dkom.si

REPUBLIKA SLOVENIJA
DRŽAVNA REVIZIJSKA KOMISIJA ZA REVIZIJO POSTOPKOV ODDAJE JAVNIH NAROČIL

Slovenska cesta 54
SI-1000 Ljubljana
T 01 234 28 00

dkom@dkom.si
www.dkom.si

Številka: 018-150/2024-9
Datum: 20. 1. 2025

SKLEP

Državna revizijska komisija za revizijo postopkov oddaje javnih naročil (v nadaljevanju: Državna revizijska komisija) je na podlagi 39. in 70. člena Zakona o pravnem varstvu v postopkih javnega naročanja (Uradni list RS, št. 43/2011, s spremembami; v nadaljevanju: ZPVPJN) v senatu Marka Medveda, kot predsednika senata, ter Igorja Luzarja in mag. Zlate Jerman, kot članov senata, v postopku pravnega varstva pri oddaji javnega naročila *»Zamenjava SŽ zaklepnega sistema z digitalnim zaklepnim sistemom«*, na podlagi zahtevka za revizijo, ki ga je vložila družba SOFRAN, trgovina in storitve, d.o.o., Kocenova ulica 2, Celje, ki jo zastopa odvetniška družba AZ ODVETNIKI o.p., d.o.o., Tivolska cesta 50, Ljubljana (v nadaljevanju: vlagatelj), zoper ravnanje naročnika Slovenske železnice - Infrastruktura, družba za upravljanje in vzdrževanje železniške infrastrukture ter vodenja železniškega prometa, d.o.o., Kolodvorska ulica 11, Ljubljana (v nadaljevanju: naročnik), dne 20. 1. 2025

odločila:

1. Zahtevku za revizijo se ugodi in se v celoti razveljavi postopek oddaje javnega naročila *»Zamenjava SŽ zaklepnega sistema z digitalnim zaklepnim sistemom«,* objavljen na Portalu javnih naročil 14. 10. 2024, pod številko objave JN007431/2024-SL3/01.

2. Naročnik je dolžan vlagatelju povrniti stroške pravnega varstva v višini 3.338,10 EUR v roku 15 dni od prejema tega sklepa, po izteku tega roka pa z zakonskimi zamudnimi obrestmi do plačila, pod izvršbo. Višja stroškovna zahteva vlagatelja se zavrne.

Obrazložitev:

Obvestilo o predmetnem javnem naročilu, ki ga naročnik oddaja po postopku naročila male vrednosti po 47. členu Zakona o javnem naročanju (Uradni list RS, št. 91/2015 s spremembami; v nadaljevanju: ZJN-3), je bilo objavljeno na Portalu javnih naročil 14. 10. 2024, pod št. objave JN007431/2024-SL3/01, s štirimi popravki.

Zoper razpisno dokumentacijo je vlagatelj 15. 11. 2024 vložil zahtevek za revizijo. Predlaga, naj se razpisna dokumentacija v spornih delih razveljavi oziroma naj se postopek oddaje predmetnega javnega naročila v celoti razveljavi. Poleg tega zahteva, da se razveljavijo vsa nadaljnja ravnanja naročnika, uveljavlja pa tudi povrnitev stroškov pravnega varstva.

Vlagatelj uvodoma navaja, da je naročnik v razpisni dokumentaciji v Obrazcu 11 (Splošne in tehnične zahteve), v točki 2 (Digitalni cilinder) zahteval od ponudnikov, da mora sistem omogočati avtonomno delovanje digitalnih cilindrov brez uporabe baterij ter da digitalni cilindri za delovanje ne smejo uporabljati zunanjih virov energije. Poleg tega je naročnik zahteval, da mora sistem omogočati odklepanje in zaklepanje digitalnih cilindrov preko mobilne naprave, ki podpira NFC komunikacijo. Vlagatelj zatrjuje, da navedene zahteve izpolnjujejo le proizvodi proizvajalca iLOQ oziroma istoimenski proizvodi iLOQ. Izključno pri proizvodih iLOQ za ključavnico/cilinder niso potrebne baterije, odklepajo pa se z mobilnimi telefoni s podporo NFC. V Republiki Sloveniji je le en pooblaščeni partner tega proizvajalca, ID Shop d.o.o., Ljubljana in tako le en ponudnik. Vlagatelj zatrjuje, da naročnik z navedenimi zahtevami neutemeljeno ne dovoljuje, da bi sistem omogočal odklepanje in zaklepanje digitalnih cilindrov prek mobilne naprave, ki podpira Bluetooth komunikacijo, med njimi izključuje tudi Bluetooth BLE. Vlagatelj pojasnjuje, da je NFC komunikacija tehnologija brezžične povezave izredno kratkega dosega, ki omogoča komunikacijo med napravami, ko se jih dotaknejo ali se jim približajo na razdaljo nekaj centimetrov. Sistemi za dostop do vrat NFC omogočajo pametnemu telefonu, da posreduje poverilnice bralniku NFC tako, da se s telefonom dotakne bralnika in odklene vrata, če so poverilnice avtorizirane. Bluetooth komunikacija / Bluetooth BLE komunikacija pa je brezžična tehnologija za kratke razdalje, ki omogoča brezžično podatkovno komunikacijo med digitalnimi napravami. Bluetooth tehnologijo se uporablja tudi za brezkontaktne mobilne poverilnice za kontrolo pristopa. Bluetooth dostop za vrata za sprejem signala uporablja pametni telefon vsakega posameznega uporabnika z nameščeno aplikacijo za brezžični prenos dostopnih poverilnic in čitalnik bližine Bluetooth Access. Ko je naprava v bližini bralnika za nadzor dostopa, aplikacija komunicira z bralnikom in izmenja varnostni ključ za preverjanje pristnosti ter odpre ključavnico in omogoči vstop. Bluetooth komunikacija, ki med drugim omogoča delovanje na večji razdalji kot NFC, je z vidika uporabniške izkušnje in delovanja digitalnega zaklepnega sistema primerljiva tehnologiji NFC, tehnični rešitvi sta istovrstni za namen odklepanja in zaklepanja digitalnih cilindrov preko mobilne naprave. Poleg tega imajo Bluetooth tehnologijo nameščene vse pametne mobilne naprave in tako naročniku ne bi bilo potrebno dodatno naročati 100 NFC obeskov, kot jih mora v konkretnem primeru za uporabnike, ki nimajo mobilne naprave z NFC tehnologijo. Uporaba fizičnega NFC ključa za uporabnika pa pomeni, da ga je potrebno napajati in ga v primeru, če ne bo napolnjen, uporabnik ne bo mogel uporabljati in dostopati do objekta. Z mobilno napravo si namreč uporabnik ne bo mogel pomagati, saj ne bo imel mobilne naprave z NFC tehnologijo. Vlagatelj še opozarja, da se aplikacija za NFC obesek preko povezave Bluetooth poveže z obeskom za ključe K55S in tako uporablja Bluetooth komunikacijo. Naročnik očitno dopušča Bluetooth tehnologijo pri NFC ključu, ne dopušča pa je kot alternativne tehnologije pri odklepanju / zaklepanju preko mobilnih naprav, kar je v nasprotju z načelom sorazmernosti in enakopravne obravnave ponudnikov ter zagotavljanja konkurence med ponudniki. Naročnik nima objektivno utemeljenega razloga, da zahteva odklepanje in zaklepanje preko mobilne naprave, ki podpira NFC komunikacijo in ne dopušča alternativnih tehnologij. Zahteva ni sorazmerna s predmetom javnega naročila, saj gre za digitalni zaklepni sistem, ki je enako funkcionalen tudi v primeru, ko bi naročnik dopuščal zaklepanje preko mobilne naprave, ki podpira Bluetooth komunikacijo. Vlagatelj še navaja, da naročnik tudi neutemeljeno zahteva, da mora sistem omogočati avtonomno delovanje digitalnih cilindrov brez uporabe baterij / zunanjih virov energije, pri čemer mora ta sistem hkrati omogočati odklepanje in zaklepanje digitalnih cilindrov preko mobilne naprave, ki podpira NFC komunikacijo. Pojasnjuje, da so enakovredne rešitve, ki bi jih naročnik moral dopustiti: 1. Sistem digitalnih cilindrov (zaklepnih elementov) z baterijo in komunikacijsko tehnologijo Bluetooth - to so digitalni cilindri, ki za delovanje potrebujejo baterijo in se odklepajo / zaklepajo z mobilnimi telefoni s

podporo Bluetooth. 2. Elektromehanski zaklepni sistem, ki nima baterije v zaklepnem elementu (cilindru) in tako izpolnjuje naročnikovo zahtevo v tem delu, vendar pa ima fizični ključ, ki odklepa zaklepni element (cilinder), zaradi česar ne izpolnjuje naročnikove zahteve, da odklepa/zaklepa digitalne cilindre prek mobilne naprave, ki podpira NFC komunikacijo. Gre za tehnologijo brezbaterijskih elektromehanskih cilindričnih vložkov, ki pa za delovanje potrebuje fizični (elektronski) ključ z baterijo. Slednji tudi napaja cilindrični vložek. Primer takega sistema je *Protec2 Clic™ System* (vlagatelj v zvezi s tem prilaga prilogo). 3. Elektromehanski zaklepni sistem, ki deluje na principu lastnega napajanja, kjer se ob vstavljanju in obračanju ključa ustvari kinetična energija, ki napaja elektroniko. Elektronski ključ in cilinder komunicirata s pomočjo šifrirane tehnologije, kar zagotavlja varen prenos podatkov. Sistem uporablja AES šifriranje in varnostne protokole, ki omogočajo zanesljivo identifikacijo in upravljanje dostopa brez potrebe po baterijah ali zunanjem napajanju. Primer takega sistema je *Assa Abloy Pulse* (vlagatelj prilaga prilogo tega sistema). Vlagatelj še navaja, da je naročnik s spremembo razpisne dokumentacije povečal število fizičnih ključev (obeskov), in sicer iz 10 na 100, kar predstavlja petino vseh ključev (naročnik razpisuje 500 mobilnih ključev), kar dodatno kaže na to, da gre pri predstavljenemu sistemu brezbaterijskih elektromehanskih cilindričnih vložkov, ki za delovanje potrebuje fizični ključ z baterijo, za enakovredno rešitev. Tudi fizični NFC ključ ima baterijo, ki jo je potrebno napolniti. Tudi pri fizičnem NFC ključu gre za ključ in ne za mobilno napravo. Naročnik tako neutemeljeno ne dopušča alternativnega sistema brezbaterijskih elektromehaničnih cilindričnih vložkov z drugim načinom odklepanja s fizičnim ključem in torej ne dopušča sistema brezbaterijskih elektromehanskih cilindričnih vložkov, ki za delovanje potrebuje fizični ključ z baterijo, dopušča pa kar 100 kosov fizičnega NFC ključa, kot alternativo odklepanju/zaklepanju digitalnih cilindrov preko mobilne naprave. Naročnikovo zahtevo je tako mogoče na popolnoma enakovreden način zagotoviti tudi z Bluetooth komunikacijo in digitalnimi cilindri, ki za delovanje potrebujejo baterije, zaradi česar naročnik krši tudi 8. člen ZJN-3. Naveden sistem omogoča tudi uro v realnem času ter beleženje zgodovine v telefonu in zaklepnem elementu. Če sistem nima baterije v zaklepnem elementu (kot jo npr. nima iLOQ) je mogoča manipulacija preko uporabe telefona. Naročnikova zahteva je nezakonita tudi sicer, saj so digitalni cilindri z baterijami po načinu delovanja enakovredni digitalnim cilindrom brez baterije. Samo napajanje ne vpliva na funkcionalnost, poleg tega ima Bluetooth, kot že navedeno, tudi prednosti. Obstaja pa tudi nevarnost, da zaklepni element (digitalni cilinder), ki ne uporablja baterije ostane odklenjen, ker cilindrični vložek ne sporoči povratne informacije. Tudi digitalni cilindri z baterijami zagotavljajo tehnologijo zaklepanja, ki je zanesljiva in ima dolgo življenjsko dobo. Poleg tega je življenjska doba baterij izjemno dolga (cca 10 let), pri čemer sistem uporabnika vnaprej opozori, kdaj je potrebna menjava. Vlagatelj še zatrjuje, da zahtevano temperaturno območje (od -30°C do +50°C) ni ovira za delovanje digitalnih cilindrov z baterijami. Pojasnjuje, da mobilni telefoni, ki so del zaklepnega sistema, uporabljajo baterije. Poleg tega same mobilne naprave, s katerimi se odklepajo/zaklepajo digitalni cilindri, delujejo v bistveno ožjih temperaturnih območjih (med 0°C in 35°C). Navedeno pa pomeni, da naročnikovi uporabniki v temperaturnem območju med - 30°C in +50°C ne morejo uporabljati mobilnih naprav. Navaja še, da sistem brezbaterijskih elektromehanskih cilindričnih vložkov, ki za delovanje potrebuje fizični (elektronski) ključ brez baterije in bi ga naročnik kot enakovrednega moral dopustiti (na primer *Assa Abloy Pulse*), deluje v navedenem temperaturnem polju od -35°C do + 85°C, ključi pa v temperaturnem območju od -30°C do + 60°C (vlagatelj prilaga katalog). Ravno tako ne drži naročnikov odgovor, da želi z digitalnim zaklepnim sistemom doseči neodvisnost od baterijskega ali omrežnega električnega napajanja. Digitalni zaklepni sistem je odvisen od baterijskega ali omrežnega električnega napajanja, saj za delovanje potrebuje mobilne naprave, ki so odvisne tako od baterijskega, kot od omrežnega električnega napajanja (vlagatelj povzema slikovni prikaz NFC ključa proizvajalca iLOQ). Vlagatelj nasprotuje še naročnikovemu odgovoru, s katerim je dovolil, da se programska oprema postavi bodisi na lastni strežniški infrastrukturi SŽ-Infrastruktura, d.o.o. ali v oblaku na območju EU, pri čemer mora ponudnik ponuditi boljšo tehnično in ekonomsko rešitev. Zatrjuje, da naročnik ni navedel kriterijev po katerih bo presojal, katera rešitev je tehnično in ekonomsko

