

TEHNIČKA SPECIFIKACIJA

Redni broj	Element / komponenta	Minimalni tehnički zahtjev	Referenca na stranicu iz kataloga ili druge tehničke dokumentacije ili izjave
1.	Vrsta uređaja	Uređaj za naplatu i validaciju prijevoznih karata - validatori	
1.1.	Centralna jedinica	OCU Procesorska platforma mora omogućavati nematan rad aplikacije za validaciju, obradu EMV transakcija, očitanje i obradu QR/2D kodova, lokalnu pohranu transakcijskih podataka te sigurnu komunikaciju sa središnjim sustavom. Uređaj mora imati viližegirani procesor industrijske izvedbe, ARM ili jednakovrijedne arhitekture. Radna memorija min. 1GB Pohrana podataka: Interna memorija najmanje 8 GB za aplikacije, konfiguraciju, sigurnosne zapise i lokalnu pohranu transakcijskih podataka. Ako se koristi dodatna izmjenjiva memorija, mora biti zaštićena od neovlaštenog pristupa i primjerena za rad u vozilu. Dodatna izmjenjiva memorija: Uređaj može podržavati dodatnu izmjenjivu memoriju, pod uvjetom da je pristup zaštićen i da se podaci pohranjuju u skladu sa sigurnosnim zahtjevima sustava. OS: Naručitelj nema preferiran operativni sustav. Ponudni operativni sustav mora omogućavati rad ponudnog aplikativnog rješenja, sigurnosne nadogradnje tijekom upravnog/jamstvenog razdoblja te integraciju s postojećim sustavom automatike naplate prijevoza putem dokumentarnih sučelja, protokola ili prilagodbi uključene u ponudu.	
1.2.	Zaslon	Igr: zaslon u boji Dijagonalno min 7" (177,8 mm) Razlučivost: najmanje 800 x 480 piksela. Zaslon mora omogućavati jasan prikaz statusa validacije, korisničkih poruka, grafičkih oznaka i viližegiranih obavijesti u uvjetima uporabe u javnom prijevozu. Visa razlučivost, npr. 1024 x 600 ili jednakovrijedna prihvativna je ako je standardno podržana ponudnim uređajem. Osvjetljav na dodir: tehnologija kapacitivni Zaštita: Zaslon mora biti zaštićen ojačanim/kaljenim ili jednakovrijednim zaštitnim staklom primjerenim za uporabu u javnom prijevozu, otpornim na udarčane udarce, habanje i vandalizam. Svojstva se dokazuju tehničkom dokumentacijom proizvođača ili odgovarajućim ispitnim izvještajem.	
1.3.	Zvučnik	Zvučnik: Da	
1.4.	Čitač pametnih kartica i bankovnih kartica	Rfid/NFC sučelja mora podržavati najmanje ISO/IEC 14443 Type A/B te NFC funkcionalnosti potrebne za očitavanje podržanih medija. Uređaj mora podržavati MIFARE DESFire EV1, EV2, EV3 ili jednakovrijednu sigurnu beskontaktnu kartičnu tehnologiju koja omogućuje rad s aplikacijama i sigurnosnim mehanizmima postojećeg ili budućeg sustava. Naručitelj mora imati u mogućnosti povezati čitačica Contactless Level 1 i Level 2 odobrenja/certifikate za relevantne kontaktless funkcionalnosti i kemele potrebne za ponudno rješenje. Ponudno rješenje mora omogućavati provedbu end-to-end testiranja i certifikacijskih postupaka koje zahtijevaju kartične sheme, payment provider, acquirer i/ili drugi nadležni sudionici platnog procesa za implementaciju EMV open-loop naplate u javnom prijevozu. Uređaj/rješenje mora podržavati suvremene kriptografske algoritme i protokole primjerene za zaštitu podataka i komunikacije, najmanje AES-128/256, 3DES samo ako je nužan radi kompatibilnosti sa zaštićenim sustavom ili kriptičnim aplikacijama te SHA-256 ili sigurniji hash algoritam. Sigurna komunikacija mora koristiti TLS 1.2 ili noviji, odnosno jednakovrijednan