AGENCIJA ZA KOMERCIJALNU DJELATNOST proizvodno, uslužno i trgovačko d.o.o. Savska cesta 31, 10000 Zagreb OIB: 58843087891	Evidencijski broj:1/INV/OPN
I. Pojašnjenje i izmjena Poziva za dostavu ponuda	

Broj: 6/2026-13

Zagreb, 12. 2. 2026.

SVIM ZAINTERESIRANIM
GOSPODARSKIM SUBJEKTIMA

Sukladno zaprimljenim upitima gospodarskih subjekata i točkama 3. i 10. Poziva za dostavu ponuda u otvorenom postupku nabave „USLUGA RAZVOJA I IMPLEMENTACIJE SUSTAVA ZA PRAĆENJE PRIJEVOZA OPASNIH TVARI U CESTOVNOM PROMETU E-ADR“, Naručitelj pojašnjava i mijenja Poziv za dostavu ponuda kako slijedi:

1. UPIT

Predmetnim nadmetanjem gradi se državna digitalna platforma za prijevoz opasnih tvari (e-ADR). Za takav vid posla dobavljači usluga i rezultantni digitalni proizvod trebaju zadovoljiti najviše zahtjeve. Svjetski standardi vezani za kriterije prihvatljivosti digitalnih proizvoda su ISO 15489 i ISO30301, a za usluge dobavljača ISO 20000 i ISO 27001.

Da li se podrazumijeva da dobavljači moraju zadovoljiti te standarde, a da njihovi certifikati moraju biti izdani od strane certifikacijskih kuća koje su registrirane kod HAA te ih treba odgovarajuće uključiti u DoN?

1. odgovor

Pozivom za dostavu ponuda nije propisana obveza dokazivanja posjedovanja navedenih normi i certifikata od strane ponuditelja. Naručitelj će usklađenost rješenja sa zahtjevima sigurnosti, upravljanja i dokumentacije ocjenjivati kroz isporučenu dokumentaciju, provjerljive tehničke dokaze i rezultate testiranja/validacije, a prihvat će se provoditi temeljem stvarnih rezultata (zapisnici o testiranju, dokaz provedenih kontrola, izvještaji i sl.), a ne temeljem deklaracija. U okviru projekta predviđena je i neovisna validacija/verifikacija isporuka te se uredno izvršenje potvrđuje zapisnicima temeljem pozitivnih nalaza verifikatora.

2. UPIT

1. pitanje

U dokumentaciji se spominje dokument “Procjena analitičkih kapaciteta i nadogradnje AFFINIS” kao referentni izvor za arhitekturu i dizajn (10. Referentni izvori i standardi za provedbu projekta). S obzirom da navedeni dokument ne nalazimo, molimo za dostavu istog.

Financira Europska unija
NextGenerationEU

1. odgovor

AFFINIS je zasebna analitička platforma koja nije predmet ove nabave te se u okviru ovog postupka ne nabavlja niti nadograđuje AFFINIS kao sustav (uključivo sizing hardvera, data-engineering pipeline, ETL/ELT transformacije i ostale analitičke obrade koje su u nadležnosti tima za AFFINIS). Navedeni dokument je statističko-analitički materijal izrađen isključivo za potrebe procjene kapaciteta i planiranja resursa AFFINIS platforme te ne sadrži zahtjeve koji utječu na opseg, arhitekturu ili izvedbu sustava eADR niti je potreban za izradu usporedive ponude.

Predmet nabave je razvoj i implementacija sustava eADR te isporuka analitičkog i izvještajnog dijela eADR-a isključivo na način opisan u Tehničkim specifikacijama Poziva za dostavu ponuda (minimalni skup pokazatelja/izvještaja i pripadni operativni zapisi), uz uspostavu stabilnog i dokazivog podatkovnog toka prema AFFINIS-u u obliku kuriranih i strukturiranih skupova podataka (t. 5.4.4 Tehničke specifikacije za razvoj i implementaciju sustava e-ADR). Time se osigurava da se podaci iz eADR-a mogu sinkronizirati prema AFFINIS-u, bez zahtjeva da Izvođač razvija ili mijenja AFFINIS analitičku platformu.

Slijedom navedenog, traženi dokument "Procjena analitičkih kapaciteta i nadogradnje AFFINIS-a za eADR" nije nužan za izradu usporedive ponude jer ne mijenja niti proširuje opseg integracije i razmjene podataka koji je već definiran u Tehničkim specifikacijama (osobito t. 5.4.4 Tehničke specifikacije za razvoj i implementaciju sustava e-ADR i povezane isporuke/testovi).

2. pitanje

U poglavlju "1.13. eFTI Mock/Simulator za DEV i TEST okruženja" zahtjeva se implementacija mock servisa uz navođenje specifikacije mock-a za eFTI. Međutim, postoji još niz vezanih sustava na e-ADR koji se navode u dokumentaciji, uz dodatne servisa koje tek treba definirati. Za sve navedene integracije molimo odgovor hoće li biti spremne do početka razvoja s pripadnom dokumentacijom ili se i one planiraju riješiti preko mock-ova (u tom slučaju molimo specifikaciju i za navedene servise radi detaljnije procjene angažmana).

2. odgovor

eFTI integracija je ključni standardizirani integracijski tok u okviru eADR-a te će do trenutka kada integracija postane potrebna za razvoj i testiranje biti osigurane odgovarajuće specifikacije i/ili testno okruženje, odnosno simulator kada stvarni servisi nisu dostupni.

Za postojeće sustave razmjene podataka (npr. SOTAH i AFFINIS) integracijski obrasci i razmjena su već razrađeni i standardizirani, te se očekuje uobičajena implementacija integracijskih točaka bez posebne kompleksnosti izvan onoga što je definirano u Tehničkim specifikacijama predmetnog Poziva za dostavu ponuda.

Ostali registri/izvori podataka koji se eventualno koriste (npr. registri dozvola, ovlaštenja, radionica, certifikata i sl., ako su primjenjivi) su po prirodi manje kompleksni, pretežito "generičkog" karaktera (identifikatori, statusi, osnovni atributi) te ne predstavljaju opterećenje usporedivo s eFTI tokom. Ako pojedini vanjski servis u trenutku razvoja nije dostupan, Naručitelj će osigurati mock/simulator specifikaciju dovoljnog opsega za razvoj i testiranje, a prijelaz na stvarne servise provest će se kroz planirane integracijske testove.

3. pitanje

Financira Europska unija NextGenerationEU

Korištenje mock servisa ne garantira ispravnost integracija pri migraciji na stvarne servise (navedeno nepostojanje specifikacija za ostale mock servise, ograničenja u opsegu podataka, smanjen skup testnih scenarija…), te povećava vjerojatnost kasnijih dorada integracija što može rezultirati neplaniranim angažmanima i potencijalnim probijanjem rokova – molimo potvrdu da se u tim (ali i drugim) opravdanim slučajevima naknadnih dorada funkcionalnosti i integracija, rokovi mogu prilagođavati u skladu s realno izvedivima - bez ugovornih posljedica za Izvođača.

3. odgovor

Ispravnost integracija i funkcionalnosti dokazuje se kroz unaprijed definirane verifikacijske/validacijske postupke, scenarije i kriterije prihvata. Mock/simulator je razvojni alat za slučajeve kada vanjski sustav nije dostupan, a prelazak na stvarne servise provodi se kroz planirane integracijske testove i regresiju.

Rokovi i eventualna prilagodba rokova uređuju se ugovorom i mehanizmom upravljanja promjenama, na temelju dokumentiranih okolnosti i objektivno provjerljivih činjenica (npr. nedostupnost vanjskog okruženja, promjena specifikacije vanjskog servisa, odgoda pristupa ili testnih podataka). U takvim slučajevima očekuje se da Izvođač bez odgode prijavi rizik, predloži mitigacije i postupi po dogovorenom planu.

Napominje se da se verifikacija (dokaz ispunjenja zahtjeva) razlikuje od puštanja u produkciju, gdje je moguće da se pojave operativni incidenti; od Izvođača se očekuje prioritetno i žurno otklanjanje nedostataka sukladno ugovorenoj podršci i SLA.

4. pitanje

Molimo potvrdu da su navedene aktivnosti/uloge koje se povremeno spominju u natječajnoj dokumentaciji osigurane od strane Naručitelja, s obzirom da nije drugačije navedeno: GDPR compliance, aktivnosti koje uobičajno obavlja DPO (Data Protection Officer), dodatno DPIA (Data Protection Impact Assessment) i Pravnik (licencni ugovor).

4. odgovor

Aktivnosti formalnog usklađenja, uključujući ulogu službenika za zaštitu podataka (DPO) te donošenje i odobravanje DPIA i pravnih akata/ugovornih rješenja, osigurava Naručitelj. Izvođač je obvezan pružiti punu stručnu i tehničku podršku za potrebe usklađenja, uključujući: opis obrada i tokova podataka, tehničke i organizacijske mjere, prijedlog kontrola, evidencije/logove koji su potrebni za dokazivost te suradnju pri procjeni rizika i definiranju mjera zaštite podataka.

5. pitanje

U poglavlju 4.2 (Zahtjevi za IT stručnjake i uvjeti stručne sposobnosti) se navodi: „Ključne uloge na strani Izvođača uključuju stručnjaka za poslovnu analizu i modeliranje procesa, stručnjaka za arhitekturu informacijskog sustava, stručnjaka za integracije i razmjenu podataka te stručnjaka za informacijsku sigurnost i usklađenost“. U nastavku tog poglavlja stručnjaci za poslovnu analizu i modeliranje procesa, te arhitekturu informacijskog sustava, nisu navedeni u popisu 11 potrebnih stručnjaka. Kasnije se u tekstu spominje i stručnjak za vođenje projekta. Očekuje li se da te uloge obavlja netko od navedenih 11 stručnjaka, jesu li to možda dodatne uloge Izvođača (uključuju li i voditelja projekta), ili se pak očekuje da će te uloge biti odgovornost Naručitelja?

5. odgovor

Financira Europska unija NextGenerationEU

U ovom postupku nabave ne zahtijeva se imenovanje niti dokazivanje zasebnih stručnjaka na strani Izvođača za uloge poslovne analize/modeliranja procesa, arhitekture informacijskog sustava niti vođenja projekta. Navedene uloge su spomenute isključivo radi boljeg razumijevanja ukupne organizacije rada na projektu. Te uloge i odgovornosti osigurava Naručitelj i nisu predmet ove nabave, ne dostavljaju se u ponudi kao stručnjaci Izvođača, ne dokazuju se kroz uvjete stručne sposobnosti i ne utječu na bodovanje. Za sve uloge koje su predmet ove nabave traženi minimalni uvjeti i dodatni uvjeti bodovanja su jasno navedeni u Pozivu za dostavu ponuda te ponuditelj u ponudi dostavlja dokaze isključivo za te uloge.

Sukladno navedenom, mijenja se tekst Priloga II. Tehnička specifikacija za razvoj i implementaciju sustava e-ADR koji je predmet ovog upita i sada glasi: *Ključne uloge na strani **Naručitelja** uključuju stručnjaka za poslovnu analizu i modeliranje procesa, stručnjaka za arhitekturu informacijskog sustava, stručnjaka za integracije i razmjenu podataka te stručnjaka za informacijsku sigurnost i usklađenost s NIS2 i drugim relevantnim propisima.*

6. pitanje

Molimo potvrdite da su sve komercijalne licence potrebne za razvoj predmeta ponude osigurane od strane Naručitelja (Razvojni alati, Baza podataka, Application server, Monitoring alati, Backup software…).

6. odgovor

Okruženje za razvoj/test i produkcijski rad bit će osigurano u infrastrukturnom okruženju Naručitelja, a korištenje konkretnih proizvoda/alata nije unaprijed definirano. Naručitelj će osigurati potrebne komercijalne licence za komponente koje su nužne za rad rješenja u okruženju Naručitelja, uz uvjet da Izvođač pravodobno specificira licencne potrebe odabrane implementacije (uključivo popis third-party komponenti, verzije i licencne modele) te dostavi potpunu licencnu dokumentaciju. Time se osigurava usporedivost ponuda (bez nametanja točno određenih alata) te kontrola licencnih obveza i troškova tijekom implementacije.

7. pitanje

U dokumentu se navodi „Faza 3: Integracije i napredne funkcionalnosti: Implementirati Analytics i Reporting module“, kao i „Dokument mora definirati minimalni skup izvještaja i pokazatelja koji se smatraju obveznima za osnovno izvještavanje: volumeni provjera, volumeni pošiljaka s DG setom, ishodi nadzora, osnovne metrike integracija i opterećenja (npr. broj dohvaćanja payload-a), te osnovni sigurnosni pokazatelji (npr. neuspjele prijave i pokušaji pristupa bez ovlasti).“. U svrhu točnije procjene potrebnog angažmana, može li se dostaviti konkretnija specifikacija opsega Analytics i Reporting modula?

7. odgovor

U okviru ove nabave traži se analitički i izvještajni dio u opsegu “osnovnog izvještavanja” usmjerenog na operativnu kontrolu i dokazivost rada sustava, a ne razvoj širokog analitičkog skladišta niti “big-data” platforme. Minimalni skup obveznih izvještaja/pokazatelja uključuje, između ostalog: volumene provjera, volumene pošiljaka (uključivo po DG setovima), ishode nadzora, osnovne metrike integracija i opterećenja (npr. broj dohvaćanja poruka/payload-a) te osnovne sigurnosne pokazatelje (npr. neuspjele prijave i pokušaji neovlaštenog pristupa). Dodatno se očekuju standardni pregledi kroz vrijeme (dnevno/tjedno/mjesečno) i mogućnost izvoza, uz jasno definirane izvore podataka i pravila

Financira Europska unija NextGenerationEU

evidentiranja. Naglašava se da se implementacija analitičkog toka prema AFFINIS-u svodi na isporuku kuriranih, strukturiranih skupova podataka i dokazive kontrole prijenosa/konzistentnosti, dok su napredne transformacije i data-engineering pipeline u domeni AFFINIS tima.

8. pitanje

U dokumentu se navodi "Usluga podrške treba biti dostupna 24 sata dnevno, 7 dana u tjednu (24/7)". Molimo pojašnjenje oko organizacije dostupnosti podrške korisnicima (L1/Helpdesk) i uspostave odgovarajućeg ticketing sustava, odnosno hoće li isto biti osigurano od strane Naručitelja?

8. odgovor

Zahtjev 24/7 odnosi se na osiguranje neprekidne mogućnosti zaprimanja prijava i eskalacije kritičnih incidenata te postupanja sukladno definiranim razinama podrške i SLA. Ticketing sustav i organizaciju korisničkog kanala (L1/helpdesk) osigurava Naručitelj, a Izvođač je obvezan osigurati integraciju u taj proces (kategorije, prioriteti, eskalacije, izvještavanje) te dostupnost i postupanje u ugovorenom opsegu (osobito za L2/L3 i kritične incidente), uz isporuku operativnih uputa i standardiziranih obrazaca prijave incidenta.

9. pitanje

U dokumentu se navodi "Odabrani ponuditelj izdaje eRačun temeljem pozitivnog izvještaja neovisnih verifikatora i validatora i obostrano potpisanog Zapisnika o izvršenju usluga.". Koji su maksimalni rokovi za provedbu verifikacije/validacije i za izdavanje konačnog izvještaja o nadzoru? Koji je postupak i rok za rješavanje spora ako Izvođač ne prihvati nalaz verifikatora? Postoji li žalba/arbitraža/ponovna provjera ako Izvođač osporava nalaz?

9. odgovor

Verifikacija/validacija provodi se prema unaprijed definiranim postupcima i kriterijima te je izdavanje eRačuna vezano uz pozitivno izvješće i obostrano potpisani zapisnik o izvršenju usluga. Operativni rokovi provedbe verifikacije/izrade izvješća te postupanje u slučaju primjedbi Izvođača (očitovanje, dopune dokaza, korektivne radnje i ponovna provjera) uređuju se dokumentacijom postupka verifikacije/validacije i ugovorom. Izvođaču se omogućuje dostava obrazloženih primjedbi i dodatnih dokaza u definiranom roku, nakon čega se provodi usuglašavanje nalaza i, po potrebi, ponovna provjera u opsegu spornih točaka.

Sukladno zaprimljenim upitima i objavljenim pojašnjenjima, Naručitelj mijenja Prilog II. Tehnička specifikacija za razvoj i implementaciju sustava e-ADR, točku 4.2. stavak 4:

*Ključne uloge na strani **Izvođača** uključuju stručnjaka za poslovnu analizu i modeliranje procesa, stručnjaka za arhitekturu informacijskog sustava, stručnjaka za integracije i razmjenu podataka te stručnjaka za informacijsku sigurnost i usklađenost s NIS2 i drugim relevantnim propisima.*

mijenja se i glasi:

*Ključne uloge na strani **Naručitelja** uključuju stručnjaka za poslovnu analizu i modeliranje procesa, stručnjaka za arhitekturu informacijskog sustava, stručnjaka za integracije i razmjenu podataka te stručnjaka za informacijsku sigurnost i usklađenost s NIS2 i drugim relevantnim propisima.*

Financira Europska unija NextGenerationEU

te se objavljuje izmijenjeni Prilog II. Poziva za dostavu ponuda – Tehnička specifikacija za razvoj i implementaciju sustava e-ADR.

Ukoliko ponuditelj u sklopu svoje ponude dostavi potpisanu prvotno objavljenu verziju Priloga II. Tehnička specifikacija za razvoj i implementaciju sustava e-ADR, smatrat će se da ponuditelj prihvaća naknadno objavljenu izmjenu te se isto neće smatrati neotklonjivim nedostatkom i/ili razlogom odbijanja ponude.

Točka 10. Poziva za dostavu ponuda:

Tijekom roka za dostavu ponuda gospodarski subjekt može zahtijevati dodatne informacije, objašnjenja ili izmjene u vezi s Pozivom najkasnije do dana 10. 2. 2026. godine do 11.00 sati, nakon navedenog roka, Naručitelj nema obvezu odgovarati na pitanja ponuditelja.
Naručitelj će na pravovremeno pristigla pitanja ponuditelja o predmetu nabave odgovoriti najkasnije do dana 12. 2. 2026. godine do 11.00 sati.
U slučaju bitne izmjene Poziva, Naručitelj može produžiti rok za dostavu ponuda.
Naručitelj može samostalno pojasniti ili izmijeniti Poziv za dostavu ponuda.

Naručitelj će izmjene Poziva i odgovore na pitanja gospodarskih subjekata objaviti na svojim internetskim stranicama: https://www.akd.hr/hr/o-nama/antikorupcijski-program/nabava.

mijenja se i glasi:

Tijekom roka za dostavu ponuda gospodarski subjekt može zahtijevati dodatne informacije, objašnjenja ili izmjene u vezi s Pozivom najkasnije do dana 16. 2. 2026. godine do 10.00 sati, nakon navedenog roka, Naručitelj nema obvezu odgovarati na pitanja ponuditelja.
Naručitelj će na pravovremeno pristigla pitanja ponuditelja o predmetu nabave odgovoriti najkasnije do dana 17. 2. 2026. godine do 10.00 sati.
U slučaju bitne izmjene Poziva, Naručitelj može produžiti rok za dostavu ponuda.
Naručitelj može samostalno pojasniti ili izmijeniti Poziv za dostavu ponuda.

Naručitelj će izmjene Poziva i odgovore na pitanja gospodarskih subjekata objaviti na svojim internetskim stranicama: https://www.akd.hr/hr/o-nama/antikorupcijski-program/nabava.

Točka 17. Poziva za dostavu ponuda:

Rok za dostavu ponude je do 11:00 sati dana 16. 2. 2026. godine bez obzira na način dostave.

Sve ponude koje Naručitelj zaprimi nakon isteka roka za podnošenje ponuda označit će se kao zakašnjelo pristigle te neće biti dio postupka pregleda i ocjene ponuda.

mijenja se i glasi:

Rok za dostavu ponude je do 11:00 sati dana 18. 2. 2026. godine bez obzira na način dostave.

Sve ponude koje Naručitelj zaprimi nakon isteka roka za podnošenje ponuda označit će se kao zakašnjelo pristigle te neće biti dio postupka pregleda i ocjene ponuda.

Točka 18. Poziva za dostavu ponuda:

Javno otvaranje ponuda obavit će se dana 16. 2. 2026. godine s početkom u 11:00 sati, u Zagrebu na adresi Naručitelja.

Ponuditelji ili njihovi ovlašteni predstavnici mogu biti nazočni javnom otvaranju ponuda. Svoje ovlaštenje predstavnici ponuditelja dokazuju u pisanom obliku.

Zbog internih procedura Naručitelja, ponuditelji su dužni najkasnije 30 minuta prije isteka roka za dostavu ponude, dostaviti podatke o osobi koja će prisustvovati javnom otvaranju ponuda (ime i prezime te broj osobne iskaznice), na e-mail adresu iz točke 3. ovog Poziva za dostavu ponude. U suprotnom neće prisustvovati javnom otvaranju ponuda.

mijenja se i glasi:

Javno otvaranje ponuda obavit će se dana **18. 2. 2026. godine s početkom u 11:00 sati**, u Zagrebu na adresi Naručitelja.
Ponuditelji ili njihovi ovlašteni predstavnici mogu biti nazočni javnom otvaranju ponuda. Svoje ovlaštenje predstavnici ponuditelja dokazuju u pisanom obliku.

Zbog internih procedura Naručitelja, ponuditelji su dužni najkasnije 30 minuta prije isteka roka za dostavu ponude, dostaviti podatke o osobi koja će prisustvovati javnom otvaranju ponuda (ime i prezime te broj osobne iskaznice), na e-mail adresu iz točke 3. ovog Poziva za dostavu ponude. U suprotnom neće prisustvovati javnom otvaranju ponuda.

Prilog

1. Tehnička specifikacija za razvoj i implementaciju sustava e-ADR – 1. izmjena

POVJERENSTVO ZA NABAVU

TEHNIČKA SPECIFIKACIJA ZA RAZVOJ I IMPLEMENTACIJU SUSTAVA E-ADR

1. izmjena

Sadržaj

Financira Europska unija
NextGenerationEU

Financira
Europska unija
NextGenerationEU

Financira Europska unija
NextGenerationEU

Financira
Europska unija
NextGenerationEU

Financira Europska unija
NextGenerationEU

1. Analiza postojećeg stanja

Postojeće stanje u području **nacionalnog cestovnog prijevoza opasnih tvari u Republici Hrvatskoj** obilježeno je time da relevantni postupci i podaci postoje, ali su raspoređeni kroz više odvojenih registara, aplikacija i organizacijskih jedinica, bez jedinstvenog informacijskokomunikacijskog sustava posvećenog praćenju prijevoza opasnih tvari. Regulativa se provodi kroz zakone i podzakonske akte iz područja prijevoza opasnih tvari, eksplozivnih tvari, radioaktivnih i nuklearnih materijala, dok je digitalna potpora za sada fragmentirana i usmjerena na pojedine procese (tahografski podaci, registri eksploziva, postupci izdavanja odobrenja). U sklopu Nacionalnog plana oporavka i otpornosti (NPOO) zasebno je definirana investicija **C1.4. R1-I5 „Praćenje prijevoza opasnih tvari u cestovnom prometu eADR“**, čime se potvrđuje da specijalizirani integrirani sustav za ovaj segment prijevoza trenutno nije uspostavljen te da je cilj projekta nadograditi postojeće prakse i digitalizirati cjelokupan proces na nacionalnoj razini.

U području praćenja vozila i vozača koji sudjeluju u prijevozu opasnih tvari **osnovni izvor podataka danas je SOTAH – Sustav za središnju obradu tahografskih podataka**. Prijevoznici koji su obveznici ugradnje tahografa i zapošljavanja mobilnih radnika dužni su, sukladno važećim propisima, u zadanim vremenskim intervalima prenositi tahografske podatke u SOTAH, pri čemu se bilježe podaci zabilježeni na tahografima u vozilima i na karticama vozača. Ovaj sustav osigurava centraliziranu pohranu i dostupnost tahografskih podataka za potrebe nadzora radnog vremena i pridržavanja propisanih obveza mobilnih radnika, ali nije uspostavljen kao specijalizirani alat za cjelovito praćenje prijevoza opasnih tvari. Podaci o tome **koji prijevoznik, koje vozilo i koji vozač** u konkretnom trenutku prevoze opasne tvari danas se ne dobivaju iz jednog jedinstvenog sustava, već kombinacijom podataka iz više evidencija i nadzornih postupaka, ovisno o nadležnosti pojedinog tijela i vrsti tvari.

Postupci **osposobljavanja vozača za prijevoz opasnih tvari i sigurnosnih savjetnika** provode se u skladu s ADR pravilima i nacionalnim propisima, preko ovlaštenih učilišta i nadležnog ministarstva, uz izdavanje svjedodžbi i potvrda koje dokazuju stručnu osposobljenost. Informacije o učilištima, programima, kandidatima, ispitnim komisijama i izdanim ispravama trenutačno su raspoređene kroz više internih evidencija i administrativnih postupaka. Iako se pojedini koraci procesa već oslanjaju na postojeće informacijske sustave nadležnih tijela i samih učilišta, **ne postoji jedinstveni digitalni sustav** koji bi na jednome mjestu pokrivao cijeli tijek – od evidentiranja ovlaštenih učilišta i nastavnog osoblja, preko prijave i praćenja polaznika, do automatskog izdavanja i provjere valjanosti ADR potvrda. Zbog toga ovlaštena tijela, prijevoznici i nadzorna tijela podatke o osposobljenosti vozača i sigurnosnih savjetnika prate kroz više odvojenih evidencija i dokumenata, umjesto kroz jedan integrirani digitalni izvor.

U segmentu **izdavanja odobrenja i dozvola za prijevoz eksplozivnih tvari** uspostavljen je funkcionalan registar eksplozivnih tvari uvezenih ili prenesenih u Republiku Hrvatsku, koji sadrži podatke o njihovoj sljedivosti – od skladištenja u odobrenim skladištima do stavljanja u

Financira
Europska unija
NextGenerationEU

promet i evidentiranja krajnjeg korisnika. Ministarstvo unutarnjih poslova (Ravnateljstvo civilne zaštite) na temelju dostavljenih zahtjeva i pripadajuće dokumentacije izdaje rješenja (odobrenja ili odbijanja) za prijevoz eksplozivnih tvari, pri čemu se rješenja izdaju u fizičkom obliku, na ime podnositelja zahtjeva, uz navođenje svih propisanih podataka o tvari, relaciji, prijevozniku i vremenu prijevoza. Trenutno **ne postoji sustav za elektroničko podnošenje zahtjeva prema MUP-u**, a rješenja se ne prate kroz jedinstveni elektronički sustav, već kroz interne evidencije i fizičku dokumentaciju. Najava prijevoza eksplozivnih tvari unutar granica Republike Hrvatske provodi se putem MUP-ovog sustava OKC, u kojem se dostavljaju podaci o vozaču, vozilu i planiranoj ruti, ali bez integracije s posebnim sustavom namijenjenim isključivo e-ADR domeni.

Kod **radioaktivnih tvari i nuklearnog materijala** postupci izdavanja odobrenja i dozvola provode se u okviru nadležnih službi, sukladno Zakonu o prijevozu opasnih tvari i posebnim pravilnicima. Za izdavanje odobrenja za prijevoz radioaktivnih izvora i pripadajućih djelatnosti propisani su detaljni zahtjevi glede podataka o podnositelju, radnicima, stručnim osposobljenostima, mjerama zaštite od ionizirajućeg zračenja i planovima za slučaj izvanrednog događaja. Međutim, **obrazac za podnošenje zahtjeva nije propisan na razini propisa**, već se u praksi koriste obrasci koje je izradilo nadležno tijelo, a zahtjev se i dalje podnosi u klasičnom (pisanom) obliku, uz potpis i priloženu dokumentaciju. Pojedinačne se dozvole izdaju na rok od 6 mjeseci, odobrenja za djelatnost prijevoza na 5 godina, a evidentiraju se u internim evidencijama nadležnih službi. Dozvole se evidentiraju u internim evidencijama nadležnih službi, ali ne postoji jedinstveni nacionalni informacijski sustav koji bi objedinjeno pratio sve izdane dozvole i prijevoze radioaktivnih i nuklearnih tvari u cestovnom prometu.

U širem kontekstu digitalizacije cestovnog teretnog prijevoza, u sklopu NPOO-a pokrenut je projekt **Nacionalnog sustava elektroničke pohrane i razmjene podataka u cestovnom prijevozu (NSCP)**, usklađen s Uredbom (EU) 2020/1056 o elektroničkim informacijama o prijevozu tereta (eFTI), s ciljem ubrzanog prijenosa informacija kroz cijeli lanac prijevoza, povećanja učinkovitosti nadzora i digitalnog praćenja putovanja tereta. Glavna zadaća tog projekta je implementacija nacionalnog eFTI čvora/gateway-a.

Ovaj sustav je koncipiran kao horizontalna platforma za elektroničku razmjenu podataka u cestovnom prijevozu općenito, dok **e-ADR projekt predstavlja zasebnu, ciljanu investiciju** usmjerenu na prijevoz opasnih tvari, koja se nadovezuje se na **nacionalni eFTI čvor/gateway** koji u trenutku izrade ove analize još nije implementirana u produkcijskom okruženju. Podaci relevantni za opasne tvari danas se stoga nalaze u pojedinačnim sustavima nadležnih tijela (SOTAH, registri eksplozivnih tvari, sustavi zavoda, OKC), bez centralizirane e-ADR platforme koja bi omogućila koordinirano upravljanje i pregled nad nacionalnim cestovnim prijevozom opasnih tvari.

Polazišna točka za uspostavu e-ADR rješenja jest, dakle, **postojanje razvijenog regulatornog okvira i nekoliko ključnih, ali međusobno odvojenih informacijskih sustava i registara**, koji podržavaju pojedine segmente procesa (tahografski nadzor, sljedivost eksploziva, odobrenja

Financira
Europska unija
NextGenerationEU

za radioaktivne i nuklearne tvari, operativne najave putem OKC-a). Istodobno, ne postoji jedinstveni informacijsko-komunikacijski sustav koji bi na razini Republike Hrvatske, isključivo za **nacionalni cestovni prijevoz opasnih tvari (bez otpada i bez prekograničnog prometa)**, objedinio podatke o vozačima i sigurnosnim savjetnicima, voznom parku, teretu, odobrenjima i tijeku prijevoza. Ovakvo postojeće stanje postavlja jasne granice i ulazne pretpostavke za projekt e-ADR: novi sustav se treba osloniti na postojeće registre i infrastrukturne resurse nadležnih tijela, ali ih povezati i nadograditi u jedno proizvodno rješenje, bez mijenjanja osnovne podjele nadležnosti i uloga dionika.

2. Svrha i ciljevi projekta

Svrha projekta **C1.4.R1-I5 „Praćenje prijevoza opasnih tvari u cestovnom prometu – e-ADR“** jest uspostava jedinstvenog, centraliziranog informacijsko-komunikacijskog sustava kojim se na nacionalnoj razini digitalno podupire planiranje, obavljanje i nadzor prijevoza opasnih tvari u cestovnom prometu na teritoriju Republike Hrvatske. Projektom se želi spojiti više odvojenih procesa – praćenje vozila putem tahografskih podataka, osposobljavanje vozača i sigurnosnih savjetnika, izdavanje dopuštenja za prijevoz te razmjena podataka s nadležnim tijelima – u **jedan pregledan i održiv sustav**.

Projekt je usmjeren na **ispunjavanje zakonskih obveza** i na pojednostavnjenje provedbe postojećih procedura, a ne na uvođenje novih složenih administrativnih ili tehničkih mehanizama. U fokusu je nacionalni cestovni prijevoz opasnih tvari, bez obuhvaćanja prijevoza otpada i bez prekograničnog prometa, pri čemu se kao temelj uzimaju već postojeći sustavi i registri (primarno SOTAH i Nacionalni sustav elektroničke pohrane i razmjene podataka o prijevozu tereta u dijelu skupa podataka za opasne tvari).

Svrha ovog dokumenta je definirati produkcijsko rješenje eADR-a na praktično provedivoj razini te propisati jasne i nedvosmislene zahtjeve za **nabavu razvoja i implementacije** sustava (funkcionalnosti, integracije, nefunkcionalni zahtjevi i kriteriji prihvata).

Dokumentacija treba omogućiti da se projekt realizira kao cjelina, bez potrebe za dodatnim fazama analize ili angažmanom dodatnih vanjskih dionika izvan onih koji su već predviđeni projektnom dokumentacijom.

Konačni cilj je da uspostavljeni sustav eADR omogući nadležnim tijelima, prijevoznicima i ostalim ovlaštenim korisnicima jednostavan, siguran i brz pristup relevantnim podacima, uz osnovno izvještavanje, jasne i razumljive procese te održivost rješenja u operativnoj eksploataciji. Sustav treba ostati dovoljno jednostavan za upravljanje i održavanje, uz jasno odvojen skup funkcionalnih cjelina koje se mogu razvijati i nadograđivati bez narušavanja stabilnosti jezgre sustava.

Financira
Europska unija
NextGenerationEU

2.1. Svrha uspostave sustava eADR

Primarna svrha uspostave sustava eADR je **digitalizacija i objedinjavanje ključnih procesa vezanih uz prijevoz opasnih tvari u cestovnom prometu** na jednom mjestu. To uključuje praćenje kretanja vozila koja prevoze opasne tvari na temelju tahografskih podataka, upravljanje osposobljavanjem vozača i sigurnosnih savjetnika, izdavanje elektroničkih dopuštenja za prijevoz te razmjenu podataka s Nacionalnim sustavom elektroničke pohrane i razmjene podataka o prijevozu tereta i nadležnim tijelima.

Sustav eADR treba omogućiti da se **postojeći zakonski propisani podaci koriste na strukturiran, ponovljiv i nadziran način**, bez potrebe za dodatnim ručnim koracima, višestrukim unosom ili paralelnim vođenjem evidencija. Time se smanjuje administrativno opterećenje za prijevoznike, učilišta i tijela državne uprave, a povećava se kvaliteta i konzistentnost podataka koji se koriste u nadzoru i planiranju.

Važan element svrhe je i **osiguravanje jedinstvenog „pouzdanog izvora" podataka o prijevozu opasnih tvari**. eADR treba u svakom trenutku pružiti jedinstven, usklađen i ažuran skup informacija o vozilu, vozaču, vrsti tereta, statusu osposobljenosti i statusu dopuštenja za prijevoz, pri čemu se izbjegava dupliciranje ili ručno usklađivanje informacija između više sustava.

Svrha je također osigurati da eADR **poštuje načelo minimalne nužne složenosti**: koristi postojeće sustave (SOTAH, Nacionalni sustav elektroničke pohrane i razmjene podataka o prijevozu tereta i postojeće registre) i postojeće postupke ovlaštenih tijela, bez uvođenja novih, tehnički složenih izvora podataka (npr. dodatne mjerne točke, posebna hardverska infrastruktura) koji su izvan opsega projekta. Projekt se oslanja na već uspostavljene podatkovne tokove i nadležnosti, a eADR služi kao objedinjeni „digitalni sloj" iznad njih.

2.2. Specifični ciljevi informacijsko-komunikacijskog sustava eADR

Specifični ciljevi sustava eADR proizlaze iz jasno definiranih funkcionalnih cjelina. Svaka cjelina ima ograničen, ali jasno definiran opseg, kako se sustav ne bi nepotrebno komplicirao, već da bi pokrio ono što je stvarno nužno za funkcioniranje procesa i ispunjavanje regulatornih obveza.

Prva skupina ciljeva odnosi se na praćenje kretanja vozila na temelju tahografskih podataka:

- **Omogućiti preuzimanje obrađenih tahografskih podataka iz SOTAH-a za vozila koja prevoze opasne tvari** radi prikaza kretanja vozila u prostoru i vremenu, u okviru zakonski propisanih rokova za prikupljanje i obradu tih podataka. Sustav se oslanja na postojeću obvezu prijevoznika da tahografske podatke redovito prenose u SOTAH, a eADR na temelju toga osigurava pregledno i ciljano korištenje podataka samo za vozila, vozače i prijevoznike koji stvarno prevoze opasne tvari.

Financira Europska unija
NextGenerationEU

- **Omogućiti nadzornim tijelima uvid u relevantne aktivnosti vozača i vozila** (npr. trajanje vožnje, pauze, rute) za konkretne prijevoze opasnih tvari, bez dodatnog ručnog izdvajanja i prijenosa podataka, uz poštivanje važećih pravila pristupa podacima i ovlasti.

Druga skupina ciljeva odnosi se na digitalni sustav za osposobljavanje vozača i sigurnosnih savjetnika:

- Uspostaviti centralizirani digitalni sustav za upravljanje procesom osposobljavanja vozača za prijevoz opasnih tvari i sigurnosnih savjetnika, uključujući registraciju ovlaštenih učilišta i predavača, prijavu kandidata, evidenciju pohađanja nastave, evidentiranje rezultata ispita i izdavanje odgovarajućih svjedodžbi i kartica.
- **Omogućiti Ministarstvu i ovlaštenim tijelima jednostavnu provjeru statusa osposobljenosti vozača i sigurnosnog savjetnika** (valjanost ADR potvrde, status položenih modula, datum isteka) bez potrebe za dodatnim upitima prema učilištima ili ručnim provjerama, pri čemu se svi ključni podaci nalaze u eADR-u.

Treća skupina ciljeva odnosi se na digitalizaciju postupka izdavanja elektroničkih dopuštenja za prijevoz opasnih tvari:

- **Uspostaviti digitalni sustav za izdavanje elektroničkog dopuštenja za prijevoz opasnih tvari**, s fokusom na dopuštenja koja izdaju nadležna tijela za eksplozivne tvari, oružje te radioaktivne i nuklearne terete, u nacionalnom cestovnom prometu. Sustav treba pojednostavniti prikupljanje podataka potrebnih za izdavanje dozvole i omogućiti digitalni uvid u izdana rješenja.
- **Omogućiti praćenje osnovnih podataka o izdanim dopuštenjima** (podnositelj, vrsta tvari, razdoblje valjanosti, vozilo, vozač) na jednom mjestu, kako bi nadležna tijela mogla jednostavno provjeriti je li dopuštenje izdano i je li još uvijek na snazi, bez dodatnih ručnih evidencija.

Četvrta skupina ciljeva vezana je uz integraciju s nacionalnim sustavom elektroničke pohrane i razmjene podataka o prijevozu tereta (eFTI):

- **Osigurati preuzimanje i korištenje podataka iz Nacionalnog sustav elektroničke pohrane i razmjene podataka o prijevozu tereta u dijelu koji se odnosi na opasne tvari (DG set)**, kako bi se izbjeglo dvostruko upisivanje istih podataka i kako bi nadležna tijela imala usklađen pogled na informacije o teretu, ruti i sudionicima prijevoza.
- **Uskladiti strukturu podataka u eADR-u sa skupom eFTI podataka za opasne tvari**, u onoj mjeri u kojoj je nužno za razmjenu i provjeru informacija, čime se osigurava interoperabilnost s postojećom i budućom nacionalnom i EU infrastrukturom za elektroničku razmjenu podataka o teretu.

Peta skupina ciljeva odnosi se na razmjenu podataka s nadležnim tijelima javne vlasti:

- **Osigurati jednostavnu i jasno definiranu razmjenu podataka između eADR-a i nadležnih tijela javne vlasti** (Ministarstvo mora, prometa i infrastrukture, Ministarstvo

Financira Europska unija
NextGenerationEU

unutarnjih poslova, Centar za vozila Hrvatske, Carinska uprava, Državni inspektorat i druga nadzorna tijela) u mjeri koja je potrebna za obavljanje njihovih zakonskih ovlasti u području nadzora nad prijevozom opasnih tvari.

- **Ograničiti razmjenu podataka na jasno definirane skupove informacija** kako bi se zadržala preglednost, smanjio opseg integracija i osigurala održivost sustava, uz poštivanje načela da se razmjenjuju samo podaci koji su stvarno potrebni nadležnim tijelima.

2.3. Ciljevi za ključne korisnike i nadležna tijela

Projekt definira ciljeve i iz perspektive **ključnih korisničkih skupina**, pri čemu se naglasak stavlja na postojeće i već ovlaštene subjekte, bez uvođenja novih organizacijskih uloga ili dodatnih vanjskih dionika. Najvažnije skupine su nositelj projekta (Ministarstvo), nadzorna tijela, prijevoznici i ovlaštena učilišta, sigurnosni savjetnici te ostali sudionici prijevoza.

Za **Ministarstvo mora, prometa i infrastrukture** i druga nadležna tijela, cilj je imati **jedinstveno mjesto za uvid u ključne podatke o prijevozu opasnih tvari**: status osposobljenosti vozača i sigurnosnih savjetnika, podatke o kretanju vozila na temelju tahografskih podataka, osnovne podatke iz nacionalnog eFTI čvora/gateway-a o prijevozu tereta te status izdanih dopuštenja. Time se omogućuje brža provjera usklađenosti s propisima i jednostavnije planiranje nadzora, bez potrebe za ručnim prikupljanjem podataka iz više odvojenih izvora.

Za nadzorna tijela (MUP, Državni inspektorat, Carinska uprava, Državni zavod za zaštitu od zračenja, Centar za vozila Hrvatske i dr.) ciljevi su usmjereni na praktičnu primjenu u svakodnevnom radu: jednostavan pristup informacijama o vozaču, vozilu, vrsti opasne tvari i izdanim dopuštenjima, kao i dostupnost osnovnih podataka o ruti i vremenu prijevoza. Sustav treba omogućiti da se u jednoj aplikaciji vidi ono što je tim tijelima već zakonski dostupno kroz različite procedure, ali sada objedinjeno i pregledno.

Za **prijevoznike i sigurnosne savjetnike** cilj je **smanjiti broj paralelnih administrativnih postupaka** i olakšati ispunjavanje zakonskih obveza. Korištenjem eADR-a prijevoznik dobiva jedno centralno mjesto na kojem su vidljivi statusi osposobljenosti vozača, osnovni podaci o vozilima i relevantna izdanja dopuštenja, čime se smanjuje potreba za opetovanim upućivanjem istih podataka prema različitim tijelima i ubrzava priprema prijevoza.

Za **ovlaštena učilišta, ispitne komisije i sigurnosne savjetnike** cilj je **upravljanje čitavim procesom osposobljavanja kroz eADR** – od upisa učilišta i predavača, prijave polaznika, vođenja evidencije pohađanja i rezultata ispita, do izdavanja svjedodžbi i ažuriranja statusa sigurnosnih savjetnika kod pojedinih prijevoznika. Time se stvara transparentan i provjerljiv trag aktivnosti, bez dodatnih paralelnih evidencija i uz jasnu podjelu odgovornosti.

Za **krajnje korisnike podataka (ovlaštene osobe u nadzornim tijelima i Ministarstvu)** cilj je da eADR bude **jednostavan za korištenje**, sa minimalnim brojem koraka do traženih informacija i osnovnim izvještavanjem koje je razumljivo i neposredno korisno za operativne odluke.

Financira
Europska unija
NextGenerationEU

Sustav ne uvodi dodatne razine složenosti, već podatke koje već postoje čini preglednijima i lakše dostupnima.

2.4. Strateško usklađenje i svrha u kontekstu šireg okvira

Projekt eADR sastavni je dio **digitalne modernizacije cestovnog prometa** i uklapa se u reformske aktivnosti predviđene u okviru pripadajuće komponente Nacionalnog plana oporavka i otpornosti. U tom smislu, svrha projekta nije samo rješavanje pojedinačnih administrativnih postupaka, nego **uspostava temeljne digitalne infrastrukture** za područje prijevoza opasnih tvari, koja će se dugoročno koristiti i nadograđivati u skladu s budućim potrebama i propisima.

Projekt je usklađen s europskim okvirom za **elektroničke informacije o prijevozu tereta (eFTI)** u dijelu koji se odnosi na opasne tvari, čime se osigurava da eADR koristi podatke sukladne eFTI specifikacijama i omogućuje njihovu provjeru i razmjenu s nadležnim tijelima. Time se eADR postavlja kao nacionalna točka za korištenje DG podataka u cestovnom prometu unutar postojećeg eFTI okvira.

Svrha projekta je i **ojačati koordinaciju između već postojećih nacionalnih registara i sustava**, bez njihovog zamjenjivanja. SOTAH ostaje primarni sustav za tahografske podatke, Nacionalni sustav elektroničke pohrane i razmjene podataka o prijevozu tereta ostaje primarni za podatke o teretu, a eADR se nadovezuje na njih kao specijalizirani sustav za opasne tvari u cestovnom prometu. Takvo usklađenje smanjuje rizik od dupliciranja funkcionalnosti i osigurava da se ulaganja u nove funkcionalnosti ograničavaju na ono što je stvarno potrebno za područje opasnih tvari.

Projektom se ujedno stvara **organizacijski i tehnički okvir** u kojem će se aktivnosti nadležnih tijela (nadzor, izdavanje dopuštenja, osposobljavanje) moći provoditi dosljedno i na temelju jedinstvenih digitalnih zapisa, što doprinosi transparentnosti, dosljednosti primjene propisa i učinkovitijem korištenju postojećih kadrovskih i tehničkih resursa.

2.5. Mjerljivi ciljevi i očekivani učinci

Mjerljivi ciljevi projekta definiraju se tako da odražavaju **minimalno nužan, ali jasno vidljiv pomak** u odnosu na postojeće stanje, uz naglasak na kvalitetu podataka, dostupnost informacija i pojednostavljenje procesa.

Na razini nadzornih tijela cilj je **skratiti vrijeme potrebno za prikupljanje i provjeru podataka o pojedinom prijevozu opasnih tvari**, jer se traženi podaci (vozač, vozilo, status osposobljenosti, dopuštenja, osnovni podaci o teretu) nalaze objedinjeni u sustavu eADR. Umjesto oslanjanja na više odvojenih izvora, nadzorna tijela dobivaju jedinstven pregled, što doprinosi učinkovitijoj provedbi nadzora na cesti i u nadzornim postupcima.

Na razini osposobljavanja cilj je **postići potpunu digitalnu vidljivost statusa osposobljenosti vozača i sigurnosnih savjetnika**, od prijave na tečaj do izdavanja potvrde, uključujući

Financira Europska unija NextGenerationEU

evidenciju prisutnosti i rezultate ispita. Time se smanjuje mogućnost pogrešaka, olakšava provjera uvjeta za obavljanje prijevoza i omogućava Ministarstvu da u svakom trenutku raspolaže ažurnim podacima o broju i statusu osposobljenih osoba.

Na razini izdavanja dopuštenja cilj je **osigurati da sva nova elektronička dopuštenja za prijevoz opasnih tvari koja su u opsegu projekta budu izdana kroz eADR**, uz mogućnost jednostavne provjere važnosti i osnovnih parametara dozvole od strane ovlaštenih tijela. Na taj način smanjuje se oslanjanje na fizičku dokumentaciju, olakšava se pregled izdanih rješenja i povećava se sigurnost i time se osigurava da se u prometu nalaze samo prijevozi s valjanim dopuštenjima.

Na razini sustava u cjelini cilj je da eADR **funkcionira kao stabilan, modularan i održiv sustav**, čija je razina složenosti prilagođena stvarnim potrebama korisnika. To znači da se u produkcijskom rješenju primjenjuju rješenja koja su dovoljno jednostavna za održavanje i nadogradnju te da su funkcionalnosti jasno razdvojene po cjelinama (tahografi, osposobljavanje, dopuštenja, integracije), uz osnovno izvještavanje nadležnim tijelima. Sustav treba omogućiti da se u svim tim cjelinama postigne jasan pomak u odnosu na postojeće stanje, bez uvođenja nepotrebnih dodatnih slojeva, procesa ili tehničkih komponenti.

3. Opseg i zahtjevi implementacije projekta

3.1. Opće određenje opsega projekta

Opseg projekta obuhvaća uspostavu produkcijskog informacijsko-komunikacijskog sustava eADR za nacionalni cestovni prijevoz opasnih tvari u Republici Hrvatskoj, uključujući isporuku dokumentacije kao sastavni dio isporuke razvoja.

U ovoj fazi definira se što sustav mora obuhvatiti, koje procese i podatke treba podržati te kojim se regulatornim i tehničkim ograničenjima mora prilagoditi, bez ulaska u detaljne korake same implementacije ili konfiguracije. Projekt je usmjeren na stvaranje jasne i ostvarive osnove za **nabavu razvoja i implementacije** rješenja, a ne na detaljnu razradu svih tehničkih koraka provedbe.

Projektni opseg je namjerno ograničen tako da **obuhvaća isključivo cestovni prijevoz opasnih tvari na području Republike Hrvatske**, bez uključivanja prekograničnog prometa i bez uključivanja drugih vrsta prometa (željeznički, pomorski, zračni, unutarnje plovne vode).U širem okviru NPOO ulaganja u digitalizaciju cestovnog teretnog prijevoza , ova tehnička dokumentacija za eADR razrađuje samo dio koji se odnosi na nacionalni cestovni prijevoz opasnih tvari, uz poštivanje eFTI zahtjeva za DG (opasne tvari) skup podataka.

Time se osigurava da rješenje ostane jednostavno i usmjereno na ono što je neposredno potrebno za rad nadležnih tijela i izvršnih dionika.

Financira
Europska unija
NextGenerationEU

Opseg funkcionalnosti sustava eADR definira se kroz **četiri osnovne funkcionalne cjeline**: praćenje kretanja vozila koja prevoze opasne tvari na temelju tahografskih podataka, digitalni sustav za osposobljavanje vozača i sigurnosnih savjetnika, digitalni sustav za izdavanje elektroničkog dopuštenja za prijevoz opasnih tvari te integraciju s nacionalnim sustavom za elektroničku pohranu i razmjenu podataka o prijevozu tereta (eFTI) u dijelu skupa podataka za opasne tvari. Svaka od tih cjelina razrađena je do razine poslovnih i tehničkih zahtjeva, ali bez propisivanja konkretne tehnologije implementacije ili detaljnog modeliranja svakog pojedinog ekrana, obrasca ili sučelja. U opseg projekta ulazi i definiranje zahtjeva za povezivanje eADR-a s postojećim informacijskim sustavima nadležnih tijela, osobito sustavom za središnju obradu tahografskih podataka (SOTAH), sustavima nadležnih tijela za izdavanje dopuštenja te s **nacionalnim eFTI čvorom/gateway-em** kao vanjskim sustavom eFTI razmjene.

Integracije se promatraju na razini razmjene nužnih podataka i osnovnih načela integracije (tipovi poruka, minimalni skup podataka, smjer razmjene), dok će detaljna tehnička razrada formata poruka, tehničkih protokola i sigurnosnih mehanizama biti obrađena u zasebnim poglavljima. Također, opsegom ovog poglavlja se ne definira nabava ICT opreme, jer je ista zasebno obuhvaćena u drugom dijelu poziva, već se polazi od pretpostavke da će infrastruktura biti osigurana kroz zasebni postupak nabave.

3.2. Regulatorni zahtjevi (opseg EU i nacionalne regulative)

Regulatorni opseg projekta određen je **kombinacijom europske i nacionalne regulative** koja se odnosi na prijevoz opasnih tvari u cestovnom prometu, elektroničke informacije o prijevozu tereta, radno vrijeme mobilnih radnika, radiološke i nuklearne tvari, inspekciju cestovnog prometa, kao i pravilnike koji uređuju osposobljavanje i uvjete prijevoza. U kontekstu eADR-a, ova regulativa se ne navodi samo informativno, već se iz nje izravno izvode zahtjevi koje sustav mora podržati: koje podatke treba obrađivati, koje postupke mora moći elektronički provoditi te kakvu razinu sljedivosti i provjerljivosti podataka mora osigurati.

Na razini Europske unije, ključni su **Uredba (EU) 2020/1056 o elektroničkim informacijama o prijevozu tereta (eFTI)**, Europski sporazum o međunarodnom prijevozu opasnih tvari u cestovnom prometu (ADR) te Direktiva 2008/68/EZ o kopnenom prijevozu opasnih tvari. Uredba o eFTI definira obvezu prihvaćanja elektroničkih informacija o prijevozu tereta te postupno stupanje na snagu provedbenih specifikacija za IT sustave nadležnih tijela i eFTI platforme. Za eADR to znači da sustav mora podržati **skup podataka za opasne tvari (DG set) kako je definiran u eFTI specifikacijama** u onom opsegu koji je potreban za prijevoz opasnih tvari u cestovnom prometu u Republici Hrvatskoj. ADR sporazum i Direktiva 2008/68/EZ definiraju zahtjeve za klasifikaciju tvari, dokumentaciju, označavanje vozila i sljedivost, što se u eADR-u odražava kroz strukturiranje podataka o teretu, opisu pošiljke i povezivanju tvari s vozilima i prijevoznikom.

Na nacionalnoj razini, opseg regulative obuhvaća Zakon o prijevozu opasnih tvari, Zakon o prijevozu u cestovnom prometu, Zakon o radnom vremenu, obveznim odmorima mobilnih

Financira
Europska unija
NextGenerationEU

radnika i uređajima za bilježenje u cestovnom prijevozu, Zakon o eksplozivnim tvarima te proizvodnji i prometu oružja, Zakon o inspekciji cestovnog prometa i cesta te odgovarajuće pravilnike, uključujući pravilnike o načinu prijevoza opasnih tvari u cestovnom prometu, o stručnom osposobljavanju vozača i sigurnosnih savjetnika te o prijenosu tahografskih podataka u središnju bazu i vođenju evidencije o radnom vremenu mobilnih radnika. Iz ovih propisa proizlazi zahtjev da eADR omogući vođenje podataka na način usklađen s pojmovima i obvezama iz zakona i pravilnika, da podrži elektronički oblik onih informacija koje su danas u papirnatom obliku te da zadrži sljedivost postupanja nadležnih tijela u skladu sa zakonskim ovlastima.

Poseban segment regulatornih zahtjeva odnosi se na **informacijsku sigurnost i zaštitu podataka**. Sustav eADR mora biti projektiran tako da omogući usklađenost s propisima o kibernetičkoj sigurnosti (uključujući zahtjeve iz Direktive NIS2 i njenog prijenosa u nacionalni pravni poredak) te sa zakonodavstvom o zaštiti osobnih podataka i čuvanju službenih evidencija. U ovoj fazi definira se opseg: eADR mora omogućiti uvođenje mjera koje će se detaljno razraditi u zasebnom poglavlju (zahtjevi za implementaciju Direktive NIS2), kao i mehanizme ograničenja pristupa, evidentiranja pristupa podacima i poštivanja načela najmanjeg nužnog skupa podataka. Tehnički i organizacijski detalji sigurnosti ostaju za kasnije faze, ali je ovdje jasno određeno da su **kibernetička sigurnost i zaštita podataka sastavni dio projektnih zahtjeva**, a ne naknadna nadogradnja.

Regulatorni opseg konačno obuhvaća i **međusobnu usklađenost propisa** u primjeni: eADR mora biti projektiran tako da se isti skup podataka može koristiti za ispunjavanje više zakonskih obveza (npr. podaci o vozaču i vozilu relevantni su i za radno vrijeme, i za prijevoz opasnih tvari, i za nadzor), bez dvostrukog unosa i bez proturječja. Time se postiže da sustav ne uvodi dodatne administrativne obveze, već omogućuje da postojeće obveze budu izvršene na učinkovitiji način, u skladu s pravnim okvirom koji je naveden u pozivu za dostavu ponuda.

3.3. Poslovni zahtjevi (poslovna arhitektura i modeli poslovnih procesa)

Poslovni zahtjevi definiraju **što sustav treba omogućiti korisnicima i na koji način treba podržati postojeće poslovne procese** nadležnih tijela, prijevoznika, ovlaštenih učilišta i drugih izvršnih dionika. U ovoj fazi ne modeliraju se detaljni dijagrami procesa, već se opisuje struktura poslovne arhitekture i ključne procesne cjeline koje eADR mora pokriti, uz naglasak na minimalno potrebnoj funkcionalnosti za ispunjavanje ciljeva projekta. Poslovna arhitektura promatra se kroz tri glavna procesa: praćenje kretanja vozila koja prevoze opasne tvari, osposobljavanje vozača i sigurnosnih savjetnika te izdavanje elektroničkih dopuštenja za prijevoz opasnih tvari, uz nadređeni sloj razmjene podataka s Nacionalnim sustavom elektroničke pohrane i razmjene podataka o prijevozu tereta i nadzornim tijelima.

U poslovnom smislu, **podsustav za praćenje prijevoza opasnih tvari** mora omogućiti da nadležna tijela, na temelju tahografskih podataka i relevantnih informacija iz nacionalnog eFTI

Financira
Europska unija
NextGenerationEU

čvora/gateway-a, dobiju uvid u kretanje vozila koja prevoze opasne tvari unutar zakonom propisanih rokova za prikupljanje i obradu tih podataka. To podrazumijeva da sustav omogućava pretraživanje i pregled putovanja prema prijevozniku, vozilu, vozaču, vrsti opasne tvari ili vremenskom razdoblju, uz osnovni geoprostorni prikaz rute i ključnih događaja. Poslovni procesi u ovoj cjelini uključuju obradu pristiglih tahografskih podataka, povezivanje prijevoza s relevantnim dopuštenjima i podacima o teretu te davanje uvida nadzornim tijelima u mjeri koja je potrebna za obavljanje njihovih zakonskih ovlasti.

Podsustav za osposobljavanje vozača i sigurnosnih savjetnika obuhvaća poslovne procese vezane uz ovlaštenje učilišta, vođenje programa osposobljavanja, prijavu kandidata, praćenje pohađanja nastave, provedbu ispita i izdavanje potvrda ili svjedodžbi. Sustav mora omogućiti da ovlaštena učilišta unose i ažuriraju podatke o programima i kandidatima, da se rezultate ispita i izdane svjedodžbe mogu vidjeti u eADR-u te da nadležna tijela imaju pouzdan uvid u status osposobljenosti vozača i sigurnosnih savjetnika.

Dakle sustav u cijelosti mora podržavati puni proces u kojem učilište izdaje svjedodžbu, a MMPI temeljem zahtjeva vozača i predmetne svjedodžbe izdaje ADR potvrdu (ADR karticu).

Poslovna arhitektura u ovom dijelu predviđa jedinstvenu evidenciju osposobljenih osoba, uz razgraničenje ovlasti između učilišta, Ministarstva i drugih nadležnih tijela koja provjeravaju ispunjenost uvjeta za obavljanje prijevoza opasnih tvari.

Podsustav za izdavanje elektroničkog dopuštenja za prijevoz opasnih tvari pokriva poslovne procese od podnošenja zahtjeva, preko obrade zahtjeva u nadležnom tijelu, do izdavanja i provjere valjanosti dopuštenja. Sustav mora podržati unos i provjeru minimalno potrebnih podataka (podnositelj zahtjeva, prijevoznik, vozilo, vozač, vrsta i količina opasne tvari, relacija, razdoblje važenja dopuštenja), kao i elektroničko evidentiranje donesenog rješenja. Nadležna tijela moraju preko eADR-a moći pretraživati izdana dopuštenja i provjeravati njihovu valjanost, dok prijevoznici trebaju imati uvid u svoja dopuštenja i njihovo važenje. Poslovni model ne uvodi nove vrste dopuštenja, već digitalizira postojeće postupke u skladu s važećim propisima.

Transverzalni poslovni zahtjev odnosi se na **integraciju poslovnih procesa eADR-a s Nacionalnim sustavom elektroničke pohrane i razmjene podataka o prijevozu tereta i sustavima nadležnih tijela**. eADR treba koristiti podatke iz nacionalnog eFTI čvora/gateway-a u dijelu opasnih tvari kako bi se izbjegla redundancija unosa i osiguralo da su ključni podaci o teretu, relaciji i sudionicima prijevoza usklađeni s ostalim sustavima. Istovremeno, sustav mora omogućiti osnovno izvještavanje za potrebe Ministarstva i drugih nadležnih tijela (npr. broj prijevoza opasnih tvari u određenom razdoblju, broj izdanih dopuštenja, broj aktivnih osposobljenih vozača i sigurnosnih savjetnika) na jednostavan i razumljiv način, bez složenih analitičkih funkcija koje bi prelazile opseg ovog projekta.

Financira
Europska unija
NextGenerationEU

3.4. Tehnički zahtjevi (dizajn sustava i tehnička arhitektura)

Tehnički zahtjevi definiraju **načelni dizajn i tehničku arhitekturu produkcijskog rješenja**, uz jasno razgraničenje od kasnijih detaljnih projekata implementacije. Osnovni princip je da se uspostavi modularan, skalabilan i održiv sustav koji se može nadograđivati u skladu s razvojem regulative (osobito eFTI i NIS2), ali da početna verzija ostane jednostavna za uvođenje i održavanje. Arhitektura se promatra kroz logičke cjeline (aplikacijski sloj, podatkovni sloj, integracijski sloj, sigurnosni sloj) koje će se u kasnijem poglavlju dodatno razraditi.

Na infrastrukturnoj razini, eADR se projektira tako da **radi u državnom podatkovnom centru, na opremi osiguranoj u okviru projekta eADR**, bez oslanjanja na javne oblake. Tehnički zahtjevi moraju osigurati da se rješenje može implementirati u takvom okruženju, koristeći standardizirane poslužiteljske, mrežne i sigurnosne komponente. U ovom poglavlju se zato ne ulazi u dimenzioniranje opreme, ali se jasno propisuje da aplikacijski i podatkovni sloj moraju biti projektirani za rad u on-premise okruženju, uz podršku za visoku dostupnost i osnovnu redundanciju, koje će biti razrađene u dokumentaciji za ICT infrastrukturu.

Na razini aplikacijskog dizajna, eADR treba biti **modularno rješenje** organizirano oko glavnih funkcionalnih cjelina (praćenje prijevoza, osposobljavanje, dopuštenja, integracija s **nacionalnim eFTI čvorom/gateway-em** i nadzornim tijelima). Svaka cjelina mora biti jasno razgraničena na razini funkcionalnosti i podataka, kako bi se omogućilo neovisno održavanje i nadogradnja bez utjecaja na ostale cjeline. Tehnički zahtjevi predviđaju korištenje standardnih web tehnologija i usluga, uz mogućnost rada u kontejnerskom okruženju s orkestracijom, što olakšava upravljanje verzijama, skaliranje i automatizirano nadgledanje rada sustava. Detaljna odluka o tehnologijama i okvirima bit će predmet kasnijih faza, ali je u ovoj fazi važno definirati da rješenje treba biti **temeljeno na suvremenoj, ali provjerenoj arhitekturi** koja ne uvodi nepotrebnu složenost.

Integracijski zahtjevi na tehničkoj razini usmjereni su na **razmjenu podataka s ključnim sustavima**: Nacionalnim sustavom elektroničke pohrane i razmjene podataka o prijevozu tereta, sustavom za središnju obradu tahografskih podataka, sustavima nadležnih tijela za izdavanje dopuštenja te sustavima nadzornih tijela javne vlasti. Razmjena podataka treba se temeljiti na otvorenim i dobro dokumentiranim formatima (primjerice uobičajeni strukturirani formati za razmjenu podataka) te standardnim protokolima koji omogućuju siguran i pouzdan prijenos. U ovoj fazi definira se minimalni skup integracijskih tokova (npr. dohvat DG skupa podataka iz nacionalnog eFTI čvora/gateway-a, dohvat agregiranih tahografskih podataka za vozila koja prevoze opasne tvari, razmjena osnovnih podataka o dopuštenjima s nadležnim tijelima), dok će se detaljna specifikacija sučelja i formata poruka razraditi u poglavlju posvećenom integracijama.

Konačno, tehnički zahtjevi uključuju i **osnovne zahtjeve za sigurnost, upravljanje korisnicima i nadzor rada sustava**, pri čemu se ne ulazi u razinu detalja propisanu NIS2 poglavljem. Sustav mora podržati integraciju s postojećom nacionalnom infrastrukturom za elektroničku identifikaciju korisnika i upravljanje pristupnim pravima, mora omogućiti uvođenje uloga i

Financira
Europska unija
NextGenerationEU

grupa koje odgovaraju stvarnim nadležnostima dionika (ministarstvo, nadzorna tijela, prijevoznici, ovlaštena učilišta) te mora imati mogućnost osnovnog nadzora rada (zapisi o pristupu, osnovna tehnička i aplikativna mjerila rada). Svi ovi zahtjevi definiraju okvir u kojem će se u kasnijim poglavljima detaljnije opisati tehnička arhitektura, integracije i sigurnosne mjere, uz zadržavanje načela da **rješenje ostane što jednostavnije za implementaciju i održavanje**, a istovremeno potpuno usklađeno s regulatornim i poslovnim zahtjevima projekta.

4. Organizacijski zahtjevi i kompetencije

4.1. Vođenje i koordinacija tehničkog tima projekta

Vođenje i koordinacija tehničkog tima projekta eADR temelji se na načelu jasno definiranih nadležnosti između Naručitelja i Izvođača uz minimalno potreban broj uloga i razina upravljanja. Naručitelj osigurava projektnog voditelja s njegove strane, odgovornog za ukupnu koordinaciju aktivnosti u okviru projekta i donošenje ključnih odluka vezanih uz prihvaćanje isporuka.

Organizacijski zahtjev je da se uspostavi **jednostavna struktura upravljanja** temeljena na redovitim koordinacijskim sastancima Naručitelja i Izvođača, pri čemu je voditelj tehničkog tima, kojeg osigurava Naručitelj, zadužen za pripremu stručnih materijala, dnevnih redova i zapisa sa sastanaka za dijelove koji se odnose na **tehničke isporuke (razvoj, integracije, testiranje i prihvat)**. Uloga voditelja nije ograničena na administrativnu koordinaciju, već uključuje i osiguravanje dosljedne primjene metodologije rada, praćenje usklađenosti izrađenih materijala s dokumentacijom iz poziva te pravovremeno uključivanje relevantnih stručnjaka kad je to potrebno.