boljša. Zato ni jasno, kaj bo naročnik storil v primeru, če bodo nekatere tehnične lastnosti boljše pri eni rešitvi, druge pa pri konkurenčni ponudbi, niti kaj bo storil v primeru, ko bo ena rešitev tehnično boljša, druga pa ekonomsko ugodnejša. Ravno tako ni podatkov, kakšna je strežniška infrastruktura naročnika - ni podatkov o strojni opremi (pomnilnik, procesorska moč …) in virtualizacijskem okolju (npr. VMware, Hyper-V, operacijski sistemi, programska oprema, omrežna infrastruktura, varnostne politike, sistemi za varnostno kopiranje, sistemi za spremljanje in upravljanje …). Naročnik krši načelo transparentnosti, enakopravne obravnave in zagotavljanja konkurence. Ponudniki nimajo zadostnih informacij, kar vodi v neprimerljivost ponudb.

Naročnik je z dokumentom št. 60402-98/2024-3 z dne 27. 11. 2024 zahtevek za revizijo zavrnil in posledično zavrnil tudi vlagateljevo zahtevo za povrnitev stroškov pravnega varstva.

Naročnik uvodoma opozarja na prakso Državne revizijske komisije in navaja, da zgolj dejstvo, da je posamezno tehnično specifikacijo ali njihovo kombinacijo mogoče izpolniti le z enim točno določenim proizvodom, še ne daje zadostne podlage za zaključek, da je naročnik tehnične specifikacije oblikoval v nasprotju z načeli zagotavljanja konkurence med ponudniki, enakopravne obravnave ponudnikov in sorazmernosti. Naročnik lahko določi tudi tehnične zahteve, ki jih izpolni samo en ponudnik ali omejeno število ponudnikov, vendar pa mora biti po stališču Državne revizijske komisije razlikovanje med ponudniki neposredno povezano s predmetom javnega naročila. Naročnik se strinja z vlagateljem, da gre pri obeh tehnologijah (NFC in Bluetooth) za tehnologiji brezžične komunikacije, pri čemer opozarja, da je vlagatelj spregledal bistvene razlike med njima, in sicer: razdaljo delovanja, postopek povezovanja, porabo energije in namen uporabe. NFC deluje na zelo kratkih razdaljah nekaj cm, medtem ko Bluetooth omogoča komunikacijo na večjih razdaljah, običajno do 10 m, v nekaterih primerih pa tudi 100 m, pri čemer navedena razlika bistveno vpliva na varnost delovanja. Pri Bluetooth tehnologiji je zaradi večjih razdalj večja možnost, da pride do motenj pri prenosu, medtem ko NFC tehnologija s svojo kratko razdaljo omogoča močno povezavo brez motenj. NFC omogoča zelo hitro in enostavno povezovanje. Navedena tehnologija ne potrebuje avtentikacije, saj se napravi povežeta takoj, ko sta v bližini. Prenos podatkov se tako zgodi samodejno in ni potrebno nobenih dodatnih del. NFC se zato pogosto uporablja za plačila in izmenjavo manjših podatkov. Pri Bluetooth tehnologiji povezovanje zahteva več korakov, vključno z iskanjem naprav in potrjevanjem povezave. Potrebna je ročna namestitev povezljivosti naprav. V večini primerov je potrebno vnesti PIN kodo in konfigurirati namestitve, da se napravi povežeta. Bluetooth tehnologijo se uporablja za prenos video vsebin, glasbe in ostalih podatkov. Tehnologiji se razlikujeta tudi pri porabi energije. NFC tehnologija ima nizko porabo energije, pri Bluetooth tehnologiji pa je poraba odvisna od različice - BLE (Bluetooth Low Energy) je zasnovan za nizko porabo, klasični Bluetooth pa porabi več energije. NFC se uporablja za izmenjavo podatkov majhnega obsega na kratki razdalji kot so: identifikacija (npr. dostopne kartice), izmenjava podatkov (npr. kontaktne informacije) in plačila (npr. bančne plačilne kartice). Bluetooth pa se uporablja za povezovanje naprav, kot so slušalke, zvočniki, tipkovnice in druge naprave, ki zahtevajo prenos podatkov (glasba, video, ostali podatki) na daljavo. To pomeni, da je NFC tehnologija v splošnem bolj sprejeta za izmenjavo kritičnih informacij, kar pomeni, da je bolj varna od Bluetooth tehnologije. Naročnik še navaja, da se Bluetooth tehnologija uporablja le v primeru programiranja NFC ključa. Naročnik dalje navaja, da so elektromehanski zaklepni sistemi, ki nimajo baterije v zaklepnem elementu (cilindru) in tako izpolnjujejo naročnikovo zahtevo v tem delu (da nimajo baterije), vendar imajo fizični ključ, ki odpira zaklepni element (cilinder), zaradi česar ne izpolnjujejo naročnikove zahteve, da odklepajo/zaklepajo digitalne cilindre preko mobilne naprave, ki podpira NFC komunikacijo. Za svoje delovanje potrebujejo fizičen (elektronski) ključ z baterijo, ki napaja cilindrični vložek (primer takega sistema je *Protec2 Cliq™ System*). Ker gre pri javnem naročilu za specifičen primer zaklepnega sistema kritične infrastrukture, kjer se zaklepajo tehnični prostori na železniških postajah, bazne postaje GSM-R in repetitorji GSM-R, je NFC tehnologija bolj primerna od Bluetooth tehnologije ali podobnih brezžičnih tehnologij. Ker je torej naročnikov zaklepni sistem

specifičen ter uporabljen za varovanje kritične infrastrukture, odklepanje na daljavo ali morebitno povezovanje več naprav (ključavnic) s pomočjo Bluetooth tehnologije (kot je to značilno za poslovne objekte, hotele, apartmaje in podobno) ni primerno. Naročnik še navaja, da morajo ključne komponente (kot je to cilinder) delovati v ekstremnih vremenskih razmerah, v čim večjem temperaturnem razponu. Pri tem je potrebno razlikovati temperaturo zraka ter temperaturo vrat, na katera je nameščen cilinder. Temperatura zraka ni enaka temperaturi vrat, ki na soncu doseže krepko čez najvišjo izmerjeno temperaturo zraka v Sloveniji. Nihanje temperatur ter ekstremne temperature pa nižajo življenjsko dobo baterij. Znano je, da baterije v idealnih pogojih dosežejo dobo delovanja okoli osem let. Na železniški infrastrukturi idealnih pogojev ni, zato se ta doba hitro zniža. Ker pa gre za zaklepanje in varovanje kritične infrastrukture, je potrebno preprečiti primere, da v ključnih oziroma izrednih dogodkih ne bi mogli hitro in varno vstopiti v tehnični prostor. V vseh izrednih dogodkih gre za varno obratovanje železniškega prometa v Sloveniji in s tem povezano varnostjo življenj potnikov in ostalega tovora. AES tehnologija uporablja simetričen algoritem šifriranja, ki šifrira podatke v blokih fiksne velikosti 128 bitov. Uporablja velikosti ključev 128, 192 ali 256 bitov. AES tehnologija je priznana po svoji varnosti, učinkovitosti in hitrosti, zaradi česar je standardna izbira za šifriranje občutljivih informacij. AES tehnologija se uporablja: za ščitenje občutljivih podatkov, datotek, hramb podatkov v oblaku, v protokolih, kot je SSL/TLS (Secure Socket Layer / Transport Layer Security) za varen spletni promet, za finančne transakcije o plačilih v bančništvu in e-trgovini, za šifriranje VPN povezav, ščitenje podatkov na pametnih telefonih in tabličnih računalnikih, za zagotavljanje zaščitene komunikacije v aplikacijah IoT (Internet of Things). AES-256 je bil izbran zaradi največje možne zaščite. V zvezi s predlaganima ključema *Protec2 Cliq* in *Assa Abloy Pulse* pa naročnik ugotavlja, da ne omogočata NFC brezstičnega odklepanja. Potrebno ju je fizično vstaviti v cilinder, ki pa je lahko v zimskem času zamrznjen, poleg tega je možno vanj vstaviti karkoli in s tem onemogočiti odklepanje in zaklepanje. Navedena ključa uporabljata Bluetooth tehnologijo za avtorizacijo oziroma prenos podatka o času odklepanja in zaklepanja ključavnice v realnem času, kar pomeni, da je potrebno naknadno ključ prisloniti na validator v notranjosti tehničnega prostora in da je potrebno ključ preko Bluetooth komunikacije povezati s telefonom in podatke naknadno poslati prek telefona (naročnik v zvezi s tem prilaga sliko). Naročnik navaja, da pri digitalnem zaklepnem sistemu ni zahteval, kje mora biti programska oprema nameščena. Programska oprema je namreč lahko nameščena v oblaku ali njegovi lastni strežniški infrastrukturi. Pojasnjuje, da je izhajal iz stališča, da pridobi ekonomsko najugodnejšo ponudbo. Da bi omogočil večjo konkurenčnost je odločitev o namestitvi programske opreme prepustil ponudnikom. Navaja še, da glede namestitve programske opreme ni predvidel primerjanja in ocenjevanja ponudb - to odločitev je prepustil ponudnikom, pri čemer je edino merilo najnižja cena. Naročnik pojasnjuje, da je v zvezi z vpisom števila NFC obeskov pri vnosu podatkov v razpisno dokumentacijo storil napako in napačno prepisal številko 100 (izpustil je eno ničlo). Takoj, ko je napako opazil, je objavil popravek. Zatrjuje, da s strani vlagatelja predlagana rešitev ključa ne ustreza razpisni dokumentaciji, saj ne želi ključa, ki ga je potrebno fizično vstaviti v cilinder - potrebuje brezstično digitalno odklepanje oziroma odklepanje z NFC tehnologijo. Naročnik ponovno opozarja, da predstavlja odklepanje z vstavljanjem ključa v cilinder težavo, saj lahko ključavnica v zimskem času zamrzne. Pojasnjuje še, da želi zaklepni sistem, ki bi onemogočal izgubo ključev in posledično nedovoljene vstope. To pomeni, da bi iz varnostnih razlogov za en izgubljeni ključ moral zamenjati ves zaklepni sistem, ki se odklepa z izgubljenim ključem. Zaklepni sistem mora biti čim bolj robusten in enostaven, v največji možni meri brezbaterijski, delovati mora v ekstremnih vremenskih razmerah, biti mora uporabniku prijazen ter omogočati kontrolo vstopa v realnem času ter revizijsko sled vstopov v tehnične prostore, bazne postaje in repetitorje.

