Belgisch Instituut voor
postdiensten en telecommunicatie

Besluit van de Raad van het BIPT van 9 september 2021 met betrekking tot het afsluiten van de inbreukprocedure ten opzichte van Proximus voor het niet waarborgen van een ononderbroken toegang tot de nooddiensten

Niet vertrouwelijke versie

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipsgebouw C | Koning Albert II-laan 35 bus 1 | 1030 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

1. Inleiding en procedure

1. Het BIPT beschikte op 12 april 2021 ten aanzien van Proximus over informatie die zou kunnen wijzen op een overtreding van haar verplichting onder artikel 107, § 1/1, eerste lid van de wet van 13 juni 2005 betreffende de elektronische communicatie ("WEC") om alle nodige, ook preventieve, maatregelen te nemen om een ononderbroken toegang tot de nooddiensten te waarborgen.

2. Op basis van die informatie en overeenkomstig artikel 21 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector ("BIPT-statuutwet") heeft het BIPT daarom op 23 april 2021 een mededeling van grieven en beoogde maatregelen aan Proximus bezorgd. Overeenkomstig artikel 21 van de BIPT-statuutwet werd Proximus uitgenodigd om schriftelijk haar opmerkingen te formuleren evenals uitgenodigd voor een hoorzitting op 20 mei 2021.

3. Proximus heeft haar visie van de feiten kunnen weergeven tijdens de voornoemde hoorzitting en heeft het BIPT zijn schriftelijke opmerkingen op 25 mei 2021 bezorgd. Proximus acht dat er geen aanwijzingen bestaan van een inbreuk en vraagt om de inbreukprocedure te staken.

4. Op basis van de bijkomende informatie die werd verschaft door Proximus, zal het BIPT de netwerkstoring van 7/8 januari 2021 evenals de handelingen van Proximus, zowel tijdens als in de aanloop naar het incident, opnieuw analyseren in het kader van artikel 107, §1/1, eerste lid van de WEC.

2. Feiten met betrekking tot de netwerkstoring van 7/8 januari 2021

5. Telefonienetwerken hebben een centrale database en voor het 4G-netwerk en het vaste-VoIP-netwerk van Proximus is dit de Home Subscriber Server ("HSS"). Deze bestaat bij Proximus uit twee delen: enerzijds uit een front-end die in verbinding staat met het netwerk en waarop de signalisatieberichten vanuit het netwerk toekomen, anderzijds uit een achterliggende back-end (ook wel gekend als de "OneNDS") waarin de eigenlijke gegevens van de toestellen op het netwerk opgeslagen worden.

6. Deze front-end en back-end hebben beveiligde verbindingen met elkaar. Deze verbindingen worden opgezet met een gebruikersnaam 'EpsUser' en een bijhorend wachtwoord. Proximus heeft de keuze gemaakt om hiervoor een eigen wachtwoord in te stellen en maakt dus geen gebruik van het standaardwachtwoord van Nokia.

7. [Vertrouwelijk]

8. Op 26 november 2020 voerde Nokia enkele geplande wijzigingen door aan de back-ends. Door een software-bug tijdens deze netwerkwijzigingen werd het wachtwoord voor de 'EpsUser' in alle kopieën van de back-end echter onbedoeld gereset naar het standaardwachtwoord van Nokia. Dit terwijl het wachtwoord voor de 'EpsUser' in alle kopieën van de front-end het door Proximus gekozen wachtwoord bleef, waardoor deze wachtwoorden dus niet langer op elkaar waren afgestemd.

9. Hierdoor konden er geen nieuwe verbindingen tussen de verschillende kopieën van de front-end en de verschillende kopieën van de back-end meer gemaakt worden. Deze wachtwoord-discrepantie werd echter destijds niet opgemerkt omdat de toen bestaande verbindingen intact bleven.

