bipt

Belgisch Instituut voor
postdiensten en telecommunicatie

Mededeling van de Raad van het BIPT van 26 juni 2026 betreffende het koninklijk besluit van 12 mei 2024 ter bestrijding van internationale spraakoproepen met gespoofte Belgische telefoonnummers

Belgisch Instituut voor postdiensten en telecommunicatie
Koning Albert II-laan 32, bus 10 | 1000 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

1. Inleiding

1. Het koninklijk besluit ter bestrijding van internationale spraakoproepen met gespoofte Belgische telefoonnummers (hierna 'KB spoofing'), aangenomen in uitvoering van artikel 121/8 van de wet van 13 juni 2005 betreffende de elektronische communicatie, stelt regels vast tegen internationale spraakoproepen met gespoofte Belgische telefoonnummers.

2. Bij CLI-spoofing (CLI staat voor 'Calling Line Identification' of 'identificatie van de oproepende lijn') wordt de bellerinformatie gemanipuleerd om de persoon die de oproep krijgt, te laten geloven dat de oproep afkomstig is van een andere persoon, entiteit of locatie. Hierdoor denken burgers een betrouwbare partij aan de lijn te hebben (bijv. hun bank of autoriteiten zoals de politie), terwijl ze in werkelijkheid worden misleid. Vaak gaat het om een cruciale stap die oplichters gebruiken om persoonsgegevens te pakken te krijgen waarmee ze vervolgens fraude kunnen plegen (zoals phishing).

3. Het KB spoofing beoogt een einde te maken aan dergelijke praktijken. Zo worden een aantal regels ingevoerd om te voorkomen dat de bellerinformatie wordt gemanipuleerd, evenals reactieve maatregelen voor als er zich toch een incident zou voordoen. De maatregelen in het KB spoofing zijn gebaseerd en geïnspireerd op Aanbeveling (23)03 van de CEPT (Conférence Européenne des administrations des Postes et Télécommunications of Europese Conferentie van de administraties van Posterijen en Telecommunicatie), getiteld 'Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers' (vrije vertaling: 'Maatregelen voor de verwerking van binnenkomende internationale spraakoproepen van vermoedelijk gespoofte nationale E.164-nummers'), hierna 'aanbeveling (23)03 van de CEPT.

4. Het KB spoofing is van kracht sinds 1 september 2024 voor vaste telefoonnummers en sinds 1 december 2024 voor mobiele telefoonnummers.

5. De nieuwe regels hebben geleid tot een aantal vragen in de sector over de concrete toepassing ervan. Na een herinnering aan het juridische kader bepaald in het KB spoofing (zie punt 2 hieronder) worden deze vragen over de tenuitvoerlegging behandeld in punt 3 van deze mededeling.

6. Deze mededeling is van algemene strekking, maar doet geen afbreuk aan de mogelijkheid dat het BIPT een afzonderlijk besluit neemt dat ervan afwijkt wanneer dat op grond van specifieke omstandigheden gerechtvaardigd is.

2. Juridisch kader bepaald in het KB spoofing

2.1. Principe om onrechtmatige oproepen te blokkeren (art. 1 en 2)

7. Artikel 1 van het KB spoofing bepaalt dat operatoren die directe inkomende internationale telefoongesprekken ontvangen via hun internationale netwerkinterface (hierna: "de ontvangende operator in België"), maatregelen moeten nemen om de oproepen te blokkeren in de gevallen bepaald in het artikel, behalve voor oproepen die onder de in artikel 3 en 4 genoemde uitzonderingen vallen.

8. Dat principe is gebaseerd op de veronderstelling dat de weergave van bepaalde oproepen vanuit het buitenland '**onwettig**' is. De blokkeringsverplichting geldt wat dat betreft voor vier soorten oproepen:

   1° Inkomende oproepen die niet voldoen aan ITU-T-aanbeveling E.157.

   Overeenkomstig die aanbeveling moet een Belgische CLI bijvoorbeeld altijd het volledige telefoonnummer bevatten: de landcode 32, voorafgegaan door + of 00 en gevolgd door de netwerkcode (bijv. 473) en het abonneenummer (met de juiste lengte).

   2° Inkomende oproepen met een Belgisch geografisch en niet-geografisch E.164-telefoonnummer (bijv. de nummers 070, 078, 0800, 090X) als identificatie van de oproepende partij.

   3° Inkomende oproepen met een Belgisch mobiel E.164-telefoonnummer, tenzij kan worden vastgesteld dat de gebruiker in het buitenland roamt. Anders, en alleen als kan worden aangetoond dat een dergelijke verificatie technisch niet mogelijk is, moet de CLI onzichtbaar worden gemaakt (verwijderd) voor de opgebelde partij in plaats van de oproep te blokkeren.

