

## CONDITIONS PARTICULIERES – CERTIFICATS DE SECURITE

### 1. PREAMBULE ET OBJET

Nameshield intervient en qualité d'intermédiaire entre les Autorités de Certification, auprès desquelles elle est accréditée, et le Client. Les présentes CP ont vocation à définir les conditions dans lesquelles Nameshield fournit au Client des Certificats de Sécurité. Toute Commande de certificats de sécurité (ci-après « Certificat(s) de Sécurité ») auprès de Nameshield implique de la part du bénéficiaire l'acceptation pleine et entière des présentes conditions particulières (ci-après CP).

Les Prestations relatives aux présentes CP concernent la fourniture des Certificats de Sécurité, selon le choix du Client, lesquels disposent de méthodes d'authentification différentes selon le type de Certificat de Sécurité sélectionné. Les Certificats de Sécurité objet des présentes sont les suivants:

- Le certificat à validation du domaine (SSL DV : « Domain Validation ») ;
- Le certificat à validation de l'organisation (SSL OV : « Organization Validation ») ;
- Le certificat à validation étendue (SSL EV : « Extended Validation ») ;
- Les certificats RGS 1, 2, et 3 étoiles.

Ces CP complètent les CGS, mais ne les remplacent pas. Elles ne peuvent pas s'appliquer indépendamment des CGS. Les termes employés dans les présentes CP débutant par une majuscule ont la même signification qui leur a été donnée dans les CGS, sauf définition particulière prévue dans les présentes CP.

### 2. DEFINITIONS

« **Autorité de Certification** » : désigne l'entité émettrice du Certificat de Sécurité. Les Autorités de Certification sont reconnues comme étant des émetteurs de Certificats de Sécurité de confiance. L'Autorité de Certification a pour rôle d'effectuer des vérifications lors de chaque commande de Certificat, différente selon le niveau d'authentification et le type de Certificat de Sécurité commandé, afin de s'assurer de l'identité du client demandeur. L'Autorité de Certification permet ainsi de démontrer l'authenticité du titulaire du Certificat de Sécurité auprès des navigateurs internet et des internautes.

« **Certificat de Sécurité** » : Un Certificat de Sécurité est un bloc de texte codé et composé d'une clé publique et d'informations le caractérisant, pouvant être utilisé pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges. Les Certificats de Sécurité sont délivrés par une Autorité de Certification, dans des conditions plus ou moins strictes selon le type de Certificat de Sécurité choisi par le Client. A titre d'exemple, le Certificat RGS 3 étoiles doit être remis en main propre contre signature et preuve de l'identité du Client.

« **Certificat RGS** » : désigne un Certificat de Sécurité permettant à une personne physique ou morale de s'authentifier auprès d'une autorité administrative et de signer électroniquement, depuis un support logiciel ou physique, suivant le type de Certificat RGS choisi par le Client. Le terme RGS est un acronyme signifiant « Référentiel Général de Sécurité », désignant des règles publiques afin de faciliter les échanges électroniques sécurisés.

« **Certificat SSL-TLS** » : désigne un Certificat de Sécurité installé sur un nom de domaine, permettant au site internet associé d'être identifié par les navigateurs internet. Les termes SSL, acronyme du terme anglais « Secure Sockets Layer », et TLS, acronyme du terme anglais « Transport Layer Security », désignent un protocole de sécurisation de la transmission de données sur internet. Un Certificat SSL-TLS est un certificat électronique constitué d'un fichier de données contenant des informations d'identification, et permettant au site internet lié au nom de domaine choisi de prouver l'authenticité de l'identité en ligne, auprès des navigateurs internet. Le certificat SSL-TLS lie ainsi les informations de propriété d'un nom de domaine à une clé cryptographique, elle-même reconnue par les navigateurs internet. Le certificat SSL-TLS permet également le chiffrement des données échangées entre les navigateurs et le site internet, garantissant la confidentialité des échanges et l'intégrité des données.

« **Clé Privée** » : désigne une clé cryptographique, liée à la Clé Publique, propriété exclusive du Client et connue uniquement par lui-même, et utilisée par lui seul pour accéder à son Certificat de Sécurité.

