Fédération des fournisseurs d'accès à Internet associatifs
(dite « Fédération FDN »)
FFDN — 16, rue de Cachy — 80 090 Amiens
Déclarée en préfecture de la Somme — W751210904

Réponse à la consultation de l'ARCEP portant sur le projet de décision relative à la caractérisation de l'environnement utilisateur dans les mesures de qualité de service d'internet fixe via la mise en place d'une interface de programmation applicative (API) dans les box

Fédération FDN

28 mai 2019

1 Remarques générales

1.1 À propos de la Fédération FDN

La Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN, créée en 2011, regroupe des fournisseurs d'accès à Internet ayant la forme d'associations sans but lucratif, régies par le droit local correspondant (lois de 1901 et 1905 en France, lois similaires dans d'autres pays). Elle rassemble aujourd'hui 30 opérateurs : 29 en France (métropolitaine et outre-mer) et un en Belgique, dont certains comptent parmi les plus anciens fournisseurs d'accès à Internet encore en activité en France. Notre fédération est constituée autour de principes forts, et pas uniquement sur une communauté de structure juridique. Les fournisseurs d'accès que nous représentons sont tous animés par des utilisateurs bénévoles du réseau. La diversité des acteurs rassemblés nourrit une expérience de terrain riche, qui lui donne un point de vue particulier dans le cadre de cette consultation : nos associations sont placées juste à la jonction entre le monde des utilisateurs finals et celui des opérateurs : nous voyons l'endroit et l'envers du décor.

Nous allons commencer par quelques remarques générales sur le projet de décision soumis à consultation, puis nous déroulerons nos réponses aux questions posées par l'Autorité.

1.2 Garantir un usage proportionné et licite des données personnelles

Le projet de décision ainsi que les annexes qui l'accompagnent font transparaitre l'attention de l'Autorité à la question des données personnelles avec notamment cette attention très forte à la manière dont l'API est sécurisée. Il reste que, mécaniquement, un outil de métrique produit une surveillance du réseau. Caractériser l'environnement utilisateur est une manière de caractériser le mode de vie de l'utilisateur final.

Comme nous l'avions noté lors d'une rencontre avec le BEREC en 2017 :

> « En premier lieu, ceci ne peut pas signifier une surveillance permanente du réseau et sans objectif défini. Il en va de même pour la surveillance globale du réseau et, bien entendu, pour tout ce qui concerne un individu spécifique. Toute récolte systématique de données sur la qualité, le débit ou l'état opérationnel de l'accès Internet d'un utilisateur final doit être considérée comme attentatoire à la vie privée » [1]

Ainsi, l'API est capable d'informer le service de tests de la nature de l'abonnement souscrit : prenons l'offre Orange qui couple fixe et mobile. Son tarif s'élève à 78 puis 113 € par mois. Très clairement, cette seule information permet d'identifier le niveau de vie de l'utilisateur : il faut un certain niveau de revenus pour pouvoir assumer ce coût mensuel.

Autre exemple, la longueur de la ligne. C'est une information utile pour l'évaluation de l'atténuation du signal. Mais couplée à la zone géographique de l'abonné, on peut en déduire non pas son adresse exacte, mais au moins sa localisation de manière assez précise (vit-il à la campagne, en centre ville, dans quelle ville... ?).

Toutes ces données sont des données personnelles, puisqu'elles identifient les personnes de manière au minimum indirecte (par exemple : niveau de vie, localisation) [2]. Leur usage dans le cadre de l'évaluation de la qualité de service peut se comprendre, mais cela doit d'une part, se faire en conscience et, d'autre part, s'accompagner de garanties.

Nous aurions pour cette raison apprécié que le projet de décision fasse apparaître une trace d'une consultation de la CNIL sur ce point, ainsi que les conclusions de cette dernière.

Ces remarques ne veulent pas dire qu'il ne faille pas du tout caractériser l'environnement utilisateur. Il est aisé de comprendre en quoi ces informations sont utiles pour améliorer la fiabilité des tests et le diagnostic (ce qui occasionne la baisse de la qualité de service éventuelle). Nous cherchons ici à bien faire comprendre au régulateur l'enjeu : ce sont des données personnelles, donc l'utilisateur final *doit* garder le contrôle sur quelles données sont partagées, à qui, et pourquoi.

Utiliser des données personnelles implique que l'utilisateur final doit être informé

1. Réponse à l'occasion de la réunion avec le BEREC à propos de neutralité du Net à Bruxelles, avril 2017. `https://www.ffdn.org/fr/etude/2017-04-21/reponse-loccasion-de-la-reunion-avec-le-berec-propos-de-neutralite-du-net-bruxelles`

2. En ce sens cela peut rentrer dans le cadre de l'article 4 du RGPD : `https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4`.

et que des garanties sont posées. Evidemment, des garanties impliquent des sanctions éventuelles, sans quoi elles sont un accord de principe, peu rassurant pour l'utilisateur final.

