Accusé de réception en préfecture
001-210101598-20221215-2022-080-DE
Date de réception préfecture : 19/12/2022

CONVENTION ENTRE LA COMMUNE ET L'AGENCE NATIONALE DES TITRES SECURISES relative à l'adhésion de la commune aux modalités d'obtention, d'attribution et d'usage des cartes d'authentification et de signature fournies par l'ANTS (carte ANTS)

Commune de :

Département de :

Code Insee :

Vu le décret n° 2007-240 modifié du 22 février 2007 portant création de l'Agence nationale des titres sécurisés,

Les parties à la convention

- La commune mentionnée en titre, représentée par son Maire,
- L'Agence nationale des titres sécurisés, représentée par son directeur.

Article I : Objet de la convention

La présente convention a pour objet de définir les modalités d'obtention, d'attribution et d'usage des cartes d'authentification et de signature fournies par l'ANTS à la commune.

Article II : Cartes d'authentification et de signature

Les cartes d'authentification et de signature permettent aux acteurs habilités des collectivités territoriales de s'authentifier et de signer électroniquement.

La carte d'authentification et de signature remise au délégataire du maire ou au maire lui-même permet, de gérer la délivrance de ces cartes aux agents territoriaux concernés et les habilitations associées.

Le maire peut désigner un ou plusieurs délégataires pour prendre en charge la délivrance et la gestion des cartes d'authentification et de signature des agents territoriaux concernés.

Article III : Conditions d'obtention des cartes d'authentification et de signature

Pour obtenir les deux premières cartes d'authentification et de signature, la collectivité territoriale doit signer la présente convention.

Les cartes à puce sont commandées, sur demande de l'ANTS, par l'autorité d'enregistrement de rattachement sur la base des informations présentes dans cette convention.

Pour la remise de cette carte, l'autorité d'enregistrement de rattachement contacte le maire ou le(s) délégataire(s) désigné(s) dans le formulaire en annexe.

La carte d'authentification et de signature est remise en face à face au(x) délégataire(s) ou au maire, qui doivent être munis d'un document d'identité en cours de validité (carte nationale d'identité ou passeport).

Article IV : Conditions générales d'utilisation des cartes d'authentification et de signature

Les conditions générales d'utilisation des cartes d'authentification et de signature des collectivités territoriales pour les maires et leur(s) délégataire(s) et les conditions générales d'utilisation des cartes d'authentification et de signature des collectivités territoriales pour les agents de mairie sont disponibles sur le site Internet de l'Agence Nationale des Titres Sécurisés

(https://sp.ants.gouv.fr/antsv2/index.html).

Article V : Obligations de l'Agence Nationale des Titres Sécurisés

L'Agence Nationale des Titres Sécurisés, par cette convention, s'engage :

- à fournir au maire, à ses délégataires et aux agents territoriaux dûment habilités, utilisant des applications référencées par l'ANTS, des cartes d'authentification et de signature contenant deux certificats : l'un à usage d'authentification et l'autre à usage de signature électronique. Ces cartes sont renouvelées dans les mêmes conditions que pour l'obtention initiale, à l'issue de 6 ans d'ancienneté. Elles pourront être remplacées gratuitement en cas de défectuosité.
- à mettre à la disposition du maire et de ses délégataires des applications accessibles via Internet permettant de gérer le cycle de vie des cartes d'authentification et de signature, l'annuaire des agents et les habilitations associées.
- à mettre à disposition du maire et de ses délégataires la documentation utilisateur et technique nécessaire à l'utilisation des applications permettant la gestion des cartes à l'adresse suivante https://sp.ants.gouv.fr/antsv2/index.html.
- à mettre à disposition des porteurs de carte une application leur permettant de révoquer leurs cartes, de les débloquer et d'en modifier les codes PIN.
- à mettre à la disposition du maire, de ses agents et de ses prestataires les informations nécessaires à l'utilisation de la carte d'authentification et de signature notamment via internet.
- à respecter le référentiel général de sécurité, de niveau trois étoiles, sur l'ensemble des composants matériels, logiciels et procéduraux.
- à assurer au profit du maire, de ses délégataires, des agents communaux habilités, une assistance accessible aux heures ouvrées.

