VOORSTEL

Overeenkomstig artikel 116, lid 6, van de wet inzake elektronische communicaties (UL RS nrs. 130/22 en 18/23 – ZDU-1O) legt het Agentschap voor communicatienetwerken en -diensten van de Republiek Slovenië, rekening houdend met de informatieprocedure overeenkomstig Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz. 1), het volgende vast:

ALGEMENE WET
inzake aanvullende veiligheidsvereisten en -beperkingen

Artikel 1
(Inhoud van de algemene wet)

Deze algemene wet bepaalt:

1. richtsnoeren die dienen te worden gevolgd door exploitanten van mobielecommunicatienetwerken (hierna “exploitanten” genoemd) die deze netwerken aanbieden aan kritieke entiteiten die beheerders van kritieke infrastructuur zijn op andere gebieden van de regelgeving inzake kritieke infrastructuur, zoals gespecificeerd in de wetgeving inzake kritieke infrastructuur (hierna “kritieke infrastructuurbeheerders” genoemd), aanbieders van essentiële diensten zoals bepaald door de wet inzake informatiebeveiliging (hierna “aanbieders van essentiële diensten” genoemd), overheidsorganen zoals bepaald door de wet inzake informatiebeveiliging (hierna “overheidsorganen” genoemd) of dragers van belangrijke onderdelen van het beveiligingssysteem van het land; en
2. kritieke elementen van het netwerk en de bijbehorende informatiesystemen met hun functies als bedoeld in artikel 116, lid 6, van de wet inzake elektronische communicaties (UL RS nrs. 130/22 en 18/23 – ZDU-1O); hierna “Wet” genoemd), zoals uiteengezet in de bijlage, die een integraal deel uitmaakt van deze algemene wet en wordt opgesteld in samenwerking met de instantie die verantwoordelijk is voor informatiebeveiliging.

Artikel 2
(Betekenissen van de termen)

(1) Onder de in deze algemene wet gebruikte termen wordt verstaan:

1. Een leveringsketen is het volledige systeem van processen, mensen, organisatie en distributie die betrokken zijn bij het ontwerp, de productie, de opslag, de distributie en de levering, evenals de installatie en het onderhoud van onderdelen van kritieke netwerkelementen die zijn geïnstalleerd in het netwerk van de exploitant of bij de clouddienstverlener die dergelijke diensten aan de exploitant levert.

2. Kritieke elementen van het netwerk zijn die netwerkelementen, functies, diensten en ondersteunende informatiesystemen in fysieke, software- of gevirtualiseerde vorm bij

de exploitant of bij de clouddienstverlener, zoals vermeld in de bijlage bij deze algemene wet.

3. Kritieke entiteiten zijn kritieke infrastructuurbeheerders op andere gebieden van regelgeving inzake kritieke infrastructuur, bepaald in overeenstemming met de wetgeving die van toepassing is op het gebied van kritieke infrastructuur, aanbieders van essentiële diensten zoals bepaald door de wet inzake informatiebeveiliging, overheidsorganen zoals bepaald door de wet inzake informatiebeveiliging en dragers van belangrijke delen van het beveiligingssysteem van het land.

(2) Andere termen die in deze algemene wet worden gebruikt, hebben dezelfde betekenis als gedefinieerd in de wet en de algemene wet inzake de beveiliging van netwerken, diensten en gegevens.

Artikel 3
(Algemene richtlijnen)

(1) Exploitanten in de toeleveringsketen van onderdelen van kritieke netwerkelementen en ondersteuningsdiensten op het derde niveau voor deze onderdelen houden gedurende de volledige levenscyclus van deze onderdelen ten minste rekening met de volgende richtsnoeren:

