Appel à candidatures pour les projets de plateforme anti-fraude appels téléphoniques frauduleux sur les réseaux fixes et mobiles et messages de signalisation frauduleux sur les réseaux mobiles

dans le cadre du

Plan national pour la reprise et la résilience
Axe 2 Transformation numérique

Composante 2.1. Cybersécurité

Personne de Contact : **Streel Yves** Chef de projet

(yves.streel@ccb.belgium.be)

TABLE DES MATIÈRES

Table des matières

1. Contexte

La fraude et les abus ont toujours été un problème dans l'industrie des télécommunications et la Belgique, comme tous les autres pays, est de plus en plus confrontée à la fraude et aux abus concernant les numéros E.164. Avec le développement de la technologie, notamment sur Internet, les utilisateurs finaux ont un accès et un contrôle beaucoup plus grands sur les réseaux de communication. Il s'agit d'une évolution positive pour la grande majorité des utilisateurs finaux en termes de choix et d'accès aux applications et aux services, mais l'effet négatif est que la fraude et les abus sont beaucoup plus faciles à réaliser. La fraude et les abus sont aujourd'hui un problème mondial dont la juridiction devient de plus en plus difficile.

Par exemple, les fraudeurs exploitent délibérément la confiance inhérente des utilisateurs finaux dans l'identification de l'appelant (CLI = Calling Line Identity) (par exemple en usurpant des numéros valides comme CLI) pour commettre des fraudes pendant les appels téléphoniques (par exemple pour soutirer des informations bancaires, des informations sur les cartes de crédit ou d'autres types d'informations personnelles). Dans de nombreux cas, les techniques sont automatisées et proviennent de pays en développement et/ou de juridictions instables où les fraudeurs savent qu'ils sont relativement à l'abri de la détection et des poursuites.

De même, les utilisateurs finaux sont de plus en plus confrontés à des appels parasites tels que les robocalls, les appels silencieux particulièrement gênants, entre autres.

L'International Revenue Share Fraud (IRSF), une forme de fraude dans laquelle l'auteur gonfle artificiellement le trafic téléphonique en générant des appels vers certaines parties des séries de numéros nationaux dans différents pays, est la principale forme de fraude aux télécommunications dans le monde, selon le rapport "Fraud Loss Survey" [1] de 2021 par la Communications Fraud Control Association (CFCA), l'IRSF est la principale forme de fraude aux télécommunications dans le monde. Pertes mondiales causées par l'IRSF - estimées à 6,7 milliards de dollars en 2021.

On trouvera une description plus détaillée des différentes techniques de fraude dans le rapport ECC 275 "The role of E.164 numbers in international fraud and or misuse of electronic communications services" [2] .

De même, un certain nombre de faiblesses ont été détectées dans le protocole de signalisation n° 7/Diameter/5G. Si des mesures de protection adéquates ne sont pas prises, des risques sérieux apparaissent, notamment un impact négatif possible sur la vie privée (comme la localisation de l'utilisateur final dans le contexte de l'espionnage). Cette situation est décrite dans un rapport [3] par l'Agence européenne de sécurité ENSIA "Signaling Security in Telecom - SS7/Diameter/5G - EU level assessment of the current situation - March 2018".

La concertation permanente entre l'IBPT, les opérateurs et FEBELFIN, entre autres, montre que le nombre de tentatives et de techniques de fraude est également en forte augmentation en Belgique. La fraude dans le domaine des télécommunications est donc un problème auquel il faut s'attaquer en priorité. La détection et la sanction étant particulièrement difficiles (les criminels peuvent facilement opérer de manière anonyme dans des juridictions instables), il est conseillé de se concentrer sur les moyens techniques qui permettent à la fois de prévenir la fraude de manière préventive et de réagir rapidement pour éviter des dommages plus importants. Le projet Stop Phishing doit être considéré dans ce contexte.

2. Objet et nature de l'accord de partenariat

Le projet Stop Phishing vise à détecter et à bloquer les tentatives de phishing et de fraude via les réseaux de télécommunications grâce à la mise en place de plateformes anti-phishing et anti-fraude

[1] https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf

[2] https://docdb.cept.org/document/3114

[3] https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

chez les opérateurs belges , en étroite collaboration avec le Centre pour la Cybersécurité Belgique et le régulateur belge des télécommunications (IBPT).