4.2. Zahtjevi za IT stručnjake i uvjeti stručne sposobnosti

Za provedbu aktivnosti **razvoja i implementacije** eADR sustava Izvođač mora osigurati IT stručnjake koji mogu u zadanim rokovima **dizajnirati, razviti, integrirati, testirati i pustiti u rad** rješenje te isporučiti pripadajuću dokumentaciju i edukaciju.

Minimalno se osigurava (zbog kratkog roka razvoja i implementacije, uz potrebu paralelnog razvoja, integracija i testiranja): 3 backend developera (core), 1 backend developer (integracije), 2 frontend developera, 1 DevOps/Infra, 1 DBA, 2 QA/test stručnjaka, 1 stručnjak za informacijsku sigurnost. Dokumentacija projekta propisuje minimalne uvjete stručne sposobnosti, a organizacijski zahtjev ovog poglavlja je da Izvođač osigura stručnjake koji ih ispunjavaju i koji se mogu dodijeliti na projekt u dovoljnom obujmu, bez fragmentiranja rada na velik broj vanjskih suradnika.

Očekuje se svakodnevna dostupnost svih traženih stručnjaka tijekom trajanja projekta (radnim danima), uključivo za dnevnu koordinaciju, razjašnjenja i otklanjanje blokera u roku istog

Financira
Europska unija
NextGenerationEU

radnog dana. Uloge ne smiju biti osigurane isključivo povremeno ili ad-hoc, već moraju biti dodijeljene projektu u obujmu koji omogućuje kontinuiran dnevni rad i isporuku unutar zadanog roka.

Ključne uloge na strani Naručitelja uključuju stručnjaka za poslovnu analizu i modeliranje procesa, stručnjaka za arhitekturu informacijskog sustava, stručnjaka za integracije i razmjenu podataka te stručnjaka za informacijsku sigurnost i usklađenost s NIS2 i drugim relevantnim propisima.

Ključne uloge na strani Izvođača uključuju backend developere (razvoj core modula), backend developera za integracije i razmjenu podataka (sa eFTI Gate, SOTAH, AFFINIS), frontend developera (web aplikacija), DevOps/infra stručnjaka (CI/CD, okruženja, deployment, monitoring), stručnjaka za baze podataka/DBA (administracija odabrane baze podataka, migracije, backup/restore, HA/DR), QA/test stručnjaka (planiranje, automatizacija i izvedba testova, UAT podrška, performance testovi) te stručnjaka za informacijsku sigurnost (DevSecOps kontrole, sigurnosne provjere i koordinacija penetracijskog testiranja).

Opis posla za IT stručnjake određuje se kroz njihove uloge u pojedinim fazama **razvoja i implementacije** sustava (dizajn, razvoj, integracije, testiranje, priprema produkcije i puštanje u rad). Stručnjak za poslovnu analizu, arhitekturu i vođenje projekta je tu izuzet no on sudjeluju u strukturiranju zahtjeva Naručitelja, izradi opisa poslovnih procesa, definiranju funkcionalnih zahtjeva i usklađivanju s relevantnim propisima. Također je odgovoran za definiranje logičkog i fizičkog koncepta rješenja, razdvajanje modula (praćenje prijevoza, osposobljavanje, dopuštenja, integracije), opis tehničkih zahtjeva za infrastrukturu te definiranje načelne arhitekture koja će biti polazište za kasnije faze.

Organizacijski je zahtjev da stručnjaci koji sudjeluju na projektu budu **stabilno prisutni u njegovom trajanju**, bez čestih izmjena ključnih članova tima. U posebnim slučajevima zamjene dopuštene su rotacije unutar iste tvrtke Izvođača, uz uvjet da zamjenski stručnjak ispunjava iste ili više uvjete stručne sposobnosti. Na taj se način osigurava kontinuitet znanja, zadržava usklađenost s uvjetima iz poziva i smanjuje rizik od usporavanja projekta zbog uhodavanja novih osoba u kratkim rokovima.

Minimalni uvjeti stručne sposobnosti predstavljaju eliminacijske uvjete (DA/NE) – ponuditelj mora dokazati da predloženi stručnjaci ispunjavaju navedene minimalne uvjete. Dodatno, u okviru kriterija ekonomski najpovoljnije ponude (ENP) boduju se dodatne kompetencije i/ili poznavanje konkretnih tehnologija iz tablica “Kriteriji dodatnog bodovanja (ENP)”, pri čemu se bodovi dodjeljuju po predloženom stručnjaku, a maksimalan broj bodova po ulozi je zbroj navedenih stavki.

Financira
Europska unija
NextGenerationEU

Potrebni stručnjaci i kvalifikacije

1) Backend developer (core moduli)- 3 stručnjaka

Minimalni uvjeti stručne sposobnosti:

- Minimalno 5 godina radnog iskustva u ulozi backend developera (razvoj i održavanje poslovnih aplikacija)
- Iskustvo rada u razvoju backend aplikacija (razvoj i održavanje servisnih aplikacija u modernom programskom jeziku i okviru rada)
- Iskustvo rada u izradi REST API-ja i rada s API specifikacijama
- Iskustvo rada s relacijskim bazama podataka (transakcije, optimizacija upita) i ORM pristupom
- Iskustvo rada u implementaciji autentikacije i autorizacije te upravljanja ulogama/ovlastima
- Iskustvo rada u izradi audit logiranja i korelacijskih identifikatora zahtjeva
- Iskustvo rada u pisanju unit i integracijskih testova
- Iskustvo rada s verzioniranjem izvornog koda i procesom code reviewa

Kriteriji dodatnog bodovanja (ENP)

- Java 17+ (Spring Boot 3.x)– 5 bodova
- .NET 8+– 5 bodova
- JUnit– 5 bodova
- Mockito– 5 bodova
- Testcontainers– 5 bodova

Maksimalno **10 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar svake grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje:

- **Programski stack:** Java 17+ (Spring Boot 3.x) / .NET 8+ → boduje se samo jedna stavka (max 5 bodova)
- **Testni alati:** JUnit / Mockito / Testcontainers → boduje se samo jedna stavka (max 5 bodova).

Financira Europska unija
NextGenerationEU

2) Backend developer – integracije (eFTI Gate, SOTAH, AFFINIS)- 1 stručnjak

Minimalni uvjeti stručne sposobnosti:

- Minimalno 5 godina radnog iskustva u razvoju integracija (REST API) i integracijskih tokova
- Iskustvo rada u implementaciji integracija s vanjskim sustavima putem API-ja
- Iskustvo rada s uspostavom mTLS komunikacije i radom s certifikatima
- Iskustvo rada s resiliency obrascima (retry, circuit breaker, graceful degradation)
- Iskustvo rada s mock/simulator pristupom za vanjske integracije
- Iskustvo rada na integracijskom testiranju (E2E tokovi)

Kriteriji dodatnog bodovanja (ENP)

- Apache Camel– 3 boda
- Spring Cloud Gateway– 2 boda
- Kafka– 3 boda
- RabbitMQ– 2 boda
- Resilience4j– 2 boda
- Polly (.NET)– 2 boda

  WireMock– 2 boda
- Pact (contract testing)– 2 boda

Maksimalno **10 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar svake grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje:

- **Integracijski okvir / gateway:** Apache Camel / Spring Cloud Gateway → boduje se samo jedna stavka (max 3 boda)
- **Poruke (messaging):** Kafka / RabbitMQ → boduje se samo jedna stavka (max 3 boda) • **Resiliency biblioteka:** Resilience4j / Polly (.NET) → boduje se samo jedna stavka (max 2 boda)
- **Mock / contract testing:** WireMock / Pact (contract testing) → boduje se samo jedna stavka (max 2 boda).

3) Frontend developer (web aplikacija)- 2 stručnjaka

Minimalni uvjeti stručne sposobnosti:

- Minimalno 3 godine radnog iskustva u razvoju web aplikacija
- Iskustvo rada u razvoju modernih web aplikacija
- Iskustvo rada integracije s REST API-jem

• Iskustvo rada s autentikacijom i autorizacijom na frontendu

• Iskustvo rada s responzivnim dizajnom i primjenom dizajn sustava

• Iskustvo rada s osnovnim principima sigurnosti u frontend razvoju

• Iskustvo rada u timu uz verzioniranje i code review

Kriteriji dodatnog bodovanja (ENP)

• React 18+ - 5 bodova
• Angular 17+ -5 bodova

Maksimalno **5 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje: • **Frontend framework:** React 18+ / Angular 17+ → boduje se samo jedna stavka (max 5 bodova).

4) DevOps / Infra inženjer- 1 stručnjak

Minimalni uvjeti stručne sposobnosti

• Minimalno 4 godine radnog iskustva na DevOps/infra poslovima (CI/CD, deployment, virtualizacija/kontejneri, monitoring)

• Iskustvo rada s Linux okruženjima i kontejnerizacijom

• Iskustvo rada s CI/CD

Iskustvo rada s automatizacijom deploymenta i konfiguracijom (Infrastructure as Code / automatizacija)

• Iskustvo rada s TLS/mTLS, certifikatima i konfiguracijom reverse proxy rješenja

• Iskustvo rada s monitoringom/observability pristupom (metrike, logovi, alerting)

• Iskustvo rada s kontroliranim isporukama i rollback procedurama • Iskustvo rada s upravljanjem tajnama i konfiguracijom po okruženjima

Kriteriji dodatnog bodovanja (ENP) :

• Docker - 2 boda
• Podman - 2 boda
• GitLab CI - 2 boda
• Azure DevOps Pipelines - 2 boda
• Ansible - 2 boda
• Terraform - 2 boda
• Prometheus/Grafana/ELK - 1 bod
• Splunk - 1 bod

Financira Europska unija
NextGenerationEU

Maksimalno **7 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar svake grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje:

- **Kontejnerizacija:** Docker / Podman → boduje se samo jedna stavka (max 2 boda)
- **CI/CD platforma:** GitLab CI / Azure DevOps Pipelines → boduje se samo jedna stavka (max 2 boda)
- **Automatizacija / IaC:** Ansible / Terraform → boduje se samo jedna stavka (max 2 boda) • **Observability (metrike/logovi):** Prometheus/Grafana/ELK / Splunk → boduje se samo jedna stavka (max 1 bod).

5) Database inženjer/ DBA (HA/backup)- 1 stručnjak

Minimalni uvjeti stručne sposobnosti:

- Minimalno 5 godina radnog iskustva na administraciji i optimizaciji baza podataka te HA/DR i backup/restore
- Iskustvo rada s administracijom i optimizacijom relacijskih baza
- Iskustvo rada s kontroliranim migracijama sheme i verzioniranjem baze kroz okruženja
- Iskustvo rada s HA/DR (replikacija, failover, oporavak)
- Iskustvo rada s backup strategijama i restore procedurama

  Iskustvo rada sa sigurnošću baze (role/privilegije, least privilege, enkripcija u tranzitu)

Kriteriji dodatnog bodovanja (ENP)

- PostgreSQL (15+)- 3 boda
- Oracle- 3 boda
- MS SQL- 3 boda
- Flyway -3 boda
- Liquibase- 3 boda

Maksimalno **6 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar svake grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje:

- **Sustav baze podataka (DBMS):** PostgreSQL (15+) / Oracle / MS SQL → boduje se samo jedna stavka (max 3 boda)
- **Alat za migracije baze:** Flyway / Liquibase → boduje se samo jedna stavka (max 3 boda)

6) QA / Test inženjer (automatizacija + UAT podrška + performance)- 2 stručnjaka

Minimalni uvjeti stručne sposobnosti:

- Minimalno 3 godine radnog iskustva u testiranju (test plan/cases, automatizacija i podrška UAT-u)
- Iskustvo rada u planiranju i provedbi testiranja (test plan, test cases, upravljanje greškama)
- Iskustvo rada s automatizacijom testova (API i/ili UI)
- Iskustvo rada s integracijskim testiranjima s mockovima/simulatorima
- Iskustvo rada s performance testiranjima i validacijom performansi
- Iskustvo rada u pripremi i podršci UAT-u
- Iskustvo rada u integraciji testova u CI/CD pipeline

Kriteriji dodatnog bodovanja (ENP):

- JMeter - 3 boda
- Gatling - 3 boda
- WireMock - 2 boda
- Mountebank -2 boda
- Playwright - 1 bod
- Cypress - 1 bod

Maksimalno **6 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar svake grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje:

- **Performance alat:** JMeter / Gatling → boduje se samo jedna stavka (max 3 boda)
- **Mock/simulator alat:** WireMock / Mountebank → boduje se samo jedna stavka (max 2 boda)
- **E2E UI automatizacija:** Playwright / Cypress → boduje se samo jedna stavka (max 1 bod)

Financira Europska unija
NextGenerationEU

7) Stručnjak za informacijsku sigurnost (DevSecOps / koordinacija penetracijskog testiranja)- 1 stručnjak

Minimalni uvjeti stručne sposobnosti:

- Minimalno 5 godina radnog iskustva u području sigurnosti aplikacija/sustava (sigurnosne provjere, koordinacija penetration testa)
- Iskustvo rada sa sigurnosnim analizama web aplikacija (npr. OWASP Top 10)
- Iskustvo rada u dizajnu sigurnog pristupa i upravljanja ulogama/ovlastima
- Iskustvo rada s mTLS i sigurnosnim postavkama integracija
- Iskustvo rada s vulnerability scanningom i CI security gate-ovima
- Iskustvo rada s provođenjem ili koordinacijom penetration testa i sigurnosnog audita
- Iskustvo rada s audit logging zahtjevima i zaštitom tajni

Kriteriji dodatnog bodovanja (ENP) – Security specialist:

- OSCP - 3 boda
- OSWE - 3 boda
- GPEN - 2 boda
- CEH - 1 bod
- OWASP ZAP - 1 bod
- Burp Suite - 1 bod
- SonarQube (SAST) -1 bod
- Snyk (SCA) - 1 bod
- HashiCorp Vault - 1 bod
- Azure Key Vault - 1 bod

Maksimalno **6 bodova** po ovoj stavci. Bodovi se zbrajaju **po grupama**, a unutar svake grupe boduje se **samo jedna** stavka (najviše bodovana koju kandidat ispunjava), uz sljedeće grupiranje:

- **Sigurnosna certifikacija:** OSCP / OSWE / GPEN / CEH → boduje se samo jedna stavka (max 3 boda)
- **DAST / proxy alat:** OWASP ZAP / Burp Suite → boduje se samo jedna stavka (max 1 bod) • **DevSecOps scanning (SAST/SCA):** SonarQube (SAST) / Snyk (SCA) → boduje se samo jedna stavka (max 1 bod)
- **Upravljanje tajnama:** HashiCorp Vault / Azure Key Vault → boduje se samo jedna stavka (max 1 bod).

Financira Europska unija
NextGenerationEU

Uloga validacije

U okviru projekta predviđena je i **neovisna uloga validacije i verifikacije** (validator/verifikator) čija je svrha osigurati da isporučeno rješenje eADR ispunjava dogovorene tehničke i sigurnosne zahtjeve te da je spremno za produkcijski rad. Validator/verifikator provodi provjere usklađenosti i kvalitete isporuka, daje nalaze i preporuke te sudjeluje u potvrdi ispunjenja kriterija prihvata po ključnim prekretnicama, bez preuzimanja odgovornosti za samu implementaciju.

Uredno izvršenje predmeta nabave potvrđuje se Zapisnicima o izvršenim uslugama po prekretnicama, temeljem pozitivnih izvještaja neovisnog verifikatora.

Detaljni zahtjevi, postupci, opseg i dokazni materijali za validaciju i verifikaciju bit će definirani u zasebnom dokumentu **"3.3. Definiranje zahtjeva za uslugu validacije i verifikacije"**, koji obuhvaća validaciju/verifikaciju: (a) arhitekture i infrastrukture, (b) procesa zaprimanja i upravljanja podacima, (c) sigurnosti i usklađenosti, (d) pristupa podacima, (e) integracije i interoperabilnosti, (f) performansi i optimizacije, (g) upravljanja sustavom, (h) monitoringa i alertinga, (i) testiranja i validacije, (j) implementacije i održavanja te (k) edukacije i dokumentacije, uključivo provjeru usklađenosti s NPOO, Operativnim sporazumom i pripadajućim prilozima. Dokument 3.3 sadrži zahtjeve, postupke, opseg i dokazni materijal za validaciju i verifikaciju.

4.3. Plan resursa projekta

Plan resursa projekta eADR definira **kako se stručni kapaciteti odabranog Izvođača raspoređuju po fazama implementacije projekta**, uzimajući u obzir zadani rok tehničke implementacije projekta i opseg zadataka navedenih u pozivu.

Plan resursa mora izričito pokazati da su sve uloge iz poglavlja 4.2 osigurane uz svakodnevnu dostupnost te da raspored angažmana omogućuje paralelni razvoj, integracije i testiranje u skladu s rokom implementacije.

U ovoj fazi se određuju načelni zahtjevi: koje uloge moraju biti raspoložive, u kojem intenzitetu i u kojim vremenskim razdobljima, bez ulaska u detaljan tjedni raspored, koji će se razraditi u planu provedbe projekta. Cilj je da se osigura dovoljna raspoloživost resursa za kontinuiran rad, a istodobno zadrži racionalan broj uključenih osoba.

Stručnjaci za poslovnu analizu i arhitekturu sustava intenzivnije sudjeluju u prvim fazama (analiza postojećeg stanja, definiranje svrhe i ciljeva, opseg i zahtjevi), dok se prema kraju razdoblja njihov angažman usmjerava na usklađivanje i provjeru cjelovitosti **isporuka**. Stručnjaci za integracije i sigurnost uključuju se po potrebi u fazama definiranja tehničkih zahtjeva, integracijskih točaka i zahtjeva za NIS2, uz mogućnost preklapanja s drugim ulogama kod izrade jedinstvenih **tehničkih isporuka i artefakata (specifikacije sučelja, sigurnosne postavke, konfiguracije)**.

Financira Europska unija
NextGenerationEU

Plan resursa predviđa i **uključenost predstavnika Naručitelja** kao ključnih sugovornika pri validaciji analitičkih zaključaka i tehničkih rješenja. Naručitelj osigurava dostupnost stručnih osoba iz nadležnih organizacijskih jedinica (promet, inspekcija, tahografi, sigurnost informacijskog sustava) na koordinacijskim sastancima i radionicama, u opsegu koji je dovoljan za pravodobno donošenje odluka i davanje povratnih informacija. Organizacijski zahtjev je da se odluke i usuglašavanja, koliko je god moguće, provode na zajedničkim sastancima, kako bi se izbjegla višestruka pojedinačna usklađivanja i dodatno opterećenje resursa.

Na razini Izvođača, plan resursa mora omogućiti da se u **kratkom vremenskom roku može pojačati angažman pojedinih uloga** (primjerice, u razdoblju intenzivnog **razvoja i ispravaka nakon testiranja (SIT/UAT)** ili pripreme **produkcijskog puštanja i prihvata**), bez potrebe za uključivanjem dodatnih podizvođača ili novih tvrtki. Time se osigurava fleksibilnost unutar jednog stručnog tima, uz zadržavanje jedinstvene linije odgovornosti prema Naručitelju.

Organizacijski zahtjev je da plan resursa ostane **transparentan i razmjeran opsegu projekta**, bez nepotrebnog povećanja broja ljudi ili uloga. To znači da se za svaku ključnu ulogu definira očekivani obujam angažmana (izražen kroz vremensko razdoblje i intenzitet sudjelovanja), ali se istodobno izbjegava razdvajanje zadataka na prevelik broj specijaliziranih funkcija.

5. Tehnička arhitektura produkcijskog rješenja

5.1. Načela arhitekture i osnovni koncept rješenja

Arhitektura produkcijskog rješenja eADR temelji se na **tri funkcionalna stupa** sustava: praćenju prijevoza opasnih tvari u cestovnom prometu na temelju tahografskih podataka i skupa podataka za opasne tvari iz eFTI okvira, upravljanju osposobljavanjem vozača i sigurnosnih savjetnika te upravljanju elektroničkim dopuštenjima za prijevoz opasnih tvari. Ova tri stupa oblikuju jezgru poslovne funkcionalnosti, oko koje se gradi tehnička arhitektura, tako da svaki stup ima svoj jasno razgraničen modul, ali da svi zajedno rade na istoj zajedničkoj platformi i koriste iste horizontalne servise (autentifikaciju, upravljanje korisnicima, zapisnike, nadzor rada sustava).

Osnovni koncept rješenja polazi od toga da je eADR **specijalizirani sustav za opasne tvari** koji se nadograđuje na već postojeće državne sustave za cestovni promet, posebno na nacionalni sustav za elektroničku pohranu i razmjenu podataka o prijevozu tereta (NSCP projekt – u fazi izrade) i na postojeće sustave za tahografske podatke i nadzor mobilnih radnika (SOTAH).

Načela arhitekture usklađena su s uobičajenim pristupima u **sličnim državnim projektima u EU** koji provode eFTI i specijalizirane sustave za opasne tvari, ali su prilagođena nacionalnom opsegu: obuhvaća se samo cestovni promet unutar Republike Hrvatske, ne obrađuje se prekogranični promet niti drugi oblici prometa, a obvezni skup podataka za opasne tvari iz eFTI specifikacija koristi se samo u mjeri nužnoj za podršku poslovnim procesima eADR-a.

Financira
Europska unija
NextGenerationEU

Arhitektura je stoga cjelovita, ali svjesno ograničena na ono što je doista potrebno za ovaj projekt, kako bi rješenje bilo jednostavno za implementaciju i održavanje.

5.1.1. Temeljna arhitektonska načela (modularnost, održivost, jednostavnost)

Temeljno načelo arhitekture eADR-a je **modularnost**. Sustav se sastoji od niza funkcionalnih modula koji odgovaraju ključnim poslovnim cjelinama: modul za praćenje prijevoza opasnih tvari, modul za osposobljavanje vozača i sigurnosnih savjetnika, modul za elektronička dopuštenja, modul za integracije s vanjskim sustavima, modul za upravljanje korisnicima i ulogama te modul za osnovno izvještavanje i pregled podataka. Svaki modul se u aplikacijskoj arhitekturi implementira kao skup međusobno povezanih, ali jasno razdvojenih usluga, koje dijele zajedničke horizontalne komponente (autentifikacija, zapisnici, nadzor) i zajedničku infrastrukturu, ali imaju vlastite logičke granice. Ovakav pristup omogućuje da se pojedini modul razvija, testira i nadograđuje bez potrebe za promjenama cijelog sustava.

eADR se projektira tako da ne duplicira postojeću funkcionalnost tamo gdje već postoje stabilni sustavi (primjerice SOTAH i srodni sustavi), već se integrira s njima putem jasno definiranih sučelja.

Treće načelo je **jednostavnost arhitekture i rješenja**. Jednostavnost se postiže ograničavanjem broja modula na one koji su nužni za ostvarenje poslovnog opsega, ograničavanjem broja integracijskih točaka na ključne državne sustave (nacionalni eFTI čvor/gateway, tahografski sustav, sustavi nadležnih tijela za dopuštenja i nadzor) te izbjegavanjem uvođenja naprednih funkcionalnosti koje nisu izričito potrebne (npr. složenih analitičkih platformi ili specijaliziranih podsustava za upravljanje tehničkim dugom). Izvještavanje se zadržava na razini osnovnih izvještaja i pregleda koji su potrebni nadležnim tijelima, bez uvođenja zasebnih sustava za poslovnu analitiku. Time se smanjuje složenost implementacije i kasnijeg održavanja, što je u skladu s ciljem da rješenje bude lako upravljivo.

Načelo **standardizacije i ponovne uporabe** dodatno podupire modularnost i održivost. Arhitektura predviđa da eADR koristi državne standarde za autentifikaciju i upravljanje identitetima (uključujući integraciju s postojećim nacionalnim rješenjima elektroničke identifikacije), koristi podatkovne strukture usklađene s eFTI skupom podataka za opasne tvari i oslanja se na jedinstveni model upravljanja zapisnicima, nadzorom i sigurnosnim postavkama na platformi.

Konačno, u arhitektonska načela ugrađeno je i načelo **sigurnosti po dizajnu**, koje će se u detalje razraditi u zasebnim poglavljima. Već na ovoj razini definira se da će moduli eADR-a raditi u segmentiranom okruženju, s jasno odvojenim mrežnim zonama za vanjske korisnike, nadležna tijela i administratore, s kontrolama pristupa u skladu s ulogama i ograničenjem pristupa podacima na načelu najmanje nužnosti. Sigurnosni zahtjevi koji proizlaze iz NIS2 okvira i nacionalnog zakonodavstva nisu dodatak arhitekturi, nego jedno od polaznih načela pri projektiranju cjelokupnog rješenja.

Financira
Europska unija
NextGenerationEU

5.1.2. Uloga eADR u odnosu na postojeće državne sustave i eFTI infrastrukturu (npr. SOTAH, nacionalni eFTI čvor/gateway)

U odnosu na postojeće državne sustave, eADR ima jasno definiranu ulogu **specijaliziranog sustava za upravljanje nacionalnim cestovnim prijevozom opasnih tvari**, koji nadograđuje i povezuje već uspostavljene funkcionalnosti. On ne zamjenjuje postojeće sustave, nego ih koristi kao izvore podataka i kao temeljnu infrastrukturu. Na taj način, eADR uspostavlja konsolidirani pogled na podatke o opasnim tvarima, vozačima, vozilima i dopuštenjima, ali ovlaštene izvore podataka (npr. tahografske evidencije ili eFTI podatke o teretu) ostavlja u njihovim matičnim sustavima.

U odnosu na **SOTAH i povezane tahografske sustave**, eADR se oslanja na postojeći mehanizam prikupljanja, obrade i pohrane tahografskih podataka. SOTAH ostaje centralni sustav za tahografske podatke i nadzor radnog vremena mobilnih radnika, dok eADR putem integracijskog sloja koristi obrađene podatke koji su relevantni za prijevoze opasnih tvari. U arhitekturi to znači da eADR nema vlastite komponente za očitavanje tahografa, već koristi postojeću infrastrukturu i pravne obveze prijenosa podataka u SOTAH, te na temelju tih podataka gradi funkcije praćenja kretanja vozila koja prevoze opasne tvari.

U logičkoj podjeli zaduženja u državnoj IT arhitekturi, **eADR preuzima ulogu referentnog sustava za objedinjavanje informacija o nacionalnim cestovnim prijevozima opasnih tvari**. Nacionalni eFTI čvor/gateway ostaje referentni sustav za elektroničke informacije o prijevozu tereta u cjelini, SOTAH i srodni sustavi ostaju referentni za tahografske podatke i radno vrijeme, dok eADR nad njima gradi specijalizirane prikaze i procese za opasne tvari (praćenje prijevoza, provjera osposobljenosti, izdavanje i provjera dopuštenja). Takva podjela uloga omogućuje da se arhitektura eADR-a zadrži relativno jednostavnom, jer se ne pokušava u jednom sustavu objediniti sve funkcije koje već postoje u drugim sustavima.

Na koncu, eADR u odnosu na druge državne sustave djeluje i kao **konsolidacijska točka za podatke relevantne za nadzorna tijela**. Nadzorna tijela ne moraju pojedinačno pristupati nacionalnom eFTI čvoru/gatewayu, SOTAH-u i registrima dopuštenja, već preko eADR-a dobivaju objedinjeni uvid u ono što je potrebno za nadzor prijevoza opasnih tvari. Time se uloga eADR-a u jasno profilira: on je tematski sustav za opasne tvari u cestovnom prometu.

5.1.3. Pregled glavnih funkcionalnih modula u arhitekturi

Arhitektura eADR-a obuhvaća nekoliko glavnih funkcionalnih modula, od kojih svaki odgovara jednoj ili više poslovnih cjelina definiranih opsegom projekta, a svi zajedno koriste zajedničku platformu i horizontalne servise. Modulima se ne daje isključivo tehnička, nego i poslovna uloga, kako bi bilo jasno koje procese i korisnike podržavaju.

Prvi i ključni modul je **modul za praćenje prijevoza opasnih tvari**. Ovaj modul preuzima i koristi podatke o opasnim tvarima iz nacionalnog eFTI čvora/gatewaya (DG skup podataka), povezuje ih s podacima o vozilima i vozačima dobivenima iz tahografskog sustava te putem osnovnih algoritama i pravila omogućava pregled kretanja vozila koja prevoze opasne tvari u zadanim

Financira Europska unija
NextGenerationEU

vremenskim okvirima. Modul omogućava pretraživanje i filtriranje prema prijevozniku, vozilu, vozaču, vrsti tvari i razdoblju, kao i prikaz osnovnih informacija o relaciji. Implementacijski gledano, modul se sastoji od aplikacijskih usluga za obradu podataka, sučelja za nadzorna tijela te podsustava za pohranu agregiranih podataka o prijevozima.

Drugi ključni modul je **modul za osposobljavanje vozača i sigurnosnih savjetnika**. U ovom modulu vode se podaci o ovlaštenim ustanovama, programima osposobljavanja, kandidatima, terminima nastave i ispita, rezultatima ispita te izdanim potvrda o osposobljenosti. Modul omogućuje ovlaštenim učilištima i nadležnom ministarstvu upravljanje kompletnim ciklusom osposobljavanja, od prijave do izdavanja dokaza o osposobljenosti, te omogućuje nadzornim tijelima provjeru statusa osposobljenosti prilikom nadzora prijevoza. Tehnički, modul obuhvaća obrasce i radne tokove za unos i ovjeru podataka, logiku provjere uvjeta za osposobljenost te repozitorij podataka o osposobljenim osobama.

Treći modul je **modul za elektronička dopuštenja za prijevoz opasnih tvari**. Taj modul podržava procese podnošenja zahtjeva za dopuštenje, obrade zahtjeva od strane nadležnih tijela, evidentiranja donesenih rješenja i upravljanja važenjem dopuštenja. Modul definira minimalni skup podataka koje je potrebno prikupiti (podnositelj zahtjeva, vozilo, vozač, vrsta i količina tvari, relacija, razdoblje važenja) te omogućuje izdavanje, izmjenu i opoziv dopuštenja u elektroničkom obliku. U arhitekturi je povezan s modulom za praćenje prijevoza, jer se podaci o važećim dopuštenjima koriste pri interpretaciji kretanja vozila i provjeri usklađenosti prijevoza s propisima.

Uz ova tri osnovna modula, arhitektura uključuje i **modul za integracije i razmjenu podataka**. Ovaj modul odgovoran je za tehničku realizaciju svih vanjskih sučelja eADR-a: razmjena podataka s nacionalnim eFTI čvorom/gatewayem, razmjena s tahografskim sustavom, razmjena s informacijskim sustavima nadležnih tijela (npr. sustavi za vođenje registara eksplozivnih tvari, sustavi nadzornih tijela) te eventualno druge integracije predviđene projektom. Modul osigurava da svi integracijski tokovi koriste ujednačene formate, da se podaci validiraju prije pohrane i da postoji sljedivost razmjene (zapisi o razmijenjenim porukama i rezultatima).

Konačno, arhitektura predviđa **modul za upravljanje korisnicima, ulogama i osnovnu administraciju sustava**, kao i **modul za osnovno izvještavanje i nadzorne ploče**. Modul za upravljanje korisnicima povezuje se s nacionalnim mehanizmima autentifikacije i omogućuje dodjelu uloga i prava pristupa po modulima, organizacijskim jedinicama i vrstama korisnika (nadležna tijela, prijevoznici, ovlaštena učilišta, administratori). Modul za izvještavanje oslanja se na podatke prikupljene u ostalim modulima i pruža osnovne pregledne izvještaje (npr. broj prijevoza opasnih tvari po razdoblju, broj izdanih dopuštenja, broj aktivnih osposobljenih vozača i savjetnika), bez uvođenja dodatnih analitičkih platformi. Zajedno, ovi moduli čine horizontalnu podršku koja koristi zajedničke komponente platforme i omogućuje jednostavnije upravljanje sustavom.

Financira
Europska unija
NextGenerationEU

5.1.4. Strukturno pozicioniranje eADR-a u državnoj IT infrastrukturi (onpremise)

eADR se ne oslanja na javne oblake, nego koristi poslužitelje, spremišta podataka, mrežnu opremu i sigurnosnu infrastrukturu nabavljenu i konfiguriranu kroz zasebne postupake nabave opreme za eADR. Arhitektura mora biti osmišljena tako da se eADR može smjestiti na tu platformu bez dodatnih specifičnih zahtjeva koji bi tražili novu infrastrukturu.

Na aplikacijskoj razini, eADR se pozicionira kao **skup aplikacijskih servisa i modula** koji rade na zajedničkoj platformi za orkestraciju kontejnerskih aplikacija i upravljanje mikroservisima. Svaki modul (praćenje, osposobljavanje, dopuštenja, integracije, administracija) može se implementirati kao skup logički povezanih servisa smještenih u odgovarajućim okruženjima (razvoj, test, produkcija), uz jasno razdvajanje konfiguracija i baza podataka po okruženju. Na taj se način postiže mogućnost odvojenog razvoja, testiranja i uvođenja novih funkcionalnosti, uz minimalne rizike po stabilnost produkcijskog sustava.

Na mrežnoj razini, eADR zauzima **segmentirani položaj u državnoj mrežnoj arhitekturi**. Pristup korisnika iz nadležnih tijela ostvaruje se preko nacionalnih mehanizama elektroničke identifikacije (NIAS). Unutarnji servisi eADR-a smješteni su u zaštićenim mrežnim zonama kojima mogu pristupati samo ovlašteni sustavi (npr. nacionalni eFTI čvor/gateway, tahografski sustav, sustavi nadležnih tijela) putem definiranih integracijskih sučelja. Time se postiže jasan razdvoj između vanjskog pristupnog sloja i unutarnje logike sustava.

eADR se, u strukturnom smislu, uklapa i u **operativni model državne IT infrastrukture**. Upravljanje sustavom, nadzor rada, vođenje zapisnika, sigurnosne kopije i oporavak od izvanrednih događaja provode se kroz standardne mehanizme. To znači da se u arhitekturu eADR-a od početka ugrađuje oslanjanje na postojeće alate za nadzor i upravljanje, umjesto da se uvode novi, samo za eADR specifični alati. U pogledu resursa, arhitektura mora biti usklađena s procjenom potrebnih računalnih kapaciteta i spremišta za eADR.

Strukturno pozicioniranje eADR-a u državnoj IT infrastrukturi tako osigurava da je sustav **stabilan, siguran i jednostavan za upravljanje**, da koristi zajedničke infrastrukturne i aplikacijske kapacitete predviđene za projekt eADR, te da je njegovo mjesto u odnosu na druge državne sustave (nacionalni eFTI čvor/gateway, tahografski sustav, sustavi nadležnih tijela) jasno definirano. Ovakav pristup omogućava da se tehnička arhitektura eADR-a razvija i detaljnije razrađuje u narednim poglavljima, bez narušavanja temeljnih načela modularnosti, održivosti i jednostavnosti.

Obrada podataka eADR sustava provodi se isključivo u AKD podatkovnim centrima na primarnoj i udaljenoj (Disaster Recovery) lokaciji, pri čemu udaljena lokacija mora ispunjavati zahtjeve visoke raspoloživosti razine TIER III. Produkcijska arhitektura mora biti dvosite i projektirana tako da osigura kontinuitet rada kritičnih funkcionalnosti i otpornost na prekid rada na jednoj lokaciji.

Ponuđeno rješenje mora biti izvedeno na infrastrukturi AKD-a i ne smije se oslanjati na vanjske usluge u oblaku. Korištenje javnih cloud usluga (npr. velikih komercijalnih pružatelja) nije

Financira
Europska unija
NextGenerationEU

dopušteno, osim iznimno kada je neizbježno i isključivo uz prethodno formalno odobrenje te provedenu procjenu rizika koja obuhvaća gubitak kontrole nad podacima/sustavima, neovlašteni pristup, prijenos preko granica, ovisnost o trećoj strani i rizik multitenant okruženja.

5.2. Poslovni slučajevi uporabe eFTI/ADR kao temelj za nadogradivi podatkovni model

Ovo poglavlje definira iscrpnu listu poslovnih situacija koje sustav mora podržati u području eFTI razmjene regulatornih informacija te ADR domene (uključujući nacionalni eADR dio). Sadržaj je namijenjen kao ulaz u izradu nadograđenog ER dijagrama i kasniju izradu aplikacije, pri čemu se posebna pažnja posvećuje pokrivanju stvarnih operativnih scenarija: **više pošiljaka u jednom vozilu**, **više pretovara**, **više prijevoznih sredstava**, **više odredišta** te **prekogranični tranzit**.

Projektna dokumentacija predviđa operativni obrazac rada temeljen na nacionalnom eFTI pristupniku (Gate) i aplikaciji za službenike (AAP), uz dvije varijante dohvaćanja podataka: **scenarij s metapodacima (metadata push + selective pull)** kao primarni, te **scenarij "samo dohvat" (pull only)** kao pričuvni. U praksi to znači da se tijekom većine provjera koristi brzi uvid u metapodatke, dok se potpuni dohvat eFTI skupa podataka radi selektivno, uz kriptiranu i potpisanu komunikaciju prema eFTI platformama.

Za ADR domenu sustav se ne smije svesti na "dokument o opasnom teretu", nego mora pokriti cijeli niz poslovnih situacija: klasifikaciju opasnih tvari, miješane terete, ograničenja rute (npr. tuneli), izuzeća, pretovare i privremena skladištenja, provjere osposobljenosti vozača i valjanosti dozvola, kao i incidente i mjere nakon utvrđene nepravilnosti. Uz to, model mora biti **nadogradiv** na promet u tranzitu na razini EU i na druge vrste prijevoza, iako je početna primjena usmjerena na cestovni prijevoz.

Katalog slučajeva uporabe strukturiran je tako da svaka skupina izravno vodi na podatkovne potrebe: koje entitete treba imati, koje veze moraju biti **više-prema-više**, koji statusi i događaji moraju biti evidentirani te kakav revizijski trag i analitika su potrebni. Posebno se naglašava razdvajanje pojmova **"što se prevozi" (pošiljka i stavke)** od **"kako se prevozi" (operacije, dionice/legovi i događaji)**, jer upravo to omogućuje pokrivanje konsolidacije, pretovara i multimodalnosti bez ograničenja u kasnijim fazama.

5.2.1. Rječnik pojmova i konceptualna razgraničenja

Za dosljedno tumačenje poslovnih situacija nužno je jasno razgraničiti osnovne pojmove eFTI i ADR domene. eFTI se u projektu koristi kao okvir za razmjenu **regulatornih informacija** između gospodarskih subjekata i nadležnih tijela, pri čemu se informacije dohvaćaju s eFTI platformi putem nacionalnog pristupnika. U operativnom smislu to znači da nadležno tijelo tijekom kontrole koristi AAP kako bi, preko Gatea, pristupilo podacima za konkretan prijevoz ili pošiljku.

Financira Europska unija
NextGenerationEU

U logističkom smislu, najvažnije je razlučiti **pošiljku** od **prijevozne izvedbe**. Pošiljka je poslovna cjelina robe koja se šalje od pošiljatelja prema primatelju (ili više primatelja), s pripadajućim stavkama, dokumentacijom i identifikatorima. Prijevozna izvedba je način na koji se pošiljka fizički kreće, što se u praksi sastoji od jedne ili više dionica (legova), pri čemu se tijekom puta mogu mijenjati vozilo, vozač, prijevoznik ili vrsta prijevoza, a mogu se događati pretovari i privremena skladištenja.

U ADR kontekstu, "opasni teret" nije jedinstvena stavka, nego skup stavki koje imaju regulatorno definirane atribute (npr. UN broj, službeni naziv za prijevoz, razred, pakirna skupina, ograničenja). U istom prijevoznom sredstvu mogu se nalaziti višestruke pošiljke i višestruke DG stavke, pa je potrebno pripremiti model i use-caseove tako da se može utvrditi **što se nalazi u vozilu u trenutku kontrole**, čak i kada je riječ o miješanom teretu i parcijalnim isporukama.

- **Pošiljka** poslovna cjelina robe s identitetom (referenca, identifikatori), sudionicima (pošiljatelj, primatelj, prijevoznik), lokacijama (utovar, istovar) i sadržajem (stavke, uključujući opasne tvari).
- **Operacija / dionica (leg)** konkretan dio prijevoza u prostoru i vremenu, vezan uz određenu vrstu prijevoza (npr. cesta), prijevozno sredstvo i odgovorne osobe; dionica može obuhvatiti više pošiljaka, a pošiljka može prolaziti kroz više dionica.
- **Događaj** poslovno relevantna promjena stanja tijekom prijevoza, kao što su utovar, istovar, pretovar, privremeno skladištenje, kontrola, incident ili promjena rute; događaji su ključni za dokazivost i rekonstrukciju tijeka prijevoza.
- **Jedinica rukovanja** praktična razina za pretovar i parcijalna kretanja (npr. paleta, IBC, bačva, kontejner); kada se pošiljka dijeli ili spaja, upravo je ova razina najčešće operativno najtočnija za praćenje.

Ova razgraničenja izravno uvjetuju kasniji ER dijagram: veze između pošiljke i dionice prijevoza ne smiju biti ograničene na "jedan-prema-više" u jednom smjeru, nego moraju dopustiti **višestruke kombinacije** koje nastaju u stvarnim logističkim tokovima, posebno kada se cilja na nadogradivost na tranzit i multimodalni prijevoz.

5.2.2. Životni ciklus eFTI skupa podataka i scenariji razmjene

Sustav mora podržati životni ciklus eFTI skupa podataka od nastanka do arhiviranja, pri čemu se kroz vrijeme mijenja i sadržaj i dostupnost informacija. U praksi se eFTI skup podataka inicijalno kreira i održava na eFTI platformi, a status se tijekom procesa mijenja iz radne pripreme u aktivno stanje, zatim u neaktivno stanje nakon završetka prijevoza te naposljetku u stanje spremno za arhivu i arhivirano. Ove promjene nisu samo tehničke, nego su poslovno važne jer utječu na to koje informacije su dostupne u trenutku kontrole i kakva je njihova dokazna vrijednost.

Projektna dokumentacija definira primarni model pristupa kroz **metapodatkovni indeks**: eFTI platforma dostavlja metapodatke u registar identifikatora na Gateu u ključnim trenucima životnog ciklusa pošiljke, tipično pri kreiranju i pri zatvaranju. Tijekom kontrole, službenik

Financira Europska unija NextGenerationEU

koristi AAP za brzi uvid u metapodatke, čime se omogućuje brzo odlučivanje treba li provesti dubinski dohvat kompletnog eFTI sadržaja. Ovaj obrazac je bitan i za performanse i za sigurnost, jer smanjuje broj slučajeva kada se dohvaća puni sadržaj.

Kada metapodatci nisu dovoljni ili postoji sumnja, sustav mora podržati **selektivni puni dohvat** s eFTI platforme, kroz potpisanu i kriptiranu razmjenu poruka putem eDelivery/AS4 mehanizma. U tom trenutku platforma vraća potpuni skup regulatornih informacija: podatke o sudionicima, sadržaju pošiljke, relevantnim dokumentima i, za DG, podatke koji odgovaraju ADR transportnoj dokumentaciji. Ova mogućnost mora postojati i u pričuvnom scenariju "pull only", kada metapodaci nisu dostupni ili nisu ažurni.

- **Kreiranje i ažuriranje eFTI podataka** obuhvaća unos i izmjene sadržaja, povezivanje sudionika i lokacija, upravljanje stavkama robe te zabilješke o promjenama, pri čemu je nužno zadržati povijest izmjena radi dokazivosti.
- **Upravljanje statusima i dostupnošću** mora omogućiti jasnu interpretaciju je li prijevoz u tijeku, je li završio, te je li skup podataka i dalje dostupan za regulatorne potrebe (npr. naknadne provjere).
- **Identifikacija i dohvat** oslanja se na jedinstvene identifikatore pošiljke i identitet platforme, pri čemu se u kontrolnom procesu prvo radi brzi metapodatkovni uvid, a potom selektivno dohvaćanje punog sadržaja.
- **Potpisivanje i potvrde sudionika** moraju biti podržani kao dio životnog ciklusa, jer u praksi predstavljaju dokazne točke (npr. potvrda preuzimanja ili isporuke) i često su predmet kontrole.

Ovi slučajevi uporabe određuju da kasniji podatkovni model mora razlikovati "poslovni objekt pošiljke" od "eFTI instance skupa podataka" te osigurati da se statusi, identifikatori i revizijski trag vode konzistentno i kroz metapodatke i kroz puni sadržaj.

5.2.3. Slučajevi uporabe nadležnih tijela u kontroli i pristupu podacima

Najčešći operativni slučaj uporabe je kontrola na cesti ili granici u kojoj službenik koristi AAP za identifikaciju pošiljke i dohvat relevantnih informacija. Proces započinje skeniranjem identifikacijskog koda i dohvatom metapodataka preko Gatea, pri čemu se provjerava vjerodostojnost pristupa i ovlasti službenika. Metapodaci služe za brzu procjenu: koje je prijevozno sredstvo, koja je osnovna vrsta tereta (uključujući oznaku da je riječ o opasnoj robi), te postoje li indikacije za detaljniju provjeru.

Dubinska provjera je drugi ključni slučaj uporabe i provodi se kada metapodaci nisu dovoljni ili kada postoji rizik i potreba za provjerom kompletnog sadržaja. U tom slučaju Gate inicira sigurnu razmjenu prema eFTI platformi i dohvaća potpune regulatorne informacije. Time se omogućuje da službenik vidi detaljne podatke o pošiljatelju, primatelju, sadržaju i, za DG, podatke koji odgovaraju ADR zahtjevima, uključujući klasifikacijske elemente i ograničenja koja mogu utjecati na zakonitost prijevoza.

Financira Europska unija
NextGenerationEU

Za DG kontrole projektna dokumentacija predviđa i paralelni poziv nacionalnog eADR sloja radi provjere nacionalnih registara i dokaza: valjanosti potvrda osposobljenosti vozača, ADR potvrde vozila te relevantnih dopuštenja i ograničenja. Time se uspostavlja jedinstvena kontrolna slika u kojoj eFTI daje regulatorne podatke o pošiljci, a eADR potvrđuje nacionalne uvjete prijevoza i ovlaštenja. Ova integracija mora raditi i u situacijama kada je dio informacija dostupan odmah, a dio se dohvaća naknadno, uz jasno evidentiranje svih koraka.

- **Standardni uvid u metapodatke** koristi se za brzu validaciju i selekciju slučajeva za detaljnu provjeru, uz minimalno opterećenje mreže i platformi te uz brzi povrat informacija službeniku.
- **Selektivni puni dohvat eFTI sadržaja** koristi se kada je potrebno provjeriti detalje sadržaja i usklađenosti, pri čemu je ključna sigurnost razmjene, dokazivost odgovora i mogućnost povezivanja dohvaćenog sadržaja s konkretnom kontrolom.
- **Integrirana DG provjera preko eADR sloja** obuhvaća provjeru valjanosti osposobljenosti vozača, potvrde vozila i dopuštenja, pri čemu se rezultat mora moći prikazati u AAP-u zajedno s eFTI sadržajem.
- **Evidentiranje ishoda kontrole** mora obuhvatiti rezultat, eventualne nepravilnosti, primijenjene mjere te povezivanje s relevantnim identifikatorima pošiljke i prijevozne izvedbe, kako bi se omogućila naknadna analiza i postupanje.

Ovi slučajevi uporabe zahtijevaju da se kasniji ER dijagram oslanja na entitete koji modeliraju kontrolu kao događaj s vlastitim identitetom, kontekstom, ovlastima i rezultatima, te da se poveže s pošiljkom, dionicama prijevoza i dokazima iz eADR registara.

5.2.4. Logistički i transportni scenariji za konsolidaciju, pretovar, multileg i multimodalnost

U stvarnom logističkom okruženju prijevoz rijetko odgovara jednostavnom obrascu “jedna pošiljka – jedno vozilo – jedno odredište”. Najčešće se susreću konsolidacije, parcijalne isporuke, pretovari i promjene vozila, pri čemu se u jednom kamionu može nalaziti više pošiljaka, a jedna pošiljka može proći kroz više kamiona i više međulokacija. Upravo iz tih razloga pošiljka i prijevozna izvedba moraju biti modelirani kao odvojeni poslovni objekti koji se povezuju prema stvarnim događajima i dionicama.

Ključni scenarij je konsolidacija, gdje jedna dionica prijevoza nosi više pošiljaka, često s različitim destinacijama. U tom slučaju, ista dionica ima više istovara, a sadržaj vozila se mijenja tijekom rute. Istovremeno, druga strana iste medalje je da jedna pošiljka može biti realizirana kroz više dionica zbog pretovara u logističkim čvorištima, zbog promjene prijevoznog sredstva, zbog promjene prijevoznika (podugovaranje), ili zbog promjene rute. Sustav mora moći rekonstruirati “što je bilo gdje i kada”, posebno u trenutku kontrole.

Posebno zahtjevni scenariji nastaju kada se pošiljka dijeli ili spaja. Dijeljenje može biti planirano (npr. dio robe ide jednom rutom, dio drugom) ili neplanirano (npr. zbog incidenta ili ograničenja). U takvim slučajevima, praćenje isključivo na razini pošiljke često nije dovoljno,

Financira
Europska unija
NextGenerationEU

nego je potrebno omogućiti povezivanje dionica s razinom stavke ili jedinice rukovanja, kako bi se točno znalo koji dio sadržaja je na kojem vozilu i kojim putem ide.

- **Više pošiljaka u jednom vozilu** obuhvaća konsolidaciju i “milk-run” rute s više istovara, pri čemu je nužno pratiti promjene sadržaja vozila po dionici i po lokaciji.
- **Jedna pošiljka kroz više dionica** obuhvaća pretovare unutar cestovnog prijevoza, promjene vozila ili vozača, te lanac prijevoznika kroz podugovaranje, pri čemu pošiljka zadržava identitet, a izvedba se mijenja.
- **Pretovar i privremeno skladištenje** zahtijevaju modeliranje događaja na lokaciji i vremenu, kako bi se razlikovalo “prijevoz u tijeku” od “zadržavanja u hubu” te kako bi se podržalo dokazivanje tijeka robe.
- **Multimodalnost i tranzit** zahtijevaju da se već u početnoj fazi uvede koncept vrste prijevoza na razini dionice, kako bi se kasnije bez strukturnih promjena mogao dodati željeznički, riječni, pomorski ili zračni dio.

Ovi scenariji izravno definiraju obveznu nadogradivost budućeg ER dijagrama: veze između pošiljki i dionica ne smiju biti ograničene, statusi moraju podržati parcijalne isporuke i prekide, a događaji moraju omogućiti rekonstrukciju toka i sadržaja po lokacijama i vremenima.

Financira
Europska unija
NextGenerationEU

5.2.5. ADR i eADR scenariji: opasne tvari, osposobljavanje, dopuštenja i incidenti

U ADR domeni, sustav mora podržati scenarije koji proizlaze iz regulatornih zahtjeva za prijevoz opasnih tvari i iz praktičnih situacija u operativi. To uključuje unos i validaciju DG stavki (npr. UN broj, klasifikacija, pakiranje, ograničenja), upravljanje miješanim teretima, provjeru ograničenja rute te dokazivu dostupnost transportne dokumentacije u elektroničkom obliku. U praksi se često javlja više različitih opasnih tvari u jednom vozilu, pri čemu svaka pripada drugoj pošiljci ili čak različitim primateljima, pa sustav mora omogućiti razdvajanje sadržaja po pošiljci, po stavci i po dionici prijevoza.

U kontrolnom procesu ADR zahtijeva da se, osim same dokumentacije o robi, može provjeriti i ispunjenost uvjeta za vozilo i vozača. Zato se u projektu uvodi nacionalni eADR sloj koji pokriva registre i procese osposobljavanja (programi, tečajevi, ispiti, potvrde) te izdavanje i upravljanje dopuštenjima (vrsta dopuštenja, tijela izdavatelji, obuhvati dopuštenja, statusi). U trenutku kontrole mora se moći dobiti konzistentan odgovor: je li vozač osposobljen za relevantnu kategoriju, je li vozilo valjano, te postoje li posebna ograničenja ili uvjeti za konkretni prijevoz.

Dodatno, ADR operativa mora obuhvatiti incidentne situacije: prosipanje, curenje, požar, prometna nesreća, privremena zabrana nastavka vožnje ili naloženo preusmjeravanje. Takvi događaji zahtijevaju povezivanje incidenta s pošiljkom, konkretnim DG stavkama, dionicom prijevoza, lokacijom i vremenom, kao i evidentiranje mjera koje su poduzete. U kontekstu nadzora i postupanja, incident se može pretvoriti u nadzorni predmet s odlukama, dokumentacijom i statusima.

- **Klasifikacija i dokumentacija DG sadržaja** mora omogućiti unos svih regulatornih elemenata potrebnih za elektroničku transportnu dokumentaciju te provjeru konzistentnosti kada se u jednom vozilu nalaze različite tvari i različite pošiljke.
- **Provjere osposobljenosti i valjanosti uvjeta** moraju obuhvatiti vozača, vozilo i dopuštenja, pri čemu se rezultat provjere mora moći povezati s konkretnom kontrolom i konkretnom dionicom prijevoza.

  Miješani tereti, parcijalne isporuke i pretovari zahtijevaju da se može evidentirati koji DG sadržaj je bio u vozilu u danom trenutku te gdje i kada je promijenio prijevozno sredstvo ili lokaciju.
- **Incidenti i mjere** moraju se voditi kao poslovni objekti s vlastitim identitetom, tijekom i ishodom, uključujući povezane nepravilnosti, odluke i povijest postupanja.

Ova skupina slučajeva uporabe osigurava da budući ER dijagram bude dovoljno bogat da podrži ADR kontrolu u stvarnim uvjetima, uključujući integraciju eFTI podataka o robi s nacionalnim eADR dokazima o osposobljenosti, valjanosti i dopuštenjima.

Financira Europska unija
NextGenerationEU

5.2.6. Prekogranični i tranzitni promet, nacionalne posebnosti, revizijski trag i analitika

Sustav mora biti spreman za scenarije u kojima se isti prijevoz ili pošiljka kontrolira u više država članica, uključujući situacije u kojima je RH polazište, odredište ili tranzitna država. To podrazumijeva mogućnost povezivanja kontrole i dohvaćenih podataka s identitetom nadležnog tijela, državom i kontekstom provjere, te evidenciju višestrukih kontrola nad istim objektom tijekom cijelog putovanja. Posebno je važno da se u prekograničnim situacijama osigura konzistentnost identifikatora i dokazivost komunikacije, jer se odluke i postupanja mogu nadovezivati između više nadležnosti.

Nacionalne posebnosti i derogacije predstavljaju dodatni sloj složenosti koji je potrebno pokriti bez "lomljenja" podatkovnog modela. U praksi se mogu pojaviti dodatni zahtjevi ili posebna pravila koja vrijede u određenoj državi ili za određenu vrstu prijevoza, što znači da sustav mora imati prostor za **proširenja** i za evidentiranje nacionalno specifičnih elemenata bez gubitka interoperabilnosti. Ovo je osobito relevantno za ADR domenu, gdje se u pojedinim situacijama traže dodatni navodi ili postupanja koja nisu identična u svim državama.

Revizijski trag i sigurnosna dokazivost nisu dodatak, nego temeljni zahtjev eFTI operativnog modela i projektne dokumentacije. Svaki pristup podacima mora biti evidentiran zajedno s time tko je pristupio, kada, s kojim ovlastima i s kojom svrhom, te koji je opseg podataka dohvaćen. Uz to se moraju evidentirati razmjene poruka prema eFTI platformama (uključujući status i integritet odgovora) te događaji metapodatkovnog ažuriranja u registru identifikatora. Ovi zapisi služe i za sigurnosni nadzor i za naknadno dokazivanje postupanja.

Analitički dio mora podržati izvještavanje i upravljanje rizicima na razini sustava, uz mogućnost praćenja volumena provjera, učestalosti nepravilnosti, ponavljača i trendova. Projektna dokumentacija predviđa intenzivne tokove podataka iz operativnog sustava u analitički sloj, s faktualnim skupovima podataka o pošiljkama i kontrolama, te s indikatorima rizika kao što su vozila s višestrukim prekršajima. Ovakav pristup zahtijeva da se već u podatkovnom modelu jasno odvoje transakcijski zapisi (događaji, kontrole, poruke) od referentnih podataka (subjekti, lokacije, vrste i statusi) kako bi analitika bila pouzdana.

- **Višedržavne kontrole iste pošiljke** zahtijevaju mogućnost da se kontrolni zapisi vežu na jedinstvene identifikatore pošiljke i da se jasno vidi slijed provjera po državama i tijelima.

  Proširenja za nacionalne zahtjeve moraju omogućiti dodavanje specifičnih elemenata bez dupliranja jezgre podataka, uz očuvanje interoperabilnosti i mogućnosti razmjene.
- **Revizijski trag pristupa i razmjene** mora obuhvatiti metapodatkovni uvid, selektivni puni dohvat, pozive prema eADR registrima te tehničke i sigurnosne atribute komunikacije radi dokazivosti.

Financira Europska unija
NextGenerationEU

- **Operativna i analitička slika** mora omogućiti izvještavanje o kontrolama, nepravilnostima i rizicima, pri čemu se podaci moraju moći grupirati po prijevozniku, vozilu, lokaciji, vrsti tereta i vremenskom razdoblju.

Ovi slučajevi uporabe osiguravaju da budući ER dijagram podrži ne samo dnevne kontrole, nego i prekogranične scenarije, nacionalne posebnosti, sigurnosnu dokazivost i analitiku, što je preduvjet za širenje sustava na razinu cijele EU i šire.

5.3. Podatkovni modeli za implementaciju eFTI/ADR slučajeva uporabe

Podatkovni modeli u ovom poglavlju definiraju strukture potrebne za potpunu implementaciju svih slučajeva uporabe iz poglavlja 5.1. Modeli su organizirani tako da istovremeno podržavaju: **brzu metapodatkovnu provjeru**, **selektivni dohvat punog eFTI sadržaja**, **ADR specifičnosti (DG stavke, ograničenja, incidenti)**, **nacionalni eADR dio (osposobljavanje i dopuštenja)** te **revizijski trag i analitiku**. Ključno je da model bude stabilan za današnji cestovni promet, ali i dovoljno općenit da bez strukturnih lomova podrži sutra **prekogranični tranzit, višedržavne kontrole i multimodalni prijevoz**.

Osnovno načelo modeliranja je razdvajanje “što se prevozi” od “kako se prevozi”. Pošiljka i njezin sadržaj (stavke, opasne tvari, dokumenti) modeliraju se neovisno od prijevozne izvedbe (transport, dionice/legovi, događaji), jer su u stvarnosti uobičajene situacije gdje **jedna pošiljka prolazi kroz više dionica**, a **jedna dionica istovremeno prevozi više pošiljaka**. Ovo načelo je preduvjet za pokrivanje konsolidacije, pretovara, parcijalnih isporuka, promjena vozila/vozača i lanaca prijevoznika.

Model je podijeljen u više logičkih cjelina koje se mogu implementirati kao zasebne sheme ili kao jasno odvojeni moduli unutar iste baze: (1) operativni logistički model, (2) eFTI integracijski model (platforme, identifikatori, metapodatci, dohvat), (3) nacionalni eADR model (osposobljavanje, dopuštenja, incidenti/predmeti), (4) sigurnost, ovlasti i revizijski trag, te (5) analitički model. Time se osigurava jasna odgovornost podataka, jednostavnije upravljanje promjenama i kontrola pristupa.

U svim modelima pretpostavlja se uporaba jedinstvenih identifikatora (npr. UUID) za interne ključeve, dok se vanjski identifikatori (npr. eFTI consignment ID, eFTI transport ID, UIL) pohranjuju kao poslovni identiteti i koriste u integracijama i pretragama. Statusi i tipovi vode se kao šifrarnici (kodne liste) radi **verzioniranja, usklađenosti s EU kodnim listama i nacionalnih proširenja**, uz strogo evidentiranje događaja i pristupa podacima.

Financira
Europska unija
NextGenerationEU

5.3.1. Referentni podaci, kodne liste i proširivost modela

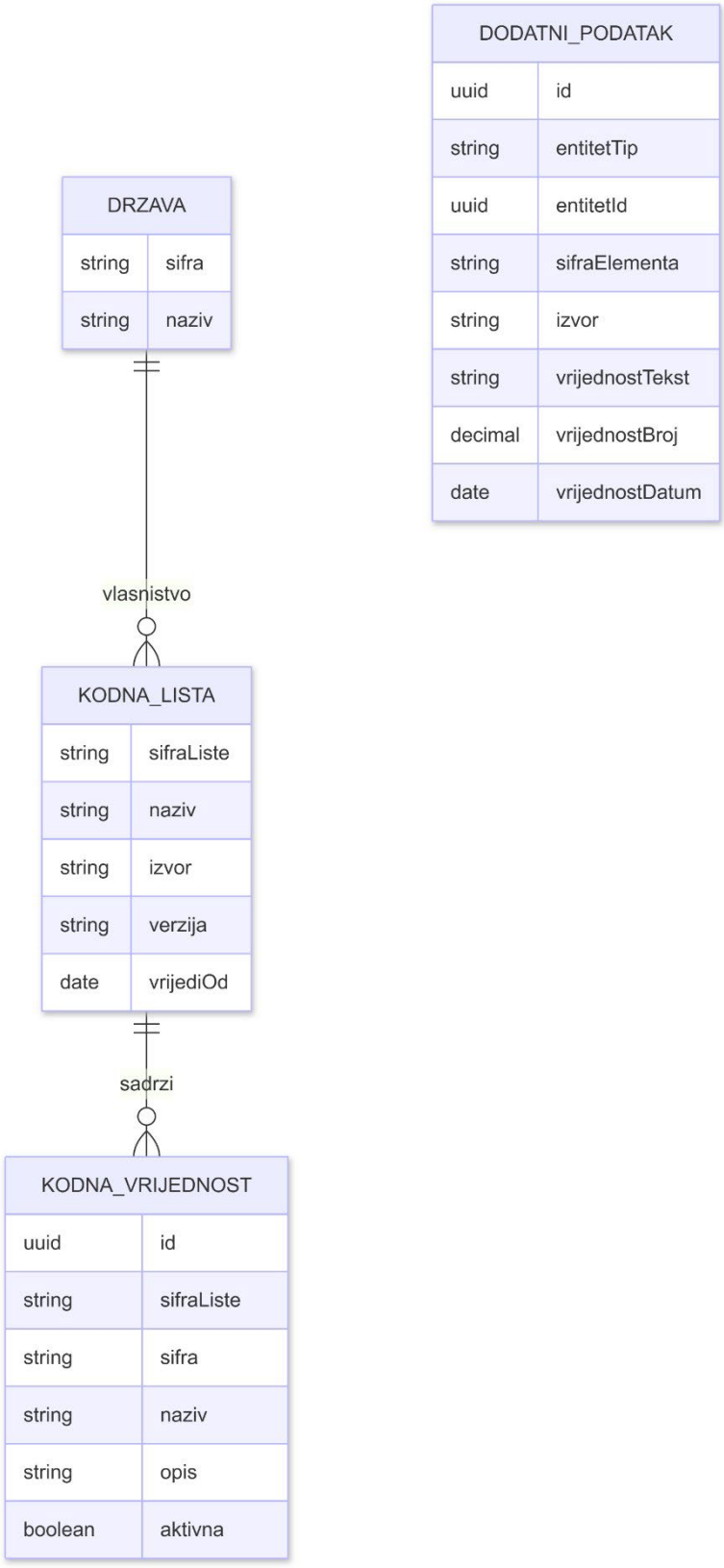
Referentni podaci (subjekti, osobe, lokacije, prijevozna sredstva) predstavljaju stabilan temelj na koji se vežu svi operativni i integracijski zapisi. U praksi to znači da se pošiljke, dionice prijevoza, kontrole i incidenti ne "nose" tekstualne duplikate, nego se pozivaju na jedinstvene zapise subjekata i lokacija. Time se omogućuje ujednačeno izvještavanje, praćenje povijesti i izbjegavanje situacija u kojima se isti sudionik pojavljuje u više varijanti imena ili adrese.

Kodne liste (šifrarnici) nužne su zbog velikog broja tipova i statusa: vrste subjekata, vrste događaja, statusi pošiljke i dionice, vrste kontrole, ishodi kontrole, tipovi dopuštenja, kao i ADR specifične kodne liste (razredi, pakirne skupine, kodovi tunela, kategorije prijevoza). Posebno je važno da šifrarnici podrže **izvor i verziju** (EU ili nacionalno), jer se u prekograničnom okruženju moraju tumačiti iste šifre jednako kroz više država.

Proširivost modela rješava se kombinacijom (a) stabilne jezgre podataka i (b) kontroliranog mehanizma dodatnih elemenata. Jezgra pokriva sve standardizirane i učestale potrebe, dok se dodatni elementi koriste za iznimke i nacionalne specifičnosti bez narušavanja interoperabilnosti. U praksi to znači da se nove nacionalne obveze mogu ugraditi kao "dodatni podaci" vezani uz pošiljku, stavku, događaj ili kontrolu, uz jasnu oznaku izvora i pravila validacije.

U ovom sloju definiraju se i opći standardi: obavezna polja, načini pohrane vremenskih oznaka (planirano/stvarno), poveznice na države (za prekogranični promet) te usklađeni identiteti (OIB gdje je primjenjivo, ali i međunarodni identifikatori subjekata kada se sustav proširi izvan RH).

Financira
Europska unija
NextGenerationEU



Slika 1. Referentni podaci i kodne liste

Financira
Europska unija
NextGenerationEU

- **KODNA_LISTA / KODNA_VRIJEDNOST** služe kao jedinstven mehanizam za statusne i tipovne šifrarnike, uključujući verzioniranje i izvor (EU/nacionalno), što je nužno za održivost u EU okruženju.
- **DODATNI_PODATAK** omogućuje kontrolirana proširenja u iznimnim slučajevima, pri čemu se svaki dodatni element veže na konkretan entitet (pošiljka, stavka, događaj, kontrola) i nosi izvor te tip vrijednosti.