1. voor een individuele fabrikant of leverancier en voor een aanbieder van ondersteuningsdiensten op het derde niveau als gevolg van relaties en overeenkomsten ermee, voeren zij een risicobeoordeling uit voor wat betreft levering en potentiële gevolgen door derde natuurlijke of rechtspersonen onder publiek- of privaatrecht (hierna “derden” genoemd), compatibiliteit met apparatuur van andere fabrikanten, productkwaliteit en -veiligheid en mogelijke negatieve gevolgen voor de exploitatie van de diensten en kritieke entiteiten van de exploitant;
2. dat beveiliging al in het ontwerp is ingebouwd en geïmplementeerd en dat contracten termijnen bevatten voor het wegnemen van vermeende kwetsbaarheden;
3. dat de belangrijkste beveiligingskenmerken (beschikbaarheid, vertrouwelijkheid, integriteit en authenticiteit) gedurende de volledige levenscyclus van het gebruik ervan worden gewaarborgd;
4. dat de beveiliging en de ononderbroken levering ervan worden gewaarborgd en dat wordt bevestigd dat hoge beveiligingskenmerken worden ondersteund in overeenstemming met internationaal erkende normen (3GPP) en Europese technische normen (ETSI);
5. dat de in de punten 2 tot en met 4 van dit lid bedoelde richtsnoeren verifieerbaar zijn in de contractuele documentatie met de fabrikant of met de leverancier;
6. voor elke fabrikant of leverancier worden ook de risico’s in verband met de gebruiksrechten van de belangrijkste technologieën, die nodig zijn voor de vervaardiging en het gebruik van de apparatuur en de risico’s in verband met de levering van apparatuur, reserveonderdelen of ondersteuningsdiensten op het derde niveau, beoordeeld en in aanmerking genomen;
7. dat de gebruikte onderdelen geen onopgeloste, bekende kritieke of actief geëxploiteerde kwetsbaarheden hebben;
8. het vermijden van één enkele fabrikant of leverancier, indien dit technisch haalbaar en economisch duurzaam is, met als doel afhankelijkheid te verkleinen en

veerkracht te vergroten in geval van kwetsbaarheden van kritieke onderdelen, catastrofale netwerkuitval of een bedreiging voor de veiligheid van netwerken en diensten van kritieke entiteiten door derde natuurlijke of rechtspersonen die onder publiek- of privaatrecht vallen.

(2) Bij de levering van informatie- en communicatieapparatuur, -systemen en -diensten voldoen exploitanten volledig aan de richtsnoeren van het Agentschap van de Europese Unie voor cyberbeveiliging (hierna “Enisa” genoemd) en de geldende regelgeving van de Europese Unie met betrekking tot fundamentele beveiligingsvereisten bij de aankoop van beveiligde ICT-producten en -diensten. Het Agentschap publiceert op zijn website links naar de huidige ENISA-documenten en EU-regelgeving op bovengenoemd gebied en houdt deze up-to-date.

(3) Bij het leveren van onderdelen van kritieke netwerkelementen of het gebruik van clouddiensten wordt prioriteit gegeven aan het kiezen van onderdelen van fabrikanten of leveranciers of diensten van clouddienstverleners die zijn gecertificeerd door conformiteitsbeoordelingsinstanties die zijn geaccrediteerd en, indien nodig, zijn gemachtigd op grond van artikel 60, lid 3, van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (hierna “Verordening” genoemd) voor de afgifte van Europese cyberbeveiligingscertificaten op bepaald zekerheidsniveau, zoals bepaald in artikel 52 van de Verordening.

(4) Voor het doeleinde van het vorige lid controleert de exploitant een door de ENISA overeenkomstig artikel 55 van de Verordening opgerichte speciale website om het publiek te informeren over Europese regelingen voor cyberbeveiligingscertificering, Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen, met inbegrip van informatie over Europese regelingen voor cyberbeveiligingscertificering die niet langer geldig of ingetrokken zijn en verlopen Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen, en een opslagplaats van links naar cyberbeveiligingsinformatie.

Artikel 4
(Risicobeoordeling)

(1) Bij het bepalen van het risico van de fabrikant of leverancier van onderdelen en de dienstverlener op het derde niveau voor kritieke elementen van het netwerk houdt de exploitant rekening met de volgende risicoaspecten, die hij evalueert.

(2) Bij de in het vorige lid bedoelde waardering beoordeelt en houdt de exploitant ten minste rekening met:

1. de algemene kwaliteit (inclusief veiligheidsaspecten) en betrouwbaarheid;
2. de mate van gebruik van open standaarden en interfaces die afhankelijkheid en het insluitingseffect bij de producten van een bepaalde fabrikant of leverancier voorkomen;
3. naleving van erkende internationale en Europese technische normen (3GPP, ETSI) en de regelgeving van de Europese Unie en standaardbeveiligingsinstellingen in overeenstemming met professionele aanbevelingen (GSMA-vereniging);
4. mate van compatibiliteit met apparatuur en netwerkfuncties van derden;