Vlagatelj se je z vlogo z dne 4. 12. 2024 opredelil do sklepa o zavrnitvi zahtevka za revizijo. Vztraja pri pravovarstvenem predlogu in očitkih iz zahtevka za revizijo ter se dodatno opredeljuje do naročnikovih navedb. Zatrjuje, da naročnik ni navedel objektivno opravičljivih razlogov za postavitev izpodbijanih zahtev. Ne drži naročnikova ugotovitev, da iz razloga, ker Bluetooth

omogoča komunikacijo na večjih razdaljah, navedeno bistveno vpliva na varnost. Bluetooth tehnologija zagotavlja primerljivo varnost delovanja in vključuje napredne varnostne protokole in šifriranje, kar zagotavlja varnost prenosa podatkov tudi na večjih razdaljah. Navaja še, da je s strani naročnika opisan postopek povezovanja zelo poenostavljen in v praksi ne drži. Tudi naprave iOS imajo še vedno veliko težav z NFC tehnologijo, tudi s povezljivostjo. V kolikor ima telefon stalno vklopljeno NFC povezavo je tudi v nevarnosti pred posnemanjem mobilne naprave. Vlagatelj pri tem ponovno opozarja, da tudi razpisani obeski za validacijo in spreminjanje pravic potrebujejo telefon in Bluetooth komunikacijo. Pojasnjuje, da Bluetooth tehnologija omogoča dodatno plast varnosti s šifrirano avtentikacijo, ki preprečuje nepooblaščen dostop. Čeprav NFC ne zahteva dodatnih korakov, to istočasno pomeni manjšo zaščito, saj se povezava vzpostavi brez preverjanja varnostnih poverilnic. Poleg tega je Bluetooth tehnologija prav tako prilagojena za sisteme za nadzor dostopa, kjer proces povezovanja poteka samodejno in brez potrebe po ročni konfiguraciji. Uporabnik ne potrebuje vnosa PIN kode ali dodatnih nastavitev, saj je vse vnaprej konfigurirano za hitro in varno uporabo. Prav tako ne držijo navedbe, da se le NFC uporablja za dostop - tudi Bluetooth tehnologija se uporablja za dostop ne le do hotelov, apartmajev in podobno, temveč tudi do kritične infrastrukture. Ne držijo niti posplošene naročnikove navedbe, da se Bluetooth uporablja le za povezovanje naprav kot so slušalke, zvočniki, tipkovnice. Vlagatelj še pojasnjuje, da naprave, ki delujejo na podlagi Bluetooth Low Energy (BLE), za svoje delovanje porabijo zelo malo energije, življenjska doba baterij pa znaša tudi do 10 let. Prav tako je neutemeljena in nesorazmerna naročnikova zahteva po izključitvi baterij. Vlagatelj ponovno poudarja, da so *Cliq* zaklepni elementi in ključi skladni s standardom EN16864:2017 in dosegajo stopnjo 4. Pri tem se ključ hrani v žepu ali predalih in praktično ni izpostavljen neprestanim ekstremnim pogojem. Glede na reference po svetu, je *Assa Abloy Cliq* rešitev, primerna za železniško infrastrukturo, kar dokazujejo številni primeri dobre prakse. Poleg tega naročnik razpisuje digitalni sistem za 625 vrat, vendar pa bo na vseh vratih ostal mehanski sistem, kjer bodo uporabniki uporabljali ključe. Ob navedenem bi moral naročnik dopustiti tudi enakovredne rešitve. Navaja še, da elektromehanski cilindri, ki jih zastopa *Assa Abloy Cliq*, dokazano delujejo v širšem temperaturnem območju. Baterije v ključu v *Cliq* sistemih so prilagojene delovanju v zahtevnih pogojih (npr. od -35°C do +85°C). Poleg tega napredni varnostni protokoli *Cliq* sistema zagotavljajo, da je ključ vedno operativen, saj sistem pravočasno opozori na potrebo po menjavi baterij. Življenjska doba baterij v *Cliq* sistemih dosega tudi do 10 let, vzdrževanje je minimalno, uporabniki pa so o stanju baterij obveščeni prek sistema. *Cliq* sistemi vključujejo napredne rešitve, ki omogočajo varno delovanje tudi v izrednih razmerah. Elektromehanski ključi z Bluetooth BLE komunikacijo zagotavljajo zanesljivost in varnost podatkov tudi ob motnjah. Poleg tega omogočajo blaženje dostopov in centralizirano upravljanje, kar dodatno izboljša varnost kritične infrastrukture. *Cliq* elektromehanski cilindrični vložki delujejo zanesljivo tudi pri nihanju temperatur - sistem je razvit posebej za robustne pogoje, kar vključuje temperaturna nihanja in delovanje na prostem. Sistemi brez baterij imajo svoje omejitve zlasti pri zagotavljanju povratnih informacij, beleženju dostopov in daljinskem upravljanju. *Cliq* tehnologija omogoča realno časovno spremljanje in varnostne protokole, ki jih sistemi brez baterij ne zagotavljajo. Naročnikova trditev, da želi neodvisnost od baterij ni skladna z dejstvom, da mobilne naprave in NFC ključi za delovanje zaklepnega sistema prav tako uporabljajo baterije. Sistemi *Assa Abloy Cliq* ponujajo celovito rešitev, kjer je uporaba baterij optimizirana za dolgotrajno in zanesljivo delovanje. Ob navedenem je *Assa Abloy Cliq* tehnologija zasnovana v ekstremnih razmerah, zagotavlja dolgoročno zanesljivost in minimalne stroške vzdrževanja. Z integracijo Bluetooth BLE omogoča napredne funkcionalnosti, ki jih NFC tehnologija ne dosega. AES-128, ki ga uporablja *Assa Abloy Cliq*, je priznana tehnologija šifriranja, ki zagotavlja varnost in učinkovitost in je še vedno standard, ki ga uporabljajo vojaške in vladne agencije po celem svetu. Pri varovanju kritične infrastrukture ni dovolj zgolj izbira šifrirnega ključa, temveč celoten varnostni sistem, ki ga zagotavlja *Cliq*. Poleg tega so *Cliq* elektromehanski cilindrični vložki skladni z vsemi evropskimi standardi in uporabljajo tehnologijo vrtljivih diskov, ki je bila razvita za najbolj ostre vremenske pogoje. *Cliq* tehnologija pa omogoča tudi več načinov preverjanja in posodobitev

pravic ključev - opcije so stenski programator, prenosni programator, Connect aplikacija za posodabljanje ključa, kadar je uporabnik brez povezave. Vlagatelj še navaja, da naročnik ni specificiral ključnega dela elektronskega sistema - lastnih serverjev, kar onemogoča oddajo ponudb na način, kot to zahteva razpisna dokumentacija - to je, da naj ponudniki ponudijo boljšo tehnično in ekonomsko rešitev. Dejstvo je, poudarja vlagatelj, da naročnik brez jasnih informacij (o strojni opremi, omrežju, varnostnih politikah in programski opremi) ustvarja okolje, ki onemogoča pripravo konkurenčne in primerljive ponudbe. Ponudniki tako tvegajo arbitrarno zavrnitev ali nerealistično oceno stroškov, kar favorizira ponudnike z notranjimi informacijami ali predhodnim dostopom do teh podatkov. Zato ne more transparentno kalkulirati ponudbene cene za oblak ali naročnikovo lastno infrastrukturo, kar ustvarja neprimerljive ponudbe. Vlagatelj še navaja, da število NFC obeskov (100) dokazuje, da je rešitev, ki je podobna *Cliq* tehnologiji, enakovredna. Naročnik pa želi *Cliq* tehnologijo izločiti, kar ni razumljivo in objektivno utemeljeno. Prav tako kot se lahko izgubi ključ, se lahko izgubita tudi telefon in NFC obesek. Izgubljeni ključ pa se da tudi izbrisati iz zaklepnega sistema, zato ne drži naročnikova ugotovitev, da bi moral zaradi enega izgubljenega ključa zamenjati ves zaklepni sistem. Navaja še, da je *Cliq* sistem hibridni sistem, ki uporabniku omogoča najvišjo stopnjo varnosti, zaščite in nadzora, poleg tega omogoča tudi racionalizacijo stroškov. Naročnik bo nadalje dejansko imel še mehanski sistem, zaradi česar ni razumljivo, zakaj ne dopušča enakovrednih rešitev. *Assa Abloy Cliq* elektromehanski cilindri so zasnovani posebej za uporabo na kritični infrastrukturi, kot so tehnični prostori, repetitorji in bazne postaje. *Cliq* tehnologija omogoča delovanje v temperaturnem območju od -35°C do +85°C, kar presega naročnikove zahteve. Poleg tega fizični ključi *Cliq* vključujejo napredne zaščitne mehanizme, ki preprečujejo vdor snega, ledu ali umazanije v cilinder. Zasnova sistema zagotavlja varnost dostopa in minimalno potrebo po vzdrževanju, kar je ključnega pomena za kritično infrastrukturo.

Po pregledu dokumentacije o javnem naročilu ter preučitvi navedb vlagatelja in naročnika, je Državna revizijska komisija odločila tako, kot izhaja iz izreka tega sklepa, iz razlogov, ki so navedeni v nadaljevanju.

V obravnavanem primeru vlagatelj najprej oporeka naročnikovima tehničnima zahtevama - da mora zaklepni sistem omogočati odklepanje in zaklepanje digitalnih cilindrov preko mobilne naprave, ki podpira izključno NFC komunikacijo ter da mora zaklepni sistem omogočati avtonomno delovanje digitalnih centrov brez uporabe baterij. Poleg tega vlagatelj očita naročniku, da v delu, ki se nanaša na postavitev programske opreme bodisi na (naročnikovi) lastni strežniški infrastrukturi bodisi v oblaku na območju EU, ni podal nobenih drugih podatkov, kar onemogoča pripravo dopustne, konkurenčne in primerljive ponudbe.