1.2.1 L'API doit faire l'objet d'un consentement libre et éclairé

Il est indiqué que l'API sera activée par défaut dans la box de l'utilisateur final, mais le texte ne donne pas de précisions sur la manière dont celui-ci en est informé. Ni si l'utilisateur final peut intervenir sur ce paramètre dans la configuration de sa box.

Or, il est important que l'utilisateur final puisse consentir de manière éclairée à l'utilisation de ces données. De la même manière qu'il parait évident d'avoir le consentement de la personne chez qui on pose une sonde matérielle, il est évident que la personne chez qui on active cette API doit avoir donné son accord. Cela implique pour commencer que l'utilisateur soit mis au courant de l'existence de l'API.

Notons, en sus des droits que l'utilisateur a sur ces données, qu'il est entendu que la box peut être considérée comme un terminal [3] [4]. Terminal, donc, que l'utilisateur doit pouvoir choisir, et sur lequel il doit avoir du contrôle.

Dans ces conditions, il semble impensable de mettre en place un dispositif de caractérisation de l'environnement utilisateur sans, au minimum, une information claire de l'utilisateur. d'autant plus qu'il s'agit d'identifier la ligne, donc l'utilisateur final. Sans directive claire dans ce sens, il est peu probable que les opérateurs prennent l'initiative d'informer leurs clients de la présence de cette API. Exiger une information claire, dans un format compréhensible des utilisateurs finals, semble pour nous un minimum.

L'API doit pouvoir être désactivable si l'utilisateur refuse de participer aux tests. On peut imaginer qu'elle soit de plus désactivable sur la base d'une granularité plus fine : par exemple, pouvoir choisir de partager telle ou telle information, mais pas les autres, ou de pouvoir partager ces informations qu'avec tel outil de test, mais pas les autres. En tous les cas, l'activation par défaut de cette API doit s'accompagner d'une information claire sur l'usage des données utilisées.

L'utilisateur final doit pouvoir être assuré que ses données seront utilisées de manière proportionnée, et donc *uniquement* dans le cadre des tests de qualité de service qu'il effectue, par *uniquement* les acteurs impliqués dans le test.

Une API activée par défaut dans le terminal de l'utilisateur, sans information claire de ce dernier, nous semble être le pire scénario en terme de respect des droits des utilisateurs finals.

3. `http://blog.fdn.fr/?post/2016/05/18/Liberte-de-choix-du-terminal`
4. `https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018.pdf`

1.3 Indépendance des tests

La dernière question générale que soulève ce projet de décision, c'est le type d'acteurs qui pourront avoir accès à cette API et la garantie de l'usage respectueux des droits fondamentaux des utilisateurs finals qui en est fait.

Nous avons bien noté l'existence d'un code de conduite des acteurs de la mesure, qui conditionnerait l'accès à cette API. Mais il n'est pas clair que la liste des services autorisés soit connue.

On peut envisager que chaque opérateur, sur la base de ce code de conduite, autorise à certains acteurs de la mesure, l'accès à l'API qu'il a implémentée dans ses box. Si cette liste n'est pas publique, ce qui est probable, l'utilisateur final ne peut pas savoir à qui sont transmises ses données, et ne consent donc pas de manière éclairée. C'est le premier problème.

Le deuxième problème réside dans le fait qu'on ne peut pas vérifier que le code de conduite est bien respecté : il faudrait déjà pour cela savoir qui accède à quelles données. Cela permet de vérifier que parmi les acteurs listés, aucun d'entre eux n'a de conflit d'intêrêt (par exemple, un accord commercial avec tel opérateur), ce qui qui fausserait les tests. Cela permet également de pouvoir indiquer à l'ARCEP si un acteur semble contrevenir aux règles.

Troisième problème : la manière dont cette liste d'acteurs de la mesure ayant accès à l'API est constituée n'est pas claire : est-ce que les opérateurs ont chacun leur liste d'acteurs autorisés ? Est-ce que c'est l'ARCEP qui donne l'autorisation d'accéder à l'API ? Si c'est l'opérateur qui le fait, il pourrait se réserver le droit de refuser l'accès à l'API à certains outils de test. Il est peu probable que les opérateurs, qui ont un intérêt commercial très clair à ce que les tests faits par leurs clients soient au beau fixe (et ne prouvent pas, par exemple, qu'il y a défaut d'entretien de la ligne), soient des arbitres de choix.