5. mogelijkheid om upgrades en aanpassingen aan te bieden;
6. het kwetsbaarheidsbeheerproces, de openbaarmaking ervan en het up-to-date-proces met updates en oplossingen;
7. beschikbaarheid en transparantie van documentatie met betrekking tot:
   - belangrijke functies en informatie over beveiliging en andere functies van het onderdeel en mogelijke instellingen, en
   - gebruikte software, met inbegrip van opensourcecode (stuklijst – SBOM);
8. mate van afhankelijkheid van ondersteuningsdiensten op het derde niveau bij het beheer en het onderhoud van apparatuur, indien de exploitant deze diensten niet alleen met zijn werknemers uitvoert;
9. voorlopige beoordeling van de conformiteit van apparatuur of een entiteit die een ondersteuningsdienst op het derde niveau zou verlenen door in de Europese Unie geaccrediteerde instanties overeenkomstig Europese regelingen voor cyberbeveiligingscertificering, waarbij de geaccrediteerde instanties in het Publicatieblad van de Europese Unie worden bekendgemaakt.

(3) De exploitant documenteert de risicofactoren en de resultaten van de risicobeoordeling voor elke geselecteerde fabrikant of leverancier of derde dienstverlener als bedoeld in de leden 2 en 3 van dit artikel en werkt dit regelmatig bij.

Artikel 5
(Algemene richtsnoeren voor de exploitatie van kritieke netwerkelementen)

(1) De onderdelen van de kritieke netwerkelementen, de exploitatie en de standaardinstellingen ervan mogen geen technische kenmerken bevatten die de beveiliging of de exploitatie van kritieke entiteiten negatief kunnen beïnvloeden, onder meer als gevolg van sabotage, spionage, diefstal van intellectueel eigendom of terrorisme.

(2) De kritieke netwerkelementen bevinden zich over het algemeen in de Republiek Slovenië of, rekening houdend met alle beveiligingsrisico's en het waarborgen van een hoog niveau aan beveiligingsmaatregelen, en indien dit niet anders is bepaald in de toepasselijke regelgeving, in de Europese Unie. De exploitant stelt het Agentschap voor communicatienetwerken en -diensten van de Republiek Slovenië (hierna het "Agentschap" genoemd) en het orgaan dat verantwoordelijk is voor de informatiebeveiliging ten minste 30 dagen vóór de verhuizing naar buiten de Europese Unie in kennis van hun voorgenomen verhuizing.

(3) Ondersteuningsdiensten op het derde niveau voor kritieke elementen van het netwerk worden in het algemeen uitgevoerd in de Republiek Slovenië of, rekening houdend met alle beveiligingsrisico's en het waarborgen van een hoog niveau aan beveiligingsmaatregelen, en indien dit niet anders is bepaald in de toepasselijke regelgeving, in de Europese Unie. De exploitant stelt het Agentschap en het voor de informatiebeveiliging verantwoordelijke orgaan ten minste 30 dagen vóór de verhuizing naar buiten de landen van de Europese Unie in kennis van de voorgenomen verhuizing van hun ondersteuningsdiensten op het derde niveau.

(4) De implementatie van ondersteuningsdiensten op het derde niveau mag de beveiliging of de exploitatie van de diensten van kritieke entiteiten of de nationale veiligheid niet in gevaar brengen.

(5) De exploitant stelt het proces voor de identificatie van kritieke netwerkelementen op en implementeert ze regelmatig. Dit dient ten minste eenmaal per jaar te worden uitgevoerd of wanneer onderdelen van kritieke netwerkelementen worden aangekocht.

(6) Indien een afzonderlijk onderdeel slechts gedeeltelijk een kritiek netwerkelement vertegenwoordigt, wordt het beschouwd als onderdeel van een kritiek netwerkelement.

(7) De exploitant houdt een bijgewerkte lijst bij van alle onderdelen van kritieke netwerkelementen, de functies, locaties, administrateurs en beheerders ervan, hun derdelijns ondersteuningsdienstverleners en hun fabrikanten of leveranciers. Op verzoek wordt de lijst ter beschikking gesteld van het Agentschap en een voor informatiebeveiliging verantwoordelijke instantie.

Artikel 6
(Veiligheidsmaatregelen voor de levering van onderdelen van kritieke netwerkelementen)

(1) De exploitant is zich bewust van de volledige toeleveringsketen en de daaraan verbonden risico's, met inbegrip van onderaannemers van afzonderlijke onderdelen van kritieke netwerkelementen, die ook coderingssleutels, UICC/eUICC en andere beveiligingselementen omvatten, waarvan het misbruik de veiligheid van kritieke entiteiten in gevaar zou kunnen brengen.