   4° Oproepen met korte telefoonnummers als identificatie van de oproepende partij.

9. Zoals vermeld in het verslag aan de Koning, zijn deze regels van toepassing op zowel het presentatie- als het netwerknummer. Voor IP-gebaseerde communicatie betekent dit dat zodra in het veld 'display number', 'from/PAI number' of 'redirect number/history' een Belgisch geografisch of niet-geografisch E.164-nummer of kort telefoonnummer verschijnt, de oproep moet worden geblokkeerd.

10. In het verslag aan de Koning staat dat het verboden is om het principe te omzeilen door een buitenlands nummer te vervangen door een Belgisch nummer tijdens een 'call forwarding' (doorschakeling van een oproep).

11. In artikel 2 wordt een technische vereiste ingevoerd voor de ontvangende operatoren in België, eveneens om te voorkomen dat de regels van artikel 1 worden omzeild. De operatoren moeten er namelijk voor zorgen dat internationale telefoongesprekken alleen kunnen worden ontvangen op speciaal hiervoor bestemde circuits die duidelijk gescheiden zijn van nationale telefoongesprekken.

12. Zoals toegelicht in het verslag aan de Koning, kan het onderscheid worden gemaakt via fysiek of virtueel gescheiden circuits, zolang beide twee soorten verkeer (nationaal/internationaal) duidelijk van elkaar kunnen worden onderscheiden.

2.2. Afwijkingen (art. 3 en 4, § 1)

13. De in artikel 3 en artikel 4, § 1, bepaalde uitzonderingen zijn bedoeld om te voorkomen dat legitieme oproepen, waarvan de band met België voldoende kan worden aangetoond, worden geblokkeerd door de tenuitvoerlegging van artikel 1.

14. De volgende oproepen worden als **legitiem** beschouwd:

14.1. **Krachtens artikel 3**: oproepen van een Belgisch geografisch of mobiel E.164-telefoonnummer vanuit België naar:

i. hetzij een roaminggebruiker in België (**scenario 2** van aanbeveling (23)03 van de CEPT);

Deze situatie wordt in de context van het verslag aan de Koning geïllustreerd met het voorbeeld van een hotelbediende in België die een oproep doet naar een klant met een buitenlands mobiel telefoonnummer terwijl die aan het roamen is in België[1].

ii. hetzij een buitenlands telefoonnummer of een gebruiker die buiten België roamt en een doorschakeling heeft naar een Belgisch nummer (**scenario 3** van aanbeveling (23)03 van de CEPT).

Doorschakelingen van oproepen naar een buitenlands nummer naar een Belgisch nummer[2] zijn enkel mogelijk voor telefoonnummers waarmee de gebelde partij uitdrukkelijk heeft ingestemd.

14.2. **Krachtens artikel 4**: nomadische oproepen en oproepen gekoppeld aan specifieke diensten, namelijk cloudgebaseerde teleconferentiediensten, klantenondersteuningsdiensten en telefonische directmarketingdiensten die worden gemaakt met Belgische geografische telefoonnummers, mits zij voldoen aan de voorwaarden van artikel 4, § 1, zoals hieronder beschreven.

15. De **voorwaarden** voor de oproepen bedoeld in artikel 4 zijn als volgt (artikel 4, § 1):

- **Voor alle beoogde oproepen:** de oproepen moeten worden afgehandeld via een speciale interface, waarbij de oproepafhandeling onder volledige controle staat van de operator die de oproep initieert: van de gebruiker die de oproep initieert, over een speciale interface, tot de ontvangende operatoren in België. Deze regel is bedoeld om elk risico op wijziging van de CLI te voorkomen. Zoals aangegeven in het verslag aan

[1]Scenario 2 van aanbeveling (23)03 van de CEPT.
[2]Scenario 3 van aanbeveling (23)03 van de CEPT.

de Koning is het niet van belang hoe dat op technologisch vlak ten uitvoer wordt gebracht.

- **Enkel voor de nomadische oproepen:** het nomadische gebruik van E.164-telefoonnummers moet incidenteel zijn ten opzichte van het gebruik van deze telefoonnummers voor oproepen vanuit België.

- **Enkel voor oproepen in verband met klantenondersteuningsdiensten en telefonische directmarketingdiensten:** de E.164-telefoonnummers in kwestie moeten volledig onder controle staan van en toegewezen zijn aan een onderneming die in België gevestigd is voor de uitvoering van deze diensten. De overeenkomsten met de ontvangende operatoren in België moeten een volledige lijst bevatten van de E.164-telefoonnummers waarop de afwijking van toepassing is.