En l'état, il n'est pas clair que des observatoires indépendants comme Ooni [5] ou RIPE Atlas [6] puissent y accéder. Il n'est pas certain que des opérateurs habitués à enfreindre la neutralité du net soient ravis de fournir des données de télémétrie à des observatoires soucieux de ces principes, alors même que ces éléments pourraient être utiles pour l'ARCEP. Il est en effet intéressant que l'utilisateur final puisse s'informer aussi auprès de sources qui ne soient pas des entreprises, pour pouvoir comparer les résultats comme souhaité par l'ARCEP.

La procédure d'accès et de révocation d'accès à l'API mérite donc d'être clarifiée. Il faudrait qu'à minima l'ARCEP tienne la liste des services autorisés à jour et à disposition des utilisateurs finals. Au mieux, qu'ils soient désignés par l'Autorité, plus à même de désigner des acteurs de mesure impartiaux (ou ayant déclaré leurs conflits d'intérêts).

5. `https://ooni.torproject.org/`

6. Le réseau des sondes Atlas, opéré par le RIPE NCC, est une référence dans le domaine de la mesure d'Internet via des sondes matérielles.

1.4 Pédagogie et capacitation de l'utilisateur final

Ce projet de décision implique une impulsion de l'utilisateur final qui lance les tests [7]. Or, si les dimensions techniques de l'API sont claires, l'interaction avec l'utilisateur final l'est moins. On comprend seulement que c'est lui, à priori, qui est à l'origine des tests, puisqu'ils sont lancés depuis un navigateur et que l'API n'est accessible qu'en local.

Si seul l'utilisateur est à l'origine des tests qui utilisent cette API, et si l'objectif est bien de mettre « à disposition d'informations fiables et comparables dans l'objectif d'améliorer la mesure de la qualité de service des réseaux fixes en France », il faut que l'utilisateur final soit à même de les comprendre.

Ainsi, il faut que la méthodologie de remontée des résultats soit expliquée, et que donc l'utilisateur comprenne qu'une partie des informations utilisées par le test viennent de sa box. Nous n'insistons pas sur le deuxième point, qu'on a largement développé précédemment.

La clarification de la méthodologie de tests a deux avantages. D'une part, elle permet de comprendre comment sont faits les tests et de les contre-vérifier au besoin, faisant ainsi baisser le risque de « triche ». Il nous semble pour cela important que les résultats bruts des tests soient accessibles à l'utilisateur : il faut qu'une contre-vérification de l'interprétation des tests soit possible.

D'autre part, elle permet à l'utilisateur de comprendre ces tests enrichis : par exemple, en quoi la longueur de ligne a un impact sur la qualité de service de son opérateur. Ce n'est pas une information si triviale que ça. Il faut l'expliquer. Plus l'utilisateur sera en mesure de comprendre, au moins dans les grandes lignes, les paramètres qui jouent dans la qualité de service de sa ligne, plus il sera en mesure d'une part de comprendre pourquoi ces informations, alors même qu'elles sont des données personnelles, sont remontées, et d'autre part ce qui doit constituer l'objet de sa plainte éventuelle au régulateur.

2 Réponses aux questions

2.1 Question 1 : Le périmètre opérateurs et box concernés par le projet de décision vous parait-il pertinent ?

Globalement, oui. On peut toutefois noter que le seuil d'un million de clients semble élevé et sorti au doigt mouillé. Il pourrait être pertinent de déterminer ce chiffre en se basant sur la volumétrie de clients déclarée par les opérateurs afin de toucher également ceux qui ont la capacité technique d'implémenter ces API sans pour autant atteindre le seul d'1 million.

La limitation aux box d'une série assez large semble pertinente, il faudrait toutefois veiller à ce que des modifications mineures dans les séries ne conduisent pas un opérateur

7. « Les paramètres principaux sont transmis par l'IAD (pour Integrated Access Device) à un outil de mesure de qualité de service à la suite d'une requête effectuée une seule fois lorsqu'un utilisateur réalise un test de mesure de la qualité de service internet. »

à déclarer « 9999 unités, joker, on n'est pas obligé, sisi, regardez, les suivantes ont une LED en plus sur la carte mère, c'est pas la même ! ».

A contrario, certains peuvent utiliser des box en très grande série sans pour autant avoir la main sur la constitution logicielle et les capacités hardware des box : est-ce pertinent d'imposer une obligation qui pourrait remettre en question le modèle économique de l'opérateur dans ce cas ?

Nous sommes également surpris de la limitation au marché grand public alors même que le sujet de la fibre à destination des professionels a pris une importance particulière pour l'ARCEP au cours des dernières années. Nous sommes conscients que ce marché peut comporter de nombreuses spécificités mais nous ne voyons pas de raison de l'exclure entièrement du champ de cette décision alors qu'il semble possible de l'inclure tout en protégeant les déploiements spécifiques grâce aux mêmes critères que ceux utilisés pour le marché grand public. Nous encourageons donc le régulateur à poursuivre dans la voie qu'il emprunte pour le grand public et à étendre le champ d'application de sa décision au marché professionnel dans les années à venir.