10. Op 3 december 2020 werd dit wachtwoordprobleem besproken op een vergadering tussen Nokia en Proximus, dewelke handelde over de status van hun 'vHLR vHSS project'. Van deze bespreking werd overigens notitie gemaakt in de minuten van deze vergadering,[1] dewelke nadien per mail werden overgemaakt aan het hele projectteam van het 'vHLR vHSS project'. In dit projectteam werken verscheidene ingenieurs, waaronder ook enkele van Proximus.[2]

11. In de nacht van 7 op 8 januari 2021 werd, tijdens een geplande installatie door Proximus van een software-patch van Nokia, één van de kopieën van de back-end uit het telefonienetwerk van Proximus gehaald. Dit had tot gevolg dat de verbindingen tussen deze kopie van de back-end en de verschillende kopieën van de front-end werd verbroken. De verschillende kopieën van de front-end trachtten deze verbroken verbinding te compenseren door extra verbindingen aan te leggen met de andere kopieën van de back-end, maar deze extra verbindingen faalden omwille van de wachtwoorddiscrepantie.

[1] Er werd in die minuten melding gemaakt van een probleem met beschrijving "LDAP password NOK on OneNDS" en opmerking "PROD OneNDS EpsUser password NOK?".
[2] Zo werd de mail verzonden naar 2 Solution Engineers en 1 Project Engineer van Proximus. Daarnaast werden er nog een paar in kopie gezet, meer bepaald de Team Leader, 2 Project Managers en 1 Engineer van Proximus.

12. Iedere front-end beschikt over een ingebouwde beveiliging om te vermijden dat het van het netwerk vragen blijft ontvangen die het niet kan beantwoorden. Dus wanneer een significant deel van de verbindingen naar de verschillende kopieën van de back-end faalt, zal iedere front-end de rest van het netwerk informeren dat het geen vragen meer kan beantwoorden. Door de automatische activatie van dit beveiligingsmechanisme beschikte het 4G- en VoIP-netwerk van Proximus niet langer over een functionele HSS.

13. Dit had tot gevolg dat het 4G-netwerk en het vaste VoIP-netwerk van Proximus voor ongeveer 6 uur lang buiten werking waren. Gezien alle Belgische 101-centrales en de 100/112-centrales in Brussel, Vlaams-Brabant, Namen, Waals-Brabant, Oost-Vlaanderen en West-Vlaanderen op het VoIP-netwerk van Proximus zijn aangesloten[3], waren deze noodcentrales gedurende die 6 uur onbereikbaar.

14. Proximus beschikt voor ASTRID over een Disaster Recovery System ("DRS") om, in geval van een falen van de gewoonlijk gebruikte methode, de oproepen naar de hiervoor genoemde noodcentrales via andere telefoonlijnen naar deze noodcentrales te routeren. Hierbij wordt gebruik gemaakt van specifieke telefoonlijnen per noodcentrale, in plaats van de business trunks die Proximus in normale omstandigheden gebruikt. Deze specifieke telefoonlijnen maken echter ook gebruik van het VoIP-netwerk van Proximus en zodus werkte ook deze noodoplossing niet.

15. Nadat Proximus, op aanraden van Nokia, de wachtwoorden in de verschillende kopieën van de back-end terug wijzigde naar het initieel door Proximus daartoe gekozen wachtwoord, herstelde de situatie zich. De verbindingen tussen de verschillende kopieën van de front-end en de verschillende kopieën van de back-end konden opnieuw gemaakt worden en dientengevolge waren de verschillende kopieën van de front-end na ongeveer 6 uur na aanvang van de problemen opnieuw in staat om vragen van het netwerk te beantwoorden.

16. Andere operatoren werden niet rechtstreeks getroffen door het incident. Desondanks viel er een duidelijk indirect effect op te merken: een significante degradatie op de interconnecties door het mislukken van oproepen naar nummers getroffen door de panne, waaronder de meerderheid van de noodnummers.

[3] Al deze noodcentrales worden beheerd door ASTRID, een gespecialiseerde telecomoperator voor de hulp- en veiligheidsdiensten in België. ASTRID en Proximus hebben de commerciële overeenkomst afgesloten om alle noodcentrales op het VoIP-netwerk van Proximus aan te sluiten.

3. Analyse

3.1. Kader bewijslast

17. Artikel 107, § 1/1, eerste lid van de WEC schrijft het volgende voor:

"De ondernemingen die openbare telefoondiensten aanbieden, nemen, in voorkomend geval, in samenspraak met de ondernemingen die de onderliggende openbare elektronische-communicatienetwerken aanbieden, alle nodige, ook preventieve, maatregelen om een ononderbroken toegang tot de nooddiensten te waarborgen."