5.3.2. Operativni logistički model: pošiljka, sadržaj, dionice i događaji

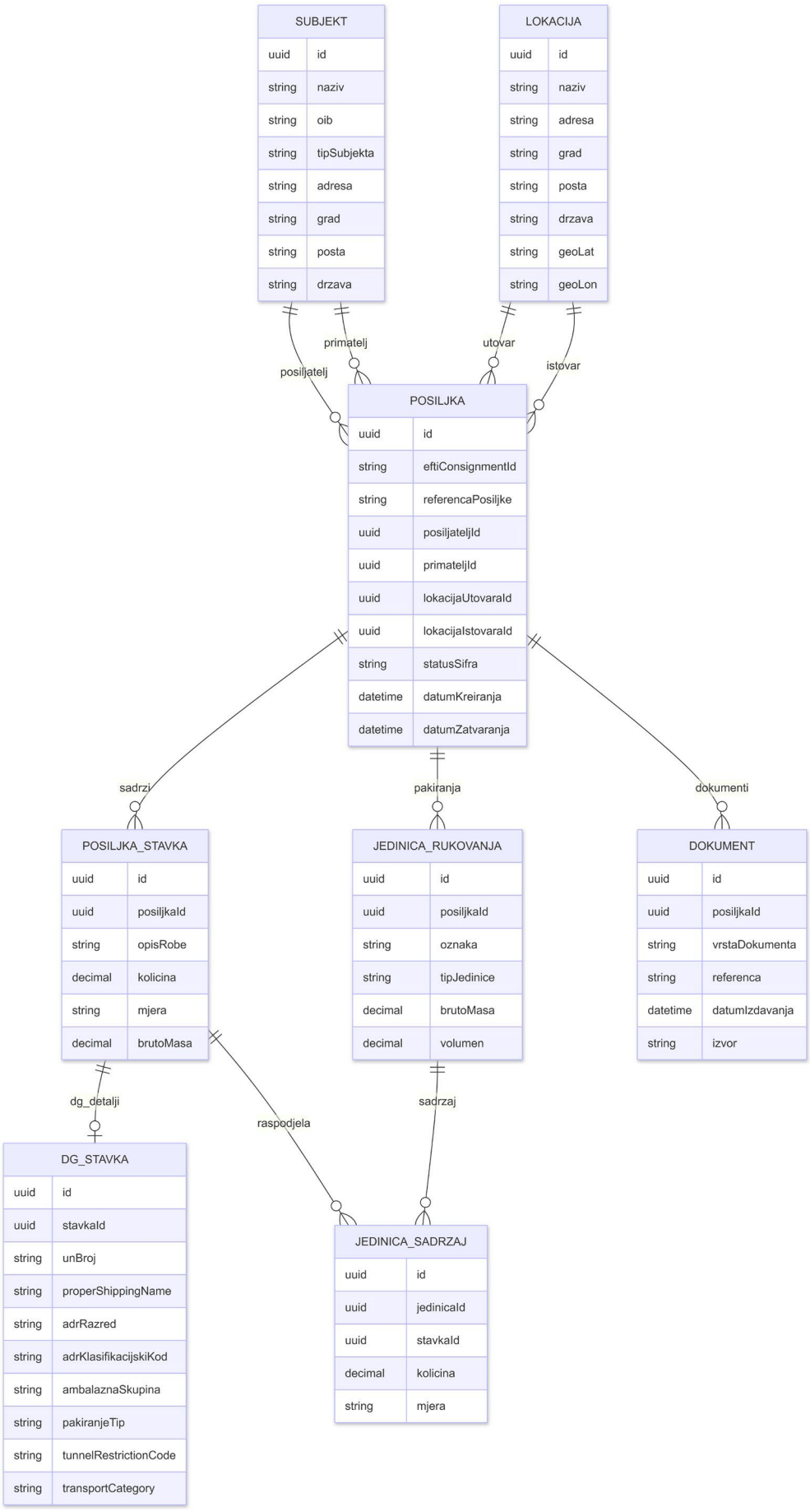
Operativni logistički model pokriva sve situacije u kojima se roba kreće kroz sustav: od nastanka pošiljke, preko modeliranja sadržaja i ambalaže, do stvarnog kretanja po dionicama i evidentiranja događaja. Model je projektiran da prirodno podrži scenarije iz 5.1 gdje jedan kamion istovremeno prevozi više različitih pošiljaka (konsolidacija), a svaka od tih pošiljaka može imati više pretovara i različite destinacije. To se postiže eksplicitnim vezama "više-premaviše" između pošiljke i dionice prijevoza, te praćenjem sadržaja na razini jedinice rukovanja.

Pošiljka se modelira kao poslovni objekt s identitetom, sudionicima (pošiljatelj, primatelj), lokacijama (utovar, istovar) i sadržajem (stavke). ADR specifičnost se u ovom modelu postiže proširenjem stavke kroz DG detalje, čime se omogućuje da ista pošiljka istovremeno sadrži i DG i ne-DG stavke, bez dupliranja osnovne strukture. Dokumenti se vežu uz pošiljku kako bi se pokrile potrebe elektroničke dokumentacije i dokazivosti.

Za pretovare i parcijalne isporuke ključna je razina **jedinice rukovanja** (paleta, IBC, bačva, kontejner, spremnik). Jedinica rukovanja omogućuje precizno praćenje "što je gdje" u trenutku kontrole i nakon promjena vozila. Sadržaj jedinice rukovanja veže se na stavke, što omogućuje da se iz kretanja jedinica rukovanja izvede kretanje DG stavki bez potrebe za dodatnim veznim tablicama na razini stavke.

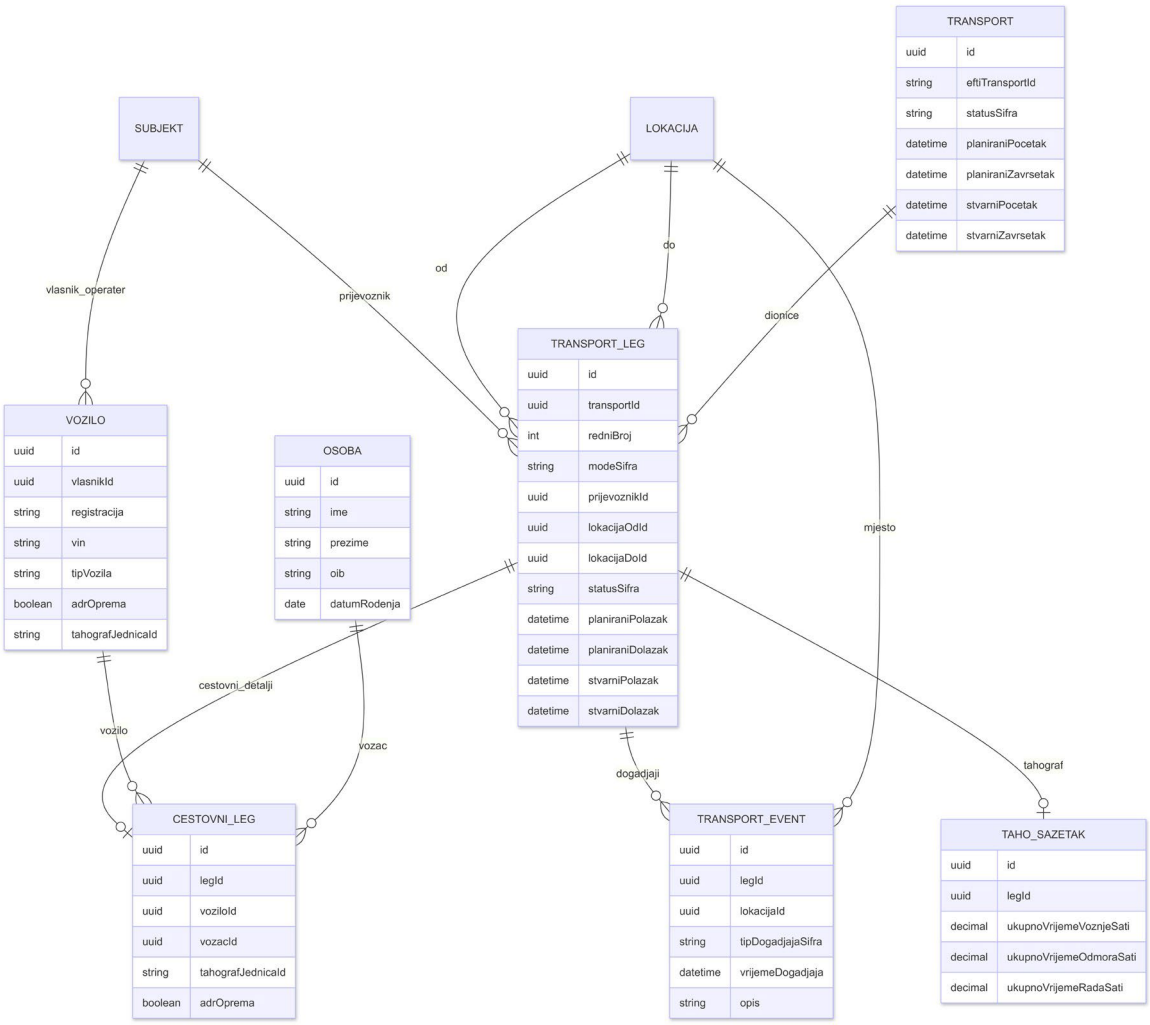
Prijevozna izvedba modelira se kroz transport i dionice (legove). Dionica nosi podatke o vrsti prijevoza (za multimodalnu nadogradnju), prijevozniku, početnoj i završnoj lokaciji, planiranim i stvarnim vremenima te statusu. Događaji (utovar, istovar, pretovar, promjena rute, promjena vozila/vozača, prelazak granice, kontrola, incident) daju vremenski i lokacijski kontekst koji je nužan za dokazivost i kasnije postupanje.

Financira
Europska unija
NextGenerationEU



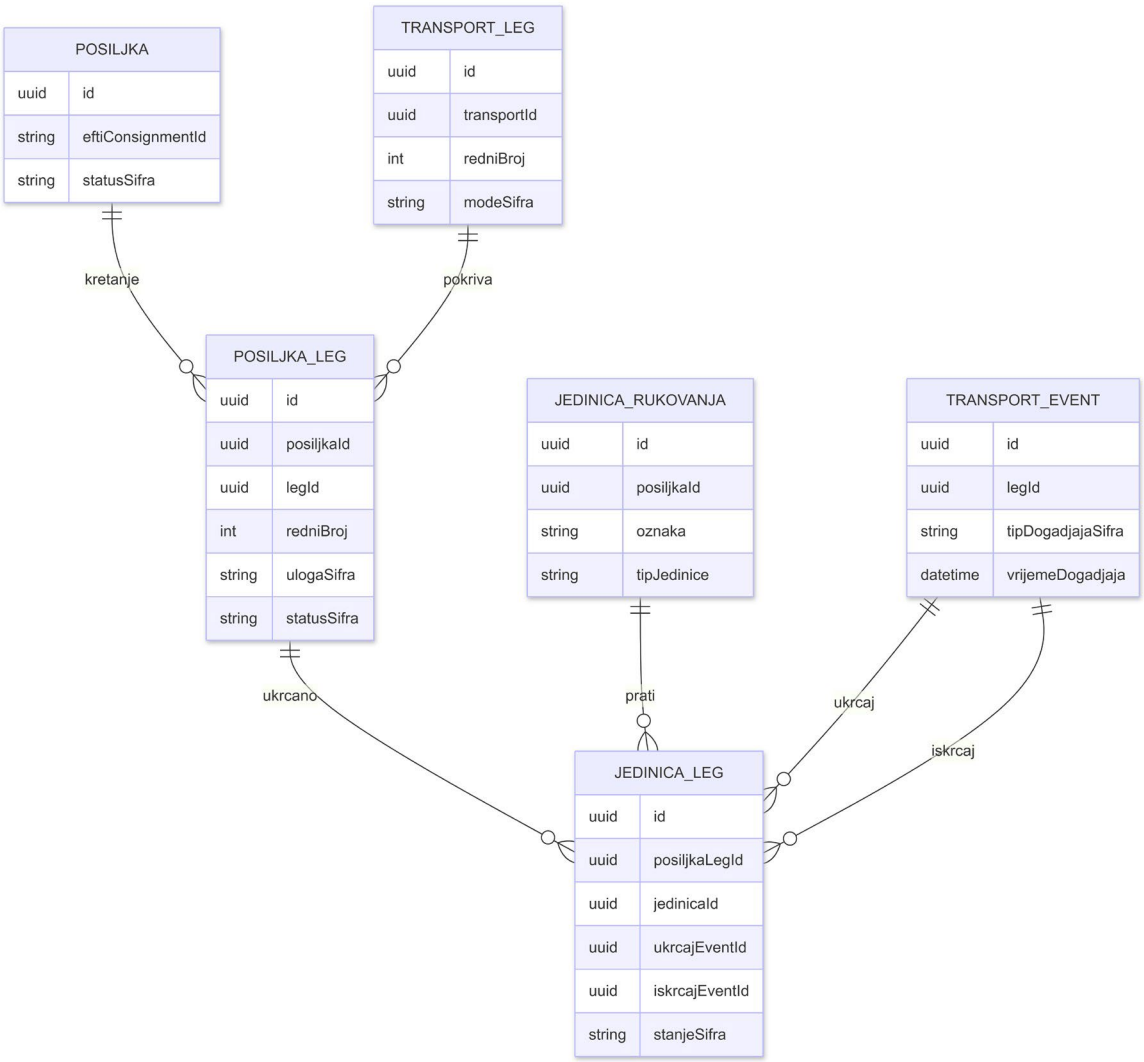
Financira
Europska unija
NextGenerationEU

Slika 2. Logistički model pošiljke i sadržaja



Slika 3. Logistički model transportnih dionica

Financira Europska unija
NextGenerationEU



Slika 4. Model veza pošiljka-dionica

Financira
Europska unija
NextGenerationEU

- **POSILJKA_LEG** je obavezna veza za pokrivanje konsolidacije i pretovara: jedna pošiljka može imati više legova, a jedan leg može nositi više pošiljaka.
- **JEDINICA_LEG** je ključna za stvarne DG scenarije: omogućuje precizno praćenje koje su jedinice rukovanja bile na kojem legu te kada su ukrcane/iskrcane, što je preduvjet za parcijalne isporuke i "više destinacija u jednom kamionu".
- **modeSifra na TRANSPORT_LEG** čini model multimodalno spremnim: cestovni detalji su zasebni (CESTOVNI_LEG), a drugi modovi se mogu dodati istim obrascem bez promjene jezgre.

5.3.3. Model eFTI integracije: platforme, registar identifikatora, metapodatci i selektivni dohvat

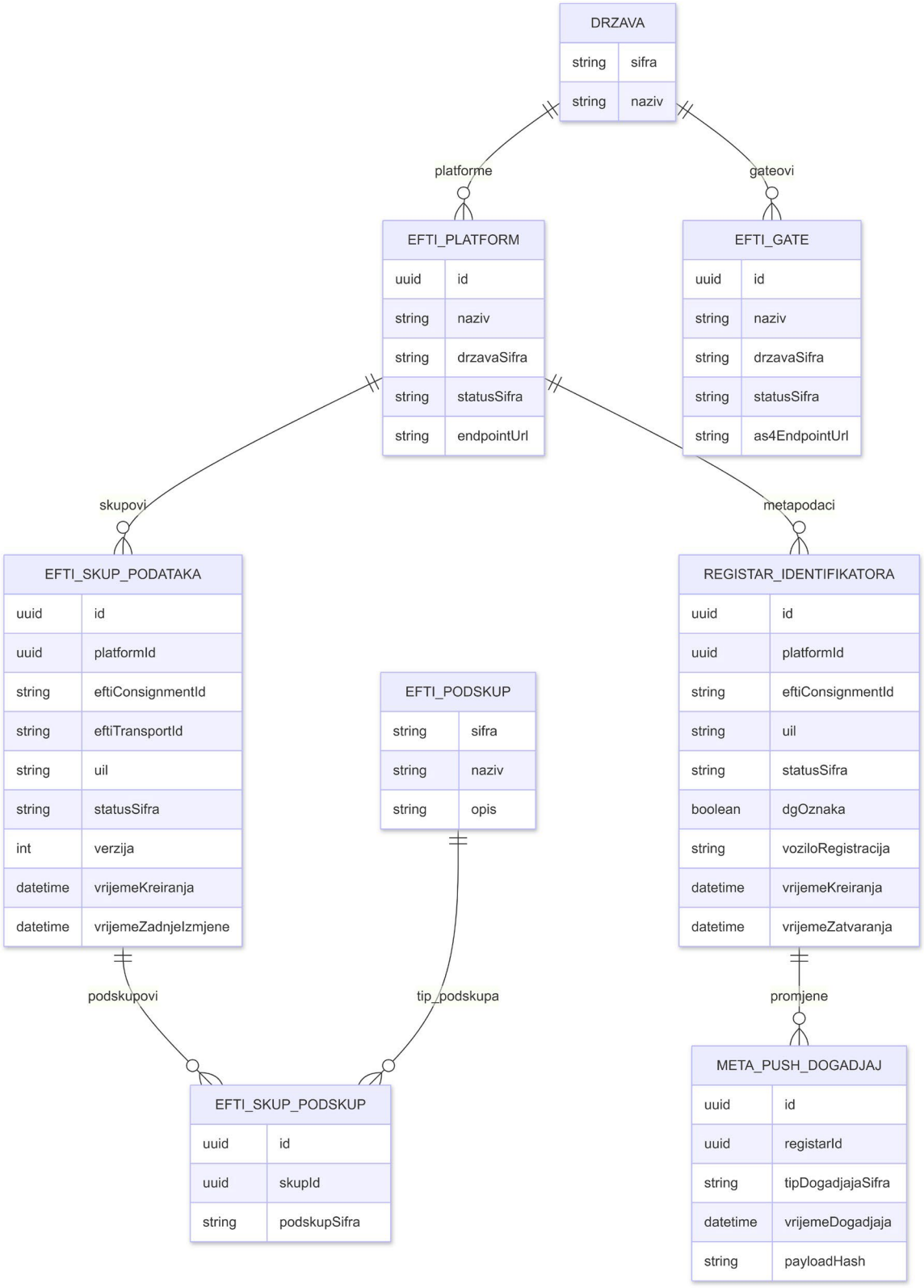
Integracijski model eFTI domene mora podržati dva operativna toka: (1) metapodatkovni uvid temeljen na registru identifikatora i (2) selektivni dohvat punog eFTI sadržaja s platforme. Registar identifikatora omogućuje brzo pretraživanje na temelju kombinacije identiteta pošiljke i identiteta platforme, uz minimalne informacije potrebne službeniku da odluči treba li detaljniju provjeru. Istovremeno, sustav mora čuvati informacije o tome kada je platforma dostavila metapodatke (npr. kreiranje i zatvaranje), te o integritetu tih podataka.

Model platformi i Gateova je nužan zbog prekograničnih scenarija i interoperabilnosti. Platforma je izvor eFTI sadržaja, dok Gate djeluje kao nacionalna točka pristupa i posredovanja. Evidencija platforme uključuje identitet, državu, operativni status i tehničke krajnje točke za razmjenu. Evidencija Gatea se koristi za upravljanje nacionalnim kontekstom, ali i za potrebe međudržavne suradnje kada je pošiljka predmet provjere u više država.

eFTI skup podataka (dataset) modelira se kao instanca koja je vezana uz platformu i identifikatore (consignment/transport), te ima vlastiti životni ciklus i verzioniranje. Uz instancu se veže popis eFTI podskupova (data subsets) koji su uključeni u taj slučaj, što omogućuje jasnu evidenciju da je, primjerice, za DG prijevoz uključen odgovarajući podskup podataka za ADR dokumentaciju. Time se dodatno povećava kvaliteta validacije i usklađenosti.

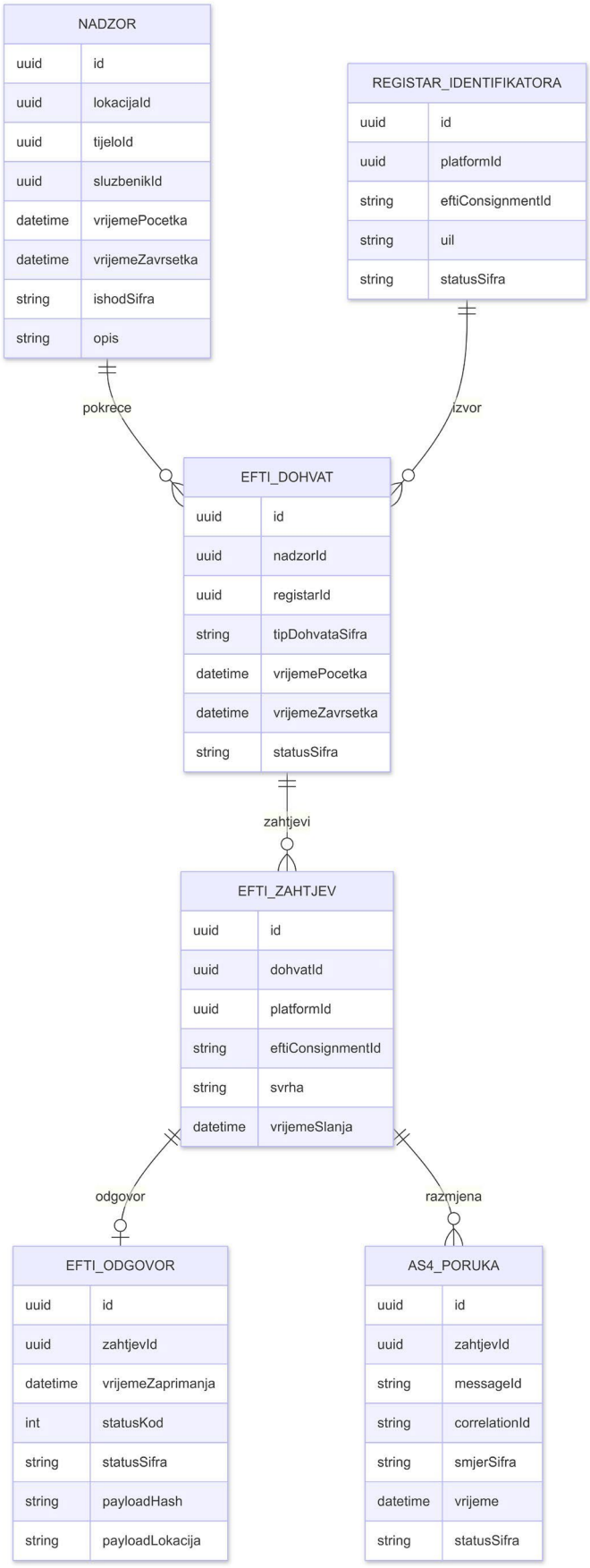
Selektivni dohvat punog sadržaja mora biti modeliran kao transakcijski proces: zahtjev i odgovor, uključujući tehničke metapodatke (vrijeme, status, integritet), vezu na konkretnu kontrolu, te referencu na pohranjeni sadržaj (npr. u repozitoriju dokumenata). Ovaj dio modela je ključan za revizijski trag i dokazivost: sustav mora moći dokazati **tko je tražio podatke, kada, na temelju kojih ovlasti i što je vraćeno**.

Financira
Europska unija
NextGenerationEU



Slika 5. eFTI registar identifikatora i metapodaci

Financira Europska unija
NextGenerationEU



Slika 6. eFTI platforma i AS4 razmjena

Financira
Europska unija
NextGenerationEU

- **REGISTAR_IDENTIFIKATORA** je operativni indeks za brze provjere i mora sadržavati minimalni skup metapodataka potreban službeniku, uz vezu na platformu i UIL.
- **EFTI_DOHVAT / EFTI_ZAHTJEV / EFTI_ODGOVOR** omogućuju potpunu sljedivost selektivnog dohvata, uključujući vezu na konkretnu kontrolu (NADZOR) i tehničke metapodatke potrebne za dokazivost.
- **EFTI_SKUP_PODATAKA i EFTI_SKUP_PODSKUP** eksplicitno bilježe koji su podskupovi podataka bili dostupni za konkretni slučaj, što je bitno za DG scenarije i provjeru usklađenosti.

5.3.4. Nacionalni eADR model: osposobljavanje, dopuštenja, incidenti i nadzorni predmeti

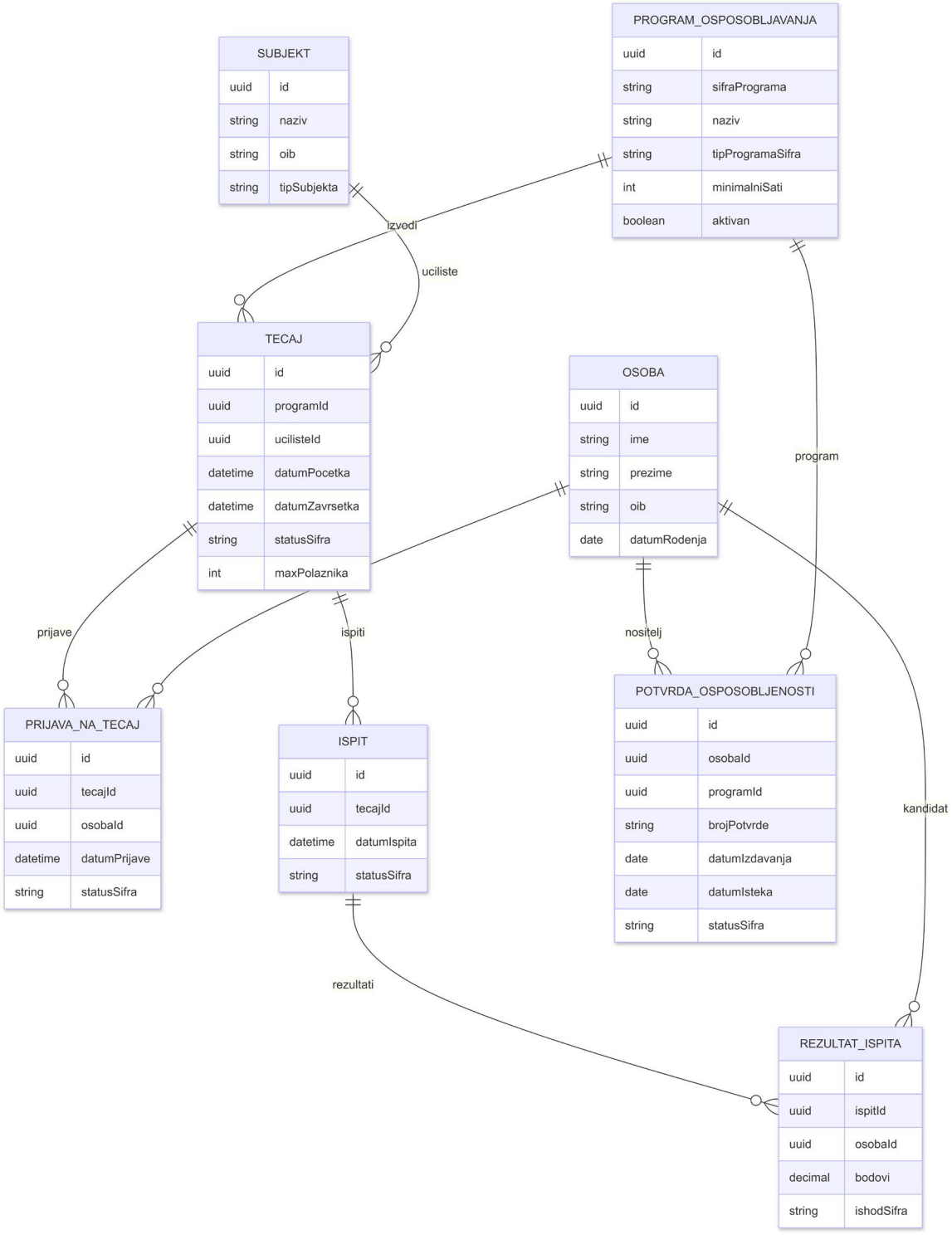
Nacionalni eADR model pokriva poslovne procese koji nisu dio eFTI jezgre, ali su nužni za provedbu ADR kontrola i za donošenje odluka tijekom nadzora. U praksi se radi o provjeri: je li vozač osposobljen, je li potvrda važeća, je li vozilo ovlašteno i opremljeno, te postoje li posebna dopuštenja ili ograničenja. Ovi procesi moraju biti integrirani u kontrolni tijek kako bi službenik dobio jedinstvenu sliku usklađenosti prijevoza.

Model osposobljavanja obuhvaća programe, tečajeve, prijave, ispite, rezultate i potvrde. Ključno je da potvrda bude vezana uz osobu i tip programa, s definiranim datumom izdavanja i isteka te statusom (važeća/istekla/poništena). Time se omogućuje automatizirana provjera valjanosti u trenutku kontrole, ali i naknadno dokazivanje da je u određenom trenutku uvjet bio ili nije bio ispunjen.

Model dopuštenja pokriva različite vrste akata (vrsta dopuštenja), tijela izdavatelje, samu dozvolu i njezin obuhvat (npr. ograničenja po UN broju, ADR razredu ili dodatnim uvjetima). Dopuštenje se može vezati na prijevoznika, vozilo i vozača te, kada je potrebno, eksplicitno povezati s dionicom prijevoza ili pošiljkom. Ovaj dio je ključan za scenarije u kojima se zahtijeva posebna dozvola za određenu tvar ili određeni način prijevoza.

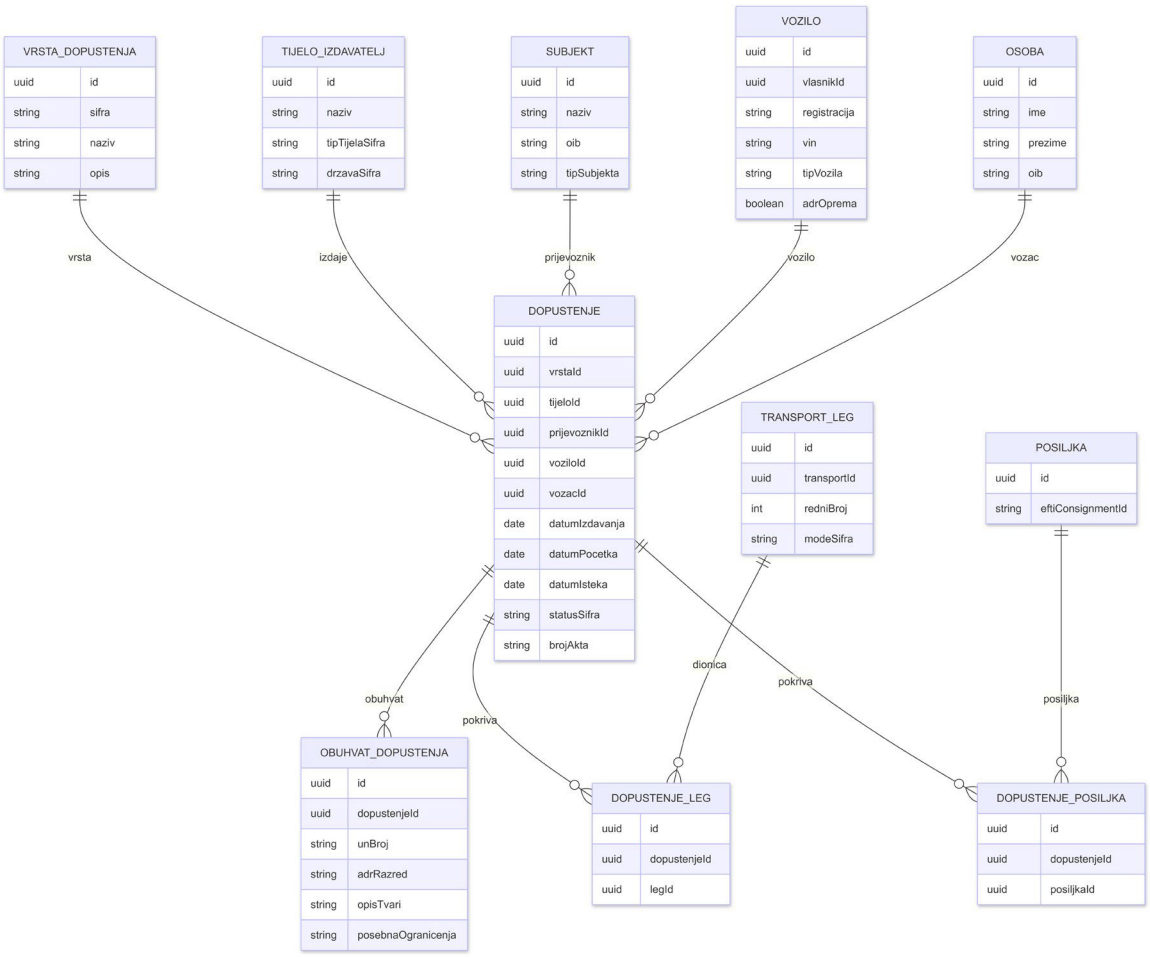
Incidenti i nadzorni predmeti modeliraju se kao proširenje događaja i kontrole. Incident je događaj s dodatnim atributima (tip, status, opis, vrijeme prijave), a nadzorni predmet služi kao “kontejner” za postupanje: povezivanje kontrola, incidenata, mjera i odluka. Time se pokrivaju situacije iz 5.1 gdje se nakon nepravilnosti primjenjuju mjere, izdaju odluke ili se vodi daljnji postupak, uz jasan revizijski trag.

Financira
Europska unija
NextGenerationEU



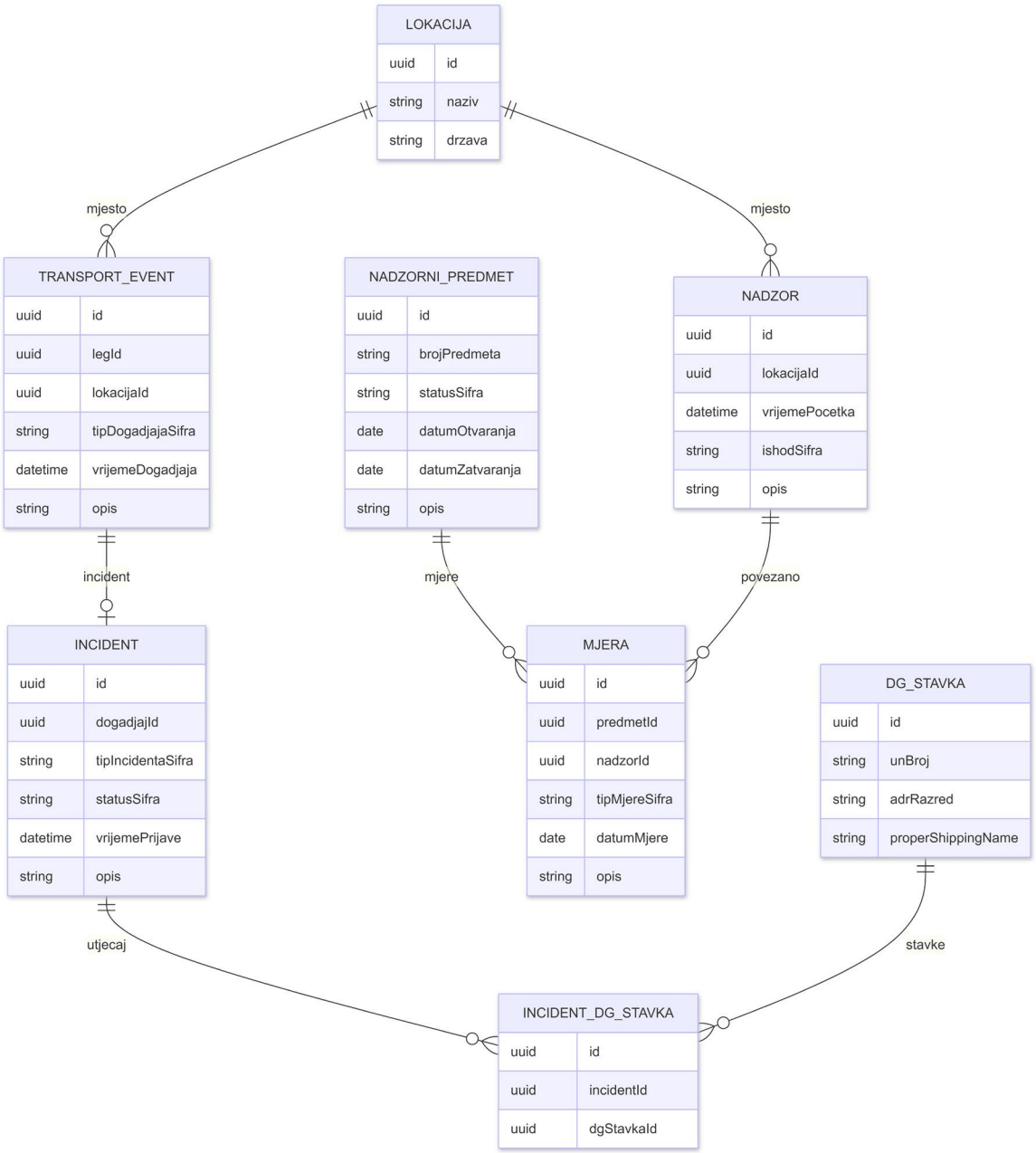
Slika 7. Model osposobljavanja i potvrda

Financira
Europska unija
NextGenerationEU



Slika 8. Model dopuštenja za prijevoz

Financira
Europska unija
NextGenerationEU



Slika 9. Model incidenata i nadzornih predmeta

- **DOPUSTENJE_LEG i DOPUSTENJE_POSILJKA** omogućuju vezivanje dopuštenja na izvedbu (dionicu) ili na poslovni objekt (pošiljku), ovisno o pravilima i vrsti akta, bez gubitka sljedivosti.

Financira
Europska unija
NextGenerationEU

- **INCIDENT i NADZORNI_PREDMET** pokrivaju situacije kada kontrola prelazi u postupanje: incidenti se vežu na događaje, a mjere i odluke vode se kroz predmet radi konzistentne evidencije i revizije.
- **INCIDENT_DG_STAVKA** omogućuje precizno evidentiranje koje su opasne tvari bile obuhvaćene incidentom, što je ključno za izvještavanje i naknadne analize.

5.3.5. Model sigurnosti, ovlasti, revizijskog traga i analitike

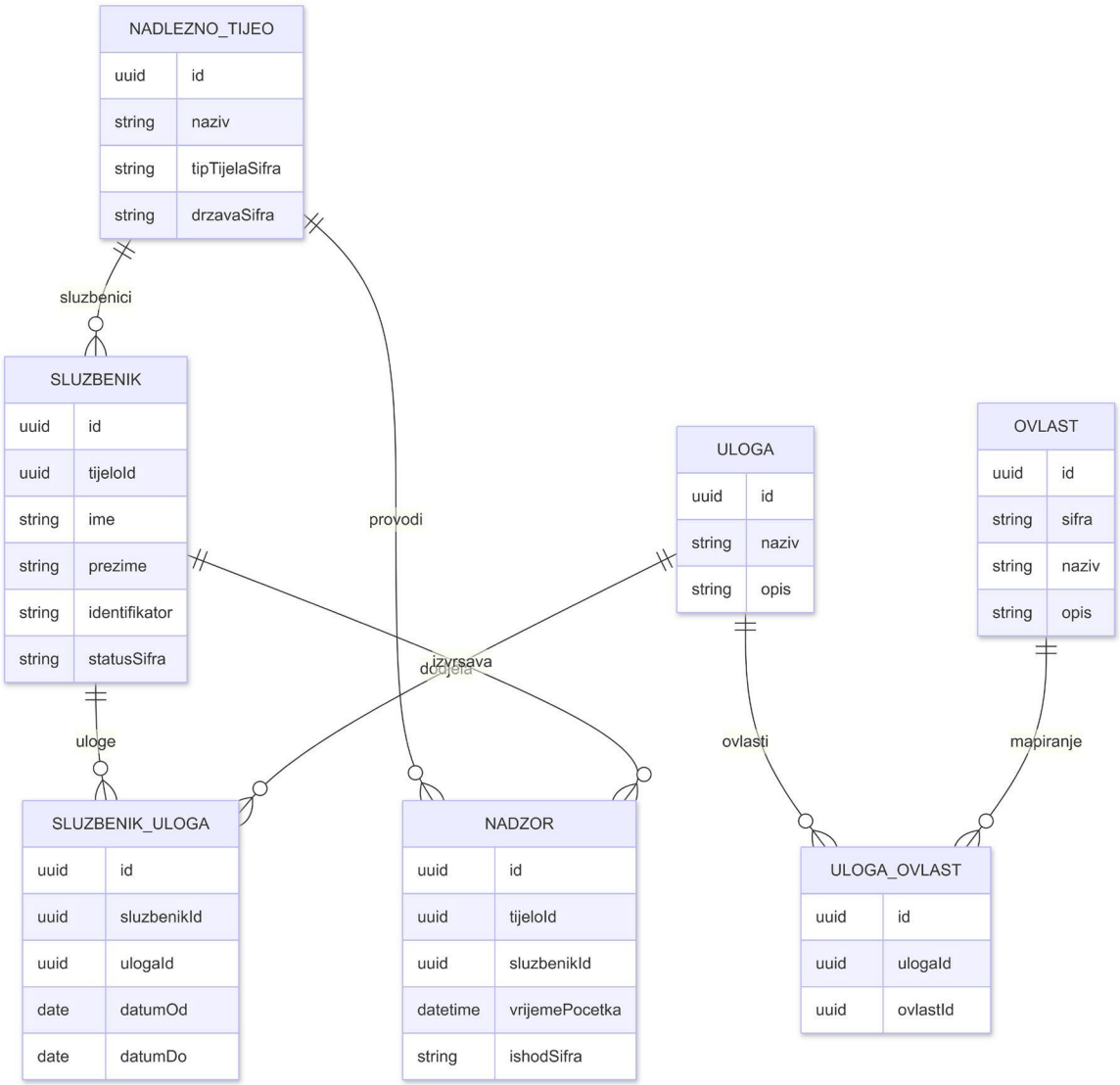
Model sigurnosti i ovlasti mora omogućiti kontrolu pristupa u skladu s ulogama nadležnih tijela i službenika te u skladu s kontekstom provjere. U praksi to znači da se mora znati tko je službenik, kojem tijelu pripada, koje ovlasti ima (npr. pregled metapodataka, selektivni dohvat punih podataka, pokretanje provjere nacionalnih registara), te u kojem razdoblju su te ovlasti bile važeće. Ovaj sloj je neposredno vezan uz dokazivost jer se svaka provjera mora moći povezati s legitimnim identitetom i ovlastima.

Revizijski trag mora obuhvatiti cijeli lanac: od skeniranja i metapodatkovnog upita, preko selektivnog dohvata punog eFTI sadržaja, do eADR provjera i eventualnog otvaranja nadzornog predmeta. Revizijski zapis mora biti dovoljno detaljan da odgovori na pitanja “tko je pristupio, čemu, kada, s kojim razlogom, s kojim ishodom”, te mora uključiti i tehničke identifikatore (korelacijske oznake, poruke) koji povezuju događaje kroz sustave. Ova razina je potrebna i za sigurnosni nadzor, i za naknadno postupanje, i za obranu odluka.

Analitički model se gradi na operativnim zapisima, ali u praksi zahtijeva optimiziranu strukturu (fakt/dimenzije) kako bi se podržalo izvještavanje o volumenu kontrola, stopama nepravilnosti, trendovima, “ponavljačima” i indikatorima rizika. Time se omogućuje da sustav ne bude samo evidencija, nego i operativni alat za upravljanje rizicima i planiranje nadzora. Analitički sloj mora biti usklađen s referentnim podacima kako bi agregacije po prijevozniku, vozilu, lokaciji ili vrsti tereta bile pouzdane.

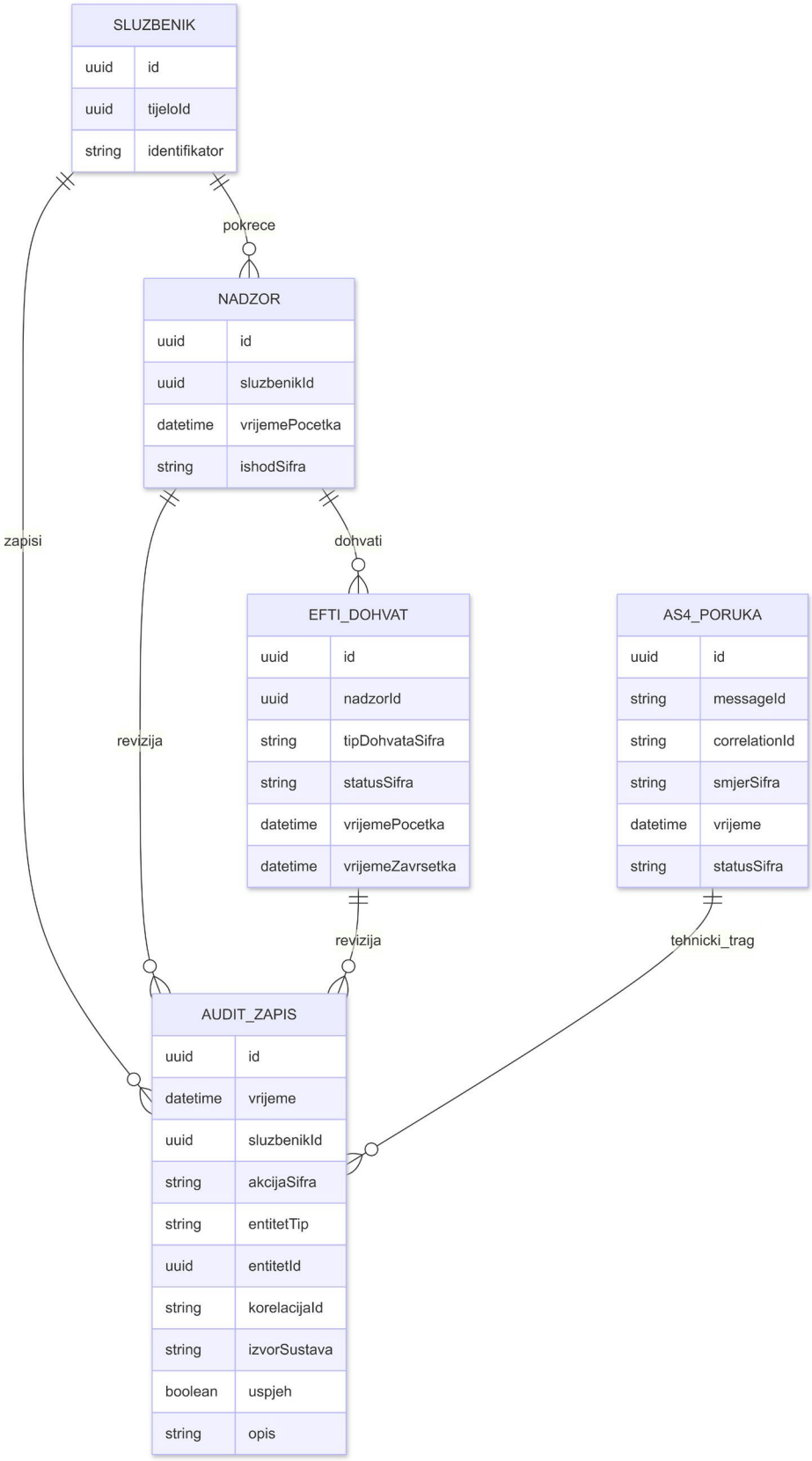
U ovom poglavlju sigurnost, revizija i analitika modeliraju se kao zasebne cjeline koje su povezane s ključnim operativnim entitetima (NADZOR, eFTI dohvat, poruke, pošiljke, dionice). Time se osigurava da se osjetljivi podaci mogu zaštititi, pristupi kontrolirati, a izvještavanje provoditi bez narušavanja performansi operativnog sustava.

Financira
Europska unija
NextGenerationEU



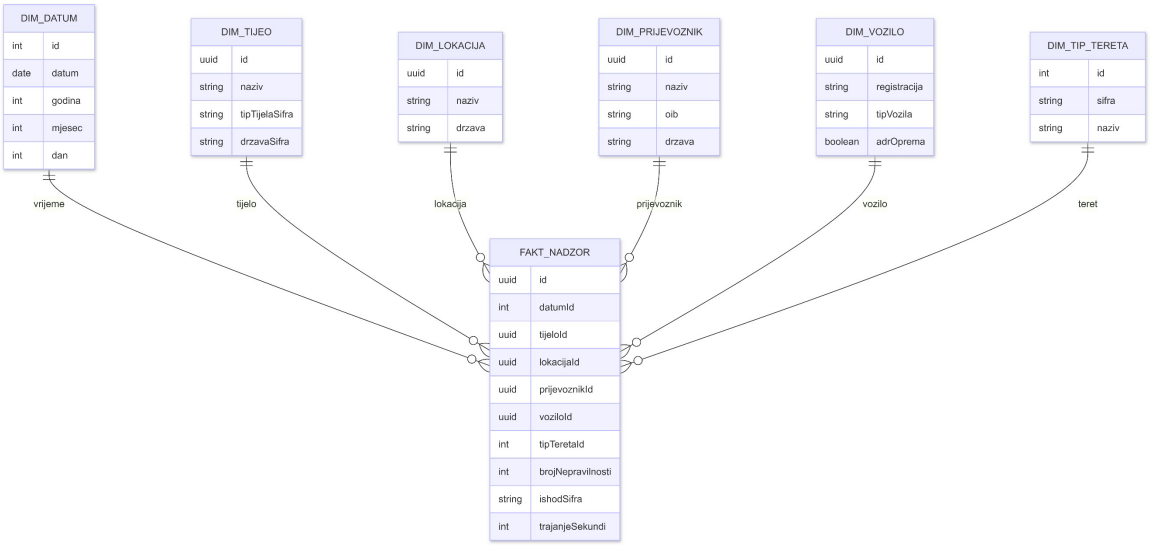
Slika 10. Model sigurnosti i ovlasti

Financira
Europska unija
NextGenerationEU



Slika 11. Model revizijskog traga

Financira
Europska unija
NextGenerationEU



Slika 12. Model analitike i izvještavanja

- **SLUZBENIK / ULOGA / OVLAST** omogućuju jasnu i revizijski provjerljivu kontrolu pristupa, uključujući vremensko važenje dodijeljenih uloga.
- **AUDIT_ZAPIS** je jedinstvena evidencija radnji i pristupa te povezuje poslovne događaje (kontrola, dohvat) s tehničkim tragovima (poruke, korelacije) i ishodima.
- **FAKT_NADZOR i dimenzije** osiguravaju stabilnu osnovu za izvještavanje i indikatore rizika, bez opterećenja operativnih tablica i bez gubitka konzistentnosti s referentnim podacima.

5.4. Integracijski sloj (eFTI, SOTAH, sustavi nadležnih tijela).

Integracijski sloj je **operativna okosnica razmjene podataka** između nacionalnog eFTI čvora, eFTI platformi gospodarskih subjekata, sustava nadležnih tijela (policija, carina, inspekcije) te nacionalnih sustava povezanih uz ADR nadzor, uključujući SOTAH i analitičku platformu AFFINIS. Njegova uloga nije “samo povezivanje”, nego **kontrola pristupa, pouzdana orkestracija tokova i dokaziv audit** za regulatorne potrebe.

U eFTI kontekstu integracijski sloj mora podržati **dva operativna režima rada**: ciljni režim “**metadata push + selective pull**” (metapodaci se unaprijed dostavljaju u Gate, a puni dohvat

Financira
Europska unija
NextGenerationEU

radi se selektivno) te pričuvni režim "**pull only**" (Gate na zahtjev nadležnog tijela dohvaća puni eFTI dataset izravno s platforme). Ova dualnost je ključna za kontinuiranu dostupnost usluge u mješovitom EU okruženju, gdje različite platforme i države mogu biti u različitim fazama zrelosti.

U ADR dijelu integracijski sloj povezuje eFTI tokove s nacionalnim pravilima i provjerama (npr. **valjanost ADR potvrda, ovlaštenja, posebna ograničenja, uvid u tahografske indikatore**). Pri tome se dosljedno odvaja transakcijski i poslovno-kritični dio (eADR evidencije i predmeti) od tahografskog "big data" dijela, gdje je **SOTAH izvor istine**, a AFFINIS služi za analitiku i dugoročnu retenciju.

Dizajn integracijskog sloja mora biti **nadogradiv po vidovima prijevoza i geografski skalabilan** (tranzit na razini EU i šire). To znači da se integracije grade kroz stabilne ugovore (API poruke i AS4 razmjena), uz jasno odvojene adaptere po domenama (eFTI/eDelivery, SOTAH, registri, sustavi tijela), te uz mogućnost dodavanja novih eFTI datasetova i modaliteta (cesta, željeznica, unutarnje vode, a kasnije i drugi).

5.4.1. Arhitekturne komponente i granice odgovornosti

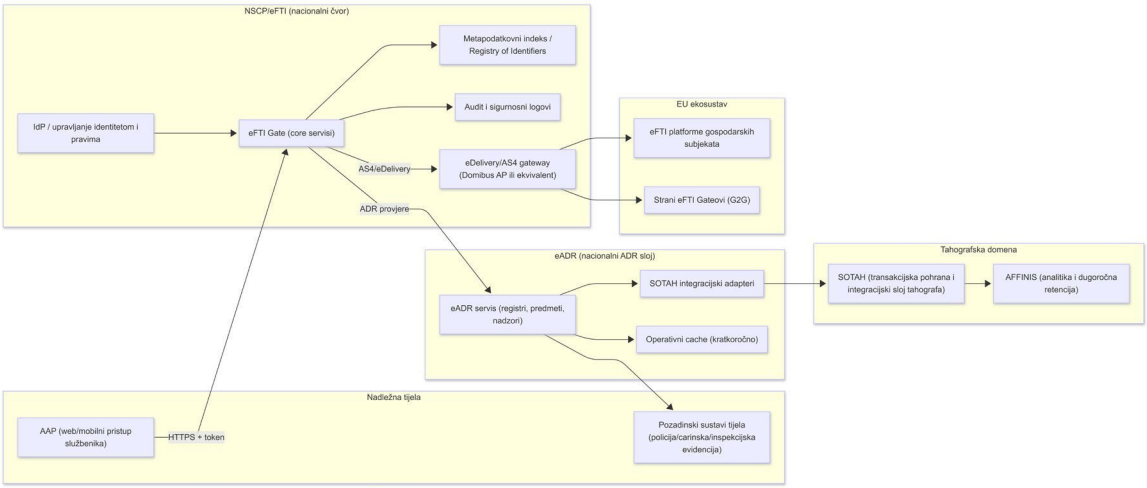
Integracijski sloj se organizira oko tri međusobno povezana bloka: **(1) pristupni i sigurnosni blok**, **(2) eFTI komunikacijski blok**, te **(3) ADR/SOTAH integracijski blok**. Pristupni blok pokriva identitet i prava službenika i tijela (autentikacija/autorizacija, tokeni, revizijski trag). eFTI komunikacijski blok pokriva eDelivery/AS4 komunikaciju prema eFTI platformama i prema drugim nacionalnim Gateovima (G2G), dok ADR/SOTAH blok pokriva specifične provjere i dohvat nacionalnih podataka potrebnih za ADR nadzor.

Ključni princip granica odgovornosti je da **nacionalni eFTI čvor/gateway ostaje "gateway" i orkestrator**, a ne spremište punog sadržaja eFTI dokumenata. U ciljanom režimu rada Gate drži **metapodatkovni indeks (registry of identifiers)** dovoljan za brzu procjenu i usmjeravanje kontrole, dok se puni dataset dohvaća samo kada to stvarno treba (selektivno). Time se smanjuje opterećenje mreže i sustava, a ujedno se zadržava regulatorno ispravan pristup podacima.

Za ADR, eADR servis se ponaša kao **domenski servis**: on konsolidira podatke o dozvolama, potvrdama, nadzorima i incidentima, te poziva SOTAH preko namjenskih adaptera kada treba uvid u tahografsku dimenziju (npr. indikatori rizika, sažeci vremena, relevantni događaji). Time se izbjegava da se u eADR gomilaju volumenski veliki tahografski zapisi, a eADR zadržava fokus na predmetima i odlukama.

Integracijski sloj mora biti projektiran za **visoku raspoloživost i sigurnosnu dokazivost**. To u praksi znači da su kritične komponente (AS4 gateway, registri, audit i eADR) redundantne, da se svi ključni događaji logiraju, te da se sustav može sigurno ponašati i u degradiranom modu (npr. privremeni neuspjeh dohvaćanja punog dataseta, uz ipak dostupne metapodatke i audit da je pokušaj učinjen).

Financira
Europska unija
NextGenerationEU



Slika 13. Arhitektura sustava eADR

5.4.2. Tokovi eFTI podataka: metadata push, metadata lookup i selective pull.

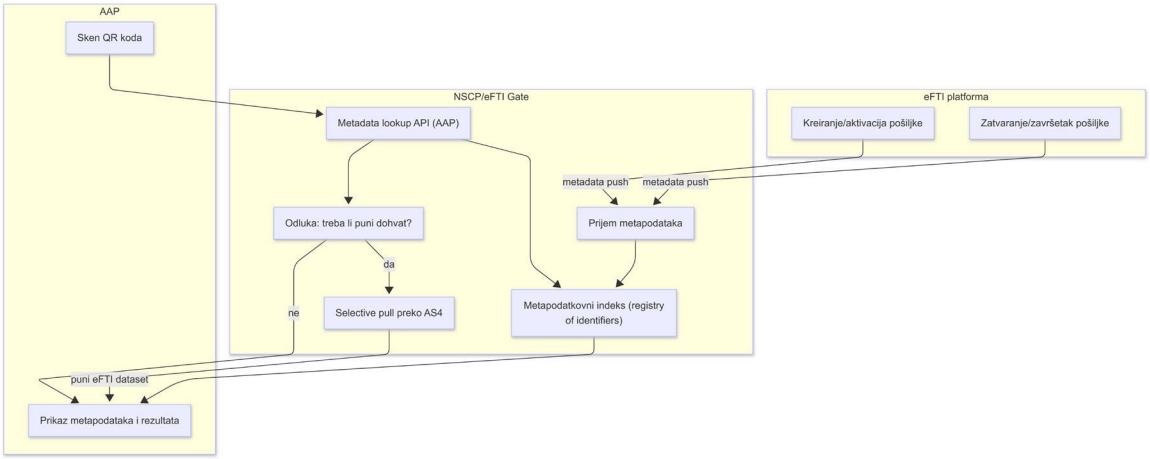
Ciljni operativni tok eFTI integracija temelji se na tome da eFTI platforme unaprijed dostavljaju **metapodatke o pošiljci** u Gateove svih relevantnih država (polazište, tranzit, odredište). Time se omogućava da službenik pri kontroli dobije brzi odgovor na pitanje **"što je ovo i pripada li mojoj nadležnosti"** bez da se svaki put dohvaća puni eFTI dataset.

U praksi se metapodaci dostavljaju najmanje u dva trenutka: **pri kreiranju/aktivaciji pošiljke** i **pri zatvaranju/završetku pošiljke**. Ovi događaji grade životni ciklus pošiljke u metapodatkovnom indeksu, što je ključno da nadzor može razlikovati aktivne od završenih pošiljaka, te da se može dokazati da je kontrola rađena nad valjanim i aktualnim zapisom.

Kada službenik (npr. na granici) skenira QR kod, AAP poziva Gate za **metadata lookup**. Gate u tom koraku, uz provjeru tokena i prava, vraća sažeti, strukturirani prikaz relevantnih elemenata (npr. identifikator pošiljke, status, osnovne podatke o relaciji, indikaciju vrste tereta – opasno/otpad/ostalo). Ako je potrebno, Gate potom pokreće **selective pull**: preko eDelivery/AS4 šalje potpisan i kriptiran zahtjev prema konkretnoj eFTI platformi i dohvaća puni dataset.

Važna implementacijska posljedica je da integracijski sloj mora imati **jasno razdvojene "lake" i "teške" pozive**. "Laki" su HTTP(S) pozivi za lookup prema metapodacima (niska latencija, male poruke), dok su "teški" AS4 pozivi za puni dohvat (kriptografija, veće poruke, veća latencija). Sustav se dimenzionira i optimira tako da većina provjera ostaje u "lakom" režimu, a "teški" dohvat se radi samo kada kontrola to opravda.

Financira Europska unija
NextGenerationEU



Slika 14. Tok eFTI podataka

5.4.3. Orkestracija nadzora: AAP → Gate → eFTI platforma → eADR → SOTAH.

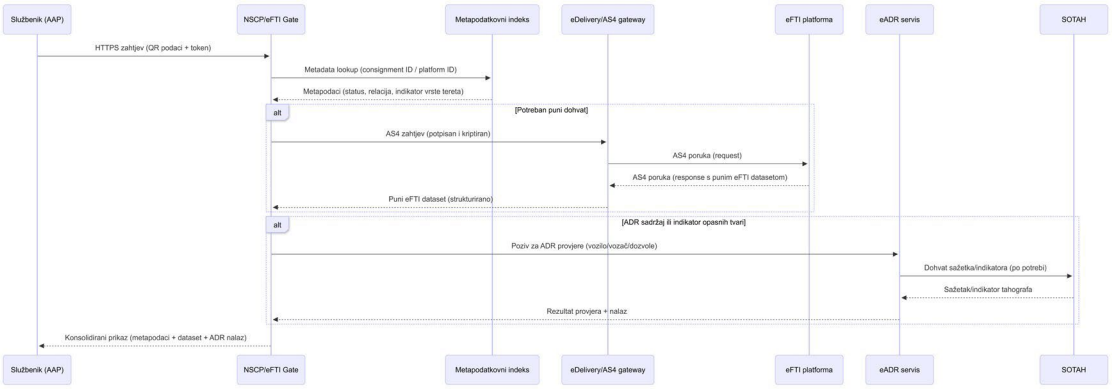
Operativni scenarij nadzora treba biti implementiran kao **orkestrirani tok** u kojem AAP ostaje "tanko" sučelje, a Gate preuzima koordinaciju provjera i dohvaćanja. Time se izbjegava da AAP mora znati detalje o AS4 komunikaciji, o pravima pristupa platformama, ili o ADR provjerama; AAP dobiva standardiziran odgovor prilagođen službeniku.

Nakon skeniranja QR-a, Gate radi tri paralelne provjere koje se međusobno dopunjuju: (1) provjera ovlasti službenika i tijela, (2) dohvat metapodataka i, po potrebi, punog eFTI dataseta, te (3) domena opasnih tvari (eADR) kada metapodaci ili dataset indiciraju ADR sadržaj. Ovakva paralelizacija je praktična jer je većina latencije u vanjskim pozivima, a kontrola na terenu mora imati odgovor u prihvatljivom vremenu.

Kada je teret opasan, Gate poziva eADR servis koji provjerava **valjanost potrebnih potvrda i ovlaštenja** (npr. za vozilo i vozača), te po potrebi dohvaća relevantan sažetak ili indikator iz SOTAHa (npr. za dodatnu procjenu rizika ili za dokazivanje usklađenosti u kontekstu kontrole). Važno je da se u ovom koraku razmjenjuju **sažeci i poslovno relevantne činjenice**, a ne masovni tahografski zapisi; time se smanjuje opterećenje i čuva jasna razdvojenost odgovornosti sustava.

Za pouzdanu implementaciju, svaki korak orkestracije mora imati **korelacijski identifikator** (za audit i dokazivost), te jasno definirane ishode: uspjeh, djelomičan uspjeh (npr. metapodaci dostupni, puni dataset privremeno nedostupan), ili odbijanje pristupa (npr. nevaljan token ili nedovoljna ovlaštenja). AAP u svakom slučaju mora dobiti strukturiran odgovor koji jasno kaže što je provjereno i što nije, bez "skrivenih" grešaka.

Financira Europska unija
NextGenerationEU



Slika 15. Orkestracija nadzora

5.4.4. Integracija eADR-a sa SOTAH-om i AFFINIS-om.

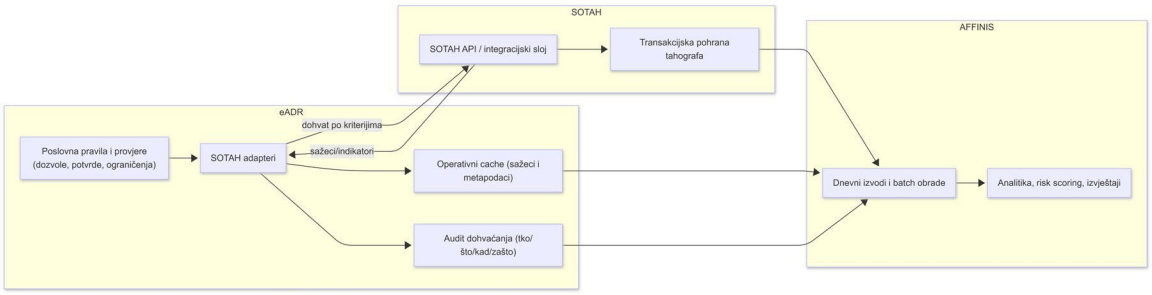
SOTAH je nacionalni sustav za tahografske podatke u kojem se nalazi **transakcijska pohrana i integracijski sloj** te domenske funkcije pristupa i kontrole tahografskih evidencija. eADR ne preuzima ulogu trajnog spremišta tahografa, nego koristi SOTAH kao **izvor istine** i dohvaća samo ono što je potrebno za konkretan nadzorni kontekst (sažeci, indikatori, događaji ograničenog vremenskog obuhvata).

U praksi to znači da eADR implementira **SOTAH integracijske adaptere** koji: (1) provode mapiranje identifikatora (vozilo/tahograf jedinica/vozač), (2) dohvaćaju relevantne podatke prema jasno ograničenim kriterijima (npr. vremenski prozor, tip događaja), te (3) vraćaju podatke u eADR-u u kanonskom obliku prilagođenom ADR provjerama. Adapteri su ključni jer omogućuju da promjene u SOTAH-u (API verzije, sigurnosni mehanizmi, semantika polja) ne "probiju" u eADR poslovnu logiku.