Nous sommes de même surpris par la limitation du périmètre à certaines technologies. Nous comprenons que certaines sont considérées comme des technologies du passé et ne bénéficiant pas de nouveaux développement mais nous estimons que la décision ne devrait pas exclure de technologie : tant que de nouvelles offres et matériels s'appuyant sur une technologie continuent d'être mis sur le marché, il semble pertinent de permettre aux abonnés de bénéficier de la meilleure fiabilité des tests voulue par le régulateur.

L'exclusion de technologie telles que le Wi-Fi et le satellite nous apparaît en particulier peu propice. Il est à noter en premier lieu que ces technologies continuent d'être déployées, développées, et de constituer un marché concurrentiel ; le domaine du satellite devrait même connaître un développement tout particulier dans un futur proche avec le déploiement de nouvelles constellations de satellites par de nombreux acteurs dans un futur proche, certains étant déjà entamés.

2.2 Question 2 : L'objectif retenu vous parait-il pertinent ?

L'objectif de permettre à chaque utilisateur final d'obtenir des informations plus fiables et comparables sur la qualité de son accès à Internet, nous apparaît très pertinent et bienvenu.

Il pourrait être pertinent d'ajouter, *de façon optionnelle*, un objectif pédagogique : les résultats retournés par l'API pourraient être habillés dans une explication fonctionnelle de la structure technique du FAI. L'ensemble pourrait être géré en natif sur la box ou sur le portail du FAI qui retournerait les résultats de l'API.

2.3 Question 3 : Les paramètres proposés dans l'Annexe 1 vous paraissent-ils pertinents pour la mise en place de l'API ? Quel(s) autre(s) paramètre(s) trouvez-vous utiles d'ajouter ou de supprimer ?

Saluons, pour commencer, le fait que l'Autorité ait choisi d'utiliser pour cette API des protocoles standards, rendant aisée l'implémentation de celle-ci dans des logiciels libres comme OpenWRT.

Certaines valeurs mentionnés peuvent, ceci dit, être améliorées. Nous les listons ci-après.

2.3.1 subscriptionSpeed/*Min

Certains opérateurs ne garantissent pas de débit minimal, il serait donc pertinent soit de rendre la chose optionnelle, soit d'autoriser les entiers positifs ou nuls.

2.3.2 Wan/Technology

Il manque à minima le WiFi, le WiMax, la 4G et 5G fixe ainsi que le satellite et ses différentes implémentations (géostationnaire, orbite basse par exemple). Il semble approprié de permettre de ne pas limiter les valeur autorisées. Nous nous interrogeons d'ailleurs sur le fait que cette API ne pourra probablement pas exister pour les terminaux mobiles qui ne se connectent jamais au travers d'une « box ».

2.3.3 Wan/Aggregtion

Le paramètre ainsi que son contenu semblent redondants avec Wan/Technology : les deux pourraient être fusionnés en utilisant un tableau de valeurs triées par ordre de préférence (voire un tableau associatif entre technologie et ordre d'utilisation). En tout état de cause, il n'est pas suffisant d'uniquement indiquer la présence d'une aggrégation sans donner son détail (aggrégation ou redondance, aggrégation type FTTH et 4G, aggrégation asymétrique type satellite et RTC, mix technologique fibre et wifi ou radio et xDSL afin de relier les lieux plus éloignés, ...).

Il nous semble pertinent d'ajouter plusieurs valeurs dans l'API. L'implémentation de celles que nous mentionnons ci-dessous ne devrait pas représenter une charge de travail supplémentaire notable car il s'agit généralement de simples extensions des valeurs déjà choisies ou bien de valeurs qui sont fixes pour tout le réseau de l'opérateur.

2.3.4 SubscriptionSpeed/FairUse/Active

Explication : indique si l'abonné est actuellement limité en débit à cause d'un dépassement de fair-use.

Motivation : les tests menés pendant une période de limitation active de débit de la part de l'opérateur ne peuvent être représentatifs et il est donc nécessaire de pouvoir les détecter.

2.3.5 SubscriptionSpeed/FairUse/Quota

Explication : volume du fair-use en bits (entier sur 64 bits, à 0 pour indiquer qu'il n'y a pas de quota).

Motivation : une telle information peut permettre d'adapter les volumes utilisés par les tests afin que le test lui-même ne consomme pas un volume de données plus important que nécessaire.

2.3.6 SubscriptionSpeed/FairUse/Used

Explication : volume du fair-use en bits (entier sur 64 bits, à 0 s'il n'y a pas de quota).

Motivation : voir SubscriptionSpeed/FairUse/Quota

2.3.7 SubscriptionSpeed/FairUse/SpeedDownload

Explication : limite de débit descendant en cas de dépassement de fair-use.