18. Bovenstaande betreft een verplichting om een welbepaald resultaat te bereiken, meer bepaald een ononderbroken toegang tot de nooddiensten. Indien dat beoogde resultaat niet bereikt wordt, is het aan diegene op wie de verplichting rust om te bewijzen dat zij nochtans alle nodige maatregelen heeft genomen om dat resultaat te bereiken.

19. Door het loutere feit dat de toegang tot de nooddiensten voor ongeveer 6 uur lang werd onderbroken ten gevolge van het incident bij Proximus, kan men reeds stellen dat Proximus niet het beoogde resultaat van artikel 107, § 1/1, eerste lid van de WEC bereikt heeft. Het is aan Proximus om te bewijzen dat zij, ondanks dat zij er klaarblijkelijk niet in is geslaagd om een ononderbroken toegang tot de nooddiensten te waarborgen, hiertoe nochtans alle nodige preventieve maatregelen heeft genomen.

20. Proximus besteedt een deel van haar activiteiten als operator uit aan Nokia.[4] Hoewel dit een gangbare praktijk is bij operatoren, betekent dit niet dat Proximus niet langer zelf verantwoordelijk zou zijn om haar verplichtingen als operator overeenkomstig het regelgevende kader te vervullen. Het is immers Proximus zelf die alle nodige, ook preventieve, maatregelen moet nemen om een ononderbroken toegang tot de nooddiensten te waarborgen.

21. Dit wil ook zeggen dat Proximus voldoende uitgebreide en transparante communicatiekanalen met haar toeleveranciers moet opzetten. De keuze om bepaalde taken uit te besteden, mag er niet toe leiden dat software-bugs of andere fouten zich ongemerkt in haar netwerk kunnen nestelen, al zeker niet wanneer die ertoe kunnen leiden dat het netwerk van Proximus wordt platgelegd. Het is en blijft de verantwoordelijkheid van Proximus om eventuele fouten tijdig op te sporen of om haar toeleveranciers te verplichten om met grote zorgvuldigheid eventuele fouten op te sporen en die op een duidelijke wijze te melden (en eventueel zelf op te lossen). In alle gevallen moet een hoge mate van transparantie en efficiënte samenwerking verzekerd worden tussen partijen die dergelijke kritische taken aan elkaar toevertrouwen.

3.2. Analyse

3.2.1. Algemeen

22. Het BIPT ging er op basis van de destijds beschikbare informatie van uit dat het voor Proximus (of tenminste voor Nokia) duidelijk moest zijn dat de wachtwoorddiscrepantie die

[4] [Vertrouwelijk]

begin december 2020 werd vastgesteld in de verbinding tussen de One-DNS (back-end) en de vHSS (virtuele front-end) zich ook naar de verbinding tussen de One-DNS en de HSS (in gebruik zijnde front-end) in de productieomgeving had gepropageerd. Op basis van de nieuwe informatie die werd aangeleverd door Proximus, lijkt het echter aannemelijk dat de discrepantie voor Proximus en Nokia beperkt leek tot de verbinding tussen de One-DNS en de vHSS[5]. De wachtwoorddiscrepantie werd immers geïntroduceerd door een patch die specifiek bestemd was voor de vHSS-omgeving. Het was ook alleen in deze omgeving dat het probleem werd opgemerkt, aangezien de LDAP-connecties niet meer werkten en de vHSS daardoor niet langer functioneerde.

23. Hoewel het dus duidelijk was dat er een probleem bestond in de virtuele omgeving, konden Proximus en Nokia niet redelijkerwijze aannemen dat deze discrepantie zich verder had gepropageerd over de andere redundante componenten en dat er een vergelijkbaar probleem zou bestaan in de productieomgeving. In de productieomgeving was alles immers probleemloos blijven draaien.