Kako bi se optimirale performanse, eADR održava **operativni cache kratkoročnih sažetaka i metapodataka**, uz strogo ograničenje opsega i retencije (npr. rolling prozor). Cache se koristi za ponavljane provjere istih vozila tijekom kratkog razdoblja, ali se pri svakom pravno relevantnom postupku mora moći dokazati izvor (SOTAH) i vrijeme dohvaćanja, zbog čega cache mora spremati i minimalne audit informacije (kada, tko, u kojem predmetu).

AFFINIS preuzima podatke iz SOTAHa i iz operativnih sustava (nacionalni eFTI čvor/gateway i eADR) radi **analitike, risk scoringa i izvještavanja**, tipično u dnevnim obradama. Integracijski sloj prema AFFINIS-u ne šalje "sirove" payloadove, nego kurirane, strukturirane zapise koji su analitički korisni (npr. događaji kontrola, ishodi nadzora, agregati po prijevozniku/ruti/ADR klasi), čime se dobiva objedinjeni pogled na operativne i sigurnosne aspekte prometa.

Financira
Europska unija
NextGenerationEU



Slika 16. Integracija eADR-SOTAH-AFFINIS

5.4.5. Integracija sa sustavima nadležnih tijela i prekogranična razmjena (G2G).

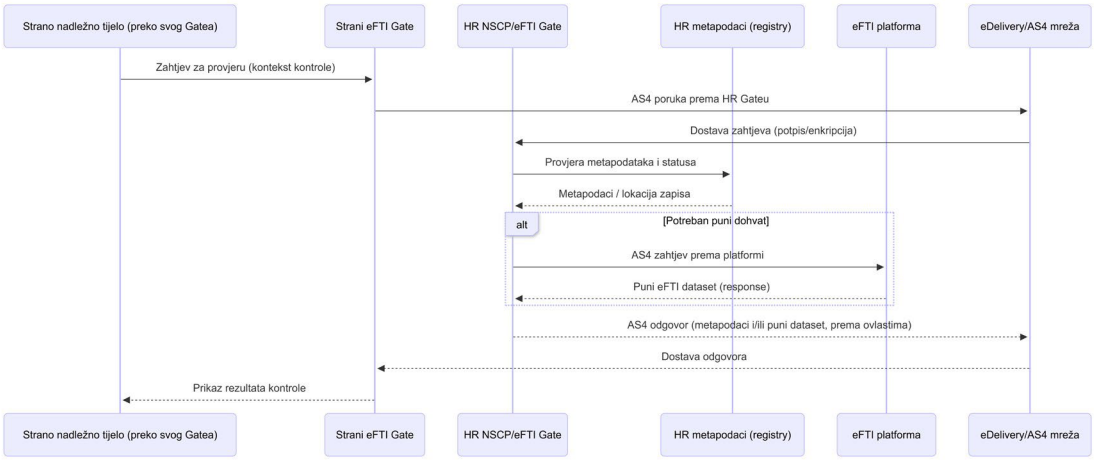
Sustavi nadležnih tijela ulaze u integracijski sloj kroz dva komplementarna kanala: **operativni kanal nadzora** (AAP kao primarno sučelje službenika) i **pozadinski kanal evidencije i postupanja** (sustavi tijela koji trebaju zaprimiti nalaz, otvoriti predmet, povezati kontrolu s internim evidencijama ili pokrenuti daljnje radnje). Integracijski sloj mora osigurati da se podaci koje službenik vidi na terenu mogu, kada je potrebno, dosljedno povezati s "predmetnim" dijelom postupanja, uz jasna pravila o tome što se prenosi, u kojem opsegu i uz koju razinu zaštite.

Prekogranična razmjena (G2G) je ključna jer pošiljke često uključuju više država (polazište, tranzit, odredište), a nadležna tijela drugih država mogu provoditi provjere nad pošiljkama koje prolaze kroz njihovu jurisdikciju. U tom modelu nacionalni Gate mora biti sposoban **primati i slati** upite i odgovore drugim Gateovima preko eDelivery/AS4 mreže, uz punu primjenu sigurnosnih pravila (certifikati, potpis, enkripcija, provjera ovlasti i konteksta provjere).

Operativno, Gate može biti upitan na dva načina: (1) domaće tijelo pita domaći Gate, pa Gate ide prema platformi ili prema drugim Gateovima; ili (2) strani Gate pita domaći Gate u kontekstu pošiljke gdje je RH polazište/odredište/tranzit i gdje domaći Gate raspolaže metapodacima ili može posredovati. U oba slučaja sustav mora striktno primijeniti **princip najmanjih privilegija**: dostupnost podataka ovisi o ulozi tijela, kontekstu provjere i pravilima datasetova.

Za praktičnu implementaciju posebno su važni mehanizmi **idempotentnosti, ponavljanja i upravljanja vremenom**. AS4 poruke i vanjske integracije moraju imati stabilne identifikatore zahtjeva, kontrolu ponovnog slanja (retry) i vremenska ograničenja (timeout) tako da se izbjegnu duplikati u audit evidencijama i da se službeniku na terenu vrati jasan status. Sustav treba podržati i degradirani način rada (npr. samo metapodaci) uz eksplicitno označavanje da puni dohvat nije bio moguć u trenutku kontrole.

Financira Europska unija
NextGenerationEU



Slika 17. Prekogranična razmjena G2G

5.5. Sigurnosni sloj (upravljanje identitetima, kontrole pristupa, zapisnici događaja)

Sigurnosni sloj osigurava da svi poslovni slučajevi uporabe iz domene eFTI/ADR budu provedeni na način koji je **pravodobno dokaziv, tehnički pouzdan i regulatorno prihvatljiv**. U ovom sustavu sigurnost nije izdvojena "IT tema", nego izravna podrška kontroli na terenu: službenik mora dobiti podatke brzo, ali samo u opsegu koji je nužan i samo ako postoje valjane ovlasti, dok sustav mora moći rekonstruirati tko je i zašto pristupio kojim podacima.

S obzirom na operativni koncept rada (metapodatkovni uvid kroz registar identifikatora te selektivni puni dohvat eFTI sadržaja), sigurnosni sloj mora razlikovati **"laki" režim pristupa** (metapodatkovni pregled) i **"teški" režim pristupa** (puni dohvat s eFTI platforme putem eDelivery/AS4). Ova razlika uvodi jasna pravila: metapodatci se koriste za brzu procjenu i usmjeravanje, dok se puni dataset dohvaća samo kada postoji potreba i valjana ovlast, uz strože nadzorne mehanizme i detaljniji revizijski trag.

Sigurnosni sloj obuhvaća tri povezane cjeline: **upravljanje identitetima** (službenici i sustavi), **kontrole pristupa** (autorizacija i filtriranje podataka) te **zapisnike događaja** (audit i sigurnosni logovi). Te cjeline moraju biti ujednačene kroz cijeli ekosustav: AAP kao pristupna aplikacija, nacionalni eFTI Gate kao centralna točka pristupa, eADR servis za nacionalne provjere, te integracijski kanali prema SOTAH-u i eFTI platformama.

U prekograničnom okruženju sigurnosni sloj mora podržati i razmjenu s drugim nacionalnim Gateovima (G2G), pri čemu se dodatno naglašava **princip najmanjih privilegija**: svaki prekogranični zahtjev mora biti vezan uz nadležno tijelo, kontekst provjere i pravnu osnovu, a odgovor mora biti ograničen na dopuštene podatkovne podskupove. Ujedno se mora osigurati da su svi zahtjevi i odgovori potpisani, kriptirani i korelirani s revizijskim tragom.

Financira
Europska unija
NextGenerationEU

5.5.1. Upravljanje identitetima i životni ciklus korisnika i sustava

Upravljanje identitetima mora obuhvatiti i **ljudske korisnike** (službenike i administratore) i **sustavne identitete** (servise i integracijske komponente). Ljudski identiteti koriste se za rad u AAP-u i za pokretanje postupaka nadzora, dok se sustavni identiteti koriste za servisne integracije (npr. Gate prema eFTI platformama putem AS4, Gate prema eADR servisu, eADR prema SOTAH-u). Obje skupine moraju imati jasno definiranu pripadnost organizaciji, status (aktivan/neaktivan) i vremensku valjanost.

Višefaktorska autentikacija obavezna je za pristup kritičnim sustavima i administraciji, uključujući udaljeni pristup (VPN), administrativni pristup kritičnoj infrastrukturi te alate i usluge izložene internetu kada je to tehnički podržano. Upravljanje korisnicima i pravima mora biti centralizirano (integracija s imenikom organizacije), a vanjski korisnici moraju pristupati sustavu putem nacionalnog identifikacijskog i autentikacijskog sustava.

Za sustave gdje višefaktorska autentikacija nije tehnički moguća, moraju se primijeniti lozinke minimalne duljine 12 znakova uz zahtjeve kompleksnosti (velika i mala slova, znamenke i posebni znakovi). Lozinke moraju biti zaštićene tijekom unosa te šifrirane/nečitljive pri prijenosu i pohrani. Grupni, zajednički ili nepersonalizirani korisnički računi moraju biti uklonjeni ili strogo kontrolirani kao generički računi uz istu razinu kompleksnosti i odgovornosti.

Privilegirane uloge moraju biti jasno definirane i ograničene načelima poslovne potrebe, najmanjih ovlasti i razdvajanja nadležnosti. Minimalno se moraju pokriti uloge: službenik za sigurnost (upravljanje sigurnosnim politikama), administrator (instalacija i održavanje), operator (nadzor i svakodnevno upravljanje) i revizor (pregled revizijskih zapisa).

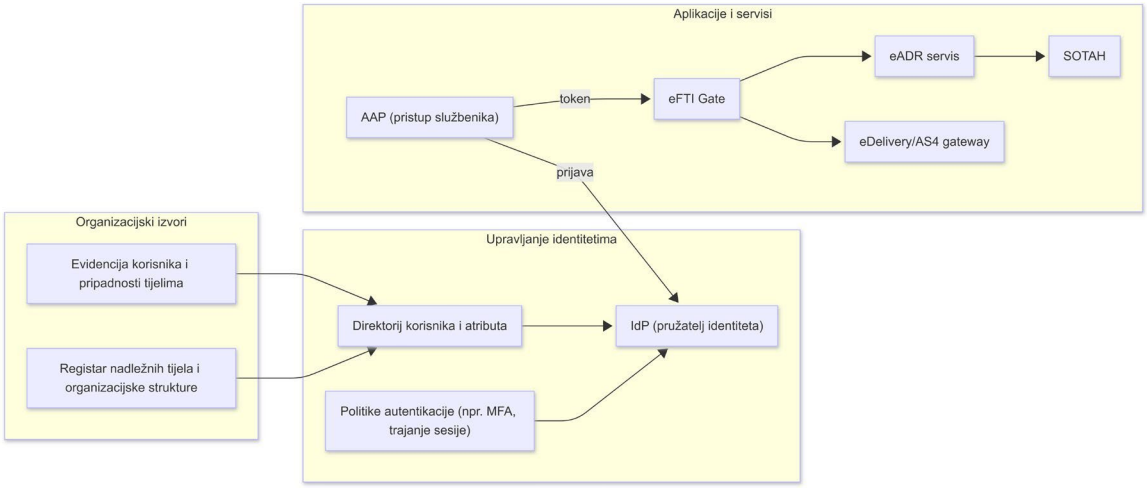
Ljudski identiteti upravljaju se preko centralnog pružatelja identiteta (IdP), uz standardizirani mehanizam prijave temeljen na suvremenim protokolima (npr. OpenID Connect/OAuth 2.0). IdP mora podržati **stroge zahtjeve autentikacije**, uključujući snažnu lozinku, višefaktorsku autentikaciju gdje je propisano, te ograničenja trajanja sesije. Posebno je važno da se identitet veže na **nadležno tijelo** i da se promjene organizacijskog statusa (zapošljavanje, premještaj, suspenzija, prestanak ovlasti) odraze kroz kontrolirani životni ciklus računa.

Sustavni identiteti trebaju koristiti **certifikate i/ili servisne tokene** s minimalnim opsegom (scopes) i jasnim pravilima rotacije. Za eDelivery/AS4 komunikaciju uobičajeno je da identitet sustava proizlazi iz certifikata i povezanih trust mehanizama, pri čemu se mora osigurati da su certifikati ažurni, opozivi provjerivi i da su ključevi zaštićeni. Sustavni identiteti moraju biti strogo odvojeni od ljudskih identiteta, uz zasebne politike i reviziju.

- **Službenik** identitet koristi za rad u AAP-u, a njegova prava proizlaze iz pripadnosti nadležnom tijelu i dodijeljenih uloga; ukidanje ovlasti mora automatski onemogućiti pristup bez odgode.
- **Administrator sustava** ima proširene ovlasti, ali uz strože kontrole (razdvajanje dužnosti, dodatna autentikacija i obvezno evidentiranje svih administrativnih radnji).

Financira Europska unija
NextGenerationEU

- **Servisni identitet** koristi se isključivo za komunikaciju između sustava (npr. Gate–platforma, eADR–SOTAH) i mora imati minimalan skup dozvola, rotaciju tajni i jasnu povezanost s komponentom koja ga koristi.



Slika 18. Upravljanje identitetima

U ovom modelu identiteti i atributi (tijelo, uloge, status, vremenska valjanost) održavaju se centralno, dok aplikacije koriste standardizirane tokove prijave i provjere tokena. Time se postiže ujednačeno ponašanje kroz cijeli sustav i izbjegava dupliciranje korisničkih baza po komponentama.

5.5.2. Kontrole pristupa, autorizacija i filtriranje podataka

Kontrola pristupa mora biti provedena tako da Gate u svakom trenutku djeluje kao **centralna točka provedbe pravila**. To znači da AAP ne smije samostalno odlučivati koji podaci su dopušteni, nego uvijek šalje zahtjev s vjerodajnicom (token) i kontekstom, a Gate provodi provjeru identiteta, ovlasti i dopuštenog opsega podataka. Takav pristup omogućuje jednoznačnu provedbu politike, jednostavnije upravljanje promjenama i konzistentan revizijski trag.

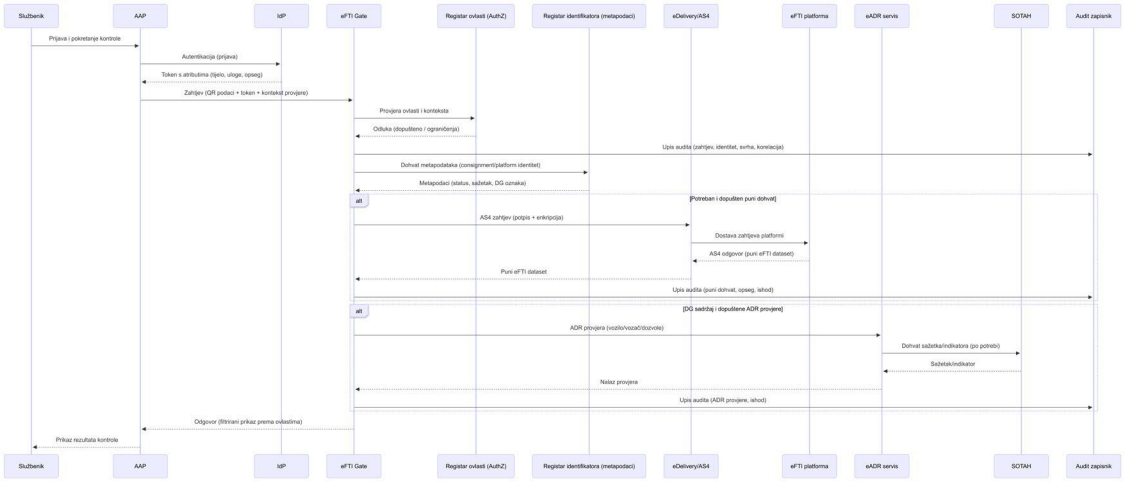
Autorizacija se provodi kombinacijom **upravljačkog modela temeljenog na ulogama** (RBAC) i **pravila ovisnih o kontekstu** (ABAC). Uloge (npr. policija, carina, inspekcija) daju osnovni skup dozvola, dok atributi konteksta (npr. lokacija kontrole, vrsta postupanja, status pošiljke, prekogranični kontekst, traženi podatkovni podskup) dodatno sužavaju ili proširuju dopuštenja. Posebno je važno da se razlikuje pristup metapodacima i pristup punom eFTI datasetu, pri čemu puni dohvat mora biti dozvoljen samo kada je svrha provjere opravdana i kada su ovlasti jasne.

Filtriranje podataka mora biti implementirano kao **sustavna mjera minimizacije podataka**. U praksi to znači da se pri metapodatkovnom uvidu vraća samo sažetak potreban za odluku o

Financira Europska unija NextGenerationEU

daljnjem postupanju, dok se kod punog dohvata dataset može dodatno filtrirati prema dopuštenim podskupovima i pravilima prikaza (npr. ograničenje polja koja nisu nužna za konkretnu provjeru). Time se smanjuje izloženost osjetljivih podataka i olakšava usklađenost s pravilima zaštite podataka.

- **Ovlasti za metapodatke** uključuju pregled statusa i osnovnih identifikatora te indikaciju vrste tereta; cilj je brza procjena bez izlaganja detalja sadržaja.
- **Ovlasti za puni dohvat** uključuju selektivno dohvaćanje kompletnog eFTI sadržaja s platforme i prikaz detalja potrebnih za dokazivanje usklađenosti; ove ovlasti su strože i zahtijevaju detaljniji audit.
- **Ovlasti za ADR provjere** uključuju pozivanje eADR servisa radi provjere valjanosti potvrda, dopuštenja i ograničenja, te po potrebi dohvat sažetaka iz SOTAHa; pristup se ograničava na podatke relevantne za predmetnu kontrolu.



Slika 19. Kontrole pristupa i autorizacija

Ovaj tok jasno razdvaja odgovornosti: AAP je korisničko sučelje, IdP izdaje vjerodajnice, Gate provodi autorizaciju i minimizaciju podataka, dok su eFTI platforme i SOTAH izvorni sustavi za specifične domene. Audit zapisnik se vodi kroz cijeli tok kako bi se svaka odluka i dohvat mogli dokazati i rekonstruirati.

5.5.3. Sigurna komunikacija i kriptografska zaštita integracijskih kanala

Sigurna komunikacija mora pokriti sve vanjske i unutarnje tokove: AAP prema Gateu, Gate prema eADR servisu, eADR prema SOTAH-u, te Gate prema eFTI platformama i drugim Gateovima preko eDelivery/AS4. Za HTTP(S) kanale obvezna je komunikacija preko TLS-a, uz primjenu stroge konfiguracije kriptografskih skupova, kontrolu certifikata i zaštitu od degradacijskih napada. U segmentima gdje se prenose osjetljivi podaci preporučuje se i **dvosmjerna autentikacija certifikatom (mTLS)**, posebno između kritičnih internih servisa.

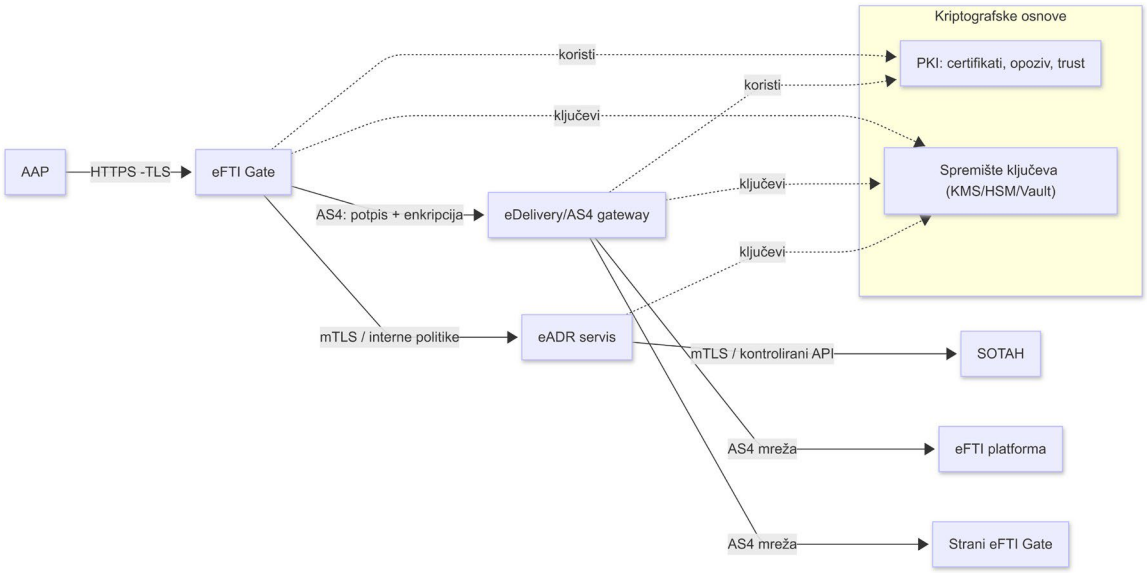
Financira Europska unija
NextGenerationEU

Za eDelivery/AS4 komunikaciju, sigurnost se provodi na razini poruka: poruke se **potpisuju i kriptiraju**, a primatelj verificira identitet i integritet. Time se osigurava da zahtjev i odgovor zadržavaju dokaznu vrijednost i u scenarijima prosljeđivanja ili odgođene isporuke poruke.

Važno je da se poruke koreliraju jedinstvenim identifikatorima kako bi se moglo dokazati koji odgovor pripada kojem zahtjevu i kojoj kontroli.

Kriptografska zaštita mora biti dopunjena pravilima pohrane: svi osjetljivi podaci koji se privremeno spremaju (npr. dohvaćeni dataset, tehnički artefakti razmjene) moraju biti šifrirani "u mirovanju" i dostupni samo kroz strogo kontrolirane servise. Ujedno, svi kriptografski ključevi moraju biti izdvojeni iz aplikacijskog koda, upravljani centralno i rotirani prema pravilima, kako bi se spriječilo dugotrajno kompromitiranje.

Dodatno, komunikacijski sloj mora imati ugrađene mjere otpornosti: ograničenja frekvencije poziva, zaštitu od preopterećenja, vremenska ograničenja i kontrolu ponavljanja (retry) tako da sustav ostane operativan i u degradiranim uvjetima, uz jasno bilježenje djelomičnih neuspjeha. Ovo je osobito važno za terenske kontrole gdje se očekuje brzi odgovor i gdje povremene mrežne poteškoće ne smiju proizvesti nedokazive ili nekonzistentne rezultate.



Slika 20. Sigurna komunikacija i kriptografija

Dijagram prikazuje kako se sigurnost provodi različitim mehanizmima ovisno o kanalu: TLS/mTLS za API komunikaciju te potpis i enkripcija na razini poruka za AS4. PKI i centralno spremište ključeva predstavljaju zajedničke temeljne ovisnosti koje moraju biti pouzdane i strogo upravljane.

Mrežna segmentacija i zone sustava

Financira Europska unija
NextGenerationEU

Infrastruktura eADR-a mora biti smještena u segmentiranim mrežnim zonama uz jasno razdvajanje sigurnih i nesigurnih mreža. Sigurne mreže koje sadrže kritične komponente (aplikacijski poslužitelji, baze podataka, sustavi za upravljanje sigurnošću i nadzor) moraju biti logički odvojene od nesigurnih mreža (internet i poslovna/uredska mreža) te tretirane kao operativno-tehnološke mreže i konfigurirane u skladu s dobrim praksama za takva okruženja.

Arhitektura mora provoditi komunikacijska pravila:

- Uspostavlja se demilitarizirana zona (DMZ) i ne smije postojati izravna konekcija između nesigurnih i sigurnih mreža.
- Sva komunikacija između nesigurnih i sigurnih mreža mora prolaziti kroz kontrolnu točku u DMZ-u gdje se provodi terminiranje konekcije, inspekcija i nadzor prometa.
- Nije dopuštena izravna komunikacija DMZ ↔ sigurnosna zona s kritičnim podacima.
- Između zona propušta se isključivo šifrirana komunikacija.
- Primjenjuju se principi nultog povjerenja u mrežnom pristupu: svi korisnici i uređaji tretiraju se kao nepouzdani dok se ne verificiraju.

Dijagram mreže i topologije su obavezna isporuka: (1) high-level dijagram s prikazom zona, kontrolnih točaka i veza prema vanjskim sustavima; (2) detaljni dijagram tijekom implementacije s prikazom fizičkih lokacija, hardvera (uključujući vatrozide i HSM), sustava za obradu/pohranu, nadzornih i sigurnosnih komponenti (uključujući centralni sustav za upravljanje identitetima i sigurnosni nadzor), te svih fizičkih/logičkih veza i pravila propuštanja prometa.

5.5.4. Zapisnici događaja, revizijski trag i integracija sa sigurnosnim nadzorom

Zapisnici događaja (logovi) moraju pokrivati tri razine: **revizijski trag pristupa podacima**, **sigurnosne događaje** (pokušaji neovlaštenog pristupa, anomalije) i **tehničke događaje integracije** (AS4 razmjena, greške platformi, vremenska ograničenja). Revizijski trag mora omogućiti da se za svaku kontrolu odgovori na pitanja: tko je pokrenuo provjeru, u koje vrijeme, s kojim ovlastima, s kojim razlogom i koji je opseg podataka bio dohvaćen ili prikazan. Ova razina je obavezna i za unutarnju kontrolu i za vanjske nadzore.

Revizijski zapisi moraju biti **strukturirani i konzistentni** kroz komponente (Gate, eADR, AS4 gateway, SOTAH adapteri), uz obveznu korelaciju. U praksi to znači da svi zapisi nose jedinstveni korelacijski identifikator nadzora, identifikator zahtjeva/poruke, identitet službenika ili servisnog računa, te ishod i trajanje. Bez korelacije, događaji se ne mogu pouzdano povezati u jedinstvenu vremensku crtu, što smanjuje dokaznu vrijednost i otežava forenziku.

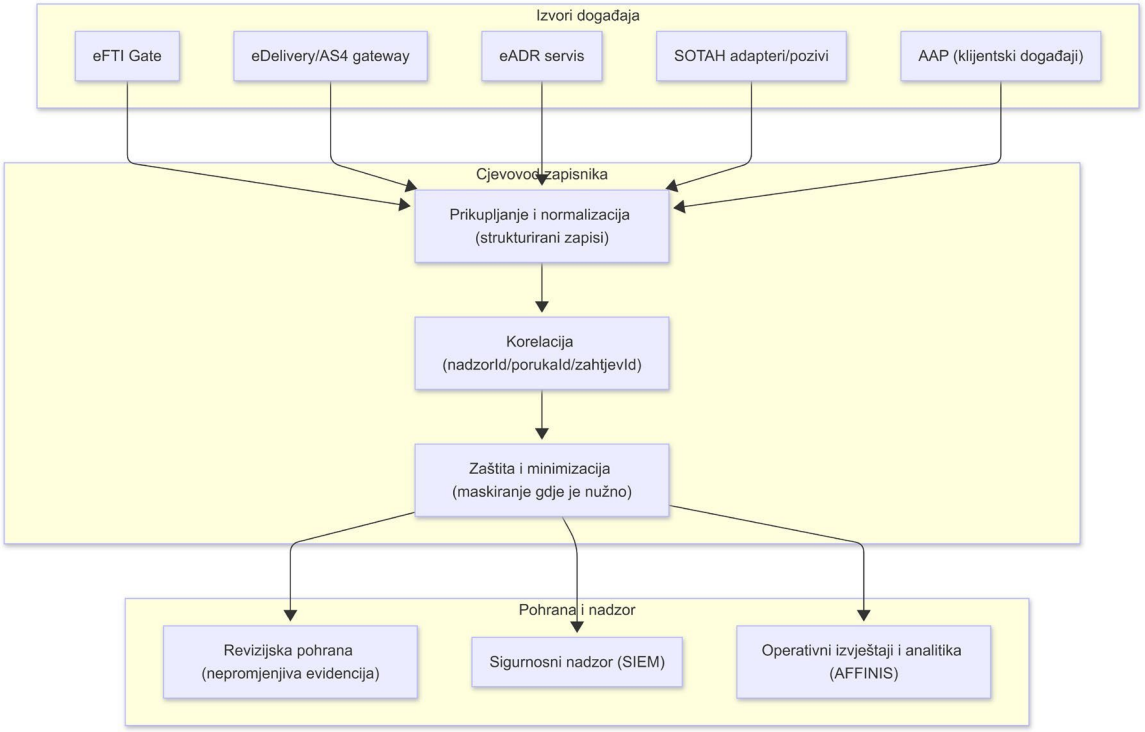
Pohrana zapisnika mora biti projektirana kao **nepromjenjiva evidencija** za revizijski kritične događaje, uz strogo ograničen pristup i jasne politike retencije. To uključuje i zaštitu od

Financira Europska unija NextGenerationEU

manipulacije (npr. pohrana s dodatnim kontrolama integriteta, ograničenja brisanja, razdvajanje operativnih i revizijskih pristupa). Posebno se naglašava da revizijski trag ne smije ovisiti o korisničkim bazama podataka aplikacija, nego mora biti odvojen i otporan na aplikacijske promjene.

Integracija sa sigurnosnim nadzorom (npr. centralni SIEM) omogućuje detekciju anomalija i brzu reakciju: neuobičajeni volumeni dohvata, ponavljani neuspjesi autentikacije, pokušaji pristupa izvan nadležnosti, ili neobične kombinacije podataka. SIEM se puni normaliziranim događajima iz svih ključnih komponenti, a alarmi se povezuju s operativnim kontekstom (koja kontrola, koje tijelo, koji sustav), čime se postiže da reakcija bude ciljano usmjerena.

- **Obavezni revizijski događaji** uključuju prijavu, pokretanje kontrole, metapodatkovni uvid, selektivni puni dohvat, pozive prema eADR-u i SOTAH-u, te završetak kontrole s ishodom i mjerama.
- **Sigurnosni događaji** uključuju odbijanja zbog ovlasti, nevaljane tokene, pokušaje pristupa tuđim jurisdikcijama, kao i odstupanja od uobičajenih obrazaca korištenja.
- **Tehnički događaji integracije** uključuju status AS4 poruka, vremenska ograničenja, ponovna slanja i korelacijske identifikatore, jer su ključni za dokazivost i za rješavanje sporova.



Slika 21. Revizijski trag i sigurnosni nadzor

Ovakav tok omogućuje da se događaji prikupe i normaliziraju na jednom mjestu, koreliraju u jedinstvenu sliku kontrole, a zatim distribuiraju u revizijsku pohranu, sigurnosni nadzor i analitički sustav bez gubitka sljedivosti i uz kontrolu osjetljivih sadržaja.

Financira
Europska unija
NextGenerationEU

Zapisnici se moraju održavati tako da sustav jamči dovoljan kapacitet i da se revizijski zapisi ne prepisuju automatski. Sustav mora generirati alarm kada preostali prostor za revizijske zapise padne ispod definiranog praga (primjerice ispod jedne petine ukupnog prostora). Zapisnici moraju biti bilježeni slijedno uz točnu informaciju o vremenu te moraju biti dostupni za pretraživanje prema datumu i vremenu, vrsti događaja i identitetu korisnika.

Pristup čitanju revizijskih zapisa mora biti ograničen na korisnike s izričito dodijeljenim pravom (uloga revizora), uz stroge kontrole i odvojene operativne i revizijske pristupe. Za centraliziranu pohranu i analizu revizijskih zapisa mora se koristiti postojeći centralni sustav organizacije, kako bi se osigurala dosljedna forenzika, dokazivost i nadzor.

5.5.5. Upravljanje tajnama i certifikatima, operativne sigurnosne kontrole i postupanje u incidentima

Upravljanje tajnama i certifikatima mora biti centralizirano kako bi se izbjeglo da su lozinke, API ključevi ili privatni ključevi “rasuti” po konfiguracijama i kodu. Sustav mora koristiti centralno spremište tajni (npr. trezor tajni) i, gdje je primjenjivo, hardversku zaštitu ključeva (HSM) za najkritičnije privatne ključeve, osobito one koji potpisuju i dešifriraju AS4 poruke. Time se smanjuje rizik kompromitacije i omogućuje kontrolirana rotacija bez prekida usluge.

Privatni ključevi certifikata koji služe za autentikaciju i sigurnu razmjenu podataka moraju biti zaštićeni sigurnim kriptografskim uređajem koji ispunjava zahtjeve najmanje Common Criteria EAL 4+ ili FIPS 140-2 razine 3, kada je riječ o najkritičnijim privatnim ključevima. Kriptografski algoritmi i parametri ne smiju biti zastarjeli i moraju biti odabrani i održavani u skladu s aktualnim preporukama relevantnih europskih sigurnosnih tijela.

Uz pravila životnog ciklusa ključeva, mora se isporučiti i popis svih kriptografskih ključeva koji se koriste u sustavu, najmanje s atributima: jedinstveni identifikator ključa, vrsta ključa, algoritam i duljina, namjena, status, datum generiranja, rok valjanosti/očekivani datum promjene, mjesto pohrane, vlasnik/odgovorna osoba ili sustav, prava pristupa (skrbnici) te evidencija korištenja ili poveznica na revizijske zapise.

Životni ciklus certifikata mora biti strogo upravljan: izdavanje, instalacija, provjera, rotacija i opoziv. Rotacija se mora provoditi planski i automatizirano gdje je moguće, a opoziv mora biti operativno provediv u kratkom roku (npr. u slučaju kompromitacije). Sve radnje nad tajnama i certifikatima moraju biti revizijski evidentirane, uz razdvajanje dužnosti (osoba koja odobrava ne smije biti ista osoba koja provodi operaciju).

Operativne sigurnosne kontrole obuhvaćaju i tehničke i organizacijske mjere: hardening poslužitelja, redovito zakrpavanje, kontrolu konfiguracija, skeniranje ranjivosti, testiranja sigurnosti te nadzor integracijskih točaka. U praktičnoj implementaciji važno je predvidjeti i “degradirani rad”: primjerice, ako puni dohvat s platforme privremeno nije moguć, sustav i

Financira
Europska unija
NextGenerationEU

dalje mora omogućiti metapodatkovni uvid, uz jasno označavanje ograničenja i uz audit da je puni dohvat pokušao i nije uspio.

Na svim komponentama sustava mora biti instalirana verzija softvera pod aktivnom podrškom proizvođača te moraju biti osigurane i primijenjene sigurnosne zakrpe prije puštanja u rad i tijekom cijelog životnog ciklusa. Osnaživanje (hardening) poslužitelja i ostalih komponenti u sigurnim zonama i demilitariziranoj zoni mora se provoditi prema industrijskim smjernicama (npr. CIS), uz uklanjanje ili onemogućavanje servisa, protokola i portova koji nisu nužni za zadanu funkciju te uz aktiviran i pravilno konfiguriran interni vatrozid operacijskog sustava.

Aplikacije i servisi moraju se pokretati pod servisnim računima bez administratorskih ovlasti na razini operacijskog sustava. Korištenje prijenosnih medija i bežičnih mreža na kritičnim poslužiteljima mora biti onemogućeno gdje je primjenjivo. Svi sustavi moraju imati sinkronizaciju vremena s pouzdanim izvorom usklađenim s univerzalnim vremenom (UTC), kako bi revizijski trag i forenzika bili dosljedni.

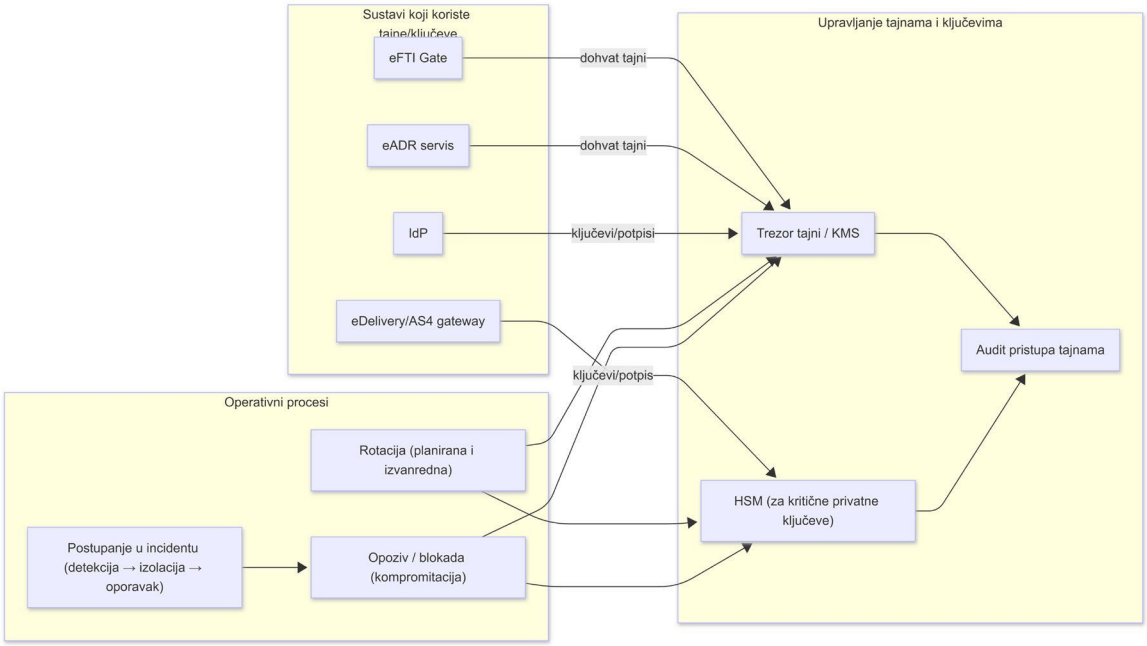
Upravljanje ranjivostima mora uključivati redovito ispitivanje ranjivosti svih kritičnih sustava prije puštanja u rad, nakon značajnijih promjena te najmanje kvartalno. Ispitivanja se provode prema relevantnim smjernicama za aplikacijske i konfiguracijske slabosti (npr. OWASP Top 10, SANS Top 25 i smjernice za sigurno kodiranje). Prije produkcije moraju biti sanirane sve identificirane ranjivosti, pri čemu nijedna usluga ne smije biti puštena u rad ako postoji nesanirana ranjivost s ocjenom 7.0 ili višom prema CVSS ili ekvivalentnom modelu.

Penetracijska ispitivanja na mrežnom sloju moraju se provoditi najmanje jednom godišnje te nakon dogradnje infrastrukture ili značajnijih arhitekturnih promjena. Ako se razvija aplikacijski kod ili konfiguracijski sloj, prema procjeni rizika moraju se provesti: statička analiza koda, dinamičko testiranje aplikacije te provjera sigurnosti komponenti trećih strana (analiza ovisnosti), uz obaveznu isporuku izvještaja i evidenciju otklanjanja nalaza prije produkcije.

Postupanje u incidentima mora biti definirano kroz operativne procedure i tehničke mehanizme: detekcija (SIEM), trijaža, izolacija, obavještavanje, otklanjanje i povrat u normalan rad. Posebno je važno imati mehanizam **privremenog ograničavanja ovlasti** (npr. za kompromitirani korisnički račun ili servis), kao i mehanizam “break-glass” za iznimne situacije, uz stroge kontrole i obaveznu reviziju.

- **Centralno spremište tajni** omogućuje da aplikacije dohvaćaju tajne u trenutku potrebe i da se tajne rotiraju bez izmjena koda; pristup trezoru mora biti ograničen na minimalni broj servisa i strogo auditiran.
- **Rotacija i opoziv certifikata** moraju imati definiran raspored i postupak, uključujući provjere kompatibilnosti s eDelivery/AS4 partnerima, kako bi se izbjegli prekidi u prekograničnim razmjenama.
- **Incidentni postupci** moraju biti povezani s tehničkim korelacijama iz zapisnika, tako da se brzo utvrdi koje su kontrole i koji dohvaćeni podaci potencijalno obuhvaćeni incidentom.

Financira
Europska unija
NextGenerationEU



Slika 22. Upravljanje tajnama i certifikatima

Ovim se osigurava da su tajne i ključevi upravljani centralno, da je svaka uporaba dokaziva kroz audit, te da postoji jasan operativni put za rotaciju i brzo opozivanje u slučaju sigurnosnog incidenta, bez narušavanja osnovne funkcije sustava u terenskim kontrolama.

5.6. Upravljanje konfiguracijom i verzijama u modularnom okruženju

Upravljanje konfiguracijom i verzijama mora osigurati da se svi moduli sustava (eADR, integracije prema eFTI platformama i G2G, SOTAH integracije te AFFINIS analitika) mogu **neovisno razvijati**, ali **kontrolirano isporučivati** kao jedinstvena cjelina. U praksi to znači da se za svaki modul mora moći točno utvrditi: koja je verzija aplikacije u radu, koja je verzija konfiguracije aktivna, koja je verzija podatkovne sheme primijenjena, te kojim je redoslijedom provedena promjena i u kojem okruženju.

S obzirom da se rješenje isporučuje **on-premise** u okruženju EU državnih projekata, potrebno je osloniti se na interne, samostalno upravljane komponente (repozitoriji koda, repozitoriji artefakata, sustav za tajne i certifikate, CI/CD, nadzor i zapisnici). Istovremeno, budući da se sustav izvodi na **virtualnim strojevima** , kontrola isporuke i promjena mora biti izvedena kroz standardne obrasce za VM okruženja: “immutable” artefakti, automatizirana konfiguracija, HA parovi, kontrolirano prebacivanje prometa i jasne strategije povratka.

Financira Europska unija
NextGenerationEU

Konfiguracija se mora promatrati kao sastavni dio proizvoda, a ne kao ad-hoc datoteke na poslužiteljima. To uključuje konfiguraciju aplikacija, integracija, baza, sigurnosnih politika, mrežnih pravila, rasporeda batch obrada i analitičkih procesa. Svaka promjena konfiguracije mora imati vlasnika, proces odobravanja, revizijski trag i mogućnost vraćanja na prethodno stanje.

Verzioniranje mora omogućiti i dugoročnu održivost: sustav će se nadograđivati prema novim eFTI datasetovima, novim pravilima i nacionalnim posebnostima, te proširenju na druge vidove prijevoza. Zbog toga su potrebni jasni ugovori verzija API-ja, poruka i shema, uz politiku kompatibilnosti unazad i planirano ukidanje zastarjelih verzija.

5.6.1. Temeljna načela konfiguracije i verzioniranja u VM okruženju

Konfiguraciju je potrebno dosljedno podijeliti u tri skupine: **(1) konfiguracija bez tajni**, **(2) tajne i kriptografski materijal**, te **(3) operativni parametri koji se mijenjaju kroz životni ciklus** (npr. pragovi, rasporedi batch obrada, pragovi rizika). Ova podjela omogućuje da se većina konfiguracije verzionira u repozitoriju, dok se tajne i ključevi drže u kontroliranom sustavu tajni, uz strogu reviziju pristupa.

Aplikacijski artefakti moraju biti **nepromjenjivi**: jednom izgrađen paket (npr. JAR/ZIP/MSI, ovisno o tehnologiji) mora se identično koristiti kroz okruženja, bez ručnih preinaka. Razlika između okruženja postiže se isključivo vanjskom konfiguracijom i parametrima. Time se izbjegavaju situacije gdje “radi na testu, ne radi na produkciji” zbog drugačije sastavljenog paketa ili ručnih intervencija.

Verzioniranje mora biti višeslojno: verzija aplikacije (semantičko verzioniranje), verzija konfiguracijskog skupa (konfiguracijski “release”), verzija podatkovne sheme (migracije), te verzija integracijskih ugovora (API/poruke). U praksi je nužno imati jedan zajednički “release manifest” koji povezuje te slojeve u jedan operativno provjerljiv zapis: koji su moduli u kojem izdanju i s kojim konfiguracijama pušteni u rad.

U VM okruženju, stabilnost se postiže kroz standardizirane obrasce: HA parovi aplikacijskih instanci iza uravnoteživača opterećenja, kontrolirane nadogradnje “instanca po instanca”, te jasno definirani health checkovi. Konfiguracijski alati moraju biti idempotentni (ponovljivo primjenjivi), a svaka promjena mora biti automatizirana i ponovljiva u više podatkovnih centara i okruženja.

5.6.2. Referentni “enterprise” stack po modulu i granice konfiguracije

Za eADR preporučuje se standardna podjela na: pristupni sloj (AAP), aplikacijske servise (Gate i eADR), integracijski sloj (eDelivery/AS4, G2G i adapteri), podatkovni sloj (operativne baze), te zajedničke servise (nadzor, zapisnici, sigurnosni posrednici). U VM okruženju svaki od tih slojeva se implementira kao skup VM-ova, po mogućnosti u parovima radi raspoloživosti, uz jasne granice konfiguracije i odgovornosti.

Financira
Europska unija
NextGenerationEU

Za AAP (pristup službenika) tipičan je obrazac **web aplikacije** s jasnim razdvajanjem korisničkog sučelja i API sloja. Konfiguracijski kritični elementi su: domene i certifikati, integracija s IdP-om, pravila sesije, ograničenja pristupa, te standardizirani zapisi događaja na razini korisničkih akcija koje su regulatorno relevantne. Konfiguracija AAP-a mora biti minimalna i usmjerena na to da se ne duplicira poslovna logika koja pripada Gateu.

Za eFTI Gate i eADR preporučuje se obrazac **stateless servisnih aplikacija** (npr. Java/.NET), gdje se stanje drži u bazama i u kontroliranim repozitorijima dokumenata. Konfiguracijski kritični elementi su: veze prema bazama, pravila autorizacije i filtriranja podataka, popisi dopuštenih eFTI podskupova po tipu tijela, pragovi za selektivni dohvat, te konfiguracija integracija (eDelivery/AS4, SOTAH adapteri). Ovdje je posebno važno da se konfiguracije koje mijenjaju ponašanje nadzora (npr. pragovi rizika, vrste upozorenja) vode kao verzionirane i odobravane promjene.

Za eDelivery/AS4 (i G2G) preporučuje se provjereni obrazac s namjenskim AS4 poslužiteljem i jasnim upravljanjem partnerima, certifikatima i porukama. Ovaj sloj je izrazito konfiguracijski osjetljiv: svaka promjena certifikata, endpointa ili partner profila mora biti planirana, testirana i korelirana s revizijskim zapisima, jer izravno utječe na prekograničnu interoperabilnost. U VM okruženju, promjene se uvode kontrolirano, uz mogućnost paralelnog rada starog i novog profila tijekom prijelaznog razdoblja.

5.6.3. Upravljanje infrastrukturom i okruženjima

Infrastruktura se mora voditi kao kod (“Infrastructure as Code”) i primjenjivati kroz automatizaciju nad VM okruženjem. To uključuje definiciju VM resursa, mrežnih segmenata, sigurnosnih zona, pravila vatrozida, uravnoteživača opterećenja, DNS-a, te standardnih poslužiteljskih postavki (hardening, korisnici, pristup). Ključna vrijednost ovog pristupa je da se isti obrazac može primijeniti na razvojno, testno i produkcijsko okruženje, uz razliku u parametrima i kapacitetu.

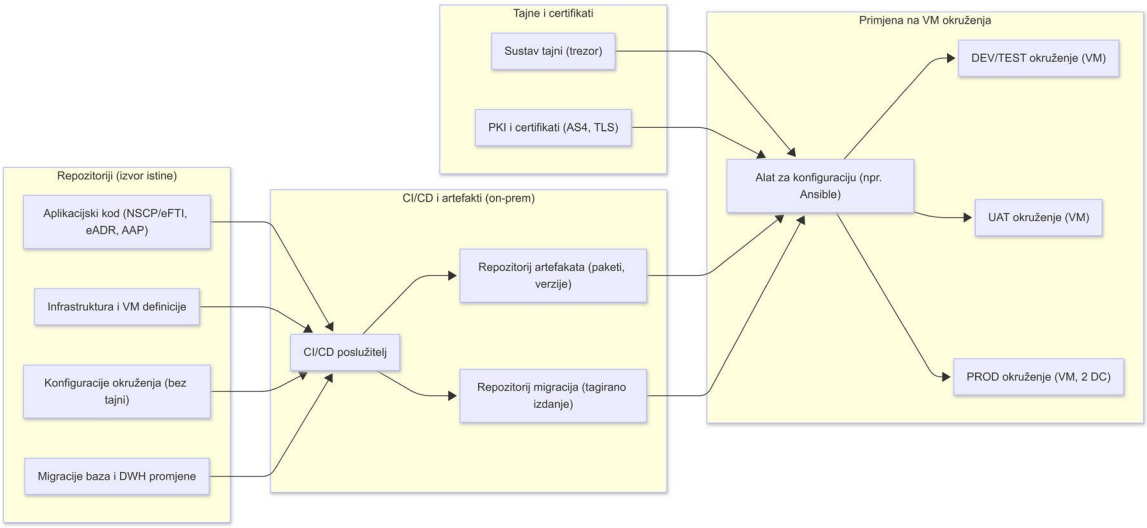
Budući da produkcija radi u režimu visoke raspoloživosti, konfiguracijski model mora predvidjeti najmanje dva podatkovna centra te sposobnost preuzimanja opterećenja u slučaju ispada jedne lokacije. U praksi to znači da se infrastruktura definira kao dva “inventoryja” (ili dva skupa varijabli) s istim logičkim modulima, ali s različitim IP rasponima, nazivima čvorova i rutama. Time se postiže da se promjene mogu primijeniti simetrično, uz preciznu kontrolu redoslijeda.

Okruženja (DEV/TEST/UAT/PROD) moraju biti strogo odvojena, ali upravljana istim mehanizmima. Razlike se svode na: veličinu resursa, razinu sigurnosnih kontrola, retenciju logova i podataka, te dopuštene vrste integracija (npr. simulirane integracije u testu, stvarne u produkciji). Ključno je da se konfiguracije ne “kopiraju ručno”, nego se generiraju iz istog izvora istine uz parametrizaciju.

U VM okruženju nadogradnje se provode kroz “rolling” pristup: jedna instanca se isključi iz prometa, nadogradi, provjeri, vrati u promet, pa se postupak ponovi. Time se postiže

Financira
Europska unija
NextGenerationEU

minimalni prekid i jasna mogućnost povratka. Ovaj obrazac mora biti podržan konfiguracijom uravnoteživača opterećenja, health checkovima te standardiziranim servisnim skriptama (systemd ili ekvivalent) za pokretanje i zaustavljanje servisa.



Slika 23. Upravljanje infrastrukturom i okruženjima

Dijagram prikazuje jedinstveni tok: sve promjene ulaze kroz repozitorije, CI/CD proizvodi nepromjenjive artefakte i verzionirane migracije, a konfiguracijski alat primjenjuje isporuku na VM okruženja uz povlačenje tajni iz kontroliranog sustava.

5.6.4. Verzije aplikacija i integracijskih ugovora (API, poruke, sheme)

Aplikacije se verzioniraju semantički (MAJOR.MINOR.PATCH) uz jasna pravila: promjene koje ruše kompatibilnost podižu MAJOR, funkcionalne nadogradnje bez rušenja kompatibilnosti podižu MINOR, a ispravci i sigurnosne zakrpe podižu PATCH. U modulnom okruženju to je nužno jer se ne nadograđuju svi dijelovi sustava istovremeno; mora biti moguće da Gate i eADR budu u različitim minor izdanjima, uz zadržavanje kompatibilnosti kroz ugovorene API-je i poruke.

API-ji se moraju verzionirati i održavati kompatibilnima kroz definirano razdoblje. Za interne API-je (npr. Gate ↔ eADR, eADR ↔ SOTAH adapter) preporučuje se jasna verzija u putanji ili zaglavlju, uz “contract testove” koji automatski provjeravaju da promjena nije prekršila ugovor. Za vanjske API-je (prema sustavima nadležnih tijela) pravila moraju biti još stroža, uz dokumentirane rokove deprecijacije.

Za eDelivery/AS4 i G2G razmjenu, ugovori se prvenstveno očituju kroz profile partnera, certifikate i strukturu poruka. Ovdje je verzioniranje praktično izvedeno kroz konfiguracijske profile i strogo upravljane promjene partner konfiguracija. Sustav mora podržati prijelazna razdoblja: paralelno važenje starog i novog certifikata ili endpointa, uz jasne datume i automatizirane provjere valjanosti.

Financira
Europska unija
NextGenerationEU

Za eFTI sadržaj, verzioniranje se pojavljuje kroz verzije datasetova, podskupova i kodnih lista. Iako se operativno radi selektivni dohvat punog sadržaja, aplikacije moraju biti spremne da u prometu postoje različite verzije datasetova, ovisno o platformi i državi. Zbog toga je nužno imati sloj mapiranja i validacije koji se može nadograđivati konfiguracijski, uz strogo verzioniranje pravila i kodnih lista.

5.6.5. Verzije podataka: baze, migracije, šifrarnici i pravila

Migracije baze podataka moraju biti dio istog "release" procesa kao i aplikacijske promjene. Svako izdanje aplikacije mora eksplicitno navesti koje migracije su obvezne te kojim redoslijedom se primjenjuju. U VM okruženju tipičan obrazac je da se migracije izvode kroz kontrolirani "job" ili administrativni korak u CI/CD-u, uz strogo ograničene ovlasti, obaveznu izradu sigurnosne kopije i jasnu mogućnost povratka (gdje je to realno).

Kako bi se omogućile nadogradnje bez prekida, migracije moraju slijediti "backward/forward compatible" pristup: prvo se uvode promjene koje su kompatibilne sa starom verzijom aplikacije (npr. dodavanje stupaca, nove tablice, neobavezna polja), zatim se nadograđuje aplikacija, a tek nakon toga se rade "cleanup" koraci (npr. uklanjanje starih stupaca) u zasebnom izdanju. Ovaj princip je osobito važan u modulnom okruženju gdje se servisi nadograđuju postupno.

Šifrarnici i poslovna pravila (npr. tipovi događaja, statusi, mapiranja datasetova, pravila filtriranja) moraju se voditi kao verzionirani skupovi podataka. Praktičan obrazac je da se šifrarnici isporučuju kroz verzionirane "seed" migracije ili kroz zaseban "reference data" proces koji je dio release-a. Ključno je da promjena šifrarnika ima revizijski trag i da se može povezati s ishodima nadzora i analitičkim izvještajima.

U analitičkom dijelu (AFFINIS) verzioniranje modela i ETL-a mora pratiti operativni model: promjene u operativnim tablicama ili kodnim listama moraju se reflektirati kroz verzionirane ETL transformacije, materijalizirane poglede i agregate. Budući da se analitika temelji na dnevnim obradama, upravljanje migracijama i promjenama mora biti usklađeno s batch prozorima i SLA-ovima, uz mogućnost ponovnog izvođenja obrade u slučaju promjene pravila ili ispravka podataka.

5.6.6. CI/CD, isporuka na VM-ove, strategije povratka i kontrola promjena

CI/CD se u on-premise kontekstu mora izvesti kao interna usluga: repozitorij koda, automatizirana izgradnja, automatizirano testiranje, repozitorij artefakata, automatizirana isporuka na okruženja i automatizirane provjere stanja. U modulnom sustavu je nužno uvesti i "release manifest" koji definira koji su artefakti i konfiguracije dio izdanja te omogućuje kontrolirano sastavljanje i povratak.

Isporuka na VM okruženja provodi se kroz automatizirani konfiguracijski alat koji na temelju inventara okruženja postavlja artefakte, generira konfiguracijske datoteke, postavlja sistemske servise, provodi health checkove i vraća instancu u promet, ključni "orchestrator"

Financira
Europska unija
NextGenerationEU

je kombinacija CI/CD-a, konfiguracijskog alata i uravnoteživača opterećenja. To mora biti izvedeno tako da se promjena može ponoviti, dokazati i auditirati.

Strategije povratka moraju biti unaprijed definirane i uvježbane. Za stateless servise povratak je najčešće povratak na prethodni artefakt i konfiguraciju, uz ponovno pokretanje servisa i vraćanje instanci u promet. Za baze podataka povratak je složeniji, pa se oslanja na kompatibilne migracije, sigurnosne kopije i jasno definiran "point-in-time" oporavak. Za eDelivery/AS4 promjene (certifikati/partner profili) povratak mora biti moguć kroz vraćanje prethodnog profila i certifikata, uz strogo vođenu evidenciju.

Kontrola promjena u državnim projektima mora uključiti minimalno: odobrenje promjene, plan implementacije, plan povratka, prozore izvođenja, komunikaciju prema dionicima i dokazni zapis nakon provedbe. Ovaj proces ne smije biti "ručni dokument koji živi odvojeno", nego se mora osloniti na stvarne tehničke artefakte: tagove u repozitoriju, manifest izdanja, logove isporuke i zapise nadzora (monitoring i zapisnici događaja).

5.6.7. Konfiguracija i verzije analitičkog sloja (AFFINIS) uz dnevne obrade

AFFINIS analitički sloj treba tretirati kao zaseban modul s vlastitim životnim ciklusom: **verzije ETL/ELT procesa**, verzije DWH/lakehouse struktura, verzije agregata i materijaliziranih pogleda, te verzije izvještaja i nadzornih ploča. Iako analitika ne upravlja operativnim nadzorom u realnom vremenu, ona je ključna za objedinjene izvještaje, indikatore rizika i strateške analize, pa promjene moraju biti jednako kontrolirane kao i u operativnom sustavu.

Konfiguracija batch obrada mora biti jasno definirana i verzionirana: učestalost, raspored, prozori izvođenja, ovisnosti između poslova, pravila ponovnog izvođenja i postupanje u slučaju djelomičnog neuspjeha. U praktičnoj implementaciji to znači da se raspored i ovisnosti drže u repozitoriju, a izvršavanje se provodi kroz standardni "job" sloj na VM-ovima, uz nadzor trajanja i potrošnje resursa. Posebno je važno da se ETL može pokrenuti i izvan redovnog termina (npr. više puta dnevno) bez potrebe za ad-hoc intervencijama.

Podatkovni tok prema AFFINIS-u mora biti stabilan i verzioniran: iz operativnog sustava se u analitiku šalju kurirani, strukturirani skupovi podataka, uz dosljedno mapiranje kodova i ključeva. Kad se promijeni operativni model (npr. novi status, nova vrsta događaja, novi dataset), promjena mora imati odgovarajuću promjenu u ETL-u i u šifrarnicima analitike. U protivnom nastaju "tihe" greške (krive agregacije, pogrešni riskscoreovi), koje su u državnim projektima operativno neprihvatljive.

Kapaciteti i izvedba analitike u VM okruženju moraju biti usklađeni s modulnim verzioniranjem. To uključuje planiranje resursa za ETL čvorove i BI/serving čvorove, posebno zato što su najskuplji dio analitike često kompleksni joinovi (npr. povezivanje pošiljaka, nadzora, eADR predmeta i tahografskih agregata). Upravljanje konfiguracijom mora zato uključiti i verzioniranje performansnih parametara (npr. paralelizam, particioniranje, strategije materijalizacije), uz jasne kriterije prihvatljivosti nakon svake promjene.

Financira
Europska unija
NextGenerationEU

6. Zahtjevi za implementaciju Direktive NIS2

Uspostava i rad sustava eADR mora biti usklađena s Direktivom (EU) 2022/2555 (NIS2) te nacionalnim provedbenim propisima i internim sigurnosnim pravilima organizacija koje sustav razvijaju i operativno održavaju. U projektnim dokumentima eADR su postavljeni kao **kritična infrastruktura** i **kritična imovina (TIER 1)**, što izravno određuje razinu tražene zaštite, razinu raspoloživosti i način oporavka nakon incidenta.

Zahtjevi NIS2 u ovom projektu prevode se u praktične obveze koje se moraju moći provesti u stvarnom okruženju i bez prekomjerne operativne složenosti. Fokus je na mjerama koje su nužne za postizanje **povjerljivosti**, **integriteta**, **dostupnosti** i **autentičnosti** podataka i usluga, uz jasno definirane procese za upravljanje incidentima i dokazivost provedenih mjera kroz osnovnu sigurnosnu dokumentaciju i dnevničke zapise.

S obzirom da se u okviru eFTI i eADR obrađuju regulatorni i poslovno osjetljivi podaci (uključujući podatke o prijevozu opasnih tvari) te osobni podaci (npr. vozači), sustav mora osigurati **strogo upravljanje pristupom**, **kriptozaštitu prijenosa i pohrane**, **centralno evidentiranje sigurnosnih događaja** te **kontinuitet rada** u skladu s postavljenom kritičnošću. Dodatno, eFTI regulatorni okvir eksplicitno zahtijeva mjere kojima se osigurava da se povjerljivim poslovnim informacijama može pristupiti i obrađivati ih samo uz ovlaštenje, što je potrebno uskladiti s NIS2 pristupom upravljanja rizicima.

Svi zahtjevi iz ovog poglavlja moraju biti primjenjivi na cjelokupnu ciljnu arhitekturu sustava: korisničke aplikacije i portale, API-je i integracije (npr. eDelivery/AS4, SOTAH i ostali registri), baze podataka, sustave autorizacije te operativne servise za monitoring, evidentiranje i oporavak. Implementacija je **on-premise** u podatkovnim centrima AKD-a (primarna i DR lokacija), uz arhitekturu temeljenu na **virtualnim strojevima**, segmentaciji mreže i troslojnoj produkcijskoj arhitekturi kako je definirano u projektnim dokumentima.

6.1. Normativni okvir i kategorizacija utjecaja (CIAA)

Direktiva NIS2 definira obvezu uspostave mjera upravljanja kibernetičkim rizicima i obvezu pravodobnog izvještavanja o značajnim incidentima. U projektnim dokumentima dodatno je jasno postavljeno da je eADR **kritična infrastruktura** te da se obrada provodi na **primarnoj i DR lokaciji** (Zagreb i Kerestinec), uz ciljane vrijednosti **RPO = 0**, **RTO ≈ 0** i **MTD = 2 sata** u najtežim scenarijima. Time se NIS2 zahtjev za kontinuitetom i otpornosti operacionalizira u mjerljive ciljeve sustava.

Kategorizacija sustava i komponenti mora se provesti kroz procjenu utjecaja na **integritet**, **povjerljivost**, **dostupnost** i **autentičnost** (CIAA), kako je predviđeno i u projektnim zahtjevima za dokumentiranje zaštite podataka i kategorizaciju. Kategorizacija mora biti dovoljno konkretna da iz nje proizlaze projektne odluke (npr. razine autorizacije, šifriranje, retencija logova, HA/DR mehanizmi), ali bez nepotrebnog administrativnog opterećenja; cilj je **jednostavna i primjenjiva matrica** po ključnim komponentama i vrstama podataka.

Financira
Europska unija
NextGenerationEU

Posebno je važno da se u obuhvatu kategorizacije ne promatra samo aplikacija, nego i **integracijski kanali** (npr. eDelivery/AS4), **identitetske usluge**, **baze podataka**, **logovi i audit**, te **dugoročna pohrana**. U praksi, većina sigurnosnih incidenata u integriranim državnim sustavima eskalira upravo preko pogrešno konfiguriranih integracija, pogrešno postavljenih mrežnih pravila ili preširokih pristupa, pa CIAA kategorizacija mora eksplicitno pokriti i te slojeve.

Normativno, uz NIS2 i nacionalne provedbene propise, potrebno je uvažiti i zahtjeve eFTI regulative u dijelu povjerljivosti poslovnih informacija, kao i opće zahtjeve zaštite osobnih podataka. To ne znači uvođenje dodatnih zasebnih okvira, nego dosljedno provođenje istih temeljnih principa: **pristup samo uz ovlaštenje**, **minimalni opseg podataka**, **sljedivost pristupa** i **sigurnost cijelog životnog ciklusa podataka** (od primitka, obrade i razmjene do arhiviranja).

6.2. Upravljačka odgovornost i organizacijske obveze u skladu s NIS2

NIS2 uvodi izravnu odgovornost upravljačkih tijela za odobravanje i nadzor provedbe mjera upravljanja kibernetičkim rizicima, uključujući obvezu osposobljavanja (edukacije) upravljačkih struktura o kibernetičkoj sigurnosti. U kontekstu ovog projekta to znači da se moraju jasno definirati: **vlasnik sustava**, **operativni upravitelj**, te **odgovorne osobe** za ključne sigurnosne procese (pristupi, incidenti, promjene, oporavak), uz formalno odobrenje sigurnosnih politika i minimalnih standarda rada sustava.

Organizacijski model mora biti izvediv unutar dionika koji su već predviđeni projektnom dokumentacijom. Ključno je uspostaviti jednoznačne kontaktne točke i odgovornosti, bez stvaranja paralelnih timova ili oslanjanja na vanjske subjekte. U praksi je nužno definirati **jedinstvenu točku kontakta** za sigurnosna pitanja i incidente (operativna i upravljačka), te osigurati da postoji 24/7 eskalacijski put (ne nužno 24/7 prisutnost, nego jasna dostupnost kroz dežurstva ili on-call model u okviru operativnog održavanja).

Minimalni skup sigurnosnih politika i postupaka mora biti kratak, ali operativno upotrebljiv i provjerljiv. Ne uvodi se složen sustav evidencija i upravljanja rizicima, nego se dokumentiraju i provode postupci koji su izravno vezani uz NIS2 obveze:

- **Politika upravljanja pristupom:** definira tko ima pravo pristupa kojim podacima i funkcijama, uz obveznu sljedivost i periodičnu provjeru aktivnih ovlaštenja.
- **Postupak upravljanja incidentima:** definira klasifikaciju incidenta, tok eskalacije, uloge, rokove i način obavješćivanja nadležnih tijela te korisnika usluge kada je to potrebno.
- **Postupak sigurnosnih promjena i nadogradnji:** definira kako se promjene uvode u produkciju, kako se osigurava povrat (rollback), te kako se osigurava da nadogradnje ne naruše raspoloživost sustava.
- **Politika sigurnosnih kopija i oporavka:** definira način izrade sigurnosnih kopija, šifriranje kopija, testove povrata i ciljeve oporavka po kritičnim komponentama.