Predmet obravnavanega javnega naročila je zamenjava obstoječega mehanskega zaklepnega sistema kritične infrastrukture (TK prostori, SV prostori, ENP, BP in RBP GSM-R omrežja …) na območju javne železnike infrastrukture (JŽI) z digitalnim zaklepnim sistemom. Naročnik želi zamenjati 625 kosov mehanskih cilindrov z digitalnimi cilindri ter dobavo 500 digitalnih mobilnih ključev za uporabnike in 100 uporabniških NFC obeskov. Kot je navedel naročnik, se opis bistvenih zahtev digitalnega zaklepnega sistema deli na tri glavne komponente: upravljanje digitalnega zaklepnega sistema, digitalni cilinder in mobilni ključ (Obrazec 11 - Splošne in tehnične zahteve, točka I - Splošni opis).

Državna revizijska zaradi nazornejše obrazložitve (in iz razloga, ker se tehnične zahteve medsebojno prepletajo) v celoti povzema vse naročnikove zahteve, ki se nanašajo na razpisan zaklepni sistem oziroma na vse tri komponente digitalnega zaklepnega sistema.

»1. Upravljanje digitalnega zaklepnega sistema

Sistem mora omogočati centralno upravljanje zaklepnega sistema oddaljenih objektov v realnem času. Omogočeno mora biti oddaljeno upravljanje avtorizacij mobilnih ključev in administracijo odklepanja oddaljenih objektov na treh nadzornih delovnih mestih. Nadzorna delovna mesta morajo pokrivati celoten sistem digitalnega zaklepanja na JŽI, in sicer: Delovno mesto 1 - Ljubljana (DM1), Delovno mesto 2 - Celje (DM2) in Delovno mesto 3 - Postojna (DM3).[1]

2. Digitalni cilinder

Delovanje brez uporabe baterij; Sistem mora omogočati avtonomno delovanje digitalnih cilindrov brez uporabe baterij. Za svoje delovanje digitalni cilindri ne smejo uporabljati zunanjih virov energije. S tem želimo odpraviti potrebo po rednem vzdrževanju in menjavi baterij. Tehnologija zaklepanja mora zagotavljati zanesljivo in dolgo življenjsko dobo brez dodatnih operativnih stroškov, povezanih z napajanjem. S tem želimo zagotoviti trajnostno rešitev.

NFC komunikacija; Sistem mora omogočati odklepanje in zaklepanje digitalnih cilindrov prek mobilne naprave, ki podpira NFC komunikacijo.

Šifriranje komunikacije; Komunikacija med mobilnim ključem in digitalnim centrom mora biti izvedena z uporabo naprednih šifrirnih metod. Vsaka komunikacija mora biti šifrirana z algoritmi, kot je to npr. AES-256. Mora se zagotoviti visoka raven varnosti. Neuporaba šifrirnih algoritmov ali uporaba šibkih šifrirnih sistemov ni dovoljena. Šifriranje mora biti zagotovljeno skozi vse faze komunikacije med ključem in cilindrom.

Omrežna povezava za odpiranje nekaterih pomembnejših lokacij; Za odpiranje digitalni cilindrov nekaterih pomembnejših lokacij mora sistem omogočati spletno avtentikacijo v realnem času. S to funkcionalnostjo se zagotovi, da se vsak dostop preveri v realnem času preko omrežne povezave. S tem želimo preprečiti vsako zlorabo uporabe mobilnega telefona v načinu brez povezave (kot je to Flight Mode). Ko mobilni telefon nima povezave z omrežjem, se dostop zavrne. Vsak dostop se mora zabeležiti v sistemu.

Drugi (alternativni) način odklepanja, ko uporabnik nima mobilne naprave z NFC tehnologijo; V primeru, da uporabnik nima mobilne naprave z NFC tehnologijo, mora sistem omogočati način dostopa v obliki fizičnega NFC ključa. Takšen način odklepanja mora biti enako varen in šifriran kot z mobilno napravo.

Revizijska sled v realnem času; Vsak dostop oz. odklepanje in zaklepanje digitalnih cilindrov mora biti zabeležen v centralnem sistemu. Zagotovljena mora biti revizijska sled v realnem času z možnostjo izpisov vseh dostopov. S tem zagotovimo popolni nadzor nad kritično infrastrukturo v realnem času.

Ostali tehnični pogoji delovanja; Digitalni cilindri morajo delovati v ekstremnih vremenskih pogojih in v temperaturnem območju med -30°C in +50°C. Morajo biti antivandal izvedbe. Sistem ne sme uporabljati baterij saj v takšnih vremenskih razmerah niso primerne za normalno delovanje.«

3. Mobilni ključ

NFC tehnologija, iOS, Android in Harmony (Huawei); Zahteva se sistem za upravljanje dostopa, ki deluje na tehnologiji NFC. Sistem mora omogočati odklepanje in zaklepanje digitalni cilindrov prek mobilnih naprav. Odklepanje in zaklepanje digitalnih cilindrov mora biti izvedeno s pametnim

[1] Pri tem je naročnik lokacijo objektov, predvidenih za zamenjavo z digitalnim zaklepnim sistemom, prikazal na shemi (»Nacionalno poimenovanje železniških prog«).

telefonom, ki podpira NFC komunikacijo med mobilnim telefonom in digitalnim cilindrom. Mobilni telefon se uporabi kot ključ za odklepanje digitalnega cilindra. Vsaka komunikacija med napravami mora biti dodatno šifrirana z algoritmi, ko je to npr. AES-256. Aplikacija za mobilni ključ mora biti na voljo na vseh glavnih mobilnih operacijskih sistemih, kot so iOS, Android in Harmony (Huawei). Sistem mora zagotavljati nemoteno delovanje in enako funkcionalnost na vseh odprtih platformah, kar omogoča široko združljivost in fleksibilnost pri uporabi različnih mobilnih naprav.

Revizija dogodkov v realnem času; Sistem mora omogočati enostavno spreminjanje, izbris in preklic avtorizacij dostopov na daljavo. Vsaka uporaba mobilnega ključa mora biti zabeležena v sistemu v realnem času. S tem se zagotovi revizijska sled za vse poskuse dostopov. Zagotovljen mora biti tudi alternativni način dostopa z uporabo fizičnega NFC ključa. Fizični NFC ključ mora zagotavljati varen dostop, ko uporabnik nima mobilne naprave z NFC tehnologijo in mobilni ključ ni na voljo.«

Naročnik je v zadnjem odstavku Obrazca 11 zapisal še:

»Ponudba mora vsebovati:
- *dobavo in instalacijo opreme za tri nadzorna mesta,*
- *dobavo 500 digitalnih mobilnih ključev z letnimi licencami,*
- *dobavo 625 kosov digitalnih cilindrov z letnimi licencami (pri ponudbi naj se upošteva skupna dolžina cilindra 80 mm),*
- *dobavo 100 kosov uporabniških NFC obeskov,*
- *demontažo obstoječih mehanskih cilindrov ter montaža in programiranje 625 kosov digitalnih cilindrov,*
- *izobraževanje uporabnikov sistema,*
- *podpora vzdrževanju najmanj 10 let.*

Naročnik dovoljuje postavitev programske opreme na lastni strežniški infrastrukturi SŽ-Infrastruktura, d.o.o. ali v oblaku na območju EU. Ponudnik naj ponudi boljšo tehnično in ekonomsko rešitev.«

V predhodno citiranem delu Obrazca 11 je že upoštevana sprememba razpisne dokumentacije - naročnik je namreč 7. 11. 2024 na Portalu javnih naročil objavil popravek razpisne dokumentacije, s katerim je število uporabniških NFC obeskov (iz zgoraj citirane četrte alineje) iz prvotnih 10 zvišal na 100 kosov.

V zvezi z izpodbijanimi zahtevami so bila preko Portala javnih naročil postavljena številna vprašanja. Državna revizijska komisija najprej povzema vprašanja in naročnikove odgovore, ki se nanašajo na zahtevi, v skladu s katerima je naročnik dovolil izključno NFC komunikacijo ter brezbaterijsko delovanje digitalnih cilindrov, nato pa še vprašanja in naročnikove odgovore v zvezi s postavitvijo programske opreme bodisi na naročnikovi lastni strežniški infrastrukturi bodisi v oblaku na območju EU.

Prvo vprašanje: *»V skladu z objavljeno razpisno dokumentacijo smo detaljno analizirali tehnične specifikacije, iz katerih je razvidno, da je edini produkt, ki v celoti ustreza tehničnim specifikacijam I-lock. To nakazuje na vnaprejšnji dogovor in preferiranje točno določenega ponudnika, kar pa je v nasprotju z Zakonom o javnem naročanju. Takšna praksa nakazuje na sum o korupciji. Po Zakonu o javnem naročanju je zaradi zagotovitve konkurence, potrebno zagotoviti razpisne pogoje, ki ustrezajo najmanj trem produktom, ki v celoti ustrezajo tehničnim specifikacijam, zato vas pozivamo, da poleg I-locka navedete še dva dodatna produkta, ki ustrezata razpisanim tehničnim specifikacijam.«* (Vprašanje je bilo objavljeno na Portalu javnih naročil 28. 10. 2024 ob 08.04.)

Drugo vprašanje: *»Prosimo za pojasnilo, ali ste pred objavo javnega naročila izvedli analizo trga za ugotovitev, koliko podjetij lahko izpolni zahteve razpisa, in zakaj niso bile dopuščene variante z različnimi tehničnimi rešitvami, kar bi povečalo tržno konkurenco?* […]*«*

Tretje vprašanje: *»Kako so definirane tehnološke zahteve za digitalni zaklepni sistem in zakaj so tako specifične, da omogočajo sodelovanje le enemu produktu, kar bo razvidno iz dospelih ponudb?«*

Naročnik je na vsa tri vprašanja na Portalu javnih naročil (28. 10. 2024 ob 08.04, 6. 11. 2024 ob 12.38 in 6. 11. 2024 ob 12.39) podal isti odgovor: *»Tehnološke zahteve so definirane na osnovi izkušenj na obstoječem zaklepnem sistemu, geografskih lokacij tehničnih prostorov in načinu dela vzdrževalnega osebja, ki vstopa v prostore in potrebnih vstopov izvajalcev ter razpoložljive infrastrukture.«*

Na četrto vprašanje: *»V tehničnih specifikacijah razpisne dokumentacije ste določili, da mora (ponujeni) sistem omogočati odklepanje in zaklepanje digitalnih cilindrov prek mobilne naprave, ki podpira NFC komunikacijo. Naročnika pozivamo, da kot ustrezen dopusti tudi sistem, ki omogoča odklepanje in zaklepanje digitalnih centrov prek mobilne naprave, ki podpira BLUETOOTH komunikacijo. Slednja je z vidika uporabniške izkušnje in delovanja sistema primerljiva tehnologiji NFC. Povedano drugače, v kolikor naročnik dopusti sistem, ki podpira BLUETOOTH komunikacijo oz. tehnologijo ,ne bo prejel nič slabše tehnične rešitve. Prav tako v tem primeru za uporabnike, ki nimajo mobilne naprave z NFC tehnologijo, ne bo potrebno omogočiti načina dostopa v obliki fizičnega NFC ključa, saj imajo BLUTOOTH tehnologijo nameščene praktično vse pametne mobilne naprave (tehnologija BLUETOOTHE je namreč bolj pogosto uporabljena kot NFC).«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.42 objavil odgovor: *»V tehničnih specifikacijah je zahtevana varnejša tehnologija NFC.«*

