REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE

Štefanova ulica 2, 1501 Ljubljana

T: 01 428 40 00
F: 01 428 47 33
E: gp.mnz@gov.si
www.mnz.gov.si

Številka: 381-1/2024/6
Ljubljana, 10. 5. 2024
EVA
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE Gp.gs@gov.si

ZADEVA: Predlog za ukinitev uporabe kriptirnega algoritma TEA1 v digitalnem radijskem omrežju TETRA do konca leta 2025

1. Predlog sklepov vlade:

Na podlagi šestega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14 in 55/17) je Vlada Republike Slovenije na .. seji dne …sprejela naslednji

SKLEP

Vlada Republike Slovenije se je seznanila s predlogom in razlogi za ukinitev uporabe kriptiranega algoritma TEA1 v digitalnem radijskem omrežju TETRA.

Številka:
V Ljubljani, dne

Barbara Kolenko Helbl
generalna sekretarka

Priloga:
- Sklep Vlade RS št. 38100-7/2015/8 z dne 8. 10. 2015

Prejmejo:
- državni organi
- uporabniki posebnega nacionalnega in varnostnega pomena
- Ministrstvo za notranje zadeve, Policija

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

/

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- Mag. Senad Jušić, generalni direktor policije
- Alen Vozelj mag. direktor Urada za informatiko in telekomunikacije

3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:

/

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

/

5. Kratek povzetek gradiva:

Vlada Republike Slovenije je na 55. redni seji (oktober 2015), potrdila izgradnjo in prenovo enotnega digitalnega radijskega omrežja TETRA po modelu GO-GO (država je lastnik sistema – država je operater in upravljavec sistema) Vlada je sprejela sklep, da bo digitalno radijsko omrežje TETRA del celotnega hibridnega sistema digitalnega radijskega omrežja državnih organov. Drugi del sistema se gradi s tehnologijo DMR in se vzpostavi za področje zaščite in reševanja ter za potrebe Ministrstva za zdravje.

MNZ – Policija je digitalno radijsko omrežje TETRA gradila v letu 2021 in 2022 ter ga tudi dokončala. V njem se lahko uporabljata dva kriptirna algoritma. Tako TEA1, kot tudi varnejši TEA2 s čimer je povezana uporaba terminalne opreme (radijske postaje) v omrežju.

Raziskava podjetja MidnightBlue (Nizozemska), katero je finančno podprla Evropska komisija, je avgusta 2023 objavilo ugotovitve o varnosti omrežja TETRA, ki so se osredotočile na ranljivost kriptirnega algoritma TEA1, ki ogroža komunikacijsko varnost.

Nekateri uporabniki digitalnega radijskega omrežja TETRA kriptirnega algoritma TEA2 še ne uporabljajo. Za prehod iz TEA1 na TEA2 kriptirni algoritem bodo potrebovali dovoljenje/licenco ter programsko nadgradnjo ali nakup nove terminalne opreme.

Glede na ugotovitve raziskave o varnostni pomanjkljivosti kriptirnega algoritma TEA1 pri prenosu govornih in podatkovnih komunikacij, predlagamo prehod na kriptirni algoritem TEA2 za vse uporabnike digitalnega radijskega omrežja TETRA.

6. Presoja posledic za:

a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	DA
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	NE
c)	administrativne posledice	NE
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	NE
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	NE
f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	NE

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:

Policija je že s pričetkom uporabe novega digitalnega radijskega omrežja TETRA začela uporabljati samo kriptirni algoritem TEA2, zato z ukinitvijo TEA1 ne bo imela stroškov.

Druga ministrstva oz. državni uporabniki iz seznama, morajo sami poskrbeti za morebitni nakup nove terminalne opreme ali pa za programsko nadgradnjo obstoječe terminalne opreme.

Ostali uporabniki sistema TETRA tudi sami poskrbijo za nakup nove terminalne opreme ali pa za programsko nadgradnjo obstoječe terminalne opreme. (Država nima finančnih posledic).

Vse sistemske nastavitve na digitalnem radijskem omrežju TETRA se bodo izvedle v okviru strokovne službe MNZ – Policije, ki upravljajo z digitalnim radijskim omrežjem TETRA.

