PASIŪLYMAS

Pagal Elektroninių ryšių įstatymo (UL RS Nr. 130/22 ir 18/23 – ZDU-1O) 116 straipsnio 6 dalį Slovėnijos Respublikos ryšių tinklų ir paslaugų agentūra, atsižvelgdama į informavimo procedūrą pagal 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos direktyvą (ES) 2015/1535, kuria nustatoma informacijos apie techninius reglamentus ir informacinės visuomenės paslaugų taisykles teikimo tvarka (OL L 241, 2015 9 17, p. 1), pateikia:

BENDRASIS ĮSTATYMAS,
dėl papildomų saugumo reikalavimų ir apribojimų

1 straipsnis
(Bendrojo akto turinys)

Šiame bendrajame teisės akte numatoma:

1. gairės, kurių turi laikytis judriojo ryšio tinklų operatoriai (toliau – operatoriai), teikiantys šiuos tinklus ypatingos svarbos subjektams, kurie yra ypatingos svarbos infrastruktūros objektų kitų ypatingos svarbos infrastruktūros reguliavimo sričių valdytojai, kaip nustatyta ypatingos svarbos infrastruktūros objektų sritį reglamentuojančiuose įstatymuose (toliau – ypatingos svarbos infrastruktūros valdytojai), esminių paslaugų teikėjai, kaip nustatyta teisės aktuose, reglamentuojančiuose informacijos saugumą (toliau – esminių paslaugų teikėjai), valstybės administravimo įstaigos, kaip nustatyta Informacijos saugumą reglamentuojančiame įstatyme (toliau – valstybės administravimo įstaigos), arba šalies saugumo sistemos pagrindinių dalių vežėjai; ir
2. svarbiausi tinklo ir susijusių informacinių sistemų elementai su jų funkcijomis, nurodytomis Elektroninių ryšių įstatymo (UL RS Nr. 130/22 ir 18/23 – ZDU-1O) 116 straipsnio 6 dalyje; toliau – Aktas), kaip nurodyta priede, kuris yra neatskiriama šio bendrojo akto dalis ir yra parengtas bendradarbiaujant su už informacijos saugumą atsakinga institucija.

2 straipsnis
(Terminų reikšmė)

(1) Šiame bendrajame akte vartojami terminai reiškia:

1. Tiekimo grandinė – visa procesų, žmonių, organizacijų ir paskirstymo sistema, susijusi su projektavimu, gamyba, laikymu, paskirstymu ir tiekimu, taip pat su operatoriaus tinkle arba tokias paslaugas operatoriui teikiančiu debesijos paslaugų teikėju įrengtų ypatingos svarbos tinklo elementų komponentų montavimu ir priežiūra.

2. Svarbiausi tinklo elementai yra tie tinklo elementai, funkcijos, paslaugos ir pagalbinės informacinės sistemos fizine, programine ar virtualia forma operatoriui arba debesijos paslaugų teikėjui, kurie yra išvardyti šio bendrojo akto priede.

3. Ypatingos svarbos subjektai yra ypatingos svarbos infrastruktūros valdytojai kitose ypatingos svarbos infrastruktūros reguliavimo srityse, nustatytose pagal ypatingos svarbos infrastruktūros sritį reglamentuojančius teisės aktus, esminių paslaugų

teikėjai, kaip nustatyta informacijos saugumą reglamentuojančiame įstatyme, valstybės administravimo įstaigos, kaip nustatyta informacijos saugumą reglamentuojančiame įstatyme, ir pagrindinių šalies saugumo sistemos dalių vežėjai.

(2) Kitos šiame bendrajame akte vartojamos sąvokos turi tą pačią reikšmę, kaip apibrėžta Įstatyme ir Bendrajame įstatyme dėl tinklų, paslaugų ir duomenų saugumo.

