Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Cahier des charges

des dispositifs de télétransmission

des actes soumis au contrôle de légalité

Version 2 2017

Table des matières

1. Définition de l'architecture globale

Cette partie vise à aider le responsable du dispositif de télétransmission des actes à comprendre le contexte global dans lequel s'inscrit leur intervention. À cette fin, elle décrit le contexte métier (a), l'architecture technique nécessaire à son accomplissement par voie électronique (b) et l'organisation technique des échanges susceptibles d'intervenir sur la chaîne de télétransmission (c).

a) Contexte métier

La chaîne de télétransmission prévue par le code général des collectivités territoriales (article R. 2131-1-B et suivant) a vocation à permettre au contrôle de légalité de s'effectuer au moyen des technologies de l'information et de la communication.

Le contrôle de légalité est une procédure administrative prévue par la Constitution et organisée par la loi. Elle conduit les préfectures à effectuer un contrôle juridique et budgétaire de certains actes que doivent transmettre les collectivités afin qu'elles vérifient leur adéquation aux règles de droit en vigueur. L'objectif de cette procédure est d'assurer la qualité du droit, d'en garantir une certaine unité sur l'ensemble du territoire national et de consolider la sécurité juridique des actes des collectivités.

Cette procédure donne lieu à une obligation de transmission d'un ensemble d'actes qu'édictent les collectivités aux services de l'État dans les départements et les territoires. Ceux-ci accusent réception des documents et procèdent au contrôle de la complétude du dossier et de la légalité de l'acte qui leur est transmis. Suite à cette transmission, une série d'échanges peuvent intervenir entre les préfectures et les collectivités. Les échanges obéissent à deux exigences métiers fortes : les délais qui interviennent entre chacun d'entre eux et la preuve de ces échanges est matérialisée par un accusé de réception.

Les délais sont encadrés juridiquement. Ils conditionnent le déroulement de la procédure administrative et sa date de fin. La préfecture ne pourra plus mettre en œuvre certaines prérogatives offertes par le droit au-delà d'un certain délai.

La preuve des échanges a une double utilité. Lors de la transmission initiale de l'acte de la collectivité, elle lui permet de déterminer la date d'entrée en vigueur. Les actes soumis à cette procédure n'entent en vigueur qu'à compter de leur réception par les services de l'État. En outre, la preuve des échanges qui suivent permet au juge de vérifier si la préfecture a mise en œuvre ses prérogatives dans le délai qui lui a été imparti.

Le contrôle de légalité peut aboutir à ce que la préfecture saisisse le juge pour qu'il prononce l'annulation de l'acte. Cette saisine doit intervenir dans un délai qui dépend des échanges intervenus entre le représentant de l'État et la collectivité.

b) Infrastructure technique

La chaîne de transmission des actes au contrôle de légalité dématérialisé repose sur un système d'information asynchrone, spécifique et urbanisé. Il est le fruit d'une expérimentation menée en 2004 généralisée entre 2005 et 2006. Sa structure a été conçue pour le rendre compatible avec la libre administration des collectivités territoriales tout en permettant de garantir la sécurité des échanges.

Le système est urbanisé puisqu'il repose sur plusieurs plates-formes. Le ministère de l'Intérieur exploite une plate-forme qu'il met à disposition de ses services. Elle comprend les applications « métier » « @CTES » et « Actes budgétaires » mises à disposition des agents des services déconcentrés pour leur permettre d'effectuer le contrôle de légalité et le contrôle budgétaires. Les actes sont intégrés dans ces deux applications. Le sas du ministère de l'Intérieur permet la réception des actes transmis par les dispositifs homologués.

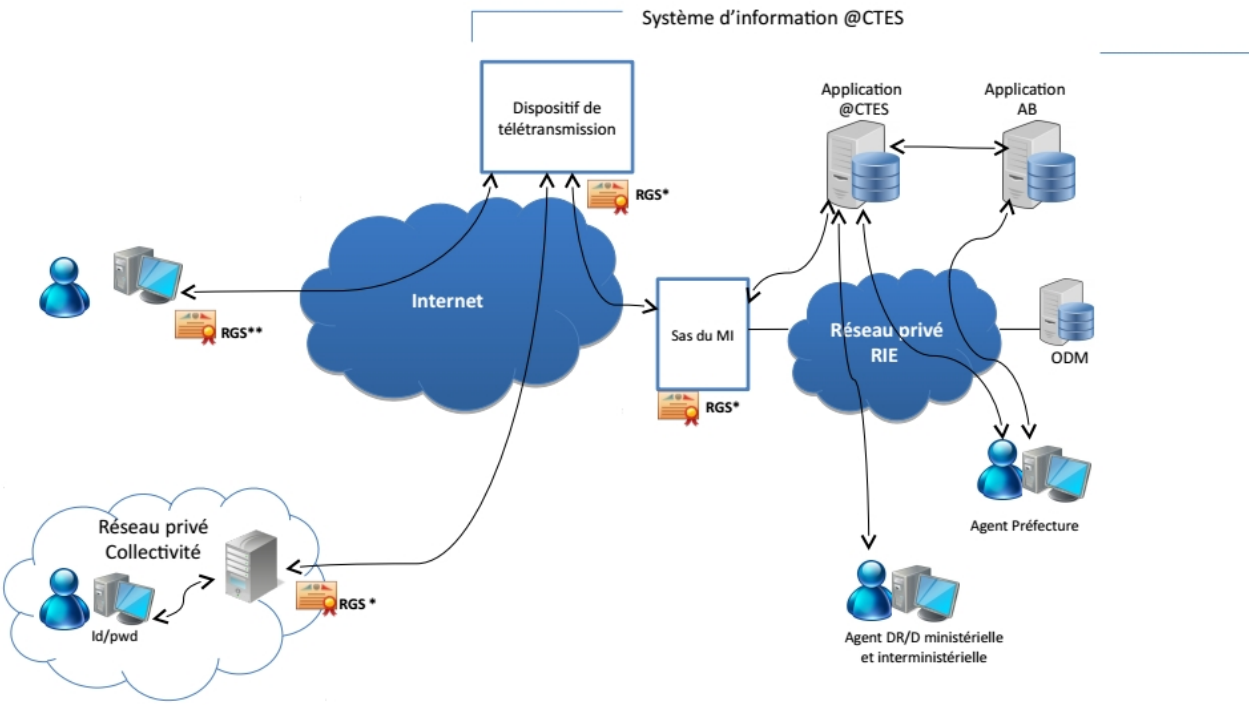

Illustration 1: Schéma global du système d'information @CTES

Le dispositif de télétransmission a pour rôle d'assurer l'identification de la collectivité émettrice, l'intégrité des flux de données entre la plate-forme du ministère de l'Intérieur et la collectivité ainsi que la sécurité des échanges.