sigurni komunikacijski protokol prihvatljiv za ponudnu arhitekturu i sukladan zahtjevima payment provider/acquirera. Kriptografski mehanizmi moraju biti usklađeni sa zahtjevima kartičnih shema, sigurnosnih standarda i sigurnosne arhitekture ponudnog rješenja. Uređaj mora imati najmanje 1 SAM utro kompatibilna s karticama koje koristi postojeći sustav. Naručitelj ili jednakovrijednan sigurnosni mehanizam koji osigurava sigurno spremanje ključeva, kriptografske operacije i pristup kartičnim aplikacijama. Ponuditelj je dužan isporučiti odgovarajući broj SAM modula ili jednakovrijednih sigurnosnih modula potrebnih za rad ponudnog rješenja te osigurati sve licence, certifikate, instalacije, aktivaciju i prava korištenja potrebna za njihovu funkcionalnost tijekom jamstvenog razdoblja. Jednakovrijedni sigurnosni mehanizam mora osigurati najmanje istu razinu zaštite ključeva, kriptografskih operacija, kontrole pristupa kartičnim aplikacijama i mogućnosti sigurnog životnog ciklusa ključeva kao SAM moduli. Svi navedeni troškovi moraju biti uključeni u cijenu ponude. Rješenje mora omogućavati sigurnu zamjenu, obnovu ili otkazivanje postojećih ključeva u bilo koje vrijeme. Uređaj/rješenje mora podržavati implementaciju EMV open-loop sustava naplate u javnom prijevozu. Uređaj mora imati ili omogućavati važeća EMVCo Contactless Level 1 i Level 2 odobrenja/certifikate za relevantne kontaktless funkcionalnosti, kemele i konfiguraciju potrebnu za ponudno rješenje. Rješenje mora omogućavati prihvati beskontaktnih platnih instrumenata kartičnih shema koje će se koristiti u implementiranom sustavu, najmanje Visa i Mastercard, odnosno drugih EMVCo kompatibilnih kartičnih shema koje su podržane od payment provider/acquirera. Aktivacija dodatnih kartičnih shema mora biti moguća konfiguracijom, nadogradnjom softvera, instalacijom odgovarajućih kemele/certifikata ili drugim prilagodbama bez zamjene hardvera uređaja. Rješenje mora omogućavati prihvati tokeniziranih EMV platnih instrumenata pohranjenih u digitalnim novčanicama na mobilnim uređajima i nosivim uređajima, uključujući Apple Pay, Google Pay, Samsung Wallet ili jednakovrijedne usluge, u skladu s pravilima kartičnih shema i payment provider/acquirera. Uređaj, odnosno platni modul, Secure Card Reader, terminala ili druga komponenta ponudnog rješenja koja prihvaća, obrađuje ili štiti osjetljive kartične podatke, mora imati važeće PCI PTS POI odobrenje/certifikat za ponudni model i relevantnu kartičnu uređaja, važeće u trenutku isporuke. Ako ponuditelj nudi arhitekturu u kojoj PCI PTS POI ne primjenjuje na sam validator, dužan je u ponudi jasno opisati arhitekturu platnog rješenja, navesti koja komponenta je certificirana ili na koji se drugi način ispujaju zahtjevi kartičnih shema, banke prihvatitelja/acquirera i pružatelja platnih usluga. Ponuditelj mora osigurati da isporučeno rješenje podržava postupke testiranja, certifikacije i odobrenja koje zahtijevaju kartične sheme, payment provider, acquirer i/ili drugi nadležni sudionici platnog procesa za produkcijsku implementaciju EMV open-loop naplate u javnom prijevozu. Svi troškovi licenci, certifikata, instalacije, konfiguracije i aktivacije potrebni za rad ponudnog rješenja moraju biti uključeni u ponudu, osim ako su uključeni u cijenu dobivena izvan predmeta nabave.	
