CERTIFICATS ÉMIS PAR L'AC « CERTIGNA ENTITY CA »

1. OBJET

Les présentes conditions ont pour objet de préciser les modalités de demande et d'utilisation d'un certificat « Certigna Entity CA », proposé à un futur RC et/ou à un RC, ainsi que les engagements et obligations respectifs des parties liées aux présentes. Les conditions générales d'utilisation découlent de la Politique de Certification identifiée par l'OID 1.2.250.1.177.2.6.1 disponible à l'adresse : http://politique.certigna.fr/PCcertignaentityca.pdf. Les certificats couverts par cette Politique de certification et les présentes conditions ont les OID suivants :

- Cachet pour la signature de mails et de documents
  - RGS * + LCP : 1.2.250.1.177.2.6.1.1.1
  - RGS ** + QCP-l-qscd : : 1.2.250.1.177.2.6.1.4.1
  - QCP-l-qscd : 1.2.250.1.177.2.6.1.41.1
  - RGS **: 1.2.250.1.177.2.6.1.42.1
- Cachet pour la signature de jetons d'horodatage
  - RGS * + LCP : 1.2.250.1.177.2.6.1.3.1
  - RGS ** + QCP-l-qscd : 1.2.250.1.177.2.6.1.6.1

2. DÉFINITIONS

- **AC** : Autorité de Certification « Certigna Entity CA » de la société DHIMYOTIS, délivrant le CERTIFICAT ;
- **AC RACINE** : Autorité de plus haut niveau de l'IGC Certigna qui certifie les AC EMETTRICES ;
- **AC EMETTRICE** : Autorité dont le certificat a été signé par l'AC RACINE. L'AC est une autorité émettrice dans l'IGC Certigna ;
- **AE** : Autorité d'Enregistrement de la société DHIMYOTIS, contrôlant les demandes de CERTIFICAT et les éventuelles demandes de REVOCATION ;
- **AUTORITE D'ENREGISTREMENT DELEGUEE (AED)** : Entité tierce externe à l'IGC avec laquelle DHIMYOTIS a conclu un contrat de délégation par lequel il sous-traite une partie de l'activité de l'AE, à savoir, la collecte et le contrôle des dossiers d'enregistrement, l'identification des demandeurs de CERTIFICAT et la soumission des demandes de REVOCATION ;
- **CACHET** : Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières ;
- **CERTIFICAT** : Certificat électronique constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations sur le service de CACHET dont est responsable le RC.
- **CONTRAT** : Relations entre l'AC et le RC ;
- **DEMANDE DE CERTIFICAT** : Ensemble constitué du formulaire de demande signé (acceptant les présentes conditions générales d'utilisation) accompagné des pièces justificatives, et de la requête générée informatiquement ;
- **LCR** : Liste des Certificats Révoqués ;
- **MANDATAIRE DE CERTIFICATION (MC)** : Personne désignée et placée sous la responsabilité de l'entité cliente. Elle est en relation directe avec l'AE et assure pour elle un certain nombre de vérifications concernant l'identité, éventuellement les attributs des porteurs de cette entité ;
- **OID** : Identifiant d'objet (Object IDentifier) ;
- **RC** : Personne physique en charge et responsable du CERTIFICAT utilisé pour le service applicatif de CACHET et de la clé privée associée ;
- **REVOCATION** : Opération consistant à anticiper la fin de validité d'un CERTIFICAT initialement prévue et dont la date est inscrite dans le CERTIFICAT ;
- **SUPPORT CRYPTOGRAPHIQUE** : Token au format clé USB ou carte à puce ou module cryptographique ;
- **UTILISATEUR** : Utilisateur d'un CERTIFICAT. Il peut s'agir de :
  - Un usager destinataire de données signées par un service applicatif de CACHET et qui utilise le CERTIFICAT ainsi qu'un module de vérification de CACHET afin d'authentifier l'origine de ces données transmises.
  - Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le CERTIFICAT et un module de vérification de CACHET afin d'authentifier l'origine de ces données transmises.
  - Un service applicatif qui signe des données électroniques.

3. CONFORMITÉ

LE CERTIFICAT est émis en conformité avec :

- Les exigences de la PC Type « *Certificats électroniques de Services Applicatifs* » pour un usage de cachet aux niveaux * et ** du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Le règlement européen eIDAS et les niveaux LCP de l'ETSI EN 319 411-1 pour un cachet LCP et QCP-l-qscd de l'EN 319 411-2 pour un cachet qualifié eIAS QCP-l-qscd ;
- Les exigences du document « Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates » du CA/BROWSER FORUM.