Ce système d'information constitue la chaîne de télétransmission au contrôle de légalité. Il a vocation à se substituer aux échanges intervenus sur support physique des échanges électronique dans l'ensemble des étapes qui composent le contrôle de légalité.

À cette chaîne initiale se sont ajoutées d'autres plates-formes. Les actes des collectivités peuvent être générés à partir de progiciels métiers mis à disposition par des éditeurs lesquels seront, selon les cas, interfacés avec les plates-formes de télétransmission ou intégrés à ces dernières. Divers acteurs ont développé d'autres services numériques à destination des collectivités. Le contrôle de légalité dématérialisé est un des services offerts aux collectivités. S'ils n'assurent pas la fonction de télétransmission, les dispositifs qu'ils mettent en œuvre n'ont pas à être homologués.

c) Organisation des échanges

Pour assurer l'ensemble des échanges entre la collectivité et les services de l'État, le système d'information @CTES organise ces échanges en transactions et en flux. Cette partie décrit ces différentes transactions, les flux qui les composent, ainsi que les exigences métiers auxquelles elles se rattachent.

1) Transaction 1 : la transmission d'un acte

La transmission d'un acte par la collectivité conditionne son entrée en vigueur. Sans cette formalité, l'acte en question ne peut être mis en application. En outre, à compter de la réception de l'acte, les services de l'État disposent, sauf exception, de deux mois pour le contrôler. C'est donc une étape importante pour les deux parties impliquées. Elle donne lieu à trois flux dans le système d'information @CTES. Le flux 1.1 est créé par le dispositif à l'aide des informations renseignées par la collectivité. Ces éléments permettent de créer un flux unique pour chaque acte transmis. Les exigences à respecter à ce stade concerne la forme du flux et les modalités de connexion du dispositif au sas du ministère de l'Intérieur.

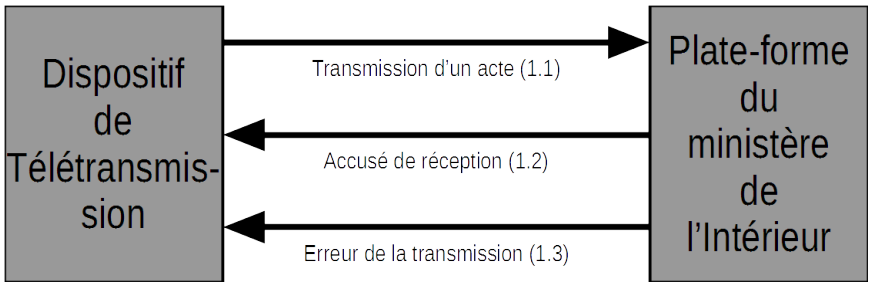

Illustration 2 : Transaction 1, transmission d'un acte

Le flux 1.2 accuse de la réception de l'acte par l'application. Celui-ci est transmis directement par le ministère de l'Intérieur à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte.

Le flux 1.3 est un flux technique. Comme l'accusé de réception, il est transmis à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte. Cependant il ne vaut pas accusé de réception. Il signifie que l'acte n'a pas pu être intégré sur la plate-forme du ministère de l'Intérieur.

2) Transaction 2 : le courrier simple

Le courrier simple appartient à la catégorie des échanges informels qui peuvent survenir entre la collectivité et les services de l'État. Ils n'ont aucune incidence contentieuse et ne modifient de fait pas les délais. Cette transaction est composée de deux flux dans l'application @CTES.

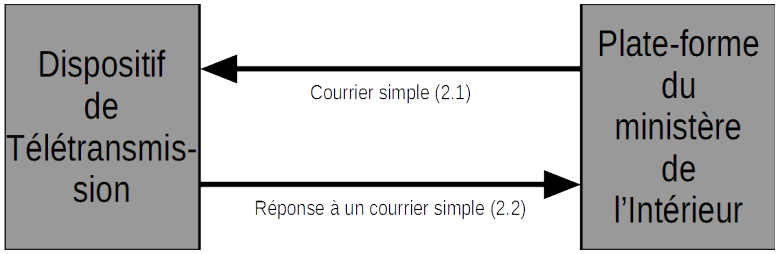

Illustration 3 : Transaction 2, courrier simple

Le flux 2.1 est le courrier simple adressé par le représentant de l'État via l'application @CTES. Il est transmis à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte.

Le flux 2.2 est la réponse de la collectivité au courrier du représentant de l'État. Celui-ci est transmis via le dispositif de télétransmission.

3) Transaction 3 : La demande de pièces complémentaires

La demande de pièces complémentaires survient une fois que l'agent de l'État en charge du contrôle a vérifié la complétude du dossier de l'acte transmis par la collectivité. Cet échange a des incidences contentieuses. Lorsqu'elle est valablement formée, elle a pour effet de modifier la durée du contrôle.

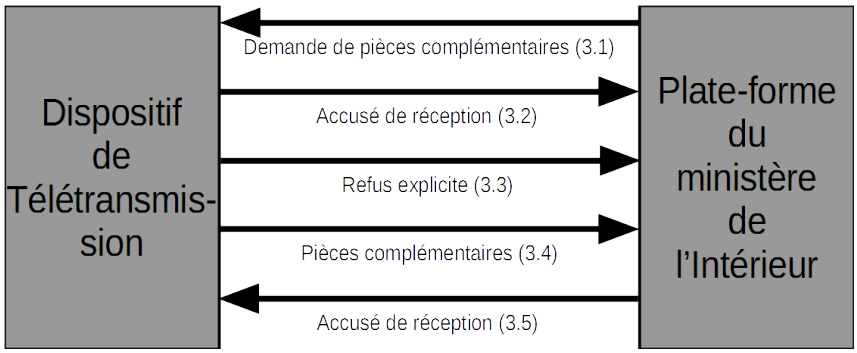

Illustration 4 : Transaction 3, demande de pièces complémentaires

Le flux 3.1 formalise la demande de pièces complémentaires de la préfecture. Il est transmis à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte.

Ce dernier adresse à la plate-forme du ministère de l'Intérieur un accusé de réception de la demande de pièces qui constitue le flux 3.2. Ce flux permet de reporter aussi bien du point de vue logiciel que juridique la date de contrôle.

Les flux 3.3 et 3.4 sont des alternatives offertes à la collectivité. Soit elle choisit de ne pas transmettre les pièces demandées (flux 3.3) soit elle accepte de les transmettre (flux 3.4). Dans un cas comme dans l'autre ce flux est émis via le dispositif.

Un accusé de réception automatique est envoyé par l'application @CTES à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte (flux 3.5). Ce flux permet également de reporter la date de contrôle. Les informations présentes dans l'accusé de réception sont prévues par le schéma des flux XML de l'application @CTES.

