

Diffusion		
HADOPI	EXTELIA	FAI

Classification : DOCUMENT CONFIDENTIEL

1 Objet du document

L'objet de ce document est de spécifier aux FAIs les modalités d'échanges attendues avec le Système d'Information de l'HADOPI. Ce document couvre :

- la phase d'identification des abonnés
- l'envoi des recommandations aux abonnés

Ce document pourra évoluer notamment pour tenir compte des modifications et compléments du cadre réglementaire applicable.

Ce document renseigne les conditions de lancement minimales de démarrage.

2 Echanges HADOPI - Opérateurs : identification des adresses IP

2.1 Caractéristiques générales de l'échange

L'échange est constitué :

- d'un flux de l'HADOPI vers les FAI portant le dossier de demandes d'identification
- d'un flux de réponse du FAI vers l'HADOPI

Les emails de l'Hadopi proviendront d'une adresse fournie par l'Hadopi ou par le prestataire hébergeant le SI de la Haute Autorité. L'adresse exacte sera communiquée ultérieurement. Les systèmes des FAI devront prévoir que cette adresse pourra être modifiée. Les demandes d'identification provenant de l'HADOPI et les réponses faites par les opérateurs se feront par cette adresse.

Les flux transitent comme pièces jointes dans des emails cryptés et signés.

Chaque dossier de demandes d'identification fera l'objet d'un acquittement de la part du FAI à réception de ce dossier dans son périmètre technique. Cet acquittement se présentera sous la forme d'un email, signé, envoyé en simple réponse au mail reçu, sans qu'il soit demandé d'ajouter de contenu dans le corps du message. L'objet de ce message d'acquittement devra être l'objet du message initial préfixé par « Re : ».

L'envoi de ce mail vaudra acquittement de réception du dossier de demandes.

L'objet du message d'origine sera « Demande_<Nom FAI>_<Num_Demande> » où <Nom_FAi> est le nom du FAI (ARCEP).

L'acquiescement de réception des réponses des FAI par l'HADOPI se présentera sous forme d'un email signé.

2.2 Caractéristiques du dossier de demandes d'identification

Le dossier de demandes d'identification est constitué :

- d'un fichier PDF portant les mentions administratives et réglementaires
- d'un fichier au format csv précisant :
 - un numéro unique du dossier de demandes (NUM_DEMANDE) sur 32 caractères alphanumériques
 - la date de la demande (format jj/mm/aaaa hh:mm:ss GMT)
 - le nombre de demandes d'identification présentes dans le fichier : pour permettre de détecter un emballement accidentel du système et d'en prévenir les conséquences, ce nombre sera borné à 50 000. Cette mesure vient en complément des mesures prises dans le système de l'Hadopi pour assurer l'intégrité du flux. Le nombre pourra être modifié ultérieurement si nécessaire.
 - l'horodatage GMT
 - la liste des adresses à identifier (détail ci-dessous).

Les demandes d'identification comportent les champs suivants :

Champ	Contenu	Format	Rempli à la demande
NUM_ORDRE	Numéro d'ordre dans la demande	[0 – 99 999]	Oui
IP	Adresse IP à identifier	IP v4 ou v6	Oui
HORODATAGE	Date et heure (GMT) pour laquelle l'identification est demandée. La précision est la seconde.	jj/mm/aaaa hh:mm:ss	Oui
CORRESPONDANCE	Précise si l'identification a pu être réalisée. Un champ vide signifie que l'identification n'a pas été traitée.	Une des valeurs suivantes : - oui - non - champ vide	Vide à la demande
MOTIF	Motif d'échec de l'identification [optionnel]	Une des valeurs suivantes : - ip inconnue - pas de connexion - multiple - plage d'IP non identifiable - format - erreur	Vide à la demande
TYPE	Type d'adresse IP [optionnel]	1 caractère	Vide à la demande
NOM	Nom de l'abonné	Maximum 32 caractères	Vide à la demande
PRENOM	Prénom de l'abonné	Maximum 32 caractères	Vide à la demande