Motivation : en cas de limitation lors du dépassement de quota de fair-use, le débit auquel la réception est limitée.

2.3.8 SubscriptionSpeed/FairUse/SpeedUpload

Explication : limite de débit ascendant en cas de dépassement de fair-use.

Motivation : en cas de limitation lors du dépassement de quota de fair-use, le débit auquel l'émission est limitée.

2.3.9 SubscriptionSpeed/FairUse/ZeroRatedServices

Explication : liste des noms des services en zero-rating.

Motivation : nécessaire par cohérence afin que l'image donnée par les paramètres ci-dessus ne soit faussée lorsqu'un abonné constate un ralentissement sur certains services ou que le test de débit s'appuie sur certains services (par exemple, l'accès au site orange.fr ne se voit pas limité en débit lorsque l'abonné a dépassé son quota de fair-use).

2.3.10 Wan/SynchroTimeStamp

Explication : horodatage correspondant à l'heure à laquelle la dernière synchronisation a eu lieu.

Motivation : peut aider à détecter des problèmes de qualité de ligne.

2.3.11 Wan/SynchroHistory

Explication : tableau listant les données suivantes pour les 20 dernières synchronisation : horodatage de la synchronisation, horodatage de la désynchronisation correspondante (si disponible), débit descendant, débit ascendant.

Motivation : peut aussi aider à détecter des problèmes de qualité de ligne à une échelle plus longue que celle indiquée par la seule dernière synchronisation.

2.3.12 Wan/DownloadedBits

Explication : volume total reçu au cours des 168 dernières heures (une semaine).

Motivation : peut permettre au client, entre autres, d'estimer sa consommation de données et de comprendre qu'un ralentissement peut avoir eu comme source une consommation accrue (mise à jour d'OS, téléchargement important, émission importante de données, ...).

2.3.13 Wan/DownloadedPackets

Explication : nombre de paquets reçus au cours des 168 dernières heures (une semaine).

Motivation : voir Wan/DownloadedBits.

2.3.14 Wan/UploadedBits

Explication : volume total émis au cours des 168 dernières heures (une semaine).

Motivation : voir Wan/DownloadedBits.

2.3.15 Wan/UploadedPackets

Explication : nombre de paquets émis au cours des 168 dernières heures (une semaine).

Motivation : voir Wan/DownloadedBits.

2.3.16 Ports/FilteredIncoming

Explication : liste des ports filtrés en entrée du réseau.

Motivation : permet de comprendre pourquoi certaines applications peuvent ne pas fonctionner (SMTP, NetBIOS over TCP, lp, ...) ; devrait ne pas avoir de sens en Europe mais l'API proposée a la possibilité d'être mondiale.

2.3.17 Ports/FilteredOutgoing

Explication : liste des ports filtrés en sortie du réseau.

Motivation : voir Ports/FilteredIncoming.

2.3.18 Ports/ThrottledIncoming

Explication : liste des ports ralentis par le FAI en entrée du réseau.

Motivation : voir Ports/FilteredIncoming.

2.3.19 Ports/ThrottledOutgoing

Explication : liste des ports ralentis par le FAI en sortie du réseau.

Motivation : voir Ports/FilteredIncoming.

2.3.20 DataAlteration/Layer3

Explication : liste de types d'équipements modifiant des données du niveau 3 du modèle OSI.

Motivation : sur certains réseaux, certains opérateurs utilisent des équipements qui modifient les paquets ; bien que cela correspondent souvent à une volonté d'amélioration du service fourni au client, ces équipements sont conçus pour mentir aux extrêmités des connexions dont ils font transiter les données et empêchent donc une analyse correcte de certains tests (par exemple, Orange, en 4G, utilise des équipements qui terminent les connexions TCP des clients dans l'infrastructure d'Orange, comme démontré en annexe).

2.3.21 DataAlteration/Layer4

Explication : liste de types d'équipements modifiant des données du niveau 4 du modèle OSI.

Motivation : voir DataAlteration/Layer3.

2.3.22 DataAlteration/Layer5

Explication : liste de types d'équipements modifiant des données du niveau 5 du modèle OSI.

Motivation : voir DataAlteration/Layer3.

2.3.23 DataAlteration/Layer6

Explication : liste de types d'équipements modifiant des données du niveau 6 du modèle OSI.

Motivation : voir DataAlteration/Layer3.

2.3.24 DataAlteration/Layer7

Explication : liste de types d'équipements modifiant des données du niveau 7 du modèle OSI.

Motivation : voir DataAlteration/Layer3.

2.3.25 IP/v6

Explication : si une adresse IPv6 est assignée (et utilisable).

Motivation : L'ARCEP a montré ne pas avoir besoin d'explications supplémentaires vis-à-vis de cette valeur, nous n'en donnerons donc pas.