4) Transaction 4 : Le recours gracieux

Le recours gracieux marque la première étape contentieuse du contrôle de légalité. Dans cette étape, le représentant de l'Etat demande à la collectivité de retirer ou réformer un acte qu'elle estime contraire au droit. Comme dans la demande de pièce, cette phase a une incidence sur la durée du contrôle. C'est pourquoi les échanges qui interviennent dans cette transaction ont juridiquement une importance particulière.

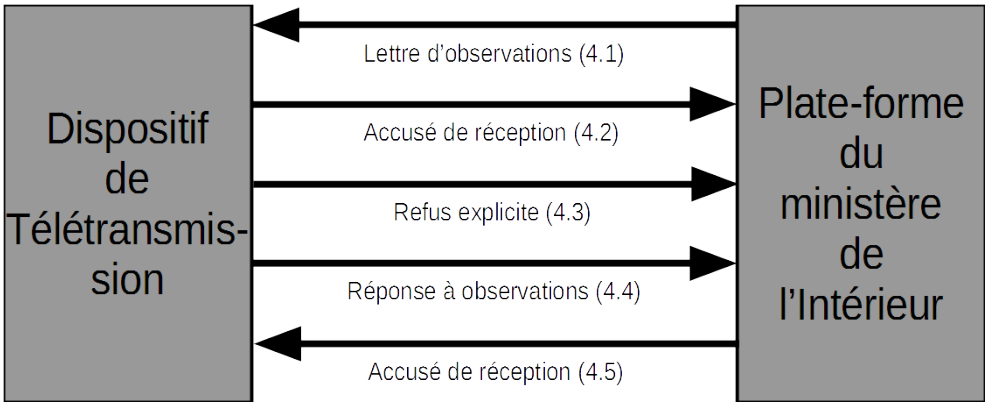

Illustration 5 : Transaction 4, lettre d'observation

Cette transaction débute par une demande sous la forme d'une lettre d'observations adressée par le représentant de l'État à la collectivité par le biais du flux 4.1. Il est transmis à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte.

Ce dernier adresse un accusé de réception qui constitue le flux 4.2. Ce flux permet de reporter aussi bien du point de vue logiciel que juridique la date de contrôle.

Les flux 4.3 et 4.4 sont des alternatives offertes à la collectivité. Soit elle choisit de refuser la demande du représentant de l'État (flux 4.3) soit elle adresse ses observations (flux 3.4). Dans un cas comme dans l'autre ce flux est émis via le dispositif.

Un accusé de réception automatique de la réponse de la collectivité à la lettre d'observation est envoyé par l'application à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte par le flux 4.5. Ce flux permet également de reporter la date de contrôle. Les informations présentes dans l'accusé de réception sont prévues par le schéma des flux XML de l'application @CTES.

5) Transaction 5 : Le déféré au tribunal administratif

Le déféré réside dans la saisine du juge administratif par le représentant de l'État. Cette étape marque le début de la phase juridictionnelle du contrôle de légalité. Le représentant de l'État adresse sa demande au juge et doit en adresser une copie à la collectivité. C'est cette dernière exigence que satisfait la transaction 5.

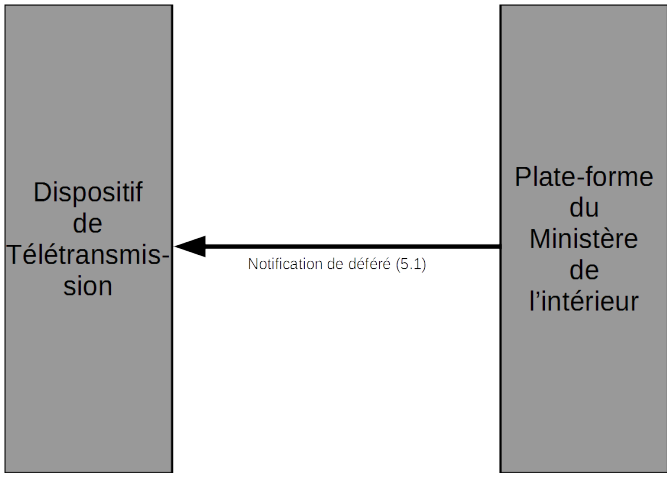

Illustration 6 : Transaction 5, déféré au tribunal administratif

Cette transaction comporte donc uniquement le flux 5.1 qui est adressé à la collectivité et au dispositif. Comme il entraîne peu de conséquences sur la recevabilité de la requête du préfet, il ne nécessite pas que le dispositif accuse réception.

6) Transaction 6 : L'annulation de la transmission d'un acte

L'annulation de la transmission d'un acte n'est pas, à proprement parler, incluse dans le contrôle de légalité. Elle permet à la collectivité d'informer les services de l'État de ne pas tenir compte de certains actes. La transaction 6 a pour objet de permettre cela. L'acte est réputé non reçu par le représentant de l'État et ne sera pas pris en compte par les services du contrôle de légalité. Le flux 6.1 permet à la collectivité d'adresser par le biais du dispositif une annulation.

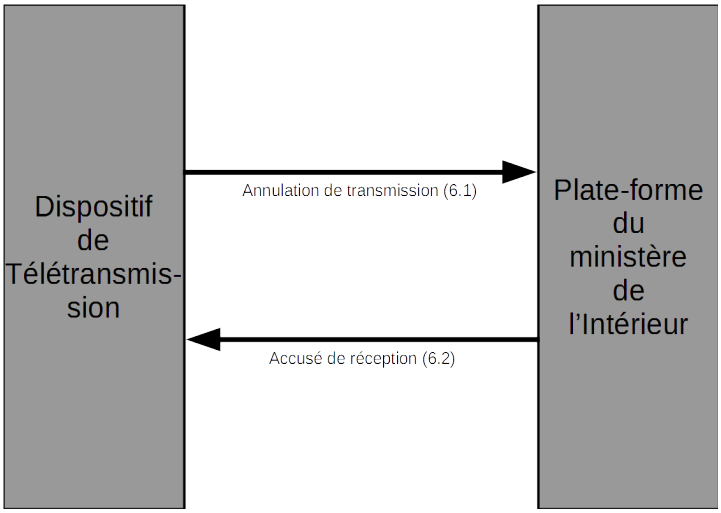

Illustration 7 : Transaction 6, annulation de la transmission d'un acte

Ce flux donne lieu à un accusé de réception matérialisé par le flux 6.2 et adressé à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission de l'acte.

7) Transaction 7 : La mise à jour des tables de référence

Cette transaction est de nature technique. L'application @CTES intègre des tables de référence modifiables qui peuvent avoir une incidence sur la transmission des actes (flux 1).