PRENOM2	Prénom de l'abonné [optionnel au cas où cette information ne serait pas disponible]	Maximum 32 caractères	Vide à la demande
PRENOM3	Prénom de l'abonné [optionnel au cas où cette information ne serait pas disponible]	Maximum 32 caractères	Vide à la demande
RAISON	Raison sociale de l'entreprise	Maximum 32 caractères	Vide à la demande
ADRESSE1	Première ligne d'adresse	Maximum 38 caractères	Vide à la demande
ADRESSE2	Deuxième ligne d'adresse [optionnel au cas où cette information ne serait pas disponible]	Maximum 38 caractères	Vide à la demande
ADRESSE3	Troisième ligne d'adresse [optionnel au cas où cette information ne serait pas disponible]	Maximum 38 caractères	Vide à la demande
CP	Code postal	Maximum 32 caractères	Vide à la demande
VILLE	Ville	Maximum 32 caractères	Vide à la demande
PAYS	Pays [optionnel pour les abonnés résidant en France]	Maximum 38 caractères	Vide à la demande
TELEPHONE	Numéro de téléphone principal de l'abonné	10 caractères (format français en 0xxxxxxxx ou format international)	Vide à la demande
TELEPHONE2	Autre numéro de téléphone de l'abonné [optionnel au cas où cette information ne serait pas disponible]	10 caractères (format français en 0xxxxxxxx ou format international)	Vide à la demande
TELEPHONE3	Autre numéro de téléphone de l'abonné [optionnel au cas où cette information ne serait pas disponible]	10 caractères (format français en 0xxxxxxxx ou format international)	Vide à la demande
EMAIL	Email de facturation ou de contact de l'abonné	Adresse email	Vide à la demande
EMAIL2	Autre email de contact de l'abonné [optionnel au cas où cette information ne serait pas disponible]	Adresse email	Vide à la demande
EMAIL3	Autre email de contact de l'abonné [optionnel au cas où cette information ne serait pas disponible]	Adresse email	Vide à la demande

	disponible]		
INST_ADRESSE1	Première ligne d'adresse physique de l'installation [optionnel au cas où cette information ne serait pas disponible]	Maximum 38 caractères	Vide à la demande
INST_ADRESSE2	Deuxième ligne d'adresse physique de l'installation [optionnel au cas où cette information ne serait pas disponible]	Maximum 38 caractères	Vide à la demande
INST_ADRESSE3	Troisième ligne d'adresse physique de l'installation [optionnel au cas où cette information ne serait pas disponible]	Maximum 38 caractères	Vide à la demande
INST_CP	Code postal de l'adresse physique de l'installation [optionnel au cas où cette information ne serait pas disponible]	5 caractères numériques	Vide à la demande
INST_VILLE	Ville de l'adresse physique de l'installation [optionnel au cas où cette information ne serait pas disponible]	Maximum 32 caractères	Vide à la demande

Les règles de gestion suivantes s'appliquent à la demande :

- Les champs ne contenant que des espaces sont considérés comme vides.
- Les champs optionnels sont à laisser vides (sans espace).
- Le séparateur est ;
- Il n'y a pas de délimiteur de contenu du champ
- Les caractères du fichier sont au format UTF8

La convention de nommage suivante doit être respectée :

- Pour le fichier PDF : demande_<Nom_FAI>_<NUM_DEMANDE>.pdf
- Pour le fichier csv : demande_<Nom_FAI>_<NUM_DEMANDE>.csv

2.3 Caractéristiques de la réponse du FAI à la demande d'identification

L'échange est constitué :

- du fichier csv de la demande remplie (pièce jointe dans un email crypté et signé).

Les règles de gestion suivantes s'appliquent :