Financira
Europska unija
NextGenerationEU

Obuka (edukacija) mora obuhvatiti najmanje tri razine: upravljačku razinu (razumijevanje odgovornosti i donošenje odluka), operativnu razinu (administratori, DevOps/infra tim, integratori) te korisničku razinu (autorizirani korisnici u nadležnim tijelima i operateri koji koriste sustav). Cilj je da se sigurnost provodi dosljedno kroz svakodnevni rad, a ne kao dodatni sloj koji se "naknadno" pokušava dokazivati.

6.3. Mjere upravljanja kibernetičkim rizicima (prevedeno u provedive zahtjeve)

NIS2 zahtijeva da se provedu **primjerene i razmjerne** tehničke i organizacijske mjere upravljanja rizicima, s ciljem sprječavanja, otkrivanja, odgovora i oporavka od incidenata, uz smanjenje utjecaja na korisnike i osiguranje kontinuiteta usluga. U ovom projektu to znači da se mjere definiraju kao konkretni zahtjevi po slojevima arhitekture (mreža, aplikacije, baze, integracije, identitet, monitoring/logiranje i oporavak), a ne kao apstraktne preporuke.

S obzirom na kritičnost sustava (TIER 1) i projektno definiranu dvosite arhitekturu, mjerama se mora postići da se incidenti **detektiraju rano**, da se može provesti **brza izolacija pogođenih komponenti** bez prekida cijelog sustava te da se može provesti **oporavak bez gubitka podataka**. Ovo u praksi podrazumijeva kombinaciju mrežnih i aplikacijskih kontrola (segmentacija, WAF/firewall, strogo kontrolirani portovi i protokoli), kriptografskih mjera (TLS/AS4, signiranje, enkripcija) te upravljanja identitetima i pravima.

NIS2 skup mjera (članak 21.) prevodi se u sljedeće projektne zahtjeve, koji moraju biti vidljivi u dizajnu i implementaciji:

- **Politike analize rizika i sigurnosti sustava:** sustav mora imati definiran minimalni model procjene rizika po domenama (integracije, identitet, baze, portal), s mapiranim kontrolama koje se primjenjuju kao standardna konfiguracija i praksa.
- **Upravljanje incidentima:** mora postojati jedinstveni operativni postupak za detekciju, trijažu, eskalaciju, forenzičko prikupljanje i oporavak, uz jasnu ulogu operativnog održavanja i sigurnosne odgovorne osobe.
- **Kontinuitet poslovanja i oporavak (backup/DR):** mora se implementirati visoka raspoloživost i oporavak sukladno ciljevima RPO/RTO/MTD; sigurnosne kopije moraju biti planirane, šifrirane i redovito testirane.
- **Sigurnost lanca opskrbe:** nabavljeni i ugrađeni proizvodi i usluge (softver/hardver) moraju biti podržani, sigurnosno održavani i ugovorno obvezani na isporuku zakrpa i sigurnosnih obavijesti; posebna pozornost daje se komponentama integracijskog sloja i identitetskih servisa.
- **Sigurnost nabave, razvoja i održavanja:** aplikacije i integracije moraju se razvijati i održavati uz sigurnosne kontrole (validacija ulaza, zaštita API-ja, kontrola konfiguracije, upravljanje tajnama/ključevima), uz obvezno postupanje po ranjivostima i odgovorno otkrivanje.

Financira Europska unija
NextGenerationEU

- **Provjera učinkovitosti mjera:** moraju se provoditi jednostavne i redovite provjere (npr. mjesečni pregled ključnih događaja, kvartalni test oporavka od incidenta, periodična provjera privilegiranih pristupa) bez uvođenja složenih audit programa.
- **Osnovna kibernetička higijena i edukacija:** minimalni standardi hardeninga, ažuriranja i sigurnog rada moraju biti definirani i provođeni; korisnici i administratori moraju imati osnovnu edukaciju (npr. prepoznavanje kompromitiranih računa, postupanje s povjerljivim podacima).
- **Kriptografija i enkripcija:** prijenos i pohrana podataka mora biti kriptozaštićena; koristi se TLS za komunikaciju, a gdje je primjenjivo i signiranje/verifikacija poruka (npr. AS4 i integracijski tokovi); ključevi i certifikati moraju biti upravljani kontrolirano.
- **Sigurnost ljudskih resursa, pristupa i imovine:** mora postojati inventar ključnih komponenti i računa; pristupi se dodjeljuju po najmanjoj potrebnoj ovlasti; odlazak korisnika/administratora mora imati jasan postupak deaktivacije prava.
- **Višefaktorska autentifikacija i sigurni komunikacijski kanali:** administrativni i osjetljivi pristupi moraju koristiti višefaktorsku autentifikaciju; komunikacija između servisa mora biti zaštićena, a kanali za kriznu komunikaciju definirani.

Ove mjere moraju biti ugrađene u arhitekturu i operativne procedure, tako da sustav u normalnom radu "prirodno" proizvodi tragove i podatke potrebne za nadzor i izvještavanje. Time se izbjegava situacija u kojoj se NIS2 pokušava dokazivati naknadno i ručno, što bi povećalo operativno opterećenje i složenost održavanja.

6.4. Upravljanje identitetima, autentifikacija i kontrola pristupa

U sustavu eADR upravljanje identitetima mora pokriti više skupina korisnika i više tipova pristupa: gospodarske subjekte (npr. prijevoznici), fizičke osobe (npr. vozači), korisnike u nadležnim tijelima (inspekcije, policija i sl.), te administrativne i operativne korisnike sustava. NIS2 mjere u ovom segmentu moraju osigurati da se pristup osjetljivim podacima i funkcijama može ostvariti samo uz pouzdanu autentifikaciju i uz provjerljivo ovlaštenje.

Za ljudske korisnike prioritet je osloniti se na nacionalne usluge autentifikacije gdje je to prikladno, čime se smanjuje broj lokalno upravljanih vjerodajnica i time smanjuje rizik kompromitacije. U projektnim zahtjevima eksplicitno se očekuje uključenje internih usluga poput domene i NIAS-a (eGrađanin) te povezanih mehanizama autentifikacije. Time se ujedno ispunjava zahtjev NIS2 u dijelu višefaktorske autentifikacije i jačih mehanizama provjere identiteta.

Kontrola pristupa mora biti projektirana kao kombinacija **uloga (RBAC)** i, gdje je potrebno, **atributa (ABAC)**. Primjerice, korisnik nadležnog tijela može imati ulogu "inspektor", ali stvarno ovlaštenje za pregled određenih podataka može ovisiti i o atributima kao što su nadležnost, teritorijalni opseg, vrsta postupka ili pravna osnova. Posebno je važno da se **pristup eFTI payloadu** i **podacima o opasnim tvarima** ograniči prema načelu "need-to-know", uz obavezno evidentiranje tko je pristupio kojim podacima i kada.

Financira
Europska unija
NextGenerationEU

Privilegirani pristupi (administratori, održavanje, pristupi bazama) moraju biti dodatno zaštićeni i strogo odvojeni od korisničkih pristupa. U praksi to znači da se koristi zaseban administrativni identitet, višefaktorska autentifikacija, zabrana dijeljenih računa te mogućnost brze revizije i opoziva privilegija. Operativno, ovo se mora nadovezati na logiranje i monitoring, tako da se sve administrativne radnje mogu pratiti kroz centralne dnevničke zapise.

Upravljanje sesijama i tokenima (za portal, API i integracijske tokove) mora biti implementirano s jasnim pravilima isteka, obnove i opoziva, osobito u slučaju incidenta. Sustav mora podržati **brzo onemogućavanje kompromitiranih računa** i rotaciju tajni/ključeva, bez potrebe za složenim ručnim intervencijama na velikom broju komponenti.

6.5. Upravljanje incidentima i obveze izvještavanja prema NIS2

Upravljanje incidentima mora biti postavljeno kao standardni operativni proces koji se provodi jednako za sve dijelove sustava: aplikacijski sloj, baze podataka, integracije, identitet, eDelivery/AS4 komunikacija te infrastrukturne komponente. Cilj je imati jedan jasan tok: **detekcija → procjena → klasifikacija → ograničavanje → oporavak → izvještavanje → učenje**, uz minimalne, ali jasne uloge i odgovornosti.

Za potrebe NIS2, posebno je važno definirati kriterije kada incident postaje **značajan incident**. Kriteriji se u praksi moraju vezati uz stvarni utjecaj na uslugu: prekid ili degradacija ključne funkcionalnosti (npr. nemogućnost provjere eFTI podataka od strane nadležnih tijela), kompromitacija povjerljivosti podataka (npr. neovlašteni pristup DG podacima ili osobnim podacima), integritet podataka (npr. neovlaštena izmjena registara ili dozvola), ili širi utjecaj na dostupnost/operacije. Klasifikacija mora biti dovoljno jednostavna da se može primijeniti odmah pri trijaži, bez složenih analiza.

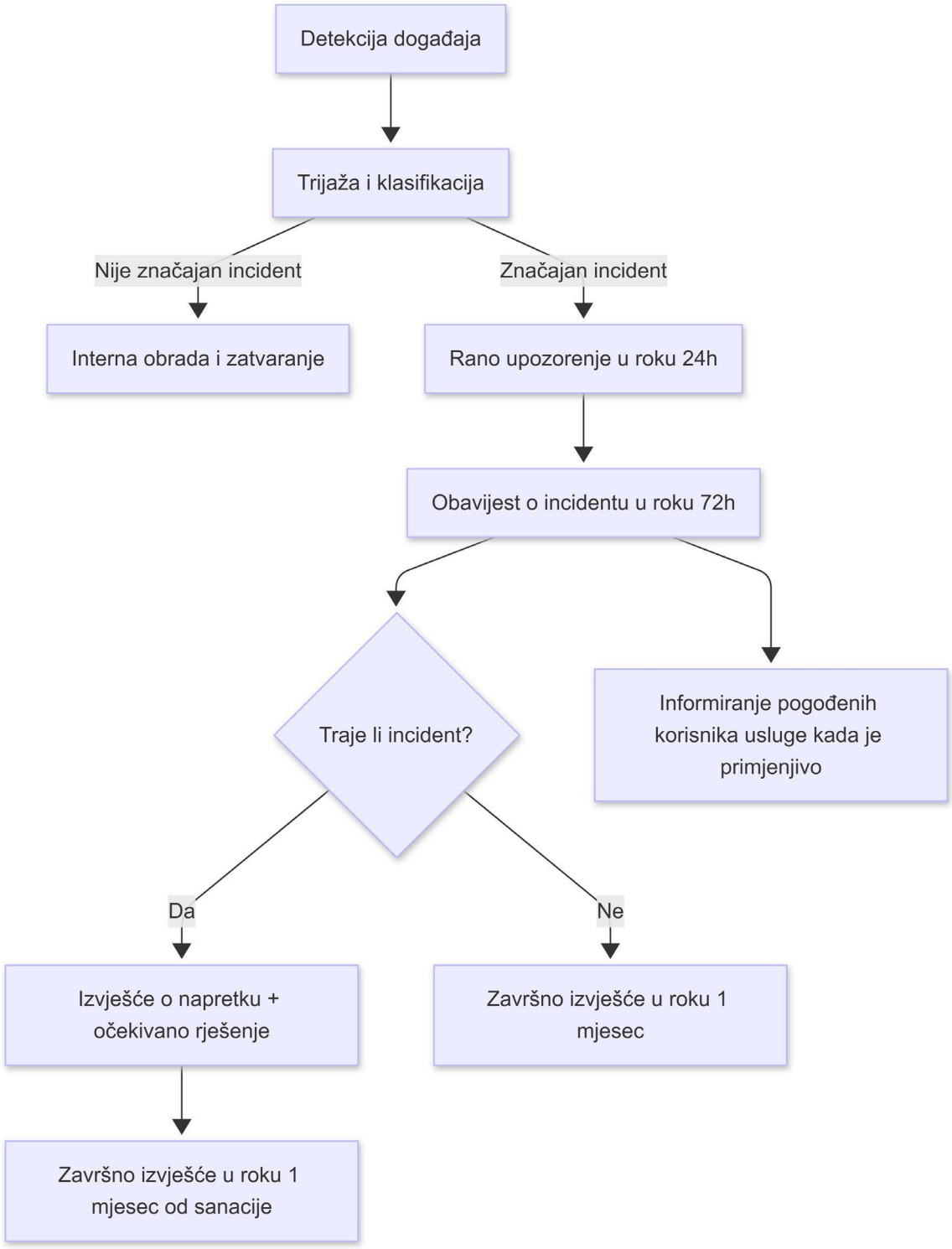
NIS2 uvodi višefazno izvještavanje o značajnim incidentima prema nadležnom CSIRT-u ili nadležnom tijelu. U svrhu praktične provedbe, sustav i operativni postupci moraju omogućiti prikupljanje podataka potrebnih za ove izvještaje (vrijeme, pogođene komponente, procjena utjecaja, indikatori kompromitacije, poduzete mjere). Obveze se provode u sljedećim rokovima:

- **Rano upozorenje (u roku 24 sata od saznanja):** prijavljuje se da je incident značajan te se navodi sumnja na zlonamjerno djelovanje i/ili moguć prekogranični utjecaj (ako je primjenjivo).
- **Obavijest o incidentu (u roku 72 sata od saznanja):** dostavlja se inicijalna procjena ozbiljnosti i utjecaja te, kada je primjenjivo, indikatori kompromitacije.
- **Međuraport:** dostavlja se na zahtjev nadležnog tijela ili kada postoji značajna promjena stanja (npr. eskalacija utjecaja, otkriven novi vektor napada, promjena procjene opsega).
- **Završno izvješće (u roku jednog mjeseca od obavijesti o incidentu):** opis uzroka ili prijetnje, mjere ublažavanja i detaljniji opis utjecaja; ako incident traje, daje se izvješće o napretku i planiranom rješenju te završno izvješće nakon sanacije.

Financira
Europska unija
NextGenerationEU

Osim izvještavanja prema nadležnim tijelima, NIS2 predviđa i obvezu informiranja korisnika usluge kada incident može negativno utjecati na njihovu uslugu ili sigurnost. U kontekstu eADR to znači da sustav mora imati pripremljen model komunikacije prema relevantnim korisnicima (npr. nadležna tijela, gospodarski subjekti) kroz službene kanale i uz jasno definiranu poruku: što se dogodilo, koji je utjecaj, koje su preporučene mjere i kada se očekuje normalizacija.

Financira
Europska unija
NextGenerationEU



Slika 24. Upravljanje incidentima prema NIS2

Dijagram iznad služi kao jedinstvena referenca za operativni tok upravljanja značajnim incidentima i usklađenost s ključnim rokovima. Cilj nije stvaranje složene "incident evidencije", nego osiguravanje da se potrebne informacije prikupljaju kroz normalan rad (logovi, monitoring, tiketi održavanja) i da se iz njih može brzo sastaviti traženo izvješće.

Financira Europska unija
NextGenerationEU

6.6. Evidentiranje, nadzor i osnovno izvještavanje (logovi, monitoring, SIEM)

NIS2 zahtijeva da organizacija može otkriti i analizirati incidente, što u praksi znači da mora postojati konzistentan sustav za prikupljanje dnevničkih zapisa, nadzor rada ključnih komponenti i osnovno izvještavanje o sigurnosnim događajima. U projektnim dokumentima je predviđeno postojanje zajedničkih servisa kao što su **LOGCOLLECTOR**, **MONITORING** te **SIEM/proxy/helper** servisi, uz mogućnost oslanjanja na interne usluge poput Splunk-a. Ovaj sloj mora biti sastavni dio produkcijske arhitekture, a ne naknadni dodatak.

Evidentiranje mora obuhvatiti najmanje sljedeće kategorije događaja, uz jasno definirane obvezne atribute (vrijeme, identitet, akcija, rezultat, izvor, cilj):

- **Autentifikacija i autorizacija:** prijave, neuspjele prijave, izdavanje/obnova tokena, odluke autorizacije (tko je tražio pristup i na temelju kojeg prava).
- **Pristup osjetljivim podacima:** pregled ili dohvat eFTI podataka, DG podataka, registara dozvola i nadzora, posebno za korisnike nadležnih tijela i administratore.
- **Administrativne promjene:** promjene konfiguracije, prava, integracijskih postavki, certifikata i ključeva, kao i promjene u mrežnim pravilima koje utječu na dostupnost ili sigurnost.
- **Integracijski tokovi:** greške u razmjeni (npr. eDelivery/AS4), neuspjele validacije poruka, greške u integraciji prema SOTAH-u i drugim registrima, abnormalna učestalost poziva.
- **Sigurnosni događaji na infrastrukturi:** sustavni eventi, pokušaji neovlaštenih pristupa, promjene privilegija, anomalije u radu servisa.

Retencija i kapacitet logova moraju biti dimenzionirani tako da podrže regulatorne i sigurnosne potrebe bez ručnog “gašenja logiranja” kada sustav dosegne kapacitete. U projektnim procjenama očekuje se red veličine oko **12 GB logova dnevno**, što na višegodišnjoj razini čini značajan volumen. Zbog toga je nužno provesti jednostavan, ali robustan model: kratkoročno pretraživi logovi za operativnu trijažu i forenziku, te dugoročna arhiva za potrebe dokazivosti i analize trendova.

Osnovno izvještavanje ne smije postati kompleksan sustav izvještavanja, nego minimalni skup praktičnih izvještaja i pregleda koji se mogu redovito pratiti:

- **Dnevni operativni pregled:** stanje ključnih servisa, greške integracija, odstupanja u performansama, neuspjele prijave i anomalije.
- **Tjedni sigurnosni pregled:** agregat neuspjelih prijava, pokušaji pristupa bez ovlaštenja, administrativne promjene, top incidenti i korelirani događaji.
- **Mjesečni pregled prava:** popis aktivnih privilegiranih računa, promjene ovlaštenja, i potvrda da su prava usklađena s ulogama.

Financira
Europska unija
NextGenerationEU

Izvještaji se moraju generirati iz istog sustava logiranja i nadzora, bez dodatnih ručnih evidencija, kako bi održavanje ostalo jednostavno i dosljedno.

6.7. Kontinuitet poslovanja, visoka raspoloživost i sigurnosne kopije

Prije finalnog dizajna kontinuiteta mora se provesti kategorizacija imovine i analiza utjecaja na poslovanje (Business Impact Analysis). Imovina se razvrstava prema funkciji i poslovnom značaju u kategorije: kritično, važno i ostalo, a rezultati analize koriste se za određivanje prioriteta oporavka i minimalnih razina usluge tijekom incidenta ili katastrofe.

NIS2 u sklopu mjera upravljanja rizicima eksplicitno uključuje kontinuitet poslovanja, upravljanje sigurnosnim kopijama i oporavak nakon katastrofe. Projektni zahtjevi ovaj dio dodatno pooštravaju: eADR su postavljeni kao **kritična imovina (TIER 1)** uz ciljeve **RPO = 0** i **RTO ≈ 0**, te uz zahtjev da se u najtežim scenarijima maksimalno dopušteno vrijeme prekida (MTD) ograniči na **2 sata**. Ovi ciljevi moraju biti ugrađeni u infrastrukturu, aplikacijski dizajn i operativne postupke.

Arhitektura kontinuiteta mora se temeljiti na dvosite modelu (Zagreb i Kerestinec) s aktivnoaktivnom logikom i sinkronom replikacijom kritičnih podataka. U praksi to podrazumijeva da obje lokacije imaju istu produkcijsku konfiguraciju te da baze podataka rade uz sinkronu replikaciju, a aplikacijski sloj se opterećenje raspodjeljuje preko obje lokacije. U slučaju gubitka jedne lokacije druga mora preuzeti sav promet **bez gubitka podataka** i bez vidljivog prekida usluge ili uz minimalno degradirani način rada koji je unaprijed definiran.

Sigurnosna pohrana i sigurnosne kopije moraju slijediti definiranu strategiju (npr. **3-2-1-1-0** ili strože), pri čemu je važno da postoji kopija izvan mjesta obrade i kopija izvan mreže (offline). U praksi to znači da se backup repozitorij dimenzionira za kombinaciju aplikacijskih podataka i baza, uz deduplikaciju i jasna pravila retencije, te da se kopije štite enkripcijom i kontrolama pristupa. Korištenje offline kopije izravno smanjuje rizik od ransomware scenarija, što je jedna od tipičnih prijetnji koje NIS2 nastoji adresirati.

Kontinuitet nije potpun bez testiranja oporavka. Testovi oporavka moraju biti planirani i periodični, ali bez narušavanja produkcijskog SLA-a, što je i projektno naglašeno kroz potrebu periodičnih testiranja DR scenarija. Minimalno je potrebno provoditi: test povrata odabrane baze iz backupa, test prebacivanja servisa na drugu lokaciju, te test provjere da aplikacijski sloj i integracije rade nakon failovera. Rezultati testova izražavaju se kroz RPO/RTO/MTD po komponentama, a izvještavanje se svodi na sažetak i potvrdu da su ciljevi ispunjeni.

6.8. Sigurnost integracija i lanca opskrbe te upravljanje ranjivostima

Integracijski sloj (API-ji, eDelivery/AS4, adapteri prema SOTAH-u i registrima) predstavlja jedan od najizloženijih dijelova sustava i mora biti projektiran s jasnim sigurnosnim granicama. U projektnim dokumentima je predviđena segmentacija mreže na sigurne i nesigurne zone, uz troslojnu produkcijsku arhitekturu, što se mora dosljedno primijeniti tako da se vanjski i

Financira Europska unija
NextGenerationEU

poluvanjski tokovi terminiraju u kontroliranim zonama (npr. DMZ), uz primjenu firewall pravila, dopuštenih portova i protokola te zaštitnih komponenti (npr. WAF) gdje je to primjenjivo.

Sigurnost integracija mora obuhvatiti i identitet integracijskih sudionika. Za tokove poput eDelivery/AS4 očekuju se kriptografski mehanizmi (TLS, signiranje/verifikacija poruka), a za API integracije stroga autentifikacija servisa (npr. međusobni TLS, tokenski pristup) i whitelisting partnera gdje je to opravdano. Posebno je važno uvesti konzistentnu validaciju ulaznih podataka i poruka (format, shema, obvezna polja), jer se time smanjuje rizik od injekcija, zlonamjernih payloadova i logičkih napada kroz integracijske kanale.

NIS2 zahtijeva da se u mjerama upravljanja rizicima obuhvati i **sigurnost lanca opskrbe**. U ovom projektu to znači da se u nabavi i ugovorima predvide minimalne sigurnosne obveze isporučitelja rješenja i opreme, bez uvođenja dodatnih vanjskih subjekata. Minimalno se ugovorno mora osigurati: pravodobna isporuka sigurnosnih zakrpa, obavještavanje o ranjivostima, jasno definiran način pristupa isporučitelja (bez nekontroliranog udaljenog pristupa) te obveza čuvanja podataka kao poslovne/službene tajne sukladno projektnim zahtjevima.

Upravljanje ranjivostima i zakrpama mora biti jednostavno, ali dosljedno. Potrebno je uspostaviti inventar softverskih i infrastrukturnih komponenti (verzije, podrška, kraj životnog ciklusa), redoviti ciklus ažuriranja te postupak hitnog ažuriranja u slučaju kritične ranjivosti. Operativno se ovo naslanja na logiranje i monitoring: nakon zakrpe mora postojati osnovna provjera da su ključne usluge funkcionalne te da nije došlo do degradacije integracijskih tokova ili sigurnosnih kontrola.

Sigurnost razvoja i održavanja mora osigurati da promjene ne uvode nove ranjivosti i da je sustav i dalje održiv. To uključuje kontrolu konfiguracije (verzioniranje konfiguracija i infrastrukture), osnovno sigurnosno testiranje prije produkcije (npr. provjera kritičnih ranjivosti u ovisnostima) te postupanje po otkrivenim ranjivostima kroz jasno definiran tok i odgovornosti. Na ovaj način se ispunjava NIS2 zahtjev sigurnosti u nabavi, razvoju i održavanju, bez uvođenja prekomjerno složenih kontrolnih mehanizama.

Prava pristupa dobavljača i izvođača moraju se dodjeljivati isključivo prema načelima poslovne potrebe, najmanjih ovlasti i razdvajanja nadležnosti. Svi pristupi moraju biti autorizirani, individualno dodijeljeni, zaštićeni višefaktorskom autentikacijom gdje je moguće te redovito revidirani. Dobavljači ne smiju imati administratorske ovlasti na razini operacijskog sustava na produkcijskim sustavima. Administratorske ovlasti na razini aplikacije mogu se odobriti trećim stranama samo pod jasno definiranim uvjetima, uz prethodno odobrenje, nadzor i vremensko ograničenje. Fizički pristupi prostorima i opremi moraju biti ograničeni i nadzirani, uz obvezu prihvaćanja sigurnosnih pravila.

Financira
Europska unija
NextGenerationEU

Eksternalizacija funkcija i korištenje vanjskih IKT usluga dopušteni su samo iznimno, uz prethodno odobrenje i obaveznu procjenu rizika koja obuhvaća gubitak kontrole, neovlašteni pristup, neusklađenost s propisima, ovisnost o trećoj strani, rizik prekida usluge, lokaciju pohrane i prijenos preko granica te rizik dijeljene infrastrukture. Ponuđeno rješenje u pravilu mora biti izvedeno na infrastrukturi AKD-a bez oslanjanja na javne cloud usluge.

6.9. Minimalni skup sigurnosne dokumentacije i dokazivost provedbe mjera

Za NIS2 usklađenost nije dovoljno samo "imati sigurnost", nego mora postojati mogućnost **dokazivanja** da su mjere implementirane i da se provode. Projektnom dokumentacijom je predviđeno da se izradi i održava konkretna dokumentacija o povezanim uslugama, mrežnoj shemi, pravilima komunikacije, zaštiti podataka, kategorizaciji i kontinuitetu. Ova dokumentacija mora biti dio isporuke rješenja i mora se moći održavati kroz životni ciklus sustava bez velikog administrativnog opterećenja.

Minimalni skup dokumentacije koji mora postojati i biti održavan uključuje:

- **Popis vezanih usluga i integracija:** za svaku vanjsku i internu uslugu na koju se sustav spaja navodi se naziv, URL, pružatelj, protokoli i portovi te vrsta podataka koji se razmjenjuju (primjerice domena, NIAS, sustav logiranja i sl.).
- **Shema mreže i segmentacija:** vizualni prikaz komponenti i povezanosti, mrežne zone, lokacije, Internet/VPN točke, IP rasponi po segmentima, redundancija i rezervne veze/komponente.
- **Pravila komunikacije (allow-list):** popis dopuštenih mrežnih prometa između komponenti (izvor → odredište, protokol/port, svrha), uz pripadajuća firewall pravila i zone.
- **Zaštita podataka:** opis pseudonimizacije gdje je primjenjivo, enkripcije, autentifikacije, autorizacija, logiranja i dugoročne pohrane.
- **Kontinuitet i oporavak:** backup strategija, ciljevi oporavka po komponentama (RPO/RTO/MTD) te sažeti rezultati periodičnih testova povrata i failovera.
- **Incidenti i održavanje:** kontaktne točke za održavanje i sigurnosne incidente, uvjeti i način održavanja te tok eskalacije.

Dokazivost se ne postiže kroz dodatne "registre" ili složene kontrolne mehanizme, nego kroz to da gore navedena dokumentacija bude verzionirana i ažurirana kroz redovni proces promjena, a dnevnički zapisi i izvještaji iz monitoringa/logiranja služe kao objektivan trag provedbe. Time se omogućava da se na zahtjev nadležnih tijela ili u internim provjerama brzo pokaže: kako je sustav segmentiran, tko može pristupiti kojim podacima, kako se incidenti detektiraju i obrađuju, te kako se osigurava oporavak i raspoloživost.

Održavanje dokumentacije mora biti usklađeno s modularnom arhitekturom sustava: svaki modul (eADR, integracije, identitet, monitoring) mora imati jasne "sigurnosne granice" i pripadajući dio dokumentacije. Na taj se način buduće nadogradnje (npr. dodavanje novih

Financira Europska unija NextGenerationEU

datasetova ili integracija) mogu uključiti u postojeći sigurnosni okvir bez preinaka temeljnih procesa i bez povećanja složenosti održavanja.

7. Zahtjevi za integraciju i interfacing (povezivanje s postojećim nacionalnim i EU sustavima)

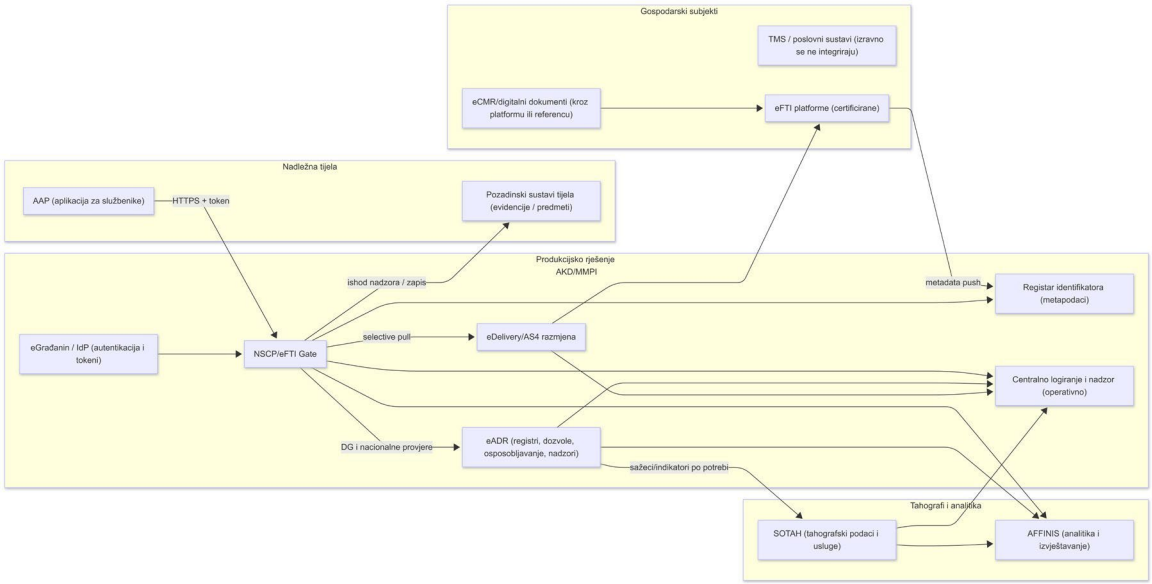
Ovo poglavlje definira zahtjeve za integraciju i sučelja (interfacing) između produkcijskog rješenja eADR te postojećih sustava u Republici Hrvatskoj i relevantnih EU ekosustava. Tekst je namjerno usmjeren na zahtjeve koji dopunjuju već opisanu ciljnu arhitekturu i integracijske tokove iz poglavlja 5., pri čemu se izbjegava ponavljanje komponenti i osnovnih tokova (metapodaci, selektivni dohvat, eADR provjere, SOTAH i analitika). Naglasak je na **praktičnim integracijskim zahtjevima**: što se mora povezati, u kojem opsegu, kojim minimalnim tehničkim ugovorima i kako osigurati stabilan rad uz jednostavno održavanje.

Opseg projekta u ovom poglavlju promatra se kroz operativne potrebe cestovnog prometa unutar Republike Hrvatske. Integracije se stoga definiraju tako da su **interoperabilne s eFTI standardom**, ali se operativno fokusiraju na nacionalne tokove i nacionalne sustave. Time se osigurava da se u produkciji implementira samo ono što je potrebno i traženo, bez uvođenja dodatnih vanjskih dionika ili višestrukih paralelnih rješenja.

Integracije se projektiraju prema principu **jednostavnog i stabilnog povezivanja**: svako sučelje mora imati jasno definiranog vlasnika, jasnu svrhu, standardizirani format poruka, sigurnosni mehanizam i operativni način nadzora. Rješenje ne smije zahtijevati specifične prilagodbe prema velikom broju različitih vanjskih sustava; umjesto toga, gospodarski subjekti se priključuju kroz eFTI platforme, a nadležna tijela kroz AAP i, gdje je potrebno, kroz standardizirane “pozadinske” integracije za razmjenu ishoda nadzora.

Za sve integracije vrijedi jedinstveni skup minimalnih načela: minimizacija podataka, sljedivost pristupa, verzioniranje sučelja, upravljanje pogreškama i ponovnim pokušajima, te jedinstveni korelacijski identifikatori koji povezuju događaje kroz sustav. Ovim se omogućuje stabilan rad sustava i osnovno izvještavanje bez dodatnih složenih evidencija ili kompliciranih operativnih kontrola.

Financira
Europska unija
NextGenerationEU



Slika 25. Integracija s nacionalnim i EU sustavima

7.1. Katalog integracijskih točaka i prioriteti implementacije

Integracijski zahtjevi u produkcijskom rješenju moraju biti popisani i upravljani kroz jasan katalog integracijskih točaka. Katalog se koristi kao operativni "popis sučelja" koji omogućuje implementaciju i održavanje bez dodatnih dionika i bez potrebe za specifičnim prilagodbama po sustavu. Svaka integracijska točka mora imati minimalno definirane: naziv sučelja, smjer komunikacije, protokol, sigurnosni mehanizam, vrstu podataka i očekivani način rada (sinkrono/asinkrono, batch/on-demand).

Prioritet implementacije sučelja mora slijediti logiku operativne kontrole: prvo se implementiraju sučelja koja omogućuju službeniku da dobije provjerljive podatke u realnom vremenu (metapodatci, selektivni dohvat, eADR provjere), zatim sučelja koja omogućuju nacionalne provjere i povezivanje s tahografskim uvidima, te naposljetku sučelja za razmjenu ishoda i osnovno izvještavanje prema pozadinskim sustavima nadležnih tijela. Ovakav prioritet osigurava da rješenje u produkciji prvo podrži ključnu funkciju – kontrolu na terenu – a zatim nadograđuje administrativne i analitičke potrebe.

Katalog integracijskih točaka mora jasno razlikovati integracije koje su **obavezne** i one koje su **uvjetno obavezne** (ovisno o procesu). Primjerice, dohvat metapodataka i selektivni dohvat punog eFTI sadržaja su obavezni za eFTI dio, dok je dohvat sažetaka iz SOTAHa uvjetan i aktivira se samo kada je potreban za ADR kontekst ili kada postoje indikatori koji zahtijevaju dodatni uvid. Na taj način sustav ostaje jednostavan i ne uvodi trajno opterećenje integracija koje nisu nužne u većini slučajeva.

Financira Europska unija
NextGenerationEU

- **Sučelja prema eFTI platformama:** obavezna sučelja za metapodatke i selektivni dohvat, uz standardizirane poruke, kriptozaštitu i korelacijske identifikatore radi dokazivosti.
- **Sučelja prema nacionalnim ADR evidencijama:** obavezna sučelja za provjere dozvola i osposobljenosti te evidenciju nadzora, jer su sastavni dio operativnog postupanja kod opasnih tvari.
- **Sučelja prema tahografskom sustavu:** uvjetna sučelja koja se koriste za sažetke i indikatore, uz strogu minimizaciju podataka i jasno definiran opseg po zahtjevu.
- **Sučelja prema pozadinskim sustavima nadležnih tijela:** sučelja za razmjenu ishoda i osnovnih podataka o kontroli, bez preuzimanja funkcije "vođenja predmeta" unutar eADR sustava.

Financira
Europska unija
NextGenerationEU

7.2. Zahtjevi za povezivanje s eFTI ekosustavom i eFTI platformama

Integracija s eFTI platformama mora biti izvedena tako da eFTI Gate može provoditi dvije ključne funkcije bez oslanjanja na dodatne sustave: **brzi uvid u metapodatke** i **selektivni dohvat punog eFTI skupa podataka**. Sučelja moraju biti standardizirana i stabilna, jer se eFTI platforme mogu razlikovati po implementacijskim detaljima, ali Gate mora imati jedinstven način rada i jedinstven način evidencije zahtjeva i odgovora.

Za metapodatke je potrebno osigurati da su informacije dovoljne za operativnu odluku, ali da ne otkrivaju više od nužnog. Metapodatci moraju sadržavati identifikatore pošiljke, status, osnovne podatke o relaciji i indikatore vrste tereta (uključujući oznaku da se radi o opasnim tvarima), uz minimalne podatke potrebne za identifikaciju prijevoza u trenutku kontrole. Metapodatkovni mehanizam mora podržavati ažuriranja tijekom životnog ciklusa pošiljke, osobito događaje otvaranja i zatvaranja, kako bi se statusi mogli pravilno tumačiti.

Za selektivni dohvat punog eFTI sadržaja sučelja moraju osigurati da se podaci dohvaćaju **samo kada je potrebno** i **samo u opsegu koji je dopušten**. Implementacijski ugovor mora jasno definirati kako se navodi svrha kontrole, kako se prenosi identitet i ovlast nadležnog tijela, te kako se u odgovoru označava koji su podskupovi podataka uključeni (osobito DG podskup za opasne tvari). Time se omogućuje da Gate i AAP prikazuju podatke konzistentno i da se može dokazati "što je točno dohvaćeno" u konkretnom nadzoru.

Operativno, sučelja s platformama moraju biti otporna na promjenjivu dostupnost i latenciju. Nije prihvatljivo da se terenska kontrola prekida bez jasnog rezultata; sučelje mora podržati povrat stanja "dostupni metapodatci, puni dohvat trenutno nedostupan", uz korektan revizijski trag. Također, sučelje mora imati standardizirano ponašanje pri ponavljanju zahtjeva (idempotentnost) kako bi se izbjegli duplikati i nekonzistentni rezultati.

- **Identifikatori i korelacija:** svaki zahtjev prema platformi mora imati jedinstveni identifikator i korelacijski identifikator koji se veže uz konkretan nadzor; isti identifikatori se koriste u logiranju i u prikazu rezultata.
- **Opseg podataka:** platforma mora omogućiti dohvat punog dataseta ili definiranih podskupova, pri čemu se DG podaci tretiraju kao obavezni element kada je teret opasan.

  Ponašanje na pogrešku: sučelje mora jasno razlikovati pogreške autorizacije (npr. nedostatak ovlasti) od tehničkih pogrešaka (npr. timeout), jer se operativno postupanje razlikuje.
- **Upravljanje verzijama:** sučelja i poruke moraju imati jasno označene verzije, uz kompatibilnost koja omogućuje postupne nadogradnje bez prekida rada nadležnih tijela.

Financira Europska unija NextGenerationEU

7.3. Zahtjevi za eCMR i digitalnu dokumentaciju u kontekstu eFTI postupanja

Povezivanje s eCMR i digitalnom dokumentacijom mora biti riješeno tako da nadležno tijelo u postupku kontrole može dobiti **regulatorno relevantan prikaz dokumentacije** bez potrebe za dodatnim vanjskim aplikacijama ili zasebnim integracijama prema velikom broju pružatelja. U praksi to znači da se eCMR i povezani dokumenti tretiraju kao dio eFTI sadržaja ili kao referencirani dokumenti koje eFTI platforma može izložiti kroz standardizirani dohvat.

Sustav ne preuzima ulogu primarnog repozitorija eCMR dokumenata, nego mora omogućiti: (1) dohvat strukturiranih podataka koji odgovaraju sadržaju dokumenta, (2) prikaz ključnih elemenata u AAP-u, te (3) provjeru integriteta i vjerodostojnosti dokumenta kroz potpis, hash ili drugi dokazni mehanizam koji platforma izlaže. Time se omogućuje da kontrola bude provediva na terenu i da postoji dokaziv trag "što je pregledano" bez potrebe da se dokument fizički pohranjuje u Gateu.

U kontekstu opasnih tvari, digitalna dokumentacija mora uključivati i elemente ADR transportne dokumentacije (DG set), što znači da eCMR sadržaj nije dovoljan sam po sebi ako ne sadrži potrebne DG podatke. Sustav mora osigurati da se u slučaju DG pošiljke kroz eFTI dohvat dobije i DG informativni set te da se u AAP-u prikaže sažetak koji je operativno koristan (UN broj, razred, ograničenja), bez prekomjernog opterećenja korisnika.

Praktična implementacija zahtijeva i standardizirani način rukovanja prilozima i dokazima: dokument može biti "ugrađen" kao strukturirani set, može biti priložen kao datoteka, ili može biti dostupan kao referenca (URL/URI) koja vrijedi u kontroliranom vremenskom prozoru. Za sve varijante mora biti jasno definirano: koliko dugo je dokument dostupan, kako se kontrolira pristup, te kako se evidentira da je dokument dohvaćen ili pregledan u okviru nadzora.

- **Prikaz ključnih elemenata:** AAP mora prikazati sažetak eCMR-a (sudionici, relacija, datum, osnovna roba) i zasebno prikazati DG elemente kada su prisutni, bez oslanjanja na vanjske preglednike ili dodatne aplikacije.
- **Integritet i vjerodostojnost:** sustav mora moći pohraniti minimalne dokaze (npr. hash i podatke o potpisu) u zapis nadzora, kako bi se kasnije moglo dokazati što je točno dohvaćeno.
- **Upravljanje datotekama:** kada se prenose prilozi, mora postojati ograničenje veličine, standardizirani tipovi datoteka i kontrolirano rukovanje vremenom dostupnosti, uz audit trag pristupa.

  Jedinstvena implementacija: integracija s eCMR pružateljima se ne provodi "po pružatelju", nego isključivo kroz eFTI platformu i eFTI standardni dohvat, čime se smanjuje složenost održavanja.

Financira Europska unija NextGenerationEU

7.4. Zahtjevi za povezivanje s tahografskim sustavima (SOTAH) i analitičkim slojem (AFFINIS)

Integracija sa SOTAH-om mora biti osmišljena kao ciljana, kontrolirana i minimalno invazivna. i eADR sustav ne preuzima ulogu spremišta tahografskih podataka, nego koriste SOTAH kao izvor za **sažetke, indikatore i odabrane činjenice** koje su potrebne u kontekstu nadzora, uz strogo ograničenje opsega po zahtjevu. Ovakav pristup osigurava da integracija ostane održiva i da se volumen tahografskih podataka ne uvodi u operativne baze eADR sustava.

Sučelje prema SOTAH-u mora podržati jasno definirane upite koji su vezani uz identifikatore vozila, tahografske jedinice i vozača, uz vremenski ograničen obuhvat. To uključuje i potrebna mapiranja identifikatora (npr. registracija vozila ↔ tahograf ID) koja se provode kroz postojeće evidencije ili kroz već uspostavljene mehanizme u tahografskoj domeni. Zahtjev je da eADR može u realnom vremenu dohvatiti ono što je potrebno za konkretnu kontrolu, a da se istovremeno zadrži minimizacija i audit.

Integracija s AFFINIS-om mora osigurati analitičku obradu i osnovno izvještavanje bez dodatnih složenih operativnih mehanizama. Tokovi prema AFFINIS-u su primarno usmjereni na dnevne obrade i agregacije: kontrole, ishodi, indikatori, volumen poziva i odabrani atributi (npr. DG/bez DG). Ovdje je važno da se podaci šalju u obliku stabilnih, strukturiranih skupova, uz dosljedne šifrarnike i ključeve, kako bi se izbjegla potreba za ručnim “krpanjem” izvještaja.

Operativno, sučelja prema SOTAH-u i AFFINIS-u moraju biti nadzirana i mjerena. Ne uvode se složeni nadzorni mehanizmi, ali mora postojati minimalna vidljivost: uspješnost poziva, trajanje, učestalost grešaka i osnovna indikacija da dnevne obrade u analitici završavaju u očekivanom vremenu. Time se osigurava da sustav ostaje stabilan i da je moguće pravodobno reagirati na degradacije bez složenih procesa.

- **On-demand dohvat iz SOTAHa:** koristi se za sažetke i indikatore u okviru konkretnog nadzora, uz stroga vremenska ograničenja i audit o svrsi i opsegu.
- **Batch tokovi u AFFINIS:** koriste se za konsolidaciju i izvještavanje, uz jasno definiran dnevni raspored i minimalne skupove podataka potrebne za osnovne pokazatelje.
- **Kontrola pristupa:** pristup tahografskim podacima provodi se kroz eADR u kontekstu ovlaštenog nadzora, bez izravnog pristupa korisnika prema SOTAH-u.
- **Stabilnost ugovora:** sučelja moraju imati stabilan ugovor (format, nazivlja, šifrarnici) kako bi nadogradnje eADR sloja minimalno utjecale na tahografsku i analitičku domenu.

Financira
Europska unija
NextGenerationEU

7.5. Zahtjevi za povezivanje sa sustavima nadležnih tijela (operativni i pozadinski sustavi)

Povezivanje sa sustavima nadležnih tijela mora podržati dva osnovna slučaja uporabe: terensku kontrolu kroz AAP i evidenciju ishoda kontrole u pozadinskim sustavima tijela. AAP ostaje primarno operativno sučelje, dok pozadinska integracija služi tome da se rezultati kontrole (ishod, osnovni identifikatori, eventualne mjere) mogu povezati s internim evidencijama tijela, bez uvođenja dodatnih ručnih postupaka i bez dupliciranja funkcionalnosti "predmetnog sustava" unutar eADR rješenja.

Sučelje prema pozadinskim sustavima tijela mora biti minimalno, standardizirano i usmjereno na razmjenu onoga što je nužno za internu evidenciju. Ne uvodi se kompleksno upravljanje predmetima, niti se uvode višestruki različiti formati po tijelu. Umjesto toga, definira se kanonski skup podataka o nadzoru: identifikator nadzora, vrijeme i lokacija, identifikatori pošiljke/vozila, indikator DG, ishod kontrole i sažetak eventualnih mjera. Ovaj skup mora biti dovoljan da se u sustavu tijela može otvoriti ili dopuniti evidencija.

Zahtjev je da integracija bude izvediva i održiva bez stalne potrebe za usklađivanjem među više vanjskih dionika. Zbog toga sučelje treba biti usmjereno na "push" iz eADR sustava prema sustavima tijela (ili periodični izvoz), uz jasno definiranu validaciju i rukovanje pogreškama. Time se osigurava da eADR ostanu sustavi provedbe eFTI/ADR provjera, a sustavi tijela zadrže svoju ulogu u vođenju evidencija i postupanja.

Operativno, mora postojati i mogućnost osnovnog povratnog statusa, primjerice potvrda da je zapis uspješno zaprimljen u sustav tijela ili da je zaprimanje privremeno neuspjelo. To je nužno kako bi se izbjegla "tiha" neuspjela integracija koja bi kasnije zahtijevala ručno usklađivanje. Potvrde se evidentiraju u logovima i prikazuju operativnom održavanju kroz osnovne nadzorne pokazatelje.

- **Jedinstveni kanonski zapis nadzora:** isti skup polja koristi se za sva tijela kako bi se izbjeglo održavanje više varijanti sučelja.
- **Ograničeni opseg podataka:** u sustave tijela ne prenosi se puni eFTI dataset; prenosi se samo ono što je potrebno za evidenciju i dokazivost postupanja.
- **Jednostavna potvrda zaprimanja:** sustav tijela vraća potvrdu primitka ili tehničku grešku, što omogućuje pouzdano ponavljanje (retry) bez dupliciranja.
- **Usklađenost s ovlastima:** podaci koji se prenose moraju biti isti ili uži od onoga što je tijelo ovlašteno vidjeti u AAP-u, kako bi se zadržao princip najmanjih privilegija.

7.6. Zahtjevi za povezivanje s gospodarskim subjektima i njihovim sustavima (TMS i srodni sustavi)

Integracijski zahtjev prema gospodarskim subjektima postavlja se tako da produkcijsko rješenje ne zahtijeva izravno povezivanje s velikim brojem različitih TMS ili internih sustava

Financira Europska unija NextGenerationEU

prijevoznika. Operativni model je da gospodarski subjekti izlažu regulatorne podatke kroz eFTI platforme, a eFTI Gate komunicira s platformama kroz standardizirani eFTI mehanizam. Time se izbjegava potreba za održavanjem mnoštva specifičnih konektora, a odgovornost za povezivanje TMS-a i eFTI platforme ostaje kod gospodarskog subjekta i njegove platforme.

Za eADR dio, integracija s gospodarskim subjektima se provodi kroz standardne korisničke kanale (portali i obrasci) i kroz eGrađanin autentikaciju gdje je to primjenjivo, umjesto kroz integracije prema internim sustavima gospodarskih subjekata. To je usklađeno s ciljem da sustav ostane održiv i da se ne uvode dodatne integracijske obveze koje bi zahtijevale angažman više vanjskih dionika ili tvrtki.

U praksi, jedini obavezni "digitalni trag" gospodarskog subjekta prema sustavu je kroz eFTI platformu: metapodatci i eFTI dataset moraju biti dostupni, ažurni i dokazivi. Ako gospodarski subjekt koristi eCMR, dodatne dokumente ili vlastite procese, oni se izlažu kroz platformu kao dio dataseta ili kao referencirani sadržaj. eADR sustavi ne uvode dodatne specifične zahtjeve prema TMS-u, osim onih koji proizlaze iz eFTI interoperabilnosti i ADR DG informativnog seta.

Važno je da se prema gospodarskim subjektima osigura jedinstven i jasan "ugovor": koji su minimalni metapodatci potrebni, koji DG elementi moraju biti popunjeni, te koji su minimalni statusi i događaji koji se trebaju slati (otvaranje/zatvaranje). Ovaj ugovor se ne provodi kroz dodatne integracije, nego kroz validaciju i pravila eFTI podataka koja platforma i Gate primjenjuju.

- **Izbjegavanje izravnih TMS integracija:** sustav se ne povezuje izravno na TMS sustave; eFTI platforma je jedina standardna točka integracije prema gospodarskim subjektima.
- **Standardizirani eFTI ugovor:** skup obveznih elemenata (uključujući DG set) mora biti jasno definiran i tehnički validiran, kako bi se smanjio broj operativnih iznimki na kontroli.
- **Jedinstveni način dokazivanja:** dokaz o dostupnosti i sadržaju eFTI podataka ostvaruje se kroz eFTI dohvat i audit, a ne kroz dodatne potvrde ili paralelne evidencije.
- **Minimalna operativna složenost:** gospodarski subjekt ne dobiva više različitih "kanala" prema državi, nego jedan standardni kanal kroz eFTI platformu.

7.7. Standardizacija sučelja, verzioniranje i operativno održavanje integracija

Sva sučelja moraju biti dokumentirana i verzionirana tako da se promjene mogu uvoditi postupno, bez prekida rada na terenu i bez potrebe za čestim koordinacijama s velikim brojem vanjskih strana. U praksi to znači da se za svako sučelje definira verzija ugovora (API ili poruka), pravila kompatibilnosti i razdoblje podrške za prethodne verzije. Posebno je važno da se promjene koje utječu na integracije (npr. format metapodataka, struktura DG seta) uvode kroz kompatibilne nadogradnje, uz jasnu obavijest i planirano gašenje zastarjelih varijanti.

Financira Europska unija
NextGenerationEU

Operativno održavanje integracija mora se svesti na jasno mjerljive elemente i jednostavne alate: status sučelja, broj uspješnih/neuspješnih poziva, latencije, te popis zadnjih pogrešaka s korelacijom na nadzor. Nije cilj uvesti složen sustav upravljanja sučeljima, nego omogućiti da operativno održavanje može prepoznati probleme i otkloniti ih kroz standardne postupke, bez ručne analize na više mjesta.

Za sučelja prema eFTI platformama i prema SOTAH-u mora postojati jasno definiran "degradirani način rada" koji je operativno prihvatljiv: primjerice, metapodatci dostupni, puni dohvat privremeno nedostupan. Takvo stanje mora biti vidljivo službeniku na terenu (u smislu informacije da puni dohvat nije dostupan) i mora biti evidentirano u audit logovima. Time se izbjegava da se kontrola mora prekidati ili da se naknadno ne može dokazati što se dogodilo.

Upravljanje konfiguracijom sučelja provodi se centralno kroz konfiguracijske parametre (npr. endpointi, certifikati, dozvoljeni podskupovi podataka), uz jasna pravila promjena. Iako se detalji konfiguracije i isporuke opisuju u zasebnim poglavljima o operativnoj arhitekturi, ovdje je zahtjev da integracije budu projektirane tako da promjene budu rijetke, predvidljive i provedive bez složenih zahvata.

- **Verzioniranje ugovora:** svako sučelje ima jasno označenu verziju i pravila kompatibilnosti, uz planirano ukidanje zastarjelih verzija.
- **Jedinstveni operativni nadzor:** integracije se nadziru kroz zajednički skup metrika i logova, bez "specijalnih" alata po sučelju.
- **Degradirani rad:** definira se što sustav vraća i kako se ponaša kada vanjski sustav privremeno nije dostupan, uz audit i vidljivost korisniku.
- **Minimalne promjene i stabilnost:** cilj sučelja je stabilan ugovor s minimalnim brojem iznimki, kako bi se održavanje svelo na osnovne postupke.

8. Testni scenariji i validacijski postupci

Testni scenariji i validacijski postupci definiraju **konkretne, ponovljive korake** kojima se provjerava da eADR rješenje ispravno radi u stvarnim uvjetima rada, da je interoperabilno s integriranim sustavima (nacionalni eFTI čvor/gateway, SOTAH, AFFINIS te ostalim povezanim sustavima (NIAS i sličnima)) te da su provedene minimalne mjere informacijske sigurnosti i zaštite osobnih podataka sukladno obvezama projekta. Naglasak je na **end-to-end** provjerama koje može izvršiti ovlaštena osoba, uz jasno definirane očekivane rezultate i dokazne artefakte.

Scenariji su strukturirani tako da pokrivaju funkcionalnu razinu (poslovni procesi), integracijsku razinu (razmjena i sinkronizacija podataka), operativnu razinu (nadzor, zapisnici događaja, oporavak) te nefunkcionalne zahtjeve (performanse, raspoloživost, sigurnost). Pri tome se sustav tretira kao cjelina, uz provjere ključnih komponenti koje su već opisane u arhitekturi (npr. nacionalni eFTI čvor/gateway, AAP, eADR aplikacijski sloj, integracijski konektori, logkolektor, monitoring).

Financira Europska unija
NextGenerationEU

Za svaki scenarij definiraju se: **cilj**, **preduvjeti**, **testni podaci**, **koraci**, **očekivani rezultati**, te **dokaz** (što se mora pohraniti kao trag testiranja). Dokaz se prikuplja u minimalnom, praktičnom obliku: snimka zaslona ključnih ekrana, izvoz rezultata (npr. JSON odgovor API-ja), te isječak relevantnog zapisa iz aplikacijskog ili sigurnosnog dnevnika s korelacijskim identifikatorom.

Validacija se provodi u jasno razdvojenim okruženjima (razvojno, integracijsko/testno, UAT i produkcijsko), uz **kontrolu verzija** i "freeze" u UAT fazi kako bi se osigurala ponovljivost rezultata i mogućnost usporedbe prije/poslije korekcija.

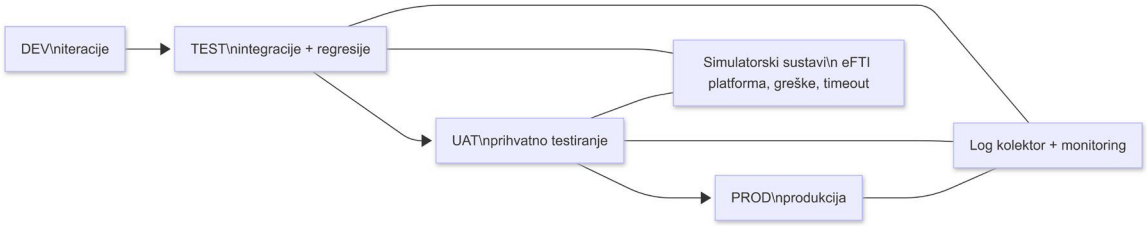
8.1. Testna okruženja i režim izvođenja testiranja

Testiranje se izvodi u najmanje tri logički odvojena okruženja: **TEST (integracijsko)**, **UAT (prihvatno)** i **PROD (produkcijsko)**. Razvojno okruženje služi izvođaču za iteracije i nije referentno za prihvat. TEST okruženje koristi se za integracijske provjere i automatizirane regresije, dok se UAT koristi za formalno prihvatno testiranje od strane ovlaštenih korisnika naručitelja i uključenih tijela.

U svim okruženjima moraju biti dostupne ključne integracije u obliku stvarne integracije ili kontrolirane simulacije. To uključuje: **NIAS/eGrađanin autentifikaciju**, **SOTAH sučelje** za dohvat/razmjenu agregata tahografskih podataka, **nacionalni eFTI čvor/gateway sučelja** za dohvat metapodataka i payload-a te **AFFINIS ulazne kanale** za dnevni batch. Kada stvarno vanjsko okruženje nije dostupno, koristi se **simulator** (mock/stub) koji reproducira iste poruke i greške (timeout, nevaljana poruka, nedostupnost).

Kako bi se spriječile promjene koje kompromitiraju rezultate, tijekom UAT-a vrijedi režim **kontroliranog upravljanja promjenama**: dopuštene su samo korekcije koje izravno uklanjaju grešku pronađenu u UAT-u, uz obveznu ponovnu validaciju povezanih scenarija. U praksi to znači da se za UAT uvodi "release kandidat" verzija aplikacije i konfiguracije (aplikacija, integracijski parametri, certifikati, sheme poruka).

Okruženja moraju imati uspostavljeno **osnovno praćenje i zapisivanje**: log-kolektor i monitoring moraju biti aktivni barem u TEST i UAT okruženju, jer su zapisnici događaja dio dokaznog materijala. Minimalno je potrebno moći pratiti: status integracija, greške obrade poruka, uspješnost autentifikacije, te korelacijske identifikatore zahtjeva.



Slika 26. Testna okruženja

Financira Europska unija
NextGenerationEU

8.2. Testni skupovi podataka i uloge testiranja

Za potrebe testiranja definira se **standardni testni skup podataka** koji se koristi konzistentno kroz više scenarija. Skup podataka mora biti dovoljno bogat da pokrije realne poslovne situacije: više pošiljaka u jednom prijevozu, jedna pošiljka raspodijeljena kroz više operacija (pretovar), različite vrste opasnih tvari (razredi), te kombinacije dozvola i osposobljenosti vozača. Podaci su fiktivni i ne smiju odgovarati stvarnim osobama; ujedno moraju zadovoljavati validacije sustava (npr. format OIB-a).

Standardni testni skup podataka (referentni identifikatori) definira se kako slijedi:

- **SUBJEKT (prijevoznik):** TransLogistika d.o.o., OIB 12345678903, adresa Savska cesta 31, 10000 Zagreb, država HR, id bdd640fb-0667-1ad1-1c80-317fa3b1799d
- **SUBJEKT (pošiljatelj):** Kemija-Distribucija d.o.o., OIB 98765432106, adresa Kukuljanovo 12, 51227 Kukuljanovo, HR, id 23b8c1e9-3924-56de-3eb1-3b9046685257
- **SUBJEKT (primatelj):** Industrija Plastike d.o.o., OIB 20250101017, adresa Vukovarska 55, 21000 Split, HR, id bd9c66b3-ad3c-2d6d-1a3d-1fa7bc8960a9
- **SUBJEKT (učilište):** ADR Centar Zagreb, OIB 11111111119, adresa Heinzelova 70, 10000 Zagreb, HR, id 972a8469-1641-9f82-8b9d-2434e465e150
- **TIJELO_IZDAVATELJ:** Ministarstvo nadležno za izdavanje dopuštenja (testno), id 17fc695a-07a0-ca6e-0822-e8f36c031199
- **OSOBA (vozač 1):** Marko Horvat, OIB 31415926539, datum rođenja 1988-05-14, id 9a1de644-815e-f6d1-3b8f-aa1837f8a88b
- **OSOBA (vozač 2):** Ivan Kovač, OIB 27182818283, datum rođenja 1990-09-02, id b74d0fb1-32e7-0629-8fad-c1a606cb0fb3
- **OSOBA (inspektor):** Petra Novak, OIB 16180339882, datum rođenja 1985-11-23, id 6b65a6a4-8b81-48f6-b38a-088ca65ed389
- **VOZILO (V1):** registracija ZG-7823-KD, VIN WDB1234561A123456, tip vozila TEGLEC, ADR oprema DA, tahograf TACHO-0001, id 47378190-96da-1dac-72ff-5d2a386ecbe0
- **VOZILO (V2):** registracija RI-4901-PT, VIN WDB1234561B654321, tip vozila KAMION, ADR oprema DA, tahograf TACHO-0002, id 8fadc1a6-060c-4776-0d30-31dcbc3a0b7d
- **LOKACIJA (utovar 1):** Zagreb – Skladište A, Heinzelova 70, 10000 Zagreb, HR, geo 45.807/15.981, id 5be6128e-18c2-6797-579a-13fdd481f4d3
- **LOKACIJA (pretovar):** Rijeka – Terminal B, Kukuljanovo 12, 51227, HR, geo 45.317/14.537, id 756e4f9b-3a8b-3f7e-7dbe-1f1a6b7d2a7b
- **LOKACIJA (istovar 1):** Split – Skladište C, Vukovarska 55, 21000, HR, geo 43.508/16.440, id 2f65d3b9-2b6b-0b47-7f3d-4a7b1c0e9d2e
- **DG_POSILJKA (C1):** referenca DG-2025-0001, eFTI consignment HR-eFTI-C-2025000001

Financira Europska unija NextGenerationEU

- **DG_STAVKA (C1-1):** UN 1203, BENZIN, ADR razred 3, klasifikacijski kod F1, ambalažna skupina II, pakiranje IBC, količina 24000, mjera L, tunnel D/E, transport category 2
- **DG_POSILJKA (C2):** referenca DG-2025-0002, eFTI consignment HR-eFTI-C-2025-000002
- **DG_STAVKA (C2-1):** UN 1090, ACETON, ADR razred 3, klasifikacijski kod F1, ambalažna skupina II, pakiranje BAČVA, količina 8000, mjera L, tunnel D/E, transport category 2

Uloge za testiranje moraju odgovarati stvarnim ovlastima u sustavu. Minimalni skup uloga koje se koriste u scenarijima je:

- **Službenik nadzornog tijela (AAP korisnik):** pokreće provjeru pošiljke/prijevoza i pregledava podatke eFTI/eADR.
- **Operater eADR registra:** unosi i održava registre subjekata, vozila, lokacija i osoba.
- **Operater osposobljavanja (učilište):** upravlja tečajevima, prijavama, ispitima i izdavanjem potvrda.
- **Operater dopuštenja (tijelo izdavatelj):** izdaje i opoziva dopuštenja te definira obuhvat dopuštenja.
- **Administrator sustava:** upravlja konfiguracijom integracija, certifikatima i osnovnim parametrima (bez "super ovlasti" nad sadržajem podataka).

Svaki testni korisnik mora biti mapiran na identitet u NIAS/eGrađanin testnom režimu, tako da se kroz autentifikaciju preuzmu identifikatori (npr. OIB) i dodijeli uloga. Time se izbjegava "ručno" kreiranje korisnika mimo predviđenog mehanizma pristupa i omogućuje realno testiranje autentifikacijskog toka.

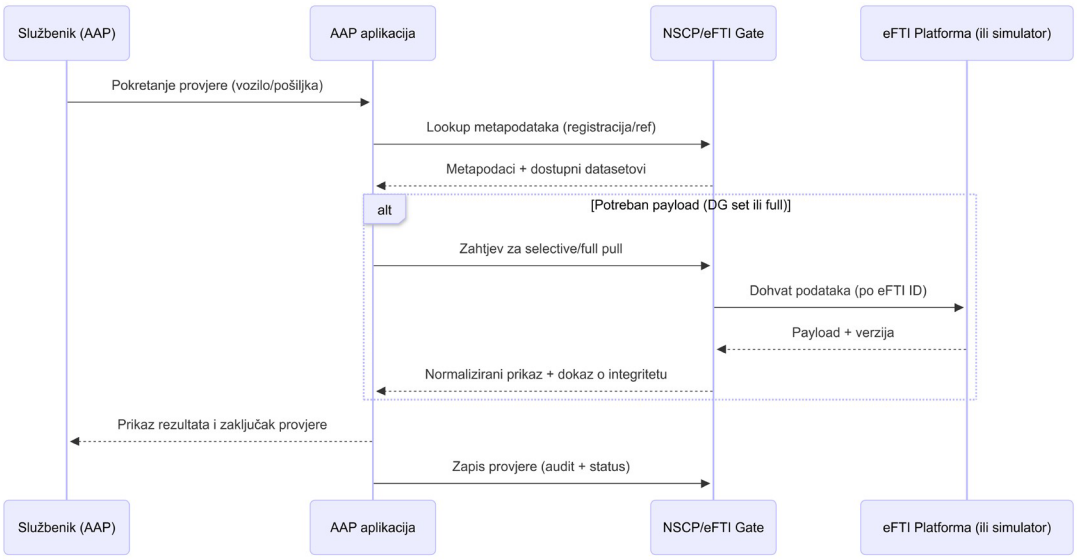
8.3. End-to-end scenariji nadzorne provjere kroz eADR

End-to-end scenariji eADR testiraju primarni operativni slučaj: **nadzorno tijelo provodi kontrolu prijevoza** i treba u kratkom vremenu dobiti pouzdane informacije o pošiljci i opasnim tvarima (DG set), uz mogućnost dodatnog dohvaćanja (payload) iz eFTI ekosustava. U ovom poglavlju scenariji su napisani tako da ih ovlaštena osoba može provesti i kada dio ekosustava nije dostupan, koristeći kontrolirani simulator.

Ključno je potvrditi da je sustav robustan na stvarne situacije: neujednačeni metapodaci, višestruki pretovari, više pošiljaka u jednom vozilu, ponovljene poruke, te situacije gdje je potrebno dohvatiti samo dio podataka (npr. DG set) umjesto cjelovitog sadržaja. Posebna pozornost je na tome da se **ne miješaju koncepti "operacije prijevoza" i "pošiljke"**: jedna operacija može pokrivati više pošiljaka, a jedna pošiljka može biti pokrivena s više operacija (pretovar, promjena vozila).

