Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR
ET DE L'AMENAGEMENT DU TERRITOIRE

Cahier des charges

des dispositifs de télétransmission des actes soumis au contrôle de légalité

Annexe 2 : sécurisation des échanges

Version 1.01 21 octobre 2005

1. OBJET DU DOCUMENT

Le présent document est une annexe au cahier des charges de la télétransmission et décrit les modalités de sécurisation des télétransmissions de données au représentant de l'Etat par les collectivités locales dans le cadre du contrôle de légalité.

2. PRINCIPES

La sécurisation de la télétransmission vise deux objectifs :
- Authentification réciproque : s'assurer qu'une transmission vient bien de celui qui dit l'avoir envoyé, et qu'il a bien été remis à son destinataire et non à un usurpateur,
- Intégrité : s'assurer que le fichier transmis n'a pas été altéré lors du transfert.

3. SECURISATION DES DEPOTS DE FICHIERS SUR LES SERVEURS DU MIAT

L'intégrité des données transmises et l'authentification réciproque est assurée par l'utilisation :
- d'une connexion HTTPs ou FTPs avec certificats ;
- d'adresses IP prédéfinies par le dispositif ;
- d'un login et d'un mot de passe de connexion pour chaque dispositif.

Exigence n° 3-1

Le dispositif doit être capable d'ouvrir et de maintenir avec le serveur du MIAT :
- soit une connexion HTTPS en SSL/TLS (conformément aux spécifications du paragraphe 6.1.1 de l'annexe 1 au présent cahier des charges)
- soit une connexion FTPs sécurisée avec TLS (conformément aux spécifications du paragraphe 6.1.2 de l'annexe 1 au présent cahier des charges).

Le dispositif doit supporter une authentification mutuelle avec le serveur MIAT par certificats d'authentification.

Exigence n° 3-2

Le dispositif doit être capable de s'authentifier auprès du serveur du MIAT à l'aide d'un certificat conforme aux spécifications du paragraphe 5.1 du présent document.

Exigence n° 3-3

Le dispositif doit être capable d'accepter l'authentification du serveur du MIAT par un certificat serveur présenté lors de la négociation SSL/TLS.

La convention de raccordement prévoit que le MIAT peut changer son certificat serveur, auquel cas il en informera l'opérateur du dispositif, qui devra si nécessaire adapter son dispositif ou le paramétrage de ce dispositif en conséquence.

Exigence n° 3-4

Le dispositif doit être capable de télétransmettre en utilisant des adresses IP fixes (au maximum 3), contrôlées par les équipements de sécurité du MIAT.

Dans le cas d'une connexion HTTPs, une fois cette connexion ouverte, la plate-forme du MIAT propose une interface HTML de dépôt de fichiers, avec authentification par un identifiant et un mot de passe. Le dépôt des fichiers manuel est donc possible, mais au moment du raccordement d'un dispositif, le MIAT fournira, à l'opérateur dudit dispositif, des informations (l'URL à utiliser pour le transfert de fichier) permettant d'automatiser le dépôt de fichier, évitant ainsi le recours à une alimentation manuelle de formulaires HTML.

Exigence n° 3-11

Dans le cas où HTTPs est utilisé, le dispositif doit être capable, une fois la connexion HTTPs ouverte, d'utiliser cette connexion pour transférer un fichier à une URL donnée (par exemple avec des outils tels que cURL).

Exigence n° 3-11 bis

Dans le cas où FTPs est utilisé, le dispositif doit être capable de déposer le fichier dans un répertoire donné du serveur FTPs du MIAT, en s'authentifiant avec identifiant et mot de passe au travers des commandes protocolaires FTP standard USER PASS.

La convention de raccordement signée entre l'opérateur du dispositif de télétransmission et le MIAT prévoit que l'opérateur doit assurer, au sein de son infrastructure, la protection en confidentialité des secrets d'identification et d'authentification au serveur MIAT :

- l'identifiant et le mot de passe,
- les adresses IP fixes, dédiées à un dispositif unique, utilisées par les machines depuis lesquelles le dispositif dépose les fichiers
- la protection de la clé privée associée au certificat d'authentification du dispositif.