- Les champs ne contenant que des espaces sont considérés comme vides.
- Les champs optionnels peuvent être laissés vides (sans espace).
- Le séparateur est ;
- Il n'y a pas de délimiteur de contenu du champ.
- Les caractères du fichier sont au format UTF8
- Le champ CORRESPONDANCE est rempli par « oui » si l'identification a réussie : le FAI a trouvé un abonné connecté avec l'IP précisée dans le champ IP à la date et à l'heure précisés dans le champ HORODATAGE.
- Dans le cas où l'identification échoue, le champ CORRESPONDANCE est renseigné par « non ».
- Si l'identification n'a pas été traitée, le champ CORRESPONDANCE est laissé vide, ainsi que tous les autres champs qui n'étaient pas remplis dans la demande.
- Le champ MOTIF précisera, le cas échéant, la raison pour laquelle l'identification a échoué. Les valeurs possibles pour le champ motif sont :
 - « ip inconnue » si l'adresse IP fournie ne correspondait pas à une adresse de l'opérateur au moment des faits
 - « pas de connexion » si aucune connexion n'était active sur l'adresse demandée au moment des faits
 - « multiple » si l'identification remonte plusieurs abonnés au moment des faits (exemple d'IP multiple tel que les bornes WIFI publiques)
 - « plage d'IP non identifiable » dans le cas où le contrôle de la plage d'IP indique par exemple une IP de MVNO
 - « format » si les données de la demande sont erronées (mauvais format)
 - « erreur » dans les autres cas, et notamment s'il subsiste un doute sur l'identification (exemple du changement de l'IP au milieu de la seconde)
- Cette liste pourra faire l'objet de modification ou évolution en fonction des besoins.
- Le champ TYPE, optionnel, est « F » pour une IP fixe et « D » pour une IP dynamique.
- Dans le cas où l'identification réussit, un des champs NOM ou RAISON est obligatoire (doit être retourné non vide).
- Le champ TELEPHONE correspond au numéro de téléphone le plus pertinent (celui de la facturation ou à défaut de contact selon le FAI).
- Le champ EMAIL correspond à l'e-mail la plus pertinente (celle de facturation ou à défaut de contact selon le FAI).
- Les champs INST_ADRESSE1, INST_ADRESSE2, INST_ADRESSE3, INST_CP et INST_VILLE sont à utiliser pour l'adresse physique de l'installation, si elle est connue.
- L'adresse à retourner (champs ADRESSE1, ADRESSE2, ADRESSE3, CP, VILLE, PAYS) doit correspondre à l'adresse de facturation ou à défaut l'adresse postal de contact.
- Le champ PAYS est optionnel pour les abonnés résidant en France.
- Si le pays est France ou non renseigné, le champ CP doit être 5 caractères numériques
- Il est souhaitable que les adresses à retourner correspondent à la norme postale AFNOR XPZ 10-011 (hors règles de positionnement physiques qui ne sont pas applicables).
- La réponse ne doit en aucun cas ajouter, supprimer ou modifier l'ordre des lignes dans le fichier csv.
- Le fichier csv devra être retourné en une seule fois.

- En cas d'erreur (mauvais format d'une demande d'identification) dans une ligne du fichier csv, le champ MOTIF est à renseigner avec 'format'. Une ou plusieurs demandes d'identification contenant des erreurs de format ne doivent pas empêcher le traitement des autres demandes.

La convention de nommage suivante doit être respectée :

- Pour le fichier csv : `reponse_<Nom_FAI>_<NUM_DEMANDE>.csv`

2.4 Authentification et chiffrement des emails

Le standard S/MIME et les certificats au format X.509 seront utilisés pour gérer l'authentification et la confidentialité des messages.

Le chiffrement des contenus sera réalisé selon l'algorithme AES avec des clés de 128 bits. Les certificats seront générés aléatoirement par les outils de messagerie.

Conformément au format S/MIME, la clé de chiffrement du contenu sera transmise dans le message, chiffrée par un processus asymétrique par l'algorithme RSA.

2.5 Processus de gestion des clés asymétriques de chiffrement

Les certificats utilisés devront être issus d'une Autorité de Certification. L'Hadopi utilisera des certificats émis par Certinomis. Les dispositifs mis en place devront s'assurer de la validité des certificats. L'Hadopi se réserve la possibilité de changer ultérieurement de fournisseur de certificat.

Chaque FAI nommera un interlocuteur en charge de la gestion des certificats.

L'échange des clés publiques sera fait via un export au format PKCS#12, échangé par email. Le destinataire vérifiera l'authenticité et la validité du certificat auprès de l'autorité de certification. Il en acquittera la bonne réception, par email auprès de l'émetteur.

2.6 Fréquence des échanges

Chaque FAI recevra au plus un fichier par jour ouvré.

2.7 Description des modalités de mise en place

La mise en place de l'échange se fera dans les étapes suivantes :

- Phase 1 : définition conjointe des paramètres spécifiques d'échange notamment
 - Email de destination des demandes
 - Provenance des réponses
 - Définition du jeu de test pour l'échange (une demande et la réponse associée)
- Phase 2 : mise en place des certificats et de procédures d'escalade
- Phase 3 : tests d'interface, déroulement d'un échange factice sur la base du fichier de tests produit en phase 1
- Phase 4 : mise en production.

Le planning de la mise en place pour ces phases est le suivant :

- Phase 1 : 24 mai
- Phase 2 : 4 juin
- Phase 3 : 18 juin
- Phase 4 : 22 juin

3 Echanges HADOPI - Opérateurs : envoi des emails de recommandation aux abonnés

3.1 Mise en place d'un serveur SMTP par le FAI

Chaque FAI mettra en place un serveur SMTP permettant l'envoi des emails de recommandation à l'attention de ses abonnés. Il communiquera l'adresse (d'identification et d'authentification) du serveur à l'HADOPI ainsi que sa configuration.