Scenariji ispod pretpostavljaju da je prijevoznik ili eFTI platforma dostavila metapodatke u nacionalni eFTI čvor/gateway (model "metadata push"), te da AAP koristi Gate za lookup i po potrebi selective/full pull. U svakom scenariju prikuplja se dokaz: identifikator provjere, vrijeme obrade, te relevantni zapis iz dnevnika događaja s korelacijskim ID-om.

Financira Europska unija NextGenerationEU



Slika 27. End-to-end scenarij nadzorne provjere

- TS-eFTI-01: Ingest metapodataka za novu pošiljku i kreiranje zapisa u Gateu ○ **Cilj:** potvrditi da Gate prima metapodatke za DG pošiljku DG-2025-0001 i kreira tražene identifikatore (eftiConsignmentId, status, vrijeme).
  - **Preduvjeti:** simulator eFTI platforme aktivan; definiran consignment HR-eFTI-C2025-000001; testni subjekti i lokacije postoje.
  - **Koraci:** (1) poslati "create consignment" metapodatke u Gate; (2) poslati "update" metapodatke s dopunom (npr. dodan DG set); (3) dohvatiti zapis kroz administrativni pregled ili API.
  - **Očekivano:** Gate vodi jednu pošiljku s verzioniranjem; ponovni "create" ne duplira zapis (idempotentnost); status je "aktivno" do zatvaranja.
  - **Dokaz:** snimka pregleda pošiljke u Gateu + izvoz JSON metapodataka + log linije s korelacijskim ID-om.
- TS-eFTI-02: Lookup po registraciji vozila i prikaz povezanih pošiljaka ○ **Cilj:** potvrditi da AAP može pronaći pošiljke koje se prevoze vozilom ZG-7823KD i da prikazuje C1 i C2 kao aktivne.
  - **Preduvjeti:** za V1 postoji operacija OP-2025-0001 koja uključuje C1 i C2; metapodaci su u Gateu.
  - **Koraci:** (1) prijava službenika u AAP (NIAS); (2) unos registracije ZG-7823-KD; (3) izvršiti pretraživanje; (4) otvoriti detalje rezultata.
  - **Očekivano:** AAP prikazuje listu pošiljaka (DG-2025-0001 i DG-2025-0002), uz osnovne podatke (pošiljatelj/primatelj, lokacije, status, zadnja izmjena).
  - **Dokaz:** snimka ekrana rezultata + zapis "audit access" za pregled pošiljaka.

Financira Europska unija
NextGenerationEU

- TS-eFTI-03: Selective pull samo za DG set (opasne tvari) za pošiljku C1 ○ **Cilj:** potvrditi da AAP može dohvatiti minimalni skup podataka potreban za provjeru opasnih tvari (UN broj, razred, količina, ograničenja) bez preuzimanja cijelog payload-a.

Financira
Europska unija
NextGenerationEU

- **Preduvjeti:** platforma/simulator podržava selective pull; C1 sadrži stavku UN 1203. ○ **Koraci:** (1) iz AAP detalja pošiljke odabrati “Dohvati DG set”; (2) potvrditi zahtjev; (3) pregledati prikaz.
  - **Očekivano:** prikazuju se svi elementi DG seta za UN 1203; zabilježeno je vrijeme dohvaćanja i identifikator verzije payload-a; nema prikaza nepotrebnih datasetova.
  - **Dokaz:** snimka ekrana DG seta + izvoz odgovora (JSON) + log o selective pull zahtjevu.

- TS-eFTI-04: Full pull cjelokupnog payload-a uz provjeru integriteta ○ **Cilj:** potvrditi da AAP može dohvatiti puni eFTI payload i da se na strani sustava provjerava integritet (npr. potpis/pečat, hash ili dokaz o izvornosti prema implementaciji).
  - **Preduvjeti:** platforma/simulator vraća payload s pripadajućim dokazom integriteta; Gate ima konfigurirane certifikate.
  - **Koraci:** (1) u AAP odabrati “Dohvati puni dokument”; (2) preuzeti payload; (3) otvoriti prikaz; (4) provjeriti da sustav prikazuje status “integritet OK”.
  - **Očekivano:** payload je dohvaćen i prikazan; sustav jasno naznačuje je li validacija uspjela; u slučaju neuspjeha payload se ne smije prezentirati kao pouzdan.
  - **Dokaz:** izvoz payload-a + snimka validacijskog statusa + log zapis o validaciji.
- TS-eFTI-05: Višestruke pošiljke u jednom prijevozu s različitim destinacijama ○ **Cilj:** potvrditi da AAP i eADR dio sustava mogu prikazati situaciju gdje vozilo prevozi više DG pošiljaka koje imaju različite primatelje i istovarne lokacije.
  - **Preduvjeti:** OP-2025-0001 uključuje C1 (istovar Split) i C2 (istovar Rijeka) uz definirane lokacije; u ruti postoje segmenti koji pokrivaju obje isporuke. ○ **Koraci:** (1) lookup po registraciji; (2) otvoriti C1, zatim C2; (3) pregledati prikaz lokacija utovara/istovara i rute; (4) provjeriti da AAP ne “spaja” destinacije.
  - **Očekivano:** svaka pošiljka prikazuje vlastite lokacije i status; nema prepisivanja destinacije između C1 i C2; ruta/segmenti se pravilno vežu na operaciju, a pošiljke ostaju zasebne.
  - **Dokaz:** snimke ekrana za C1 i C2 + logovi “view consignment”.
- TS-eFTI-06: Jedna pošiljka pokrivena s više operacija (pretovar i promjena vozila) ○ **Cilj:** potvrditi poslovnu logiku “pošiljka se može prevoziti kroz više operacija” i da sustav to prikazuje bez gubitka sljedivosti.
  - **Preduvjeti:** C1 se prevozi kroz OP-2025-0001 (ZG→RI, V1) i OP-2025-0002 (RI→ST, V2); veza operacija-pošiljka postoji u modelu.
  - **Koraci:** (1) u AAP otvoriti C1; (2) prikazati “povezane operacije”; (3) otvoriti detalje svake operacije; (4) provjeriti da se vidi gdje je došlo do pretovara (Rijeka – Terminal B).

    C1 ima dvije operacije s različitim vozilima; vremenski i lokacijski slijed je konzistentan; pretovar se vidi kao točka prijelaza; nema dupliciranja pošiljke.

- **Očekivano:**
- **Dokaz:** snimka prikaza “povezane operacije” + izvještaj (print/PDF) iz AAP-a ako je predviđen.

- TS-eFTI-07: Idempotentnost i obrada ponovljenih poruka metapodataka ○ **Cilj:** potvrditi da Gate ne kreira duplikate kada primi istu poruku (npr. zbog ponovnog slanja platforme).
  - **Preduvjeti:** simulator šalje identičan “create/update” s istim identifikatorima.
  - **Koraci:** (1) poslati create; (2) poslati isti create još jednom; (3) provjeriti broj zapisa; (4) poslati update dva puta.
  - **Očekivano:** broj zapisa ostaje 1; verzija se ne povećava bez stvarne promjene; log jasno označava “duplicate ignored” ili ekvivalentno.
  - **Dokaz:** izvoz zapisa iz Gatea prije/poslije + logovi s oznakom duplikata.
- TS-eFTI-08: Negativni slučaj – nedostaju obvezna polja DG seta ○ **Cilj:** potvrditi da sustav odbija ili označava podatke kao nevaljane kada nedostaju obvezna polja (npr. UN broj ili ADR razred). ○ **Preduvjeti:** simulator šalje DG set bez UN broja za C2.
  - **Koraci:** (1) poslati selective pull odgovor bez UN; (2) u AAP pokušati prikazati DG set; (3) provjeriti poruku greške.
  - **Očekivano:** AAP prikazuje jasnu poruku da je dataset nevaljan i ne može se koristiti za provjeru; incident se evidentira u aplikacijskim logovima.
  - **Dokaz:** snimka greške + log zapis validacije sheme.
- TS-eFTI-09: Timeout i kontrolirano ponavljanje dohvaćanja ○ **Cilj:** potvrditi da AAP/Gate uredno obrađuju situaciju kada platforma ne odgovara u definiranom vremenu, te da ponavljanje zahtjeva radi bez duplikata. ○ **Preduvjeti:** simulator namjerno kasni s odgovorom; definiran limit vremena.
  - **Koraci:** (1) pokrenuti full pull; (2) simulirati timeout; (3) ponoviti zahtjev; (4) zatim omogućiti brzi odgovor i provjeriti uspjeh.
  - **Očekivano:** korisnik dobiva razumljivu obavijest; sustav ne stvara “zaleđene” zapise; ponovljeni zahtjev nakon dostupnosti platforme uspijeva i ispravno se bilježi. ○ **Dokaz:** snimka poruke timeouta + logovi retry mehanizma.
- TS-eFTI-10: Zatvaranje pošiljke i post-factum provjera ○ **Cilj:** potvrditi da nakon zatvaranja pošiljke (deliver/close) metapodaci ostaju dostupni za naknadne provjere sukladno pravilima retencije, te da se status odražava u AAP-u.
  - **Preduvjeti:** simulator šalje “close consignment” za C1; retencija je konfigurirana.
  - **Koraci:** (1) poslati close; (2) u AAP dohvatiti C1; (3) provjeriti status; (4) pokušati selective pull i provjeriti dopuštenost nakon zatvaranja (prema pravilima sustava).

    status je “zatvoreno”; dohvat povijesnih podataka radi; sustav jasno označava datum zatvaranja i zadnju verziju. ○ **Dokaz:** snimka prikaza statusa + log “close processed”.

Financira Europska unija NextGenerationEU

- **Očekivano:**

8.4. Funkcionalni scenariji eADR sustava (registri, osposobljavanje, dopuštenja, nadzor)

Funkcionalno testiranje eADR sustava pokriva operativne procese koji su specifični za prijevoz opasnih tvari u cestovnom prometu: vođenje registara (subjekti, vozila, osobe, lokacije), upravljanje osposobljavanjem (programi, tečajevi, ispiti, potvrde), izdavanje dopuštenja te vođenje nadzora i povezivanje s eFTI podacima. eADR dio uvodi dodatne nacionalne poslovne elemente i mora ih moći povezati s pošiljkama i operacijama prijevoza.

Scenariji u ovom poglavlju fokusirani su na **realne kombinacije podataka**: vozač koji ima važeću potvrdu, vozač kojem je istekla potvrda, vozilo s ADR opremom i bez nje, dopuštenje ograničeno na određene UN brojeve, te slučajevi gdje je prijevoz u tijeku i nadzorno tijelo treba u jednoj sesiji vidjeti i eFTI DG set i nacionalne registre (dopuštenja, osposobljenost).

Kako bi testovi bili praktično provedivi, preporuka je da se u UAT okruženju pripreme inicijalni registri (subjekti, vozila, osobe) i da se kroz scenarije nadograđuju. Time se izbjegava da svaki scenarij mora ponavljati cijeli unos osnovnih podataka, a ipak se zadržava sljedivost što je nastalo u kojem testu.

U dokaznom dijelu ovih scenarija naglasak je na tome da se može rekonstruirati “tko je što promijenio”: zato se uz snimke ekrana čuvaju i zapisi audit dnevnika (kreiranje/izmjena brisanjem se ne simulira u poslovnim registrima, osim ako je predviđeno statusima poput “poništeno”).

- TS-eADR-01: Kreiranje i validacija subjekta prijevoznika u registru ○ **Cilj:** potvrditi unos subjekta TransLogistika d.o.o. i validacije ključnih polja (OIB, adresa, tip subjekta).
  - **Preduvjeti:** operater eADR registra prijavljen; sustav povezan s NIAS.
  - **Koraci:** (1) otvoriti modul “Subjekti”; (2) kreirati zapis s OIB 12345678903; (3) označiti tip “prijevoznik”; (4) spremiti; (5) otvoriti detalje i provjeriti audit zapis.
  - **Očekivano:** subjekt je kreiran; OIB format prihvaćen; audit bilježi korisnika i vrijeme kreiranja; subjekt je dostupan za odabir u operacijama.
  - **Dokaz:** snimka ekrana detalja subjekta + audit zapis.
- TS-eADR-02: Unos vozila i povezivanje s prijevoznikom ○ **Cilj:** potvrditi da se vozilo V1 može unijeti, validirati i povezati s prijevoznikom. ○ **Preduvjeti:** subjekt prijevoznik postoji.
  - **Koraci:** (1) otvoriti modul “Vozila”; (2) unijeti ZG-7823-KD, VIN WDB1234561A123456, ADR oprema DA, tahograf TACHO-0001; (3) odabrati vlasnika/operatera TransLogistika; (4) spremiti.

Financira Europska unija NextGenerationEU

- **Očekivano:**

- vozilo je kreirano; vidljiva je veza na prijevoznika; vozilo se može dodijeliti operaciji prijevoza.
  Dokaz: snimka ekrana vozila + izvoz zapisa (ako postoji) + audit.

- TS-eADR-03: Unos vozača i povezivanje s prijevoznikom ○ **Cilj:** potvrditi da se OSOBA "Marko Horvat" može unijeti i koristiti kao primarni vozač operacije.
  - **Preduvjeti:** modul osoba aktivan; definiran format datuma i OIB validacija.
  - **Koraci:** (1) otvoriti "Osobe"; (2) kreirati Marko Horvat, OIB 31415926539, datum 1988-05-14; (3) spremiti; (4) provjeriti da se osoba može odabrati kao vozač.
  - **Očekivano:** osoba je kreirana; može se koristiti u operacijama i potvrđivanju osposobljenosti.
  - **Dokaz:** snimka ekrana osobe + audit.
- TS-eADR-04: Definicija programa osposobljavanja i kreiranje tečaja ○ **Cilj:** potvrditi da se program "ADR osnovni" i tečaj u ADR Centru Zagreb mogu definirati i aktivirati.
  - **Preduvjeti:** učilište ADR Centar Zagreb postoji kao subjekt tipa "učilište".
  - **Koraci:** (1) kreirati program (šifra ADR-OSN, tip ADR_OSNOVNI, minimalni sati 18, aktivan DA); (2) kreirati tečaj (datum početka 2026-02-02, završetka 202602-04, maxPolaznika 20). ○ **Očekivano:** program i tečaj su vidljivi; status tečaja "PLANIRAN"; tečaj se može otvoriti za prijave.
  - **Dokaz:** snimke ekrana programa i tečaja + audit.
- TS-eADR-05: Prijava kandidata na tečaj, održavanje ispita i upis rezultata ○ **Cilj:** potvrditi cjelovit tok od prijave Marko Horvat na tečaj do rezultata ispita. ○ **Preduvjeti:** tečaj iz TS-eADR-04 postoji; kandidat postoji.
  - **Koraci:** (1) prijaviti Marka na tečaj (status PRIJAVLJEN); (2) kreirati ispit (datum 2026-02-04); (3) označiti ispit "ODRŽAN"; (4) unijeti rezultat (bodovi 86, ishod POLOŽIO).
  - **Očekivano:** kandidat prelazi u status "ZAVRSIO"; rezultat je vezan uz ispit; audit bilježi unos rezultata.
  - **Dokaz:** snimka ekrana prijave + rezultat ispita + audit.
- TS-eADR-06: Izdavanje potvrde osposobljenosti i provjera valjanosti ○ **Cilj:** potvrditi izdavanje potvrde za Marka Horvata i provjeru valjanosti pri kreiranju operacije.
  - **Preduvjeti:** položen ispit; konfigurirana pravila trajanja potvrde prema programu.
  - **Koraci:** (1) izdati potvrdu (broj ADR-POT-2026-00015, datum izdavanja 2026-0205, datum isteka 2031-02-05, status VAZECA); (2) otvoriti profil osobe i provjeriti potvrdu; (3) pokušati dodijeliti vozača operaciji prijevoza opasnih tvari.

potvrda je vezana uz osobu i program; operacija prihvaća vozača s

važećom potvrdom; u slučaju isteka sustav mora upozoriti ili blokirati prema pravilima.
    - **Dokaz:** snimka potvrde + snimka dodjele vozača u operaciji.
- TS-eADR-07: Izdavanje dopuštenja za prijevoz s obuhvatom UN brojeva ○ **Cilj:** potvrditi izdavanje dopuštenja koje je ograničeno na UN 1203 i UN 1090 te povezano na vozilo i vozača.
    - **Preduvjeti:** postoji tijelo izdavatelj; postoje vozilo V1 i vozač Marko.
    - **Koraci:** (1) definirati vrstu dopuštenja (šifra DOP-ADR-OP, naziv "Dopuštenje za prijevoz opasnih tvari"); (2) kreirati dopuštenje (broj akta DOP-2026-0011, datum početka 2026-02-10, datum isteka 2027-02-10, status IZDANO); (3) dodati obuhvat: UN 1203 i UN 1090; (4) spremiti.
    - **Očekivano:** dopuštenje je važeće i povezano na V1 i Marka; obuhvat se prikazuje u detaljima; sustav dopušta povezivanje s operacijom samo ako operacija sadrži DG stavke koje su pokrivene dopuštenjem.
    - **Dokaz:** snimka dopuštenja i obuhvata + audit.
- TS-eADR-08: Kreiranje operacije prijevoza s više pošiljaka i ruta segmentima ○ **Cilj:** potvrditi da se može kreirati operacija OP-2025-0001 koja obuhvaća C1 i C2, uz rutu i planirane datume. ○ **Preduvjeti:** postoje lokacije Zagreb – Skladište A i Rijeka – Terminal B i Split – Skladište C; postoje C1 i C2; postoji vozilo i vozač.
    - **Koraci:** (1) kreirati operaciju (eftiTransportId HR-eFTI-T-2025-000001, planirani polazak 2025-12-15 06:00, dolazak 2025-12-15 12:00); (2) povezati prijevoznika, vozilo, vozača; (3) povezati pošiljke C1 i C2; (4) dodati rutu segmente Zagreb→Rijeka (redoslijed 1), Rijeka→Split (redoslijed 2).
    - **Očekivano:** operacija sadrži više pošiljaka; ruta je pravilno poredana; provjera valjanosti dopuštenja i potvrde osposobljenosti prolazi za stavke C1/C2.
    - **Dokaz:** snimka operacije s listom pošiljaka i rute.
- TS-eADR-09: Pretovar – kreiranje nove operacije i povezivanje iste pošiljke (C1) na drugu operaciju ○ **Cilj:** potvrditi da ista pošiljka C1 može biti vezana na OP-2025-0002 nakon pretovara, bez dupliciranja pošiljke.
    - **Preduvjeti:** OP-2025-0001 postoji; C1 postoji; vozilo V2 i vozač Ivan Kovač postoje.
    - **Koraci:** (1) kreirati OP-2025-0002 (Rijeka→Split); (2) povezati C1; (3) označiti mjesto pretovara Rijeka – Terminal B; (4) u prikazu C1 provjeriti da su vidljive obje operacije.
    - **Očekivano:** C1 je vezana na dvije operacije; slijed operacija je logičan; sustav prikazuje povijest i trenutni aktivni segment.
    - **Dokaz:** snimka pošiljke C1 s povezanim operacijama + snimka OP-2025-0002.
- TS-eADR-10: Nadzor eADR – evidentiranje kontrole i nalaza

Financira Europska unija NextGenerationEU

- **Očekivano:**

  Cilj: potvrditi da službenik može evidentirati nadzor operacije/pošiljke, unijeti nalaz i generirati zapis.

  Preduvjeti: postoji operacija OP-2025-0001; službenik Petra Novak ima ovlasti.

- **Koraci:** (1) prijava u AAP; (2) pokrenuti nadzor za ZG-7823-KD; (3) pregledati DG set; (4) označiti rezultat nadzora “Usklađeno” ili “Neusklađeno” s obrazloženjem; (5) spremiti.
- **Očekivano:** kreiran je zapis nadzora s jedinstvenim ID-om; vidljiv je datum/vrijeme, korisnik, referenca operacije/pošiljke; audit bilježi pristup i unos.
- **Dokaz:** snimka potvrde pohrane nadzora + izvoz zapisa (ako postoji) + audit.

- TS-eADR-11: Integracija sa SOTAH – prikaz tahografskog sažetka za operaciju
  - **Cilj:** potvrditi da eADR može dohvatiti ili prikazati sažetak (ukupno vrijeme vožnje/odmora/rada) za operaciju iz SOTAH izvora.
  - **Preduvjeti:** za tahograf TACHO-0001 postoje testni agregati u SOTAH; konektor je konfiguriran.
  - **Koraci:** (1) otvoriti detalje operacije OP-2025-0001; (2) odabrati “Taho sažetak”; (3) dohvatiti podatke; (4) provjeriti prikaz ukupnih sati.
  - **Očekivano:** prikaz se popunjava vrijednostima; u slučaju nedostupnosti SOTAH sustav prikazuje poruku “podaci privremeno nedostupni” bez rušenja procesa.
  - **Dokaz:** snimka ekrana tahografskog sažetka + log integracijskog poziva.
- TS-eADR-12: Dnevni batch u AFFINIS – validacija da su nadzori i operacije ušli u analitiku
  - **Cilj:** potvrditi da se novi zapisi (operacija, pošiljka, nadzor) prenose u AFFINIS kroz dnevni batch i dostupni su u analitičkim pogledima.
  - **Preduvjeti:** batch raspored aktivan; definiran minimalno jedan ciklus obrade u 24h.
  - **Koraci:** (1) osigurati da su kreirani OP-2025-0001 i nadzor; (2) pokrenuti batch; (3) u AFFINIS provjeriti da postoji zapis u odgovarajućim fakt tablicama/pogledima; (4) usporediti ključne identifikatore (npr. eftiTransportId, broj nadzora).
  - **Očekivano:** zapisi su vidljivi u AFFINISu; referencijalne veze na dimenzije (vozilo, vozač, prijevoznik) su popunjene; batch log prikazuje uspješan završetak.
  - **Dokaz:** izvoz retka/izvještaja iz AFFINISa + batch log.

Financira Europska unija NextGenerationEU

8.5. Integracijski scenariji i validacija sučelja prema vanjskim sustavima

Integracijski scenariji provjeravaju da svi ključni kanali razmjene podataka rade stabilno i konzistentno: od autentifikacije i autorizacije, preko dohvaćanja tahografskih agregata iz SOTAH, do razmjene eFTI metapodataka/payload-a i predaje podataka u AFFINIS analitiku. Fokus je na **praktičnoj interoperabilnosti**: sustav mora raditi i kada je jedna integracija privremeno nedostupna, uz jasne poruke korisniku i evidentiranje u zapisnicima.

Validacija sučelja mora obuhvatiti: **sheme poruka**, **mapiranje polja**, **kodove statusa**, **idempotentnost**, **kontrolu pristupa** i **rukovanje greškama**. Posebno je važno potvrditi da su u porukama i zapisima prisutni korelacijski identifikatori, jer bez toga je u stvarnom radu teško spajati događaje preko više komponenti.

Integracijski testovi se u pravilu izvode u TEST okruženju, dok se u UAT okruženju radi smanjeni, ali reprezentativan skup scenarija koji demonstrira da integracije rade u “realnom” načinu rada (s NIAS prijavom i ovlaštenjima stvarnih uloga). U slučaju razlike između TEST i UAT, UAT rezultat se smatra referentnim za prihvat.

U nastavku su integracijski scenariji organizirani po integraciji, s naglaskom na konkretne provjere.

Financira
Europska unija
NextGenerationEU

- TS-INT-01: NIAS/eGrađanin prijava – mapiranje identiteta i dodjela uloge ○ **Cilj:** potvrditi prijavu u AAP i eADR uz preuzimanje OIB-a i dodjelu pripadne uloge bez ručnog unosa korisnika.
    - **Preduvjeti:** konfiguriran NIAS testni režim; postoje mapiranja uloga (npr. "Službenik nadzornog tijela").
    - **Koraci:** (1) prijava kao Petra Novak; (2) pristup modulu nadzora; (3) odjava; (4) prijava kao operater učilišta; (5) pristup modulu tečajeva.
    - **Očekivano:** Petra vidi samo funkcije nadzora; operater učilišta vidi samo module osposobljavanja; audit bilježi prijave/odjave.
    - **Dokaz:** snimke ekrana vidljivih izbornika po ulozi + audit log.
- TS-INT-02: SOTAH integracija – dohvat agregata prema tahograf jedinci ○ **Cilj:** potvrditi da sustav dohvaća sažetak za TACHO-0001 i da je odgovor mapiran u TAHO_SAZETAK model.
    - **Preduvjeti:** SOTAH testni endpoint aktivan; postoje podaci za TACHO-0001.
    - **Koraci:** (1) pozvati dohvat iz eADR (UI ili servis); (2) provjeriti prikazane vrijednosti; (3) usporediti s očekivanim vrijednostima u SOTAH testnom zapisu.
    - **Očekivano:** vrijednosti se podudaraju; ne pojavljuje se duplo spremanje za isti vremenski interval; greške se bilježe u logu ako poziv ne uspije.
    - **Dokaz:** snimka prikaza + log integracije.
- TS-INT-03: AFFINIS batch – provjera "T+1" obrade i konzistentnosti dimenzija ○ **Cilj:** potvrditi da dnevni batch preuzima sve nove zapise i da dimenzije (vozilo, vozač, prijevoznik) nisu duplicirane.
    - **Preduvjeti:** batch mehanizam aktivan; pristup AFFINIS analitičkom pregledu ili SQL-u.
    - **Koraci:** (1) kreirati novu operaciju OP-2025-0002 i nadzor; (2) pokrenuti batch; (3) u AFFINISu pronaći operaciju i nadzor; (4) provjeriti da vozilo ZG-7823-KD postoji samo jednom u dimenziji.
    - **Očekivano:** fakt zapisi postoje; dimenzije su jedinstvene; batch ima status "uspješno".
    - **Dokaz:** izvoz rezultata iz AFFINISa (npr. CSV ili screenshot upita) + batch log.
- TS-INT-04: eFTI platforma – provjera kompatibilnosti selektivnog i punog dohvaćanja
    Cilj: potvrditi da se i selective pull i full pull mogu izvršiti za istu pošiljku te da verzije odgovaraju.
    Preduvjeti: platforma/simulator podržava oba načina; Gate konfiguriran.
    - **Koraci:** (1) za C1 izvršiti selective pull DG seta; (2) odmah nakon toga izvršiti full pull; (3) usporediti verziju i vrijeme generiranja.
    - **Očekivano:** verzije su konzistentne; full pull sadrži DG set koji je već viđen u selective pull; log jasno povezuje oba poziva.
    - **Dokaz:** izvoz oba odgovora + log s korelacijom.

Financira Europska unija NextGenerationEU

- TS-INT-05: Integracija sa sustavima nadležnih tijela – minimalni izvoz zapisa nadzora ○ **Cilj:** potvrditi da se zapis nadzora može izvesti u obliku koji je pogodan za razmjenu (npr. standardizirani JSON/CSV ili službeni izvještaj), bez dodatne ručne obrade.
    - **Preduvjeti:** kreiran nadzor u TS-eADR-10; definiran format izvoza.
    - **Koraci:** (1) otvoriti nadzor; (2) odabrati "Izvoz"; (3) preuzeti datoteku; (4) provjeriti da sadrži ključne identifikatore i zaključak.
    - **Očekivano:** izvoz je uspješan; sadržaj uključuje ID nadzora, datum/vrijeme, korisnika, povezanu pošiljku/operaciju i ishod. ○ **Dokaz:** spremljena izvezena datoteka + snimka ekrana izvoza.

8.6. Sigurnosni scenariji testiranja i validacijski postupci sukladno NIS2 i nacionalnim pravilima

Sigurnosno testiranje se provodi tako da potvrdi **minimalni, ali obvezni skup sigurnosnih kontrola**: upravljanje identitetima kroz NIAS/eGrađanin gdje je primjenjivo, kontrolu pristupa prema ulogama, zapisivanje događaja (audit), sigurnu komunikaciju (TLS) te osnovne operativne postupke (backup i oporavak). Naglasak nije na "kompleksnim kontrolama", nego na dokazivoj funkcionalnosti i ponovljivosti.

Validacija mora pokazati da sustav sprječava pristup bez ovlasti, da svaka kritična radnja ostavlja trag (tko, kada, što), te da se u slučaju sigurnosnog incidenta mogu brzo prikupiti osnovne informacije za procjenu i izvještavanje. U praksi to znači: audit događaji za prijavu, pregled osjetljivih podataka, izmjene registara, izdavanje potvrda i dopuštenja te kreiranje nadzora.

Sigurnosni testovi se izvode u TEST i UAT okruženju. U UAT-u se provodi smanjeni skup koji demonstrira ključne elemente (prijava, role-based pristup, audit trag), dok se detaljniji testovi (npr. skeniranje ranjivosti) izvode u TEST okruženju kako ne bi ometali prihvatno testiranje.

Scenariji ispod definiraju praktične provjere koje se mogu izvesti bez dodatnih vanjskih dionika i bez uvođenja novih, održavanju teških mehanizama.

- TS-SEC-01: Kontrola pristupa po ulogama – zabrana pristupa modulu dopuštenja za neovlaštenog korisnika

  Cilj: potvrditi da korisnik u ulozi "učilište" ne može pristupiti modulu izdavanja dopuštenja.

  Preduvjeti: NIAS mapiranje uloga aktivno; korisnik učilišta postoji. ○ **Koraci:** (1) prijava kao operater učilišta; (2) pokušaj otvaranja modula "Dopuštenja"; (3) pokušaj direktnog URL pristupa (ako je web). ○ **Očekivano:** pristup odbijen; korisnik vidi jasnu poruku o nedostatku ovlasti; događaj je zapisan u audit log (neuspješan pokušaj).

Financira Europska unija NextGenerationEU

- **Dokaz:** snimka poruke + audit zapis.

- TS-SEC-02: Audit trag – pregled osjetljivih podataka pošiljke i evidentiranje pristupa ○ **Cilj:** potvrditi da se svaki pregled DG seta bilježi (tko je pristupio, kojoj pošiljci, u koje vrijeme).
  - **Preduvjeti:** postoji pošiljka C1; službenik ima ovlasti.
  - **Koraci:** (1) prijava kao Petra Novak; (2) otvoriti C1; (3) dohvatiti DG set; (4) otvoriti audit pregled; (5) pronaći događaj.
  - **Očekivano:** audit sadrži OIB/korisnički identitet, akciju "view DG set", referencu C1 i korelacijski ID.
  - **Dokaz:** snimka audit zapisa + log linija iz log-kolektora.
- TS-SEC-03: Sigurna komunikacija – TLS provjera između ključnih komponenti ○ **Cilj:** potvrditi da se komunikacija AAP↔Gate i Gate↔platforma odvija isključivo šifrirano te da je odbijen nešifrirani pristup. ○ **Preduvjeti:** TLS konfiguriran; pristupne točke dostupne.
  - **Koraci:** (1) pokušati pristup HTTP endpointu (ako postoji); (2) potvrditi da je preusmjerenje na HTTPS ili zabrana; (3) izvršiti normalan zahtjev i provjeriti TLS handshake (npr. kroz evidenciju reverse proxyja).
  - **Očekivano:** HTTP nije dopušten; HTTPS radi; logovi pokazuju važeći certifikat i bez grešaka.
  - **Dokaz:** snimka rezultata + relevantni log iz reverse proxyja.
- TS-SEC-04: Upravljanje sesijom – odjava i istek sesije ○ **Cilj:** potvrditi da odjava prekida sesiju i da se nakon isteka sesije zahtijeva nova prijava.
  - **Preduvjeti:** NIAS prijava radi.
  - **Koraci:** (1) prijava; (2) otvoriti osjetljivi ekran (pošiljka/dopuštenje); (3) odjava; (4) pokušati "back" i pristup; (5) ostaviti sesiju neaktivnom do isteka i pokušati radnju.
  - **Očekivano:** nakon odjave nema pristupa; nakon isteka sesije sustav vraća na prijavu; audit bilježi događaje.
  - **Dokaz:** snimke ekrana + audit.
- TS-SEC-05: Osnovna provjera ranjivosti aplikacijskog sučelja (OWASP) u TEST okruženju ○ **Cilj:** potvrditi da su implementirane osnovne zaštite (npr. validacija ulaza, zabrana SQL injection kroz parametre pretraživanja, CSRF zaštita gdje je relevantno).

  Preduvjeti: TEST okruženje; odobrenje za izvođenje; korištenje standardnog alata za DAST.

  Koraci: (1) izvršiti automatizirani sken na AAP i eADR web sučelje; (2) pregledati nalaze; (3) za nalaze visoke kritičnosti provesti ručnu potvrdu.
  - **Očekivano:** nema nalaza visoke kritičnosti; eventualni srednji nalazi imaju plan korekcije prije produkcije.
  - **Dokaz:** izvještaj alata (PDF/HTML) spremljen u dokazni repozitorij.

Financira Europska unija NextGenerationEU

- TS-SEC-06: Simulacija sigurnosnog incidenta – višestruki neuspjeli pokušaji prijave i alarmiranje ○ **Cilj:** potvrditi da sustav evidentira sumnjive pokušaje i da su događaji vidljivi u log-kolektoru/SIEM-u, bez potrebe za dodatnim ručnim prikupljanjem.
    - **Preduvjeti:** log-kolektor i (ako postoji) SIEM integracija aktivni u TEST/UAT.
    - **Koraci:** (1) izvršiti 10 neuspjelih prijava zaredom; (2) provjeriti log-kolektor; (3) provjeriti da postoji događaj/oznaka "sumnjiva aktivnost".
    - **Očekivano:** događaji su zabilježeni i pretraživi; sustav po potrebi primjenjuje ograničenje (rate limit) ili privremenu blokadu, prema konfiguraciji. ○ **Dokaz:** izvoz log pretrage s timestampovima + snimka ekrana.

8.7. Testovi performansi, opterećenja i stabilnosti

Testovi performansi potvrđuju da sustav može obraditi očekivani broj provjera, dohvaćanja metapodataka i payload-a te istovremene korisnike bez degradacije koja bi onemogućila rad nadzornih tijela. Ovi testovi se provode ciljano, u kontroliranom okruženju (TEST), uz jasno definiran scenarij opterećenja koji reflektira stvarne obrasce: veliki broj "lookup" zahtjeva, manji broj "full pull" zahtjeva te kontinuirani rad batch obrada.

Opterećenje se ne testira samo na aplikacijskom sloju, nego i na pratećim komponentama koje mogu biti usko grlo: baza podataka, integracijski konektori, log-kolektor i storage. Pri opterećenju mora se pratiti minimalni skup metrika: vrijeme odgovora, postotak grešaka, iskorištenje CPU/RAM, broj otvorenih konekcija te brzina zapisa logova.

Stabilnost se validira kroz "soak" testove (više sati kontinuiranog rada) jer se problemi često javljaju nakon duljeg rada: curenje memorije, prepunjenje diskova logovima ili degradacija konekcija prema vanjskim sustavima. Pri tome cilj nije maksimalna sofisticiranost, nego dokaz da sustav u realnom režimu može stabilno raditi i da je njegovo ponašanje predvidivo.

Testovi performansi moraju završiti jasnim rezultatima: ostvarene vrijednosti vremena odziva i propusnosti, te potvrda da sustav u zadanim parametrima ne gubi podatke (npr. nema "izgubljenih" audit događaja).

- TS-PERF-01: Opterećenje lookup metapodataka (najčešći slučaj nadzora) ○ **Cilj:** potvrditi da Gate može izdržati opterećenje pretraživanja/lookup metapodataka uz stabilno vrijeme odziva.
    - **Preduvjeti:** generirani metapodaci za najmanje 10 000 testnih pošiljaka (simulacija); alat za load test.

Financira Europska unija NextGenerationEU

- **Koraci:** (1) generirati 20 zahtjeva u sekundi tijekom 15 minuta prema “lookup” endpointu; (2) pratiti vrijeme odziva i greške; (3) provjeriti log-kolektor i DB metrika.
- **Očekivano:** stopa grešaka ostaje minimalna; vrijeme odziva ostaje u prihvatljivim granicama definiranima za operativni nadzor; sustav ne pokazuje rast latencije kroz vrijeme.
- **Dokaz:** izvještaj load testa + snimka ključnih metrika iz monitoringa.

- TS-PERF-02: Kombinirano opterećenje lookup + selective pull + full pull ○ **Cilj:** potvrditi da sustav može istovremeno obrađivati velike količine lookup zahtjeva i manji udio payload dohvaćanja.
  - **Preduvjeti:** platforma/simulator vraća payload; Gate ima konfigurirano spremanje snapshot-a prema pravilima. ○ **Koraci:** (1) 20 RPS lookup; (2) 6 RPS selective pull; (3) 3 RPS full pull; trajanje 30 minuta; (4) pratiti metričke pokazatelje.
  - **Očekivano:** sustav zadržava stabilnost; nema nekonzistentnih verzija; payload dohvaćanja ne blokiraju lookup.
  - **Dokaz:** izvještaj opterećenja + uzorak logova za uspješne i neuspješne zahtjeve.
- TS-PERF-03: UAT test responzivnosti korisničkog sučelja (AAP) ○ **Cilj:** potvrditi da AAP u UAT okruženju ostaje responzivan pri realnom broju istovremenih korisnika.
  - **Preduvjeti:** najmanje 20 istovremenih sesija (ovlaštene osobe) ili simulacija.
  - **Koraci:** (1) simultano izvođenje pretrage po registraciji i otvaranje DG seta; (2) mjerenje vremena učitavanja ključnih ekrana; (3) bilježenje sporih operacija.
  - **Očekivano:** sučelje ostaje upotrebljivo; nema “zamrzavanja”; greške su minimalne i vidljivo obrađene.
  - **Dokaz:** zapis vremena učitavanja + snimke ekrana eventualnih grešaka.
- TS-PERF-04: Batch stabilnost – dnevni batch za AFFINIS u planiranom vremenskom prozoru ○ **Cilj:** potvrditi da batch obrada može završiti unutar predviđenog vremenskog prozora bez ručnog interveniranja.
  - **Preduvjeti:** pripremljen dnevni ulaz (operacije, nadzori, pošiljke); batch scheduler aktivan.
  - **Koraci:** (1) pokrenuti batch; (2) pratiti trajanje; (3) provjeriti broj obrađenih zapisa; (4) potvrditi dostupnost u AFFINISu.
  - **Očekivano:** batch uspješno završava; svi zapisi su prebačeni; log prikazuje jasne statistike (broj zapisa, trajanje, eventualne greške).
  - **Dokaz:** batch log + AFFINIS dokazni izvoz.
- TS-PERF-05: Log volumen – provjera da log-kolektor može trajno prihvatiti povećan broj događaja ○ **Cilj:** potvrditi da se pri opterećenju ne gube audit i sigurnosni događaji te da pohrana ne prelazi pragove bez alarma.
  - **Preduvjeti:** log-kolektor aktivan; definirani pragovi.

Financira Europska unija NextGenerationEU

- **Koraci:**

  (1) tijekom TS-PERF-02 pratiti stopu ingestiranja logova; (2) simulirati dodatne audit događaje (prijave/odjave); (3) provjeriti da su svi događaji vidljivi u pretrazi.

- **Očekivano:** nema gubitaka; alarmi se aktiviraju samo kada pragovi budu stvarno prijeđeni; sustav ostaje stabilan. ○ **Dokaz:** izvoz log pretrage + snimka metrika log-kolektora.

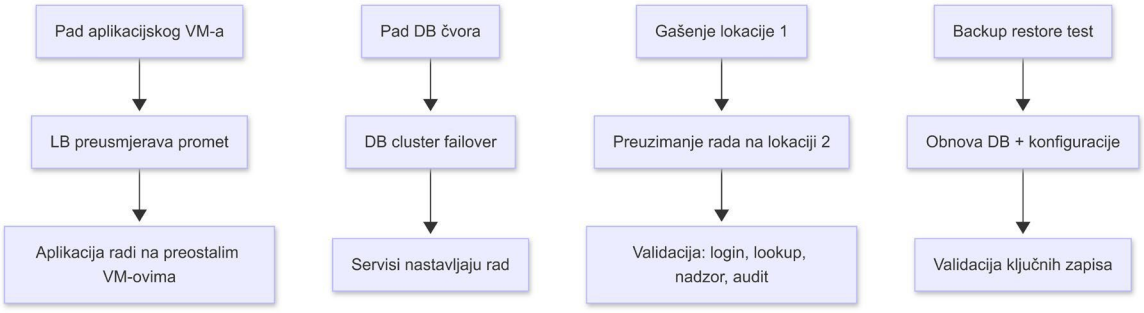
8.8. Validacija visoke raspoloživosti, oporavka i sigurnosnih kopija

Validacija raspoloživosti i oporavka potvrđuje da sustav može nastaviti rad u slučaju ispada pojedine komponente i da se može oporaviti nakon većeg incidenta (npr. prekid rada jedne lokacije). U projektnoj arhitekturi je cilj da produkcijski sustav radi u režimu koji omogućuje **kontinuitet usluge**, uz jasno definirane ciljeve oporavka (RPO/RTO/MTD) i provjerenu proceduru.

Za potrebe testiranja razlikuju se dva tipa scenarija: (1) **lokalni failover** unutar iste lokacije (pad VM-a, pad aplikacijskog servisa, failover baze), i (2) **lokacijski failover** (kontrolirano gašenje primarne lokacije i preuzimanje rada na sekundarnoj). Kod lokalnog failovera očekuje se kratkotrajna degradacija ili kratki prekid, dok kod lokacijskog failovera cilj je zadržati uslugu unutar definiranog MTD-a.

Sigurnosne kopije i povrat podataka testiraju se kroz procedure “backup-restore”, a ne kroz teorijski opis. Minimalno se mora dokazati: uspješno stvaranje kopije, čitljivost kopije, povrat baze i aplikacijskih konfiguracija, te provjera konzistentnosti (npr. postoje li operacije/pošiljke koje su unesene prije incidenta).

Scenariji u nastavku su pisani tako da su izvedivi u kontroliranim uvjetima, uz jasnu evidenciju što se gasi i što se očekuje da preuzme rad.



Slika 28. Validacija visoke raspoloživosti

- TS-DR-01: Failover aplikacijskog sloja (pad jedne VM instance AAP ili Gate komponente) ○ **Cilj:** potvrditi da pad jedne instance ne prekida rad sustava i da promet preuzima druga instanca.
  - **Preduvjeti:** barem dvije instance kritičnih servisa; load balancer konfiguriran.

Financira Europska unija NextGenerationEU

- **Koraci:** (1) aktivna sesija u AAP-u; (2) namjerno ugasiti jednu VM instancu servisa; (3) ponoviti lookup; (4) provjeriti da korisnik može nastaviti.
- **Očekivano:** kratkotrajna degradacija je dopuštena; funkcionalnost se vraća bez ponovne prijave ako je sesija valjana; incident je evidentiran u monitoringu.
- **Dokaz:** snimke ekrana prije/poslije + monitoring događaj.

- TS-DR-02: Failover baze (pad primarnog DB čvora u klasteru) ○ **Cilj:** potvrditi automatski failover i nastavak rada bez gubitka podataka. ○ **Preduvjeti:** DB klaster aktivan; mehanizam failovera testiran.
  - **Koraci:** (1) kreirati novi nadzor ili novi zapis (npr. novi tečaj) i potvrditi spremanje; (2) ugasiti primarni DB čvor; (3) ponoviti spremanje nove radnje; (4) provjeriti da su oba zapisa dostupna.
  - **Očekivano:** failover se dogodi; aplikacija nastavlja rad; nema gubitka zapisa; u logu postoji jasan trag failovera.
  - **Dokaz:** snimke zapisa + DB/monitoring log.
- TS-DR-03: Lokacijski failover – kontrolirano gašenje primarne lokacije i provjera ključnih funkcija ○ **Cilj:** potvrditi da sekundarna lokacija može preuzeti rad i da su ključne funkcije dostupne.
  - **Preduvjeti:** produkcijski ili produkciji sličan setup s obje lokacije; definirana procedura.
  - **Koraci:** (1) prije gašenja provesti lookup i spremiti referentni rezultat; (2) ugasiti usluge primarne lokacije; (3) provjeriti DNS/LB preusmjerenje; (4) ponovno: login, lookup, selective pull, spremanje nadzora.
  - **Očekivano:** sustav postaje dostupan na sekundarnoj lokaciji u planiranom vremenu; funkcije rade; podaci su konzistentni i ne nedostaju zapisi prije failovera.
  - **Dokaz:** zapis vremena preuzimanja + snimke ključnih ekrana + monitoring događaji.
- TS-DR-04: Backup i restore baze eADR – povrat na testnu instancu i validacija konzistentnosti ○ **Cilj:** dokazati da se baza može vratiti iz sigurnosne kopije i da su podaci čitljivi. ○ **Preduvjeti:** dostupna kopija; pripremljena restore instanca u TEST okruženju.
  - **Koraci:** (1) izvršiti restore; (2) otvoriti eADR aplikaciju na restore instanci; (3) provjeriti postojanje subjekta, vozila, potvrde i nadzora iz testnog skupa; (4) izvršiti jedan read-only upit i potvrditi konzistentnost.
  - **Očekivano:** restore uspješan; ključni zapisi postoje; aplikacija se može podići; nema korupcije.
  - **Dokaz:** zapis restore procedure + snimke ključnih zapisa.
- TS-DR-05: Backup i restore konfiguracije integracija (certifikati, endpointi, parametri) ○ **Cilj:** potvrditi da se konfiguracija može vratiti bez ručnog rekonfiguriranja cijelog sustava.
  - **Preduvjeti:** konfiguracije su u centralnom repozitoriju i backupirane.

Financira Europska unija NextGenerationEU

- **Koraci:**
  (1) namjerno promijeniti endpoint u TEST okruženju (kontrolirano); (2) potvrditi da integracija ne radi; (3) vratiti konfiguraciju iz backup/repo; (4) potvrditi da integracija radi.
- **Očekivano:** povrat konfiguracije vraća ispravnu funkcionalnost; audit bilježi promjenu. ○ **Dokaz:** prije/poslije snimke statusa integracije + audit zapis promjene.

8.9. Kriteriji prolaznosti, evidencija rezultata i postupak prihvata testiranja

Kriteriji prolaznosti moraju biti jasni i operativni: scenarij je "prošao" ako su svi očekivani rezultati zadovoljeni i ako su prikupljeni dokazni artefakti. Scenarij je "nije prošao" ako bilo koji ključni očekivani rezultat nije ostvaren, ako je došlo do greške koja onemogućuje provedbu poslovnog procesa ili ako se ne može dokazati trag (npr. nedostaje audit zapis za kritičnu radnju).

Radi praktičnosti održavanja i izbjegavanja prekomjerne administracije, rezultati se vode u jedinstvenom registru testova (npr. tablica ili alat za praćenje), uz minimalni skup polja: ID scenarija, datum, okruženje, tester, rezultat, link na dokaz i napomena. Greške se evidentiraju samo kada imaju utjecaj na prolaznost scenarija ili predstavljaju sigurnosni/operativni problem (npr. nekontrolirani pristup ili gubitak podataka).

Prihvat testiranja u UAT fazi provodi se tako da se potvrdi minimalno: (1) end-to-end nadzor kroz AAP i Gate (lookup + DG set), (2) osnovni eADR tokovi (registri, osposobljavanje, dopuštenja), (3) integracije (NIAS, SOTAH, AFFINIS), te (4) audit i zapisnici događaja. Time se osigurava da sustav može ući u produkciju bez "skrivenih" ovisnosti i bez dodatnih neplaniranih aktivnosti.

U završnom UAT izvještaju prilažu se dokazni paketi za svaki ključni scenarij. Minimalni dokazni paket za scenarij sadrži: snimku ekrana rezultata, izvoz relevantnog zapisa (gdje je primjenjivo) i isječak loga s korelacijskim ID-om. Za performansne i DR testove dokazni paket uključuje izvještaj opterećenja i snimke metrika/monitoringa.

- **Minimalni set scenarija za UAT prihvat (obvezno):** TS-eFTI-02, TS-eFTI-03, TS-eADR-05, TS-eADR-07, TS-eADR-10, TS-INT-01, TS-INT-02, TS-SEC-01, TS-SEC-02, TS-DR-01.
- **Minimalni set scenarija za produkcijsku spremnost (preporučeno):** TS-eFTI-06, TS-INT03, TS-PERF-01, TS-PERF-02, TS-DR-02, TS-DR-04.

U slučaju da se u UAT-u provede korekcija greške, obvezno se ponavljaju svi scenariji koji direktno ovise o ispravku (regresija), te se u evidenciji jasno označava koja je verzija sustava testirana prije i poslije korekcije. Rezultat UAT-a smatra se konačnim tek kada svi obvezni scenariji prođu i kada su dokazni artefakti potpuni i pregledni.

Financira Europska unija
NextGenerationEU

9. Zahtjevi za dokumentaciju

Dokumentacija je **obvezna isporuka ugovora o razvoju eADR sustava** i mora biti operativno upotrebljiva za svakodnevni rad nadležnih tijela i administracije, te dovoljna za instalaciju, konfiguraciju, nadogradnje i sigurnosne postavke.

Za potrebe praktične implementacije i kasnijeg održavanja, dokumentacija se mora izrađivati po načelu **jedinstvenog izvora istine**: tehničke činjenice (konfiguracijski parametri, popisi sučelja, dijagrami, verzije, certifikati, mrežna pravila, obrasci nadzora i slično) moraju se preuzimati iz kontroliranih izvora (repozitorij konfiguracije, repozitorij koda, repozitorij dijagrama, manifest izdanja), a ne ručno prepisivati u više dokumenata. Time se smanjuje rizik da se dokumenti razilaze od stvarnog stanja sustava nakon prvih nadogradnji.

Dokumentacija mora pokriti cjelinu sustava kako je definirana kroz ranije arhitekturne cjeline: eADR (registri, osposobljavanje, dopuštenja i nadzori), integracijski sloj (eFTI sučelja, eDelivery/AS4, SOTAH i AFFINIS), sigurnosni sloj (identitet, ovlasti, zapisnici) te operativni sloj (monitoring, logiranje, sigurnosne kopije i oporavak). Pritom dokumentacija mora biti usmjerena na opseg projekta, tj. **cestovni promet unutar Republike Hrvatske**, uz jasno označavanje gdje se primjenjuju eFTI zahtjevi za DG informativni set i gdje se primjenjuju nacionalna pravila eADR domene.

Način izrade i isporuke dokumentacije mora biti postavljen tako da ne uvodi potrebu za angažmanom dodatnih vanjskih dionika izvan onih predviđenih projektnom dokumentacijom. Dokumenti se izrađuju i održavaju unutar projektnog okvira AKD/MMPI i ugovorenog izvođača, koristeći alate koji su prihvatljivi za on-premise rad i za državne projekte, uz jasnu verzioniranost, preglednost i mogućnost brze izmjene u okviru nadogradnji sustava.

9.1. Načela izrade dokumentacije i jedinstveni izvori istine

Dokumentacija se mora izraditi po načelu da svaki tip informacije ima **točno jedan primarni izvor** iz kojeg se ta informacija preuzima i u dokumentima samo prikazuje. Primjerice, popis sučelja i njihovih verzija ne smije postojati u tri različita dokumenta u tri različite varijante; mora postojati jedan kanonski popis (katalog sučelja) koji se u korisničkim i administratorskim uputama referencira samo u potrebnom opsegu.

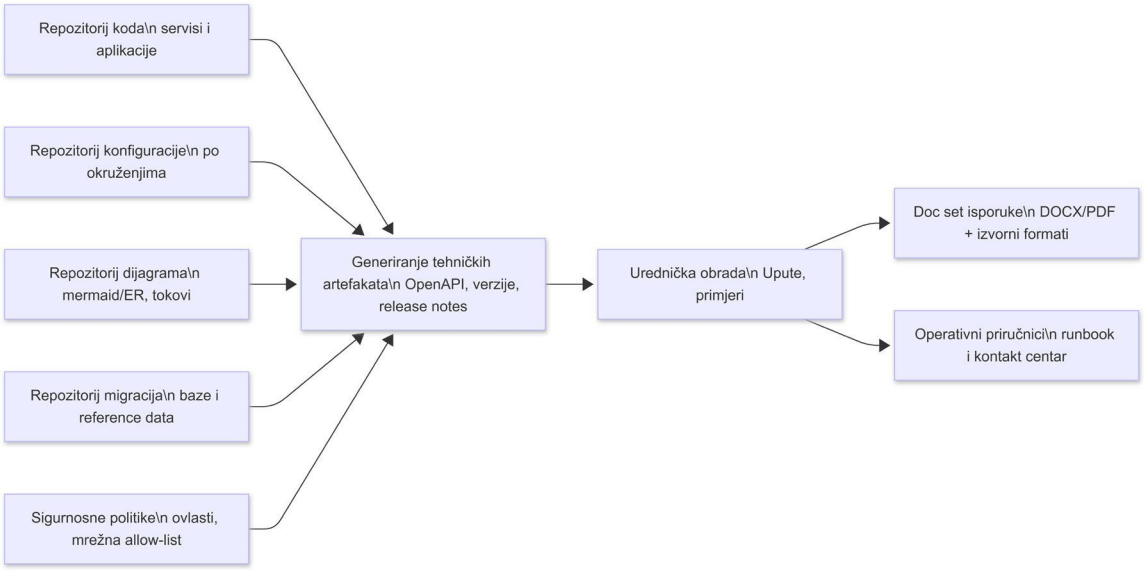
U praksi se izvori istine raspodjeljuju po domenama: arhitekturni dijagrami i modeli (npr. ER dijagrami i tokovi) održavaju se u verzioniranim izvornim datotekama; API ugovori održavaju se kao OpenAPI specifikacije; konfiguracijski parametri održavaju se u repozitoriju konfiguracije po okruženjima; a sigurnosne postavke i pravila pristupa održavaju se kroz konfiguracijske politike (role mapping, dopušteni podskupovi podataka, mrežna allow-lista). Dokumenti se generiraju konsolidacijom tih izvora, uz uredničku obradu koja dodaje objašnjenja i operativne upute.

Dokumentacija mora imati jasno definiranu “razinu detalja” po publici. Korisničke upute moraju biti orijentirane na zadatke i procedure (što kliknuti, što očekivati, kako tumačiti

Financira
Europska unija
NextGenerationEU

status), dok tehnička dokumentacija mora biti orijentirana na konfiguraciju, integracije i održavanje (što instalirati, kako povezati, kako provjeriti rad). Sigurnosni dokumenti moraju biti orijentirani na postavke, nadzor i minimalnu dokazivost (audit događaji, osnovni izvještaji), bez uvođenja složenih evidencija.

Za upravljanje time da dokumenti ostanu ažurni, svaki dokument mora imati definiran “okidač ažuriranja”. Okidač nije apstraktan, nego konkretan: promjena konfiguracije integracije, promjena sheme baze, promjena uloga i ovlasti ili promjena sučelja. Takav pristup osigurava da dokumentacija nije “jednokratna isporuka”, nego dio redovnog ciklusa isporuke i održavanja.



Slika 29. Načela izrade dokumentacije

9.2. Verzioniranje dokumentacije i povezivanje s izdanjima sustava

Svaki dokument mora biti verzioniran i povezan s izdanjem sustava na način da je u svakom trenutku moguće utvrditi: koja dokumentacija vrijedi za koju verziju aplikacije i konfiguracije. To se ostvaruje kroz “manifest izdanja” koji navodi verzije ključnih modula (eADR, integracije, analitika) i verzije konfiguracijskih paketa, a dokumentacija se isporučuje kao sastavni dio istog izdanja.

Verzioniranje dokumentacije mora biti usklađeno s načinom isporuke: dokumenti se ne smiju ručno preimenovati ili držati u više kopija po mapama bez kontrole, nego se za svako izdanje isporučuje jedinstveni paket dokumentacije s jasnim oznakama. U paket se uključuju i “release notes” u kojima se opisuje što je promijenjeno u odnosu na prethodno izdanje, uz fokus na promjene koje utječu na korisnike i administraciju (npr. novi ekran u AAP-u, promjena pravila validacije DG seta, promjena integracijskog endpointa).

Povezivanje dokumentacije s konfiguracijom je posebno važno zato što se sustav izvodi onpremise i jer okruženja mogu imati različite parametre (TEST/UAT/PROD), iako se aplikacijski artefakti nastoje držati nepromjenjivima. Dokumentacija mora jasno razlikovati:

Financira
Europska unija
NextGenerationEU

što je opće pravilo rada sustava (vrijedi za sva okruženja), a što je “parametar okruženja” (npr. URL-ovi, certifikati, rasporedi batch obrada) koji se vodi u konfiguracijskom repozitoriju i u dokumentima se prikazuje kao kontrolirani popis za konkretno okruženje.

Kako bi održavanje ostalo jednostavno, dokumentacija mora koristiti dosljedan model označavanja promjena: promjene koje utječu na postupanje na terenu (nadzor i prikaz podataka) moraju biti jasno istaknute, promjene koje utječu na instalaciju i konfiguraciju moraju biti grupirane u “instalacijske napomene”, a promjene koje utječu na sigurnost moraju biti grupirane u “sigurnosne napomene”. Time se omogućuje da različite ciljne skupine brzo pronađu relevantne promjene bez pretraživanja kroz sve dokumente.

9.3. Skup obveznih dokumenata i kriteriji potpunosti dokumentacije

Skup obveznih dokumenata mora biti definiran kao minimalan, ali potpun paket koji pokriva: pravnu i licencnu osnovu, rad korisnika, rad administratora, instalaciju i konfiguraciju, sigurnosne postavke, kontakt centar, integracije, te analitiku i izvještavanje. Paket mora biti dovoljno precizan da omogućuje rad sustava i nakon završetka projekta, bez potrebe za dodatnim “usmenim znanjem” ili ad-hoc priručnicima.

Kriteriji potpunosti dokumentacije moraju biti operativni, ne apstraktni. Dokumentacija je potpuna kada se iz nje može: instalirati sustav u ciljnom on-premise okruženju, konfigurirati integracije i sigurnosne postavke, provesti osnovne validacije rada, te provesti ključne poslovne postupke (nadzor eFTI/DG i eADR provjere). Ako dokument ne omogućava izvođenje postupka bez dodatnih konzultacija, smatra se nepotpunim.

Dokumentacija mora biti strukturirana tako da je moguće korištenje po ulogama i po zadacima. Korisnik na terenu ne smije morati čitati tehničku arhitekturu da bi proveo kontrolu, dok administrator ne smije tražiti konfiguracijske parametre kroz korisničke upute. Zbog toga se dokumenti moraju jasno razdvojiti, a preklapanja se svesti na minimalne definicije pojmova (rječnik) i zajedničke reference (npr. popis statusa i osnovnih šifrarnika).

Minimalni obvezni skup dokumenata za isporuku mora uključiti sljedeće vrste, pri čemu svaki dokument ima svoju ciljnu publiku i svrhu:

- **Uvjeti korištenja i licencna dokumentacija:** definira prava korištenja, opseg licence, prava naručitelja, podržane instalacije i ograničenja, uključujući treće komponente i njihove licence.
- **Korisničke upute:** odvojene upute za ključne uloge (nadzor/AAP, operateri eADR registara, učilišta i ispitni centri, tijela izdavatelji), s postupcima i primjerima.
- **Administratorske upute i operativni priručnik:** postavljanje okruženja, upravljanje pristupima i ulogama, nadzor rada, postupanje kod grešaka, sigurnosne kopije i osnovni DR postupci.

Financira Europska unija
NextGenerationEU

- **Upute za instalaciju i konfiguraciju:** koraci instalacije u on-premise virtualiziranom okruženju, mrežna segmentacija, preduvjeti, konfiguracijski parametri, inicijalizacija i validacija.
- **Sigurnosne postavke:** konfiguracija sigurnosnih kontrola (TLS, certifikati, ovlasti, audit), osnovni sigurnosni nadzor i minimalne provjere sukladno NIS2.
- **Dokumentacija integracija i sučelja:** katalog sučelja, format poruka/API, verzije, scenariji grešaka, korelacijski identifikatori i minimalne validacije.
- **Dokumentacija analitike i izvještavanja (AFFINIS):** dnevne obrade, strukture ulaza, osnovni izvještaji i provjere konzistentnosti.
- **Upute za kontakt centar:** trijaža i rješavanje najčešćih problema, prikupljanje potrebnih podataka i eskalacija.

9.4. Uvjeti korištenja i licencna dokumentacija

Licencna dokumentacija mora biti izrađena tako da jasno definira pravni okvir korištenja rješenja u državnom on-premise okruženju te da eliminira operativne nejasnoće oko toga što je dopušteno instalirati, u kojem opsegu i pod kojim uvjetima. Dokument se mora koristiti kao praktična osnova za nabavu i kasnije operativno korištenje, a ne kao općenita pravna izjava bez tehničke primjenjivosti.

Sadržaj licencne dokumentacije mora eksplicitno pokriti cjelokupni modularni sustav: eADR, integracijski sloj (uključivo eDelivery/AS4), te analitički sloj (AFFINIS nadogradnje i pripadajući moduli). Za svaki modul mora biti jasno navedeno što je isporučeno (komponente, servisi, baze, konektori), kako se licencira (po instanci, po procesoru, po korisniku ili drugo) i što se smatra “produkcijskim okruženjem” u kontekstu primarne i DR lokacije.

Licencna dokumentacija mora uključiti i pregled komponenti trećih strana (uključujući opensource) s pripadajućim licencama i obvezama, kako bi naručitelj imao transparentan uvid u pravne i operativne implikacije. Ovaj dio mora biti napisan jasno, s naglaskom na to što naručitelj treba napraviti ili poštovati u svakodnevnom radu (npr. čuvanje licence datoteka, ograničenja redistribucije, uvjeti korištenja biblioteka). Cilj nije pravna rasprava, nego operativna jasnoća.

Dokument mora propisati i način dokazivanja valjanosti licence u produkciji: gdje se pohranjuju licencni ključevi ili datoteke, tko ima pravo pristupa, kako se radi obnova ili rotacija, te što se događa u slučaju isteka ili promjene infrastrukture (npr. zamjena VM-a). Na taj način se sprječavaju incidenti gdje sustav prestane raditi zbog licencne nejasnoće ili pogrešne operativne procedure.

9.5. Korisničke upute i operativne procedure po ulogama

Korisničke upute moraju biti napisane kao upute “po zadatku”, s jasnim koracima i očekivanim rezultatima, te moraju pokrivati sve ključne procese koje sustav podržava: nadzor eFTI

Financira
Europska unija
NextGenerationEU

pošiljaka i DG seta kroz AAP, upravljanje registrima u eADR sustavu, upravljanje osposobljavanjem (programi, tečajevi, ispiti, potvrde), te upravljanje dopuštenjima i obuhvatom dopuštenja. Upute moraju dosljedno koristiti nazive entiteta i statusa koji se pojavljuju u aplikaciji (npr. statusi pošiljke, operacije, ispita, potvrde i dopuštenja), kako bi korisnik mogao izravno mapirati dokument na ekran.

Za AAP (nadzor) korisničke upute moraju sadržavati postupke: prijava korisnika, iniciranje provjere (po registraciji vozila, referenci pošiljke ili drugom identificirajućem podatku), pregled metapodataka, dohvat DG seta (selektivno) i dohvat punog sadržaja kada je potrebno, te evidentiranje ishoda nadzora. Posebno moraju biti opisane situacije degradiranog rada (npr. platforma nedostupna) tako da korisnik zna što sustav može i što ne može u tom trenutku, te kako postupiti bez improvizacije.

Za eADR upute moraju biti organizirane po operativnim ulogama, jer su procesi različiti: operater registra (subjekti, vozila, osobe, lokacije), operater učilišta (tečajevi i ispiti), ispitivač (unos i potvrda rezultata), te tijelo izdavatelj (izdavanje, produljenje i opoziv dopuštenja). Svaka uloga mora imati jasno objašnjene granice ovlasti i tipične radne procedure, uključujući provjere prije spremanja (validacije) i objašnjenja poruka sustava u slučaju pogrešaka.

Upute moraju uključiti i dio “najčešća pitanja i problemi” koji je usmjeren na rad korisnika, a ne na tehničko održavanje. Ovaj dio mora obuhvatiti situacije koje se realno događaju: nevidljiva pošiljka u sustavu, nevaljani DG podaci, istekla potvrda osposobljenosti, neusklađenost dopuštenja s UN brojem, te što učiniti kada sustav pokaže da podaci nisu dostupni. Time se smanjuje opterećenje kontakt centra i administracije, jer korisnik dobiva jasne smjernice za postupanje.

9.6. Administratorske upute i operativni priručnik za održavanje

Administratorske upute moraju objediniti sve postupke potrebne za stabilan rad sustava u produkciji, uz fokus na jednostavne i ponovljive radnje. Dokument mora jasno razlikovati administraciju sustava (konfiguracije, integracije, certifikati, uloge, batch) od administracije podataka (koja je u domeni ovlaštenih operatera kroz aplikacijske module). Administrator mora imati jasne procedure za ono što stvarno radi: održava dostupnost i ispravnost, a ne ručno “popravlja” poslovne zapise.

Operativni priručnik mora sadržavati procedure za svakodnevni rad: provjera statusa servisa, provjera integracija, pretraživanje logova, praćenje osnovnih metrika, postupanje kod najčešćih grešaka i kontrolirano ponovno pokretanje servisa. Posebno moraju biti opisane procedure povezane s integracijama (eDelivery/AS4, SOTAH, AFFINIS i sustavi nadležnih tijela) jer su to točke gdje se u praksi najčešće javljaju pogreške koje korisnici prijavljuju kao “sustav ne radi”.

Upute moraju pokriti upravljanje identitetima i ulogama u smislu konfiguracije: kako se mapiraju uloge iz autentifikacijskog sustava na aplikacijske ovlasti, kako se provjerava da

Financira
Europska unija
NextGenerationEU

korisnik ima očekivana prava, te kako se brzo onemogućava pristup u slučaju incidenta. Ovdje je nužno opisati i audit trag administrativnih promjena: koje promjene se bilježe, gdje su vidljive i kako se iz njih rekonstruira što je promijenjeno.