Article VI : Obligations du maire

Le maire s'engage :

- à faire doter de cartes d'authentification et de signature individuelles les agents territoriaux affectés à des fonctions nécessitant son utilisation,
- à conserver les documents relatifs à la remise des cartes sous forme papier ou à les stocker numériquement (par exemple la copie du titre d'identité certifiée conforme à l'original par le porteur),
- à mettre à jour l'annuaire ou les annuaires, mis à disposition par l'ANTS, permettant d'identifier les agents disposant d'une carte d'authentification et de signature,
- à mettre à jour les droits et les habilitations des agents territoriaux disposant d'une carte d'authentification et de signature au regard des délégations attribuées,
- à déclarer sans délai, via l'Internet, la perte ou le vol de sa carte d'authentification et de signature individuelle d'un délégataire ou d'un agent dès que le fait est porté à sa connaissance,
- à révoquer sans délais les cartes des agents qui n'assumeraient plus les fonctions nécessitant l'usage de la carte (départ, changement de service …),

- à informer, dans les plus brefs délais, le service d'assistance de l'Agence Nationale des Titres Sécurisés, dont les coordonnées figurent sur le site (http://www.ants.gouv.fr/), de tout problème technique affectant la bonne mise en œuvre de la présente convention,
- à veiller au respect des bonnes pratiques de sécurité informatique et notamment celles relatives à l'utilisation des cartes d'authentification et de signature individuelles comme mentionné d'une part dans les Conditions Générales d'Utilisation des cartes agents des collectivités territoriales, et d'autre part, dans la Politique de Certification « Acteurs des Collectivités Territoriales »,
- à nommer au moins un délégataire chargé de la gestion des cartes et des droits afférents si le maire ne remplit pas cette fonction lui-même,
- à retourner la présente convention accompagnée de ses annexes dûment renseignées à l'ANTS,
- à se doter des cartes d'authentification et de signature de l'ANTS et à les utiliser uniquement pour les usages et applications logicielles référencées par l'ANTS en annexe,
- à payer, le cas échéant, les frais afférents à ces cartes.

Article VII : Obligations de la collectivité territoriale en termes de sécurité

Les mesures de sécurité présentées dans le « Guide de sécurité des postes de travail en collectivités territoriales » (ci-après désigné « Guide SSI ») définissent le niveau minimum de sécurité que doivent respecter les postes de travail utilisés par la collectivité dans la délivrance des cartes aux agents.

En signant la présente convention, la commune s'engage :

- à mettre en œuvre les mesures de sécurité décrites dans le « Guide SSI » sur les postes de travail utilisés dans le cadre de la présente convention,
- à transmettre à l'ANTS le niveau actuel de sécurité de ces postes de travail en répondant aux questions proposées dans le « Guide SSI » tout en s'engageant sur l'exactitude des informations retournées (cf annexe 4- Guide SSI),
- à permettre au(x) prestataire(s) agréés par l'ANSSI (Agence nationale de sécurité des systèmes d'information) d'auditer les responsables de la gestion des cartes conformément au référentiel général de sécurité (http://references.modernisation.gouv.fr/securite).

L'ANTS, en tant qu'opérateur de service de confiance se réserve le droit d'effectuer des contrôles relatifs à la sécurité des postes de travail afin de vérifier leur conformité vis à vis des exigences de sécurité présentées dans le « Guide SSI » joint avec la présente convention.

Tout contrôle de l'ANTS au sein d'une collectivité territoriale mettant en évidence une non-conformité majeure peut induire la suspension des rôles de confiance au sein de cette collectivité. Dans ce cas, toutes les commandes et remises de cartes seront effectuées en préfecture.

Article VIII : Prix des prestations

Les prix des prestations décrites dans cette convention sont précisés dans l'annexe 2.

Les prestations, les prix et les modalités de paiement associées sont définis selon les usages avec les ministères en charge de la mise en œuvre des solutions de dématérialisation.

Article IX : Durée de la convention

Pour les communes non soumises à l'obligation prévue dans la loi susvisée, la présente convention est conclue pour une durée de 6 ans, renouvelable par tacite reconduction et par période de 6 ans, à compter de la date de signature par les parties.

Pour les communes soumises à l'obligation, cette convention est conclue durant toute la durée de l'obligation prévue par la loi susvisée.

Chaque partie peut demander à tout moment la suspension et / ou la résiliation de la présente convention, sous réserve d'un préavis de 3 mois.

Le cas échéant, le non-respect des obligations de chacune des parties est un motif de la suspension, de la résiliation de l'abonnement de la commune au dispositif COMEDEC.

Article X : Règlement des litiges

En cas de litige résultant de l'interprétation ou de l'application de la présente convention, les parties s'engagent à tout mettre en œuvre pour parvenir à un règlement amiable du litige.