Toute divulgation ou suspicion d'atteinte à la confidentialité de ces éléments est de nature à favoriser l'usurpation d'identité du tiers. L'opérateur, par son organisation et les mécanismes de sécurité mis en œuvre dans son système, devra être en mesure de détecter ces événements. En cas de survenance, il informera immédiatement les équipes techniques du MIAT.

La convention de raccordement prévoit également que le mot de passe attribué au dispositif pour le raccordement au système mis en place par le MIAT doit être **changé** régulièrement, à l'initiative du MIAT, et que si l'opérateur souhaite changer les adresses IP depuis lesquelles son dispositif, se connecte, il doit en faire la demande aux équipes techniques du MIAT avec un délai préalable de 15 jours.

Exigence n° 3-12

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 gestion des adresses IP fixes, clés privées et mots de passes, et les échanges avec le MIAT sur le sujet.

Même si le schéma XML décrivant les échanges métier inclut les espaces réservés pour les signatures électroniques des fichiers joints, la prise en compte de la signature dans le système ACTES n'est pas encore effective. La présence de ces signatures, incluses à l'emplacement prévu, dans les fichiers envoyés aux préfectures, ne sont pas encore obligatoires. Toutefois, cette obligation est prévue dans une évolution future du système et donc du présent cahier des charges d'homologation.

Exigence n° 3-13

Ainsi, au cas où la signature d'un document joint (acte ou annexe) serait incluse, le dispositif de télétransmission doit être en mesure d'en effectuer le contrôle, et empêcher la transmission à la plate-forme du MIAT les actes dont la signature n'était pas valide au moment de la signature par l'expéditeur.

4. SECURISATION DES ECHANGES ENTRE LA COLLECTIVITE ET SON DISPOSITIF DE TELETRANSMISSION

Ce paragraphe porte sur la sécurisation des envois d'informations d'une collectivité à son dispositif de télétransmission, quand ces informations sont ensuite transmises à la sphère Etat. Il est important de remarquer que selon la répartition décidée entre la collectivité et son dispositif, le dispositif peut assurer l'intégralité de la mise en forme des informations conformément à la norme d'échange, ou bien avoir un rôle limité à transmettre des informations déjà mises en forme en amont.

Exigence n° 3-5

Pour chaque transmission, le dispositif de télétransmission doit authentifier la collectivité émettrice aux moyens de certificats présentés par les agents et/ou les infrastructures de cette dernière.

Exigence n° 3-14

Le dispositif de télétransmission doit disposer d'un certificat serveur afin d'assurer l'authentification mutuelle par certificat avec les agents ou infrastructures des collectivités clientes. Ce certificat respectera les spécifications du paragraphe 5.2 du présent document.

Exigence n° 3-15

La documentation de mise en œuvre et d'exploitation du dispositif prévoira les mesures de protection de la clé privée du certificat serveur du dispositif, qui devra être conforme à la politique de certification type (PC Type) niveau « 2 étoiles ».

Exigence n° 3-6

Un dispositif doit être capable d'accepter les transmissions d'information par des collectivités, s'authentifiant avec des certificats. Il devra, en toute hypothèse, accepter au moins certains des certificats conformes aux spécifications du paragraphe 5.2 du présent document.

Exigence n° 3-16

La documentation de mise en œuvre et d'exploitation du dispositif doit prévoir et détailler les processus de mise à jour du paramétrage du dispositif permettant d'accepter, pour l'authentification des collectivités, uniquement les certificats conformes aux spécifications du paragraphe 5.2 du présent document.

Exigence n° 3-7

Lorsqu'une collectivité transmet des informations à destination de la « sphère Etat », avant d'en effectuer le transfert effectif à la sphère Etat, le dispositif doit contrôler la validité du certificat d'authentification utilisé au regard de la liste de révocation mise à disposition par l'Autorité de Certification.

Exigence n° 3-18

La documentation de mise en œuvre et d'exploitation du dispositif prévoira la vérification que les certificats présentés par les collectivités sont valides (contrôle total de la chaîne de confiance et de la CRL).

Exigence n° 3-17

Le dispositif de télétransmission devra disposer d'un référentiel des collectivités qui lui sont raccordées et autorisées à télétransmettre, identifiées par leur numéro SIREN, et en concordance avec les conventions signées (conformément aux termes du décret n° 2005-324 du 7 avril 2005) entre les préfets et les collectivités locales. Le référentiel inclura les certificats d'authentification utilisés par chaque collectivité raccordée.