24. Dat noch Proximus noch Nokia de reflex hebben gehad om te verifiëren of er zich geen vergelijkbaar probleem had voorgedaan in de productieomgeving, wijst niet noodzakelijk op een inbreuk op Proximus haar verplichting om alle noodzakelijke maatregelen te nemen overeenkomstig artikel 107, §1/1, eerste lid van de WEC. In een grote IT-omgeving is het immers quasi onmogelijk om alle verschillende teams op de hoogte te houden van problemen die zich in een ander team voordoen (des te meer als het gaat om teams die afzonderlijk werken aan systemen waarvan de ene zich in een productie- en de andere zich in een laboratoriumomgeving bevindt) en om dan ook nog eens na te gaan of deze een impact zouden kunnen hebben op de eigen omgeving.

25. Het vHSS-projectteam had de LDAP-connecties in de vHSS-omgeving midden december reeds hersteld. Nokia gaf daarbij aan verder onderzoek te zullen voeren naar hoe het kon dat de wachtwoorddiscrepantie zich had voorgedaan. Dit onderzoek moest eerst duidelijkheid brengen alvorens de vHSS effectief in gebruik genomen zou worden, maar daarvoor had Nokia nog ruim de tijd. In afwachting van dit verder onderzoek had Nokia Proximus bovendien expliciet aangeraden om de wachtwoorddiscrepantie niet zomaar recht te zetten, zonder te begrijpen wat er de concrete oorzaak van was, uit vrees voor mogelijke schadelijke onvoorziene gevolgen.

26. Zoals gezegd, bleef de rest van het netwerk van Proximus zonder problemen draaien. Er waren dus geen indicaties dat het vHSS-projectteam had moeten weten of verwachten dat de impact van de wachtwoorddiscrepantie groter was dan ingeschat. Dat de discrepantie in de rest van het netwerk onder de radar is gebleven, lijkt aannemelijk. De bewering van Proximus dat het probleem voor hen tot aan het incident op 7/8 januari beperkt leek tot de vHSS-omgeving is een geloofwaardige en redelijke bewering.

27. Ook het team dat de triggerpatch installeerde op 7/8 januari 2021 had geen reden om aan te nemen dat er een eventuele wachtwoorddiscrepantie aanwezig zou kunnen zijn. De patch op zich had immers geen invloed op het wachtwoord van de One-DNS voor de HSS en het wachtwoord van de HSS voor de One-DNS, dus een controle van de coherentie tussen die wachtwoorden stond (logisch gezien) ook niet in de pre-checks van die patch.

[5] Dit is een belangrijk verschil, omdat op de vHSS nog geen klantenverkeer liep. Door bepaalde tests eerst in een virtuele omgeving uit te voeren, wordt het risico op incidenten met een concrete impact op eindgebruikers normaal gezien vermeden.

28. Verder werd de triggerpatch reeds begin 2020 zonder problemen geïnstalleerd in de lab-omgeving, maar op dat moment was de root-cause-patch nog niet geïnstalleerd in de lab-omgeving en was de wachtwoorddiscrepantie daar dus niet aanwezig. Er waren dus geen indicaties dat de triggerpatch een probleem kon veroorzaken.

3.2.2. Alle noodzakelijke preventieve maatregelen

29. Uit de evaluatie hierboven blijkt dat het incident niet te wijten is aan een fout of nalatigheid die door Proximus veroorzaakt werd. Artikel 107, §1/1, eerste lid van de WEC legt echter een verdergaande verplichting op aan Proximus. Naast de analyse of het incident te wijten was aan een fout of nalatigheid van Proximus, moet tevens de vraag gesteld worden of Proximus wel degelijk alle nodige, inclusief preventieve, maatregelen heeft genomen om een ononderbroken toegang tot de nooddiensten te waarborgen.

30. Gezien het BIPT geen perfect zicht heeft op de technische en operationele elementen van het netwerk van Proximus, noch op de onderlinge relatie tussen Proximus en Nokia (inclusief operationele afspraken), is het voor het BIPT zeer moeilijk om na te gaan of Proximus alle nodige, inclusief preventieve, maatregelen heeft genomen om een ononderbroken toegang tot de nooddiensten te waarborgen. Het is in dat opzicht aan Proximus om alle maatregelen op te lijsten die zij in dit kader genomen heeft, teneinde een evaluatie door het BIPT mogelijk te maken.

