



Развој система за аутоматизацију процеса издавања података о техничким карактеристикама возила



Садржај

1	Увод.....	3
2	Дефиниције и скраћенице	4
3	Функционалности система	5
3.1	Улоге и корисници система.....	5
3.2	Лабораторије.....	6
3.3	Аутоматизован послови процес	6
3.3.1	Креирање захтева/предмета	6
3.3.2	Обрада захтева и израда података о техничким карактеристикама	7
3.3.3	Провера издатих података	7
3.3.4	Измена и дорада података.....	8
3.3.5	Остали захтеви везани за аутоматизован пословни процес	8
3.3.5.1	Повлачење захтева	8
3.3.5.2	Прерасподела задатака	8
3.3.5.3	Измена и дорада издатих података.....	8
3.3.5.4	Обавештења	8
4	Технички захтеви система	9
4.1	Архитектура система.....	9
4.2	Скалабилност.....	9
4.3	Висока доступност.....	9
4.4	Безбедност и заштита података.....	10
4.4.1	Cloud Web Application Firewall (WAF).....	10
4.4.2	DDoS заштита.....	11
4.5	Остали захтеви	11

1 Увод

Агенција за безбедност саобраћаја (Агенција, у даљем тексту) представља кључну институцију за имплементацију регулативе везане за безбедност саобраћаја у Републици Србији. За својих 15 година постојања Агенција се истакла својим софтверским решењима, обезбеђујући дигитализован и ефикасан процес рада свим ученицима на тржишту саобраћаја, почевши од овлашћених правних лица за испитивање возила, радионица и техничких прегледа, преко ауто-школа и тренинг центара до професионалних возача. Агенција за безбедност саобраћаја пружа виталне информације како јавности кроз свој портал саобраћајних података, тако и државним институцијама као што је Министарство за саобраћај и Министарство унутрашњих послова.

Идеја јесте да се овим софтверским решењем обезбеди комуникација и синхронизован рад између овлашћених правних лица које врше испитивање возила (у даљем тексту: лабораторије), правног лица које ће да доставља податке о техничким карактеристикама возила (у даљем тексту: правно лице) и АБС-а. За свако појединачно возило издају се подаци на начин да се захтев подноси преко овлашћених Лабораторија, а правно лице доставља податке о техничким карактеристикама возила АБС-у која надзире, контролише и издаје податке за конкретно возило.

Очекивани резултати пројекта укључују:

- Оптимизацију и аутоматизацију пословних процеса који утичу на рад Агенције
- Смањење ризика од губитка докумената
- Обезбеђивање централне локације (система) преко којег ће се спроводити процес
- Формирање квалитетне и функционалне базе о техничким карактеристикама возила



2 Дефиниције и скраћенице

Дефиниција / скраћеница	Опис
АБС	Агенција за безбедност саобраћаја
Агенција	Агенција за безбедност саобраћаја

Табела 1 дефиниције и скраћенице

3 Функционалности система

У наредним поглављима дат је преглед функционалности које будући систем треба да задовољава.

3.1 Улоге и корисници система

Корисници будућег система су:

- Овлашћена правна лица која врше испитивање возила (лабораторије)
- Запослени у правним лицима које обављају послове испитивања возила
- АБС
- Запослени у АБС-у
- Овлашћено правно лице
- Запослени у овлашћеном правном лицу

Улоге које систем треба да подржи су:

- Супер администратор – лице које је запослено у АБС-у. Супер администраторима треба обезбедити следеће функционалности:
 - Претрагу, преглед, креирање, активирање/деактивирање лабораторија
 - Претрагу, креирање, активирање/деактивирање корисничких налога за све улоге у систему
 - Претрагу, креирање, активирање/деактивирање корисничких налога овлашћених лица која издају податке о техничким карактеристикама возила као и запослених у АБС-у
- Корисник из АБС-а, коме треба обезбедити следеће функционалности:
 - Претрагу, преглед предмета који се налазе у систему
 - Одобравање или неодобравање издавања података о техничким карактеристикама возила
- Администратор лабораторије – лице ван АБС-а. Администратору лабораторије треба обезбедити следеће функционалности:
 - Претрагу, преглед предмета који се налазе у систему за припадајућу лабораторију
 - Претрагу, креирање, активирање/деактивирање корисничких налога за улогу „Корисник из лабораторије“
- Корисник из лабораторије – лице запослено у лабораторији. Кориснику треба обезбедити следеће функционалности:
 - Креирање предмета/захтева за издавање података о техничким карактеристикама возила
 - Претрагу, преглед предмета који се налазе у систему за припадајућу лабораторију
- Овлашћено лице за издавање података о техничким карактеристикама возила – лице ван АБС-а. Кориснику треба обезбедити следеће функционалности:
 - Претрагу предмета који се налазе у систему
 - Рад на предметима у систему