Conformément à l'article R. 312-11 du Code de justice administrative, le Tribunal administratif de Paris, 7 rue de Jouy Cedex 04, F-75181 Paris. E-mail : greffe.ta-paris@juradm.fr. Tél. 01 44 59 44 00. Fax 01 44 59 46 46 est seul compétent pour connaître de tout litige relatif à l'interprétation ou à l'exécution de la présente Convention.

Fait le / / à

Le maire Le Directeur de l'ANTS

ANNEXE 1 – Liste des applications compatibles et prix des prestations

Liste des applications compatibles

Applications	Prestations
COMEDEC	Fourniture d'une carte d'authentification et de signature ANTS aux officiers et agents de l'état civil ainsi qu'aux responsables cartes.
Hélios / PES V2	Utilisation d'une carte d'authentification ANTS délivrée aux officiers et agents de l'état civil dans le cadre de l'application COMEDEC pour l'application Hélios/PES V2.
ACTES (*Aide au Contrôle de légaliTé dématErialiSé*)	Utilisation d'une carte d'authentification ANTS délivrée aux officiers et agents de l'état civil dans le cadre de l'application COMEDEC pour l'application ACTES.
SAIP (*Système d'Alerte et d'Information des Populations*)	Utilisation d'une carte d'authentification ANTS permettant l'accès à l'application SAIP.
TES (Titres Electroniques Sécurisés)	Fourniture d'une carte d'authentification et de signature ANTS aux officiers et agents de recueil / remise ainsi qu'aux responsables cartes des sites non encore équipés COMEDEC.

Liste des prestations et des prix.

Applications	Prestations	Prix de la prestation
COMEDEC	Fourniture d'une carte d'authentification et de signature ANTS aux officiers et agents de l'état civil ainsi qu'aux responsables cartes.	Gratuite, dans la limite d'une carte par officier et/ou agent d'état civil et par responsable cartes, par période de 6 ans, par collectivité.
COMEDEC	Fourniture des lecteurs de cartes d'authentification et de signature ANTS.	Gratuit*, dans la limite d'un lecteur de carte par poste de travail du service état civil au moment de l'installation du service COMEDEC et par poste de travail des responsables cartes.
COMEDEC / TES / CARTES	Fourniture d'une nouvelle carte d'authentification et de signature ANTS (remplacement suite à perte, vol, casse, perte de code PIN...) ou au-delà du contingent fixé précédemment.	30 euros HT par carte.
ACTES (*Aide au Contrôle de légaliTé dématErialiSé*)	Utilisation d'une carte d'authentification ANTS délivrée aux officiers et agents de l'état civil dans le cadre de	L'ANTS autorise les officiers et agents de l'état civil utilisateurs de l'application COMEDEC, à utiliser leur carte nominative pour les transmissions à l'application ACTES et les

et HELIOS / PES V2	l'application COMEDEC pour l'application ACTES et/ou HELIOS / PES V2.	signatures des flux comptables PES V2 dans HELIOS L'ANTS se réserve le droit de contrôler que les utilisateurs de l'application ACTES et/ou HELIOS / PES V2 soient bien utilisateurs actifs de COMEDEC.
ACTES (*Aide au Contrôle de légaliTé dématErialiSé*) et HELIOS / PES V2	Fourniture de lecteurs de cartes pour l'application ACTES.	L'ANTS ne fournit pas de lecteur de cartes dans le cadre de cette application. Les utilisateurs ACTES sont déjà dotés des lecteurs utilisés pour COMEDEC.
SAIP (*Système d'Alerte et d'Information des Populations*)	Fourniture d'une carte d'authentification ANTS permettant l'accès à l'application SAIP.	L'ANTS fournit le Ministère de l'Intérieur en carte d'authentification et ne facture pas de frais supplémentaire à la commune.
SAIP (*Système d'Alerte et d'Information des Populations*)	Fourniture de lecteurs de cartes pour l'application SAIP.	L'ANTS ne fournit pas de lecteur de cartes dans le cadre de cette application.
TES	Fourniture d'une carte d'authentification et de signature ANTS aux officiers et agents de recueil / remise ainsi qu'aux responsables cartes.	Gratuite, dans la limite d'une carte par officier et/ou agent de recueil / remise et par responsable cartes, par période de 6 ans, par collectivité.
TES	Fourniture des lecteurs de cartes d'authentification et de signature ANTS.	Gratuit*, dans la limite de deux lecteurs de carte par mairie pour les responsables CARTES (ces lecteurs ne doivent pas être connecté au DR) Pour les utilisateurs de DR, les DR sont déjà munis de lecteurs de cartes.

