivre et d'assurer un lien avec la contremarque de temps à laquelle il s'attache. Le cachet d'une contremarque de temps satisfait aux obligations suivantes :

a) Être propre au prestataire de services d'horodatage électronique ;

b) Être créé par des moyens que le prestataire de services d'horodatage électronique peut garder sous son contrôle exclusif ;

c) Garantir avec la contremarque de temps à laquelle il s'attache un lien tel que toute modification ultérieure de la contremarque de temps est détectable ;

6° Données de signature d'une contremarque de temps : éléments propres au prestataire de services d'horodatage électronique, tels que des clés cryptographiques privées, utilisés pour créer un cachet d'une contremarque de temps ;

7° Module d'horodatage : dispositif, matériel ou logiciel, comportant un module cryptographique et une horloge interne synchronisée avec une ou plusieurs sources de temps, et destiné à mettre en application les données nécessaires à la production d'une contremarque de temps, dont les données de signature de la contremarque de temps ;

8° Données de vérification d'une contremarque de temps : éléments tels que des clés cryptographiques publiques, utilisés pour vérifier le cachet d'une contremarque de temps ;

9° Certificat d'horodatage : document sous forme électronique attestant du lien entre les données de vérification de la contremarque de temps et le prestataire de services d'horodatage électronique ;

10° Abonné : personne physique ou morale bénéficiant, selon des conditions définies et acceptées, d'un service d'horodatage électronique assuré par un prestataire de services d'horodatage électronique ;

11° Utilisateur : personne physique ou morale, dont l'abonné, qui se fie à une contremarque de temps.

CHAPITRE I - HORODATAGE ÉLECTRONIQUE FIABLE

Article 9.- En application des articles 1369-7 et 1369-8 du code civil, un procédé d'horodatage électronique est présumé fiable si le prestataire de services d'horodatage électronique mettant en œuvre ce procédé et le module d'horodatage utilisé satisfont aux exigences fixées au présent chapitre.

Article 10.- Le prestataire de services d'horodatage électronique se conforme aux exigences suivantes :

1° Disposer de personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services d'horodatage électronique ;

2 Appliquer des procédures de sécurité appropriées ;

3° Utiliser des systèmes et des produits assurant la sécurité technique et cryptographique des fonctions qu'ils assurent, notamment un module d'horodatage satisfaisant aux exigences de l'article 11 de la présente délibération ;

4° Assurer que l'horloge interne du module d'horodatage est synchronisée avec une ou plusieurs sources de temps fiable selon les performances garanties par le prestataire de services d'horodatage électronique et cesser de délivrer des contremarques de temps en cas de désynchronisation en dehors des performances garanties ;

5° Prendre toute disposition propre à prévenir la falsification des contremarques de temps ;

6° Disposer d'un certificat d'horodatage ;

7 Conserver toutes les informations relatives au fonctionnement du service d'horodatage électronique et utiles à la manifestation de la preuve d'une date selon des règles appropriées de confidentialité et d'intégrité ;

8° Mettre à disposition des utilisateurs et des abonnés par les moyens les plus appropriés les informations suivantes :

a) Ses coordonnées permettant d'entrer en contact rapidement et de communiquer directement avec lui ;

b) Les conditions générales d'utilisation des services d'horodatage électronique ;

c) Les conditions générales de vérification des contremarques de temps et notamment le certificat d'horodatage ;

d) Les performances garanties et notamment la précision de la date des contremarques de temps et l'échelle de temps utilisée ;

e) Les principales caractéristiques techniques des dispositifs utilisés et les procédures qu'il met en place ;

f) Le cas échéant la mention de la qualification visée à l'article 13 de la présente délibération ;

g) Les voies ouvertes pour les réclamations et le règlement des litiges ;

9° Avoir défini un plan de cessation d'activité permettant de garantir la continuité du service de vérification des contremarques de temps émises ; en particulier, en cas de cessation d'activité le prestataire de services d'horodatage électronique doit informer préalablement les utilisateurs de cette cessation et des conditions dans lesquelles sera assurée la continuité du service de vérification des contremarques de temps ;

10° Publier sans délai tout événement affectant la fiabilité des contremarques de temps émises ;

11° Être capable de démontrer le respect des exigences précitées.

Un arrêté pris en Conseil des Ministres fixe la liste des spécifications techniques relatives aux prestataires de services d'horodatage électronique en vue de la reconnaissance de leur qualification.