Le projet Stop Phishing se compose de quatre parties différentes. La mise en œuvre des deux premières parties, c'est-à-dire l'anti-phishing pour les SMS (smishing) et le courrier électronique est actuellement en cours. Les troisième et quatrième parties, qui sont combinées dans ces spécifications, visent à déployer des plateformes anti-hameçonnage avancées pour protéger les utilisateurs finaux belges de services vocaux.

Ce projet contribue donc de manière significative à la transition numérique en augmentant la confiance dans l'économie numérique. Cette confiance accélère la transition numérique : les citoyens utilisent les services publics numériques et le commerce électronique en toute sérénité ; les PME développent leur transition numérique et sont mieux protégées contre les fraudes et les abus de ; les services publics et les administrations fournissent des services en ligne plus sécurisés ....

Sous la supervision du Comité de pilotage (voir chapitre 9), le Centre pour la Cybersécurité Belgique et l'IBPT coordonnent les actions avec les candidats télécoms. Le CCB est chargé de la gestion administrative et du suivi de ce projet pour le compte de la Ministre des télécommunications.

Public cible :

Les bénéficiaires directs de ce projet sont les opérateurs de télécommunications offrant des services de communication vocale électronique publique aux utilisateurs finaux belges en utilisant des numéros de téléphone E.164 belges.

Période de mise en œuvre du projet

Le projet débutera au plus tard en avril 2023 avec l'appel à candidatures et devrait s'achever fin 2024.

3. Critères d'éligibilité

Qui peut participer à ce projet ?

Tout candidat qui souhaite participer à ce projet doit remplir toutes les conditions ci-dessous :

1. fournir des services de communication vocale publique aux utilisateurs finaux belges sur la base de numéros de téléphone E.164 belges ;
2. sont notifiées à l'IBPT conformément à l'art. 9 de la LCE (loi du 13 juin 2005 relative aux communications électroniques) ;
3. disposer d'une infrastructure de réseau et/ou de commutation sur le territoire belge ;
4. Fournir une description des plateformes existantes à la date du 1er mars 2023 (équipements et interconnexion) et des outils anti-fraude statiques/réactifs et dynamiques/proactifs existants pour détecter et arrêter la fraude sur les services publics de communications électroniques pour la téléphonie vocale ;
5. Ouvert à investir dans une nouvelle plateforme anti-fraude ou dans son extension en ajoutant de nouvelles fonctionnalités à leur plateforme actuelle pour améliorer son fonctionnement et/ou traiter d'autres phénomènes de fraude ou son extension dans le temps. Pour y parvenir, le candidat peut, entre autres, procéder à des développements internes, acheter des services anti-fraude auprès de parties externes ou opter pour d'autres solutions ;
6. Le candidat doit démontrer qu'il respecte l'ensemble de la législation applicable, y compris sur la vie privée et la LCE (voir annexe 1).

4. Phénomènes de fraude pour lesquels des projets peuvent être soumis

Pour les phénomènes de fraude énumérés ci-dessous, les candidats répondant aux critères d'éligibilité ci-dessus peuvent obtenir des subventions pour investir et opérer dans les conditions définies dans le présent cahier des charges dans des plateformes anti-fraude. Notez que la plupart des plateformes anti-fraude peuvent traiter plusieurs phénomènes de fraude en même temps.

1. CLI spoofing de numéros géographiques (utilisateur final victime)
2. CLI spoofing de numéros de téléphone mobile (utilisateur final victime)
3. Refiling/re-origination du trafic (CLI spoofing au détriment de l'opérateur)
4. Wangiri (ou ping calls)
5. PBX/comptes hacking (piratage de compte)
6. Collecteurs de trafic et fraude à l'itinérance
7. Call hijacking (arrêt court)
8. Robocalls et appels frauduleux
9. Intrusion par le nr. 7 / Diameter / 5G
10. Autres phénomènes de fraude (doivent être documentés de manière adéquate)

Une description plus détaillée des phénomènes de fraude 1 à 7 figure au chapitre 3 du rapport 275 du ECC (voir note de bas de page 2). Une description des phénomènes d'intrusion à travers le No 7 peut être trouvée dans le rapport de l'ENISA mentionné ci-dessus (voir note de bas de page 3).