« **Clé Publique** » : désigne une clé cryptographique, liée à la Clé Privée, communiquée et stockée par l'audience destinataire (navigateurs internet, administrations publiques, etc.), qui permet au Client de prouver son identité et s'authentifier auprès de l'audience destinataire.

« **Fichier CRT** » : désigne un fichier propriété du Client, contenant le Certificat SSL-TLS final. La récupération sur l'Interface de Gestion et la conservation du Fichier CRT par le Client s'exercent sous sa seule responsabilité.

« **Fichier CSR** » : désigne un fichier propriété du Client, contenant les informations de la demande de Certificat de Sécurité du Client, y compris la Clé Publique. La création, la récupération sur l'Interface de Gestion, et la conservation du Fichier CSR du Client s'exercent sous sa seule responsabilité.

« **Phrase Challenge** » ou « **Passphrase** » : désigne le mot de passe constitué d'un certain nombre de caractère créé par le Client afin de générer la Clé privée. La création et la conservation confidentielle de la Phrase Challenge du Client s'exercent sous sa seule responsabilité.

« **Éléments du Certificat de Sécurité** » : désigne la Clé Privée, le Fichier CRT et le Fichier CSR, le certificat intermédiaire, ainsi que la Phrase Challenge.

### 3. CONDITIONS DE REALISATION DES PRESTATIONS

Dans le cadre des Prestations, Nameshield agit en qualité d'intermédiaire auprès de l'Autorité de Certification. A ce titre, le Client donne mandat à Nameshield afin de procéder à la confirmation de la Commande de Certificat de Sécurité auprès de l'Autorité de Certification, et à réaliser un suivi de la demande jusqu'à l'émission ou la livraison du Certificat de Sécurité.

### 4. COMMANDE

Nameshield intervient sur demande expresse du Client. Ainsi, les Commandes de Prestations relatives aux présentes CP peuvent être effectuées dans les conditions des CGS, à savoir depuis l'Interface de Gestion, par retour d'un Devis signé par le Client, ou par courrier électronique.

### 5. OBLIGATIONS DU CLIENT

#### 5.1 GENERALITES

Le Client s'engage à coopérer avec Nameshield, ainsi qu'à lui fournir toutes informations et documentations strictement nécessaires à la création et/ou à la validation du Certificat de Sécurité. Le Client s'engage à fournir des informations exactes et mises à jour le cas échéant.

Les Eléments du Certificat de Sécurité sont stockés et accessibles sur l'Interface de Gestion. Le Client détient la pleine propriété des Eléments du Certificat de Sécurité et s'engage à prendre toutes les précautions adéquates pour empêcher toute violation, perte de contrôle ou divulgation non autorisée.

Le Client autorise Nameshield à conserver les Eléments du Certificat de Sécurité, susceptibles d'être utilisés par Nameshield sur demande expresse du Client dans l'hypothèse où ces Eléments de Certificat de Sécurité auraient été perdus ou détruits chez le Client. En revanche, la Phrase Challenge, bien que conservée sur l'Interface de Gestion, n'est pas accessible par Nameshield.

Toute Commande de Certificat de Sécurité est soumise aux conditions d'utilisation de l'Autorité de Certification concernée. Ainsi, toute Commande vaut acceptation expresse et sans réserve des conditions d'utilisation concernées.

## 5.2 DISPOSITIONS RELATIVES AUX CERTIFICATS SSL-TLS

Le Client reconnaît que le Certificat SSL-TLS commandé est lié à un nom de domaine choisi par le Client au moment de la Commande. Ainsi, le Client est informé qu'il n'est pas possible de transférer le Certificat SSL-TLS commandé sur un autre nom de domaine que celui déterminé lors de la Commande.

Le Client est tenu de procéder à la création du Fichier CSR, ainsi qu'à la création et la conservation sous son unique responsabilité d'une Phrase Challenge. Lorsque la Clé Privée est créée et transmise par l'Autorité de Certification, le Client est responsable de sa conservation et de sa confidentialité.