(2) De exploitant zorgt ervoor dat de beveiligingsvereisten tussen de exploitant en de fabrikanten of leveranciers van onderdelen van kritieke netwerkelementen of zijn derdelijns ondersteuningsdienstverleners contractueel zijn overeengekomen en gedocumenteerd en vereisen dat fabrikanten of leveranciers de overeengekomen veiligheidsmaatregelen in de volledige toeleveringsketen naleven.

(3) Om de exploitatie van kwetsbaarheden door kwaadwillige medespelers tijdig te voorkomen, zorgt de exploitant ervoor dat de fabrikant of leverancier van onderdelen van een kritiek netwerkelement zich contractueel verbindt om de exploitant onmiddellijk op de hoogte te stellen van de geconstateerde kwetsbaarheid en van maatregelen om risico's te beperken en advies te geven over beschermende of corrigerende maatregelen die de exploitant kan nemen als reactie op de dreiging.

(4) De exploitant verifieert ten minste eenmaal per jaar de toereikendheid van toegangsrechten op kritieke netwerkelementen of actualiseert ze onverwijld in overeenstemming met wijzigingen in de organisatie of aan de kant van derdelijns ondersteuningsdienstverleners.

(5) De exploitant voorkomt zijn afhankelijkheid van een individuele leverancier of dienstverlener op het derde niveau (d.w.z. "insluitingseffect"), indien dit technisch haalbaar en economisch duurzaam is, met als doel afhankelijkheid te verkleinen en veerkracht te vergroten in geval van kritieke kwetsbaarheden van onderdelen, onder meer door langetermijncontracten met individuele fabrikanten of leveranciers of aanbieders van ondersteuningsdiensten op het derde niveau te vermijden, of door deze te wijzigen met als

doel verstoringen in de dienstverlening aan kritieke entiteiten tot het laagst mogelijke niveau te beperken.

Artikel 7
(Contractuele voorwaarden met fabrikanten, leveranciers of ondersteuningsdienstverleners op het derde niveau)

Om een hoog beveiligingsniveau te waarborgen, neemt de exploitant ten minste het volgende op in nieuwe contractuele voorwaarden met fabrikanten, leveranciers of ondersteuningsdienstverleners op het derde niveau:

1. een verklaring van de fabrikant of de leverancier dat het onderdeel of de standaardinstellingen ervan geen ongedocumenteerde achterdeuren of negatieve gevolgen voor de exploitatie van kritieke entiteiten hebben;
2. een verbintenis van de fabrikant, de leverancier of de dienstverlener op het derde niveau ter bescherming van de gegevens waarmee hij kennismaakt tijdens het verlenen van diensten of de toegang daartoe in verband met de verlening van de toegangsdienst;
3. een verbintenis van de fabrikant, de leverancier of de dienstverlener op het derde niveau om de exploitant onmiddellijk in kennis te stellen van schendingen van de bescherming van communicatiegegevens of verkeersgegevens die de exploitant of de kritieke entiteiten als bedoeld in artikel 1, punt 1, van deze algemene wet beïnvloeden of kunnen beïnvloeden;
4. een verbintenis van de fabrikant, de leverancier of de dienstverlener op het derde niveau om de exploitant onmiddellijk in kennis te stellen van beveiligingsincidenten en kwetsbaarheden die van invloed kunnen zijn op de beveiliging van het netwerk, de bijbehorende diensten of gegevens van de exploitant;
5. een verbintenis van de fabrikant, de leverancier of de dienstverlener op het derde niveau om de door de exploitant vastgestelde beveiligingsnormen en -regels na te leven en passende beveiligingsmaatregelen te nemen om de beveiliging van informatiesystemen en -netwerken en de gegevens van de exploitant of kritieke entiteit te waarborgen;
6. het vermogen van de exploitant om de omgevingen, procedures, beveiligingsmaatregelen en hulpmiddelen die door de ondersteuningsdienstverlener op het derde niveau worden gebruikt, te allen tijde te beoordelen tijdens toegang tot het netwerk en de gegevens van de exploitant;
7. de verantwoordelijkheid van de fabrikant, de leverancier of de ondersteuningsdiensverlener op het derde niveau voor schade die zou worden veroorzaakt door vastgestelde kwetsbaarheden of misbruik van onderdelen van kritieke netwerkelementen, de standaardinstelling ervan of tijdens de levering van ondersteuningsdiensten op het derde niveau die de fabrikant of de leverancier of derdelijns ondersteuningsverlener heeft verwaarloosd of opzettelijk geïmplementeerd;
8. een verplichting om het personeel van de fabrikant of leverancier of derdelijns ondersteuningsdienstverlener regelmatig te trainen op het gebied van gegevensbeveiligings- en informatiesystemen en -netwerken.