3 straipsnis
Bendrosios gairės

(1) Ypatingos svarbos tinklo elementų komponentų tiekimo grandinės operatoriai ir šių komponentų trečiojo lygio paramos paslaugos per visą šių komponentų gyvavimo ciklą atsižvelgia bent į šias gaires:

1. Individualaus gamintojo ar tiekėjo ir trečiojo lygio paramos paslaugų teikėjo dėl santykių ir susitarimų su jais atveju, jie atlieka rizikos vertinimą, susijusį su trečiųjų šalių fizinių ar juridinių asmenų tiekimu ir galimu poveikiu pagal viešąją ar privatinę teisę (toliau – trečiosios šalys), suderinamumu su kitų gamintojų įranga, produktų kokybe ir sauga bei galimu neigiamu poveikiu operatoriaus paslaugų ir ypatingos svarbos subjektų veiklai;
2. kad saugumas būtų integruotas ir įgyvendintas jau projektuojant ir kad sutartyse būtų numatyti terminai, iki kurių turi būti pašalintas nustatytas pažeidžiamumas;
3. kad pagrindinės saugumo priemonės (prieinamumas, konfidencialumas, vientisumas ir autentiškumas) būtų užtikrinamos per visą jų naudojimo laikotarpį,
4. kad būtų užtikrintas saugumas ir nenutrūkstamas jų tiekimas, ir patvirtinama, kad palaikomos aukštos saugumo savybės, atitinkančios tarptautiniu mastu pripažintus standartus (3GPP) ir Europos techninius standartus (ETSI);
5. kad šios dalies 2–4 punktuose nurodytas gaires galima patikrinti sutarties su gamintoju arba tiekėju dokumentuose;
6. taip pat įvertinama kiekvieno gamintojo ar tiekėjo rizika, susijusi su pagrindinių technologijų, kurios yra būtinos įrangai gaminti ir naudoti, naudojimo teisėmis, ir rizika, susijusi su įrangos, atsarginių dalių ar trečiojo lygio pagalbinių paslaugų tiekimu, ir į ją atsižvelgiama;
7. kad naudojami komponentai neturi neišspręstų žinomų svarbių ar aktyviai išnaudojamų pažeidžiamumo problemų;
8. vengti vieno gamintojo ar tiekėjo, kai tai techniškai įmanoma ir ekonomiškai tvaru, siekiant sumažinti priklausomybę ir padidinti atsparumą ypatingos svarbos komponentų pažeidžiamumo, katastrofiško tinklo gedimo arba grėsmės ypatingos svarbos subjektų tinklų ir paslaugų saugumui, kurią vykdo viešosios arba privatinės teisės reglamentuojami tretieji fiziniai ar juridiniai asmenys, atveju.

(2) Teikdami informaciją ir ryšių įrangą, sistemas ir paslaugas, operatoriai, pirkdami saugius IRT produktus ir paslaugas, visiškai laikosi Europos Sąjungos kibernetinio saugumo agentūros (toliau – ENISA) gairių ir galiojančių Europos Sąjungos reglamentų dėl pagrindinių saugumo reikalavimų. Agentūra savo interneto svetainėje skelbia nuorodas į dabartinius ENISA dokumentus ir pirmiau minėtos srities ES reglamentus ir nuolat juos atnaujina.

(3) Teikiant ypatingos svarbos tinklo elementų komponentus arba naudojantis debesijos paslaugomis, pirmenybė teikiama komponentų pasirinkimui iš tų gamintojų, tiekėjų ar paslaugų iš debesijos paslaugų teikėjų, kurie yra sertifikuoti atitikties vertinimo įstaigų, kurios yra akredituotos ir, jei reikia, kurioms pagal 2019 m. balandžio 17 d. Europos Parlamento ir

Tarybos reglamento (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (toliau – Reglamentas), 60 straipsnio 3 dalį suteikė leidimą išduoti Europos kibernetinio saugumo sertifikatus tam tikru saugumo lygiu, kaip nustatyta reglamento 52 straipsnyje.