4. DURÉE

Le CONTRAT est conclu pour une durée choisie par le futur RC (3 ans maximum) et démarre le jour de la délivrance du CERTIFICAT par l'AE.

5. TARIF

Sauf accord écrit et préalable de l'AC, les conditions tarifaires et de paiement sont les suivantes :

- Le prix de vente du CERTIFICAT est celui fixé dans la grille tarifaire disponible sur demande auprès du service commercial de Certigna,
- Le prix de vente du CERTIFICAT est à payer lors de la DEMANDE DE CERTIFICAT par l'un des moyens suivants :
  - carte bancaire sur le site https://certigna.fr ;
  - virement bancaire, en joignant le récépissé fourni par la banque ;
  - chèque libellé à l'ordre de DHIMYOTIS,
  - espèces pour tout montant n'excédant pas 1000 Euros ;
  - mandat administratif, pour les établissements publics uniquement, en joignant un bon de commande au nom de l'Établissement.
- La REFABRICATION d'un CERTIFICAT logiciel est gratuite durant les 3 mois qui suivent la délivrance du CERTIFICAT par l'AC ;
- Le DEBLOCAGE du SUPPORT CRYPTOGRAPHIQUE dans lequel est fourni le CERTIFICAT est une prestation facturée ;

Sauf accord écrit et préalable de l'AC, tout CERTIFICAT dont le prix de vente n'a pas été payé intégralement, pourra soit ne pas être délivré, soit être révoqué après sa délivrance par l'AC. Conformément à l'article L.441-6 du Code de commerce, en cas de non-paiement à la date d'échéance indiquée sur la facture, sans obligation d'envoi d'une relance, seront appliquées des pénalités de retard calculées au taux de 3 fois le taux d'intérêt légal en vigueur au jour d'exigibilité de la facture, ainsi qu'une indemnité forfaitaire de 40€ pour frais de recouvrement.

6. OBLIGATIONS DU RC

Le RC a le devoir de :

- Effectuer sa demande de CERTIFICAT en suivant toutes les étapes de la procédure figurant sur le site https://www.certigna.fr.
- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du CERTIFICAT ;
- Transmettre à l'AE, le cas échéant à l'AED, ou à un MC de son entité, en main propre ou par voie postale, le formulaire d'inscription généré lors de la demande de CERTIFICAT en ligne sur le site https://www.certigna.fr, le paiement, ainsi que les pièces justificatives.
- Générer la bi-clé associée au CERTIFICAT dans un dispositif ou SUPPORT CRYPTOGRAPHIQUE conforme aux exigences du chapitre 11 de la Politique de Certification « CERTIGNA ENTITY CA » et qui est :
  - pour les cachets QCP-l-qscd, qualifié « QSealCD » par l'ANSSI;
    Dans le cas où le dispositif est géré par un Prestataire de Service de Confiance autre que Certigna, le Responsable de Certificat devra fournir lors de la demande, les justificatifs (Ex : Attestation de qualification en tant qu'Opérateur de certification, attestation de qualification en tant que PSCE pour le niveau QCP-l-QSCD et accord contractuel signée associé entre l'entité et ce prestataire, etc.) attestant que ce prestataire est en capacité de répondre aux exigences de la Politique de Certification et notamment du chapitre 11.
  - pour les cachets RGS ** et * :
    - Soit un dispositif matériel de type carte à puce ou module cryptographique qualifié par l'ANSSI ;
    - Soit une solution logicielle respectant les exigences du chapitre 11.1 de la Politique de Certification via la mise en place de mesures de sécurité additionnelles propres à l'environnement dans lequel est déployé la clé privée. Cet environnement dans lequel est déployée la clé privée doit avoir fait l'objet d'un audit de sécurité.

Des justificatifs attestant que le dispositif est bien conforme aux exigences du chapitre 11 de la Politique de Certification (A minima la facture d'achat du dispositif et des photos/impressions d'écran des caractéristiques matérielles et logicielles du dispositif et du numéro de série associé) doivent être fournis lors de la demande par le RC permettant d'attester de la détention du dispositif par le Responsable du Certificat. L'AC se réserve le droit de refuser la demande de certificat s'il était avéré que ce dispositif ne réponde pas à ces exigences.