Le Client est informé et accepte que l'Autorité de Certification, afin de procéder à la validation du Certificat SSL-TLS, le contacte directement par courrier électronique et/ou téléphone. Le défaut de réponse du Client entraîne l'absence de création du Certificat SSL-TLS, qui ne saurait engager la responsabilité de Nameshield.

## 5.3 DISPOSITIONS RELATIVES AUX CERTIFICATS RGS

La création d'un Certificat RGS est conditionnée, selon le niveau de sécurité choisi, à la remise en main propre dudit Certificat RGS au Client.

Nameshield, en relation avec l'Autorité de Certification, procède à la mise en relation du Client avec le tiers délivrant le Certificat RGS. Le défaut de présence du Client lors de l'émission du Certificat RGS entraîne l'absence de création du Certificat RGS, qui ne saurait engager la responsabilité de Nameshield. Les éléments du Certificat RGS sont accessibles depuis la console d'administration de l'Autorité de Certification. Le Client est tenu de les télécharger, Nameshield n'ayant pas accès à ces éléments.

## 6. OBLIGATIONS DE NAMESHIELD

Dans le cadre de la fourniture des Prestations, Nameshield a un rôle d'intermédiaire entre le Client et l'Autorité de Certification fournissant le Certificat de Sécurité. Nameshield est tenue à une obligation de moyens, et plus spécifiquement s'engage à :

- procéder à la demande de Certificat de Sécurité commandé par le Client,
- fournir les documents nécessaires à l'Autorité de Certification,
- réaliser le suivi de la demande du Client,
- faciliter la remise du Certificat RGS au Client,
- fournir une assistance au Client dans l'installation du Certificat de Sécurité.

Nameshield n'est pas tenue de procéder à la création du Fichier CSR, ni de la Phrase Secrète. Dans l'hypothèse où le Client souhaiterait que Nameshield procède à ces créations, Nameshield ne serait en aucun cas tenue pour responsable des dommages pouvant survenir du fait de l'échange d'Éléments du Certificat de Sécurité par courrier électronique, notamment la Clé Privée générée par la création du Fichier CSR.

Pour des raisons de sécurité, Nameshield ne communique pas les Éléments du Certificat de Sécurité par courrier électronique au Client. Si toutefois le Client souhaitait la communication des Éléments du Certificat de Sécurité par voie électronique, Nameshield les communiquera par l'intermédiaire d'une plateforme sécurisée. Le Client garantit Nameshield contre toute atteinte sur les Éléments du Certificat de Sécurité, qui pourrait notamment résulter d'un accès frauduleux à un compte de courrier électronique, une divulgation non autorisée ou toute autre violation. Concernant les éléments du Certificat RGS, ils sont accessibles depuis la console d'administration de l'Autorité de Certification. Le Client est tenu de les télécharger, Nameshield n'ayant pas accès à ces éléments.

Le Client est informé que Nameshield peut, suivant un délai de préavis de trente (30) jours après avoir notifié le Client, mettre un terme à la fourniture de nouveaux Certificats de Sécurité dans le cas où Nameshield ne disposerait plus du droit de fournir des Certificats de Sécurité. Dans cette hypothèse, les Certificats de Sécurité existants resteraient valables jusqu'à leur date d'expiration.

## 7. EMISSION DU CERTIFICAT DE SECURITE

Les délais d'émission des Certificats de Sécurité indiqués par Nameshield lors de la Commande sont indicatifs et basés sur un délai moyen prévisionnel fourni par l'Autorité de Certification. Ces délais peuvent varier sensiblement selon la capacité du Client à fournir les éléments demandés permettant le travail d'authentification. Aucune indemnité ne sera accordée au Client en cas de non-respect de ces délais.

Le Client s'engage à vérifier le bon fonctionnement du Certificat de Sécurité et sa conformité à la suite de sa livraison. La livraison des Certificats de Sécurité de type Certificat RGS 2 ou 3 étoiles nécessite la réalisation d'un face à face auprès d'un tiers spécifiquement désigné. Ce tiers agit en qualité d'autorité d'enregistrement déléguée de l'Autorité de Certification. Nameshield ou l'Autorité de Certification choisissent ce tiers, au bénéfice du Client, dans une zone géographique située à proximité du Client.