2.3. Specifieke maatregelen van het BIPT bij een vermoedelijke inbreuk (art. 4, § 2 en 5)

16. Om het BIPT in staat te stellen in te grijpen bij een vermoedelijke inbreuk op het KB spoofing, bepaalt artikel 4, § 2, dat ontvangende operatoren in België op eenvoudige vraag van het BIPT binnen 24 uur de identiteit[3] moeten meedelen van de gebruiker die een bepaalde oproep heeft gemaakt. Als deze informatie niet tijdig verstrekt wordt of onvolledig of onjuist is, dan moet die operator alle inkomende oproepen van deze gebruiker binnen de 24 uur blokkeren.

17. Bovendien kan het Instituut overeenkomstig artikel 5 ook het recht van een operator intrekken of opschorten om zich te beroepen op een afwijking zoals bedoeld in artikel 3 en 4, indien niet aan de voorwaarden is voldaan voor die afwijking of indien op basis van concrete feiten misbruik of fraude wordt vastgesteld bij de toepassing van deze afwijking.

[3] De naam, het adres en de contactgegevens of, in voorkomend geval, andere identificatiegegevens die via een directe of indirecte methode verkregen zijn, zoals vastgelegd in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

3. Vragen in verband met de tenuitvoerlegging van het KB spoofing

3.1. Voor welke operator geldt de verplichting bepaald in artikel 1?

18. Het afhandelen van een telefonische oproep vereist netwerkinfrastructuur. Die omvat capaciteit op het vlak van transmissie (bijv. glasvezel) en schakeling (bijv. SIP-servers, routers enz.), plus de bijbehorende besturingssoftware (netwerkprotocollen).

19. Twee netwerken worden met elkaar verbonden via een netwerkinterface. We spreken over een internationale netwerkinterface wanneer het ene netwerk zich in België bevindt en het andere in het buitenland. In de praktijk wordt 'binnenlands' verkeer gewoonlijk afgehandeld via nationale interconnectie-interfaces, die duidelijk gescheiden zijn van internationale interconnectie-interfaces.

20. Inkomende internationale telefoongesprekken worden geblokkeerd via de switch, bijvoorbeeld via een SIP/SBC-server ('Session Border Controller'). Het is dan ook logisch om de geografische locatie van deze SIP-servers te bepalen om de ontvangende operator in België te identificeren.

21. De verplichting bepaald in artikel 1 van het koninklijk besluit 'spoofing' geldt dus voor de operator die een SIP/SBC-server op Belgisch grondgebied heeft en die als eerste de telefonische oproep ontvangt vanuit het buitenland, van een SIP/SBC-server in het buitenland.

22. Of een operator zich al dan niet heeft aangemeld bij het BIPT (zie artikel 9 van de WEC), is geen criterium in het KB spoofing om te bepalen of het om nationaal of internationaal verkeer gaat, noch om de entiteit aan te wijzen die de blokkering moet uitvoeren.

23. In België aangemelde operatoren kunnen zowel nationaal als internationaal verkeer aanbieden. Verkeer tussen verschillende operatoren met SIP-servers in derde landen kan in principe niet als Belgisch nationaal verkeer worden beschouwd.

24. Oproepen die afkomstig zijn van, afgehandeld worden door en eindigen via netwerkinfrastructuur (d.w.z. zowel transmissie als schakeling) die zich uitsluitend op Belgisch grondgebied bevindt (en dus nooit België verlaten), behoren niet tot het toepassingsgebied van het KB spoofing.

3.2. Voor welke telefoonnummers geldt de verplichting bepaald in artikel 1, 2° en 3°?

25. Artikel 1, 2° en 3°, geldt voor alle oproepen waarvan de CLI een Belgisch telefoonnummer is[4]. Het gaat dus niet om CLI's van buitenlandse telefoonnummers en CLI's zonder telefoonnummer, maar met de melding 'privé', 'onbekend' enz.

[4] Dit zijn Belgische geografische of niet-geografische E.164-nummers (bijvoorbeeld nummers die beginnen met 070, 078, 0800, 090X) of korte telefoonnummers.

3.3. Wat met doorgegeven oproepen?

26. Over de kwestie van doorgegeven oproepen kwamen heel wat vragen uit de sector. Het gaat om oproepen die gemaakt worden vanuit België en bestemd zijn voor België, maar waarvan de afwikkeling de doorgifte omvat via fysieke infrastructuur (een SIP-server) in het buitenland. Voor dergelijke oproepen is de vraag hoe ze gekwalificeerd worden in verband met het KB spoofing en hoe de regels in het KB erop moeten worden toegepast.