Na peto vprašanje: *»V tehničnih specifikacijah zahtevate, da mora ponujeni sistem omogočati avtonomno delovanje digitalnih cilindrov brez uporabe baterij in da za svoje delovanje digitalni cilindri ne smejo uporabljati zunanjih virov energije. Hkrati pa mora ponujeni sistem omogočati odklepanje in zaklepanje digitalnih centrov preko mobilne naprave, ki podpira NFC komunikacijo. Takšna zahteva (oz. kombinacija zahtev) je nesorazmerna in določena v nasprotju z določili ZJN-3. Ta med drugim določa, da morajo tehnične specifikacije vsem gospodarskim subjektom zagotavljati enak dostop do postopka javnega naročanja in neupravičeno ne smejo ovirati odpiranja javnih naročil konkurenci.* […]*«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.44. objavil odgovor, ki je podoben odgovorom na prva tri vprašanja, in sicer: *»V tehničnih specifikacijah je zahtevana varnejša tehnologija NFC in avtonomno delovanje cilindrov brez uporabe baterij. Izhajamo iz izkušenj na obstoječem zaklepnem sistemu, geografskih lokacij tehničnih prostorov in načinu dela vzdrževalnega osebja, ki vstopa v prostore in potrebnih vstopov izvajalcev ter razpoložljive infrastrukture.«*

Na šesto vprašanje: *»Naročnika pozivamo, da dopusti, da ponudimo tudi sisteme, ki za svoje delovanje potrebujejo baterij oziroma zunanji vir energije. Namreč ravno ti sistemi bodo v primeru izpada električne energije prav zaradi baterij še vedno delovali in ravno s tem bo naročniku zagotovljena vzdržna rešitev brez morebitnih vmesnih izpadov. Poleg tega je življenjska doba baterij izjemno dolga (cca 10 let), pri čemer sistem uporabnika vnaprej opozori, kdaj je potrebna menjava. Potreba po rednem vzdrževanju in menjavi baterij je zato minimalna. Prav tako tudi sami stroški menjave baterij, saj se te redko menjajo. Hkrati pa so ti stroški nedvomno nižji od stroškov, ki bi jih v primeru vaše zdajšnje želene tehnične rešitve povzročil izpad sistema. Še posebej na kritični infrastrukturi, kjer so morebitni izpadi toliko bolj alarmantni. Ker gre v primeru menjave baterij za minimalne stroške vzdrževanja, smo v primeru, da boste dopustili predložitev*

ponudb s sistemi, ki za svoje delovanje potrebujejo baterije oziroma zunanji vir energije, kot zainteresiran ponudnik ta strošek pripravljeni kriti sami. Ob tem izpostavljamo še, da tudi drugi naročniki kritične infrastrukture uporabljajo sisteme, ki za svoje delovanje potrebujejo baterij oziroma zunanji vir energije, pa pri teh naročnikih ne prihaja do nobenih posebnih težav. Zahteva naročnika je tako povsem neutemeljena in nesorazmerna predmetu javnega naročila.« je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.45 odgovoril: *»Z digitalnim zaklepnim sistemom želimo doseči neodvisnost od baterijskega ali omrežnega električnega napajanja.«*

Sedmo vprašanje: *»Poleg NFC komuniciranja obstajajo tudi drugi tipi komunikacije. Zakaj zahtevate samo NFC komunikacijo, ki je komunikacija kratkega dosega? Naročnika pozivamo, da dopusti tudi druge tipe komunikacije.«*

Osmo vprašanje: *»Želeli bi opozoriti, da NFC tehnologije ne omogočajo oziroma podpirajo vse naprave, kar jasno izhaja že iz samih tehničnih specifikacij, saj zahtevate, da mora sistem v primeru, da uporabnik nima mobilne naprave z NFC tehnologijo, omogočati način dostopa v obliki fizičnega NFC ključa. Tudi te ključke je potrebno polniti, zato za uporabnika ne predstavljajo najenostavnejše rešitve. Lahko se tudi zgodi, da zaradi tega, ker ključ ne bo napolnjen, uporabnik ne bo mogel dostopati do objekta. S svojo mobilno napravo si namreč ne bo mogel pomagati, saj na njen NFC (glede na to, da potrebuje ključek), ne bo deloval. Z vidika uporabnika bi bila zato veliko bolj prijazna uporaba tehnologije BLUTOOTH, ki jo podpirajo vse naprave, ki jih zahtevate v tehničnih specifikacijah. Tehnologija BLUETOOTH je namreč precej bolj dostopna tehnologije NFC. Prav tako omogoča delovanje na večji razdalji kot NFC, kar je z vidika uporabnika bolj prijazna. Potreba po fizičnem NFC ključu v primeru uporabe tehnologije BLUTOOTH povsem odpade, s tem pa tudi strošek za nakup teh ključkov. Kar nenazadnje pomeni tudi prihranek sredstev za naročnika. Naročnika pozivamo, da tehnologijo NFC spremeni v tehnologijo BLUETOOTH oziroma vsaj, da dopusti predložitev ponudb z obema tehnologijama.«*

Naročnik je na sedmo in osmo vprašanje na Portalu javnih naročil (6. 11. 2024 ob 12.47 in 6. 11. 2024 ob 12.48) podal enak odgovor, kot na četrto vprašanje, in sicer: »*V tehničnih specifikacijah je zahtevana varnejša tehnologija NFC.*«

Na deveto vprašanje: *»Naročnika opozarjamo, da s trenutno določenimi tehničnimi specifikacijami omejujete konkurenco, kar je v nasprotju z določili ZJN-3. Prav tako so tehnične zahteve nesorazmerne predmetu javnega naročila. Javno naročilo omejujete na en sistem, ki podpira NFC, ki ne uporablja baterij. Posledično pa izključujete vse ostale primerljive sisteme, ki podpirajo tehnologijo BLUETOOTH in prav tako ne uporabljajo baterij. Rezultat takšnega naročila bo visoka ponudbena cena, kar z vidika gospodarnosti in prepovedi omejevanja konkurence ni ne primerno, ne dopustno.* […]*«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.49 odgovoril: *»Naročnik ne bo spreminjal določil razpisne dokumentacije.«*

Na deseto vprašanje: *»Naročnika pozivamo, da dopusti rešitve z zaklepnimi sistemi, ki uporabljajo alternativne tehnologije, ker lahko tudi ti naročniku zagotovijo enako ali višjo raven varnosti. S tem pa tudi (večjo) konkurenco med ponudniki in skladnost tehničnih zahtev z ZJN-3.«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.50 odgovoril: *»Ker gre za varovanje kritične infrastrukture si prizadevamo za močne šifrirne algoritme, ki so trenutno mogoči.«*

Na enajsto vprašanje: *»Ali bo naročnik kot ustrezno sprejel tehnologijo brezbaterijskih mehatronskih cilindričnih vložkov? Pri brezbaterijskih mehatronskih cilindričnih vložkih menjava baterij ni potrebna. Prav tako ta tehnologija zagotavlja zanesljivo in dolgo življenjsko dobo brez dodatnih operativnih stroškov povezanih z napajanjem.«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.54 odgovoril: *»V tehničnih specifikacijah je napisano kakšen digitalni zaklepni sistem potrebujemo.«*

Naslednji sklop treh vprašanj in naročnikovih odgovorov nanje se nanašajo na namestitev programske opreme.

Na prvo vprašanje: *»Spoštovani, pri sistemu upravljanja digitalnega zaklepnega sistema ne navajate kje je nameščena programska oprema za upravljanje s sistemom - ali na lastni strežniški infrastrukturi ali gre za »cloud« solucijo? Te informacije so namreč bistvene pri izbiri sistema - iz vidika varnosti, dostopnosti, vzdrževanja ter vplivajo na same stroške nakupa programske opreme in tehnične podpore, prav tako skladnost z NIS 2.«* je naročnik na Portalu javnih naročil 28. 10. 2024 ob 08.09 odgovoril: *»Pri digitalnem zaklepnem sistemu ne navajamo načina kje naj bo nameščena programska oprema (cloud, lastna strežniška infrastruktura), ker lahko uporabimo prvo ali drugo izvedbo.«*

Na drugo vprašanje: *»*[…] *Naročnika opozarjamo, da je podatek o tem, kje bo nameščena programska oprema bistvenega pomena z vidika priprave same ponudbe. Na podlagi trenutnih tehničnih zahtev naročnika, ni mogoče pripraviti primerljive ponudbe za izpolnitev predmeta javnega naročila, saj se ponudba (in s tem tudi ponudbena cena) znatno razlikuje v primeru, da bo programska oprema nameščena na »cloud« ali v primeru, da bo nameščena na »lastni strežniški infrastrukturi. Naročnika zato pozivamo, da bodisi dovoli oddajo variantnih ponudb (te zdaj ni dovoljena), bodisi, da se opredeli do tega, kje bo nameščena strežniška infrastruktura.«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.34 odgovoril: *»Naročnik dovoljuje postavitev programske opreme na lastni strežniški infrastrukturi SŽ- Infrastruktura, d.o.o. ali v oblaku na območju EU. Ponudnik naj ponudi boljšo tehnično in ekonomsko rešitev.«*

Na tretje vprašanje: *»Januarja 2023 je pričela veljati nova Direktiva EU 2022/2555 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (Directive on the Security of Network and Information Systems - direktiva NIS 2). Ta priporoča, da mora biti programska oprema nameščena na lastni strežniški infrastrukturi (in ne na »cloud«). Naročnika pozivamo, da spremeni razpisno dokumentacijo na način, da bo ta usklajena z veljavno zakonodajo.«* je naročnik na Portalu javnih naročil 6. 11. 2024 ob 12.41 odgovoril: *»Direktiva NIS 2 še ni prenesena v nacionalno zakonodajo RS.«*

Državna revizijska komisija je najprej obravnavala vlagateljeve očitke, ki se nanašajo na naročnikovi zahtevi, v skladu s katerima mora ponujeni zaklepni sistem omogočati odklepanje in zaklepanje digitalnih cilindrov preko mobilne naprave, ki podpira izključno NFC komunikacijo ter omogočati avtonomno delovanje digitalnih centrov brez uporabe baterij. Vlagatelj namreč zatrjuje, da obe izpodbijani tehnični zahtevi izpolnjujejo le proizvodi iLOQ, da sta zahtevi nesorazmerni z razpisanim predmetom in da naročnik za njuno postavitev nima objektivno opravičljivih razlogov. Kot zatrjuje vlagatelj, bi moral naročnik dopustiti tri enakovredne rešitve: 1. Sistem digitalnih cilindrov (zaklepnih elementov) z baterijo in komunikacijsko tehnologijo Bluetooth - digitalne cilindre, ki za svoje delovanje potrebujejo baterijo in se odklepajo / zaklepajo z mobilnimi telefoni s podporo Bluetooth, 2. Elektromehanski zaklepni sistem, ki nima baterije v zaklepnem elementu (cilindru), vendar imajo fizični ključ, ki odklepa zaklepni element (cilinder). 3. Elektromehanski zaklepni sistem, ki deluje na principu lastnega napajanja, kjer se ob vstavljanju in obračanju ključa ustvari kinetična energija, ki napaja elektroniko. Vlagatelj ob tem pojasnjuje, da prva rešitev ne izpolnjuje nobene izmed obeh izpodbijanih tehničnih zahtev, druga in tretja rešitev pa delujeta brez uporabe baterij (in tako izpolnjujeta naročnikovo zahtevo, da delujeta brez baterij), vendar imata fizični ključ, ki odklepa zaklepni element in s tem ne izpolnjujeta naročnikove zahteve, da odklepata in zaklepata digitalne cilindre prek mobilne naprave, ki podpira NFC komunikacijo.