L'annulation d'une Commande de Certificat SSL-TLS est possible dans un délai de trente (30) jours suivants l'émission du Certificat SSL-TLS par l'Autorité de Certification. Le remplacement à l'identique d'un Certificat SSL-TLS annulé dans le délai précité est gratuit et illimité. Passé ce délai, le Certificat SSL-TLS peut être révoqué, sans possibilité de remboursement du Client.

Toute Commande de Certificat RGS est ferme. Aucun remboursement ne pourra être effectué en cas d'annulation de Commande de Certificat RGS.

## 8. DUREE DES PRESTATIONS

La durée des présentes CP est conditionnée à la durée de vie du Certificat de Sécurité, différente selon le type de Certificat de Sécurité. Les CP cessent de s'appliquer lorsque le Client ne dispose plus de Certificat de Sécurité géré par Nameshield, sous réserve de l'absence de retard de paiement.

Le Client est informé que les Certificats de Sécurité ne peuvent être renouvelés de manière automatique.

### 8.1 DISPOSITIONS RELATIVES AUX CERTIFICATS SSL-TLS

En fonction du type de Certificat SSL-TLS choisi par le Client, la durée de la Prestation ne peut être inférieure à un (1) an ni supérieure à deux (2) ans à compter de la date d'émission du Certificat SSL-TLS concerné, sauf cas de révocation anticipée.

Nameshield envoie au Client des notifications par courrier électronique préalablement à l'expiration du Certificat SSL-TLS, dans les délais suivants : 90 jours, 60 jours, 30 jours, et 7 jours avant la date d'expiration du Certificat SSL-TLS. Le certificat est expiré à l'issue du dernier de ces délais.

A l'expiration du Certificat SSL-TLS, si le Client souhaite renouveler la Prestation, il devra procéder à une commande de renouvellement, consistant à demander un nouveau Fichier CRT.

### 8.2 DISPOSITIONS RELATIVES AUX CERTIFICATS RGS

En fonction du type de Certificat RGS choisi par le Client, la durée de la Prestation ne peut être inférieure à un (1) an ni supérieure à trois (3) ans à compter de la date d'émission du Certificat RGS concerné, sauf cas de révocation anticipée.

Le Client recevra des notifications d'expiration régulières du Certificat RGS par courrier électronique à partir de 120 jours avant la date de fin de validité.

Pendant la période de 120 jours précédant l'expiration du Certificat RGS, si le Client souhaite renouveler la Prestation, il devra procéder à une commande de renouvellement.

## 9. REVOCATION

Si le Client le souhaite, ou s'il découvre ou a des raisons de croire à une compromission du Certificat de Sécurité, il peut procéder à la révocation anticipée du Certificat de Sécurité en le signalant à Nameshield. Dans une telle hypothèse, le Certificat de Sécurité ne pourra plus être réactivé ou renouvelé.

Le Client est informé qu'un Certificat de Sécurité révoqué ne peut pas être renouvelé ou réactivé. Afin de bénéficier de nouveau d'un Certificat de Sécurité, le Client doit passer une nouvelle Commande de renouvellement.

## 10. GARANTIE ET RESPONSABILITE

Le Client reconnaît et accepte que Nameshield ne puisse être tenue responsable vis-à-vis du Client de toute perte, vol, divulgation non autorisée, manipulation non autorisée, altération, privation de jouissance ou de toute autre compromission concernant tout Élément d'un Certificat de Sécurité.

Le Client s'engage à utiliser le Certificat de Sécurité exclusivement à des fins autorisées et légales.

## 11. TARIFS

Le Client est informé que les prix sont susceptibles de varier et sont ainsi modifiables sans préavis.

La prestation de remise physique du Certificat RGS fait l'objet d'un tarif déterminé par le tiers désigné. Le Client dispose du choix de procéder au paiement direct du tiers désigné, ou au paiement indirect par l'intermédiaire de Nameshield.