(4) Ankstesnės dalies tikslais operatorius patikrina pagal reglamento 55 straipsnį ENISA sukurtą specialią interneto svetainę, skirtą visuomenei informuoti apie Europos kibernetinio saugumo sertifikavimo schemas, Europos kibernetinio saugumo sertifikatus ir ES atitikties deklaracijas, įskaitant informaciją apie nebegaliojančias arba atšauktas ir nebegaliojančias Europos kibernetinio saugumo sertifikavimo schemas ir ES atitikties deklaracijas, taip pat nuorodų į kibernetinio saugumo informaciją saugyklą.

4 straipsnis.
Rizikos vertinimas

(1) Nustatydamas komponentų gamintojo ar tiekėjo ir trečiojo lygio paslaugų teikėjo riziką, susijusią su ypatingos svarbos tinklo elementais, operatorius atsižvelgia į šiuos rizikos aspektus, kuriuos jis vertina.

(2) Atlikdamas pirmesnėje dalyje nurodytą vertinimą, operatorius įvertina ir atsižvelgia bent į:

1. bendrą kokybę (įskaitant saugos aspektus) ir patikimumą;
2. atvirų standartų ir sąsajų, kuriomis užkertamas kelias priklausomybei nuo konkretaus gamintojo ar tiekėjo produktų ir susaistymo su jais, naudojimo lygį;
3. atitiktį pripažintiems tarptautiniams ir Europos techniniams standartams (3GPP, ETSI) ir Europos Sąjungos taisyklėms bei numatytoms saugumo nuostatoms pagal profesines rekomendacijas (GSMA asociacija);
4. suderinamumo su trečiosios šalies įranga ir tinklo funkcijomis lygį;
5. gebėjimą teikti atnaujinimus ir pritaikymus;
6. pažeidžiamumo valdymo procesą, jo atskleidimą ir naujausią procesą su atnaujinimais ir pataisymais;
7. dokumentų prieinamumą ir skaidrumą, susijusį su:
   - pagrindinėmis funkcijomis ir informacija apie komponento saugumą ir kitomis funkcijomis bei galimais nustatymais ir
   - naudojama programine įranga, įskaitant atvirojo kodo kodą (medžiagų važtaraštis – SBOM);
8. priklausomumo nuo trečiojo lygmens pagalbinių paslaugų lygį valdant ir prižiūrint įrangą, jei operatorius šias paslaugas teikia ne vienas su savo darbuotojais;
9. preliminarų įrangos arba subjekto, kuris pagal Europos kibernetinio saugumo sertifikavimo schemas akredituotų Europos Sąjungoje akredituotų įstaigų trečiojo lygio paramos paslaugą, atitikties vertinimą pagal kurį akredituotos įstaigos skelbiamos Europos Sąjungos oficialiajame leidinyje.

(3) Operatorius dokumentuoja kiekvieno atrinkto gamintojo, tiekėjo ar trečiojo lygio paslaugų teikėjo, nurodyto šio straipsnio 2 ir 3 dalyse, rizikos veiksnius ir rizikos vertinimo rezultatus ir reguliariai juos atnaujina.

5 straipsnis
(Ypatingos svarbos tinklo elementų veikimo bendrosios gairės)

(1) Ypatingos svarbos tinklo elementų komponentai, jų veikimas ir numatytieji nustatymai neturi turėti techninių charakteristikų, kurios galėtų neigiamai paveikti ypatingos svarbos subjektų saugumą ar veikimą, *inter alia*, dėl sabotažo, šnipinėjimo, intelektinės nuosavybės vagystės ar terorizmo.

(2) Svarbiausi tinklo elementai paprastai yra Slovėnijos Respublikoje arba, atsižvelgiant į visą saugumo riziką ir užtikrinant aukšto lygio saugumo priemones, ir, jei tai nenumatyta taikomuose reglamentuose, Europos Sąjungoje. Operatorius ne vėliau kaip prieš 30 dienų iki perkėlimo už Europos Sąjungos ribų informuoja Slovėnijos Respublikos ryšių tinklų ir paslaugų agentūrą (toliau – Agentūra) ir už informacijos saugumą atsakingą įstaigą apie numatomą jų perkėlimą.