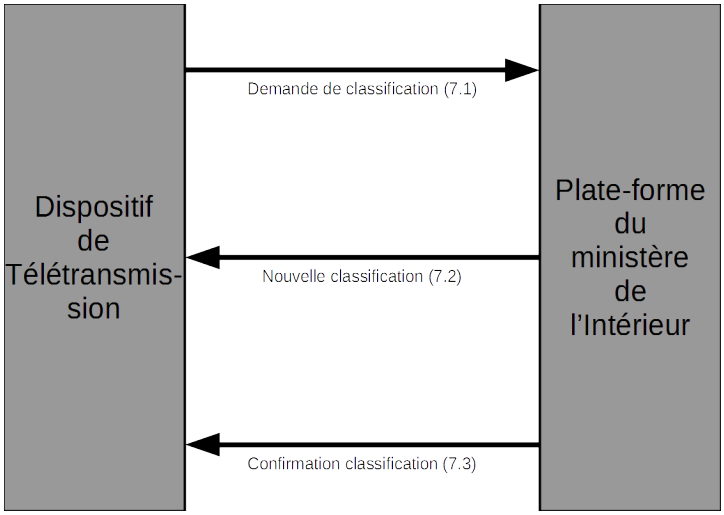

Illustration 8 : Transaction 7, mise à jour de la table des références

La demande de classification par le dispositif (flux 7.1) permet de demander les dernières listes de valeurs des tables de références. À l'issue de quoi, l'application @CTES transmet un flux (7.2) comprenant la nouvelle classification des matières, la nature des actes et la codification des pièces jointes. Suite à ce flux, l'application envoie un flux de confirmation (7.3). Celui-ci est transmis que la demande de mise à jour ait échoué ou non.

2. Caractéristiques exigées en vue de l'homologation du dispositif

Cette partie fixe les exigences que doit respecter le dispositif pour pouvoir être homologué par les services du ministère de l'Intérieur. Elles sont identifiées par la typologie suivante :

Exigence TYPE-XX :

Les éléments énoncés avant ou après ces exigences ne sont pas requis mais servent à leur interprétation.

L'audit mené par le CESTI mentionné dans l'arrêté ne porte que sur les exigences. Celles-ci ont pour vocation à assurer le bon fonctionnement du contrôle de légalité dématérialisé mais aussi l'identification de la collectivité émettrice, l'intégrité des flux de données et la sécurité et la confidentialité des échanges sur le système d'information @CTES.

Ainsi, le présent cahier des charges précise les fonctionnalités nécessaires à l'insertion du dispositif dans l'architecture globale de la télétransmission (a), la norme des échanges entre le dispositif et l'application @CTES (b), la sécurisation de ces échanges (c), les fonctionnalités de traitement des données échangées (d) et les modalités d'exploitation et de gestion des incidents de fonctionnement (e).

a) Fonctionnalités liées à son insertion dans l'architecture globale de la télétransmission

Le dispositif a vocation à s'inscrire dans un écosystème de services numériques aux collectivités. Le contrôle de légalité constitue seulement une des étapes de la vie des actes qu'elles édictent. Les exigences qui suivent visent à permettre au dispositif de s'intégrer efficacement dans ce paysage tout en respectant les exigences d'intégrité des flux et d'identification des parties.

Exigence ARCH-01 : Le dispositif doit intégrer une unité d'horodatage permettant de générer des contremarques de temps des flux qu'il émet vers le dispositif technique du ministère de l'Intérieur ou qu'il reçoit de ce dernier.

L'unité d'horodatage doit :

- Être synchronisée avec le temps UTC selon l'exactitude déclarée ;
- Comporter les fonctionnalités :
  - De maintien du calibrage permettant au dispositif de ne pas dériver à l'extérieur de l'exactitude déclarée ;
  - De détection du respect de l'exactitude déclarée ;
  - D'interruption d'émission des contremarques de temps lorsque l'heure de l'unité est en dehors de l'exactitude déclarée ;
  - Permettant de garantir la synchronisation de l'horloge.

Chaque contremarque de temps générée par l'unité d'horodatage doit :

- Inclure le trigramme d'identification de l'opérateur générant la contremarque ;
- Comporter les informations suivantes : un identifiant unique ; les dates, heures et minutes de la transaction : le numéro de SIREN de la collectivité destinatrice ; le numéro du type de transac-

tion ; le numéro d'acte auquel elle se rapporte.

Les informations de temps portées dans les contremarques doivent pouvoir être reliées à un temps fourni par un laboratoire UTC.

L'horodatage permet de d'accroitre la fiabilité des échanges survenus dans la chaîne de télétransmission. Les contremarques de temps sont susceptibles d'être versées à titre de preuve dans l'hypothèse où la fiabilité de la transmission serait discutée dans le cadre d'un recours juridictionnel. Sous réserve des exigences susvisées, le responsable du dispositif est libre de choisir le mode d'intégration de l'unité d'horodatage ainsi que des flux horodatés.

Exigence ARCH-02 : Le dispositif de transmission doit transmettre en utilisant des adresses IP fixes (au maximum 9) contrôlées par le sas du ministère de l'Intérieur. Si le responsable du dispositif souhaite changer les adresses IP depuis lesquelles il se connecte, il doit en faire la demande aux équipes techniques du ministère de l'Intérieur dans un délai préalable de 15 jours.

Exigence ARCH-03 : Seuls les protocoles de transport HTTP et PESIT, associés au protocole de sécurisation des échanges TLS, sont autorisés. Seules les versions à l'état de l'art de ces protocoles doivent être mises en œuvre. Lors de l'établissement d'une connexion avec le sas ministère de l'Intérieur, la plate-forme de transmission doit être en mesure d'utiliser un couple identifiant/mot de passe qui sera fourni par le ministère de l'Intérieur. Le responsable du dispositif doit être en capacité de changer ce mot de passe régulièrement, à l'initiative du ministère de l'Intérieur.

Exigence ARCH-04 : Le dispositif de télétransmission doit accepter l'authentification du serveur du ministère de l'Intérieur par un certificat d'authentification serveur TLS. En cas de changement il doit être en capacité d'accepter sous 15 jours tout nouveau certificat présenté par le ministère de l'Intérieur.

Exigence ARCH-05 : Le dispositif de télétransmission doit s'authentifier auprès du serveur du ministère de l'Intérieur avec un certificat d'authentification serveur de type client, d'un degré de sécurité au moins égal au niveau * (une étoile) du référentiel général de sécurité. En cas de changement du certificat et de la clé privée associée, le responsable du dispositif transmet le certificat aux équipes techniques du ministère de l'Intérieur 15 jours avant la date de changement.

L'établissement de la connexion entre la plate-forme du dispositif de télétransmission et celle du ministère de l'Intérieur donne lieu à un échange préalable de clés. Il intervient à l'issue de la demande de raccordement et en amont des phases de test qui permettent d'établir ou de rejeter l'homologation. Le renouvellement des certificats et des clés associées donne lieu à un échange direct entre les équipes techniques du ministère de l'Intérieur et le responsable du dispositif.