Par ailleurs, les candidats répondant aux critères d'éligibilité ci-dessus peuvent obtenir des subventions dans les conditions prévues par le présent cahier des charges pour développer et exploiter conjointement des plates-formes ou des systèmes de partage d'informations utiles à la lutte contre la fraude. Cette coopération ne peut pas avoir d'effets anticoncurrentiels.

Si le candidat le souhaite, il peut diviser son dossier en plusieurs sous-dossiers qui seront alors évalués séparément selon les critères d'évaluation énumérés au chapitre 5.

5. Critères d'évaluation

Les critères d'évaluation suivants seront utilisés :

1. L'efficacité de la solution proposée (60 points)

Le candidat doit démontrer que la solution proposée répond à la méthode la plus avancée pour combattre le phénomène de la fraude. Par exemple, la plateforme proposée devrait détecter et bloquer de manière significative les fraudes en temps réel, automatiquement et grâce à des techniques d'apprentissage automatique. Pour vérifier l'efficacité, les solutions des différents candidats seront également comparées les unes aux autres en termes de fonctionnalités et de prix. Le développement de plateformes communes aura également un impact favorable sur le score.

2. Coût (20 points)

Le candidat doit démontrer qu'il a choisi la solution disponible la plus efficace en termes de prix et qui permet de lutter suffisamment contre le phénomène de la fraude. A cette fin, le candidat doit fournir une ventilation aussi détaillée que possible des coûts selon les modalités énumérées au chapitre 6.

3. Rapports et statistiques (10 points)

Le candidat doit faire une proposition suffisamment pertinente et détaillée selon les modalités énumérées au chapitre 8 sur le reporting et les statistiques afin de mesurer et de suivre les performances de la solution.

4. Plan du projet (10 points)

Le candidat doit présenter un plan de projet détaillé selon les modalités énumérées au chapitre 7 pour rendre le système anti-fraude pleinement opérationnel.

Le candidat doit obtenir un minimum de 60 points sur 100 pour être sélectionné et invité à conclure un protocole d'accord (voir chapitre 12).

6. Aspects financiers

Les candidats doivent démontrer qu'ils prendront en charge au moins 50% du coût d'achat et d'utilisation de la nouvelle plateforme anti-fraude (voir chapitre 3 point 4) qui sera introduite au cours des trois premières années.

A cette fin, le demandeur doit fournir toutes les informations relatives aux coûts du prestataire de services et à ses propres coûts (par exemple, gestion interne du projet, coût opérationnel, coût réglementaire,...) pour la plateforme anti-fraude.

Dans le dossier de candidature, chaque candidat doit mentionner tous les coûts ventilés et démontrés en détail : pour la mise en place et le fonctionnement de la plateforme pendant trois ans, ventilés sur les différentes années pour chaque type de dépenses (logiciel, matériel, personnel, maintenance et autres).

7. Planification du projet

Le candidat devra mettre en œuvre une ou plusieurs plates-formes anti-fraude à la pointe de la technologie (« state of the art ») dans son réseau en suivant une approche par projet, notamment :

1. en évaluant le « state of the art » et les techniques les plus avancées pour lutter contre les phénomènes de fraude énumérés au chapitre 4 ;
2. en évaluant le marché et en sélectionnant le fournisseur ;
3. en mettant en œuvre la solution choisie ;
4. en utilisant cette plateforme et en évaluant les résultats.

Les candidats doivent partager un plan de mise en œuvre détaillé couvrant toutes les phases du projet, de la définition à la mise en œuvre ainsi que son fonctionnement complet.

Les plateformes anti-fraude financées doivent être disponibles et opérationnelles au plus tard le 31 décembre 2024.