L'AC consigne les caractéristiques du dispositif, qu'il soit ou non élaboré par l'AC et contrôle mensuellement jusqu'au terme de la période de validité du certificat de l'entité, le maintien du statut de certification du dispositif. En cas de perte de la certification du dispositif, l'AC demandera au Responsable du Certificat les preuves attestant que la bi-clé est stockée dans un dispositif répondant aux exigences du chapitre 11. Le Responsable de Certificat s'engage à fournir ces preuves (Ex : Facture d'achat d'un nouveau dispositif certifié QSCD, Procès-verbal de cérémonie des clés en cas de migration des clés, Procès-verbal de mise à jour du dispositif pour le maintien de la certification, etc.) dans un délai de 15 jours suivants la demande. Dans le cas où aucune preuve ne seraient fournies ou que ces dernières ne permettraient pas de déterminer si les conditions de

stockage de la bi-clé, et de transfert dans un autre dispositif le cas échéant, répondent aux exigences de la Politique de Certification, l'AC se donne le droit de révoquer le certificat.
- Informer l'AE en cas de non réception d'un e-mail confirmant la prise en compte de sa demande de CERTIFICAT ou de REVOCATION.
- Suite à la réception d'un e-mail de l'AE signalant la non-conformité de la demande ou que le dossier est incomplet, d'effectuer les modifications sous 7 jours calendaires après la réception de cet e-mail.
- Télécharger son certificat dans les 30 jours qui suivent la validation de son dossier qui est notifiée par e-mail au RC. Au-delà de ce délai, le CERTIFICAT est révoqué automatiquement par l'AE ;
- Accepter explicitement le CERTIFICAT depuis son espace client CERTIGNA lors de la procédure de téléchargement du CERTIFICAT ou bien par courrier papier signé par le RC sur demande expresse de l'AE. En cas de non-acceptation explicite, le certificat est automatiquement révoqué par l'AE ;
- Protéger la clé privée associée au CERTIFICAT de CACHET dont il a la responsabilité par des moyens appropriés à son environnement ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du service applicatif de CACHET ;
- Respecter les conditions d'usages du CERTIFICAT et de la clé privée associée citées au chapitre 10 de ce document ;
- Informer l'AC de toute modification concernant les informations contenues dans le CERTIFICAT ;
- Faire, sans délai, une demande de révocation du CERTIFICAT dont il est responsable auprès de l'AE, de l'AED auprès de laquelle la DEMANDE DE CERTIFICAT a été effectuée ou le cas échéant du MC de l'entité, lorsque l'une des causes de révocation du chapitre 9 est rencontrée.
- Sauvegarder la clé privée associée au CERTIFICAT. Si elle est stockée sur disque dur, il doit créer, pour sa protection, un mot de passe complexe (c'est-à-dire constitué d'une combinaison de 8 caractères minimum parmi chiffres, lettres minuscules et majuscules, et caractères spéciaux).
- Prendre toutes les mesures propres à s'assurer la sécurité du ou des ordinateurs sur lesquels est installé le CERTIFICAT. Le RC est le seul responsable de l'installation du CERTIFICAT
- Ne plus utiliser un CERTIFICAT et à supprimer la bi-clé associée suite à l'expiration ou la révocation de ce CERTIFICAT ;
- Informer l'AE de son départ de l'entité ou de son changement de responsabilités et du besoin d'enregistrer un nouveau RC.

7. OBLIGATIONS DE L'AC ET DE L'AE

L'AC est tenue à une obligation de moyens pour toutes les obligations relatives à la gestion du cycle de vie du CERTIFICAT qu'elle émet. L'AC s'engage à :
- Pouvoir démontrer, aux utilisateurs du CERTIFICAT, qu'elle a émis le CERTIFICAT pour un service applicatif de CACHET donné et que le RC correspondant a accepté le CERTIFICAT ;
- Prendre toutes les mesures raisonnables pour s'assurer que les RC sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.
- Fournir un service de maintenance technique par téléphone aux heures ouvrées;
- Fournir un service de consultation en ligne sur le site https://www.certigna.fr permettant à tout moment aux tiers de vérifier la validité du CERTIFICAT émis par l'AC (cf. chapitre 12).
- Réaliser toute collecte et tout usage de données à caractère personnel dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, notamment par rapport à la CNIL et à l'article 226-13 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002) du Code Pénal.

L'AE s'engage à :
- Vérifier et à valider les dossiers de demande et de révocation de CERTIFICAT ;
- Générer et mettre à la disposition du RC le CERTIFICAT dans un délai de 30 jours dans le cas où la demande de CERTIFICAT est conforme et le dossier de demande complet.
- Révoquer le certificat sous 24 heures dans le cas où la demande de REVOCATION est conforme et le demandeur est authentifié et autorisé.