27. Het KB spoofing bevat geen definitie van het begrip 'internationale oproep' of het begrip 'nationale oproep'. Om deze vragen te beantwoorden moet dus gekeken worden naar de beoogde doelstellingen van het KB spoofing, die uiteengezet worden in bijbehorende verslag aan de Koning. Dat verwijst dan weer naar aanbeveling (23)03 van de CEPT. De inleiding bij het verslag aan de Koning bevestigt dat de verplichtingen die door het KB spoofing aan de operatoren worden opgelegd aansluiten bij die aanbeveling. Het is dan ook redelijk om de verplichtingen te lezen in het licht van de aanbeveling, die er de rechtstreekse inspiratie voor vormt.

28. Als eerste moet worden opgemerkt dat het verslag aan de Koning uitgaat van het principe dat "*voor oproepen die uit het buitenland worden gemaakt, geen Belgische nummers als identificatie van de oproepende partij mogen worden getoond, behalve voor gebruikers van Belgische mobiele nummers die aan het roamen zijn in het buitenland en de andere uitzonderingen beschreven in artikel 4*."[5] Hieruit volgt dat artikel 1 tot doel heeft oproepen gemaakt vanuit het buitenland te blokkeren, niet oproepen gemaakt vanuit België, Dat wordt bevestigd in de inleiding bij het verslag aan de Koning, waarin staat dat "*het allergrootste deel van oproepen met gespoofde* [sic] *telefoonnummers wordt veroorzaakt door oproepen met Belgische telefoonnummers die worden gemaakt vanuit het buitenland*.

29. Vervolgens moet worden benadrukt dat die aanpak ook de benadering is van aanbeveling (23)03 van de CEPT. Meer specifiek wordt in punt 2 van deze aanbeveling gesteld dat de administraties van de CEPT erop zouden moeten toezien dat de genomen maatregelen noch de verwerking van legitieme inkomende internationale spraakoproepen belemmeren, noch de uitzonderingen op nationaal niveau verhinderen. Bovendien beschrijft de informatieve bijlage 1, waarnaar wordt verwezen, in scenario 4 de situatie waarbij de nationale oproep via de cloud verloopt (land B), buiten het grondgebied van het land van de gespreksopbouw en het land van de gespreksafgifte (land A). In die hypothese, en om de legitieme aard van de oproep te controleren, wordt aanbevolen om bepaalde maatregelen te nemen die de nationale oorsprong van de oproep in kwestie vrijwaren. Dergelijke maatregelen kunnen de verplichting of aanbeveling inhouden dat operatoren gebruikmaken van een speciaal hiervoor bestemde interface.

30. Ter herinnering: als maatregel om de herkomst van de oproep te garanderen verplicht artikel 2 van het KB spoofing de ontvangende operator in België om inkomende internationale oproepen te ontvangen via speciaal hiervoor bestemde circuits die duidelijk gescheiden zijn van nationale telefoongesprekken. Het verslag aan de Koning preciseert in dit opzicht het volgende: *"Artikel 2 zorgt ervoor dat de bepalingen in de andere artikelen niet eenvoudig kunnen worden omzeild door internationaal verkeer in te koppelen via nationale circuits, wat uiteraard niet toegelaten is. Dit verkeer moet duidelijk worden onderscheiden zodat dit eenvoudig te identificeren is. Deze vereiste is gericht op operatoren die het internationaal verkeer direct ontvangen. Een strikte handhaving van dit*

[5] Onderstreping toegevoegd.

principe zal nodig zijn om ervoor te zorgen dat niet via deze weg gespoofde [sic] *oproepen Belgische burgers bereiken. Het beoogde onderscheid kan via fysieke gescheiden circuits maar eveneens virtueel, door oproepen te onderscheiden via signalering, worden gerealiseerd."* [6] Met het oog op technologische neutraliteit worden aan de operatoren twee opties geboden voor de verplichting in artikel 2 om een onderscheid te maken tussen inkomend nationaal en inkomend internationaal verkeer. Deze twee types verkeer mogen telkens worden afgehandeld op ofwel een specifiek fysiek circuit ofwel een specifiek virtueel circuit.

31. Gelet op het nagestreefde doel van deze bepaling van het KB spoofing – namelijk de nationale of internationale oorsprong van de oproep garanderen (zie punt 28 hierboven) om meer algemeen de legitimiteit ervan te kunnen verifiëren – is het BIPT van mening dat de oproepen bedoeld in punt 26 hierboven, kunnen worden aangemerkt **als nationale oproepen in doorgifte**, mits ze tijdens die doorgifte volledig afgehandeld worden via specifieke circuits voor nationaal verkeer en volledig onder controle blijven van de operator bij wie de oproep is gemaakt. Het begrip 'volledig onder controle' verwijst volgens het BIPT naar de technische controle over de betrokken netwerkelementen, en dat end-to-end, tot aan de interface van de ontvangende operator in België, zodat de CLI niet kan worden gewijzigd.