31. Volgende relevante overwegingen worden door Proximus aangehaald:

- Haar netwerkinfrastructuur is gebaseerd op meervoudige redundanties die precies bedoeld zijn om netwerkincidenten te kunnen ondervangen.
- Proximus gebruikt eigen wachtwoorden op het netwerk precies omwille van veiligheids- en beveiligingsredenen voor haar netwerk. Het werken met standaard wachtwoorden is in principe een minder veilige wijze van handelen met een groter risico op netwerk- en veiligheidsincidenten.
- De specifieke toegang tot de nooddiensten, inclusief de daarvoor voorziene redundanties op het vlak van de aansluitlijnen, is vastgesteld in samenwerking met die nooddiensten.
- Geplande interventies op het netwerk worden 's nachts uitgevoerd bij wijze van maatregel om de impact van een mogelijk netwerkincident te beperken.
- Geplande interventies op het netwerk worden voorbereid via passende labtesten die bedoeld zijn om netwerkincidenten in de mate van wat redelijkerwijze voorzienbaar is te vermijden.
- De vastgestelde wachtwoorddiscrepantie in de virtuele HSS was het voorwerp van onderzoek en opvolging. Er werd uit voorzichtigheidsoverwegingen gewacht met het terugzetten van het wachtwoord.
- In parallel heeft Proximus met de bevoegde instanties en de nooddiensten een noodoplossing in plaats gesteld die snel operationeel was en via de geijkte kanalen aan de bevolking kon worden meegedeeld.
- Na het incident heeft Proximus in overleg met de bevoegde instanties en de nooddiensten een alternatief voorzien, gelijkaardig met wat onder het voorgaande punt werd aangehaald, dat onmiddellijk kan geactiveerd worden indien er zich nog een dergelijk incident in de toekomst zou kunnen voordoen.

- Proximus stelt dat het altijd het initiatief heeft gesteund om ook een toegang tot de nooddiensten via een tweede infrastructuur van een andere operator te verzekeren waarop zou kunnen overgeschakeld worden indien er zich op haar eigen infrastructuur een incident zou voordoen.

32. Hoewel voorgaande maatregelen onvoldoende zijn gebleken om een ononderbroken toegang tot de nooddiensten te waarborgen, kan het BIPT – op basis van de informatie waar het op dit ogenblik over beschikt – niet concluderen dat Proximus klaarblijkelijk te weinig heeft gedaan om het incident in casu te vermijden.

33. Het BIPT neemt er ook akte van dat Proximus maatregelen zal nemen, zodat dergelijke incidenten in de toekomst nog sneller kunnen opgevangen worden. Meer bepaald gaat het om een extra technische maatregel om noodoproepen rechtstreeks om te leiden naar mobiele nummers van de nooddiensten. Bovendien verwacht het BIPT dat Proximus de redundantie van het netwerk verder optimaliseert[6] (of andere maatregelen treft), zodat vergelijkbare incidenten niet langer dezelfde impact zullen hebben.

34. In dezelfde zin heeft het BIPT naar aanleiding van dit incident samen met de operatoren en de nooddiensten de mogelijkheid van een redundante oplossing onderzocht via een andere operator dan Proximus. Gezien artikel 107, §1/1, eerste lid WEC een verplichting aan Proximus oplegt om een ononderbroken toegang tot de nooddiensten te voorzien en daarvoor alle nodige maatregelen te treffen, verwacht het BIPT de volledige en proactieve medewerking van Proximus zodat dit project kan bijdragen aan de optimale werking van de nooddiensten. Dit betekent eveneens dat Proximus de nodige middelen inzet opdat deze bijkomende redundantie zo snel mogelijk kan verwezenlijkt worden.

35. Rekening houdende met voorgaande analyse en de door Proximus aangehaalde initiatieven en maatregelen, stelt het BIPT vast dat er geen duidelijke indicatie van een inbreuk op het regelgevend kader, en meer specifiek op artikel 107, §1/1, eerste lid van de WEC, bestaat. Het BIPT maakt hierbij wel een voorbehoud ten aanzien van eventuele informatie (waaronder communicatie tussen Nokia en Proximus) waarvan het op dit ogenblik niet op de hoogte zou zijn.

[6] Proximus heeft hiervoor reeds een interne audit opgestart teneinde te analyseren of en hoe de bestaande redundantie op zijn netwerk kan versterkt worden.