Artikel 8
(Regels met betrekking tot de toegang tot en het gebruik van kritieke netwerkelementen)

(1) Bij fysieke of logische toegang tot de onderdelen van kritieke netwerkelementen, hun instellingen en de daarin opgeslagen, verwerkte of gewijzigde gegevens van de exploitant, zorgt de exploitant ervoor dat:

1. de toegang strikt wordt beperkt tot personen die daarvoor eerder toestemming hebben gekregen;
2. alle werkzaamheden aan kritieke netwerkelementen die ter plaatse of via toegang op afstand worden uitgevoerd, door de exploitant worden beheerd;
3. multifactorverificatie wordt uitgevoerd voor gebruikers aan wie de hoogste privileges of rechten zijn toegekend om toegang te krijgen tot afzonderlijke onderdelen van kritieke netwerkelementen, hun instellingen of de daar opgeslagen of verwerkte gegevens;
4. elke gemachtigde persoon aan wie toegang wordt verleend, een uniek gebruikersaccount en wachtwoord heeft;
5. alleen wachtwoorden die regelmatig of onmiddellijk worden gewijzigd in geval van gedetecteerd misbruik en ten minste 15 tekens bevatten, evenals hoofd- en kleine letters, cijfers en speciale tekens, indien de software dit toestaat, worden gebruikt;
6. het concept van nultolerantie of vertrouwen zo mogelijk wordt geïmplementeerd bij toegang;
7. de beveiliging van de communicatieverbinding van de geautoriseerde gebruiker naar de afzonderlijke onderdelen wordt beschermd door het gebruik van versleuteling, rekening houdend met de nieuwste technologische ontwikkelingen en de beste industriële goede praktijken op het gebied van informatiebeveiliging, of aanbevolen door gevestigde instellingen op het gebied van informatiebeveiliging;
8. er een onuitwisbare registratie van toegangen en toegangspogingen wordt uitgevoerd, die ten minste 6 maanden wordt bewaard, met inbegrip van een back-upexemplaar, maar ook voor een langere periode, wanneer uit de analyse van het risicobeheer en de beoordeling van aanvaardbare risiconiveaus blijkt dat de risico's voldoende dienenb te worden beheerd door de logboeken voor een langere periode bij te houden;
9. waar mogelijk alle softwareinterventies op onderdelen worden geregistreerd en gemonitord, met inbegrip van configuratiewijzigingen. Registers, met inbegrip van een back-up van deze gegevens, worden net zo lang bewaard als in het vorige punt is aangegeven;
10. de toegang tot afzonderlijke onderdelen en tot de daarop opgeslagen of verwerkte gegevens wordt beperkt en is alleen toegankelijk voor de duur van de noodzakelijke werkzaamheden.

(2) In het geval van toegang tot individuele onderdelen van kritieke netwerkelementen door personeel of werknemers van een derdelijns ondersteuningsdienstverlener dienen zij:

1. uitsluitend een beveiligd tussentijds speciaal werkstation ("jumpserver") te gebruiken, dat regelmatig aan beveiligingscontroles wordt onderworpen;
2. de absoluut noodzakelijke hulpmiddelen, onderdelen en actieve diensten voor toegang tot andere hulpbronnen op het netwerk die absoluut noodzakelijk zijn en dienen te worden bijgewerkt met de nieuwste beveiligingspatches, uitsluitend te installeren op een speciaal werkstation;
3. veilige cryptografische bewerkingen en sleutels te gebruiken op een speciaal werkstation, dat zich in het netwerk van de exploitant bevindt en onder zijn exclusieve zeggenschap valt;
4. te zorgen dat elke toegang handmatig wordt goedgekeurd en geactiveerd door de exploitant en alleen voor de duur van de toegang;

5. te zorgen dat alle toegangen en activiteiten fysiek worden gecontroleerd en geregistreerd door de exploitant;
6. verificatie met twee factoren te gebruiken, evenals wachtwoorden met een lengte van ten minste 15 tekens en met hoofd- en kleine letters, cijfers en speciale tekens, die dienen te worden gewijzigd op basis van beoordeelde risico's.