2.3.26 IP/v6Public

Explication : si une adresse IPv6 publique est assignée (et utilisable).

Motivation : Paramètre nécessaire à la compréhension du fonctionnement ou non de l'hébergement de services.

2.3.27 IP/v6Static

Explication : si une adresse IPv6 est fournie, si elle est fixe.

Motivation : Paramètre nécessaire à la compréhension du fonctionnement ou non de l'hébergement de services.

2.3.28 IP/v4

Explication : si une adresse IPv4 est assignée (et utilisable).

Motivation : par cohérence avec la fourniture de valeurs similaires pour l'IPv6.

2.3.29 IP/v4Public

Explication : si une adresse IPv4 publique est assignée (et utilisable).

2.3.30 IP/v4Static

Explication : si une adresse IPv4 est fournie, si elle est fixe.

2.3.31 IP/ProtocolsFiltered

Explication : liste des numéros de protocoles IP filtrés.

Motivation : De nombreux protocoles transitant par IP et autres que TCP et UDP sont filtrés par les FAI ; liste de ceux-ci (une liste blanche pourrait être plus aisée à dresser qu'une liste noire).

2.3.32 DNS/ISPProvided

Explication : est-ce que le résolveur utilisé par l'IAD est celui du fournisseur d'accès.

Motivation : une configuration DNS inconnue peut empêcher de reproduire les résultats des tests d'un utilisateur ; cette valeur ne couvre pas la configuration de l'ordinateur de l'utilisateur, ni celle de son navigateur mais couvre tout de même une partie importante des configurations.

2.3.33 DNS/DNSSEC

Explication : est-ce que le résolveur utilisé par l'IAD supporte DNSSEC.

Motivation : La qualité des résolveurs DNS est souvent débattue ; l'ARCEP même mentionne DNSSEC dans cette consultation. Il est nécessaire d'indiquer si DNSSEC est supporté par l'IAD et le FAI.

2.3.34 DNS/A

Explication : est-ce que le résolveur utilisé par l'IAD est capable de retourner des résultats en IPv4.

2.3.35 DNS/AAAA

Explication : est-ce que le résolveur utilisé par l'IAD est capable de retourner des résultats en IPv6.

Motivation : voir le paramètre IP/v6.

Il semble difficile d'harmoniser un format de données pour l'ensemble des autres données qui pourraient apparaitre dans la réponse de l'API. Si la spécification n'a pas vocation a évoluer régulièrement, un sous arbre json à structure libre serait à envisager.

2.4 Question 4 :L'implémentation de l'API et les restrictions d'accès retenues par l'Arcep (détaillées à l'annexe 2) vous paraissent-elles les plus appropriées ? Sinon, quelles modifications proposez-vous ?

Il convient de mentionner en tout premier lieu l'absence de modèle de menace dans la consultation. Il est particulièrement difficile d'estimer la sécurité d'une spécification ou d'une implémentation en-dehors du contexte d'un modèle de menace [8]. Nous nous attendons ainsi à ce que les différents opérateurs répondent de manière très variée, chacun utilisant un modèle de menace différent. Il est d'autant difficile de justifier ses raisonnements et choix sans un tel cadre (puisque l'Autorité doit faire une synthèse). Il apparaît donc important que l'ARCEP précise le modèle de menace choisi lorsque cela est possible ou à défaut enjoigne les participants aux futures consultations et ateliers ou groupes de travail à préciser le modèle de menace dans lequel ils choisissent de se placer. Sans cela, les choix faits en matière de sécurité sont difficiles à évaluer.

Ceci dit, l'ARCEP note à juste titre qu'il est primordial de restreindre l'accès à l'API et que celui-ci soit sécurisé lorsqu'il a lieu. Nous estimons cependant que les opérateurs ne sont pas le groupe approprié vers lequel se tourner lorsqu'il s'agit d'évaluer la sécurité d'une API ou la possibilité d'en sécuriser une. La communauté de la sécurité en informatique est suffisamment développée pour être en mesure de répondre à de telles questions. L'intérêt de l'API proposée par l'ARCEP est mondial et son implémentation peut donc intéresser de nombreux groupes y compris hors de France. Il conviendrait de lancer une consultation dédiée à ce sujet et de demander aux opérateurs de contribuer à sa diffusion. Il est d'ailleurs possible que la meilleure approche n'utilise pas TLS et sa PKI pour la sécurisation des données mais d'autres mécanismes.

Nous attirons cependant simplement l'attention de l'ARCEP sur l'utilisation de DNS over HTTPS par les navigateurs car celle-ci rendra plus difficile à terme certains scénarios qui pourraient avoir été envisagés.