Exigence ARCH-06 : Les données suivantes doivent être conservées et stockées de façon à être protégées de toute tentative non autorisée d'appropriation, de suppression ou de modification :

- Adresses IP du sas du ministère de l'Intérieur ;
- Clés publiques des certificats d'identification machines et personnes ;
- Données d'identités des personnes utilisatrices du dispositif.

En cas de compromission avérée ou suspectée de l'une de ces données, le responsable du dispositif en informe sans délai les équipes techniques du ministère de l'Intérieur.

Exigence ARCH-07 : Dans le cas où un document joint serait signé électroniquement au format PAdES, le dispositif de télétransmission doit être en mesure d'effectuer la vérification de cette signature électronique. La vérification doit au moins porter sur :

- la signature respecte les formats PAdES,
- les dates de validité et le statut de révocation du certificat de signature à la date ou elle a été apposée,
- la bonne validité cryptographique de la signature
- la cohérence entre le document transmis et l'empreinte sur laquelle porte la signature.

En cas de signature électronique invalide, l'acte concerné ne doit pas être transmis au sas du ministère de l'Intérieur. Cette information doit être mise à disposition la collectivité émettrice. Elle doit préciser le motif ayant conduit à juger la signature invalide.

b) Normes des échanges techniques avec l'application @CTES

Cette partie établit les caractéristiques techniques que doit revêtir le flux des différentes transactions exposées précédemment. Les flux entrant acceptés par le système d'information @CTES sont encapsulés dans une archive « .tar.gz ». Pour pouvoir être intégré l'archive doit contenir au moins deux fichiers XML : l'un constituant l'« enveloppe métier » qui contient les informations de transmission et l'autre le « message métier » constituant le flux tel que décrit précédemment. À ceux-ci sont joints, selon les cas, des fichiers.

Exigence NORME-01 : Le dispositif doit permettre la réception de flux par le protocole SMTP. Il doit vérifier la conformité de ces flux au schéma XML et les porter à la connaissance de la collectivité.

L'application @CTES n'utilise pas le protocole HTTP ou PESIT pour transmettre un flux au dispositif de télétransmission. L'ensemble des flux qui émanent de l'application @CTES sont transmis par le protocole SMTP à la collectivité, au dispositif et à tout autre destinataire mentionné dans le flux de transmission.

Exigence NORME-02 : L'envoi de fichiers sur le sas du ministère de l'Intérieur doit être réalisé via les protocoles HTTP ou PESIT conformément à la norme ARCH-03.

Exigence NORME-03 : Les fichiers XML émis par le dispositif doivent être conformes au schéma XML accessible sur le portail de l'État à destination des collectivités. Le dispositif de création des fichiers XML doit pouvoir être mis à jour sur modification du schéma par les services du ministère de l'Intérieur. Tout fichier XML non valide ne doit pas être transmis vers le sas du ministère de l'Intérieur.

Exigence NORME-04 : L'intégralité des champs prévus par le schéma XML doit être renseignée dans le fichier correspondant. Le dispositif de télétransmission doit vérifier qu'aucun champ n'est vide avant la transmission au sas du ministère de l'Intérieur. Le dispositif ne doit pas inclure des champs autres que ceux indiqués dans le schéma des flux précité.

Exigence NORME-05 : Les fichiers transmis par le dispositif doivent être regroupés dans une archive « tar » compressée au moyen du logiciel de compression « gzip ». Le « fichier archive » doit être nommé suivant les règles suivantes :

- les trois premiers caractères doivent correspondre au trigramme du dispositif,
- les caractères suivants doivent correspondre au nom de l'« enveloppe métier » tel que décrit dans l'exigence NORME-08.

Par exemple un fichier dont le nom du fichier « enveloppe métier » qu'il contient sera :

EACT--179712708--20160101-751.xml

Et dont le trigramme du dispositif est GNU, sera nommé :

GNU-EACT--179712708--20160101-751.tar.gz

Exigence NORME-06 : Le « fichier archive » doit contenir au moins une « enveloppe métier » au format XML à la racine suivie d'un « message métier » au format XML. Il doit contenir une seule « enveloppe métier ».

Un même « fichier archive » peut contenir plusieurs « messages métiers » auxquels peuvent être joint des fichiers aux formats « .pdf », « .xml », « .jpg » et « .png ». L'« enveloppe métier » contient la liste des différents « messages métiers » ce qui permet à l'application @CTES d'effectuer un traitement différencié et à une même collectivité de transmettre plusieurs actes en même temps sans avoir à se ré-authentifier pour chaque envoi.

Exigence NORME-07 : Avant la transmission du « fichier archive » vers le sas du ministère de l'Intérieur, le dispositif doit vérifier :

- qu'il contient au moins deux fichiers XML,
- qu'un seul fichier XML correspond à l'« enveloppe métier »,
- qu'il est correctement nommé,
- que son nom est cohérent avec celui du fichier « enveloppe » qu'il contient,
- qu'il ne dépasse pas la limite de 150 méga octets.

Tout « fichier archive » non conforme ne doit pas être transmis vers le sas du ministère de l'Intérieur.

Exigence NORME-08 : L'« enveloppe métier » doit être établie dans un fichier « .xml » conformément à la structure décrite dans le schéma XML accessible sur le portail de l'État à destination des collectivités. Le fichier « .xml » doit être nommé suivant les règles suivantes :

- le premier champ est composé des caractères EACT,
- le champ suivant est libre,
- le champ suivant est le numéro de SIREN à 9 chiffres de la collectivité émettrice,
- le champ suivant est libre,
- le champ suivant est la date d'envoi composé de huit chiffres au format AAAAMMJJ,
- le champ suivant est un numéro séquentiel de un à 4 chiffres.

Chaque champ doit être séparé d'un tiret.

Le dispositif doit remettre à zéro le numéro séquentiel quotidiennement.

Ainsi, un acte transmis le 1er janvier 2016 par la commune de Fort-de-France qui constitue le 751e envoi de la journée sera nommé de la façon suivante :

EACT--179712708--20160101-751.xml

Exigence NORME-09 : Avant la transmission de l'« enveloppe métier » vers le sas du ministère de l'Intérieur, le dispositif doit vérifier :

- que le nom du fichier respecte les règles de l'exigence NORME-08,

- qu'il y a concordance entre le numéro de SIREN présent dans le nom du fichier XML, et le numéro de SIREN présent à l'intérieur de ce fichier XML,

- que la date correspond à celle de l'unité d'horodatage du dispositif,

- que le ou les fichiers XML « message métier » annoncés par le fichier XML « enveloppe métier » sont présents dans l'envoi.