8. Objectifs - résultats attendus (information et rapports statistiques)

Le projet vise à réduire considérablement le nombre de communications vocales frauduleuses [4] reçues par les utilisateurs. En outre, les systèmes de signalisation n° 7 / Diameter / 5G devraient être mieux protégés contre les intrusions et les abus.

Le candidat devra proposer dans sa réponse un moyen de mesurer les éléments suivants :

1. décomposer l'évolution dans le temps du nombre de fraudes par les différents phénomènes de fraude ;
2. le nombre de communications qui ont été bloquées dans une période donnée par rapport au nombre total dans la même période (en tenant compte du trafic exclu) ;
3. le nombre de communications pour lesquelles des actions (énumérer et décrire lesquelles) autres que le blocage et aucune action ont été prises ;
4. le candidat doit fournir des chiffres pour mesurer l'efficacité de la plate-forme ;
5. tout autre chiffre pertinent que la plate-forme peut présenter régulièrement (par exemple, tous les trimestres) pour démontrer que la plate-forme fonctionne.

De plus, le candidat retenu devra collaborer avec les autres candidats pour harmoniser au mieux ces données. Le chef de projet coordonnera cette activité.

9. Comité de pilotage

Le comité de pilotage est composé de :

La Ministre des télécommunications, représentée par M. Gertjan Boulet ;
L'IBPT, représenté par M. Jan Vannieuwenhuyse ;

[4] Pour la définition de la fraude : voir l'annexe 1.

le CCB, représenté par M. Miguel de Bruycker et Mme Phédra Clouner et le chef de projet Yves Streel.

Le comité de pilotage se réunira pour valider et évaluer les différentes phases du projet, en tenant compte des jalons qui seront fixés en concertation avec les personnes sélectionnées.

10. Propriétés des résultats

Chaque candidat sélectionné doit partager les résultats obtenus grâce à la mise en place de cette nouvelle plateforme dans toutes les phases du projet, ainsi qu'un rapport semestriel à partir du lancement officiel pour évaluer le retour sur investissement dans les mois et années à venir.

Les détails et modalités exacts de la distribution (type d'information, granularité et unité) seront déterminés par le Comité de pilotage et les candidats au cours du projet, après sélection de la solution choisie par le candidat.

11. Dossier de candidature et engagements

Le candidat doit présenter un dossier de candidature ou plusieurs sous-dossiers qui seront alors évalués séparément selon les critères d'évaluation énumérés au chapitre 5.

Le candidat doit démontrer dans ce dossier de candidature qu'il répond à tous les critères d'éligibilité décrits dans la section 3. Si l'un des critères d'éligibilité énumérés n'est pas rempli, la demande d'octroi de la subvention ne sera pas retenue.

Le candidat doit décrire en détail comment il répondra aux critères d'évaluation énumérés au chapitre 5.

Le candidat doit fournir des éléments supplémentaires qu'il juge importants pour atteindre l'objectif du projet et qui démontrent l'expertise du candidat et, le cas échéant, du fournisseur prévu (par exemple, des prestations à l'étranger).

Il est également demandé au candidat d'identifier un point de contact unique dans le cadre de ce projet.

Le candidat doit s'engager à faire un point hebdomadaire sur l'état d'avancement de son projet avec le chef de projet.

12. Mécanisme d'attribution des subsides

Dans le cadre de son budget, le gouvernement fédéral dispose d'une enveloppe minimum estimée à : 2.982.000 euros pour la réalisation de ce projet qui est considéré comme un service public avec les différents candidats qui seront sélectionnés. A cette enveloppe pourrait éventuellement s'ajouter le budget non utilisé pour les phases précédentes, phase 1 (SMS) et la phase 2 (e-mails). Sur base des informations dont nous disposons actuellement, le budget non utilisé pour la phase 1-SMS est estimé à 885.000 €.

Dans les limites budgétaires ci-avant précisées, l'Etat fédéral financera jusqu'à maximum 50 % des coûts totaux. Les 50 % restants ou plus resteront à la charge de chaque candidat .

Ainsi, l'intervention totale ne dépassera pas 50% du coût total du projet. Toutefois, les subventions accordées par l'État fédéral devront être utilisées pour les dépenses engagées par le candidat en 2023, 2024 et 2025 et devront être justifiées par des pièces justificatives (voir ci-dessous).