Operativni priručnik mora uključiti i minimalne procedure za sigurnosne kopije i oporavak: kako provjeriti da su kopije uspješno izrađene, kako provesti test povrata na testnu instancu, te kako provesti failover osnovnih komponenti prema definiranom modelu primarne i DR lokacije. Ove procedure moraju biti pisane kao konkretni koraci, s jasnim očekivanim ishodima i "točkama provjere" koje administrator potvrđuje nakon izvođenja.

9.7. Upute za instalaciju, konfiguraciju i nadogradnje u on-premise okruženju

Upute za instalaciju i konfiguraciju moraju omogućiti da se sustav pouzdano implementira u ciljnom on-premise okruženju AKD podatkovnog centra, uključujući primarnu i DR lokaciju. Dokument mora biti praktičan: mora navesti preduvjete (virtualizacijska infrastruktura, mrežne zone, baze, storage, certifikati), korake instalacije po komponentama, te obvezne validacije nakon instalacije (health check, provjera pristupa, probni dohvat metapodataka, probni zapis nadzora).

Konfiguracijski dio mora razlikovati tri skupine: konfiguracije bez tajni (npr. endpointi, portovi, naziv okruženja), tajne i ključevi (npr. certifikati za TLS i AS4, tajne za baze i integracije) te operativni parametri (npr. pragovi timeouta, rasporedi batch obrada, retencija logova). Upute moraju jasno navesti gdje se koja vrsta konfiguracije održava i kako se primjenjuje, tako da se izbjegne ručno uređivanje konfiguracijskih datoteka na produkcijskim poslužiteljima.

Nadogradnje moraju biti opisane kao kontrolirani postupak: priprema izdanja, primjena migracija baze (gdje je potrebno), isporuka aplikacijskih artefakata, primjena konfiguracijskih promjena, te validacija kroz minimalni set testnih scenarija. Posebno je važno da dokument sadrži i postupak povratka (rollback) u slučaju neuspjeha, pri čemu se rollback definira kao povrat aplikacijskih artefakata i konfiguracije, a za baze se koristi pristup kompatibilnih migracija i sigurnosnih kopija prema pravilima sustava.

Upute moraju sadržavati i "kontrolni popis" za instalaciju i nadogradnju koji ovlaštena osoba može pratiti korak po korak. Kontrolni popis mora biti kratak i fokusiran na ključne točke: dostupnost servisa, dostupnost baza, uspješna autentifikacija, uspješna integracija prema eFTI platformi/simulatoru, uspješna integracija prema SOTAH, te uspješan završetak batch obrade u analitici kada je primjenjivo.

9.8. Sigurnosne postavke i dokumentacija sukladno NIS2

Dokument "Sigurnosne postavke" mora objediniti sve konfiguracije i operativne postupke koji osiguravaju da sustav radi u skladu s traženim sigurnosnim načelima: kontrola pristupa, kriptozaštita komunikacije, upravljanje tajnama i certifikatima, zapisnici događaja te osnovni

Financira
Europska unija
NextGenerationEU

nadzor sigurnosnih događaja. Dokument mora biti praktičan i usmjeren na postavke koje se stvarno primjenjuju, bez opsežnih teoretskih razmatranja.

Sigurnosne postavke moraju obuhvatiti minimalno: konfiguraciju TLS-a i certifikata, konfiguraciju eDelivery/AS4 kriptozaštite poruka, pravila za pristup mrežnim zonama (allowlista), upravljanje privilegiranim računima, te audit događaje koji se moraju bilježiti. Posebno se mora opisati kako se postiže sljedivost: koji korelacijski identifikatori se koriste, gdje se zapisuju i kako se u logovima pronalazi događaj povezan s konkretnom kontrolom na terenu.

Dokument mora sadržavati i minimalne postupke za sigurnosne incidente u smislu operativne provedivosti: kako identificirati sumnjive događaje u logovima, kako privremeno ograničiti pristup kompromitiranom računu, kako rotirati tajne i certifikate, te kako provesti osnovnu provjeru integriteta sustava nakon incidenta. Ove procedure moraju biti usklađene s općim postupkom upravljanja incidentima i rokovima izvještavanja, ali prikazane kao konkretni koraci za administratora.

Sigurnosna dokumentacija mora biti povezana s uputama za kontakt centar i s administratorskim runbookom, tako da se incidenti rješavaju kroz standardni proces, a ne adhoc. Time se održavanje sustava pojednostavljuje i osigurava da se minimalne NIS2 obveze mogu ispuniti bez složenih dodatnih evidencija, oslanjajući se na audit trag i osnovne izvještaje iz log-kolektora i monitoringa.

9.9. Dokumentacija integracija i sučelja (interfacing)

Dokumentacija integracija mora biti izrađena kao jedan konzistentan skup koji sadrži: katalog sučelja, opis tokova, tehničke ugovore (format poruka ili API), sigurnosne mehanizme, pravila validacije i rukovanje pogreškama. Ovaj dokument mora biti glavni operativni alat za integracijsku konfiguraciju i za rješavanje integracijskih problema, jer se najveći dio operativnih poteškoća u praksi manifestira kroz integracije (nedostupnost, promjene certifikata, promjene endpointa, nevaljane poruke).

Za eFTI sučelja mora biti jasno dokumentirano: metapodatkovni tok (push), dohvat podataka (selective/full), obvezni identifikatori (npr. eftiTransportId i eftiConsignmentId), verzije datasetova te minimalne validacije DG seta. Dokument mora navesti i očekivano ponašanje u slučaju degradacije (timeout, nedostupnost platforme) te kako se to stanje prikazuje korisniku u AAP-u i kako se bilježi u audit zapisima.

Za SOTAH i AFFINIS sučelja dokumentacija mora biti usmjerena na opseg koji sustav stvarno koristi: dohvat tahografskih sažetaka i indikatora po potrebi, te batch tokove prema analitici. Potrebno je jasno dokumentirati mapiranje identifikatora (vozilo, tahograf, vozač), vremenski opseg dohvaćanja, te što se smatra uspješnim i neuspješnim pozivom, kako bi operativno održavanje moglo brzo izolirati problem bez dubinske analize.

Financira
Europska unija
NextGenerationEU

Dokument mora uključivati i standardizirani način praćenja integracija: koje metrike se prate (broj poziva, greške, latencije), gdje se gledaju logovi, te koji se podaci moraju prikupiti kada se prijavi incident (korelacijski ID, timestamp, identifikator pošiljke/operacije). Time se izbjegava da svaka integracija "ima svoje pravilo", što otežava održavanje i povećava broj eskalacija.

9.10. Dokumentacija analitike i izvještavanja (AFFINIS)

Dokumentacija analitike mora omogućiti da se AFFINIS nadogradnje i dnevne obrade održavaju stabilno i predvidljivo, bez potrebe za složenim operativnim zahvatima. Dokument mora opisati što se analitički preuzima iz operativnog sustava eADR, kojim ritmom (dnevno), te koje minimalne provjere konzistentnosti se provode nakon obrade.

Opis analitičkih tokova mora uključiti: strukture ulaznih skupova podataka, osnovna pravila transformacije (npr. mapiranje šifrarnika i statusa), te način na koji se u analitici održava jedinstvenost dimenzija (vozila, osobe, subjekti). Naglasak mora biti na praktičnoj održivosti: kako prepoznati da se u analitici stvorio duplikat, kako provjeriti da su svi zapisi od prethodnog dana učitani, te kako ponoviti dnevnu obradu u slučaju tehničkog prekida.

Dokument mora definirati minimalni skup izvještaja i pokazatelja koji se smatraju obveznima za osnovno izvještavanje: volumeni provjera, volumeni pošiljaka s DG setom, ishodi nadzora, osnovne metrike integracija i opterećenja (npr. broj dohvaćanja payload-a), te osnovni sigurnosni pokazatelji (npr. neuspjele prijave i pokušaji pristupa bez ovlasti). Cilj je da se izvještavanje zadrži "bazično" i održivo, bez uvođenja velikog broja specijaliziranih izvještaja koji zahtijevaju stalno održavanje.

Dokumentacija mora sadržavati i operativne upute za batch: gdje se vidi status obrade, gdje se nalazi log, koji je očekivani prozor izvođenja i što je minimalni postupak ako obrada ne završi uspješno. Time se osigurava da analitički sloj bude pouzdan i da se može održavati u redovnom režimu rada on-premise podatkovnog centra.

9.11. Upute za kontakt centar i podršku korisnicima

Upute za kontakt centar moraju biti usmjerene na brzo prepoznavanje problema, prikupljanje minimalno potrebnih informacija i usmjeravanje na ispravnu razinu rješavanja. Dokument ne smije postati tehnički priručnik administratora, ali mora sadržavati dovoljno informacija da prva linija podrške može razlikovati: problem autentifikacije, problem ovlasti, problem dostupnosti integracije, te problem vezan uz konkretne podatke (npr. nevaljan DG set ili istekla potvrda osposobljenosti).

Upute moraju sadržavati standardni obrazac prijave incidenta koji je prilagođen sustavu: korisnički identitet/uloga, vrijeme događaja, identifikator pošiljke/operacije (ako postoji), registracija vozila, opis poruke na ekranu i, gdje je moguće, korelacijski identifikator koji sustav

Financira
Europska unija
NextGenerationEU

prikazuje ili koji se može dobiti iz audit zapisa. Ovaj obrazac mora biti kratak i operativan, jer je cilj ubrzati rješavanje bez dodatne komunikacije.

Dokument mora uključiti "katalog najčešćih problema" s jasnim uputama što se prvo provjerava i kada se eskalira. Katalog mora obuhvatiti tipične situacije: korisnik se ne može prijaviti (NIAS problem ili uloga nije dodijeljena), ne vidi pošiljku (metapodaci nisu dostavljeni), ne može dohvatiti DG set (platforma nedostupna ili nevaljan dataset), dobiva poruku o nedostatku ovlasti, te greške u unosu eADR procesa (validacije, statusi). Za svaku situaciju mora postojati preporučena radnja i kriterij eskalacije.

Upute moraju jasno definirati kome se eskalira u okviru predviđenih dionika projekta: prema administratorskom timu AKD/MMPI i prema ugovorenoj tehničkoj podršci izvođača, bez uključivanja dodatnih vanjskih subjekata. Eskalacija mora biti jednostavna: što poslati, u kojem formatu, te koji je minimalni skup informacija bez kojeg se eskalacija ne prihvaća, kako bi se izbjeglo "pogađanje" i nepotrebni povratni upiti.

10. Referentni izvori i standardi za provedbu projekta

Referentni izvori i standardi predstavljaju obveznu osnovu za projektiranje, izradu, integraciju, sigurnost, testiranje i operativno održavanje produkcijskog rješenja eADR. U ovom projektu referentni izvori nisu samo "literatura", nego skup dokumenata i standarda prema kojima se izravno projektira funkcionalnost (npr. obvezni informativni skupovi podataka za eFTI, DG informativni set za opasne tvari, zahtjevi za interoperabilnost), definira način razmjene i sučelja (integracijski ugovori i formati), te osigurava usklađenost s obvezama informacijske sigurnosti i zaštite podataka.

Ključna dokumentacija definira okvir **razvoja i implementacije**, očekivani opseg isporuke, obvezne dijelove tehničke dokumentacije te kriterije prihvatljivosti rješenja u državnom onpremise okruženju. Svi standardi i izvori navedeni u nastavku primjenjuju se na način koji je usklađen s tim pozivom i projektnim pretpostavkama.

Dodatni primarni projektni izvor za dimenzioniranje i očekivani operativni režim analitičkog sloja je dokument **Procjena analitičkih kapaciteta i nadogradnje AFFINIS-a za eADR.docx**. Ovaj dokument se koristi kao referenca za organizaciju analitičkih tokova, ulazne podatkovne skupove, osnovno izvještavanje i operativnu održivost analitike, uz usklađenje s ostatkom ciljnih komponenti eADR sustava.

Standardi i izvori u ovom poglavlju navedeni su s jasnom namjenom: za svaki skup standarda definira se **što pokrivaju u projektu**, **na kojoj razini se primjenjuju** (poslovna pravila, podatkovni model, integracije, sigurnost, testiranje) te **koji su minimalni rezultati** koji se moraju vidjeti u isporuci (npr. sučelja koja prate eFTI specifikacije, sigurnosne postavke koje podržavaju NIS2 obveze, dokumentacija i testni scenariji koji su ponovljivi).

Financira
Europska unija
NextGenerationEU

10.1. Hijerarhija referentnih izvora i pravila primjene

Hijerarhija referentnih izvora u projektu mora biti jednoznačna kako bi se spriječila situacija da različiti timovi implementiraju različita tumačenja istih obveza. Najvišu razinu čine **obvezujući pravni akti EU i Republike Hrvatske** te obvezni međunarodni sporazumi koji su primjenjivi na cestovni prijevoz opasnih tvari. Sljedeću razinu čine **tehničke specifikacije i provedbeni dokumenti** koji operacionaliziraju pravila (npr. eFTI specifikacije, datasetovi, strukture podataka i tehničke smjernice interoperabilnosti). Treću razinu čine **nacionalne i organizacijske smjernice** (AKD/MMPI i postojeći nacionalni sustavi) koje definiraju operativnu provedbu u onpremise okruženju.

U slučaju kolizije izvora (npr. različito nazivlje ili različita interpretacija podatkovnog elementa), pravilo je da se prioritet daje: (1) obvezujućem pravnom aktu, zatim (2) provedbenoj eFTI specifikaciji i službenim kodnim listama, a zatim (3) projektnim odlukama dokumentiranim u službenoj projektnoj dokumentaciji (uključujući odobrene specifikacije sučelja i podatkovne modele). Ovakav pristup osigurava da sustav bude i regulatorno usklađen i tehnički interoperabilan.

Primjena standarda mora biti **svrsishodna i minimalno potrebna**, bez uvođenja standarda koji bi povećali složenost održavanja ili zahtijevali angažman dodatnih vanjskih dionika. Standardi se koriste kao “ugovor” o interoperabilnosti i kvaliteti, ali se implementacija vodi načelom jednostavne operativnosti: jasna sučelja, jasni format podataka, jasni testni scenariji i osnovno izvještavanje bez dodatnih složenih evidencija.

Za potrebe projekta svaki referentni izvor mora biti mapiran na isporučive artefakte. To mapiranje se održava kroz jedinstveni popis (katalog) u kojem se jasno navodi: koji dokument/standard utječe na koji modul (eADR, integracije, analitika, sigurnost), te u kojem se dijelu dokumentacije rješenja to vidi (npr. u tehničkoj specifikaciji sučelja, u podatkovnom modelu, u sigurnosnim postavkama ili u testnim scenarijima).

10.2. EU regulatorni okvir relevantan za eFTI i digitalnu razmjenu podataka u prijevozu

Temeljni regulatorni okvir za eFTI proizlazi iz EU pravila kojima se uređuje elektronička dostava i uporaba informacija u teretnom prijevozu te interoperabilnost između gospodarskih subjekata, nadležnih tijela i platformi. U okviru ovog projekta eFTI regulatorni okvir se operacionalizira kroz zahtjeve nacionalnog eFTI čvora/gatewaya, AAP aplikacije za službenike te kroz sučelja prema eFTI platformama, pri čemu je obvezno poštivati obvezne informativne skupove podataka i pravila dostupnosti, selektivnog dohvaćanja i dokazivosti pristupa.

U provedbi projekta posebno je važna činjenica da eADR sustav mora implementirati eFTI standard u dijelu podataka o opasnim tvarima (DG informativni set), jer eADR generira i obrađuje podatke koji ulaze u obvezni informativni set za DG u eFTI specifikacijama.

Financira
Europska unija
NextGenerationEU

EU regulatorni okvir obuhvaća i pravila o elektroničkoj identifikaciji i pouzdanim uslugama (u dijelu gdje se oslanjamo na nacionalne mehanizme autentifikacije te gdje se koristi potpisivanje i dokazivanje integriteta poruka/dokumenata). U praktičnom smislu, to se u isporuci mora vidjeti kroz dosljedno provođenje autentifikacije, autorizacije i dokazivosti pristupa eFTI podacima i dokumentima, bez uvođenja dodatnih identitetskih sustava izvan predviđenog nacionalnog okvira.

U primjeni EU regulatornog okvira u ovom projektu vrijedi načelo fokusiranja na nacionalni opseg: iako eFTI okvir ima prekograničnu dimenziju, projektni opseg je cestovni promet unutar Republike Hrvatske. U dokumentaciji i implementaciji standardi i pravila eFTI-ja se primjenjuju onoliko koliko je nužno za interoperabilnost i usklađenost, bez širenja funkcionalnosti na prekogranične procese koji nisu dio opsega.

10.3. EU i međunarodni okvir za opasne tvari u cestovnom prijevozu i eADR domenu.

Za eADR domenu temeljni referentni okvir čini **ADR** (Europski sporazum o međunarodnom cestovnom prijevozu opasnih tvari), koji definira klasifikaciju, označavanje, dokumentaciju, ograničenja i uvjete prijevoza opasnih tvari. Iako je projektni opseg nacionalan, pravila ADR-a su relevantna za sadržaj podataka (npr. UN broj, ADR razred, ambalažna skupina, ograničenja tunela) i za provjere koje nadležna tijela provode u stvarnom postupku nadzora.

U provedbi eADR sustava ADR pravila se ne implementiraju kao “tekstualni pravilnik” u aplikaciji, nego kao strukturirani skup podataka i validacija: obvezna polja DG seta, šifrarnici, logičke provjere (npr. konzistentnost razreda i klasifikacijskog koda), te prikaz sažetka koji je operativno primjenjiv tijekom kontrole. Ovaj pristup omogućuje da sustav bude upotrebljiv na terenu i da ne zahtijeva od korisnika “ručno tumačenje” podataka bez sustavne pomoći.

U domeni dokumentacije prijevoza relevantan je i okvir elektroničke dokumentacije (npr. eCMR) u mjeri u kojoj se koristi kao izvor ili prikaz transportne dokumentacije, ali u ovom projektu se integracija prema eCMR-u provodi kroz eFTI platforme i eFTI dohvat, bez izravnog povezivanja s velikim brojem pružatelja. Time se zadržava održivost rješenja i izbjegava uvođenje dodatnih integracijskih obveza.

Kako ADR okvir evoluira (a ažurira se periodično), projektna dokumentacija mora definirati postupak ažuriranja šifrarnika i pravila u eADR sustavu. U praksi to znači da se kodne liste i validacijska pravila održavaju kao verzionirani skupovi (reference data), a dokumentacija mora jasno navesti kako se nove verzije uvode i kako se osigurava da povijesni zapisi nadzora ostanu interpretabilni prema pravilima koja su vrijedila u trenutku događaja.

Financira
Europska unija
NextGenerationEU

10.4. Nacionalni regulatorni okvir Republike Hrvatske koji se primjenjuje na projekt

Nacionalni okvir čine zakoni i podzakonski akti Republike Hrvatske koji uređuju: cestovni prijevoz, prijevoz opasnih tvari, ovlasti i postupanje nadzornih tijela, te obradu i zaštitu podataka u državnim informacijskim sustavima. U provedbi projekta nacionalni propisi daju kontekst za to koje funkcije eADR mora podržati (npr. izdavanje i evidencija dopuštenja, evidencija osposobljavanja i potvrda, postupanje nadzora) i koje su minimalne informacije potrebne za zakonito postupanje.

Nacionalni okvir također određuje organizacijski kontekst sustava: gdje se sustav fizički i operativno nalazi (on-premise u AKD podatkovnom centru), tko su operativni korisnici, te koje se evidencije smatraju službenim. Dokumentacija i implementacija moraju biti usklađene s tim pravilima kako se ne bi stvarale paralelne evidencije ili procesi koji nisu usklađeni s nacionalnim postupanjima.

Za potrebe informacijske sigurnosti nacionalni okvir obuhvaća i propise koji prenose NIS2 obveze u nacionalni pravni sustav te relevantne zahtjeve državnih sustava za kategorizaciju, segmentaciju, upravljanje pristupima i evidentiranje događaja. U ovom poglavlju ti se propisi tretiraju kao referentni izvori, dok su konkretni zahtjevi i implementacijski obrasci obrađeni u poglavlju o NIS2 i sigurnosnom sloju.

U kontekstu elektroničke identifikacije i autentifikacije, nacionalni okvir uključuje pravila i tehničke uvjete korištenja nacionalnih usluga autentifikacije (eGrađanin/NIAS) i povezanih mehanizama identiteta. Implementacija sustava mora se osloniti na te mehanizme gdje je prikladno (korisnici nadležnih tijela, gospodarski subjekti, vozači, učilišta i ispitni centri), pri čemu se u dokumentaciji moraju jasno opisati ovisnosti, preduvjeti i način mapiranja uloga i ovlasti.

10.5. Standardi interoperabilnosti i razmjene: eFTI specifikacije, sučelja i format podataka

Interoperabilnost u ovom projektu temelji se na standardizaciji sučelja i podatkovnih ugovora, s naglaskom na to da nadležna tijela dobiju pouzdane podatke kroz AAP i Gate, a da gospodarski subjekti ne moraju implementirati niz različitih integracija prema državi. Referentni okvir za to su eFTI tehničke specifikacije, datasetovi i kodne liste, koji se u sustavu moraju odraziti kroz: definiciju metapodataka, selektivni dohvat, pun dohvat, te konzistentno mapiranje DG seta prema eADR modelu.

Za razmjenu poruka i integracije koje se oslanjaju na eDelivery, referentni standardi uključuju profilirane specifikacije razmjene poruka (AS4/ebMS), kriptozaštitu poruka, potvrde isporuke i pouzdanu razmjenu. U projektu je ključno da integracijski sloj bude provjerljiv i održiv: poruke moraju imati korelacijske identifikatore, mora postojati jasan katalog partnera i konfiguracija

Financira Europska unija
NextGenerationEU

certifikata, te moraju postojati standardizirani načini rukovanja greškama (npr. nevaljana poruka, nedostupan endpoint, neuspjela validacija potpisa).

Za API sučelja i internu razmjenu podataka referentni standardi su usmjereni na konzistentnost i dokumentiranost: definicija API-ja mora biti formalizirana (npr. OpenAPI), format razmjene mora biti jednoznačno definiran (JSON/XML prema dogovoru), te se mora provoditi verzioniranje sučelja kako bi sustav ostao nadogradiv bez prekida rada. Ovo se izravno odražava na tehničku dokumentaciju integracija i na testne scenarije koji potvrđuju kompatibilnost selektivnog i punog dohvaćanja.

U kontekstu eCMR i digitalne dokumentacije, referentni standardi i protokoli se koriste u mjeri u kojoj se dokumentacija prenosi ili referencira kroz eFTI platformu. Sustav mora biti sposoban prikazati strukturirane podatke i dokaz integriteta dokumenta (npr. potpis, hash ili drugi dokaz), ali bez preuzimanja uloge univerzalnog repozitorija dokumenata. Ovakav pristup zadržava fokus na eFTI interoperabilnosti i održivosti, a dokumentacija sučelja mora jasno navesti koje su varijante podržane i kako se njima upravlja.

- **eFTI specifikacije i datasetovi:** primjenjuju se za strukturu metapodataka, selektivni dohvat i DG informativni set; u isporuci moraju postojati validacije i mapiranja koja osiguravaju konzistentan prikaz u AAP-u.
- **eDelivery/AS4 profili:** primjenjuju se na pouzdanu razmjenu poruka i kriptozaštitu; u isporuci moraju postojati konfiguracije partnera, certifikati, potvrde isporuke i logovi s korelacijom.
- **OpenAPI i ugovori sučelja:** primjenjuju se na dokumentiranje i verzioniranje API-ja; u isporuci moraju postojati formalne specifikacije i testovi kompatibilnosti.
- **Standardi formatiranja poruka i kodiranja:** primjenjuju se na konzistentno kodiranje podataka (npr. UTF-8), datumsko-vremenske formate i identifikatore; u isporuci se mora vidjeti jednoznačno tumačenje i validacija.

10.6. Referentni standardi za informacijski sigurnosni okvir i zaštitu podataka

Referentni okvir informacijske sigurnosti u projektu proizlazi iz NIS2 i nacionalnih propisa, uz primjenu praktičnih standarda i smjernica koje omogućuju konzistentnu implementaciju bez nepotrebne operativne složenosti. U ovom poglavlju standardi se navode kao temelj za strukturiranje sigurnosnih postavki, upravljanje pristupima, evidentiranje događaja i minimalne provjere, dok su konkretne implementacijske mjere detaljno opisane u poglavlju posvećenom sigurnosnom sloju i NIS2 zahtjevima.

Za upravljanje sigurnošću i politikama uobičajeni referentni standardi uključuju ISO/IEC 27001 i ISO/IEC 27002 u smislu strukture kontrola i terminologije (upravljanje pristupom, kriptografija, operativna sigurnost, upravljanje incidentima). U ovom projektu ovi standardi se

Financira Europska unija NextGenerationEU

koriste kao okvir za strukturiranje dokumentacije i postupaka, a ne kao obveza uspostave složenog sustava upravljanja koji bi povećao opterećenje održavanja.

Za upravljanje incidentima i evidentiranje događaja relevantne su smjernice koje definiraju što se smatra sigurnosnim događajem, kako se klasificira i kako se izvještava, uz oslanjanje na logkolektor i osnovno izvještavanje. Cilj je da sustav "po dizajnu" proizvodi audit tragove potrebne za dokazivost (prijave, pristupi osjetljivim podacima, administrativne promjene) i da se iz njih može izvući minimalni set informacija za postupanje, bez dodatnih evidencija.

Za zaštitu osobnih podataka referentni okvir je GDPR i pripadajuća nacionalna provedbena pravila. U praksi to znači da se dokumentacija i implementacija oslanjaju na načela minimizacije, ograničenja svrhe, ograničenja pristupa i sljedivosti, što je posebno važno jer sustav obrađuje identifikatore osoba (npr. vozače) i podatke povezane s nadzorom. Referentni standardi se u ovom segmentu moraju odraziti na to da se u dokumentaciji jasno definira: tko ima pravo vidjeti koje podatke, u kojoj svrsi i kako se pristup evidentira.

- **NIS2 i nacionalni provedbeni propisi:** referentni su za obveze upravljanja rizicima, incidentima, kontinuitetom i izvještavanjem; u dokumentaciji se moraju vidjeti postupci i minimalni dokazni tragovi.
- **ISO/IEC 27001 i 27002:** referentni su za strukturiranje sigurnosnih postavki i politika; koriste se kao okvir, bez uvodenja dodatne operativne složenosti.
- **ISO/IEC 27035 (upravljanje incidentima) i srodne smjernice:** referentne su za konzistentan tok incidenta i prikupljanje informacija; u isporuci se moraju vidjeti jasne upute i logovi koji to podržavaju.
- **GDPR i nacionalna pravila zaštite podataka:** referentni su za obradu osobnih podataka i sljedivost pristupa; u isporuci se moraju vidjeti pravila pristupa, audit i minimalizacija podataka u integracijama.

10.7. Standardi za podatkovne modele, šifrarnike, kvalitetu podataka i semantiku

Podatkovni modeli u projektu moraju biti utemeljeni na standardiziranim pojmovima i šifrarnicima kako bi se osigurala interoperabilnost između eADR i integriranih sustava. Referentni izvori u ovom segmentu su eFTI datasetovi i kodne liste, ADR klasifikacijski elementi te nacionalni šifrarnici i evidencije kada su relevantni. U praksi to znači da se u podatkovnom modelu i u validacijama mora vidjeti jednoznačna semantika: što je pošiljka, što je operacija prijevoza, što je stavka opasne tvari, kako se bilježe pretovari, te kako se povezuju dozvole i osposobljenost s konkretnom operacijom i DG sadržajem.

Jedno od ključnih načela je odvajanje pojmova koji se u praksi često pogrešno izjednačavaju. Pošiljka (consignment) je poslovni entitet koji može biti pokriven s više operacija (npr. pretovar, promjena vozila), dok operacija prijevoza predstavlja konkretno izvršenje prijevoza s konkretnim vozilom i vozačem. Referentni standardi eFTI-ja i ADR-a zahtijevaju da se ova

Financira Europska unija
NextGenerationEU

razlika može pratiti u podacima jer se inače gubi sljedivost i onemogućuje korektna interpretacija nadzora.

Šifrarnici i kodne liste moraju biti održavani kao verzionirani skupovi referentnih podataka. To uključuje: tipove subjekata, statuse operacija i pošiljaka, vrste programa osposobljavanja, vrste dopuštenja, te ADR klasifikacijske elemente. Referentni izvori ovih šifrarnika moraju biti jasno navedeni u dokumentaciji, a postupak ažuriranja mora biti opisan tako da se može provesti unutar redovnog ciklusa nadogradnji bez ručnih intervencija na produkciji.

Kvaliteta podataka i validacije trebaju biti postavljene kao praktičan skup pravila koji sprječava najčešće greške, a ne kao složeni sustav nadzora kvalitete. U isporuci se to mora vidjeti kroz: validaciju obveznih polja DG seta, validaciju formata identifikatora, konzistentnost veza (npr. dozvola pokriva UN broj), te jasne poruke pogreške koje korisnik može razumjeti i ispraviti.

- **eFTI kodne liste i datasetovi:** referentni su za semantiku i strukturu podataka; u modelu se moraju vidjeti odgovarajući identifikatori i veze (npr. consignment, transport).
- **ADR klasifikacijski elementi:** referentni su za UN broj, razrede, ambalažne skupine i ograničenja; u modelu i validacijama moraju biti podržani kao strukturirani podaci.
- **Nacionalni šifrarnici procesa eADR:** referentni su za statuse tečaja, ispita, potvrde i dopuštenja; u modelu moraju biti jednoznačni i dosljedno korišteni kroz sve module.
- **Pravila kvalitete podataka:** referentna su za minimalne validacije i konzistentnost; u isporuci se moraju vidjeti kroz UI i API poruke greške te kroz testne scenarije.

10.8. Standardi za testiranje, validaciju i dokazivost usklađenosti.

Referentni standardi i prakse za testiranje u projektu služe tome da testni postupci budu ponovljivi, mjerljivi i dokazivi. U praksi, referentni okvir je definiran zahtjevima poziva i projektne dokumentacije za provedbu prihvatnog testiranja, uz oslanjanje na standardne obrasce testiranja: funkcionalni end-to-end testovi, integracijski testovi, sigurnosni testovi, performansni testovi te testovi oporavka i visoke raspoloživosti. Ovaj okvir mora biti dosljedan s ranije definiranim testnim scenarijima i validacijskim postupcima.

Za tehničku validaciju sučelja i ugovora referentni standard je formalna specifikacija sučelja (npr. OpenAPI) i automatizirana provjera ugovora, pri čemu se u projektu naglasak stavlja na praktično: provjeru da su sučelja kompatibilna između verzija i da se promjene ne uvode bez ažuriranja dokumentacije i testova. U testnim artefaktima mora biti vidljivo da se svaka ključna integracija može validirati bez ručnih improvizacija (npr. selektivni dohvat DG seta, dohvat tahografskog sažetka, batch ulaz u AFFINIS).

Za sigurnosno testiranje referentne su smjernice koje omogućuju osnovnu provjeru aplikacijskih i konfiguracijskih slabosti, uz fokus na provjerljive rezultate (izvještaj skeniranja, dokaz TLS konfiguracije, dokaz RBAC ograničenja). Ovdje se ne uvodi složen program

Financira Europska unija
NextGenerationEU

testiranja, nego minimalni skup provjera koji je dovoljno robustan za državne sustave i usklađen s NIS2 obvezama u smislu sposobnosti otkrivanja i odgovora na incidente.

Za testove kontinuiteta (backup/restore, failover) referentni okvir je projektna definicija ciljeva oporavka i operativnih procedura. Validacija se provodi kroz praktične scenarije oporavka i kroz zapis rezultata (vrijeme preuzimanja, dostupnost ključnih funkcija, konzistentnost podataka). U dokumentaciji testiranja mora biti jasno definirano što se smatra uspješnim oporavkom i koje se minimalne funkcije provjeravaju nakon failovera.

- **Standardizirani testni zapisi i dokazni paketi:** referentni su za prihvatno testiranje; u isporuci se mora vidjeti evidencija testova i dokaz (snimke, izvještaji, logovi).
- **Validacija ugovora sučelja:** referentna je za integracijska testiranja; u isporuci se mora vidjeti formalna specifikacija i testovi kompatibilnosti.
- **Osnovna sigurnosna provjera (DAST/SAST prema potrebi):** referentna je za dokaz minimalne sigurnosne higijene; u isporuci se mora vidjeti izvještaj i korekcije prije produkcije.
- **Testovi oporavka:** referentni su za dokaz kontinuiteta; u isporuci se mora vidjeti zapis izvedenih testova (backup/restore i failover) i rezultat u skladu s očekivanjima sustava.

10.9. Standardi i izvori za arhitekturu, modeliranje i tehničku dokumentaciju projekta.

Za arhitekturno modeliranje i dokumentiranje rješenja referentni standardi i prakse služe da se arhitektura, procesi i podatkovni modeli mogu razumjeti i održavati kroz životni ciklus sustava. U projektu se koriste praktični oblici modeliranja koji su razumljivi širokom krugu dionika: modeliranje podatkovnih odnosa (ER), modeliranje tokova integracije (sequence i data flow), te opis komponenti i zona (component i deployment prikazi). U dokumentaciji se ti modeli koriste kao dio tehničkih specifikacija, a ne kao “odvojeni crteži” bez veze s implementacijom.

Referentni izvori za arhitekturu i dizajn uključuju projektnu dokumentaciju isporučenu uz poziv (uključujući očekivane produkcijske komponente, on-premise pretpostavke, sigurnosne i operativne zahtjeve) te dokument Procjena analitičkih kapaciteta i nadogradnje AFFINIS-a, koji definira analitičke tokove i očekivanja u dijelu izvještavanja. Ovi izvori se koriste za oblikovanje “ciljne arhitekture” i za definiranje minimalno potrebnih komponenti bez uvođenja dodatnih tehnologija ili dodatnih organizacijskih ovisnosti.

U dijelu tehničke dokumentacije referentni standard je struktura dokumentacije koja omogućuje operativnu provedbu: instalacija i konfiguracija, integracijska sučelja, sigurnosne postavke, operativni priručnik i upute za korisnike. Dokumentacija mora biti održiva, verzionirana i povezana s izdanjima sustava, što se u praksi postiže povezivanjem dokumentacije s repozitorijima specifikacija i konfiguracije te održavanjem kataloga sučelja, šifrarnika i konfiguracijskih parametara.

Financira
Europska unija
NextGenerationEU

Dodatno, referentni izvor za dosljednost terminologije je projektni rječnik pojmova koji mora uskladiti eFTI nazivlje (npr. transport, consignment, consignment item) s eADR nazivljem (npr. prijevozna operacija, pošiljka, DG stavka) i nacionalnim pojmovima postupanja. Ovaj rječnik je ključan da dokumentacija, korisničko sučelje i integracijske specifikacije koriste iste pojmove i da se izbjegnu pogrešna tumačenja u stvarnom radu.

11. Zahtjevi za edukaciju i plan edukacije djelatnika AKDa

Edukacija je sastavni dio isporuke produkcijskog rješenja i usmjerena je na osposobljavanje djelatnika AKD-a koji će sustav operativno voditi, administrirati i pružati podršku korisnicima. Edukacija mora omogućiti da AKD samostalno upravlja aplikacijskim modulima eADR sustava (registri, osposobljavanje, dopuštenja), prati integracije, provodi osnovne operativne provjere i izvještavanje, te postupa u slučaju uobičajenih poteškoća (npr. nedostupnost integracije, poruke validacije, ograničenja ovlasti).

Edukacija se provodi tako da izravno podržava procese i modele opisane u poglavlju 5. (arhitektura) i validacijske scenarije iz poglavlja 8. (testiranje), bez uvođenja novih procesa ili dodatnih organizacijskih ovisnosti.

Opseg edukacije u okviru projekta ograničen je na uloge i aktivnosti koje obavlja AKD (operativno upravljanje sustavom, aplikativna administracija, integracije i analitika, kontakt centar i prva linija podrške). Edukacija krajnjih korisnika izvan AKD-a (npr. nadzorna tijela, učilišta, ispitni centri i tijela koja izdaju dopuštenja) nije predmet isporuke ovog projekta; eventualne obuke tih korisnika AKD može provoditi naknadno koristeći isporučene materijale i provedeni prijenos znanja.

Edukacija mora biti održiva nakon završetka projekta, bez stalne potrebe za angažmanom izvođača. To se postiže prijenosom znanja na superkorisnike u AKD-u, standardiziranim i verzioniranim materijalima koji se ažuriraju uz izdanja sustava, te jasno definiranim radnim procedurama za administratore i kontakt centar koje se koriste kao dnevni priručnik za rad..

11.1. Ciljne skupine, uloge i opseg edukacije

Ciljne skupine edukacije definiraju se prema stvarnim ulogama djelatnika AKD-a u sustavu i prema odgovornostima u operativnom upravljanju eADR rješenjem. Edukacija mora biti usklađena s modelom autentifikacije i ovlasti te s principom najmanjih privilegija: mora jasno objasniti što svaka uloga smije, a što ne smije raditi, i kako sustav komunicira ta ograničenja kroz poruke sustava i audit trag.

Financira Europska unija
NextGenerationEU

U operativnom smislu, opseg edukacije pokriva aktivnosti koje AKD provodi u svakodnevnom radu i podrški: aplikativna administracija i održavanje podataka u eADR modulima (registri, osposobljavanje i dopuštenja), podrška funkcionalnostima nadzora kroz pregled i tumačenje poruka sustava, praćenje i osnovna dijagnostika integracijskih tokova, te operativni analitički uvidi i osnovno izvještavanje u opsegu predviđenom ovim projektom.

Eksplicitno je izvan opsega edukacije: upravljanje internim sustavima gospodarskih subjekata, administracija eFTI platformi koje nisu u domeni projekta, te edukacija krajnjih korisnika izvan AKD-a (nadzorna tijela, učilišta, ispitni centri i tijela koja izdaju dopuštenja). Za takve korisnike AKD može naknadno organizirati obuku koristeći isporučene materijale.

Edukacija se organizira za sljedeće ciljane skupine unutar AKD-a, pri čemu svaka skupina dobiva prilagođen sadržaj i praktične vježbe:

- Administratori sustava (AKD): operativno održavanje servisa u virtualiziranom okruženju, sigurnosne postavke, certifikati, sigurnosne kopije i povrat, osnovni postupci oporavka, pregled logova i nadzor rada.
- Aplikativni operateri (AKD): administracija eADR modula (registri, osposobljavanje, dopuštenja), validacije, statusi i korekcije uz audit trag, obrada iznimki i podrška poslovnim procesima.

- Operateri integracija i analitike (AKD): praćenje integracijskih tokova, tumačenje poruka greške, osnovne provjere uspješnosti razmjene i analitičkih obrada.

- Kontakt centar / prva linija podrške (AKD): trijaža prijava, prikupljanje ključnih informacija (identifikatori i poruke sustava), osnovne upute i kriteriji eskalacije prema administratorima i integracijskom timu.

11.2. Struktura edukacijskih modula i očekivani ishodi učenja.

Edukacija se provodi kroz standardizirane module koji se mogu kombinirati ovisno o ulozi. Svaki modul mora imati jasno definirane ishode učenja koji se provjeravaju praktičnim zadatkom u trening okruženju. Ishodi se definiraju tako da su mjerljivi: korisnik mora moći izvršiti određenu radnju, protumačiti rezultat, te znati koje je sljedeće ispravno postupanje kada sustav vrati grešku ili ograničenje ovlasti.

Moduli moraju biti usklađeni s realnim poslovnim situacijama: više pošiljaka u jednom prijevozu, jedna pošiljka s više operacija (pretovar), različite DG stavke s različitim destinacijama, te kombinacije važećih i nevažećih potvrda i dopuštenja. U modulima se koriste isti koncepti i terminologija kao u sustavu (pošiljka/operacija, DG stavka, statusi, obuhvat dopuštenja), kako bi se spriječila pogrešna tumačenja u radu.

Struktura modula mora pokriti i **sigurnosni minimum** koji je potreban za ispravno postupanje: zaštita vjerodajnica, postupanje s osobnim podacima, razumijevanje audita i razlog zašto se pristupi bilježe. Ovaj dio se ne provodi kao opća edukacija “o sigurnosti”, nego kao praktična

Financira
Europska unija
NextGenerationEU

uputa koja je vezana uz konkretne radnje u sustavu (npr. što znači da je selective pull zabilježen i zašto se ne dijele snimke ekrana izvan ovlaštenih kanala).

Minimalni set edukacijskih modula koji se pripremaju kao standardna ponuda unutar projekta je:

Minimalni set edukacijskih modula koji se pripremaju u okviru projekta, fokusirano na djelatnike AKD-a, je:

- Modul 1 – Osnove sustava za AKD: ključni pojmovi i životni ciklus podataka, uloge i ovlasti, audit trag i osnovna pravila postupanja.
- Modul 2 – Operativni rad i aplikativna administracija: rad u modulima registri, osposobljavanje i dopuštenja, validacije i korekcije, tipične iznimke i postupanje u operativnim situacijama, uz pregled funkcionalnosti nadzora radi korisničke podrške.
- Modul 3 – Integracije i analitičke obrade: pregled tokova razmjene, statusi i poruke greške, osnovne provjere uspješnosti, obrada iznimki i praćenje analitičkih obrada.
- Modul 4 – Administracija i podrška korisnicima: pokretanje i zaustavljanje servisa, konfiguracije okruženja, upravljanje certifikatima, sigurnosne kopije i povrat, osnovni postupci oporavka, pregled logova i monitoring, postupci trijaže i eskalacije iz kontakt centra.

Za svaki modul definiraju se minimalni praktični zadaci (vježbe) koji predstavljaju “prolazni prag” edukacije. Primjerice, u Modulu B službenik mora moći dohvatiti DG set za zadanu pošiljku i evidentirati ishod nadzora, dok u Modulu E operater mora moći izdati dopuštenje s obuhvatom UN brojeva i dokazati da je dopuštenje konzistentno s DG stavkama u operaciji.

11.3. Metodologija izvođenja edukacije, materijali i okruženje za vježbu.

Edukacija se provodi kombinacijom vođenih radionica i praktičnog rada u trening okruženju, jer je cilj da korisnici razviju sigurnost u radu kroz realne scenarije, a ne samo kroz prezentacije. U svakoj radionici mora postojati jasna struktura: kratko objašnjenje pojmova i pravila, demonstracija procesa u aplikaciji, zatim samostalna vježba polaznika uz kontrolni popis, te kratka provjera zadatka. Ovakav format je učinkovit jer se odmah otkrivaju tipične pogreške i nerazumijevanja (npr. miješanje operacije i pošiljke, pogrešno tumačenje statusa).

Materijali za edukaciju moraju biti izravno povezani s dokumentacijom sustava, ali prilagođeni edukaciji. To znači da se korisničke upute i administratorski priručnici koriste kao temelj, dok se za edukaciju pripremaju: vodiči “korak-po-korak”, radne bilježnice s vježbama, kontrolni popisi, kratki rječnik pojmova i tipične poruke sustava s tumačenjem. Materijali moraju biti verzionirani uz izdanje sustava kako bi se izbjeglo da se korisnici uče po starim ekranima ili starim pravilima.

Financira Europska unija
NextGenerationEU

Trening okruženje mora biti pripremljeno tako da podržava sve ključne procese bez rizika za stvarne podatke. Okruženje mora sadržavati realističan skup fiktivnih podataka: subjekte, vozila, vozače, lokacije, pošiljke i DG stavke, uključujući scenarije pretovara (jedna pošiljka kroz više operacija) i scenarije više pošiljaka s različitim destinacijama. Važno je da su podaci i scenariji usklađeni s testnim scenarijima iz poglavlja 8., jer se na taj način postiže konzistentnost između validacije sustava i edukacije korisnika.

Metodologija mora uključiti komponentu prijenosa znanja na trenere u AKD-u, jer se time osigurava održivost bez stalnog angažmana izvođača. U praksi AKD imenuje superkorisnike (po mogućnosti po jednom za aplikativni dio, integracije i analitiku te administraciju) koji prolaze proširenu edukaciju s naglaskom na tumačenje pravila, rješavanje tipičnih situacija i vođenje praktičnih vježbi. Nakon toga superkorisnici u AKD-u provode ponovljene edukacije za nove djelatnike i kratka osvježenja nakon nadogradnji, koristeći iste materijale i isto trening okruženje.

11.4. Plan edukacije po fazama implementacije.

Plan edukacije mora biti vremenski usklađen s isporukom funkcionalnosti i dostupnošću trening okruženja, kako bi edukacija bila praktična i odmah primjenjiva. Kako je edukacija usmjerena na AKD, planira se u tri faze.

U prvoj fazi (priprema za prihvatno testiranje korisnika) provodi se edukacija administratora, integracijskog tima i aplikativnih operatera u AKD-u, kako bi mogli samostalno provjeravati status servisa i integracija, razumjeti poruke greške i učinkovito sudjelovati u prihvatnom testiranju korisnika.

U drugoj fazi (operativno uvježbavanje prije produkcije) provodi se objedinjena edukacija za sve AKD uloge kroz scenarije “dan 1”: administracija podataka u modulima, praćenje integracija, osnovno izvještavanje te postupci zaprimanja i eskalacije prijava. Faza završava praktičnim zadacima za svaku AKD ulogu.

U trećoj fazi (stabilizacija nakon produkcije) provode se kratka osvježenja i ciljane radionice temeljem stvarnih upita i uočenih obrazaca rada. Aktivnosti primarno provode AKD superkorisnici uz podršku ugovorene tehničke podrške u okviru projekta.

- Faza 1 – Priprema za prihvatno testiranje korisnika: edukacija ključnih AKD uloga i rad u trening okruženju.
- Faza 2 – Operativno uvježbavanje prije produkcije: objedinjena edukacija svih AKD uloga i provjera kroz praktične zadatke.
- Faza 3 – Stabilizacija: kratka osvježenja i ciljane radionice nakon puštanja u produkciju.

Financira
Europska unija
NextGenerationEU

11.5. Provjera osposobljenosti, minimalna evidencija i prijenos znanja.

Provjera osposobljenosti mora biti praktična i usmjerena na stvarne zadatke. Umjesto opsežnih testova i složene administracije, koristi se model “prolaznih zadataka”: za svaku ulogu definira se mali broj zadataka koje korisnik mora izvršiti u trening okruženju, uz jasno očekivani rezultat. Time se dobiva pouzdana potvrda da korisnik može obaviti posao u sustavu, a istovremeno se ne uvodi složen sustav certificiranja koji bi otežao održavanje.

Minimalna evidencija edukacije mora biti dovoljna za operativne potrebe i za dokaz da su ključne uloge prošle obuku. Evidencija se svodi na: popis polaznika, datum i modul koji su prošli, te oznaku “zadaci izvršeni” uz eventualnu kratku napomenu (npr. potrebna dodatna vježba za određeni ekran). Ova evidencija se vodi centralno i verzionirano, bez dodatnih paralelnih tablica i bez kompleksnih obrazaca.

Prijenos znanja je ključan za održivost i mora biti jasno strukturiran. Superkorisnici dobivaju prošireni sadržaj koji uključuje: tumačenje poslovnih pravila, uobičajene greške i njihovo rješavanje, te način prikupljanja informacija za eskalaciju (korelacijski identifikator, vrijeme, identifikatori pošiljke/operacije, poruke sustava). Administratori dobivaju dodatno: postupke za osnovnu dijagnostiku integracija, pregled logova i minimalne procedure za oporavak (restore i failover provjere).

Uloga kontakt centra u prijenosu znanja mora biti jasno definirana, jer kontakt centar čini “filter” koji sprječava da administratori budu opterećeni trivijalnim pitanjima. Kontakt centar se educira da razlikuje probleme autentifikacije, ovlasti, dostupnosti integracije i pogrešaka validacije, te da zna koji je minimalni skup informacija potreban za eskalaciju. Time se postiže da eskalacije budu kvalitetne, a vrijeme rješavanja kraće, bez uvođenja dodatnih organizacijskih slojeva.

- Praktični zadaci po ulozi: svaka AKD uloga mora izvršiti 2–5 ključnih zadataka (npr. unos i korekcija podataka u registrima uz audit trag, obrada iznimke u osposobljavanju ili dopuštenjima, provjera statusa integracije i tumačenje poruke greške, provođenje sigurnosne kopije i povrata u trening okruženju, pravilna trijaža i eskalacija prijave iz kontakt centra).
- Minimalna evidencija:prisustvo + oznaka izvršenih zadataka, bez dodatnih složenih formi i bez paralelnih evidencija.
- Prijenos znanja na superkorisnike:superkorisnici postaju prva točka pomoći korisnicima i pokrivaju ponovljene edukacije za nove korisnike.
- Osposobljavanje kontakt centra:kontakt centar prikuplja standardizirane informacije i provodi trijažu prije eskalacije.

Financira Europska unija
NextGenerationEU

11.6. Isporuke edukacije i održivost edukacijskog paketa nakon završetka implementacije.

Isporuke edukacije moraju biti definirane kao konkretni i ponovno upotrebljivi artefakti koji ostaju naručitelju i koji se mogu ažurirati uz svako izdanje sustava. To uključuje: prezentacije po modulima, radne bilježnice s vježbama i kontrolnim popisima, rječnik pojmova koji usklađuje eFTI i eADR terminologiju, te set fiktivnih trening podataka i scenarija koji se mogu ponovno koristiti za uvježbavanje novih korisnika. Artefakti moraju biti konzistentni s dokumentacijom definiranom u poglavlju 9., kako bi korisnik nakon edukacije imao jedan jasan izvor uputa za rad.

Edukacijski paket mora sadržavati i posebne materijale za administratore i operativno održavanje: kratke “runbook” postupke za najčešće operacije (provjera statusa servisa, provjera integracije, rotacija certifikata, provjera batch obrade, restore test), te minimalne “checkliste” za postupanje u uobičajenim situacijama (npr. platforma nedostupna, SOTAH ne vraća podatke, batch nije završio). Ovi materijali moraju biti pisani jednostavno, kao koraci koje administrator može provesti bez dodatnih konzultacija.

Održavanje edukacijskih materijala mora biti povezano s održavanjem dokumentacije i verzija sustava. Kada se u izdanju promijeni ekran, status, validacija ili integracijska poruka, mora se ažurirati pripadajući modul i pripadajući zadatak vježbe. Time se osigurava da edukacija uvijek prati stvarno stanje sustava i da se izbjegne situacija da novi korisnici uče po zastarjelim primjerima.

Kako bi edukacija ostala operativno jednostavna, nakon završetka implementacije preporučeni model je da superkorisnici i administratori provode periodične kratke edukacije za nove korisnike i za osvježenja nakon nadogradnji, koristeći iste materijale i isto trening okruženje. Uloga izvođača u tom trenutku svodi se na ažuriranje materijala kada su dio isporuke novog izdanja i na podršku kroz ugovorene kanale, bez uvođenja dodatnih angažmana ili dodatnih organizacijskih dionika.

- Edukacijski paket po modulima:prezentacije, radne bilježnice, vježbe i kontrolni popisi, usklađeni s korisničkim uputama i statusima u sustavu.
- Trening scenariji i podaci:fiktivni, realistični skup podataka koji pokriva DG set, pretovare, više pošiljaka i različite statuse osposobljenosti i dopuštenja.
- Materijali za administratore:runbook postupci i checkliste za integracije, logiranje, backup/restore i osnovne provjere ispravnosti.
- Verzioniranje i ažuriranje:materijali su vezani uz izdanja sustava i ažuriraju se kada se mijenjaju ekrani, pravila ili integracije.

Financira
Europska unija
NextGenerationEU

12. Plan provedbe, vremenski okvir, faze implementacije i ključne prekretnice

Plan provedbe projekta definira strukturirani pristup implementaciji produkcijskog rješenja eADR u on-premise okruženju AKD/MMPI.U tom vremenskom okviru plan mora osigurati da su funkcionalnosti koje pokrivaju nadzor eADR podataka (uključujući DG informativni set), eADR procesi (registri, osposobljavanje, dopuštenja) te integracije (eFTI ekosustav, SOTAH, AFFINIS i sustavi nadležnih tijela) implementirane, testirane, dokumentirane i operativno predane.

Plan je postavljen tako da ne pretpostavlja dodatne vanjske dionike izvan onih predviđenih projektnom dokumentacijom, te da se oslanja na postojeće nacionalne usluge autentifikacije i postojeće sustave koji su dio ciljne arhitekture. Poseban naglasak stavlja se na to da rješenje bude praktično implementabilno i održivo: postupci instalacije i nadogradnji moraju biti ponovljivi, integracije moraju biti provjerljive kroz standardizirane testove, a operativni tim mora dobiti dovoljno znanja i dokumentacije da sustav može stabilno raditi bez stalne ovisnosti o izvođaču.

Provedba se organizira fazno uz jasne prekretnice (gate točke) koje omogućuju kontrolu opsega i kvalitete bez uvodenja složenih upravljačkih mehanizama. Svaka faza završava provjerljivim isporukama (npr. potvrđena specifikacija i dizajn, implementirane i demonstrirane funkcionalnosti, završeno integracijsko testiranje, potpisan UAT, pripremljeno produkcijsko okruženje i provedeni “go-live” koraci). Time se postiže da je napredak mjerljiv i da se problemi otkrivaju rano, dok su korekcije još jednostavne.

Vremenski okvir se izražava isključivo kroz trajanja i relativne oznake (npr. T0 je potpis ugovora i početak provedbe). U planu se koristi okvirna podjela po tjednima kako bi se omogućilo precizno praćenje bez navođenja kalendarskih datuma.

12.1. Polazne pretpostavke i načela planiranja

Provedba se planira uz pretpostavku da je ciljna infrastruktura dostupna u AKD podatkovnom centru te da se sustav implementira **on-premise** na virtualnim poslužiteljima (VM) sukladno projektnoj dokumentaciji. Plan podrazumijeva da se u ranoj fazi provedbe uspostavljaju sva potrebna okruženja (minimalno DEV/TEST/UAT/PROD), pri čemu se TEST i UAT koriste kao ključni oslonac za integracijske provjere i prihvatno testiranje korisnika.

Plan pretpostavlja da se za autentifikaciju i identitete koristi nacionalni okvir gdje je primjenjivo (eGrađanin/NIAS) te da se ovlasti implementiraju kroz uloge unutar sustava, uz jasna pravila pristupa po ciljanim skupinama korisnika. Time se izbjegava paralelno upravljanje korisnicima i održava usklađenost s očekivanim načinom rada državnih sustava, uz audit trag ključnih radnji i pristupa.

Financira Europska unija
NextGenerationEU

U dijelu integracija plan se temelji na tome da nacionalni eFTI čvor/gateway i eADR nisu izolirani sustavi, nego da eADR mora generirati i obrađivati podatke koji su dio obveznog eFTI informativnog skupa za opasne tvari (DG set). To ima praktičnu posljedicu na faziranje: podatkovni modeli, šifrarnici i validacije DG seta moraju biti definirani i verificirani dovoljno rano, kako bi integracije i testni scenariji mogli biti izvedeni u realnim uvjetima (više pošiljaka, pretovari, više operacija po pošiljci).

Plan provedbe se vodi načelom **minimalne složenosti za održavanje**. To znači da se u provedbi preferiraju standardizirani postupci (ponovljive instalacije i konfiguracije), jasna segmentacija okruženja i konfiguracija, te dokumentacija i edukacija koja omogućuje operativni rad bez dodatnih "ručnih" procedura koje bi kasnije postale teret održavanja.

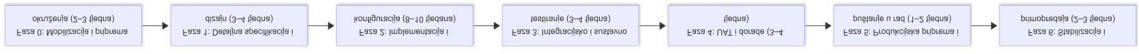
12.2. Okvirna dinamika provedbe i faze implementacije

Faze se planiraju tako da se kritični tokovi (infrastruktura, integracije, sigurnosne postavke) pokreću dovoljno rano, a da se izbjegne situacija u kojoj se većina posla gura u završnicu projekta. Posebno se naglašava paralelizacija aktivnosti gdje je to opravdano, primjerice: dok se implementira dio eADR registara, može se paralelno pripremati integracijski sloj i katalog sučelja, te pripremati analitički tokovi za AFFINIS.

Faziranje je postavljeno tako da se nakon inicijalne specifikacije i dizajna što prije dođe do demonstrabilnog inkrementa: AAP osnovni tok nadzora (lookup + prikaz metapodataka + selective dohvat DG seta), eADR osnovni registri, te minimalni integracijski "end-to-end" tok u TEST okruženju. Time se osigurava da ključne pretpostavke interoperabilnosti budu potvrđene rano, a ne tek pred UAT.

U svakoj fazi definiraju se jasne isporuke koje služe kao preduvjet za nastavak. Primjerice, bez potvrđenog podatkovnog modela i šifrarnika ne ulazi se u završno povezivanje integracija, a bez završenih osnovnih sigurnosnih postavki i audita ne ulazi se u UAT koji uključuje stvarne uloge i postupanje nadležnih tijela.

U nastavku je prikazan okvirni slijed faza s preporučenim trajanjem. Trajanja su namjerno izražena u rasponima gdje je to potrebno, kako bi se omogućilo prilagođavanje bez mijenjanja koncepta plana.



Slika 31. Dinamika provedbe i faze implementacije

- Faza 0 – Mobilizacija i priprema okruženja:obuhvaća formalni početak provedbe (kick-off), uspostavu radnih kanala, potvrdu pristupa okruženjima, te osnovnu instalaciju i konfiguraciju DEV/TEST okruženja uz inicijalni monitoring i logiranje.

Financira
Europska unija
NextGenerationEU

- Faza 1 – Detaljna specifikacija i dizajn:obuhvaća potvrdu detaljne specifikacije, podatkovnog modela i integracijskih ugovora, uključujući DG set, šifrarnike i pravila validacije te dogovor o prioritetima inkremenata.
- Faza 2 – Implementacija i konfiguracija:obuhvaća razvoj i konfiguraciju eADR modula, implementaciju integracija, pripremu analitičkih tokova prema AFFINIS te izradu operativnih procedura i inicijalne dokumentacije.
- Faza 3 – Integracijsko i sustavno testiranje:obuhvaća provedbu sustavnih i integracijskih testova u TEST okruženju, korekcije, te potvrdu da ključni end-to-end tokovi rade stabilno. • Faza 4 – UAT i dorade:obuhvaća prihvatno testiranje korisnika u UAT okruženju prema definiranim scenarijima, uz kontrolirane dorade i regresije.
- Faza 5 – Produkcijska priprema i puštanje u rad:obuhvaća finalnu konfiguraciju produkcije, validacijske provjere spremnosti, prijenos konfiguracija i certifikata, te kontrolirano puštanje u rad.
- Faza 6 – Stabilizacija i primopredaja:obuhvaća pojačani operativni nadzor, rješavanje uočenih problema, finalizaciju dokumentacije “as-built” i formalnu primopredaju sustava i znanja.

12.3. Sadržaj faza i minimalne isporuke po fazi

Faze provedbe moraju imati jasno definirane minimalne isporuke koje su provjerljive, jer se na taj način osigurava da projekt napreduje kroz stvarno završene cjeline, a ne kroz parcijalne aktivnosti. Minimalne isporuke su usmjerene na ono što je nužno da sustav bude implementiran, testiran i spreman za operativni rad, bez uvođenja dodatnih administrativnih slojeva.

U fazama se posebna pozornost daje “okosnici” sustava: podatkovnim modelima (pošiljka, operacija, DG stavke, osposobljavanje, dopuštenja), integracijskim tokovima (eFTI metapodaci i selective/full dohvat, SOTAH dohvat sažetaka, batch prema AFFINIS), sigurnosnim postavkama (identiteti, ovlasti, audit i zapisnici), te operativnim procedurama (instalacija, konfiguracija, backup/restore, osnovni DR postupci). Time se osigurava da svi elementi iz poglavlja 5. (arhitektura), 8. (testiranje), 9. (dokumentacija) i 11. (edukacija) imaju svoje mjesto u realnom planu provedbe.

Isporuke se u planu ne tretiraju kao “dodatni dokumenti”, nego kao instrument koji omogućuje brzu provjeru. Primjerice, katalog sučelja nije samo dokument, nego ulaz za integracijsko testiranje i za rješavanje problema u produkciji; testni scenariji nisu samo popis, nego baza za UAT i za kasnije regresije; edukacijski materijali nisu samo prezentacije, nego osnova za operativno uvođenje korisnika.

U nastavku su opisane minimalne isporuke po fazama, s fokusom na praktičnu provedivost i usklađenost s ciljnim opsegom projekta.

Financira
Europska unija
NextGenerationEU

- Faza 0 – Minimalne isporuke:postavljena DEV/TEST okruženja, definirani pristupi i korisničke uloge za tehnički tim, inicijalni log-kolektor i monitoring uključen, te osnovna provjera da se servisi mogu deployati i pokretati u ciljnom VM okruženju.
- Faza 1 – Minimalne isporuke:potvrđen detaljan podatkovni model (uključujući vezu pošiljka–operacija), potvrđeni šifrarnici i statusi, potvrđeni integracijski ugovori (katalog sučelja), te potvrđen plan testiranja i plan edukacije usklađen s fazama.
- Faza 2 – Minimalne isporuke:implementirani ključni moduli (AAP nadzorni tok, eADR registri, osposobljavanje i dopuštenja), implementirane integracije u TEST okruženju (eFTI tokovi, SOTAH, AFFINIS batch), te inicijalne administratorske procedure i tehnička dokumentacija.
- Faza 3 – Minimalne isporuke:provedeno integracijsko i sustavno testiranje s dokazima, zatvorene kritične greške, potvrđen stabilan end-to-end tok nadzora (lookup + DG set) i ključni eADR tokovi, te potvrđena spremnost za UAT.
- Faza 4 – Minimalne isporuke:proveden UAT prema unaprijed definiranim scenarijima, provedene potrebne korekcije uz regresije, te formalna potvrda prihvata funkcionalnosti od ovlaštenih korisnika.
- Faza 5 – Minimalne isporuke:postavljeno produkcijsko okruženje, provedena produkcijska validacija (health check, integracije, sigurnosne postavke), pripremljen i izveden plan puštanja u rad, te aktiviran pojačani operativni nadzor.
- Faza 6 – Minimalne isporuke:finalna “as-built” dokumentacija, potvrđen prijenos znanja (superkorisnici i administratori), stabilizirani ključni tokovi, te formalna primopredaja uz definirane operativne procedure podrške.

12.4. Ključne prekretnice i kriteriji prolaznosti

Ključne prekretnice (prekretnice projekta) služe kao kontrolne točke na kojima se potvrđuje da je određena cjelina završena do razine koja omogućuje nastavak provedbe bez akumuliranja tehničkih i organizacijskih nejasnoća. Prekretnice moraju biti jasno razumljive svim uključenim stranama i moraju imati mjerljive kriterije prolaznosti, kako bi se izbjeglo situacije da se faza “zatvori” iako još nije funkcionalno spremna.

Kriteriji prolaznosti moraju biti usmjereni na demonstraciju: funkcionalnost radi, integracije su provjerene, sigurnosne postavke su postavljene na minimalno potrebnoj razini, te postoje dokazni artefakti (izvještaji testiranja, izvoz konfiguracije, audit zapisi, evidencije UAT scenarija). Time se osigurava da se sustav ne oslanja na “neformalno znanje” nego da je stanje provjerljivo i ponovljivo.

Prekretnice se planiraju tako da prate prirodni tok implementacije: od potvrde specifikacije i dizajna, preko “feature complete” stanja, do završetka integracijskog testiranja i prihvata. U praksi, to omogućuje i jasno planiranje edukacije: edukacija UAT korisnika može krenuti kada je funkcionalnost dovoljno stabilna da korisnici ne uče na ekranima koji se svakodnevno mijenjaju.

Financira
Europska unija
NextGenerationEU

U nastavku je preporučeni skup ključnih prekretnica, s kriterijima i rokovima koji su prilagođeni opsegu projekta (rokovi se računaju od datuma Kick-offa):

Prekretnica 1 – Spremnost okruženja i potvrda specifikacije i dizajna

Datum izvršenja: do 10.04.2026.

Kontrolne točke

1. Izrađuje se i potvrđuje popis projektnih korisničkih računa i pripadajućih ovlasti za razvoj, testiranje i administraciju, uz evidentiranje odobrenja i odgovornih osoba.
2. Uspostavlja se razvojno i testno okruženje u ciljnoj infrastrukturi, uključujući mrežne postavke i sve osnovne tehničke preduvjete, te se provodi provjera dostupnosti okruženja.
3. Provodi se inicijalno pokretanje aplikacijskih servisa u predviđenim konfiguracijama, pri čemu se potvrđuje da se sustav može podići i da su dostupne osnovne provjere ispravnosti rada.
4. Uspostavlja se osnovni nadzor rada sustava i prikupljanje zapisnika rada te se potvrđuje da se ključne tehničke informacije uredno prikupljaju i da su dostupne za pregled i analizu.
5. Potvrđuje se podatkovni model te se usuglašavaju i zaključuju šifrarnici i statusi koji se koriste u procesima, uz osiguranje verzioniranja i sljedivosti izmjena.
6. Potvrđuje se katalog sučelja, definira se opseg i redoslijed implementacije po sučeljima te se usuglašavaju osnovne pretpostavke razmjene podataka.
7. Gdje je primjenjivo, provodi se demonstracija prototipa ključnih zaslona ili tokova rada te se usvajaju zaključci koji se prenose u provedbu.

Dokazna dokumentacija i zapisi

- Službeni zapisnik o izvršenju prekretnice s popisom provedenih aktivnosti, ocjenom ispunjenosti kontrolnih točaka i zaključkom o prihvaćanju prekretnice, ovjeren od ovlaštenih predstavnika.
- Evidencija dodijeljenih ovlasti i pristupa u obliku popisa, bez objave povjerljivih podataka.
- Tehnička evidencija uspostavljenih okruženja s opisom osnovnih postavki i potvrdom dostupnosti.
- Zapisi o inicijalnom pokretanju servisa, uključujući rezultate provjera ispravnosti rada i reprezentativne isječke zapisnika rada.