Ces vérifications doivent s'effectuer avant la transmission de l'enveloppe métier. Elle peut ainsi intervenir avant son archivage dans le « fichier archive ».

Exigence NORME-10 : Le « message métier » doit être établi dans un fichier « .xml » conformément à la structure décrite dans le schéma XML accessible sur le portail de l'État à destination des collectivités. Le fichier « .xml » doit être nommé suivant les règles suivantes :

- le premier champ est composé de trois caractères correspondant au numéro de département dans lequel se situe la collectivité,

- le champ suivant est le numéro de SIREN à 9 chiffres de la collectivité émettrice,

- le champ suivant est la date d'envoi composé de huit chiffres au format AAAAMMJJ,

- le champ suivant est composé de un à 15 caractères alphanumériques indiquant le numéro de l'acte de la collectivité,

- le champ suivant est composé de deux lettres correspondant au code nature de l'acte,

- le champ suivant indique le numéro de la transaction à un chiffre,

- le champ suivant indique le numéro de flux à un chiffre,

- le champ suivant indique le numéro séquentiel de 1 à deux chiffres du fichier dans l'ensemble des fichiers relatifs au même message métier.

Le dispositif doit remettre à zéro le numéro séquentiel du fichier pour chaque message métier. Le fichier « message métier » doit avoir 0 pour numéro séquentiel.

Le numéro séquentiel doit être séparé des autres par un tiret bas. Les autres champs doivent être séparés par un tiret.

Ainsi, le contrat numéro FDF24122015 transmis le 1er janvier 2016 par la commune de Fort-de-France qui constitue le 751e envoi de la journée sera nommé de la façon suivante :

972-179712708-20160101-FDF24122015-CC-1-1_0.xml

Exigence NORME-11 : Le nom des fichiers joints au « message métier » doit être nommé suivant les règles suivantes :

- le premier champ est composé de 5 caractères et doit correspondre au code de la pièce jointe,

- les champs suivants doivent correspondre au nom du « message métier » tel que décrit dans l'exigence NORME-10.

Les champs doivent être séparés par un tiret.

Tout fichier dont le nom n'est pas conforme à ces exigences ne doit pas être transmis. Un message d'erreur est mis à disposition de la collectivité. Il indique les raisons qui conduisent à l'échec de la transmission.

Il s'agit des pièces jointes à l'acte. Ainsi, l'acte d'engagement du contrat numéro FDF24122015 transmis le 1er janvier 2016 par la commune de Fort-de-France qui constitue le 751e envoi de la

journée sera nommé de la façon suivante :

01_AE-972-179712708-20160101-FDF24122015-CC-1-1_1.pdf

Exigence NORME-12 : Le dispositif doit vérifier au moment de l'envoi du « message métier » et des fichiers qui sont joints :

- que le nom du fichier respecte les règles des exigences NORME-11 et NORME-12,

- qu'il y concordance entre le numéro de SIREN présent dans le nom du fichier XML, et le numéro de SIREN présent à l'intérieur de ce fichier XML,

- que la date correspond à celle de l'unité d'horodatage du dispositif,

- que le ou les documents joint annoncés dans le fichier XML « message métier » sont présents dans l'envoi,

- que les documents joints sont au format « .pdf », « .xml », « .jpg » ou « .png ».

Exigence NORME-13 : Pour former le nom des fichiers transmis, le dispositif doit utiliser les codes nature, matière et pièces jointes tel que retournés dans le flux 2 de la transaction 7 émis par l'application @CTES.

Afin de faciliter l'intégration des schémas XML au dispositif de télétransmission, une notice explicative y sera jointe. Elle comprendra une description des balises métier et de leur finalité ainsi qu'une liste des codes matière, nature et pièces jointes de l'application.

c) Sécurisation des échanges avec l'application @CTES

La sécurisation de la télétransmission vise principalement quatre objectifs ;

1. **Assurer l'authenticité et la confidentialité de l'ensemble des échanges effectués entre les diffférents partenaires du système d'information @CTES sur Internet ;**
2. **Assurer l'intégrité et la disponibilité des dispositifs de télétransmission ;**
3. **Assurer l'identification des agents ou collectivités qui télétransmettent dans @CTES, la traçabilité et de la date de leur transmission ;**
4. **Assurer le respect de la réglementation en vigueur en matière de sécurité des systèmes d'information.**

Exigence SEC-01 : Pour l'authentification d'un agent d'une collectivité lors de l'accès à la fonction de transmission le dispositif doit exiger l'usage exclusif d'un moyen d'identification personnel, d'un degré de sécurité au moins égal au niveau substantiel du référentiel général de sécurité. Le dispositif doit vérifier le niveau de sécurité du moyen d'identification présenté lors de l'enrôlement de l'agent, ainsi que sa bonne adéquation à l'usage prévu.

Exigence SEC-02 : Pour l'authentification d'une application métier ou d'un serveur d'une collectivité lors des échanges avec le dispositif de télétransmission, il est exigé l'usage exclusif d'un moyen d'identification de serveur d'un degré de sécurité au moins égal au niveau élémentaire du référentiel général de sécurité. Le dispositif doit vérifier le niveau de sécurité du moyen d'identification présenté lors de l'enrôlement de la collectivité, ainsi que sa bonne adéquation à l'usage prévu.

Ces exigences ont pour but d'identifier la collectivité émettrice de l'acte. Cette identification peut être rapportée de deux façons.

Soit l'agent d'une collectivité accède au dispositif au moyen d'un portail. Le cas échéant, l'exigence

SEC-01 s'applique : un certificat d'identification personnel est exigé de l'agent lors de l'accès à la fonction de transmission.

Soit l'agent accède à la fonction par l'intermédiaire d'une application métier ou d'un serveur auxquels il accède par un réseau interne à la collectivité. Auquel cas, le dispositif de télétransmission exige une authentification au moyen d'un certificat serveur conformément à l'exigence SEC-02.

Exigence SEC-03 : Le dispositif peut intégrer le moyen d'authentification « France connect agent » sous réserve que celui-ci accepte les certificats de niveau égal ou supérieur à celui exigé dans l'exigence SEC-01.

Exigence SEC-04 : Pour l'authentification serveur du dispositif de télétransmission auprès des collectivités, il est exigé l'emploi de certificats d'authentification serveur TLS répondant au degré de sécurité au moins égal au niveau élémentaire du référentiel général de sécurité.

Exigence SEC-05 : L'authentification de la collectivité n'a pas à répondre aux exigences SEC-01, SEC-02 et SEC-04 lorsque le dispositif est localisé sur un réseau local accessible uniquement à cette dernière et qu'elle l'exploite dans son intérêt exclusif.