(3) Trečiojo lygio paramos paslaugos, skirtos svarbiausiems tinklo elementams, paprastai teikiamos Slovėnijos Respublikoje arba, atsižvelgiant į visą saugumo riziką ir užtikrinant aukšto lygio saugumo priemones, ir, jei tai nenumatyta taikomuose reglamentuose, Europos Sąjungoje. Operatorius praneša Agentūrai ir už informacijos saugumą atsakingai įstaigai apie numatomą savo trečiojo lygio paramos paslaugų perkėlimą ne vėliau kaip prieš 30 dienų iki perkėlimo iš Europos Sąjungos šalių.

(4) Trečiojo lygio paramos paslaugų įgyvendinimas neturi kelti pavojaus ypatingos svarbos subjektų saugumui ar paslaugų teikimui ar nacionaliniam saugumui.

(5) Operatorius nustato ir reguliariai įgyvendina ypatingos svarbos tinklo elementų nustatymo procesą. Tai turi būti atliekama bent kartą per metus arba perkant ypatingos svarbos tinklo elementų komponentus.

(6) Jei atskiras komponentas tik iš dalies atitinka ypatingos svarbos tinklo elementą, jis laikomas ypatingos svarbos tinklo elemento dalimi.

(7) Operatorius nuolat atnaujina visų ypatingos svarbos tinklo elementų komponentų, jų funkcijų, vietų, administratorių ir valdytojų, jų trečiojo lygmens pagalbinių paslaugų teikėjų ir jų gamintojų ar tiekėjų sąrašą. Gavus prašymą, sąrašas pateikiamas Agentūrai ir už informacijos saugumą atsakingai įstaigai.

6 straipsnis
(Ypatingos svarbos tinklo elementų komponentų tiekimo saugumo priemonės)

(1) Operatorius turi išmanyti visą tiekimo grandinę ir su ja susijusią riziką, įskaitant ypatingos svarbos tinklo elementų atskirų komponentų subrangovus, kurie taip pat apima šifravimo raktus, UICC/eUICC ir kitus saugumo elementus, kuriais piktnaudžiaujant galėtų kilti pavojus ypatingos svarbos subjektų saugumui.

(2) Operatorius užtikrina, kad operatoriaus ir ypatingos svarbos tinklo elementų komponentų gamintojų ar tiekėjų arba jo trečiojo lygio pagalbinių paslaugų teikėjų saugumo reikalavimai būtų sutarti sutartimi ir dokumentuoti, ir reikalauja, kad gamintojai ar tiekėjai laikytųsi sutartų saugumo priemonių visoje tiekimo grandinėje.

(3) Siekdamas užkirsti kelią piktavališkiems subjektams laiku naudotis pažeidžiamumu, operatorius užtikrina, kad ypatingos svarbos tinklo elemento komponentų gamintojas ar tiekėjas sutartimi įsipareigotų nedelsiant informuoti operatorių apie nustatytą pažeidžiamumą ir apie rizikos mažinimo priemones bei patarti dėl apsaugos ar taisomųjų priemonių, kurių operatorius gali imtis reaguodamas į grėsmę.

(4) Operatorius bent kartą per metus patikrina prieigos prie ypatingos svarbos tinklo elementų teisių tinkamumą arba nedelsdamas jas atnaujina, atsižvelgdamas į organizacijos arba trečiojo lygmens pagalbinių paslaugų teikėjų pokyčius.

(5) Operatorius užkerta kelią savo priklausomybei nuo atskiro tiekėjo arba trečiojo lygmens paslaugų teikėjo (t. y. pardavėjo susaistymo), kai tai techniškai įmanoma ir ekonomiškai tvaru, siekiant sumažinti priklausomybę ir padidinti atsparumą ypatingos svarbos komponentų pažeidžiamumo atveju, taip pat vengiant ilgalaikių sutarčių su atskirais gamintojais, tiekėjais ar trečiojo lygmens paramos paslaugų teikėjais arba galimybe jas pakeisti, siekiant kuo labiau sumažinti paslaugų teikimo ypatingos svarbos subjektams sutrikimus.