1.5.	'Open-loop' funkcionalnosti	Čitač mora podržavati očitavanje 2D barkodova i QR kodova s papirnatih i digitalnih medija, uz vrijeme očitavanja primjerno masovnoj validaciji putnika. Konkretno udaljenosti i kutni očitava prihvaća se prema tehničkoj dokumentaciji proizvođača, uz obvezno funkcionalno testiranje u vozilu ili na testnom okruženju. Naručitelj. Podržano napajanje 24 V DC. Uređaj mora biti kompatibilan s električnom instalacijom vozila. Nominalna i vrhina potrošnja moraju biti iskazane u tehničkoj dokumentaciji proizvođača. Ako se za postotjevu instalaciju primjenjuje ograničenje potrošnje, ponudni uređaj mora biti usklađen s raspoloživim kapacitetom napajanja u vozilu i ne smije zahtijevati izmjene izvan predmeta nabave. Zaštita od obrnutog polara: Da Zaštita od prevelikog napona: Da Zaštita od kratkotrajnog preopterećenja: Da	
1.6.	Barcode-QR kod čitač	Čitač mora podržavati očitavanje 2D barkodova i QR kodova s papirnatih i digitalnih medija, uz vrijeme očitavanja primjerno masovnoj validaciji putnika. Konkretno udaljenosti i kutni očitava prihvaća se prema tehničkoj dokumentaciji proizvođača, uz obvezno funkcionalno testiranje u vozilu ili na testnom okruženju. Naručitelj. Podržano napajanje 24 V DC. Uređaj mora biti kompatibilan s električnom instalacijom vozila. Nominalna i vrhina potrošnja moraju biti iskazane u tehničkoj dokumentaciji proizvođača. Ako se za postotjevu instalaciju primjenjuje ograničenje potrošnje, ponudni uređaj mora biti usklađen s raspoloživim kapacitetom napajanja u vozilu i ne smije zahtijevati izmjene izvan predmeta nabave.	
1.7.	Napajanje	Zaštita od obrnutog polara: Da Zaštita od prevelikog napona: Da Zaštita od kratkotrajnog preopterećenja: Da	
1.8.	Povezivost	Najmanje 10/100 Mbps Ethernet, TCP/IP komunikacija, uz podršku sigurnih protokola potrebnih za komunikaciju s OCU-om i/ili centralnim sustavom. Validator mora omogućavati komunikaciju s OCU-om ili centralnim sustavom, ovisno o ponudnom arhitekturi rješenja. Ako validator nema vlastitu mobilnu/WiFi komunikaciju, ponuditelj mora osigurati da se via komunikacija prema centralnom sustavu, uključujući prijenos transakcija, konfiguracija, sigurnosnih zapisa i ažuriranja, otvaranje autem OCU-a ili druge usluge uključene u ponudu. Bluetooth 4.2 ili noviji, uz mogućnost sigurnog isklučivanja ili ograničavanja pristupa	
1.9.	Kućište	Kućište mora biti izrađeno od materijala otpornog na uvjete uporabe u javnom prijevozu, uključujući udarce, vibracije, UV zračenje, sredstva za čišćenje, povišenu temperaturu i vjerojatno širenje plamena. Svojstva se dokazuju tehničkom dokumentacijom proizvođača, certifikatom ili jednakovrijednim dokazom. Maks. dimenzije (WxDxH): 320 x 170 x 140mm IP zaštita: min. IP54 Radna temperatura: od -20°C do +60°C	
1.10.	Oprema	Oružaj za lipku promjera 30-40mm	
1.10.	Jamstvo	Minimalno 24 mjeseca na lokaciji naručitelja.	
2.	Vrsta uređaja	Centralno računalo OCU	
2.1.	Dimenzije:	Do približno 80x180x230 mm, prilagođene raspoloživom prostoru ugradnje. Dimenzije moraju omogućiti ugradnju na postojeće pozicije u vozilima bez izmjene konstrukcije vozila. Ponudene dimenzije moraju biti dokazane tehničkom dokumentacijom i potvrđene u fazi ugradnje/testiranja.	
2.2.	Nazivni napon:	24 V	
2.3.	Opseg radnog napona:	od 16 V do 32 V	
2.4.	Maksimalna struja:	do 2A	
2.5.	Radna temperatura:	od -30°C do +60°C	
2.6.	Komunikacija	Mreža: Da Komunikacija: IEEE 802.11 a/b/g/n/ac ili novije. OCU mora imati integrirani LTE4G modem ili mogućnost povezivanja na LTE4G komunikaciju modulu uključenu u predmet ponude. Podrška za 5G može biti ponuđena kao dodatna ili buduća mogućnost, ali ne smije biti uvjet koji isključuje rješenja koja osiguravaju traženu funkcionalnost putem 4G/LTE mreže. OCU/rješenje mora omogućavati komunikaciju s centralnim sustavom. Naručitelj putem postojećeg SOAP sučelja ili drugog dokumentiranog i sigurnog protokola kompatibilnog s postojećim sustavom. Naručitelj, pri čemu su sve potrebne prilagodbe, konfiguracije i testiranje