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu				
	Tekoče leto (t)	t + 1	t + 2	t + 3
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva				

II. Finančne posledice za državni proračun				
II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				
II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:		
Novi prihodki	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ		

OBRAZLOŽITEV:

I. **Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu** /

II. Finančne posledice za državni proračun

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene: /

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo: /

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna: /

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR: / **Kratka obrazložitev: /**	
8. Predstavitev sodelovanja z združenji občin:	
Vsebina predloženega gradiva (predpisa) vpliva na: - pristojnosti občin, - delovanje občin, - financiranje občin.	NE
Gradivo (predpis) je bilo poslano v mnenje: – Skupnosti občin Slovenije SOS: NE – Združenju občin Slovenije ZOS: NE – Združenju mestnih občin Slovenije ZMOS: NE	
9. Predstavitev sodelovanja javnosti:	
Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	NE
Narava gradiva, glede na vsebino, ne predvideva sodelovanja javnosti.	
10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	DA
11. Gradivo je uvrščeno v delovni program vlade:	NE
Boštjan Poklukar **Minister**	

PREDLOG

Številka:
Datum:

Na podlagi šestega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14 in 55/17) je Vlada Republike Slovenije na .. seji dne …sprejela naslednji

SKLEP

Vlada Republike Slovenije se je seznanila s Predlogom in razlogi za ukinitev uporabe kriptiranega algoritma TEA1 v digitalnem radijskem omrežju TETRA.

Barbara Kolenko Helbl
generalna sekretarka

Priloga:
- - Sklep Vlade RS št. 38100-7/2015/8 z dne 08.10.2015

Prejmejo:
- državni organi
- uporabniki posebnega nacionalnega in varnostnega pomena
- Ministrstvo za notranje zadeve, Policija

OBRAZLOŽITEV:

Vlada Republike Slovenije se je na 55. redni seji dne 8. 10. 2015 pod točko 6. seznanila s stanjem obstoječih sistemov radijskih zvez državnih organov. Vlada Republike Slovenije je potrdila izgradnjo oziroma prenovo enotnega digitalnega radijskega omrežja TETRA po modelu GO-GO, »država je lastnik sistema – država je operater in upravljavec sistema«. Vlada RS je sprejela sklep, da je sistem TETRA del celotnega hibridnega sistema digitalnega radijskega omrežja državnih organov, ki se vzpostavi za Policijo, pravosodje, Finančno upravo Republike Slovenije, nekatere manjše državne in ostale uporabnike.

Drugi del hibridnega sistema digitalnega radijskega omrežja državnih organov se zgradi s tehnologijo DMR. Nosilec izvedbe drugega dela projekta je Ministrstvo za obrambo in se vzpostavi za področje zaščite in reševanja ter Ministrstva za zdravje. Po dokončanju obeh ločenih sistemov se ta med seboj povežeta v hibridni digitalni radijski sistem državnih organov.

MNZ – Policija je digitalno radijsko omrežje TETRA gradila v letu 2021 in 2022 ter ga tudi dokončala. Osemdeset baznih postaj v starem radijskem omrežju je bilo nadomeščenih s 150 novimi (pokritost ozemlja RS se je povečala). Bazne postaje vsebujejo več sprejemno-oddajnih modulov, kar uporabnikom omogoča večjo kapaciteto prenosa govornih in podatkovnih komunikacij, na vseh lokacijah je bilo zagotovljeno avtonomno napajanje za primer izpada električne energije (napajalniki z baterijami, kjer je avtonomija od 6 – 8 ur). Z vključevanjem zunanjih – nepolicijskih uporabnikov v novo digitalno radijsko omrežje TETRA smo pričeli v januarju 2022.

Novo omrežje TETRA uporabnikom omogoča komunikacijo s starim kriptirnim algoritmom TEA1 in novim kriptirnim algoritmom TEA2 zaradi višje zaščite prenosa govornih in podatkovnih komunikacij. Kriptirni algoritem TEA1 ostaja še naprej v uporabi za vse uporabnike, ki prehoda na novi algoritem TEA2 niso izkoristiti. Neposrednega povezovanja med uporabniki TEA1 in TEA2, novo omrežje TETRA ne omogoča.

Avgusta 2023 so raziskovalci podjetja za kibernetsko varnost MidnightBlue objavili svoje ugotovitve o varnosti omrežja TETRA. MidnightBlue je specializirano varnostno svetovalno podjetje, ki se ukvarja z varnostnimi raziskavami s posebnim poudarkom na vgrajenih sistemih na področjih, od kibernetskih fizičnih sistemov (CPS) do komunikacijske in varnostne opreme. Raziskava, ki jo je finančno podprla Evropska komisija, se je osredotočila na kriptirni algoritem TEA1, pri čemer je bila izpostavljena ranljivost »zmanjšanja« ključa, ki bi lahko ogrozila komunikacijsko varnost. Domnevne ranljivosti so bile odkrite s postopkom obratnega inženiringa in analize algoritmov TETRA Authentication Algorithm (TAA1) in TETRA Encryption Algorithm (TEA).

Standard TETRA[1] je leta 1995 standardiziral Evropski inštitut za telekomunikacijske standarde (ETSI), uporablja se v več kot 100 državah in je najbolj razširjen policijski radijski komunikacijski sistem zunaj ZDA, tako kot njegov severnoameriški analogni P25 in drugi standardi, kot sta DMR in TETRAPOL. TETRA se lahko uporablja za prenos govora in podatkov.