7 straipsnis
(Su gamintojais, tiekėjais arba trečiojo lygio paramos paslaugų teikėjais sudarytos sutartinės sąlygos)

Siekdamas užtikrinti aukštą saugumo lygį, operatorius į naujas sutarčių su gamintojais, tiekėjais ar trečiojo lygio paramos paslaugų teikėjais sąlygas įtraukia bent šiuos dalykus:

1. gamintojo arba tiekėjo pareiškimą, kad komponentas arba jo numatytieji nustatymai neturi dokumentuose neminimų apėjimų arba jokio neigiamo poveikio ypatingos svarbos subjektų veiklai;
2. gamintojo, tiekėjo arba trečiojo lygio paslaugų teikėjo įsipareigojimą apsaugoti duomenis, su kuriais jie susipažino teikiant paslaugas arba prieigą prie jų teikiant prieigos paslaugą;
3. gamintojo, tiekėjo arba trečiojo lygio paslaugų teikėjo įsipareigojimą nedelsiant informuoti operatorių apie ryšių duomenų arba srauto duomenų apsaugos pažeidimus, kurie daro arba gali daryti poveikį operatoriui arba ypatingos svarbos subjektams, nurodytiems 1 straipsnio 1 punkte, apie šį bendrąjį aktą;
4. gamintojo, tiekėjo arba trečiojo lygio paslaugų teikėjo įsipareigojimą nedelsiant pranešti operatoriui apie visus saugumo incidentus ir pažeidžiamumą, kurie galėtų turėti įtakos tinklo saugumui, susijusioms paslaugoms ar operatoriaus duomenims;
5. gamintojo, tiekėjo arba trečiojo lygio paslaugų teikėjo įsipareigojimą laikytis operatoriaus nustatytų saugumo standartų ir taisyklių ir imtis tinkamų saugumo priemonių informacinių sistemų ir tinklų bei operatoriaus arba ypatingos svarbos subjekto duomenų saugumui užtikrinti;
6. operatoriaus gebėjimą bet kuriuo metu peržiūrėti aplinką, procedūras, saugumo priemones ir priemones, kurias naudoja trečiojo lygio paramos paslaugų teikėjas, naudodamas prieigą prie operatoriaus tinklo ir duomenų;
7. gamintojo, tiekėjo arba trečiojo lygmens paramos paslaugų teikėjo atsakomybę už žalą, kuri būtų padaryta dėl nustatytų pažeidžiamumo arba netinkamo ypatingos svarbos tinklo elementų komponentų naudojimo, jų numatytųjų nustatymų arba

teikiant trečiojo lygio paramos paslaugas, kurių gamintojas, tiekėjas ar trečiojo lygmens paramos teikėjas nepaisė arba sąmoningai įgyvendino;

8. įpareigojimą reguliariai mokyti gamintojo, tiekėjo arba trečiojo lygio pagalbinių paslaugų teikėjo darbuotojus duomenų saugumo ir informacinių sistemų bei tinklų srityje.

8 straipsnis
(Prieigos prie ypatingos svarbos tinklo elementų ir jų naudojimo taisyklės)

(1) Fiziškai ar logiškai prisijungdamas prie ypatingos svarbos tinklo elementų komponentų, jų nustatymų ir juose saugomų, tvarkomų ar modifikuotų operatoriaus duomenų, operatorius užtikrina, kad:

1. prieiga suteikiama tik asmenims, kuriems anksčiau buvo suteiktas leidimas;
2. visus su ypatingos svarbos tinklo elementais susijusius darbus, atliekamus vietoje arba naudojantis nuotoline prieiga, kontroliuoja operatorius;
3. kelių veiksnių autentifikavimas atliekamas naudotojams, kuriems suteikiamos didžiausios teisės naudotis atskirais ypatingos svarbos tinklo elementų komponentais, jų nustatymais arba ten saugomais ar tvarkomais duomenimis;
4. kiekvienas įgaliotas asmuo, kuriam suteikiama prieiga, turi unikalią vartotojo paskyrą ir slaptažodį;
5. naudojami tik tie slaptažodžiai, kurie reguliariai arba nedelsiant keičiami nustačius netinkamą naudojimą ir kuriuos sudaro ne mažiau kaip 15 ženklų, įskaitant didžiąsias ir mažąsias raides, skaičius ir specialius simbolius, jei tai leidžia programinė įranga;
6. jei įmanoma, įgyvendinama visiško netoleravimo arba pasitikėjimo koncepcija prieigos srityje;
7. įgaliotojo naudotojo ryšio su atskirais komponentais saugumas būtų apsaugotas naudojant šifravimą, atsižvelgiant į naujausius technologinius pokyčius ir geriausią pramonės gerąją patirtį informacijos saugumo srityje, arba kaip rekomenduoja įsteigtos institucijos informacijos saugumo srityje;
8. būtų atliekamas neištrinamas prieigos ir bandymų prieiti įrašas, saugomas ne trumpiau kaip 6 mėnesius, įskaitant atsarginę kopiją, bet taip pat galimai ilgiau, jei iš rizikos valdymo analizės ir priimtino rizikos lygio vertinimo matyti, kad rizika turėtų būti tinkamai suvaldoma laikant ilgesnio laikotarpio įrašų žurnalus;
9. jei įmanoma, būtų registruojamos ir stebimos visos su komponentais susijusios programinės įrangos priemonės, įskaitant konfigūracijos pakeitimus. Įrašai, įskaitant šių duomenų atsarginę kopiją, saugomi tiek, kiek nurodyta ankstesniame punkte;
10. prieiga prie atskirų komponentų ir juose saugomų ar tvarkomų duomenų yra ribota ir atvira tik reikiamam darbui.

(2) Tuo atveju, kai trečiojo lygio paramos paslaugų teikėjo darbuotojai arba darbuotojai turi prieigą prie atskirų ypatingos svarbos tinklo elementų komponentų, jie:

1. naudoja tik saugią tarpinę specialią darbo vietą („jump server“), kuri turi būti reguliariai tikrinama;
2. specialioje darbo vietoje įdiegia tik absoliučiai būtinus įrankius, komponentus ir aktyvias paslaugas, kad būtų galima pasiekti kitus tinklo išteklius, kurie yra būtini ir turi būti atnaujinti naujausiais saugumo pataisymais;
3. naudoja saugias kriptografines operacijas ir raktus specialioje darbo vietoje, kuri turi būti operatoriaus tinkle ir kurią jis išimtinai kontroliuoja;

4. kiekvieną prieigą patvirtina ir rankiniu būdu aktyvuoja operatorius ir tik per prieigos laikotarpį;
5. operatorius fiziškai kontroliuoja ir registruoja visus prieigos ir veiklos būdus;
6. naudoja dviejų veiksnių autentifikavimą ir slaptažodžius, kurie yra ne trumpesni kaip 15 ženklų ir apima didžiąsias ir mažąsias raides, skaičius ir specialius simbolius, kurie keičiami atsižvelgiant į įvertintą riziką.

(3) Prieš perduodamas ypatingos svarbos tinklo elementų arba jų atskirų komponentų valdymo, priežiūros ar atnaujinimo paslaugą trečiajai šaliai, operatorius patikrina ir užtikrina, kad jo saugumo mechanizmai ir saugumo valdymo procesai būtų bent tokie patys arba geresni, palyginti su jo mechanizmais ir procesais. Apie ketinimą perduoti informaciją jis nedelsdama informuoja atitinkamą ypatingos svarbos subjektą, Agentūrą ir už informacijos saugumą atsakingą įstaigą.

(4) Operatorius patikrina faktinę saugumo procesų būklę prieš pradedant teikti paslaugas, o vėliau – bent kartą per metus. Operatorius saugo trečiųjų šalių paramos paslaugų teikimo vidaus peržiūrų ir kontrolės įrašus ir saugo juos paslaugų teikimo laikotarpiu ir vienerius metus po jų nutraukimo, bet ne ilgiau kaip penkerius metus.