uključeni u ponudu. Komunikacija s ugrađenim računalom sustava za nadzor i upravljanje prometom u vozilu mora biti omogućena putem IBS IP protokola (VDV 301) ili jednakovrijednog protokola koji koristi postojeći/ciljani sustav. Naručitelj. Sva oprema, licence, konfiguracije i prilagodbe potrebne za funkcionalnu integraciju moraju biti uključene u ponudu. Komunikacija s validatorima mora se odvijati putem TCP/IP protokola uz korištenje sigurnih prijenosnih mehanizama kao što su DTLS, HTTPS/TLS ili jednakovrijedni sigurni protokoli. Korištenje FTP-a isključeno je isključivo ako je nužno radi interoperabilnosti sa zaštićenim sustavom. Naručitelj, uz odgovarajuće kompetencijske sigurnosne mjere i odobrenje. Naručitelja. Ethernet port za servisu i opcu upotrebu	
2.7.	Potrebni priključci	SAM utor ili jednakovrijednan sigurnosni modul potreban za funkcionalnost ponudnog rješenja, ako je primjenjivo. Utor za SIM karticu, GSM ili jednakovrijednan mehanizam za pristup mobilnoj LTE4G mreži, ako je komunikacijski modul dio ponudnog rješenja. USB priključak ili jednakovrijedna servisa/prijenosna sučelja potrebna za instalaciju, servisiranje, konfiguraciju i prijenos podataka, prema arhitekturi ponudnog rješenja. Uređaj mora omogućavati hardverski reset i softversko ponovno pokretanje/administrativno upravljanje na način izveden od proizvođača, uz zaštitu od neovlaštenog pristupa. Standardni antenski konektor odgovarajući ponudnom WiFi/LTE anteni i uvjetima ugradnje u vozilu, svi potrebni antenski kabeli, adaptori i pribor moraju biti uključeni u ponudu. Priključak ili komunikacijsko sučelje potrebno za povezivanje s ugrađenim računalom sustava za nadzor i upravljanje prometom. Naručitelj, uključujući sve potrebne kabele, adaptere, licence i konfiguracije.	
2.8.	Kompatibilnost s postojećim sustavom naplate	Ponudni uređaji moraju omogućiti integraciju s postojećim sustavom automatike naplate prijevoza. Naručitelj, uključujući razmjenu podataka i funkcionalnosti koje koristi postojeći sustav, bez potrebe za izmjenama drugih ključevih komponenti sustava izvan predmeta nabave. Kompatibilnost se dokazuje tehničkom dokumentacijom, opisom arhitekture integracije, izvjom ponuditelja/proizvođača te funkcionalnim testiranjem u testnom okruženju ili vozilu. Naručitelj.	
2.9.	Jamstvo	Minimalno 24 mjeseca na lokaciji naručitelja. Tipkom jamstva ponuditelj mora osigurati otkrivanje kvara na lokaciji. Naručitelj ili isporučitelj funkcionalno jednakovrijednog zamjenjivog uređaja. Ponuditelj mora zapoliti postupanje po prigodi kvara naknadno slijedeći radni dan od zapijanja prijave.	
2.10.	Dokazivanje jednakovrijednosti	Ako je u ovoj tehničkoj specifikaciji navedena određena norma, tehnologija, protokol, kartična shema, proizvod, tip, model, pretežba ili komercijalni naziv, ispušten je u ponudi jednakovrijedno rješenje. Jednakovrijednost se dokazuje tehničkom dokumentacijom proizvođača, certifikatima, ispitnim izvješćima, opisom arhitekture rješenja, izvjom proizvođača/ponuditelja ili funkcionalnim testiranjem u okruženju. Naručitelj, ako je primjenjivo. Jednakovrijedno rješenje mora osigurati istu ili višu razinu funkcionalnosti, sigurnosti, interoperabilnosti, održivosti i kompatibilnosti s postojećim sustavom. Naručitelja. Uređaj/rješenje mora podržavati mehanizam sigurnog pokretanja ili jednakovrijednan mehanizam kojim se sprječava pokretanje neovlaštenog ili neovjerenog softvera. Uređaj/rješenje mora podržavati sigurnu pohranu i obnovu digitalnih certifikata te autentifikaciju prema centralnom sustavu korištenjem sigurnih protokola.	
2.11.	Sigurnost i upravljanje uređajem	Uređaj/rješenje mora evidencirati sigurnosne, transakcijske, operativne i administrativne zapise, pri čemu zapisi moraju biti zaštićeni od neovlaštenih izmjena i dostupni centralnom sustavu. Rješenje mora omogućavati centralno upravljanje uređajima, nadzor statusa uređaja i sigurnu udaljenu instalaciju softvera/firmwarea, ako je takva funkcionalnost predviđena ponudnom arhitekturom.	