De plus, il semble nécessaire d'établir dès à présent les procédures à suivre lorsque des problèmes seront trouvés dans les implémentations de cette API ou dans la conception

8. Autrement dit : suivant ce de quoi on veut se protéger, on ne choisit pas les mêmes outils. Certains outils de chiffrement, par exemple, ne sont pas utiles dans le cadre de certains de modèle de menace. Comme il n'y a pas de sécurité absolue, ce de quoi on se protège est primordial.

même de celle-ci. Il importe aussi de noter qu'une implémentation problématique peut être le signe d'un problème de conception : il est possible qu'une fonctionnalité ne puisse être implémentée de manière sûre. Pour ces raisons nous estimons qu'il est nécessaire que des statistiques sur l'utilisation de l'API soient remontées régulièrement par les opérateurs à l'ARCEP (par exemple : nombre d'appels à cette API pour chaque jour et proportion d'erreurs, liste des sites utilisateurs et volume d'appel), que les FAI disposent d'une adresse de contact pour les problèmes de sécurité liés à cette API et qu'elle soit clairement indiquée pour ceux qui s'intéresseront à cette API, qu'un contact à l'ARCEP soit de même indiqué afin de rapidement estimer le volume des problèmes de sécurité à travers tous les FAI, que les FAI informent l'ARCEP sans délai des problèmes qui leur sont remontés ainsi que de leur progression dans la correction de ceux-ci (de l'analyse au déploiement des correctifs, en passant par le développement).

2.5 Question 5 : Le calendrier retenu vous parait-il réaliste et adapté aux contraintes de développement ? Pour quelles raisons ? Sinon, quelles modifications proposez-vous ?

Le calendrier semble réaliste au vu de la charge de développement et des cycles matériels.

Nous ne pensons pas que les modifications que nous proposons ajoutent une charge de travail notable qui permettrait de justifier d'un décalage du calendrier. En effet, ces informations sont soit des extensions simples des valeurs déjà listées (historique de synchronisation, volume de données récemment échangées), soit constantes pour chaque opérateur (ports filtrés, équipements d'altérations des données, informations sur le résolveur DNS), voire devraient être constantes et vides (équipements d'altération des données, ports, services ou protocoles ralentis, ...).

De même, nous insistons sur le fait que la prise en compte de nos commentaires sur la sécurité ne devraient pas ralentir sensiblement le développement de ces API par les opérateurs. En effet une part importante du travail consistera en la récolte et la centralisation d'informations. Dans l'éventualité où il serait impossible de rendre, de manière sécurisée, une telle API automatiquement accessible par les sites de tests de connexion, celle-ci n'en serait pas moins intéressante pour l'utilisateur final qui y accéderait alors directement pour lui-même ou pourrait copier-coller manuellement les informations remontées sur le site de test de connexion.

Annexe : terminaison de connexion TCP par l'infrastructure de l'opérateur sur Orange 4G

Interception des connexions TCP sur le port 80 et serveur distant fonctionnel

Test avec mtr sur le domaine arcep.fr sur une connexion Orange 4G.

```
# mtr -r -c 4 -n arcep.fr
Start: 2019-05-27T18:12:20+0200
HOST: quasar.intranet             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 192.168.43.1               0.0%     4    2.9   3.5   2.7   4.8   0.9
  2.|-- 10.164.67.64               0.0%     4   31.8  40.9  31.6  65.0  16.1
  3.|-- 10.164.66.49               0.0%     4   36.8  30.4  21.8  36.8   6.7
  4.|-- 10.164.66.54               0.0%     4   26.6  34.4  26.6  55.8  14.3
  5.|-- 10.164.66.62               0.0%     4   33.2  46.5  33.1  84.6  25.4
  6.|-- 10.164.66.65               0.0%     4   37.7  33.7  30.1  37.7   3.5
  7.|-- 193.252.137.33             0.0%     4   36.0  33.5  28.1  36.0   3.7
  8.|-- 193.249.215.214            0.0%     4   32.8  34.8  30.8  39.4   3.8
  9.|-- 81.253.130.1               0.0%     4   37.4  37.5  28.7  51.3   9.9
 10.|-- 193.252.160.46             0.0%     4   35.2  31.4  28.0  35.2   3.4
 11.|-- 193.252.137.14             0.0%     4   39.7  41.2  39.7  42.4   1.3
 12.|-- 193.251.132.38             0.0%     4   36.4  39.7  36.4  41.7   2.3
 13.|-- 193.251.128.125            0.0%     4   42.9  41.1  39.8  42.9   1.3
 14.|-- 81.52.179.22               0.0%     4   31.1  40.1  31.1  51.8   9.5
 15.|-- 94.199.152.10              0.0%     4   35.7  42.7  35.7  48.4   6.5
 16.|-- 94.199.152.2               0.0%     4   43.3  38.9  35.5  43.3   3.4
 17.|-- ???                      100.0     4    0.0   0.0   0.0   0.0   0.0
```