PEREINAMOJO LAIKOTARPIO IR BAIGIAMOJI NUOSTATA

9 straipsnis
(Pereinamojo laikotarpio nuostatos)

(1) Operatorius praneša Agentūrai ir už informacijos saugumą atsakingai įstaigai apie esamas ypatingos svarbos tinklo elementų vietas per 30 dienų nuo šio bendrojo akto įsigaliojimo.

(2) Operatorius per 30 dienų nuo šio bendrojo akto įsigaliojimo praneša Agentūrai ir už informacijos saugumą atsakingai įstaigai apie esamas trečiojo lygio pagalbinių paslaugų, susijusių su ypatingos svarbos tinklo elementais, vietas.

(3) Agentūra pirmą kartą paskelbia šio bendrojo akto 3 straipsnio 2 dalyje nurodytus dokumentus nuo jo įsigaliojimo dienos.

PASIŪLYMAS

10 straipsnis
(Įsigaliojimas)

Šis bendrasis aktas įsigalioja trisdešimtą dieną po jo paskelbimo Slovėnijos Respublikos oficialiajame leidinyje, pagal kurį operatoriai gali naudotis įranga ir toliau teikti trečiojo lygio paramos paslaugas iki Įstatymo 312 straipsnio 2 ir 3 dalyse nurodytų terminų pabaigos.

Nr. _____ mag. Marko Mišmaš

Liubliana, [data] _____ direktorius

EVA 2023-3150-0034

PASIŪLYMAS

Priedas

Svarbiausių tinklo elementų ir susijusių informacinių sistemų sąrašas:

Ypatingos svarbos tinklo elementai	**Tinklų ir informacinių sistemų funkcijos**
Abonento valdymo ir šifravimo mechanizmai	- Sesijos valdymas (balsas ir duomenys), - naudotojų ir įrangos tapatumo nustatymas tinkle, - abonentų ir tinklo komponentų leidimų išdavimo raktų valdymas ir saugojimas (UICC/eUICC, skaitmeniniai sertifikatai/HSM), - saugaus tapatumo nustatymo, ryšio vientisumo apsaugos (šifravimo) ir naudotojo raktų, tinklo ir valdymo komponentų saugojimo funkcijos, - prieigos teisių valdymas.
Sujungimas	- Prieglobos funkcijos ir sąsajos su kitais tinklais ir paslaugomis.
Valdomo tinklo paslaugos	- Tinklo paslaugų registravimas ir leidimų išdavimas, - ryšių, vietos ir srauto duomenų saugojimas ir tvarkymas, - tinklo ir tinklo funkcijų poveikis išorės taikomosioms programoms ir paslaugoms.
Virtualizuoto tinklo funkcijų (NFV) ir tinklo orkestravimo (MANO), įskaitant virtualizavimo infrastruktūrą, valdymas ir derinimas	- Valdymo funkcijos, susijusios su NFV orkestravimu ir konfigūracija, neatsižvelgiant į įgyvendinimo tipą (VM, konteineris, mikropaslaugos), - virtualizavimo funkcijos, skirtos NFV įgyvendinimui ir naudojimui, - Tinklo „Slice“ atrankos funkcija (NSSF)
Radijo prieigos tinklas	- Bazinės stotys, palaikančios 5G ar aukštesnę technologiją.
Valdymo sistemos ir kitos pagalbinės sistemos	- Judriojo ryšio tinklo, įskaitant prieigos dalį (RAN/O-RAN), veikimo ir valdymo stebėsena, - saugumo įvykių, anomalijų, grėsmių ir jų valdymo nustatymo sistemos (saugumo funkcijos, įskaitant SIEM/SOAR).
Teisinis perėmimas	- Kompetentingos institucijos prieigos prie ryšio turinio ir duomenų apie naudotojų srautą funkcijos.