(3) Voordat de exploitant de dienst voor het beheer, het onderhoud of de actualisering van kritieke netwerkelementen of hun afzonderlijke onderdelen aan een derde overdraagt, verifieert en zorgt hij ervoor dat hij ten minste over dezelfde of betere beveiligingsmechanismen en beveiligingsbeheerprocessen beschikt in vergelijking met zijn mechanismen en processen. Hij stelt de betrokken kritieke entiteit, het Agentschap en het voor de informatiebeveiliging verantwoordelijke orgaan onmiddellijk in kennis van het voornemen tot overdracht.

(4) De exploitant verifieert de werkelijke stand van de beveiligingsprocessen vóór het begin van de dienstverlening en daarna ten minste eenmaal per jaar. De exploitant houdt registers bij van interne beoordelingen en controles op de verlening van ondersteuningsdiensten van derden en bewaart deze gedurende de duur van de verlening van de diensten en gedurende één jaar na de beëindiging ervan, maar niet langer dan vijf jaar.

OVERGANGS- EN SLOTBEPALINGEN

Artikel 9
(Overgangsbepalingen)

(1) De exploitant stelt het Agentschap en het orgaan dat verantwoordelijk is voor de informatiebeveiliging van de bestaande locaties van kritieke netwerkelementen binnen 30 dagen na de inwerkingtreding van deze algemene wet in kennis.

(2) De exploitant stelt het Agentschap en het orgaan dat verantwoordelijk is voor de informatiebeveiliging van de bestaande locaties van ondersteuningsdiensten op het derde niveau voor kritieke netwerkelementen binnen 30 dagen na de inwerkingtreding van deze algemene wet in kennis.

(3) Het Agentschap maakt vanaf de datum van inwerkingtreding de in artikel 3, lid 2, van deze algemene wet bedoelde documenten voor het eerst bekend.

Artikel 10
(Inwerkingtreding)

Deze algemene wet treedt in werking op de dertigste dag na de bekendmaking ervan in het Staatsblad van de Republiek Slovenië, waarbij exploitanten de apparatuur mogen gebruiken en de verlening van ondersteuningsdiensten op het derde niveau kunnen handhaven tot het verstrijken van de in artikel 312, leden 2 en 3, van de wet genoemde termijnen.

Nr _____

Ljubljana, op _____

EVA 2023-3150-0034

mag. Marko Mišmaš
directeur

VOORSTEL

Bijlage

Lijst van kritieke netwerkelementen en bijbehorende informatiesystemen:

kritieke netwerkelementen	**Functionaliteiten van de netwerk- en informatiesystemen**
Beheer van abonnees en versleutelingsmechanismen;	- Sessiebeheer (spraak en gegevens); - Verificatie van gebruikers en apparatuur met het netwerk; - Beheer en opslag van sleutels voor autorisatie van abonnees en netwerkonderdelen (UICC/eUICC, digitale certificaten/HSM); - Functies voor veilige verificatie, bescherming van communicatie-integriteit (versleuteling) en opslag van gebruikerssleutels, netwerk- en beheeronderdelen; - Beheer van toegangsrechten;
Interconnectie;	- Hostingfuncties en interfaces met andere netwerken en diensten;
Beheerde netwerkdiensten;	- Registratie en autorisatie van netwerkdiensten; - Opslag en verwerking van communicatie-, locatie- en verkeersgegevens; - Blootstelling van netwerken en netwerkfuncties aan externe toepassingen en diensten;
Beheer en orkestratie van gevirtualiseerde netwerkfuncties (NFV) en netwerkorkestratie (MANO), inclusief virtualisatie-infrastructuur;	- Beheerfuncties van orkestratie en configuratie van NFV, ongeacht het type implementatie (VM, container, microservices); - Virtualisatiefuncties voor de implementatie en het gebruik van NFV; - Selectiefunctie voor netwerkslicing (NSSF);
Radiotoegangsnetwerk;	- Basisstations die 5G-technologie of hoger ondersteunen;
Beheersystemen en andere ondersteuningssystemen;	- Monitoring van de exploitatie en het beheer van het mobiele-communicatienetwerk, met inbegrip van het toegangsgedeelte (RAN/O-RAN); - Systemen voor het detecteren van beveiligingsgebeurtenissen, anomalieën, bedreigingen en het beheer daarvan (beveiligingsfuncties waaronder SIEM/SOAR);
Wettelijke onderschepping;	- Toegangsfuncties tot de communicatie-inhoud en gegevens over gebruikersverkeer door de bevoegde autoriteit.