4. Raadpleging mediaregulatoren

36. Artikel 3 van het samenwerkingsakkoord[7] voorziet in de raadpleging door een reguleringsinstantie van de andere reguleringsinstanties voor elk ontwerpbesluit betreffende de elektronische-communicatienetwerken.

37. De geraadpleegde reguleringsinstanties beschikken over een termijn van 14 kalenderdagen om hun opmerkingen mee te delen aan de reguleringsinstantie die het ontwerp heeft voorgelegd. Binnen die termijn kan elk van de geraadpleegde reguleringsinstanties ook vragen om het ontwerpbesluit aanhangig te maken bij de CRC. De betrokken reguleringsinstantie neemt de opmerkingen in aanmerking die de andere regulerende instanties eraan bezorgd hebben en bezorgt de gewijzigde ontwerpbeslissing aan de andere regulerende instanties. Deze laatste beschikken dan over een termijn van 7 kalenderdagen waarbinnen zij kunnen vragen dat de gewijzigde ontwerpbeslissing aanhangig wordt gemaakt bij de CRC.

38. Een ontwerpbesluit is aan de mediaregulatoren meegedeeld op 19 augustus 2021. VRM, CSA en Medienrat hebben gemeld geen opmerkingen te hebben op het ontwerpbesluit.

[7] Samenwerkingsakkoord van 17 november 2006 tussen de Federale Staat, de Vlaamse Gemeenschap, de Franstalige (sic) Gemeenschap en de Duitstalige Gemeenschap betreffende het wederzijds consulteren bij het opstellen van regelgeving inzake elektronische-communicatienetwerken, het uitwisselen van informatie en de uitoefening van de bevoegdheden met betrekking tot elektronische-communicatienetwerken door de regulerende instanties bevoegd voor telecommunicatie of radio-omroep en televisie, M.B., 28 december 2006, 75371.

5. Besluit

39. Op 9 september 2021 heeft de Raad van het BIPT besloten dat er, op basis van de informatie die ter beschikking is van het BIPT, geen duidelijke overtreding ten hoofde van Proximus kan vastgesteld worden met betrekking tot het netwerkincident van 7/8 januari 2021. Om deze redenen besluit het BIPT om de inbreukprocedure ten aanzien van Proximus zonder gevolg af te sluiten.

40. Het BIPT neemt er wel akte van dat Proximus verdere maatregelen zal nemen om de redundantie te optimaliseren en in overleg met de nooddiensten performante alternatieven voorziet zodat de impact van dergelijke incidenten zo klein mogelijk wordt gehouden. Verder verwacht het BIPT dat Proximus zich constructief opstelt en actief bijdraagt aan de mogelijke opstelling van een bijkomende redundantie op het netwerk van een andere operator.

6. Beroepsmogelijkheden

41. Overeenkomstig artikel 2, § 1, van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector hebt u de mogelijkheid om tegen dit besluit beroep in te stellen bij het Marktenhof, Poelaertplein 1, B-1000 Brussel. Het beroep wordt, op straffe van nietigheid die ambtshalve wordt uitgesproken, ingesteld door middel van een ondertekend verzoekschrift dat wordt ingediend ter griffie van het hof van beroep van Brussel binnen een termijn van zestig dagen na de kennisgeving van het besluit of bij gebreke aan een kennisgeving, na de publicatie van het besluit of bij gebreke aan een publicatie, na de kennisname van het besluit.

42. Het verzoekschrift bevat op straffe van nietigheid de vermeldingen vereist door artikel 2, § 2, van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector. Indien het verzoekschrift elementen bevat die u als vertrouwelijk beschouwt, dan moet u dat uitdrukkelijk aangeven en op straffe van nietigheid, een niet-vertrouwelijke versie van dat verzoekschrift indienen. Het Instituut publiceert op zijn website het verzoekschrift dat door de griffie van het gerecht genotificeerd is. Elke belanghebbende partij kan in de zaak tussenkomen binnen dertig dagen na deze publicatie.

Axel Desmedt
lid van de Raad

Jack Hamande
lid van de Raad

Luc Vanfleteren
lid van de Raad

Michel Van Bellinghen
voorzitter van de Raad