***** L'ANTS n'assure pas la maintenance et le renouvellement des lecteurs de cartes dont le coût varie entre 5 et 15 euros.

Accusé de réception en préfecture
001-210101598-20221215-2022-080-DE
Date de réception préfecture : 19/12/2022

ANNEXE 2 – Caractéristiques techniques informatiques pour COMEDEC uniquement

INFORMATIONS	A RENSEIGNER	AIDE
Maternité		*Indiquer par "OUI" ou par "NON" si la commune dispose ou a disposé d'une maternité sur son territoire*
Dispositif de Recueil Passeport		*Indiquer par "OUI" ou par "NON" si la mairie est équipée d'un dispositif de recueil de demandes de passeports*
Volume annuel de délivrance d'actes		*Indiquer le volume annuel d'actes délivrés par la commune (ex : 80 000 en 2013)*
Système d'exploitation des postes utilisateurs du service Etat-Civil		*Indiquer le système d'exploitation des postes informatiques de la mairie (ex.: Windows 7)*
Base des données		*Indiquer la date à partir de laquelle les actes ont été dressés informatiquement*
Base d'actes image (période)		*Indiquer le cas échéant, la période pour laquelle la base d'état civil de la commune contient des images des actes*
Base de rattrapage des données (période)		*Indiquer le cas échéant, la période pour laquelle les actes ont été ressaisis sous forme de données*
Commentaires		*Indiquer ici tout complément d'information, ou renseignement jugé utile par la commune*

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Annexe 3 : Guide Sécurité des Postes de Travail

Carte Acteurs de l'Administration de l'Etat
Carte Acteurs des Collectivités Territoriales

Les 9 mesures énoncées dans le présent document, permettent de vous prémunir contre les risques courants qui peuvent affecter le poste de travail utilisé pour les demandes de Cartes Agents. Elles ne prétendent pas avoir un caractère d'exhaustivité. Elles représentent cependant le socle minimum des règles à respecter pour protéger les informations que vous allez manipuler.

Ces recommandations sont en partie issues du guide « d'hygiène informatique » publiés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[1]. Ne pas les suivre vous expose à des risques d'incidents majeurs[2].

Chaque mesure décrite ci-dessous est complétée par un ou plusieurs points de contrôle. Ces points de contrôle simples et pragmatiques doivent vous permettre de déterminer si vous appliquez actuellement la mesure ou non. La première partie du document présente les règles propres au poste de travail et à sa configuration. La seconde partie se concentre sur les bonnes pratiques d'utilisation de ce poste de travail.

Dans la suite du document, le terme « poste de travail » désigne le poste informatique utilisé pour la commande et la gestion des Cartes Agents délivrées pour la collectivité territoriale. Un « administrateur » désigne la personne qui dispose des droits suffisants pour configurer/administrer le poste de travail.

ANTS - v.1.1
08/11/2012

[1] http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

[2] En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 3 ans d'emprisonnement assortis d'une amende allant de 15.000 à 225.000 euros pour les personnes morales.

Sécurité relative à l'utilisation du poste de travail

Mesure 1 - Chaque personne ayant accès au système doit être connue

Chaque personne ayant accès au poste de travail doit utiliser une session de travail nominative et personnelle, protégée par un identifiant (nominatif) et un mot de passe. Les sessions partagées ou communes sont donc à proscrire. Une liste des personnes ayant accès (ou ayant eu accès) au poste de travail doit être conservée par le responsable de la collectivité territoriale.

- ☐ **Chaque utilisateur dispose de sa session de travail personnelle (identifiant/mot de passe)**
- ☐ **La liste des utilisateurs du poste de travail existe et est tenue à jour**

Mesure 2 - Ne pas avoir les « droits d'administrateur » sur le poste

L'accès aux fonctions d'administration du poste de travail doit être restreint aux seuls administrateurs de celui-ci. Il doit donc y avoir un compte administrateur en plus du ou des comptes utilisateurs (mentionnés dans la mesure 1). Les applications nécessitant des droits de niveau « administrateur » pour leur exécution doivent, dans la mesure du possible, être évitées et l'installation et la mise à jour de logiciels sur le poste de travail sont sous le contrôle de l'administrateur du poste de travail. L'utilisation d'internet à partir d'une session administrateur est à proscrire.