8. PUBLICATION DES CERTIFICATS

Le CERTIFICAT du PORTEUR ne fait pas l'objet de publication.

9. RÉVOCATION

Les principales causes de révocation possibles sont les suivantes :
- Le RC, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service et/ou de son support) ;
- Le représentant légal de l'entité à laquelle il appartient informe l'AC que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- Le RC n'a pas respecté les Conditions Générales d'Utilisation du certificat ou l'AC obtient la preuve que l'usage du certificat est détourné ;
- L'AC est informée que le RC a violé une ou plusieurs de ses obligations en vertu des Conditions Générales d'Utilisation ;
- L'AC est informée de toute circonstance indiquant que l'utilisation d'une information dans le certificat n'est plus autorisée légalement ;
- Les informations du service figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple, modification de l'identité ou de la fonction du service), ceci avant l'expiration normale du certificat ;
- Le RC, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC ou de la DPC ;
- L'AC détecte que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;
- L'AC cesse ses activités pour quelque raison que ce soit et n'a pas pris de dispositions pour qu'une autre AC assure le relai en cas de révocation du certificat ;
- Le droit de l'AC pour émettre des certificats sous ces exigences expire ou est révoqué ou est terminé, à moins que l'AC n'ait pris des dispositions pour maintenir la publication des CRL/OCSP ;
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats en cours de validité signés par la clé privée correspondante) ;
- Le contenu ou le format des certificats présente un risque inacceptable pour les fournisseurs de logiciels applicatifs ou les utilisateurs ;
- L'arrêt définitif du service ou la cessation d'activité de l'entité du RC de rattachement du serveur ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
- Pour des raisons techniques (échec de l'envoi du certificat, …).

La demande de révocation peut être effectuée par :
- Le RC, un représentant légal de l'entité de rattachement du service applicatif de CACHET, ou le cas échéant un MC de cette entité ;
- L'AC ou l'AE.

La demande de révocation peut être effectuée :
- Par courrier signé, accompagné de la photocopie d'une pièce d'identité officielle du demandeur ;
- En ligne, sur le site https://www.certigna.fr depuis l'espace client du RC ou du MC le cas échéant.

10. CONDITIONS D'USAGE DU CERTIFICAT ET DE LA CLÉ PRIVÉE ASSOCIÉE

- Pour le cachet pour la signature de mails et de documents, les usages sont la signature électronique de données et la vérification de signature électronique. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un mail, un document ou encore une archive.
- Pour le cachet pour la signature de jeton d'horodatage, les usages sont la signature électronique de jeton d'horodatage et la vérification de signature électronique.

Le CERTIFICAT est utilisé par des applications pour lesquelles les besoins de sécurité sont moyen (cachet *) ou forts (cachet **) eu égard aux risques qui les menacent. En cas de non-respect de ces usages, la responsabilité du RC ou de l'entité à laquelle le service applicatif de CACHET est rattachée pourrait être engagée.

11. OBLIGATIONS DES UTILISATEURS

Les UTILISATEURS doivent :
- Respecter les usages autorisés du CERTIFICAT et de la clé privée associée. Dans le cas contraire, leur responsabilité pourrait être engagée.
- Vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante via les moyens offerts pour la vérification des certificats cités ci-dessous.
- Si le certificat de l'AC racine Certigna n'est pas installé sur le poste de l'UTILISATEUR, ce dernier doit le Télécharger à partir du site https://www.certigna.fr , précisément aux adresses suivantes :
  - http://autorite.certigna.fr/ACcertignarootca.crt ;
  - http://autorite.dhimyotis.com/ACcertignarootca.crt.

  Le certificat de l'AC peut être téléchargé depuis les adresses suivantes :
  - http://autorite.certigna.fr/entityca.crt ;
  - http://autorite.dhimyotis.com/entityca.crt.

12. MOYENS OFFERTS POUR LA VÉRIFICATION DES CERTIFICATS

Afin de vérifier la chaîne de certification, l'UTILISATEUR d'un CERTIFICAT peut télécharger les certificats d'autorité (AC RACINE et AC EMETTRICES) depuis le site :

https://www.certigna.fr. Le certificat d'AUTORITE RACINE peut être déjà installé sur le poste de travail de l'UTILISATEUR suivant la configuration logicielle de ce dernier. Afin de vérifier le statut de REVOCATION d'un CERTIFICAT, l'AC publie de façon périodique la LCR et offre un service d'information sur le statut de révocation des CERTIFICATS (serveur OCSP, pour On-line Certificate Status Protocol). Cette liste des certificats révoqués et ces services sont accessibles pour les applications utilisant les certificats aux adresses contenues dans les CERTIFICATS.