Test de début de connexion TCP (envoi d'un paquet TCP SYN) avec le domaine arcep.fr et le port 22 (ssh) sur une connexion Orange 4G.

```
# mtr -r -c 4 -n --tcp --port 22 arcep.fr
Start: 2019-05-27T18:12:46+0200
HOST: quasar.intranet             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 192.168.43.1               0.0%     4    3.0   3.0   2.2   3.5   0.6
  2.|-- 10.164.67.64               0.0%     4   34.2 112.9  29.2 332.5 146.8
  3.|-- 10.164.66.62               0.0%     4   28.4  81.3  26.6 232.3 100.8
  4.|-- 10.164.66.65               0.0%     4   23.1  50.5  21.0 132.1  54.4
  5.|-- 193.252.137.33             0.0%     4   31.1  30.0  25.5  32.0   3.0
  6.|-- 193.249.215.214            0.0%     4   31.6  28.9  21.7  35.4   5.9
  7.|-- 81.253.130.1               0.0%     4   35.4  30.3  19.9  35.4   7.0
  8.|-- 193.252.160.46             0.0%     4   41.9  32.4  24.1  41.9   7.7
  9.|-- 193.252.137.14             0.0%     4   42.7  41.1  34.6  47.7   5.5
 10.|-- 193.251.132.42             0.0%     4   37.0  40.3  37.0  44.2   3.1
```

```
 11.|-- 193.251.128.127            0.0%     4   41.1  35.3  27.6  41.1   6.0
 12.|-- 81.52.179.22               0.0%     4   33.8  38.8  33.8  43.9   4.3
 13.|-- 94.199.152.10              0.0%     4   37.8  39.2  37.8  41.8   1.9
 14.|-- 94.199.152.2               0.0%     4   39.7  38.2  35.7  40.0   2.0
 15.|-- ???                       100.0     4    0.0   0.0   0.0   0.0   0.0
```

Test similaire au test précédent mais avec le port 80 (http) sur une connexion Orange 4G.

```
# mtr -r -c 4 -n --tcp --port 80 arcep.fr
Start: 2019-05-27T18:13:00+0200
HOST: quasar.intranet             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 192.168.43.1               0.0%     4    4.3   3.8   2.7   4.8   0.9
  2.|-- 10.164.67.64               0.0%     4   67.7  62.7  27.5  91.8  26.5
  3.|-- 217.115.162.46             0.0%     4   53.7  44.8  32.4  54.5  11.1
```

Nous devons insister sur le fait que ce dernier rapport de mtr n'est pas tronqué : seuls trois nœuds sont indiqués car une machine dans l'infrastructure d'Orange a intercepté les ouvertures de connexions TCP réalisées par mtr tout en prétendant être la machine derrière le domaine arcep.fr (217.115.162.46).

Interception des connexions TCP sur le port 80 et serveur distant non fonctionnel

Test avec mtr et l'adresse 1.2.3.4 sur une connexion Orange 4G.

```
# mtr -r -c 4 -n --tcp --port 80 1.2.3.4
Start: 2019-05-27T18:15:43+0200
HOST: quasar.intranet             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 192.168.43.1               0.0%     4   69.4  63.0  29.3 100.3  29.8
  2.|-- 10.164.67.64               0.0%     4   93.7  77.8  63.9  93.7  13.2
  3.|-- 1.2.3.4                    0.0%     4   40.0  62.7  31.6  91.7  31.3
```

Durant ce test, l'hôte 1.2.3.4 semble répondre sur le port 80 en TCP.

Test avec mtr et l'adresse 1.2.3.4 sur une connexion du fournisseur associatif Franciliens.net.

```
# mtr -r -c 4 -n --tcp --port 80 1.2.3.4
Start: Mon May 27 18:16:10 2019
HOST: melchi                      Loss%   Snt   Last   Avg  Best  Wrst StDev
```

```
1.|-- 79.143.250.65            0.0%     4   17.7  21.2  16.8  32.4   7.4
2.|-- 79.143.250.12            0.0%     4   25.1  34.0  24.7  60.9  17.9
3.|-- 79.143.241.25            0.0%     4   79.0  38.7  24.9  79.0  26.9
4.|-- ???                     100.0     4    0.0   0.0   0.0   0.0   0.0
```

L'hôte 1.2.3.4 ne répond pas sur le port 80 en TCP. La machine réalisant l'interception de connexion TCP ne pouvant déterminer à l'avance si la machine que le client souhaite réellement joindre répondra au paquet TCP SYN envoyé, elle répond au client de manière optimiste et fait apparaître la machine distante comme joignable alors même qu'elle ne l'est pas (généralement, la « solution » consiste à envoyer un paquet TCP RST au client dès que l'état réel du serveur est découvert).