ARRETE n° 647 CM du 18 mai 2017 déterminant les caractéristiques techniques d'accès et d'utilisation du système de dédouanement informatisé FENIX et les procédés techniques garantissant sa sécurité.

NOR : DDI1720700AC-1

Le Président de la Polynésie française,

Sur le rapport du vice-président, ministre de l'économie et des finances, en charge des grands projets d'investissement et des réformes économiques,

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 complétant le statut d'autonomie de la Polynésie française ;

Vu l'arrêté n° 676 PR du 16 septembre 2014 modifié portant nomination du vice-président et des ministres du gouvernement de la Polynésie française, et déterminant leurs fonctions ;

Vu la loi du pays n° 2016-35 du 12 septembre 2016 portant création et organisation d'un système de dédouanement dématérialisé - Fenua Import-Export (FENIX) en Polynésie française ;

Vu la délibération n° 63-1 du 16 janvier 1963 modifiée portant réglementation du service des douanes de la Polynésie française, valant code des douanes ;

Le conseil des ministres en ayant délibéré dans sa séance du 17 mai 2017,

Arrête :

Article 1er.— En application des articles LP. 14 et LP. 15 de la loi du pays n° 2016-35 du 12 septembre 2016 susvisée, le présent arrêté détermine les caractéristiques techniques d'accès et les procédés techniques de sécurisation du système de dédouanement informatisé FENIX.

Art. 2.— Les opérateurs habilités (les transitaires en douane, les importateurs, les transporteurs ou leur représentant, les exploitants de magasins et aires de dédouanement) ont accès au système de dédouanement FENIX par l'intermédiaire d'internet. Les caractéristiques du réseau, du matériel et du logiciel nécessaires sont décrites en annexe I.

Art. 3.— Les administrations partenaires (port autonome, ISPF) sont reliées au système de dédouanement FENIX par l'intermédiaire d'internet.

Art. 4.— Les autres usagers du système de dédouanement FENIX (bureaux de douane, paierie) sont reliés par une ligne spécialisée numérique au serveur FENIX installé dans les locaux du service informatique de Polynésie française.

Art. 5.— La fiabilité de l'identification des parties à la communication électronique repose sur un portail d'authentification, paramétré sur la base des mentions reprises dans la convention d'accès signé par l'opérateur.

Art. 6.— L'intégrité des documents, la sécurité et la confidentialité des échanges et la conservation des transmissions reposent sur l'utilisation de certificats électroniques dont les caractéristiques sont décrites en annexe II.

Art. 7.— L'attestation de la date d'envoi et celle de réception par le destinataire repose sur un système d'horodatage électronique dont les caractéristiques sont décrites en annexe III.

Art. 8.— Le vice-président, ministre de l'économie et des finances, en charge des grands projets d'investissement et des réformes économiques, est chargé de l'exécution du présent arrêté qui sera publié au *Journal officiel* de la Polynésie française.

Fait à Papeete, le 18 mai 2017.
Pour le Président absent :
Le vice-président,
Teva ROHFRITSCH.

Par le Président de la Polynésie française :
Le vice-président,
Teva ROHFRITSCH.

ANNEXE I

Configuration type pour les opérateurs connectés

Réseau

- 1 liaison Internet d'un débit supérieur ou égal à 1 Mbit/s

Matériel

- 1 terminal hébergeant un navigateur Web compatible, connecté à 1 liaison Internet
- 1 écran d'une résolution minimum de 1280*1024 pixels, relié au terminal
- 1 imprimante au format A4 sans marge, accessible du terminal

Logiciel

- 1 navigateur Web Mozilla Firefox version 51 minimum, ou Internet Explorer version 11 minimum
- 1 lecteur de fichier PDF, de préférence Adobe Reader version X minimum
- Le bloqueur de Pop-up désactivé

Sécurité

- Système d'exploitation et navigateur à jour des derniers patchs de sécurité
- Anti-virus installé et à jour

ANNEXE II

Caractéristiques des certificats électroniques garantissant l'*intégrité des documents, la sécurité et la confidentialité des échanges et la conservation des transmissions*

Les mentions au RGS de cette annexe seront remplacées par le Référentiel Général de Sécurité adapté à la Polynésie française instauré par la loi du Pays relative à la dématérialisation des actes des autorités administratives et aux téléservices.

Certificat Serveur SSL RGS ★

Le certificat Serveur SSL RGS ★ est un certificat répondant aux exigences du Référentiel Général de Sécurité de la République française (version 2.0) du niveau exigé de sécurité ★ (1 étoile).

Le certificat électronique est un document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Certificat Cachet Serveur RGS ★

Le certificat Cachet Serveur RGS ★est un certificat répondant aux exigences du Référentiel Général de Sécurité de la République française (version 2.0) du niveau exigé de sécurité ★ (1 étoile).

Le certificat Cachet Serveur est une signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation dans le cadre d'échanges dématérialisés entre usagers et Autorités administratives ou entre Autorités administratives.

ANNEXE III

Caractéristiques du *système d'horodatage électronique*
garantissant l'attestation *de la date d'envoi et celle de réception par le destinataire*

Les mentions au RGS de cette annexe seront remplacées par le Référentiel Général de Sécurité adapté à la Polynésie française instauré par la loi du Pays relative à la dématérialisation des actes des autorités administratives et aux téléservices.

Horodatage RGS

L'horodatage électronique utilisé dans F.E.N.I.X. répond aux exigences du Référentiel Général de Sécurité de la République française (version 2.0).

Une fonction d'horodatage permet d'attester qu'une donnée sous forme électronique existe à un instant donné. Cette fonction met en œuvre une contremarque de temps générée à l'aide d'un mécanisme cryptographique respectant les règles et, si possible, les recommandations contenues dans les référentiels [RGS_B1] et [RGS_B2].

Les exigences concernant le composant « contremarque de temps » sont décrites dans l'annexe du RGS « Politique d'horodatage type » ([RGS_A5]). Elles portent sur le contenu des contremarques de temps et sur les conditions dans lesquelles il est émis par un prestataire de services d'horodatage électronique (PSHE).

Cette contremarque, délivrée par un prestataire de services d'horodatage électronique (PSHE), doit respecter les exigences de l'annexe [RGS_A5], appelée « Politique d'horodatage type ». Cette annexe ne distingue qu'un niveau unique de sécurité, auquel les autorités administratives doivent se conformer dès lors qu'elles souhaitent mettre en œuvre la fonction d'horodatage électronique au sein de leur système d'information.