Exigence SEC-06 : Les clés privées associées aux certificats d'authentification du dispositif doivent faire l'objet d'une protection appropriée, conformément aux prescriptions contenues dans le référentiel général de sécurité.

Exigence SEC-07 : Le dispositif doit disposer d'un référentiel des personnes ou plates-formes qui lui sont raccordés et autorisés à transmettre électroniquement. Le référentiel doit inclure une liste des révocations.

Ce référentiel doit être mis à jour de façon régulière et doit comprendre au moins :

- Pour chaque entité référencée, la raison sociale de cette entité et le numéro SIREN correspondant.
- Les données d'identification des collectivités, des agents des collectivités, et les certificats des plates-formes référencés.

Exigence SEC-08 : Lors de la présentation d'un certificat, le dispositif doit assurer le contrôle :

- des dates de validité et du statut de révocation du certificat présenté,
- de la chaîne de certification associée, jusqu'à une racine de confiance,
- de la bonne appartenance du certificat à une collectivité ou un agent d'une collectivité.

L'échec de l'un d'entre eux doit entraîner le rejet de l'authentification.

Exigence SEC-09 : La documentation de mise en œuvre et d'exploitation du dispositif doit inclure explicitement la prise en compte organisationnelle et technique des modalités décrites ci-dessus de protection des clés privées, d'enrôlement initial et de mise à jour le cas échéant des données relatives aux collectivités référencées.

Exigence SEC-10 : Le dispositif doit intégrer les mesures de sécurité permettant de lutter, efficacement et de façon proportionnée, contre les attaques Internet connues telles que l'intrusion, le déni de service et les programmes malveillants. Il appartient au responsable du dispositif de maintenir le niveau de sécurité du dispositif à l'état de l'art, en tenant compte, de l'évolution des risques numériques et des technologies de sécurité disponibles.

Exigence SEC-11 : Le dispositif de télétransmission doit être isolé et cloisonné des autres environ-

nements ne faisant pas également l'objet d'une homologation par les services de l'État.

Le dispositif doit, en principe être isolé des autres applications mises en œuvre par l'opérateur. Il est possible cependant de l'installer sur une machine (physique ou virtuelle) contenant d'autres dispositifs homologués par les services de l'État tel qu'HELIOS / PES V2.

Exigence SEC-12 : Le responsable du dispositif assure lui-même la gestion du référentiel des certificats délivrés pour la télétransmission. En aucun cas le responsable ne peut sous-traiter ou permettre à des tiers d'assurer la gestion de ce référentiel. Le responsable effectue la révocation des certificats sur demande du porteur ou à leur expiration et ajoute les nouveaux certificats.

Afin d'assurer une exploitation répondant aux exigences de sécurités précitées, le responsable du dispositif est invité à respecter les règles de sécurité figurant dans le guide d'hygiène informatique publié par l'ANSSI, ainsi qu'à se référer aux autres guides de bonnes pratiques disponibles dans les domaines « Applications Web », « Postes de travail et serveurs » et « Réseaux », et publiés sur le site de l'ANSSI.

Plus généralement, il a un devoir de conseil, de sensibilisation et de promotion de la sécurité envers les collectivités qui lui sont raccordés. Le respnsable du dispositif a également un devoir d'information et d'alerte envers le ministère de l'Intérieur quant à toute constatation d'atteinte à la sécurité ou de non-conformité aux exigences du présent cahier des charges de la part d'une collectivité ou d'une plate-forme lui étant raccordé.

d) Fonctionnalités de traitement des données échangées

Exigence FONCT-01 : Le dispositif doit intégrer des fonctionnalités de contrôle de flux, permettant la limitation des transmissions vers le sas du ministère de l'Intérieur :

- limitation du volume de données transmis (en nombre de mégaoctets par heure) ;
- limitation à des créneaux horaires de transmission paramétrables.

Exigence FONCT-02 : Le dispositif doit avoir la capacité de stocker provisoirement les transactions venant de collectivités, afin de faire face à une limitation des flux ou à un arrêt provisoire, prévu ou non, du service technique du ministère de l'Intérieur. Ce stockage doit pouvoir être assuré au moins sur une durée de deux jours ouvrés.

Exigence FONCT-03 : Le dispositif doit intégrer une fonctionnalité de relance automatique permettant de garantir l'acheminement des actes des collectivités à l'infrastructure centralisée du ministère de l'Intérieur sans intervention complémentaire des collectivités, même en cas d'indisponibilité temporaire de la plate-forme du ministère de l'Intérieur.

Exigence FONCT-04 : Le dispositif doit permettre à la collectivité d'émettre les flux suivants :

- transaction 1, flux 1 : transmission d'un acte,
- transaction 2, flux 2 : réponse à un courrier simple,
- transaction 3, flux 3 : refus explicite de transmission de pièces complémentaires,
- transaction 3, flux 4 : transmission de pièces complémentaires,
- transaction 4, flux 3 : refus explicite à une lettre d'observation,
- transaction 4, flux 4 : réponse à une lettre d'observation,
- transaction 6, flux 1 : annulation de transmission.

Exigence FONCT-05 : Le dispositif doit conserver les traces des fichiers transmis au ministère de l'Intérieur. Ces traces doivent identifier intelligiblement la nature et les noms des documents, les « date et heure » de transmission et les informations concernant l'agent ou la collectivité à l'origine de la transmission.

Elles doivent pouvoir être exportables, interprétables dans un tableur, avec une ligne pour chaque fichier transmis, et une colonne pour chacun des éléments suivants relatifs aux fichiers transmis : date de transmission, heure de transmission, fuseau horaire, nom du fichier transmis « .tar.gz. », nom des fichiers contenus dans le fichier « .tar.gz. », le numéro de SIREN, le département et l'arrondissement de la collectivité émettrice, les informations relatives à l'agent transmetteur le cas échéant.

Cette exigence vise à identifier les auteurs d'une transaction. S'agissant des personnes ou des collectivités, elles se bornent à reprendre celles contenues dans le certificat présenté lors de l'accès à la fonction de transmission.

Exigence FONCT-06 : Le dispositif doit intégrer les fonctionnalités nécessaires pour permettre à la collectivité d'émettre et de recevoir l'ensemble des transactions décrites dans le schéma des flux XML.

Exigence FONCT-07 : Le dispositif intègre une fonctionnalité destinée à assurer le collationnement et la mise à jour régulière des informations fournies par la collectivité.

Exigence FONCT-08 : Le dispositif intègre une fonction d'accusé de réception. Cette fonctionnalité est automatiquement activée à la réception d'un flux de la plate-forme du ministère de l'Intérieur. Elle doit également informer instantanément la collectivité de la réception du flux au moyen d'un courrier électronique adressé à la boite mail renseignée au moment de la transmission de l'acte. Cette fonction est horodatée dans les conditions prévues à l'exigence ARCH-01 du présent cahier des charges.