- ☐ **Les utilisateurs du poste de travail ne disposent pas des droits « administrateur »**
- ☐ **L'administrateur n'utilise pas (ou peu) sa session pour aller sur Internet**

Mesure 3 - Le poste de travail est protégé contre les virus.

Un unique logiciel antivirus doit être installé (par l'administrateur) sur le poste de travail et configuré pour recevoir ses mises à jour automatiquement. L'utilisateur du poste de travail ne doit pas pouvoir le désactiver.

- ☐ **Un unique antivirus est installé et configuré sur le poste de travail**
- ☐ **Un utilisateur quelconque du poste de travail ne doit pas pouvoir le désactiver**

Mesure 4 - Le poste de travail exploite des logiciels « à jour »

L'administrateur doit régulièrement procéder à la mise à jour du système d'exploitation et des logiciels installés sur le poste de travail (notamment du navigateur web). Ces mises à jour permettent de contrer les dernières failles de sécurité. Les mises à jour critiques des systèmes d'exploitation peuvent être installées sans délai en programmant une vérification automatique périodique hebdomadaire.

- ☐ **La mise à jour du système d'exploitation est programmée de façon automatique**
- ☐ **L'état du poste de travail est régulièrement contrôlé par l'administrateur**

Mesure 5 - Le poste de travail est protégé un pare-feu (firewall)

Un unique pare-feu logiciel (compatible avec l'antivirus installé sur le poste de travail) ou matériel doit protéger le poste de travail. Les systèmes d'exploitation Windows 7 et Windows 10 sont déjà équipés d'un pare-feu compatible avec les antivirus actuels.

☐ **Un unique pare-feu (matériel ou logiciel) protège le poste de travail**

Mesure 6 - L'exécution automatique des clés USB doit être désactivée.

Les supports amovibles (clés USB, disques durs externes, téléphones portables, baladeurs numériques, …) sont un moyen privilégié de propagation des codes malveillants et de fuite de données. L'administrateur du poste de travail doit donc interdire techniquement la connexion de ces supports amovibles sauf si c'est strictement nécessaire. Dans le cas contraire, l'exécution automatique (autoruns) depuis de tels supports doit être désactivée.

☐ **Les supports amovibles de stockage ne peuvent être connectés sur le poste de travail**

Mesure 7 - Limiter l'utilisation des technologies sans-fil

Les technologies sans fil (WiFi, Bluetooth, 3G) présentent de nombreuses failles de sécurité si elles sont mal configurées. L'usage de ces technologies doit être évité, au profit d'une connectivité filaire standard. Lorsque les technologies sans fil sont utilisées, les connexions doivent être sécurisées.

☐ **Le poste de travail est connecté au réseau à l'aide d'un câble réseau standard**

☐ **Le clavier et la souris du poste de travail sont connectés à l'aide de fils**

Sécurité relative à l'environnement de travail

Mesure 8 - Travailler sur un bureau dégagé

L'espace de travail ne doit pas être encombré par du matériel inutile dans la fonction du poste et aucun matériel suspect ne doit être branché sur le poste. En cas de doute, demandez conseil à l'administrateur du poste de travail. Aucune information confidentielle (code PIN, mot de passe) ne doit être apparente sur l'espace de travail. De la même façon, aucune Carte Agent active ne doit être laissée à la portée d'une tierce personne.

- ☐ **Le bureau du poste de travail est dégagé (pas de matériel inconnu à proximité)**
- ☐ **Les Carte Agents ne sont pas stockées à proximité du poste de travail**
- ☐ **Aucun élément sensible (mot de passe, code PIN) n'est affiché sur le poste de travail**

Mesure 9 - Soyez prudents

- Ne jamais ouvrir les pièces jointes d'un email ou cliquer sur des liens sans vous assurer de la fiabilité du message en termes de source d'émission et de contenu.
- Ne « surfez » pas sur des sites illégaux ou potentiellement vecteurs de risques lorsque vous êtes sur le poste de travail
- Refusez toujours les installations de logiciels qui vous sont proposées spontanément lorsque vous surfez sur Internet et refusez systématiquement l'installation des barres d'outils (« toolbar ») à destination des navigateurs internet.
- N'installez jamais des programmes piratés et/ou qui ne sont pas nécessaires à l'utilisation du poste de travail.

- ☐ **Les consignes ci-dessus ont été diffusées aux utilisateurs du poste de travail**
- ☐ **Les navigateurs installés n'ont pas de barres d'outils spécifiques (Ask, Google, Hotmail, …)**
- ☐ **Les logiciels installés sur le poste de travail proviennent d'éditeurs fiables**