Article 11.- Le module d'horodatage satisfait aux exigences suivantes :

1° Délivrer des contremarques de temps comportant chacune, selon les règles et normes en vigueur, au moins les éléments suivants :

a) La représentation de la donnée horodatée ;

b) La valeur du temps au moment de sa production ;

c) Le cachet de la contremarque de temps ;

2° Générer des données de signature des contremarques de temps du prestataire de services d'horodatage électronique, garantir que cette production peut être réalisée exclusivement par des personnes autorisées et empêcher toute importation ou exportation de ces données ;

3° Assurer, par des moyens techniques et des procédures appropriés, la confidentialité et l'intégrité des données de signature des contremarques de temps du prestataire de services d'horodatage électronique durant tout le cycle de vie de ces données et permettre la destruction sûre de ces mêmes données en fin de vie ;

4° Assurer, par des moyens techniques appropriés, la fiabilité de la synchronisation de l'horloge interne avec une ou plusieurs sources de temps fiables ;

5° Être capable d'identifier et d'authentifier les personnes accédant au module d'horodatage ;

6° Contrôler l'accès aux composantes du module d'horodatage selon l'identité et la fonction des personnes ;

7° Détecter toute compromission ou tentative de compromission et d'altérations physiques à l'encontre du module cryptographique et entrer dans un état sûr lorsque de telles tentatives sont détectées sur la protection des données de signature de contremarque de temps ;

8° Être capable de mener une série de tests pour vérifier que le module cryptographique fonctionne correctement et entrer dans un état sûr si ce module cryptographique détecte une erreur ;

9° Créer des enregistrements d'audit pour chaque modification concernant la sécurité du module cryptographique et la synchronisation de l'horloge interne avec une ou plusieurs sources de temps fiables ;

10° Permettre de créer un cachet de contremarque de temps qui ne révèle pas les données de signature de contremarque de temps du prestataire de services d'horodatage électronique et qui ne peut pas être falsifié sans la connaissance de ces données.

CHAPITRE II - CERTIFICATION DU MODULE D'HORODATAGE ET QUALIFICATION DES PRESTATAIRES DE SERVICES D'HORODATAGE ÉLECTRONIQUE

Article 12.- Le module d'horodatage peut être certifié conforme aux exigences définies à l'article 11 dans les conditions prévues au titre IV de la présente délibération.

Article 13.- Les prestataires de services d'horodatage électronique peuvent obtenir une qualification qui vaut présomption de conformité aux exigences fixées à l'article 10 et dont le module d'horodatage est certifié conforme dans les conditions fixées par l'article 12.

Cette qualification correspond à la qualification délivrée par les autorités de métropole en application du décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat.

Un arrêté pris en Conseil des Ministres précise les modalités d'application du présent chapitre et fixe la liste de référence des prestataires de services d'horodatage électronique par référence à la liste dressée par les autorités nationales dans le cadre de la mise en œuvre du décret mentionné au précédent alinéa.

TITRE III - DE L'ENVOI D'UNE LETTRE RECOMMANDÉE PAR COURRIER ÉLECTRONIQUE POUR LA CONCLUSION OU L'EXÉCUTION D'UN CONTRAT

Article 14.- L'expéditeur doit avoir recueilli le consentement du destinataire non professionnel à recevoir une lettre recommandée électronique, préalablement à son dépôt auprès du tiers acheminer, entendu au sens de la personne en charge de l'acheminement d'une lettre recommandée électronique conformément à la présente délibération.

Article 15.- L'indication de l'adresse électronique par le destinataire à l'expéditeur apporte une présomption de garantie de l'identité du destinataire.

Article 16.- Dans le cas d'une distribution d'une lettre recommandée par voie électronique, la fiabilité de la date et de l'heure d'expédition et de la date et de l'heure à laquelle le destinataire a accepté ou refusé de recevoir la lettre recommandée électronique ou l'absence de prise de connaissance de celle-ci, est présumée jusqu'à preuve du contraire, lorsque le procédé électronique employé satisfait aux exigences fixées au titre II de la présente délibération.

TITRE IV - DE L'ÉVALUATION ET DE LA CERTIFICATION DE LA SÉCURITÉ OFFERTE PAR LES PRODUITS ET LES SYSTÈMES DE TECHNOLOGIES DE L'INFORMATION

Article 17.- Les produits ou systèmes des technologies de l'information peuvent être certifiés conformes aux exigences visées par la présente délibération.

Cette certification correspond à la certification délivrée par les autorités de métropole dans les conditions du décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Un arrêté pris en Conseil des Ministres précise les modalités d'application du présent titre et fixe la liste de référence des produits et des systèmes des technologies de l'information certifiés par référence aux listes dressées par les autorités nationales dans les conditions du décret mentionné au précédent alinéa.

TITRE V - ÉQUIVALENCES ENTRE SERVICES DE CONFIANCE QUALIFÉS

Article 18.- Le procédé d'horodatage électronique présumé fiable au sens de la présente délibération est équivalent au procédé d'horodatage électronique qualifié au sens du référentiel général de sécurité, visé à l'article LP 20 de la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices.

TITRE VI - DISPOSITIONS FINALES

Article 19.- La présente délibération abroge les dispositions du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique et du décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information telles qu'applicables en Polynésie française.

Article 20.- Le Président de la Polynésie française est chargé de l'exécution de la présente délibération qui sera publiée au *Journal officiel* de la Polynésie française.

La secrétaire, *Le président,*

Béatrice LUCAS Gaston TONG SANG