Financira Europska unija
NextGenerationEU

- Dokaz o uključenom nadzoru i prikupljanju zapisnika rada, primjerice izvoz ili snimke prikaza metrika i zapisnika.
- Potvrđena verzija dokumentacije podatkovnog modela, šifrarnika i statusa te potvrđena verzija kataloga sučelja i prioriteta.
- Zapis o demonstraciji prototipa, uključujući zaključke i popis dogovorenih dorada.

Prekretnica 2 – Funkcionalno dovršenje u testnom okruženju

Datum izvršenja: do 29.05.2026.

Kontrolne točke

1. Implementiraju se ključni poslovni tokovi eADR procesa i tokovi nadzora u dogovorenom opsegu te se potvrđuje da se scenariji mogu izvesti od početka do kraja u testnom okruženju.
2. Implementiraju se i provjeravaju ključne integracije potrebne za provedbu glavnih tokova, pri čemu se potvrđuje ispravna razmjena podataka u tipičnim scenarijima korištenja.
3. Provode se provjere obrade podataka, uključujući validacije ulaznih poruka, pravila obrade i izlazne poruke, te se evidentiraju rezultati i odstupanja.
4. Uspostavlja se početni skup automatiziranih ili u potpunosti ponovljivih testova te se definira postupak njihova izvođenja i način evidentiranja rezultata.
5. Provodi se pregled stabilnosti i poznatih nedostataka te se potvrđuje da ne postoje nedostaci koji onemogućuju izvođenje ključnih tokova, uz popis otvorenih stavki s prioritetima i planom otklona.

Dokazna dokumentacija i zapisi

- Službeni zapisnik o izvršenju prekretnice s pregledom provjera i zaključkom o prihvaćanju prekretnice, ovjeren od ovlaštenih predstavnika.
- Popis implementiranih funkcionalnosti i pripadajućih izmjena, povezan s evidencijom zadataka i isporuka.
- Evidencija provjere integracija u testnom okruženju s opisom scenarija i rezultatima.
- Evidencija provedenih provjera obrade podataka i validacija, uključujući primjere ulaza i izlaza.
- Izvještaj o izvođenju automatiziranih ili ponovljivih testova s prikazom rezultata.
- Pregled poznatih nedostataka s klasifikacijom ozbiljnosti, statusom i planiranim datumima otklona.

Financira
Europska unija
NextGenerationEU

- Reprezentativni zapisi rada sustava koji podupiru zaključak o izvedivosti ključnih tokova. **Prekretnica 3 – Završetak integracijskog i sustavnog testiranja te prihvat korisnika**

Datum izvršenja: do 26.06.2026.

Kontrolne točke

1. Provodi se integracijsko i sustavno testiranje sukladno usuglašenom planu testiranja, uz evidentiranje rezultata po svakom testnom scenariju.
2. Otklanjaju se svi kritični nedostaci, a za preostale nedostatke izrađuje se i odobrava plan rješavanja koji ne blokira prihvat korisnika.
3. Provode se provjere potpunih tokova rada od početka do kraja, uključujući integracije, te se potvrđuje stabilnost ključnih scenarija.
4. Provodi se prihvatno testiranje korisnika prema unaprijed pripremljenim scenarijima, uz sudjelovanje ključnih uloga, te se evidentiraju rezultati i zaključci.
5. Nakon eventualnih korekcija provodi se regresijsko testiranje kako bi se potvrdilo da izmjene nisu negativno utjecale na već provjerene funkcionalnosti.

Dokazna dokumentacija i zapisi

- Službeni zapisnik o izvršenju prekretnice s rezultatima testiranja i zaključkom o prihvaćanju prekretnice, ovjeren od ovlaštenih predstavnika.
- Plan testiranja i evidencija izvršenja integracijskog i sustavnog testiranja, uključujući izvještaje o rezultatima.
- Evidencija otklanjanja kritičnih nedostataka i potvrda njihova zatvaranja te odobren plan rješavanja preostalih nedostataka.
- Dokazni zapisi o provedenim potpunim tokovima, uključujući odabrane zapisnike rada i izvještaje.
- Zapisnici o prihvatnom testiranju korisnika s jasno navedenim ishodom po scenariju i ovjerom sudionika.
- Izvještaj regresijskog testiranja s popisom ponovljenih provjera i rezultatima. **Prekretnica 4 – Priprema produkcije, puštanje u rad, verifikacija do roka i primopredaja**

Datum izvršenja: do 27.07.2026.

Kontrolne točke

1. Priprema se produkcijsko okruženje u skladu s ciljanom arhitekturom, uključujući resurse, mrežne postavke i sigurnosne postavke, te se provodi provjera dostupnosti i osnovne funkcionalnosti okruženja.
2. Postavljaju se produkcijske konfiguracije i certifikati te se provode dogovorene sigurnosne provjere radi potvrde usklađenosti i prihvatljive razine rizika.
3. Provodi se provjera integracija u produkcijskom kontekstu prema unaprijed dogovorenom postupku, uz evidentiranje rezultata i eventualnih ograničenja.
4. Provodi se kontrolirano puštanje sustava u rad prema planu puštanja u rad, uz jasno definirane korake, odgovornosti i pripremljen postupak povrata na prethodno stanje u slučaju potrebe.
5. Provodi se verifikacija ključnih tokova rada u produkciji te se prikupljaju dokazi da sustav radi stabilno i da su ključni scenariji uspješno izvedeni.
6. Provodi se primopredaja rješenja, pri čemu se isporučuju operativne upute, tehnička dokumentacija izvedenog stanja te se provodi prijenos znanja na administratore i superkorisnike.

Dokazna dokumentacija i zapisi

- Službeni zapisnik o izvršenju prekretnice s opisom provedenih aktivnosti, ispunjenosti kontrolnih točaka i zaključkom o prihvaćanju prekretnice, ovjeren od ovlaštenih predstavnika.
- Evidencija pripreme produkcijskog okruženja, uključujući osnovne konfiguracijske podatke i rezultate provjera dostupnosti.
- Dokaz o postavljenim konfiguracijama i certifikatima u mjeri koja ne otkriva povjerljive podatke te izvještaji o provedenim sigurnosnim provjerama.
- Evidencija provjere integracija u produkcijskom kontekstu s opisom scenarija, rezultatima i pripadajućim zapisnicima rada.
- Plan puštanja u rad i zapis o provedbi puštanja u rad, uključujući evidentirane korake, odluke i primijenjene kontrole, te opis postupka povrata.
- Verifikacijski zapisi za ključne tokove, uključujući zapisnike rada, izvještaje i snimke koji se mogu izravno povezati s konkretnim scenarijima.
- Operativne upute za rad i održavanje, tehnička dokumentacija izvedenog stanja te zapis o provedenoj edukaciji i prijenosu znanja.

Financira Europska unija NextGenerationEU

12.5. Plan okruženja, instalacije i prijelaza u produkciju

Plan provedbe mora eksplicitno uključiti uspostavu i uporabu okruženja jer se većina kvalitete i operativne održivosti dobiva pravilnim razdvajanjem DEV/TEST/UAT/PROD i pravilnim upravljanjem konfiguracijama po okruženju. Okruženja se ne postavljaju samo "tehnički", nego tako da podrže realne tokove rada: u TEST okruženju se provode integracijska testiranja i regresije, dok se u UAT okruženju provodi prihvat korisnika uz realne uloge i realne procedure.

Instalacija i konfiguracija moraju biti ponovljive i dokumentirane, jer se sustav implementira on-premise i jer su nadogradnje očekivane. To znači da plan mora uključiti: inicijalnu instalaciju, postupke konfiguracije integracija i certifikata, inicijalno punjenje šifrarnika i referentnih podataka, te procedure validacije nakon instalacije (health check, probni tokovi integracije, provjera audita). U provedbi se posebno naglašava da se konfiguracijski parametri po okruženju vode kontrolirano, kako bi se spriječilo ručno "krpanje" na produkciji.

Prijelaz u produkciju mora biti organiziran kao kontrolirani postupak s jasno definiranim koracima i točkama provjere. Budući da je opseg sustava nacionalan i operativno važan, plan mora uključiti minimalni "production readiness" kontrolni popis: autentifikacija radi, uloge su mapirane, integracije su dostupne, audit i zapisnici rade, te se mogu provesti osnovni nadzorni tokovi i eADR postupci. U ovom dijelu se izbjegava uvođenje složenih režima paralelnog rada; fokus je na praktičnom puštanju u rad uz stabilizaciju.

Plan mora predvidjeti i pripremu trening podataka i inicijalnih šifrarnika, jer bez toga nije moguće provesti kvalitetan UAT i edukaciju. Ovi podaci su fiktivni, ali realistični, i pokrivaju ključne scenarije (više pošiljaka, pretovari, različite DG stavke, važeće i nevažeće potvrde i dopuštenja). Time se omogućuje da korisnici u UAT-u i edukaciji rade na scenarijima koji nalikuju stvarnom radu, bez izlaganja stvarnih osobnih podataka.

- Okruženja koja se uspostavljaju u provedbi:DEV za iterativni razvoj, TEST za integracijska i sustavna testiranja, UAT za prihvatno testiranje korisnika, te PROD za produkcijski rad uz mogućnost DR lokacije prema ciljnom dizajnu.
- Validacije nakon instalacije:provjera dostupnosti servisa, provjera baze i migracija, provjera autentifikacije i uloga, probni eFTI tok (metapodaci + DG set), probni eADR tok (registri → dopuštenje/potvrda), te provjera audita.
- Prijelaz u produkciju:kontrolirani "cutover" s jasno definiranim koracima i minimalnim skupom provjera koje se moraju proći prije otvaranja sustava korisnicima.

12.6. Plan testiranja, prihvata i puštanja u rad po fazama

Testiranje i prihvat moraju biti integralni dio plana provedbe, a ne aktivnost koja se ostavlja za kraj. U fazama implementacije planira se kontinuirana provjera: osnovne provjere funkcionalnosti i integracija se rade čim su inkrementi dostupni, dok se sustavno integracijsko

Financira Europska unija NextGenerationEU

testiranje (u TEST okruženju) provodi kada su ključne funkcionalnosti “feature complete”. Time se osigurava da se greške otkrivaju i rješavaju postupno, a ne kumulativno.

Prihvat korisnika (UAT) mora biti planiran kao formalna faza s unaprijed definiranim scenarijima i dokazima, pri čemu se koristi skup scenarija koji je već definiran u poglavlju o testnim scenarijima i validacijskim postupcima. UAT nije samo provjera “radi li ekran”, nego provjera da korisnici mogu izvršiti svoje ključne zadatke: provesti nadzor i dohvatiti DG set, izdati dopuštenje s obuhvatom, provesti osposobljavanje i izdati potvrdu, te evidentirati nadzor i nalaz. UAT mora biti proveden s realnim ulogama i ovlastima.

Puštanje u rad mora imati jasno definiranu “production readiness” provjeru koja uključuje i sigurnosni minimum: ovlasti su postavljene, audit bilježi ključne radnje, TLS i certifikati su ispravno konfigurirani, te su integracije operativno provjerene. Ova provjera se provodi neposredno prije puštanja u rad i čini osnovu za odluku o otvaranju sustava korisnicima.

Nakon puštanja u rad planira se razdoblje stabilizacije koje nije “nova faza razvoja”, nego operativna faza pojačanog nadzora u kojoj se rješavaju uočeni problemi, usklađuju procedure i finalizira dokumentacija “as-built”. Stabilizacija se vodi tako da se ne uvode nove funkcionalnosti, nego se osigurava pouzdanost i jasnoća postupanja u realnim situacijama.

- Integracijsko i sustavno testiranje (TEST):provjerava se interoperabilnost eFTI tokova, DG set validacije, SOTAH dohvat sažetaka i AFFINIS batch, uz dokazne pakete (logovi, izvještaji, snimke) i jasno označene korelacijske identifikatore.
- UAT (UAT okruženje):provodi se prema unaprijed dogovorenim scenarijima s ključnim ulogama, uz kontrolirane korekcije i regresije te formalnu potvrdu prihvata.
- Go-live i stabilizacija (PROD):kontrolirano puštanje u rad, pojačani operativni nadzor, te zatvaranje uočenih problema bez širenja opsega.

12.7. Plan edukacije u provedbi i priprema operativne organizacije

Edukacija se vremenski uvezuje u plan provedbe tako da je maksimalno učinkovita i da korisnici uče na stabilnoj verziji sustava. U ranijim fazama (priprema i dizajn) edukacija je fokusirana na superkorisnike i administratore kako bi mogli aktivno sudjelovati u UAT-u i u pripremi operativnih procedura. U kasnijim fazama (UAT i pred go-live) edukacija se širi na sve operativne uloge, uz naglasak na “dan-1” postupke.

Plan edukacije mora biti usklađen s raspoloživošću trening okruženja i testnih podataka. To je praktični preduvjet: bez realističnih scenarija (pošiljke, operacije, DG stavke, pretovari, dopuštenja i potvrde) edukacija postaje teorijska i ne priprema korisnike za realan rad. Zbog toga se u fazi implementacije planira i priprema trening scenarija paralelno s razvojem funkcionalnosti.

Operativna organizacija (administratori, integracijski operateri, kontakt centar) mora biti uključena dovoljno rano kako bi procedure bile provjerene prije produkcije. To znači da se tijekom TEST i UAT faze provode i “operativne vježbe”: provjera logova, provjera statusa

Financira
Europska unija
NextGenerationEU

integracija, postupanje kod uobičajenih grešaka, te provjera osnovnih backup/restore koraka u kontroliranom okruženju. Time se smanjuje broj iznenađenja u produkciji i skraćuje vrijeme rješavanja problema.

U završnoj fazi provedbe provodi se prijenos znanja (train-the-trainer) tako da naručitelj zadrži sposobnost samostalnog uvođenja novih korisnika i samostalnog održavanja osnovnih operativnih postupaka. Materijali edukacije se verzioniraju uz izdanje sustava kako bi se osigurala konzistentnost nakon budućih nadogradnji.

- Edukacija superkorisnika i administratora:provodi se prije i tijekom UAT faze kako bi superkorisnici mogli voditi prihvatne scenarije i prepoznati pogreške u postupcima ili prikazu podataka.
- Edukacija operativnih uloga:provodi se neposredno prije produkcije uz fokus na ključne postupke (nadzor, osposobljavanje, dopuštenja, evidencija nadzora) i tumačenje poruka sustava.
- Priprema kontakt centra:provodi se kroz praktičnu trijažu i standardni obrazac prijave, uz jasno definirane kriterije eskalacije prema administratorima i integracijskom timu.

12.8. Plan dokumentacije, primopredaje i zatvaranja provedbe

Dokumentacija se izrađuje iterativno tijekom provedbe, a ne tek na kraju, jer dokumentacija mora pratiti stvarno stanje sustava i biti provjerena kroz testiranje i operativne vježbe. U ranim fazama fokus je na tehničkim specifikacijama i katalogu sučelja, dok se u srednjim fazama nadograđuju administratorske upute i integracijska dokumentacija, a u završnim fazama se finaliziraju korisničke upute, sigurnosne postavke i “as-built” prikazi implementacije.

Primopredaja sustava mora biti strukturirana tako da naručitelj dobije: produkcijski deployane komponente, konfiguracije po okruženjima, dokumentaciju, edukacijske materijale, te operativne procedure. Primopredaja nije samo predaja datoteka, nego i potvrda da su procedure provedive: administrator mora moći samostalno provjeriti status sustava, provesti osnovne dijagnostičke korake i izvršiti standardne operativne radnje, a superkorisnici moraju moći provesti ključne postupke u aplikaciji.

Zatvaranje provedbe uključuje finalizaciju dokaznih artefakata: rezultati testiranja, evidencije UAT scenarija, izvještaji sigurnosnih provjera u minimalno potrebnom opsegu, te zapis provedene edukacije. Ovi artefakti nisu dodatna administracija, nego praktični trag koji potvrđuje da je sustav prošao kroz potrebne faze i da je spreman za operativni rad u državnom okruženju.

U završnoj fazi se potvrđuje i operativni režim nakon projekta: tko prati sustav, kako se prijavljuju problemi, koji su osnovni kanali podrške, te gdje se nalaze ključne upute i runbook postupci. Time se osigurava da sustav nakon puštanja u rad ne ovisi o neformalnim dogovorima, nego da ima jasno definiran i održiv način rada unutar organizacije naručitelja.

Financira
Europska unija
NextGenerationEU

13. Procjena rizika i upravljanje rizicima vezanim uz tehničku implementaciju

Tehnička implementacija eADR rješenja u on-premise okruženju mora biti vođena svjesnom procjenom rizika kako bi se izbjegle situacije u kojima sustav formalno postoji, ali nije operativno upotrebljiv (npr. integracije nisu stabilne, podaci nisu konzistentni, ovlasti nisu ispravno postavljene ili je produkcijska instalacija teško ponovljiva). Procjena rizika u ovom poglavlju fokusira se isključivo na tehničke rizike koji mogu utjecati na uspješnu isporuku i stabilan rad sustava.

Upravljanje rizicima mora biti jednostavno i provedivo u praksi, bez uspostave složenih procedura i dodatnih organizacijskih slojeva. Umjesto kompleksnih "registara", koristi se jedna zajednička lista tehničkih rizika koja se održava i ažurira tijekom implementacije te se pregledava u redovnim projektnim sastancima i na ključnim prekretnicama (npr. završetak dizajna, završetak integracijskog testiranja, početak UAT-a, puštanje u rad). Svaki rizik mora imati jasno imenovanog nositelja (AKD/MMPI ili izvođač) i dogovorenu mjeru ublažavanja koja je izvediva bez angažmana dodatnih vanjskih dionika.

Rizici u ovoj domeni najčešće nastaju na rubovima između modula i organizacija: tamo gdje se sustavi povezuju (eFTI tokovi, SOTAH, AFFINIS), gdje se mapiraju identiteti i ovlasti (eGrađanin/NIAS i uloge u aplikaciji), te gdje se poslovni pojmovi moraju pretočiti u podatkovni model (pošiljka, operacija prijevoza, pretovari, DG stavke, dopuštenja i osposobljenost). Upravo zato naglasak nije na "općenitim IT rizicima", nego na specifičnim točkama koje proizlaze iz arhitekture i obuhvata sustava.

Cilj upravljanja rizicima nije eliminacija svih rizika, nego postizanje razine kontrole koja omogućuje pravodobno otkrivanje i korekciju, uz minimalno opterećenje operativnog održavanja nakon puštanja u rad. U tom smislu, mjere ublažavanja u nastavku predlažu prvenstveno: ranije potvrde integracija, jasna pravila podataka i validacija, ponovljive instalacije i konfiguracije, te osnovne provjere sigurnosti i zapisnika događaja.

13.1. Način procjene rizika i minimalni proces upravljanja

Procjena rizika provodi se kroz jednostavnu metodu vjerojatnosti i utjecaja, prilagođenu državnom on-premise projektu. Vjerojatnost označava koliko je realno da će se rizik ostvariti u uvjetima implementacije (ovisnosti o vanjskim sustavima, složenost integracije, zrelost podataka, promjene specifikacija). Utjecaj označava posljedicu na isporuku i operativnost (blokira integracijsko testiranje, onemogućuje UAT, uzrokuje pogrešne rezultate nadzora, narušava sigurnosne zahtjeve ili uzrokuje nestabilnost produkcije).

Za svaki rizik definira se minimalan skup atributa koji omogućuje praktično upravljanje bez administrativnog opterećenja: opis rizika, pogođeni modul(i), uzrok, indikator ranog upozorenja, mjera ublažavanja, nositelj i ciljano stanje (kada se smatra da je rizik sveden na

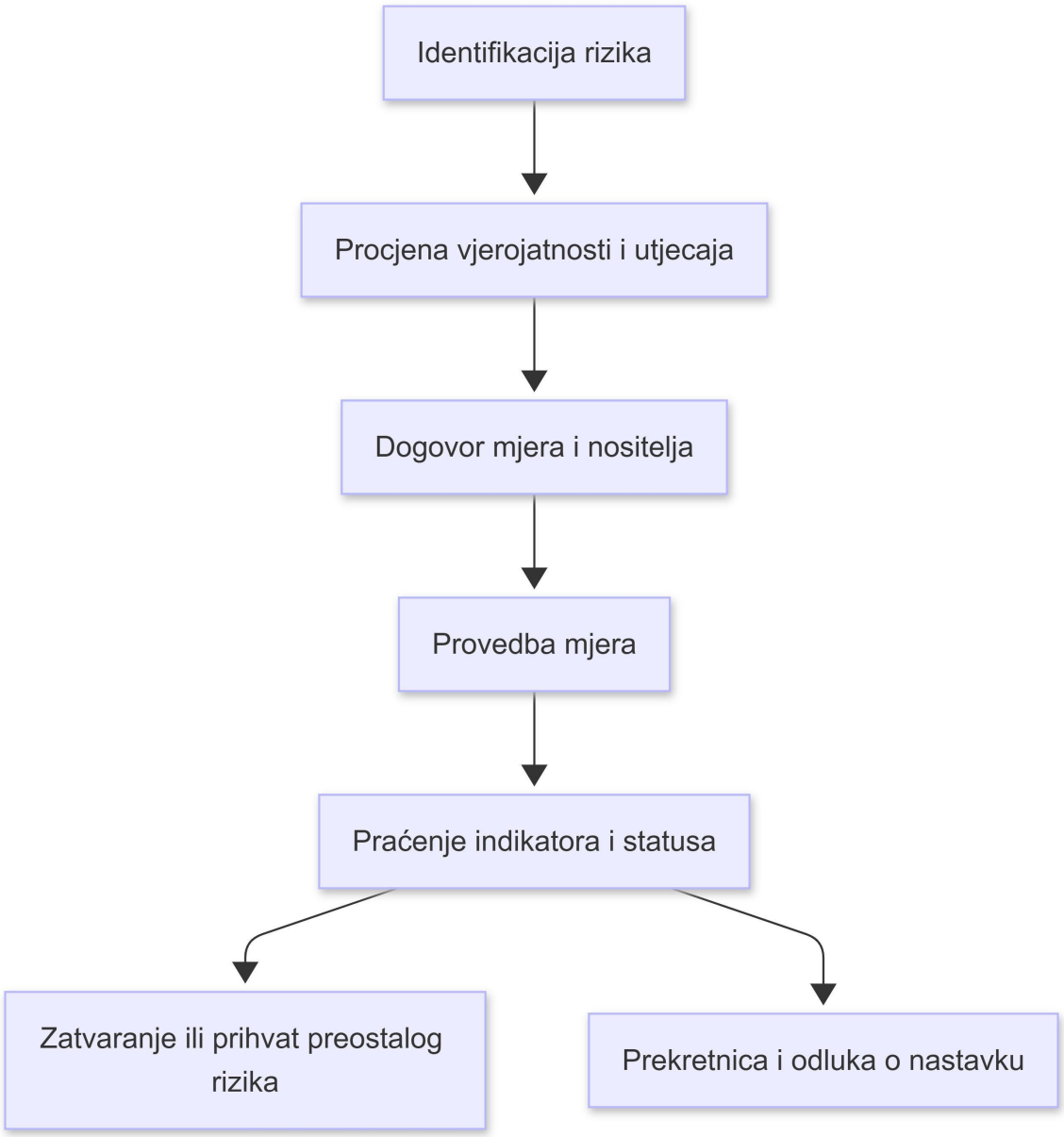
Financira Europska unija NextGenerationEU

prihvatljivu razinu). Posebno je važno da indikator ranog upozorenja bude mjerljiv ili uočljiv (npr. ponavljajuće greške u integraciji, poruke o neusklađenim šifrarnicima, rast vremena odziva, učestale pogreške ovlasti), jer to omogućuje reakciju prije nego rizik postane incident.

Upravljanje rizicima povezuje se s prekretnicama iz plana provedbe. Primjerice, prije prelaska u UAT mora biti potvrđeno da su ključne integracije stabilne u TEST okruženju, da su ovlasti i audit postavljeni minimalno ispravno te da su testni scenariji provedeni s dokazima. Time se izbjegava situacija da se UAT koristi kao “debug” integracija ili sigurnosnih postavki, što u pravilu stvara kašnjenja i opterećenje korisnika.

Minimalni proces upravljanja rizikom može se prikazati kao ponovljivi tok koji se izvršava kroz cijelu implementaciju:

Financira
Europska unija
NextGenerationEU



Slika 32. Procjena rizika i upravljanje

- Razina vjerojatnosti: niska (rijetko, samo u iznimnim uvjetima), srednja (može se dogoditi bez posebnih anomalija), visoka (očekivano ako se ne poduzmu mjere).
- Razina utjecaja: nizak (lokalni utjecaj, ne blokira ključne tokove), srednji (utječe na više modula ili otežava testiranje), visok (blokira ključne tokove, UAT ili produkciju, ili predstavlja sigurnosni neprihvatljiv ishod).
- Pravilo eskalacije: svaki rizik s visokim utjecajem ili visokom vjerojatnošću mora imati mjeru ublažavanja definiranu i započetu prije sljedeće projektne prekretnice.

Financira Europska unija
NextGenerationEU

13.2. Kategorije tehničkih rizika specifične za eADR

Kategorizacija rizika služi tome da se osigura da su pokrivena sva ključna područja sustava: infrastruktura i okruženja, podatkovni modeli i šifrarnici, integracije i interoperabilnost, sigurnosne postavke i zapisnici, performanse i raspoloživost, te operativna održivost (dokumentacija, edukacija i ponovljive procedure). U ovom projektu posebno su kritične integracije i podaci, jer eADR mora biti usklađen s eFTI obveznim informativnim skupovima za opasne tvari, a AAP nadzorni tokovi ovise o stabilnom dohvaćanju i interpretaciji podataka.

Rizici se moraju promatrati kroz "životni ciklus" implementacije. U početnoj fazi tipično dominiraju rizici dizajna i modela (npr. pogrešno modeliranje odnosa pošiljka–operacija, pogrešno razumijevanje DG seta), dok u srednjoj fazi dominiraju integracijski rizici (npr. nedostupnost testnih endpointa, razlike u verzijama datasetova, problemi s certifikatima). U završnoj fazi dominiraju produkcijski i operativni rizici (npr. razlike između UAT i produkcije, nepripremljene procedure oporavka, nedostatak jasnih uputa za kontakt centar).

Kategorizacija je također važna zbog buduće nadogradivosti. Iako je trenutni opseg isključivo cestovni promet unutar Republike Hrvatske, arhitektura se planira modularno kako bi sutra omogućila proširenje (npr. tranzit ili drugi oblici prijevoza) bez lomljenja postojećih podataka. Tehnički rizik koji se tu javlja nije "implementirati sve odmah", nego osigurati da današnji modeli i sučelja ne zatvaraju vrata nadogradnji (npr. rigidno vezanje pošiljke na jednu operaciju bez mogućnosti pretovara).

U praksi, kategorije rizika koje se moraju kontinuirano pratiti su:

- Infrastruktura i okruženja: pogrešna dimenzioniranost VM resursa, mrežna segmentacija, storage performanse, razlike okruženja i konfiguracijski drift.
- Podaci i modeli: neusklađenost eFTI i eADR semantike, šifrarnici, validacije DG seta, jedinstvenost identifikatora i idempotentnost integracija.
- Integracije: stabilnost eFTI tokova (metapodaci i selective/full dohvat), eDelivery/AS4 konfiguracija, SOTAH i AFFINIS tokovi, povezivanje sa sustavima nadležnih tijela.
- Sigurnost: mapiranje identiteta i uloga, kontrola pristupa, zapisnici i audit, upravljanje certifikatima i tajnama, minimalne provjere sukladno NIS2.
- Operativnost: ponovljive instalacije i nadogradnje, jasnoća runbook procedura, edukacija superkorisnika i administratora, jednostavno praćenje integracijskih grešaka.

13.3. Rizici integracija i interoperabilnosti

Integracijski rizici su među najkritičnijima jer eADR ne funkcionira izolirano: AAP koristi podatke koji dolaze kroz eFTI tokove, eADR mora biti usklađen s DG informativnim setom, a analitika (AFFINIS) ovisi o konzistentnom dotoku podataka iz operativnih modula. Tipičan rizik u ovakvim sustavima nije samo "integracija ne radi", nego "integracija radi parcijalno", primjerice selective dohvat radi, ali full dohvat povremeno pada, ili dohvat radi, ali mapiranje identifikatora uzrokuje pogrešno povezivanje pošiljke i operacije.

Financira
Europska unija
NextGenerationEU

Posebno osjetljivo područje je upravljanje certifikatima i sigurnom razmjenom poruka/poziva. U on-premise okruženju i uz eDelivery/AS4 mehanizme, rizici se često pojavljuju u konfiguraciji partnera, rokovima važenja certifikata, dopuštenim kriptografskim postavkama i mrežnim pravilima. Ako se ti elementi ne potvrde dovoljno rano u TEST okruženju, problem se tipično otkrije tek u UAT-u ili pred produkciju, kada je vrijeme za korekcije ograničeno.

Integracije prema SOTAH-u i prema AFFINIS-u nose specifične rizike mapiranja i obrade. Kod SOTAH-a kritično je mapiranje vozila, tahografskog identifikatora i vozača (gdje je primjenjivo), te konzistentnost vremenskih opsega podataka. Kod AFFINIS-a kritično je da dnevne obrade ne stvaraju duplikate, da se "inkrementalni" učit radi ispravno, te da se greške mogu otkriti i ponoviti obrada bez ručnih intervencija nad produkcijskim podacima.

Praktične mjere ublažavanja integracijskih rizika moraju biti jednostavne, ali sustavne: ranije uspostavljanje integracijskih "smoke testova", standardizirani korelacijski identifikatori u logovima, te jasni scenariji grešaka koji su pokriveni testnim slučajevima. U provedbi to znači da se već u ranoj implementaciji uspostavlja minimalni end-to-end tok (eFTI metapodaci → AAP prikaz → selective dohvat DG seta), pa se zatim proširuje na full dohvat i dodatne tokove.

- Rizik: nedostupnost ili nestabilnost eFTI tokova u testnom okruženju zbog neusklađenih endpointa i mrežnih pravila. Mjera: u ranoj fazi potvrditi mrežnu povezivost i osnovni testni poziv; implementirati jasne timeout/retry postavke i logiranje uz korelacijski identifikator. • Rizik: razlike u verzijama datasetova ili kodnih lista uzrokuju pogrešne validacije DG seta. Mjera: verzionirati šifrarnike i validacijska pravila, te provoditi regresijske testove s istim skupom scenarija pri svakoj promjeni.
- Rizik: certifikati i kriptografske postavke (AS4/TLS) uzrokuju povremene prekide. Mjera: standardizirati postupak postavljanja i rotacije certifikata, te provoditi periodičnu provjeru roka važenja i osnovnu provjeru handshake-a u svim okruženjima.
- Rizik: integracija SOTAH ne vraća očekivane podatke zbog mapiranja identifikatora ili vremenskog opsega. Mjera: uvesti jasna pravila mapiranja i testirati s poznatim referentnim primjerima; logirati upit i odgovor u tehničkim zapisnicima (u skladu s pravilima zaštite podataka).
- Rizik: AFFINIS dnevna obrada stvara duplikate ili preskače podatke. Mjera: definirati minimalne kontrole konzistentnosti nakon obrade (broj zapisa, ključne agregacije), te postupak ponavljanja obrade bez ručnog mijenjanja podataka.

13.4. Rizici podatkovnih modela, šifrarnika i kvalitete podataka

Najveći podatkovni rizik u ovoj domeni nastaje kada se poslovni pojmovi ne modeliraju dovoljno precizno. Primjer je odnos pošiljke i operacije prijevoza: jedna pošiljka može biti pokrivena s više operacija (pretovari, promjena vozila), a jedna operacija može pokrivati više pošiljaka i više DG stavki. Ako se taj odnos pojednostavi (npr. pošiljka ima samo jednu operaciju), sustav brzo postaje neupotrebljiv u realnim situacijama i generira pogrešne zaključke u nadzoru.

Financira Europska unija NextGenerationEU

DG informativni set predstavlja zasebno osjetljivo područje. Rizik je da se DG podaci unesu ili dohvaćaju djelomično, neusklađeno ili bez jasne validacije, što može dovesti do pogrešne interpretacije opasne tvari (UN broj, ADR razred, ambalažna skupina, ograničenja tunela). U sustavu je nužno imati validacije koje sprječavaju očite pogreške i koje korisniku daju jasne poruke, jer se u suprotnom greška prenosi u nadzor i u analitiku.

Šifrarnici i statusi također nose rizik, posebno kada ih koristi više modula. Ako eADR i nacionalni eFTI čvor/gateway koriste različite kodne liste za iste pojmove ili ako se statusi različito tumače (npr. “u tijeku”, “završeno”, “otkazano”), dolazi do neusklađenih prikaza i pogrešnih izvještaja. U on-premise rješenju taj se rizik ublažava kroz centralizirano upravljanje referentnim podacima i kroz jasnu verzioniranost šifrarnika.

U podatkovne rizike spada i idempotentnost integracija i jedinstvenost identifikatora. Sustav mora tolerirati ponovljene poruke ili ponovljene dohvaćaje bez stvaranja duplikata ili nekonzistentnih veza. To je posebno važno za integracije koje mogu ponovno slati metapodatke ili za batch obrade prema analitici. Mjera ublažavanja nije složen sustav kontrole, nego pravilno postavljene jedinstvene ključeve, kontrolirane veze (npr. join tablice gdje je potrebno) i jasna pravila upisa.

- Rizik: pogrešno modeliranje pošiljka–operacija onemogućuje pretovare i složene rute. Mjera: u podatkovnom modelu osigurati mnogostruke veze pošiljke i operacije (join tablica), te testirati scenarije s više pošiljaka i više operacija prije UAT-a.
- Rizik: neusklađenost DG seta između eADR i eFTI rezultira nevaljanim ili nečitljivim podacima u AAP-u. Mjera: uskladiti polja DG seta s eFTI specifikacijama, uvesti minimalne validacije i automatizirane provjere mapiranja.
- Rizik: šifrarnici se razlikuju po modulima ili se ručno mijenjaju u produkciji. Mjera: šifrarnike održavati verzionirano i isporučivati kroz kontrolirani postupak nadogradnje; dokumentirati promjene i provoditi regresiju.
- Rizik: dupliciranje subjekata, vozila ili osoba zbog neusklađenih identifikatora (OIB, registracija, interni identifikatori). Mjera: definirati pravila jedinstvenosti i obvezne atribute; provoditi osnovne kontrole pri unosu i integracijskom upisu.
- Rizik: analitika dobiva nekonzistentne podatke zbog promjena modela ili nepotpunih transformacija. Mjera: definirati stabilni ugovor između operativnog sloja i AFFINIS-a, te provjeriti ključne agregacije nakon svake dnevne obrade.

13.5. Rizici sigurnosne implementacije i usklađenosti s NIS2 u tehničkoj provedbi

Sigurnosni rizici u tehničkoj provedbi najčešće nastaju iz pogrešnog mapiranja identiteta i ovlasti, te iz nedostatnog evidentiranja ključnih događaja. Sustav obuhvaća korisnike različitih uloga (nadzorna tijela, operateri registara, učilišta, ispitni centri, tijela izdavatelji, administratori), pri čemu svaki profil mora imati ograničen pristup isključivo funkcijama i

Financira
Europska unija
NextGenerationEU

podacima koji su nužni za njegov posao. Ako je model ovlasti preširok ili nedovoljno precizan, posljedica je ili sigurnosno neprihvatljivo izlaganje podataka ili praktično onemogućavanje rada korisnika.

U on-premise okruženju rizik je i konfiguracijski: TLS postavke, certifikati, upravljanje tajnama i mrežna segmentacija. Tehničke pogreške u tom području mogu rezultirati prekidima integracija (npr. zbog certifikata), ali i sigurnosnim slabostima (npr. preširoka dostupnost servisa u mreži). Budući da se sustav ne oslanja na cloud usluge, sve sigurnosne postavke moraju biti ispravno postavljene i provjerene unutar AKD podatkovnog centra, uz jasno definirane procedure rotacije i provjere.

Zapisnici događaja i audit predstavljaju ključnu komponentu i za sigurnost i za operativnost. Rizik je da sustav ne bilježi ono što je potrebno za dokazivost i za rješavanje incidenata: prijave i odjave, neuspjele prijave, dohvat osjetljivih podataka (npr. DG set i puni sadržaji), administrativne promjene u ovlastima, promjene konfiguracija integracija. Ako se audit ne postavi konzistentno od početka, naknadno ga je teško “dodati” bez utjecaja na sustav i bez rizika da ostanu rupe u sljedivosti.

Mjere ublažavanja moraju ostati jednostavne i praktične: jasno definirane uloge i prava, centralno prikupljanje zapisnika, osnovne provjere sigurnosnih postavki prije UAT-a i prije produkcije, te standardizirani postupci za rotaciju certifikata i tajni. Nije cilj uvesti složene sigurnosne mehanizme, nego osigurati minimalni sigurnosni standard koji je potreban za ovakav državni sustav i koji podržava NIS2 obveze.

- Rizik: pogrešno mapiranje uloga uzrokuje preširok pristup podacima. Mjera: definirati uloge po poslovnim funkcijama, provesti provjeru ovlasti kroz testne scenarije i uključiti superkorisnike u validaciju prije UAT-a.
- Rizik: audit ne bilježi ključne događaje pa nije moguće rekonstruirati tko je pristupao kojim podacima. Mjera: definirati minimalni skup audit događaja i provjeriti ih u TEST okruženju; centralno prikupljati zapisnike.
- Rizik: certifikati isteknu ili nisu konzistentno postavljeni po okruženjima. Mjera:

standardizirati postupak upravljanja certifikatima (postavljanje, rotacija, provjera roka), te uvesti osnovni podsjetnik/izvještaj o isteku.

- Rizik: izlaganje servisa izvan potrebnih mrežnih zona. Mjera: primijeniti mrežnu segmentaciju i allow-liste, te provjeriti dostupnost servisa samo iz potrebnih zona prije produkcije.
- Rizik: nekonzistentno upravljanje tajnama (lozinke, ključevi) otežava održavanje i povećava sigurnosni rizik. Mjera: koristiti centralizirani i kontrolirani način pohrane tajni u on-premise okruženju i ograničiti pristup na administratore koji moraju imati taj pristup.

Financira
Europska unija
NextGenerationEU

13.6. Rizici infrastrukture, okruženja i raspoloživosti u AKD podatkovnom centru

Infrastrukturni rizici u on-premise implementaciji najčešće su povezani s dimenzioniranjem, mrežom, storage performansama i razlikama između okruženja. Ako se VM resursi podcijene ili ako se ne provede osnovno opterećenje u testnim uvjetima, sustav može postati spor ili nestabilan upravo u fazi kada se provodi UAT ili kada počinje produkcijski rad. To je posebno važno za komponente koje obrađuju integracije i dohvat podataka, jer su osjetljive na latenciju i I/O.

Rizik "razlike okruženja" tipično se pojavljuje kada TEST/UAT ne odražavaju produkcijske uvjete (npr. drugačija mrežna pravila, drugačiji certifikati, drugačiji storage ili drugačija konfiguracija servisa). Posljedica je da se sustav ponaša drugačije u produkciji nego u testiranju, a problem se otkrije prekasno. Mjera ublažavanja je održavanje konzistentnih konfiguracijskih obrazaca i kontrolirani prijenos konfiguracija po okruženjima, uz jasno dokumentirane razlike koje su nužne (npr. endpointi i certifikati).

Backup i oporavak su dio infrastrukturne održivosti. Rizik nije samo "nema backup-a", nego "backup postoji, ali oporavak nije provjeren". U državnom on-premise sustavu minimalno je potrebno imati ponovljive procedure izrade sigurnosnih kopija i periodičnu provjeru povrata na kontrolirano okruženje. Bez toga, incidenti se rješavaju improvizacijom, što produžuje prekid rada i povećava mogućnost gubitka podataka.

Raspoloživost i kontinuitet rada moraju se promatrati kroz ključne servise: AAP i Gate (nadzor), eADR (registri, osposobljavanje, dopuštenja), integracijski sloj (eDelivery/AS4 i konektori), baze podataka i log-kolektor. Mjere ublažavanja trebaju biti u skladu s jednostavnošću održavanja: osnovni monitoring i alarmiranje, standardizirano ponovno pokretanje servisa, jasna procedura failovera gdje je predviđena, te provjere integriteta nakon oporavka.

- Rizik: nedovoljna dimenzioniranost VM resursa uzrokuje spor rad AAP-a i integracija. Mjera: osloniti se na procjenu kapaciteta i definirati minimalni bazni profil resursa; provesti osnovno opterećenje prije UAT-a.
- Rizik: storage I/O postaje usko grlo za baze i zapisnike. Mjera: definirati očekivane I/O profile, postaviti monitoring (latencija, IOPS) i provesti testove s realističnim scenarijima dohvaćanja.
- Rizik: razlike u mreži i certifikatima između UAT i produkcije uzrokuju probleme pri go-live. Mjera: uspostaviti checklistu produkcijske spremnosti koja uključuje mrežne i certifikacijske provjere u svim okruženjima.
- Rizik: backup nije moguće vratiti u razumnom vremenu ili je povrat nekompletan. Mjera: periodično provoditi test povrata na kontroliranu instancu i dokumentirati postupak kao dio runbook-a.
- Rizik: nedostatak centralnog pregleda stanja sustava produžuje rješavanje problema. Mjera:

Financira Europska unija NextGenerationEU

uvesti osnovni monitoring i centralno prikupljanje zapisnika s jasnim korelacijskim identifikatorima za integracije.

13.7. Rizici testiranja, prihvata i puštanja u rad

Rizici testiranja najčešće nastaju kada testni scenariji nisu dovoljno realistični ili kada se testiranje usmjeri na pojedinačne ekrane, a ne na end-to-end tokove koji su stvarno potrebni u radu. U ovom projektu ključni tokovi uključuju: nadzor kroz AAP s dohvatom DG seta, eADR procese osposobljavanja i izdavanja dopuštenja, te integracijske tokove prema SOTAH-u i analitici. Ako se ti tokovi ne testiraju kao cjelina, greške se otkrivaju tek u UAT-u ili u produkciji.

UAT nosi specifičan rizik zbog ovisnosti o raspoloživosti korisnika nadležnih tijela i operatera. Ako sustav uđe u UAT s nedovršenim integracijama ili nestabilnim funkcionalnostima, UAT se pretvara u rješavanje tehničkih problema umjesto u provjeru poslovne upotrebljivosti. Zato UAT mora imati jasne ulazne kriterije: integracijsko testiranje završeno, kritične greške zatvorene, ovlasti i audit postavljeni minimalno ispravno, te pripremljeni testni podaci koji pokrivaju realne situacije (više pošiljaka, pretovari, više DG stavki).

Puštanje u rad (go-live) nosi rizike konfiguracije i prijelaza, posebno u on-premise okruženju gdje je potrebno pravilno postaviti produkcijske certifikate, mrežna pravila i parametre integracija. Mjera ublažavanja nije složen proces, nego jasno definiran kontrolni popis za produkcijsku spremnost i dogovoren postupak povratka na prethodno stanje u slučaju da se kritični tokovi ne mogu potvrditi nakon puštanja u rad. Takav postupak mora biti provježban barem u kontroliranom okruženju prije produkcije.

Nakon go-live mora postojati kratko razdoblje stabilizacije u kojem se sustav pojačano prati i u kojem se otklanjaju uočene greške bez širenja opsega. Rizik u ovoj fazi je da se u stabilizaciji počnu uvoditi nove funkcije ili neplanirane promjene, što destabilizira sustav i otežava dokazivost. Mjera je da se stabilizacija vodi isključivo kao otklanjanje nedostataka i podešavanje konfiguracija, uz regresijske provjere ključnih tokova.

- Rizik: testni scenariji ne pokrivaju složene realne slučajeve (više pošiljaka, pretovari, više destinacija). Mjera: koristiti scenarije koji eksplicitno uključuju takve slučajeve i provoditi ih prije UAT-a.
- Rizik: UAT kasni jer su integracije nestabilne ili jer testni podaci nisu spremni. Mjera: definirati ulazne kriterije za UAT i osigurati da su testni podaci i osnovni tokovi potvrđeni u TEST okruženju.
- Rizik: razlika konfiguracije između UAT i produkcije uzrokuje probleme pri go-live. Mjera: koristiti kontrolirani prijenos konfiguracija i provesti produkcijsku validaciju (mreža, certifikati, integracije) prije puštanja u rad.
- Rizik: nedostatak jasnog postupka povratka otežava reakciju na kritične probleme nakon golive. Mjera: definirati minimalni rollback pristup za aplikacijske artefakte i konfiguracije, te ga provjeriti u kontroliranom okruženju.

Financira
Europska unija
NextGenerationEU

- Rizik: stabilizacija se pretvara u razvoj novih zahtjeva i destabilizira sustav. Mjera: ograničiti stabilizaciju na korekcije i podešavanja, uz obaveznu provjeru ključnih tokova nakon svake promjene.

13.8. Rizici održavanja i nadogradnji nakon puštanja u rad

Nakon puštanja u rad, rizici se pomiču s implementacije na održivost. Najčešći rizik u onpremise sustavima je konfiguracijski drift, odnosno postupne ručne promjene po poslužiteljima i okruženjima koje nisu dokumentirane i nisu ponovljive. Posljedica je da se sljedeća nadogradnja ne može provesti predvidljivo ili da se problem ne može reproducirati u TEST/UAT okruženju. Mjera ublažavanja je da se konfiguracije vode kontrolirano i da se promjene provode kroz standardizirani postupak, uz jasno evidentirane parametre po okruženjima.

Dokumentacija i edukacija su dio održivosti sustava. Rizik je da dokumentacija ostane na stanju "iz vremena implementacije" i da se ne ažurira uz nadogradnje, što s vremenom dovodi do pogrešnih operativnih postupaka i opterećenja administratora. Mjera ublažavanja je povezati dokumentaciju s izdanjima sustava: kada se promijeni sučelje, validacija ili integracija, mora se ažurirati pripadajući dio uputa i runbook-a, te minimalno osvježiti superkorisnike.

Specifičan operativni rizik su certifikati i promjene u vanjskim specifikacijama (npr. verzije datasetova i kodnih lista, ažuriranja šifrarnika). U praksi, problemi se često događaju na rokovima važenja certifikata ili na promjenama kodnih lista koje utječu na validacije. Mjere ublažavanja su jednostavne: postupak rotacije certifikata, periodična provjera isteka, te kontrolirani postupak ažuriranja šifrarnika i validacija kroz izdanje sustava, uz regresijsku provjeru na poznatim scenarijima.

Održavanje analitike (AFFINIS) nosi dodatni rizik jer batch obrade mogu "tiho" prestati raditi ili početi davati nekonzistentne rezultate. Mjera ublažavanja je osnovno dnevno praćenje statusa obrade i nekoliko jednostavnih provjera konzistentnosti (broj zapisa, ključne agregacije), uz jasno definiran postupak ponavljanja obrade kada je potrebno. Cilj je da se problemi uoče rano i da se mogu riješiti bez ručnih intervencija nad podacima.

- Rizik: konfiguracijski drift otežava nadogradnje i rješavanje problema. Mjera: konfiguracije i parametre po okruženjima voditi kontrolirano, uz standardizirani postupak promjene i minimalnu provjeru nakon promjene.
- Rizik: dokumentacija i edukacijski materijali zastare i više ne odgovaraju sustavu. Mjera: povezati dokumentaciju s izdanjima i osvježiti superkorisnike pri svakoj promjeni koja utječe na postupanje korisnika ili administraciju.
- Rizik: certifikati isteknu i prekidaju integracije. Mjera: uvesti jednostavnu periodičnu provjeru roka važenja i standardnu proceduru rotacije, testiranu u kontroliranom okruženju.
- Rizik: promjene kodnih lista i validacija uzrokuju neočekivane greške u DG setu. Mjera:

Financira Europska unija NextGenerationEU

promjene uvoditi kroz verzionirane šifrarnike i provesti regresiju na standardnim scenarijima prije produkcije.

- Rizik: AFFINIS obrade prestanu raditi ili daju nekonzistentne rezultate bez da se odmah uoči. Mjera: pratiti status obrade i provoditi osnovne provjere konzistentnosti nakon svakog ciklusa, uz definirani postupak ponavljanja obrade.

14. Isporuke i očekivani rezultati projekta

U okviru projekta „Praćenje prijevoza opasnih tvari u cestovnom prometu eADR" isporuke se definiraju kao skup provjerljivih rezultata rada koji omogućavaju: (1) nabavu i implementaciju produkcijskog rješenja u AKD podatkovnim centrima, (2) uspostavu i operativni rad eADR procesa za cestovni promet opasnih tvari u Republici Hrvatskoj, te (3) provedbu nadzora i razmjenu podataka u skladu s eFTI okvirom.

Druga razina su isporuke koje nastaju tijekom implementacije i puštanja u rad (instalirano rješenje, konfigurirana okruženja, integracije, testni rezultati, korisničke upute i operativna dokumentacija).

Očekivani rezultati projekta su mjerljivi učinci koji proizlaze iz navedenih isporuka: digitalizirani i standardizirani postupci vezani uz prijevoz opasnih tvari, pouzdana dostupnost podataka nadležnim tijelima tijekom nadzora, te jedinstven i nadogradiv informacijski temelj za operativno upravljanje, analitiku i izvještavanje u okviru nacionalnog obuhvata (cestovni promet u RH).

Radi praktične provedbe i kasnijeg održavanja, isporuke se definiraju tako da su: (1) jednoznačne i verzionirane, (2) dovoljno detaljne za nabavu bez dodatnih „prevođenja" zahtjeva, te (3) usklađene s on-premise okruženjem i postojećim državnim sustavima i servisima koji su u projektnom obuhvatu (npr. autentifikacija putem eGrađanin gdje je primjenjivo, povezivanje sa sustavima tahografa i analitičkom platformom te integracije prema nadležnim tijelima).

14.1. Isporuke u fazi implementacije i puštanja u rad produkcijskog rješenja

U fazi implementacije isporuke su prvenstveno „opipljive" i provjerljive: instalirano i konfigurirano rješenje u predviđenim okruženjima, implementirane integracije, te provedeni testovi s dokumentiranim rezultatima. U ovoj fazi je važno da svaka isporuka bude vezana uz prethodno definirane zahtjeve i da se može prihvatiti na temelju stvarnog rada sustava, a ne na temelju deklaracija.

Produkcijsko rješenje se isporučuje kao skup aplikacijskih modula i servisa koji pokrivaju ključne funkcionalnosti eADR sustava: registri, evidencije postupaka nadzora, upravljanje

Financira Europska unija NextGenerationEU

podacima o pošiljkama i stavkama opasnih tvari, povezivanje s relevantnim sustavima (npr. tahografski sustavi i analitika), te pružanje funkcionalnosti nadležnim tijelima za provedbu nadzora u cestovnom prometu.

Uz aplikacijske module, obvezna isporuka je i implementacija podatkovnog sloja: fizički model baze podataka, migracijski skripti (gdje su potrebni), inicijalni referentni podaci, te jasna pravila o retenciji i arhiviranju podataka u skladu s potrebama operativnog rada i nadzora. Posebno je važno da su u podatkovnom sloju jasno odvojeni poslovni podaci eADR sustava od vanjskih skupova podataka (npr. tahografski podaci koji se ne pohranjuju trajno u eADR sustavu, nego se dohvaćaju iz specijaliziranih sustava).

Za puštanje u rad potrebno je isporučiti i minimalni operativni paket: konfiguracija nadzora rada sustava, prikupljanje zapisnika događaja radi otklona poteškoća i osnovne sigurnosti, te postupci sigurnosnog kopiranja i oporavka u skladu s on-premise operativnim modelom. Ovaj paket mora biti dovoljno jednostavan za svakodnevno održavanje bez uključivanja dodatnih vanjskih dionika, uz jasno definirane odgovornosti između naručitelja i izvođača.

- Instalacijski i konfiguracijski paket rješenja: Jasno strukturirani artefakti za instalaciju aplikacije i pripadajućih servisa u on-premise okruženju, uključujući konfiguracijske datoteke, parametre i upute za postavljanje u svim okruženjima.

- Implementirane integracije i adapteri: Tehnički realizirana sučelja prema predviđenim sustavima (npr. tahografski sustavi, analitika, relevantni registri), s mogućnošću nadzora statusa integracije i osnovnim mehanizmima ponovnog pokušaja u slučaju privremenih grešaka.

- Podatkovni sloj i migracije: Implementirana baza podataka (klaster), sheme, indeksi, procedure, inicijalni šifrarnici i referentni podaci, te eventualne migracije podataka (ako su predviđene), uz provjeru integriteta i konzistentnosti.

- Testni paket s rezultatima: Dokumentirani rezultati sustavnog testiranja, integracijskog testiranja, sigurnosnog testiranja u mjeri potrebnoj za puštanje u rad, te korisničkog prihvatnog testiranja, uz jasne zapise što je testirano i s kojim ishodom.

- Operativni paket za rad i održavanje: Upute za administratore, osnovni postupci nadzora, sigurnosne kopije i oporavka, te minimalne operativne provjere koje omogućavaju stabilan rad bez složenih i teško održivih procedura.

Zaštita podataka mora osigurati da je svaki osobni podatak i povjerljiva informacija šifrirana tijekom prijenosa između mrežnih zona te tijekom pohrane na vanjske medije i u mirovanju. Posebne kategorije osobnih podataka i poslovne tajne moraju biti šifrirane tijekom cijele pohrane u bazama podataka, a dešifriranje se smije provoditi samo tijekom minimalnog vremena potrebnog za obradu, unutar sigurnog i kontroliranog mrežnog okruženja. Metode i procesi šifriranja moraju biti dokumentirani i testirani.

Financira
Europska unija
NextGenerationEU

Kada je potrebno prema procjeni rizika, moraju se primijeniti tehnike pseudonimizacije i anonimizacije. Poveznice ili dodatne informacije koje omogućuju ponovno povezivanje pseudonimiziranih podataka s ispitanikom moraju se čuvati odvojeno i štititi tehničkim i organizacijskim mjerama. Korištene metode pseudonimizacije/anonimizacije moraju biti dokumentirane i testirane.

Ako se obrađuju osobni podaci, moraju se isporučiti evidencije obrade i, kada su ispunjeni kriteriji (npr. profiliranje, osjetljivi podaci, opsežna obrada, nove tehnologije ili praćenje), procjena učinka i procjena rizika obrade. Sustav mora imati definirane rokove čuvanja, metode brisanja/uništavanja, automatizirano brisanje nakon isteka roka te dokaze (logove) o brisanju. Postupci brisanja moraju biti dokumentirani, a kvartalno se mora provjeriti da su podaci pravovremeno obrisani. Arhiva mora biti zaštićena integritetom, mogućnošću pretraživanja, šifriranjem povjerljivih podataka i zahtjevom autentikacije te mora postojati popis arhivske građe s rokovima čuvanja.

14.2. Očekivani poslovni rezultati projekta

Primarni poslovni rezultat projekta je uspostava jedinstvenog digitalnog postupanja za područje opasnih tvari u cestovnom prometu u Republici Hrvatskoj, s naglaskom na dostupnost i standardizaciju podataka koje nadležna tijela trebaju tijekom nadzora. Time se smanjuje ovisnost o papirnatoj dokumentaciji i neujednačenim praksama, te se uvodi jednoznačan način prikaza i korištenja podataka.

Dodatni poslovni rezultat je povećanje učinkovitosti nadzornih postupaka. Nadležna tijela dobivaju mogućnost da na temelju jedinstvenih registara i strukturiranih podataka o pošiljkama i stavkama opasnih tvari brže pripreme i provedu nadzor, uz manji broj ručnih provjera i smanjenu potrebu za višestrukim prepisivanjem podataka.

Projekt također stvara standardizirani temelj za koordinaciju između različitih korisničkih skupina unutar nacionalnog okvira: prijevoznici, vozači, obrazovne institucije i ispitni centri, te tijela koja izdaju dopuštenja i provode nadzor. Očekivani rezultat je da svaka uloga koristi isti “izvor istine” za podatke koji su relevantni za njezin dio procesa, uz jasno definirana prava pristupa.

Konačno, očekuje se da će projekt omogućiti jednostavno i dosljedno izvještavanje o ključnim operativnim pokazateljima (npr. osnovne statistike o nadzorima, vrstama opasnih tvari po razredima, učestalosti provjera i sličnim indikatorima), bez uvođenja složenih i teško održivih evidencija. Izvještavanje se postavlja kao praktičan alat za upravljanje sustavom i planiranje nadzornih aktivnosti.

- Digitaliziran nadzor i ujednačen prikaz podataka: Nadležna tijela dobivaju standardiziran prikaz ključnih podataka o prijevozu opasnih tvari, što skraćuje vrijeme nadzora i smanjuje mogućnost pogrešnog tumačenja.

Financira
Europska unija
NextGenerationEU

- Jedinstveni registri i konzistentnost: Podaci o subjektima, vozilima, vozačima, dopuštenjima i osposobljavanjima dostupni su kroz jedan sustav i povezani su kroz jasno definirane relacije, čime se izbjegavaju paralelne evidencije.

- Operativna podrška procesima: Sustav podržava tipične tijekove rada (prijava i provođenje tečajeva, ispiti, izdavanje potvrda, izdavanje dopuštenja, vođenje nadzornih predmeta), uz jasno definirane uloge i odgovornosti.

- Osnovna analitika i statistike: Uspostavlja se temelj za jednostavne operativne izvještaje i, gdje je predviđeno, povezivanje s analitičkom platformom za složenije analize bez opterećenja operativnog sustava.

14.3. Očekivani tehnički rezultati projekta

Tehnički rezultat projekta je implementirano, stabilno i skalabilno on-premise rješenje koje radi u virtualiziranom okruženju AKD podatkovnih centara i podržava ključne funkcionalnosti bez oslanjanja na vanjske usluge u oblaku. Tehnička arhitektura mora podržavati odvojena okruženja (razvojno, testno, korisničko prihvatno i produkcijsko) kako bi se promjene mogle uvoditi kontrolirano i bez rizika za produkcijski rad.

Sustav mora osigurati pouzdanu razmjenu podataka s relevantnim sustavima u opsegu projekta. To uključuje stabilne integracijske tokove, jasne mehanizme autentifikacije i autorizacije, te jednoznačno definirane formate poruka i podatkovne strukture, posebno za skup podataka o opasnim tvarima u eFTI okviru. Očekivani tehnički rezultat je da integracije nisu ad-hoc, nego su standardizirane i dokumentirane do razine koja omogućava održavanje i nadogradnje.

Tehnički rezultat je i jasno definiran podatkovni sloj: relacijski model za operativne registre i postupke, uz mogućnost dugoročnog razvoja i proširenja (npr. dodatni podskupovi eFTI podataka ili dodatni procesni moduli). U implementaciji se očekuje dosljedno provođenje pravila konzistentnosti podataka, kao i razumna razina optimizacije za svakodnevni rad nadzora (brzi dohvat, filtriranje, pregled povijesti predmeta i sl.).

Minimalni tehnički rezultat za operativnost uključuje postavljen nadzor dostupnosti i osnovnih performansi sustava, centralizirano prikupljanje zapisnika događaja radi otklona poteškoća i sigurnosnih potreba, te provedene sigurnosne kopije i mogućnost oporavka. Ove funkcionalnosti moraju biti implementirane tako da su jednostavne za administriranje i ne uvode složene operativne procese koji bi otežavali održavanje.

- On-premise produkcijska instalacija u dva podatkovna centra: Rješenje je postavljeno u skladu s potrebama visoke raspoloživosti i kontinuiteta rada, uz jasno definirane komponente i način preuzimanja rada u slučaju ispada jedne lokacije.

Financira
Europska unija
NextGenerationEU

- Standardizirana sučelja i verzioniranje API-ja: Integracije su stabilne, dokumentirane i verzionirane, kako bi se promjene mogle uvoditi bez prekida rada nadležnih tijela i poslovnih korisnika.

- Podatkovni model spreman za rast: Operativni podaci eADR sustava čuvaju se strukturirano i s mogućnošću proširenja, uz jasno odvajanje od vanjskih skupova podataka koji se dohvaćaju iz drugih sustava.

- Osnovni operativni alati: Nadzor rada sustava, zapisnici događaja i sigurnosne kopije postavljeni su kao standardna operativna sposobnost sustava, a ne kao dodatni „projekt u projektu".

14.4. Prihvat isporuka i način dokazivanja izvršenja

Prihvat isporuka mora biti organiziran tako da je jednostavan, ponovljiv i nedvosmislen. Svaka isporuka mora imati: jednoznačan naziv, verziju, datum predaje, opis sadržaja i popis promjena u odnosu na prethodnu verziju. Time se osigurava da su isporuke provjerljive i da se tijekom projekta izbjegne situacija u kojoj se raspravlja o tome „što je točno dogovoreno".

Za isporuke dokumentacije, prihvat se provodi kroz stručni pregled od strane naručitelja i vraćanje komentara u strukturiranom obliku (npr. popis primjedbi i prijedloga). Prihvat dokumentacije se potvrđuje tek kada je uključen dogovoreni krug izmjena i kada dokumenti postanu dovoljno stabilni da se mogu koristiti u **implementaciji, produkcijskom radu i održavanju** bez dodatnih interpretacija.

Za isporuke implementacije (u fazi puštanja u rad) prihvat se provodi kroz testne scenarije i validacijske postupke definirane ranije u dokumentaciji. Prihvat se temelji na stvarnim rezultatima (npr. zapisnici o testiranju, zapisnici o uspješnim integracijskim tokovima, dokaz da su ključne funkcionalnosti dostupne korisnicima), pri čemu se izbjegava nepotrebno kompliciranje dokazivanja i administrativno opterećenje.

U okviru ugovora o **razvoju i implementaciji** sustava, izvršenje se potvrđuje zapisnikom o prihvatu isporuka. Uz zapisnik se prilaže popis isporučenih stavki i sažetak aktivnosti u promatranom razdoblju:

- Kontrolne liste za prihvat: Za svaku isporuku se koristi kratka kontrolna lista koja potvrđuje da su ispunjeni ključni formalni i sadržajni kriteriji (verzija, potpuna struktura, obuhvat zahtjeva, ažuriran rječnik pojmova i sl.).

- Dokaz ispunjenja zahtjeva kroz testove: Svaki ključni zahtjev ima pridruženi testni scenarij i očekivani rezultat, a prihvat se temelji na dokumentiranom ishodu, ne na opisima ili prezentacijama.

- Zapisnik o izvršenim uslugama: Dokument koji formalno potvrđuje izvršenje usluge i preuzimanje isporuka, uz popis predanih artefakata i kratki opis provedenih aktivnosti.

Financira
Europska unija
NextGenerationEU

- Minimalno periodično izvještavanje: Jednostavan pregled napretka i predanih isporuka (npr. mjesečno), bez uvođenja složenih upravljačkih procedura i dodatnih opterećenja za operativni tim.

14.5. Isporuke koje osiguravaju održivost i nadogradivost rješenja

Održivost rješenja se osigurava tako da se ključna znanja i odluke ne zadržavaju u glavama pojedinaca, nego su ugrađena u dokumentaciju i strukturu sustava. Isporuke moraju uključivati jasan rječnik pojmova, standardizirane nazive i šifrarnike, te pravila versioniranja koja omogućavaju kontrolirane promjene bez gubitka kompatibilnosti.

Nadogradivost se osigurava modularnim pristupom: poslovne cjeline (registri, nadzori, osposobljavanje, dopuštenja, integracije) trebaju biti odvojene tako da se mogu razvijati i širiti bez „rušenja" sustava. U kontekstu eFTI, posebno je važno da su podatkovni skupovi i razmjena podataka definirani tako da je moguće dodavati nove podatkovne elemente ili podskupove, bez promjene temeljnih načina pristupa i autorizacije.

Operativna održivost zahtijeva i minimalan, ali kompletan skup administratorskih uputa: kako nadzirati servis, kako provjeriti integracije, kako postupiti u slučaju zastoja, te kako provesti rutinske aktivnosti poput izmjene konfiguracije ili uvođenja nove verzije. Upute moraju biti pisane u skladu s on-premise modelom rada i organizacijom održavanja, bez oslanjanja na vanjske pružatelje usluga koji nisu dio projektnog opsega.

Konačno, održivost se postiže i standardizacijom isporuka kroz vrijeme: svaka nova verzija rješenja mora imati bilješke o izdanju, popis promjena na sučeljima i podatkovnom modelu, te jasne upute za povrat na prethodnu verziju u slučaju potrebe. Ovi elementi se definiraju kao obvezni dio isporuka jer smanjuju složenost održavanja i ubrzavaju rješavanje poteškoća u produkciji.

Financira
Europska unija
NextGenerationEU

Pri tome je važno koristiti konzistentne:

- Rječnike pojmova i šifrarnike: Jedinstveni popis pojmova i šifri koji se koristi u sustavu, dokumentaciji i sučeljima, kako bi svi korisnici i sustavi tumačili podatke jednako.
- Pravila verzioniranja i kompatibilnosti: Definicija kako se mijenjaju sučelja, podatkovni model i konfiguracija, uz jasno označavanje promjena koje utječu na korisnike ili integracije.
- Administratorske upute i operativne provjere: Jednostavne i provjerljive procedure za svakodnevni rad (provjera servisa, provjera integracija, osnovna dijagnostika), bez složenih i teško održivih procesa.
- Bilješke o izdanju i evidencija promjena (changelogs): Sažetak promjena po izdanju, s fokusom na utjecaj na korisnike, integracije i podatkovni model, kako bi održavanje bilo predvidivo i kontrolirano.

ZA PONUDITELJA

Financira Europska unija
NextGenerationEU