Exigence FONCT-09 : Si le dispositif transmet un document budgétaire au format XML, il doit vérifier :

- que le fichier comprend une balise de scellement,
- qu'il est accompagné d'un fichier au format « .pdf », « .jpeg » ou « .png ».

Les documents budgétaires sont identifiés par leur transmission dans la matière 7.1 et la nature 5. Le fichier accompagnant le document budgétaire au format XML est la délibération qui l'approuve.

e) Modalités d'exploitation et de gestion des incidents de fonctionnement

Les exigences détaillées ci-dessous ne seront généralement pas vérifiées au moment de l'audit permettant l'homologation. Elles sont des conditions à son maintien. Tout manquement constaté pourra, le cas échéant, donner lieu à l'une des sanctions prévues dans l'arrêté approuvant le présent cahier des charges.

Exigence EXPL-01 : Le responsable du dispositif s'assure de la confidentialité des informations échangées qu'il détient au titre de l'activité qu'il exerce en application du présent cahier des charges. Il ne peut exploiter aucune donnée à caractère personnel, en dehors de l'exploitation nécessaire à la transmission des actes. Il ne peut diffuser d'informations contenues dans les actes soumis au contrôle de légalité et au contrôle budgétaire excepté celles nécessaires à la transmission au représentant de l'Etat.

Exigence EXPL-2 : Le responsable du dispositif doit être en mesure de gérer les éventuels incidents de fonctionnement survenant sur son dispositif tout en garantissant une assistance aux collectivités. Il doit traiter les demandes des dites collectivités et ne peut les renvoyer vers les représentants de l'Etat ou le ministère de l'Intérieur.

Exigence EXPL-3 : Le responsable ne peut inclure dans les contrats le liant avec les collectivités de clause d'exclusion ou de limitation de sa responsabilité concernant la mise en place, le fonctionnement et la maintenance du dispositif de télétransmission des actes. Seules les clauses d'exclusion ou de limitation de la responsabilité pour force majeure peuvent être incluses dans le contrat.

Exigence EXPL-4 : En cas d'incident majeur portant potentiellement atteinte à la sécurité et à l'intégrité du système d'information @CTES, le responsable du dispositif informe le ministère de l'Intérieur dans les plus brefs délais. Le cas échéant, il joint à son courrier un rapport de gestion d'incident.

Exigence EXPL-5 : Le responsable adresse au ministère de l'Intérieur une déclaration de changement avant le 31 décembre de chaque année et ponctuelle dès qu'intervient un changement technique majeur sur le dispositif, un changement juridique sur la personne morale responsable du dispositif ou encore un changement des conditions d'hébergement.

Par changement technique majeur, on entend toute mise à jour logicielle ou modification matérielle pouvant impacter l'identification de la collectivité, la sécurité de la télétransmission @CTES ou l'intégrité des flux de données.

Exigence EXPL-6 : Le responsable fournit aux équipes techniques du ministère de l'Intérieur, lors de la demande de raccordement, une adresse de messagerie tenue à jour.

Cette adresse permet au ministère de l'Intérieur de communiquer au responsable du dispositif des avis de maintenance, des informations générales sur la transmission des actes, des demandes de régulation de flux ainsi que des demandes liées à la mise en œuvre des obligations du présent cahier des charges. Aussi, il est préférable qu'il s'agisse d'une adresse fonctionnelle régulièrement consultée par les personnes responsables de l'exploitation du dispositif.

Exigence EXPL-8 : Le responsable doit maintenir à jour un document d'architecture globale du dispositif décrivant notamment l'architecture de sécurité, ses composants, flux et accès associés.

Un document d'exploitation doit regrouper l'ensemble des procédures concernant les opérations courantes effectuées sur le dispositif (gestion des comptes, mise à jour logicielle, modification de configuration, détection d'incident...).

Exigence EXPL-09 : La documentation de mise en œuvre et d'exploitation du dispositif doit prévoir explicitement les modalités de prise en compte des demandes de limitation des flux du ministère de l'Intérieur.

Exigence EXPL-10 : La documentation de mise en œuvre et d'exploitation du dispositif de télétransmission doit inclure explicitement la prise en compte organisationnelle et technique des modalités décrites ci-dessus de gestion des adresses IP fixes, clés privées et mots de passes, les échanges avec le ministère de l'Intérieur, ainsi que les politiques de vérification des signatures électroniques.

Exigence EXPL-11 : Le responsable du dispositif doit être en mesure de fournir, à la demande du ministère de l'Intérieur, la liste des documents transmis sur une période donnée. Cette liste fera l'objet d'un archivage pendant une durée de deux ans.

Exigence EXPL-12 : Le responsable du dispositif doit conserver pendant deux ans les traces relatives à l'accès à la fonction de transmission électronique des actes, les contremarques de temps ainsi

que les accusés de réception émis par l'application @CTES.

Ces traces doivent permettre de prouver l'implication d'un partenaire dans une transaction de transmission de données, et ce, de manière irréfutable.

Exigence EXPL-13 : À la demande du ministère de l'Intérieur, le responsable devra suspendre la transmission des actes.

Pour les besoins de maintenance du système, la connexion au sas du ministère de l'Intérieur pourra être interrompue une demi-heure par mois en heures ouvrables. Les équipes techniques du ministère avertiront le responsable trois jours ouvrés à l'avance.

Avant toute sollicitation du ministère de l'Intérieur, le responsable du dispositif contactera le service en charge du maintien opérationnel du système d'information @CTES afin d'aborder le problème rencontré. Dans l'éventualité où la résolution du problème ne serait pas possible en local, les sollicitations réciproques entre les équipes techniques du ministère et le responsable se feront par voie de messagerie électronique.

Le responsable peut solliciter les équipes techniques du ministère de l'Intérieur :

- **En cas de problèmes de transmission des fichiers entre le dispositif de télétransmission et le sas du ministère de l'Intérieur en ayant effectué au préalable les opérations de diagnostic de l'incident ;**
- **En cas d'indisponibilité des serveurs du ministère de l'Intérieur ;**
- **En cas de problèmes ou de sollicitations liées à la sécurité des échanges (changement de mot de passe, etc.).**

Le cas échéant, les services techniques du ministère de l'Intérieur, répondront dans les quatre heures ouvrées.

Les services techniques du ministère de l'Intérieur doivent pouvoir en tant que de besoin prendre contact avec les responsables d'exploitation de la plate-forme d'exploitation de transmission, afin de mettre en œuvre ponctuellement des mesures de limitation de flux. La prise en compte de ces limitations doit être faite dans les quatre heures suivant la demande du ministère de l'Intérieur (entre 8h30 et 18h30, heures métropole, les jours ouvrables).