32. Indien dat echter niet het geval is en de nationale of internationale oorsprong van de oproepen bijgevolg niet kan worden gegarandeerd, dan mogen de betrokken oproepen volgens het BIPT niet worden beschouwd als nationale oproepen in doorgifte en moeten ze worden behandeld als **inkomende internationale oproepen**, waardoor alle regels van het KB spoofing erop moeten worden toegepast.

33. Ongeacht de contractuele bepalingen tussen beide betrokken operatoren, die de wijze kunnen bepalen waarop zij toezien op de naleving van het KB spoofing, blijft de ontvangende operator in België in ieder geval als enige verantwoordelijk voor de naleving van het KB spoofing en, indien van toepassing, de blokkering van frauduleuze oproepen in het kader van dat besluit.

[6] Onderstreping toegevoegd.

4. Conclusie

34. Het KB spoofing bepaalt dat het de taak is van de operator die de inkomende internationale oproep rechtstreeks via zijn internationale netwerkinterface ontvangt ("de ontvangende operator in België") om de gepaste blokkeringsmaatregel te nemen.

35. Aangezien de blokkering van inkomende internationale oproepen op switchniveau plaatsvindt, dient er rekening gehouden te worden met de geografische locatie van de SIP/SBC-servers die betrokken zijn in het routeren van de oproep om de ontvangende operator in België te bepalen Daarom rust de verplichting voor het blokkeren van de inkomende frauduleuze internationale oproep op de operator die een SIP/SBC-server heeft op het Belgisch grondgebied en die als eerste de oproep uit het buitenland ontvangt van een SIP/SBC-server die zich in het buitenland bevindt.

36. Deze mededeling licht een bijzonder geval bijkomend toe, namelijk transitoproepen. Het gaat hier om een oproep die vanuit België vertrekt en bestemd is voor België, maar waarbij de afwikkeling een doorgifte omvat via de fysieke infrastructuur (een SIP-server) die zich in het buitenland bevindt.

37. Het is duidelijk dat het de bedoeling is van het KB spoofing en het bijhorende Verslag aan de Koning, gelezen in het licht van de CEPT-aanbeveling, om frauduleuze oproepen vanuit het buitenland te blokkeren, en niet oproepen vanuit België. Daarom kunnen de nodige maatregelen genomen worden zodat een legitieme oproep, die vanuit België naar België wordt gerouteerd via het buitenland, niet onterecht geblokkeerd wordt.

38. Om dit mogelijk te maken, wordt toegelaten dat dit verkeer als nationaal behandeld wordt indien de operator het nationaal en internationaal verkeer strikt gescheiden houdt. De operator waarbij de oproep werd geïnitieerd kan dit doen door het inkomend nationaal verkeer te onderscheiden van het internationaal verkeer door het verkeer te routeren via een speciaal hiertoe bestemd circuit.

39. Het BIPT beschouwt bijgevolg dat dit soort oproepen gezien kunnen worden als nationale oproepen in transit voor zover deze oproepen tijdens hun transit volledig worden verstuurd via circuits die speciaal bestemd zijn voor nationaal verkeer en die volledig onder controle staan van de operator waarbij de oproep werd geïnitieerd. Deze volledige controle houdt in dat de operator de technische controle heeft over alle betrokken netwerkelementen, tot aan de interface van de operator die de oproep ontvangt in België. Op deze manier is er een garantie dat de CLI niet aangepast kan worden.

40. In het geval dat niet aan deze voorwaarden kan worden voldaan, en de nationale of internationale oorsprong van de oproep niet kan worden gegarandeerd, behandelt de ontvangende operator in België deze oproep als inkomend internationaal verkeer. Bijgevolg dient deze operator daar de regels voorzien in het KB spoofing op toe te passen.

41. Enige onderlinge contractuele afspraken tussen operatoren hebben geen invloed op de verplichting voor de ontvangende operator in België. Deze operator blijft in elk geval verantwoordelijk voor de naleving van het KB spoofing, en dus het blokkeren van frauduleuze oproepen indien van toepassing.

Bernardo Herman
Lid van de Raad

Peggy Valcke
Lid van de Raad

Stefaan Vyverman
Lid van de Raad

Michel Van Bellinghen
Voorzitter van de Raad