S tehničnimi specifikacijami naročnik opredeli zahtevane značilnosti (lastnosti) predmeta javnega naročila, ki naj bi izražale njegova pričakovanja glede namena, ki ga želi doseči z izvedbo javnega

naročila. Tehnične specifikacije tako določajo zahtevane značilnosti gradnje, storitve ali blaga. Te značilnosti se lahko nanašajo tudi na točno določen postopek ali način proizvodnje ali zagotavljanja zahtevanih gradenj, blaga ali storitev ali na točno določen postopek za kakšno drugo stopnjo v njihovi življenjski dobi, tudi če takšni dejavniki fizično niso del njih, a pod pogojem, da so značilnosti povezane s predmetom javnega naročila ter sorazmerne z vrednostjo in cilji naročila (prvi odstavek 68. člena ZJN-3).

Naročnik določi tehnične specifikacije ob upoštevanju 68. člena ZJN-3, ki v četrtem odstavku določa, da morajo slednje vsem gospodarskim subjektom zagotavljati enak dostop do postopka javnega naročanja in neupravičeno ne smejo ovirati odpiranja javnih naročil konkurenci. Če tega ne upravičuje predmet javnega naročila, v skladu s šestim odstavkom 68. člena ZJN-3 v tehničnih specifikacijah ne smejo biti navedeni določena izdelava ali izvor ali določen postopek, značilen za proizvode ali storitve določenega gospodarskega subjekta, ali blagovne znamke, patenti, tipi ali določeno poreklo ali proizvodnja, ki dajejo prednost nekaterim podjetjem ali proizvodom ali jih izločajo. Take navedbe so izjemoma dovoljene, če sicer ni mogoče dovolj natančno in razumljivo opisati predmeta naročila, vsebovati pa morajo tudi besedi »ali enakovredni«. Naročnik je pri opisovanju predmeta javnega naročila omejen tudi s temeljnimi načeli javnega naročanja, pri čemer mora tehnične specifikacije določiti na način, ki na eni strani zagotavlja konkurenco med ponudniki, na drugi pa njihovo enakopravno obravnavo (5. in 7. člen ZJN-3).

Četudi torej pravila javnega naročanja določajo, kako naj naročnik blago nabavi, pa po drugi strani ne določajo, katero blago sme nabaviti, kakor tudi ne, katere konkretne lastnosti mora imeti blago, ki ga naročnik naroča. Na podlagi navedenega gre tako ugotoviti, da je naročnik pri ugotavljanju svojih potreb in oblikovanju tehničnih specifikacij načeloma samostojen oziroma avtonomen, kar pomeni, da tehnične zahteve določi ob upoštevanju lastnih potreb ter pričakovanj glede na predmet javnega naročila. Avtonomija naročnika pri oblikovanju tehničnih specifikacij pa ni neomejena - naročnik tako ne sme postavljati zahtev, ki niso objektivno opravičljive in bi lahko določenim ponudnikom bodisi dajale neupravičeno prednost bodisi bi jim onemogočale udeležbo v postopku javnega naročanja.

V tej zvezi je Državna revizijska komisija že večkrat opozorila, da načela zagotavljanja konkurence med ponudniki ni mogoče interpretirati v smislu zahteve po vzpostavljanju konkurenčnosti tudi na tistih področjih oziroma v tistih primerih, ko te iz upravičenih razlogov ni mogoče doseči. Prav tako tudi načela enakopravnosti v pravu javnih naročil ni mogoče razumeti kot absolutne kategorije. Enakopravnost namreč ne pomeni, da mora naročnik vsem potencialnim ponudnikom omogočiti enak položaj v postopku oddaje javnega naročila. Nasprotno, pravo praviloma ne sme neposredno vplivati na razmerja na trgu z ukrepi, ki bi povzročali ekonomsko ali dejansko enakost. Zaradi različnih ekonomskih, tehničnih, kadrovskih in tudi naravnih danosti je dejanski položaj ponudnikov in njihovih ponudb različen, prednosti, ki jih te dajejo, pa je dovoljeno in pogosto celo gospodarno upoštevati. Zato zgolj dejstvo, da naročnik z določeno zahtevo razlikuje ponudnike, še ne pomeni, da je takšna zahteva že sama po sebi diskriminatorna. V naravi same zahteve je, da ponudnike razvršča na tiste, ki določeno zahtevo izpolnjujejo in je zato njihovo ponudbo mogoče obravnavati kot dopustno (takšno, ki ustreza potrebam in zahtevam naročnika), ter na tiste, ki te zahteve ne izpolnjujejo in posledično ne morejo sodelovati v postopku oddaje javnega naročila. Naročniki so zato v postopkih oddaje javnih naročil upravičeni postavljati zahteve, ki imajo za posledico razlikovanje ponudnikov, vendar le iz razlogov, ki so neposredno povezani s predmetom javnega naročila in so objektivno opravičljivi. Ni pa dopustno razlikovanje ponudnikov glede na kriterije, ki niso objektivno opravičljivi in pomenijo zlasti krajevno, predmetno ali osebno diskriminacijo, s čimer je določen gospodarski subjekt bodisi postavljen v bistveno slabši položaj bodisi je privilegiran, ne da bi za to obstajali utemeljeni razlogi (v tej zvezi smiselno prim. tudi sodbo Sodišča EU v zadevi C-513/99, Concordia Bus Finland Oy Ab).

Ob upoštevanju predstavljenih zakonskih določb gre torej ugotoviti, da ZJN-3 naročniku ne prepoveduje določitve tehničnih zahtev, s katerimi se omejuje konkurenca, temveč mu prepoveduje zgolj določitev takšnih tehničnih zahtev, s katerimi se neupravičeno omejuje konkurenca. Naročnik torej v dokumentaciji v zvezi z oddajo javnega naročila lahko določi tudi tehnične zahteve, ki jih lahko izpolni samo en ponudnik ali omejeno število ponudnikov, vendar pa mora biti razlikovanje med ponudniki, ki lahko ponudijo produkt z zahtevanimi tehničnimi specifikacijami, in ponudniki, ki takšnega produkta ne morejo ponuditi, neposredno povezano s predmetom javnega naročila in objektivno opravičljivo.

V konkretnem primeru je treba ugotoviti, da je naročnik s postavljenimi zahtevami nedvomno omejil konkurenco oziroma zožil krog gospodarskih subjektov, ki lahko v konkretnem primeru pridobijo javno naročilo - med vlagateljem in naročnikom ni spora, da lahko obe sporni tehnični zahtevi izpolnjujejo le proizvodi proizvajalca iLOQ oziroma istoimenski proizvodi iLOQ. Izključno pri navedenih proizvodih za ključavnico / cilinder namreč niso potrebne baterije, odklepajo pa se z mobilnimi telefoni s podporo NFC. Ker pa je ravnanje naročnika, s katerim se omejuje konkurenca in vzpostavlja razlikovanje med ponudniki (glede na predhodno pojasnjeno) v nasprotju z določili ZJN-3 le v primeru, v kolikor je takšna omejitev oziroma razlikovanje neupravičena, je Državna revizijska komisija presojala, ali je naročnik za ravnanje (to je za določitev obeh izpodbijanih zahtev), s katerim je zožil krog gospodarskih subjektov, ki lahko pridobijo predmetno javno naročilo, ter s tem vzpostavil razlikovanje med njimi, imel podlago v objektivno in strokovno opravičljivih razlogih, povezanih s predmetom javnega naročila.

Med vlagateljem in naročnikom ni spora, da je NFC komunikacija (Sistem za bližnjo komunikacijo, *Near Field Communication*) tehnologija izredno kratkega dosega, ki omogoča komunikacijo med napravami, ki se jih dotaknejo ali se jim približajo na razdaljo nekaj centimetrov, navedena tehnologija pa med drugim omogoča tudi fizični dostop. Med njima tudi ni spora, da NFC sistem za dostop do vrat omogoča pametnemu telefonu, da posreduje poverilnice bralniku NFC tako, da se s telefonom dotakne bralnika in odklene vrata, če so poverilnice avtorizirane. Dalje sta si stranki edini tudi v tem, da je Bluetooth komunikacija / Bluetooth BLE komunikacija brezžična tehnologija na kratke razdalje, ki omogoča brezžično podatkovno komunikacijo med digitalnimi napravami in se uporablja tudi za brezkontaktne mobilne poverilnice za kontrolo pristopa. Strinjata se tudi v tem, da Bluetooth dostop za vrata za sprejem signala uporablja pametni telefon vsakega posameznega uporabnika z nameščeno aplikacijo za brezžični prenos dostopnih poverilnic in čitalnik Bluetooth Access. Ko je naprava v bližini bralnika za nadzor dostopa, aplikacija komunicira z bralnikom in izmenja varnostni ključ za preverjanje pristnosti ter odpre ključavnico in omogoči vstop.

Državna revizijska komisija ugotavlja, da naročnik v postopku pravnega varstva ni navedel okoliščin, ki bi predstavljale strokovno utemeljene in objektivno opravičljive razloge za odločitev, da bo kot ustrezno dopustil le NFC tehnologijo. Čeprav je vlagatelj pojasnil konkretne razloge, zaradi katerih navedena zahteva ni sorazmerna s predmetom javnega naročila ter navedel tudi, da je digitalni zaklepni sistem, ki uporablja Bluetooth komunikacijo, enako funkcionalen - ima enak način delovanja v smislu digitalnega odklepanja / zaklepanja preko mobilne naprave oziroma gre pri obeh tehnologijah le za različne protokole komuniciranja preko mobilnih naprav, ki pa so glede na predmet popolnoma primerljive, se je naročnik odzval le pavšalno. Naročnik je, kot bo razvidno iz nadaljnje obrazložitve, svojo odločitev za NFC tehnologijo oprl na štiri, po njegovem mnenju bistvene razlike med obema tehnologijama (na razdaljo delovanja, postopek povezovanja, porabo energije in namen uporabe, pri čemer je razliki, ki se nanašata na razdaljo delovanja in namen uporabe utemeljil predvsem v povezavi z varnostjo delovanja), a s svojimi navedbami ni uspel izkazati objektivno opravičljivih razlogov, ki bi takšno omejevanje opravičili.