[1] *https://www.etsi.org/technologies/tetra*

Algoritem TEA1 je bil na zahtevo ETSI razvit v letih 1996/97 na Nizozemskem. Ker je algoritem tajen ni bil nikoli predložen v strokovni pregled ali poglobljeno varnostno analizo – je bila pa ta izvedena v sklopu ETSI organizacije oziroma njenih članov.

Algoritma TEA2 in TEA3 zaenkrat veljata za varna, medtem ko so bili algoritmi TEA5, TEA6 in TEA7, predstavljeni leta 2022, kot nadgradnja obstoječih z večjimi dolžinami ključev (192-bitna dolžina ključa). Predvideva se, da bodo novo predstavljeni enkripcijski algoritmi (TEA5, TEA6, TEA7) v bodoče lahko zamenjali obstoječe, če se izkažejo varnostne pomanjkljivosti tudi znotraj TEA2, TEA3 algoritma.

Policija že od samega začetka operativnega delovanja novega omrežja uporablja izključno TEA2 algoritem za komunikacijo med uporabniki.

Tabela: Seznam uporabnikov, ki uporabljajo omrežje TETRA

Uporabnik (državni uporabniki* in uporabniki posebnega nacionalnega in varnostnega pomena)**	**Kriptirni algoritem**
Urad vlade RS za oskrbo in integracijo migrantov* [2]	TEA1
Finančna uprava Republike Slovenije, Ministrstvo za finance*	TEA2
Ministrstvo za kulturo*	TEA1
Ministrstvo za obrambo*	TEA1+TEA2
Uprava za izvrševanje kazenskih sankcij, Ministrstvo za pravosodje*	TEA1
Univerzitetni klinični center Ljubljana*	TEA2
Slovenska obveščevalno varnostna agencija	TEA2
Ministrstvo za notranje zadeve, Policija*	TEA2
Medobčinski inšpektorat in redarstvo občin Bled, Bohinj in Železniki, Občina Bled**	TEA2
Mestno redarstvo, Mestna občina Ljubljana**	TEA1
Medobčinski inšpektorat in redarstvo Mestne občine Celje, Občine Braslovče, Občine Laško, Občine Polzela, Občine Štore, Občine Tabor, Občine Vransko in Občine Žalec, Mestna občina Celje**	TEA1
DARS, Družba za avtoceste v Republiki Sloveniji d.d. **	TEA2
Medobčinsko redarstvo, Mestna občina Kranj**	TEA2
Medobčinski inšpektorat in redarstvo občin Jesenice, Gorje, Kranjska Gora in Žirovnica, Občina Jesenice**	TEA2
Skupna občinska uprava Medobčinski inšpektorat in redarstvo občin Vrhnika, Brezovica, Dobrova – Polhov Gradec, Gorenja vas – Poljane, Žiri, Borovnica, Log – Dragomer in Horjul, Občina Vrhnika**	TEA1
Skupna občinska uprava občin Dolenjske in Bele krajine, Mestna občina Novo mesto**	TEA2
Medobčinsko redarstvo SOU občin Postojna, Cerknica, Pivka, Loška dolina in Bloke, Občina Postojna**	TEA2
Medobčinski inšpektorat in redarstvo občin Rogaška Slatina, Rogatec, Podčetrtek, Šmarje pri Jelšah in Kozje, Občina Rogaška Slatina**	TEA2

[2] *prehod na TEA2 že v postopku*

Vsi trenutni uporabniki, ki uporabljajo algoritem TEA1, bodo za prehod na uporabo TEA2 morali pri pristojnemu organu[3] pridobiti ustrezno dovoljenje/licenco za uporabo TEA2 ter programsko nadgraditi ali kupiti novo terminalno opremo. Uporabnik, ki bo pridobil licenco za uporabo TEA2, bo postal primarni uporabnik in bo lahko kupoval/nabavljal terminalno opremo po svoji izbiri (ob izpolnjevanju standardov TETRA) in z opremo prosto razpolagal.

Na podlagi ugotovitev podjetja MidnightBlue (Nizozemska) katere raziskavo je finančno podprla Evropska komisija, ugotavljamo, da uporaba terminalne opreme TETRA z vgrajenim kriptirnim algoritmom TEA1 za uporabnike ne zagotavlja nivo potrebne varnosti pri prenosu govornih in podatkovnih komunikacij.

Zato predlagamo prehod na kriptirni algoritem TEA2 za vse uporabnike omrežja TETRA v Republiki Sloveniji in sicer najkasneje do konca leta 2025.

[3] *The TETRA + Critical Communications Association, Chair of the Security and Fraud prevention Group (SFPG), Wildenborch 63, NL-2261 XK Leidschendam, The Netherlands,* <SFPG@TCCA.info>