Les subventions peuvent couvrir tous les aspects/coûts du projet. Les fonds seront alloués sur la base des données relatives aux coûts du projet (investissement, mise en œuvre et fonctionnement) fournies dans le dossier de candidature.

Si 50% des coûts totaux des candidatures sélectionnées s'avèrent supérieurs au budget total prévu, une clé de répartition sera appliquée pour distribuer les subventions entre les candidats sélectionnés : chaque candidat sélectionné recevra une part des subventions au prorata de la somme du nombre de connexions de téléphonie fixe et mobile dont dispose le candidat et du nombre total de connexions de

téléphonie fixe et mobile de tous les partis sélectionnés au 1er janvier 2023. La clé de répartition sera déterminée par l'IBPT.

La compensation de service public sera libérée comme suit

- Une première tranche de 40% des coûts éligibles après la conclusion du protocole ;

- Une deuxième tranche de 40% des coûts éligibles pour la mise en service de la plateforme pour les emails ;

- une troisième tranche dont le montant correspond à 50% des coûts éligibles réels moins le montant déjà versé dans la première et la deuxième tranche, si le candidat démontre que la plateforme de blocage des emails répond pleinement aux résultats attendus tels que décrits dans le protocole et au plus tard le 31 décembre 2024.

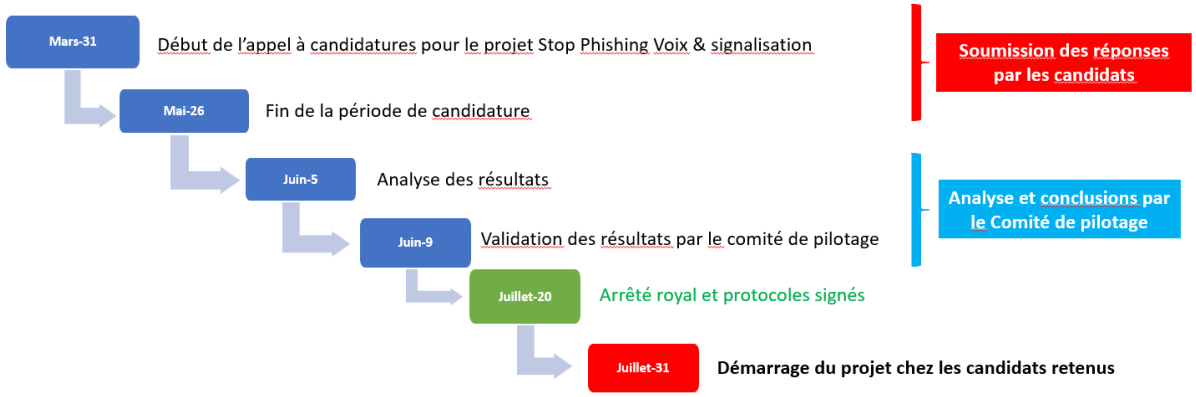
L'élaboration des subventions fera l'objet d'une décision d'attribution (arrêté royal) et d'un protocole d'accord avec le ministre des télécommunications. Ils pourront être versés en 2023 et 2024.

Pour effectuer les transferts du troisième paiement, les candidats seront invités à présenter toutes les pièces justificatives nécessaires. Cette partie sera décrite dans le protocole d'accord à signer.

Les subventions ne peuvent être utilisées à d'autres fins que les ajustements nécessaires à la mise en œuvre de la nouvelle plateforme antifraude ou à l'extension de la plateforme actuelle, comme stipulé au chapitre 3.

13. Candidature, calendrier et confidentialité

Les demandes doivent contenir toutes les informations mentionnées dans le présent appel à candidatures et être soumises au plus tard le 26 mai 2023.



Les réponses seront envoyées au responsable du projet : Yves Streel

par courrier électronique yves.streel@ccb.belgium.be

Toutes les informations fournies par le candidat seront traitées dans la plus stricte confidentialité par l'IBPT, la CCB et le ministre des télécommunications ou sa cellule politique.