Naročnik je v zvezi z razdaljo delovanja (ki je pri NFC tehnologiji, kot že izhaja iz te obrazložitve in med strankama ni sporno, krajša kot pri Bluetooth tehnologiji) zgolj splošno in pavšalno ugotovil, da je pri Bluetooth tehnologiji zaradi večje razdalje tudi večja možnost, da pride do motenj pri prenosu, medtem ko NFC tehnologija s svojo kratko razdaljo omogoča močno povezavo brez motenj oziroma da je potrebno NFC napravo (kartico, digitalni obesek ali telefon) fizično približati, kar povečuje varnost. Pri tem naročnik ni pojasnil, zakaj mu daljša razdalja pri Bluetooth tehnologiji ne bi zagotavljala ustrezne stopnje varnosti. Vlagatelj je namreč v zahtevku za revizijo navedel, da je Bluetooth komunikacija, kljub temu, da deluje na večji razdalji kot NFC komunikacija, z vidika uporabniške izkušnje popolnoma primerljiva tehnologiji NFC. Pojasnil je tudi, da Bluetooth tehnologija zagotavlja primerljivo varnost delovanja, saj vključuje napredne varnostne protokole in šifriranje, kar zagotavlja varnost prenosa podatkov brez motenj. Poleg tega je vlagatelj v zvezi s tem opozoril tudi na prednosti Bluetooth tehnologije - navedel je, da Bluetooth komunikacija omogoča dodatno plast varnosti s šifrirano avtentikacijo, ki preprečuje nepooblaščen dostop.

Ravno tako so pavšalne tudi naročnikove ugotovitve, ki se nanašajo na postopek povezovanja. Naročnik je v zvezi s tem navedel le, da NFC tehnologija ne potrebuje avtentikacije, saj se napravi povežeta takoj, ko sta v bližini, pri Bluetooth tehnologiji pa naj bi povezovanje zahtevalo več korakov, pri čemer je potrebna ročna namestitev povezljivosti naprav. Državna revizijska komisija se strinja z vlagateljem, da je s strani naročnika opisan postopek povezovanja pavšalen in poenostavljen. Vlagatelj je namreč v nasprotju z naročnikom navedene naročnikove ugotovitve ovrgel s prepričljivejšimi razlogi. Navedel je, da čeprav NFC ne zahteva dodatnih korakov, to posledično pomeni tudi manjšo zaščito, saj se povezava vzpostavi brez preverjanja varnostnih poverilnic. Zlasti pa je vlagatelj v zvezi s tem ovrgel tudi naročnikov temeljni argument, torej navedbo, ki se nanaša na povezovanje naprav pri Bluetooth tehnologiji - vlagatelj je pojasnil, da je tudi Bluetooth tehnologija prilagojena za sisteme za nadzor dostopa (kar med vlagateljem in naročnikom, kot že izhaja iz te obrazložitve, ni sporno), kjer proces povezovanja poteka samodejno in brez potrebe po ročni konfiguraciji. Uporabnik tako ne potrebuje vnosa PIN kode ali dodatnih nastavitev, saj je vse vnaprej konfigurirano in optimizirano za varno uporabo.

Naročnik je neprepričljiv in celo kontradiktoren tudi pri pojasnjevanju razlike med obema tehnologijama v delu, ki se nanaša na porabo energije. Pojasnil je namreč, da se je odločil za NFC komunikacijo tudi iz razloga, ker ima NFC tehnologija nizko porabo energije, po drugi strani pa je naročnik priznal, da je pri Bluetooth tehnologiji porabe energije odvisna od ponujene različice oziroma se celo strinja z vlagateljem, da je Bluetooth Low Energy (BLE) zasnovan za nizko porabo energije.

Naročnikovo zavzemanje za NFC komunikacijo je splošno in pavšalno tudi v delu, ki se nanaša na namen uporabe obeh tehnologij. Naročnik v tem delu navaja le, da se NFC pogosto uporablja za plačila (npr. bančne plačilne kartice), izmenjavo podatkov (npr. kontaktne informacije) in identifikacijo (npr. dostopne kartice), kar vse naj bi pomenilo, da je NFC tehnologija v splošnem bolj sprejeta za izmenjavo kritičnih informacij in s tem tudi varnejša od Bluetooth tehnologije. S tem v zvezi je vlagatelj prepričljivo pojasnil, da se tudi Bluetooth tehnologija uporablja za dostop - ne le do hotelov, apartmajev in podobno, ampak tudi do objektov kritične infrastrukture. Da je temu tako je nenazadnje razvidno tudi iz naročnikove referenčne zahteve, v skladu s katero so morali ponudniki izkazati vsaj tri reference digitalnega zaklepnega sistema s področja kritične infrastrukture na območju EU, torej pogoja, ki dopušča reference z obema vrstama tehnologij ob predpostavki, da so bile pridobljene na kritični infrastrukturi znotraj EU.

Kot že navedeno v tej obrazložitvi, se naročnik pri zavzemanju za zgolj NFC tehnologijo sklicuje predvsem na varnost njenega delovanja. Naročnik je v ta namen zahteval od ponudnikov, da mora biti komunikacija med mobilnim ključem in digitalnim cilindrom izvedena z uporabo

naprednih šifrirnih metod oziroma je zahteval, da mora biti vsaka komunikacija šifrirana z algoritmi, kot je to npr. AES-256. Med vlagateljem in naročnikom sicer ni spora, da AES tehnologija uporablja simetričen algoritem šifriranja, ki šifrira podatke, vendar pa se ni mogoče strinjati z naročnikom tudi v tem, da je bil v konkretnem primeru *»zaradi največje možne zaščite izbran AES-256«* - naročnik je namreč naveden algoritem navedel le primeroma, saj je izrecno zapisal, da mora biti vsaka komunikacija šifrirana z algoritmi, kot je to npr. AES -256. Naročnik je prav tako zahteval, da mora sistem za odpiranje digitalnih cilindrov nekaterih pomembnejših lokacij omogočati spletno avtentikacijo v realnem času ter da mora biti vsak dostop oziroma odklepanje in zaklepanje digitalnih cilindrov zabeležen v centralnem sistemu, zahteval pa je tudi, da mora biti zagotovljena revizijska sled v realnem času z možnostjo izpisov vseh dostopov, s čimer bo, kot je navedel, zagotovil popolni nadzor nad kritično infrastrukturo v realnem času. Navedenim varnostnim protokolom vlagatelj ni oporekal, kar pomeni, da jih je mogoče zagotoviti tudi s primerljivim digitalnim zaklepnim sistemom.

Nenazadnje vlagatelj upravičeno opozarja (o čemer med strankama ni spora), da imajo za razliko od NFC tehnologije, Bluetooth tehnologijo nameščeno vse pametne mobilne naprave in da v primeru dopustitve te tehnologije naročniku ne bi bilo potrebno dodatno naročati še 100 NFC obeskov (ključev), ki jih mora v obravnavanem primeru zagotoviti tistim uporabnikom, ki nimajo mobilne naprave z NFC tehnologijo. Glede na to, da je naročnik razpisal 500 digitalnih mobilnih ključev z letnimi licencami in 100 kosov uporabniških NFC obeskov, očitno vsak peti naročnikov uporabnik nima pametne mobilne naprave z NFC tehnologijo. Vlagatelj v zvezi s tem tudi opozarja, da se aplikacija za NFC obesek preko povezave Bluetooth poveže z obeskom za ključe K55S in tako uporablja Bluetooth komunikacijo, da NFC obesek uporablja Bluetooth komunikacijo, pa med vlagateljem in naročnikom tudi sicer ni sporno. Navedeno pa pomeni, da naročnik dopušča Bluetooth tehnologijo pri NFC ključu (obesku), ne dopušča pa je kot alternativne tehnologije pri odklepanju / zaklepanju preko mobilnih naprav.

Ravno tako so naročnikove navedbe neprepričljive tudi v delu, ki se nanašajo na vprašanje dopustitve fizičnih ključev (vlagatelj je kot enakovredna predlagal dva fizična ključa – *Protec2 Cliq* in *Assa Abloy Pulse*). Naročnik namreč navaja le, da predlagana ključa ne omogočata NFC brezstičnega odklepanja. Predlagana ključa je, tako naročnik, potrebno fizično vstaviti v cilinder, ki pa je lahko v zimskem času zamrznjen, poleg tega je možno vanj vstaviti karkoli in s tem onemogočiti odklepanje in zaklepanje. Ključa uporabljata Bluetooth tehnologijo za avtorizacijo prenos podatka v času odklepanja in zaklepanja ključavnice. Zlasti pa naročnik navaja, da želi zaklepni sistem, ki bi onemogočal izgubo ključev in posledično nedovoljene vstope - zatrjuje, da bi moral za en izgubljeni ključ zamenjati ves zaklepni sistem, ki se odklepa z izgubljenim ključem. S tem v zvezi vlagatelj pravilno opozarja, da gre tudi pri fizičnem NFC ključu za ključ in ne za mobilno napravo. Naročnik tako v obravnavanem primeru ne dopušča sistema brezbaterijskih elektromehanskih cilindričnih vložkov in elektromehanskega zaklepnega sistema, ki deluje na podlagi lastnega napajanja iz razloga, ker za svoje delovanje potrebujeta fizični ključ, dopušča pa 100 kosov fizičnega NFC ključa kot alternativo odklepanju in zaklepanju digitalnih cilindrov preko mobilne naprave. Poleg tega vlagatelj pravilno navaja, da se prav tako, kot se lahko izgubi ključ, lahko izgubita tudi telefon in NFC obesek. Poleg tega se lahko izgubljeni ključ z zaklepnega sistema tudi izbriše, kar pomeni, da iz tega razloga ni potrebno (kot to napačno navaja naročnik) zamenjati celotnega zaklepnega sistema, ki se odklepa z izgubljenim ključem. Zlasti pa v obravnavanem primeru vlagatelj tudi opozarja, da so *Assa Abloy Cliq* elektromehanski cilindri zasnovani posebej za uporabo na kritični infrastrukturi, da *Cliq* tehnologija omogoča delovanje v temperaturnem območju od -35°C do +85°C, ter da fizični ključi *Cliq* vključujejo napredne zaščitne mehanizme, ki preprečujejo vdor snega, ledu in umazanije v cilinder, kar zagotavlja zanesljivo delovanje tudi v najtežjih razmerah.

Državna revizijska komisija nadalje ugotavlja, da naročnik v postopku pravnega varstva prav tako ni navedel okoliščin, ki bi predstavljale strokovno utemeljene in objektivno opravičljive razloge za postavite tehnične zahteve, v skladu s katero bo dopustil le digitalne cilindre brez uporabe baterij oziroma digitalne cilindre, ki ne uporabljajo zunanjih virov energije. Tudi v tem delu so namreč naročnikove navedbe le splošne in pavšalne. Naročnik je navedel le, da morajo ključne komponente, kot je to cilinder, delovati v ekstremnih vremenskih razmerah, v čim večjem temperaturnem razponu, pri čemer temperatura zraka ni enaka temperaturi vrat, ki na soncu krepko preseže najvišjo izmerjeno temperaturo zraka v Sloveniji, nihanje temperatur in ekstremne temperature pa nižajo življenjsko dobo baterij. Vlagatelj v zvezi s tem zatrjuje, da zahtevano temperaturno območje (od -30°C do +50°C) ni ovira za delovanje digitalnih cilindrov z baterijami, navedeno pa potrjuje tudi dejstvo, da vlagatelj zahtevanemu temperaturnemu območju ne oporeka. Vlagatelj pri tem tudi pravilno navaja, da mobilni telefoni, ki so del zaklepnega sistema, ki ga razpisuje naročnik, ravno tako uporabljajo baterije, na polnilni akumulator / baterijo pa delujejo tudi NFC obeski, ki za validacijo in spreminjanje pravic, kot že navedeno, potrebujejo telefon in Bluetooth komunikacijo. Tudi NFC ključ je torej potrebno napajati oziroma ga v primeru, če ne bo napolnjen, uporabnik ne bo mogel uporabljati in dostopati do objekta. Poleg tega je temperaturno območje delovanja mobilnih naprav bistveno ožje od temperaturnega območja, ki je zahtevano za delovanje digitalnih cilindrov. Ob navedenem pa naročnikovemu argumentu, da želi v konkretnem primeru doseči neodvisnost od baterijskega ali omrežnega napajanja, ni mogoče slediti. Tudi digitalni zaklepni sistem, ki podpira NFC komunikacijo je torej odvisen od baterijskega ali omrežnega napajanja, saj za svoje delovanje potrebuje mobilne naprave, ki so odvisne od baterijskega, kot tudi od omrežnega električnega napajanja. Nenazadnje pa je vlagatelj tudi navedel, da so digitalni cilindri z baterijami po načinu delovanja enakovredni digitalnim centrom brez baterije in da samo napajanje ne vpliva na njihovo funkcionalnost. Navedel je tudi, da digitalni cilindri z baterijami zagotavljajo zanesljivo obliko zaklepanja in imajo dolgo življenjsko dobo, poleg tega je življenjska doba baterij izjemno dolga, pri čemer sistem uporabnika vnaprej opozori, kdaj je potrebna menjava.