Pour accéder à la LCR :
http://crl.certigna.fr/entityca.crl
http://crl.dhimyotis.com/entityca.crl

Pour accéder au serveur OCSP :
http://entityca.ocsp.certigna.fr
http://entityca.ocsp.dhimyotis.com

13. ÉTENDUE DE RESPONSABILITÉ

La responsabilité de l'AC ne peut être engagée en cas de compromission de la clé privée associée au CERTIFICAT. L'AC ne sera en aucun cas responsable des éventuels dommages ayant leur origine dans l'utilisation du CERTIFICAT. L'AC ne pourra pas être impliquée par des retards ou pertes que pourraient subir les données transmises sur lesquelles est apposé un CACHET par le service applicatif.
L'AC ne saurait être tenue responsable de problèmes relevant de la force majeure, au sens du Code civil. Si un cas de force majeure a une durée supérieure à quinze jours, le RC sera autorisé à mettre un terme au CONTRAT et il n'y aura pas de préjudice.

14. CONTRAT ET MODIFICATIONS

Le CONTRAT annule tout engagement antérieur. Le RC convient que, pendant la durée du CONTRAT, l'AC pourra modifier les conditions générales d'utilisation. Toutefois, les conditions acceptées et signées par le RC restent valides pendant toute la durée du CONTRAT, sauf si le RC accepte explicitement les nouvelles conditions émises et publiées par l'AC sur le site https://www.certigna.fr. Un courrier doit dans ce cas être adressé à l'AC en y joignant les nouvelles conditions générales d'utilisation sur lesquelles sont portées la mention "lu et approuvé", la date et la signature du RC. En cas de renouvellement du CONTRAT (renouvellement du CERTIFICAT à la fin de validité de ce dernier ou après sa révocation), le nouveau CERTIFICAT est soumis aux conditions générales d'utilisation en vigueur.

15. RÉSILIATION

Au cas où l'une des parties n'exécuterait pas l'une des obligations découlant des présentes conditions générales, l'autre partie pourra lui notifier d'exécuter ladite obligation. A défaut pour la partie défaillante de s'être exécutée dans les quinze jours de cette notification, l'autre partie pourra résilier le CONTRAT.

16. CONDITIONS DE REMBOURSEMENT

La commande de CERTIFICAT ne peut être annulée dès lors que le dossier est en cours de traitement. Tout CERTIFICAT émis ne peut faire l'objet d'une demande de remboursement.

17. DONNÉES PERSONNELLES

Les dossiers de demande de certificat électronique comportant les données personnelles sont archivés à minima sept ans et aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. Les informations personnelles d'identité peuvent être utilisées comme données d'authentification lors d'une éventuelle demande de REVOCATION.
Par ailleurs, DHIMYOTIS conserve les données à caractère personnel pendant une durée de trois ans à compter de la fin des relations commerciales avec le client et 3 ans à compter du dernier contact émanant avec le prospect. Le délai commence à partir de la dernière connexion au compte client ou du dernier envoi d'un courriel au service client, ou d'un clic sur un lien hypertexte d'un courriel adressé par DHIMYOTIS, d'une réponse positive à un courriel demandant si le client souhaite continuer à recevoir de la prospection commerciale à l'échéance du délai de trois ans.
Conformément à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et au règlement européen « 2016/679/ UE du 27 Avril 2016 » relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, vous bénéficiez d'un droit d'accès, d'opposition, de rectification, de suppression et de portabilité de vos données personnelles. Vous pouvez exercer votre droit en vous adressant par mail à : privacy@certigna.com, ou par courrier à l'adresse suivante : DHIMYOTIS, Service du DPO, 20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France.

18. CESSION DU CONTRAT

Le RC ne peut pas céder ses droits liés au CONTRAT.

19. REGLEMENT DE CONFLITS

Le CONTRAT est soumis au droit français.
Les parties s'engagent à tenter de résoudre à l'amiable tout différend susceptible d'intervenir entre elles, soit directement soit via un médiateur, dans les 2 mois de la réception du courrier avec accusé réception informant du différend. Les éventuels frais de médiation seront supportés par moitié par chacune des parties. Le cas échéant, l'affaire sera portée devant le tribunal de commerce de Lille.

20. COORDONNÉES DE LA SOCIÉTÉ DHIMYOTIS

Dhimyotis S.A.
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq
Tél : +33 320 792 409 - Fax : +33 956 952 412
Email : contact@dhimyotis.com