La convention de raccordement prévoit que l'opérateur du dispositif a pour obligation de mettre à jour ce référentiel en fonction des conventions locales (signées entre le préfet et la collectivité) qui lui sont communiquées par les collectivités avec lesquelles il contracte. Seules les collectivités qui auront transmis à l'opérateur un exemplaire de cette convention locale, et pour lesquelles la durée de validité de la convention locale n'a pas expiré, pourront figurer dans ce référentiel.

Exigence n° 3-8

Lorsqu'une collectivité transmet des informations à destination de la « sphère Etat », avant d'en effectuer le transfert effectif à la sphère Etat, le dispositif doit contrôler que le certificat présenté par la collectivité appartient bien à une collectivité (ou à un agent d'une collectivité) inscrite dans le référentiel mentionné ci-dessus.

Exigence n° 3-9

Lorsqu'un fichier est transmis à la « sphère Etat », le dispositif doit s'assurer que le numéro de SIREN émetteur présent dans les fichiers transmis à la sphère Etat (ce numéro de SIREN étant présent dans des noms de fichiers et dans un élément du fichier XML "enveloppe", cf. annexe 1 au présent cahier des charges) correspond bien au numéro SIREN de la collectivité tel qu'inscrit dans le référentiel mentionné ci-dessus.

Exigence n° 3-10

Pour les transmissions d'information en provenance des collectivités, le dispositif doit prévoir des mécanismes garantissant que les données reçues de la collectivité n'ont pas été altérées ou modifiées au cours de la transmission. A titre de recommandation, les protocoles suivants peuvent être utilisés : SSL/TLS, IPSEC, SSH et toute autre évolution technologique.

5. CERTIFICATS

5.1. Certificats acceptables pour l'authentification des dispositifs auprès du MIAT

Les certificats que peuvent utiliser les dispositifs pour s'authentifier auprès du serveur du MIAT sont :

1) Les certificats émis par une autorité de certificat référencée au niveau de sécurité fort (**) de la PRIS v1 (Politique de Référencement Intersectorielle de Sécurité version 1), et ce durant toute la validité juridique de la PRIS v1.

2) Les certificats délivrés par une autorité de certification agréée pour les téléservices du MINEFI. La liste de ces autorités de certifications est disponible à l'adresse : http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm.

3) Les certificats serveurs émis par une autorité de certification référencée au niveau de sécurité fort (**) de la PRIS v2, dès que la PRISv2 s'appliquera.

La convention de raccordement prévoit que l'opérateur mettra à jour, en tant que de besoin, le certificat qu'utilise son dispositif pour s'authentifier auprès de la plate-forme du MIAT. Il transmettra le certificat aux équipes techniques du MIAT, pour prise en compte, au minimum 15 jours avant la date de changement.
En particulier, en fonction de la rapidité d'entrée en vigueur de la PRIS v2, de se mettre en conformité avec la PRIS v2 , le MIAT pourra demander à l'opérateur de se mettre, dans un délai de 3 mois, en conformité avec la PRIS v2, quel que soit le certificat utilisé auparavant.

5.2. Certificats acceptables pour l'authentification des collectivités auprès des dispositifs

Les certificats que pourra accepter un dispositif pour l'authentification des collectivités sont :

1) Les certificats émis par une autorité de certificat référencée au niveau de sécurité fort (**) de la PRIS v1 (Politique de Référencement Intersectorielle de Sécurité version 1), et ce durant toute la validité juridique de la PRIS v1.

2) Les certificats délivrés par une autorité de certification agréée pour les téléservices du MINEFI. La liste de ces autorités de certifications est disponible à l'adresse : http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm#Les familles de certificats référencées.

3) Les certificats émis par une autorité de certification référencée au niveau de sécurité fort (**) ou « 3 étoiles » (***) de la PRIS v2, dès que la PRISv2 s'appliquera :
   - certificat d'authentification « agent » si la transmission est effectuée directement par un agent de la collectivité,
   - certificat serveur si la transmission est effectuée par un système (serveur d'une infrastructure)