Zadnji vlagateljev očitek se nanaša na naročnikovo tehnično zahtevo, v skladu s katero je lahko programska oprema postavljena bodisi na (naročnikovi) lastni strežniški infrastrukturi bodisi v oblaku na območju EU. Vlagatelj namreč v tem delu, kot že izhaja iz te obrazložitve, očita naročniku, da ni podal nobenih drugih podatkov, kar mu onemogoča pripravo dopustne, konkurenčne in primerljive ponudbe.

Naročnik je tekom pojasnjevanja razpisne dokumentacije oziroma na podlagi prejetih vprašanj potencialnih ponudnikov pojasnil, da je lahko programska oprema za upravljanje sistema digitalnega zaklepnega sistema nameščena bodisi na njegovi lastni strežniški infrastrukturi (SŽ-Infrastruktura, d.o.o.) ali v oblaku na območju EU, pri čemer naj ponudniki ponudijo boljšo tehnično in ekonomsko rešitev. Drugih podatkov v zvezi s tem naročnik ni podal, poleg tega je naročnik zadnji odgovor v zvezi s tem na Portalu javnih naročil objavil 6. 11. 2024, kar je po roku za postavljanje vprašanj (ta je potekel 29. 10. 2024), zato vlagatelj pravilno opozarja, da v zvezi z navedeno tehnično zahtevo ponudniki niso več mogli postavljati (nadaljnjih) vprašanj.

Naročnik v sklepu, s katerim je zavrnil zahtevek za revizijo, sicer pravilno navaja, da je odločitev, ali bo programska oprema za upravljanje z razpisanim sistemom nameščena na naročnikovi strežniški infrastrukturi ali v oblaku na območju EU, prepustil ponudnikom. Vendar pa je naročnik hkrati tudi zahteval od ponudnikov, naj ponudijo boljšo tehnično in ekonomsko rešitev, pri čemer ni navedel nobenih kriterijev, v skladu s katerimi bo presojal, katero rešitev je boljša v tehničnem in katera je boljša v ekonomskem smislu. Poleg tega naročnik ni podal nobenih podatkov o svoji strežniški strukturi (ni informacij o strojni opremi, omrežju, varnostnih politikah in programski opremi), zato vlagatelj upravičeno zatrjuje, da nima nobene podlage oziroma nobenih informacij, na podlagi katerih bi lahko ocenil »boljšo tehnično« in »boljšo ekonomsko« postavitev rešitve na

eno izmed obeh opcij, prav tako niti ne ve, kaj bi storil naročnik v primeru, ko bo rešitev nekega ponudnika »tehnično boljša«, rešitev drugega ponudnika pa »ekonomsko ugodnejša«. Odsotnost kakršnihkoli informacij pa onemogoča vlagatelju in ostalim ponudnikom, da bi lahko ponudili (konkurenčno) ponudbeno ceno za postavitev programske opreme oziroma da bi se sploh lahko odločili za eno izmed obeh možnosti. Kot pravilno opozarja vlagatelj, takšna netransparentna določila lahko vodijo v neenakopravno obravnavo ponudnikov, saj omogočajo arbitrarnost naročnika pri presoji ponudb. Če naročnik v zvezi s tehničnimi zahtevami ravna nepregledno oziroma tako, da ponudniki ne vedo, v kakšni obliki in vsebini so vključene v razpisno dokumentacijo in kaj naročnik sploh zahteva, naročnik ne more zagotoviti niti enakopravnega sodelovanja ponudnikov niti enakopravne presoje njihovih ponudb. Trditvam naročnika, da je v konkretnem primeru edino merilo cena in da ni predvidel nikakršnega primerjanja in ocenjevanja ponudb v zvezi s ponujeno lokacijo programske opreme zato ni mogoče slediti, saj je določitev same lokacije programske opreme s strani ponudnika neposredno povezana z naročnikovimi tehničnimi zahtevami, ki niso bile jasno podane, navedeno pa nedvomno vpliva tudi na oblikovanje ponudbene cene. Poleg tega naročnik brez jasnih informacij o tehničnih zahtevah ustvarja tudi okolje, ki onemogoča oddajo ne le konkurenčnih in dopustnih ponudb, pač pa tudi medsebojno primerljivih ponudb.

Ob vsem navedenem je treba ugotoviti, da naročnik v zvezi z zahtevama, ki kot ustrezno sprejema le NFC tehnologijo in le brezbaterijske digitalne cilindre, ni uspel izkazati objektivno opravičljivih in strokovno utemeljenih razlogov, ki bi takšno omejevanje opravičili. Poleg tega je vlagatelj z zahtevkom za revizijo uspel tudi izkazati, da je naročnikova zahteva, ki se nanaša na namestitev programske opreme bodisi na naročnikovi infrastrukturi bodisi v oblaku znotraj EU ni dovolj jasna in dorečena in ne omogoča oddaje konkurenčnih, dopustnih in primerljivih ponudb. Z opisanim je naročnik posegel v načelo transparentnosti (6. člen ZJN-3), kršil pa je tudi določilo šestega odstavka 68. člena ZJN-3 ter posledično načelo zagotavljanja konkurence med ponudniki (5. člen ZJN-3), načelo enakopravne obravnave ponudnikov (7. člen ZJN-3) in načelo sorazmernosti (8. člen ZJN-3).

Ker je v konkretnem primeru rok za prejem ponudb že potekel (15. 11. 2024), poleg tega je naročnik prejete ponudbe že odprl, ugotovljene kršitve pri oblikovanju določb dokumentacije v zvezi z oddajo javnega naročila ni mogoče sanirati z milejšim ukrepom (tj. z delno razveljavitvijo postopka), zato je Državna revizijska komisija postopek oddaje javnega naročila razveljavila v celoti.

V skladu s tretjim odstavkom 39. člena ZPVPJN daje Državna revizijska komisija naročniku napotke za pravilno izvedbo postopka. Ker je Državna revizijska komisija razveljavila celoten postopek oddaje javnega naročila, naročnika napotuje, naj v primeru, če se bo odločil izvesti nov postopek oddaje javnega naročila, pri oblikovanju določb dokumentacije v zvezi z oddajo javnega naročila ravna v skladu z ZJN-3 in temeljnimi načeli javnega naročanja, pri tem pa naj upošteva tudi ugotovitve Državne revizijske komisije, kot izhajajo iz tega sklepa.

S tem je utemeljena odločitev Državne revizijske komisije iz 1. točke izreka tega sklepa.

Vlagatelj je v obravnavanem primeru priglasil naslednje stroške: takso v višini 2.000,00 EUR, za sestavo zahtevka za revizijo 9.000 točk ter materialne stroške po tretjem odstavku 11. člena Odvetniške tarife. Zahteval je tudi povrnitev 22 % DDV. Poleg tega je za sestavo vloge z dne 4. 12. 2024, s katero se je opredelil do naročnikove odločitve o zahtevku za revizijo priglasil še 9.000 točk ter materialne stroške po tretjem odstavku 11. člena Odvetniške tarife in DDV.

Če je zahtevek za revizijo utemeljen, mora naročnik iz lastnih sredstev vlagatelju povrniti potrebne stroške, nastale v predrevizijskem in revizijskem postopku, vključno s takso (tretji odstavek 70.

člena ZPVPJN). Državna revizijska komisija je vlagatelju (skladno z Odvetniško tarifo - Uradni list RS, št. 2/15 s spremembami; v nadaljevanju: OT) kot potrebne priznala naslednje stroške: strošek plačane takse v višini 2.000,00 EUR, strošek odvetniške storitve za sestavo zahtevka za revizijo v višini 1.800 točk (prva točka tar. št. 44 OT), kar ob upoštevanju vrednosti točke (tj. 0,60 EUR) in 22 % DDV znaša 1.317,60 EUR, in izdatke v pavšalnem znesku po tretjem odstavku 11. člena OT (in sicer 2 % od skupne vrednosti storitve do 1.000 točk in 1 % od presežka nad 1.000 točk, t.j. 800 točk) v višini 28 točk, kar ob upoštevanju vrednosti točke (tj. 0,60 EUR) in 22 % DDV znaša 20,50 EUR.

Državna revizijska komisija je tako vlagatelju kot potrebne priznala stroške v višini 3.338,10 EUR. Naročnik je dolžan vlagatelju povrniti stroške pravnega varstva v roku 15 dni od prejema tega sklepa, po izteku tega roka pa z zakonskimi zamudnimi obrestmi do plačila. Razliko do priglašenih stroškov za sestavo zahtevka za revizijo (in s tem povezane izdatke po 11. členu Odvetniške tarife) je Državna revizijska komisija zavrnila, saj za njeno priznanje, glede na vrednost spora (to je ocenjene vrednosti predmetnega javnega naročila brez DDV), podlage v Odvetniški tarifi ni najti. Državna revizijska komisija vlagatelju tudi ni priznala priglašenih stroškov za sestavo vloge, s katero se je opredelil do navedb naročnika v odločitvi o zahtevku za revizijo (vloga z dne 4. 12. 2024) in v zvezi z njo priglašenih materialnih stroškov, saj ti v konkretnem primeru niso bili potrebni (peti odstavek 70. člena ZPVPJN v povezavi z osmim odstavkom istega člena, pa tudi drugi odstavek 2. člena OT). Navedbe v navedeni vlogi namreč niso pripomogle ne k hitrejši ne k enostavnejši rešitvi zadeve.

Naročnik mora vlagatelju znesek v višini 3.338,10 EUR, v skladu z drugim in tretjim odstavkom 313. člena Zakona o pravdnem postopku (Uradni list RS, št. 26/1999, s spremembami), v povezavi s prvim odstavkom 13. člena ZPVPJN, povrniti v roku 15 dni od vročitve tega sklepa, v primeru zamude skupaj z zakonskimi zamudnimi obrestmi, ki tečejo od prvega dne po poteku roka za izpolnitev obveznosti do plačila.

S tem je utemeljena odločitev Državne revizijske komisije iz 2. točke izreka tega sklepa.

Pravni pouk: Zoper to odločitev upravni spor ni dovoljen.

Predsednik senata:
Marko Medved, univ. dipl. prav.
član Državne revizijske komisije

Vročiti:
- naročnik,
- vlagatelj - po pooblaščencu,
- Republika Slovenija, Ministrstvo za javno upravo.

Vložiti:
- v spis zadeve, tu.