Le système d'information de l'HADOPI se comportera comme un proxy SMTP en mode authentifié (TLS) permettant d'adresser l'ensemble des serveurs SMTP ainsi mis en place. Chaque email de recommandation sera émis, à l'attention de l'adresse email fournie lors de la phase d'identification, sur le serveur SMTP du FAI ayant réalisé cette identification.

Il est demandé que l'échange se fasse en mode sécurisé, via un mode TLS, et que l'authentification SMTP se fasse par certificat.

Il n'est pas demandé de confirmation de l'envoi des emails aux abonnés : les acquittements seront uniquement gérés au niveau technique par les mécanismes classiques du protocole SMTP.

Les envois se font au fil de l'eau, sans planification particulière, ce qui n'exclut pas des phénomènes de pic.

Lors d'un échec d'envoi lié à une erreur protocolaire reçu d'un serveur distant, les messages de retour sont à supprimer directement.

3.2 Sécurisation des échanges

Les sécurisations suivantes seront mises en place

- authentification des serveurs SMTP (mode TLS)
- mise en place de certificats SSL côté HADOPI et côté FAI, le cas échéant fournis par une Autorité de Certification
- le cas échéant, une vérification des adresses IP

3.3 Caractéristiques du message

Le message présente les caractéristiques suivantes

- les messages seront entièrement rédigés par l'HADOPI, au format texte et / ou HTML
- a priori les mails ne contiendront pas de liens, mais cela pourra changer

3.4 Gestion des effets de bord

Les mails de recommandations envoyés par les serveurs SMTP installés chez les FAI doivent pouvoir transiter sur les réseaux des FAI et être délivrés dans les BAL sous leur contrôle sans être bloqués (ou considérés comme du SPAM).

Les contrôles mis en place sur les réseaux des FAI ne devront pas perturber les envois des mails des agents de l'HADOPI (exemple : provenant des adresses mails en xxx@hadopi.fr, envoyés à partir de serveurs utilisés par l'HADOPI).

L'adresse exacte d'envoi (expéditeur) sera communiquée ultérieurement. Il peut s'agir d'un sous-domaine de hadopi.fr, ou d'un autre nom de domaine appartenant à l'Hadopi.

3.5 Éléments de volumétrie

Chaque FAI émettra hebdomadairement, en début de semaine, un fichier csv contenant la volumétrie de la période précédente avec les informations suivantes:

Champ	Contenu	Format
DATE	Date	jj/mm/aaaa
QUANTITE_RECUE	Nombre d'emails reçus de la part de l'HADOPI	Numérique
QUANTITE_ENVOYEE	Nombre d'email envoyés	Numérique

Ce fichier csv sera transmis par email, selon les mêmes modalités de sécurité que pour celui concernant les demandes d'identification.

Le nommage du fichier respectera la convention suivante : recommandations_<Nom FAI>_<Date>.csv où

- <Nom FAI> est le nom du FAI émettant le reporting
- <Date> est la date au format aaaammjjj : la date à indiquer est celle du dernier envoi inclus dans le reporting.

3.6 Description des modalités de mise en place

La mise en place se fera selon les étapes suivantes :

- Phase 1 : définition conjointe des paramètres spécifiques d'échange notamment
 - Identification des serveurs
 - Contenus et paramètres définitif des emails (adresse émetteur)
 - Données de tests
- Phase 2 : mise en place des certificats, échange des clés et de procédures d'escalade
- Phase 3 : tests d'interface, déroulement d'un envoi factice sur la base du fichier de tests produit en phase 1
- Phase 4 : mise en production.

Le planning de la mise en place pour ces phases est le suivant :

- Phase 1 : 24 mai

- Phase 2 : 4 juin
- Phase 3 : 18 juin
- Phase 4 : 22 juin

3.7 Engagement de service

Chaque FAI fera le maximum pour que les serveurs SMTP soient sécurisés et opérationnels en permanence, avec un engagement de disponibilité les jours ouvrés et une GTR à J+1 (ouvrés).

Chaque FAI communiquera à l'HADOPI le calendrier des opérations de maintenance et arrêts planifiés, en respectant un délai d'information de 2 semaines minimum et essaiera, dans la mesure du possible, de planifier les opérations en accord avec l'Hadopi.

En cas d'incident, le FAI devra avertir l'HADOPI dans un délai de max. 24h.