Vice-Première Ministre Petra De Sutter

Annexe 1 : Dispositions pertinentes de la LCE en matière de lutte contre la fraude

Directives CLI

Le 4 décembre 2020, après une large consultation du secteur, l'IBPT a publié les lignes directrices relatives aux lignes d'appel (voir https://www.ibpt.be/operateurs/publication/lignes-directrices-pour-lidentification-de-la-ligne-appelante-cli-du-4-decembre-2020). Celles-ci définissent les bonnes pratiques que tous les opérateurs devraient adopter pour les CLI afin d'éviter les abus : chaque appel sur le territoire belge doit être associé à un numéro de réseau ; le numéro de réseau identifie de manière unique la connexion appelante ; le numéro de présentation peut être appelé et les deux numéros de réseau et de présentation sont des numéros de téléphone conformes au plan de numérotation public international.

La loi du 13 juin 2005 sur les communications électroniques

La loi du 21 décembre 2021 a introduit le nouvel article 121 §4 suivant :

"*Il est interdit de modifier l'identification de la ligne appelante ou de l'expéditeur dans le cas d'un SMS/mms dans l'intention de nuire ou de frauder l'appelé ou le destinataire de ce SMS/mms.*

L'identification de la ligne appelante ou de l'expéditeur dans le cas d'un message SMS/MMS, fournie avec une communication électronique basée sur le numéro doit :

1° être transmis sans modification à l'appelé ou au destinataire dans le cas d'un SMS/mms ;

2° contenir un numéro de téléphone valide qui identifie de manière unique la connexion ou la personne appelante ou l'expéditeur dans le cas d'un message SMS/mms.

§ 5° L'Institut détermine les modalités de présentation, de format et de transmission de l'identification de la ligne appelante ou de l'identification de l'expéditeur dans le cas d'un message SMS/mmS aux fournisseurs de réseaux et de services de communications électroniques impliqués dans le traitement des communications électroniques basées sur le numéro dans le but d'en maximiser la fiabilité.

Pour les appels ou les SMS/mms provenant de l'extérieur du territoire belge, si le numéro de téléphone n'est pas jugé fiable, l'Institut doit imposer aux opérateurs de réseaux et de services de communications électroniques, par voie d'arrêté et dans la mesure où cela est techniquement possible, des mesures visant à en informer l'appelé ou le destinataire en cas de SMS/mms ou à empêcher la présentation du numéro de téléphone.

§ 6 L'Institut détermine les numéros de téléphone qui ne peuvent jamais être affichés comme identification de la ligne appelante ou de l'expéditeur dans le cas d'un message SMS/mms."

La loi du 20 juillet 2022 définit la notion de fraude dans le cadre des communications électroniques, à savoir à l'article 2 5/5° *: " on entend par fraude un acte déloyal commis dans l'intention de tromper, en violation de la loi, des règlements ou d'un contrat, en vue d'obtenir un avantage indu pour soi-même ou pour autrui, au détriment de l'opérateur ou de l'utilisateur final, par l'utilisation d'un service de communications électroniques* ".

En outre, l'article 121/8 § 1 prévoit :

"*Sans connaître le contenu des communications, les opérateurs prennent des mesures appropriées, proportionnées, préventives et curatives, en tenant compte des capacités techniques les plus récentes, pour détecter les fraudes et les utilisations malveillantes sur leurs réseaux et services et pour éviter de nuire aux utilisateurs finaux ou de les harceler".*

Le Roi peut préciser les mesures à prendre par les opérateurs en vertu du premier alinéa.

L'Institut est autorisé à émettre des instructions contraignantes, y compris des instructions sur les délais de mise en œuvre, aux fins du présent paragraphe."

et l'article 121/8 §2

" *Lorsque la gravité des circonstances le justifie, à examiner au cas par cas, les mesures appropriées visées au paragraphe 1, point 1), peuvent notamment comprendre les éléments suivants .*

- *- des mesures au niveau du réseau, telles que le blocage de numéros, de services, d'URL, de noms de domaine, d'adresses IP ou de tout autre élément identifiant les communications électroniques ;*
- *- des mesures au niveau de l'utilisateur final, telles que la désactivation totale ou partielle de certains services ou équipements.*"