Приступ систему могу имати само регистровани корисници, преко својих корисничких налога. Корисничке налоге креира корисник који се налази у некој од администраторских улога. Приликом креирање корисничког налога, администратор уноси:

- Име корисника
- Презиме корисника
- Е-маил адреса
- Категорија – корисник мора припадати једној од категорија корисника.

- Уколико се као категорија одабере „Супер администратор“ није потребно уносити додатне податке
- Уколико се као категорија одабере „Администратор лабораторије“ или „Корисник из лабораторије“ потребно је одабрати компанију и испитно место за које се кориснички налог региструје

Након потврде уноса, корисник на наведену е-маил адресу стиже обавештење да је потребно активирати налог у систему уносом лозинке. Након уноса лозинке, налог постаје активан.

Корисник мора да има могућност промене лозинке.

3.2 Лабораторије

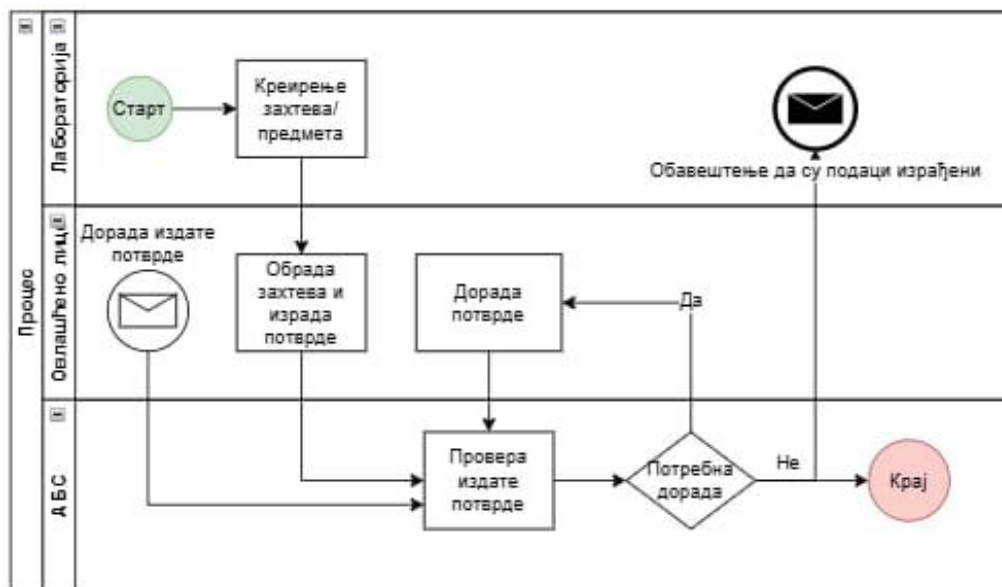
У систему је потребно евидентирати лабораторије. Податке о лабораторијама одржавају корисници у категорији „Супер администратор“. Приликом креирања нове лабораторије корисник уноси:

- Назив
- Адресу
- Контакт телефон
- Е-маил адресу
- Статус (активна/неактивна)

Корисницима у улози „Супер администратор“ треба омогућити претрагу лабораторија по називу.

3.3 Аутоматизован послови процес

Дијаграм тока пословног процеса дат је на слици испод.



Илустрација 1 – аутоматизован пословни процес

3.3.1 Креирање захтева/предмета

Запослени у лабораторији креира захтев/предмет за издавање података о техничким карактеристикама возила.

Запослени приликом креирање захтева уноси податке који се налазе на произвођачкој плочици или налепници која се налази на возилу. Скуп података који уноси укључује најмање следеће податке:

- Назив произвођача
- ЕУ број одобрења типа (European Community (EC) type-approval number)
- Идентификациону ознаку возила (VIN)
- Највећу дозвољену масу возила
- Највећа дозвољена осовинска оптерећења

Поред ових, запослени уноси и податке са иностране саобраћајне дозволе, који укључује:

- Назив произвођача
- Марку и тип
- Идентификациону ознаку возила (VIN)
- Масу празног возила
- Највећу дозвољену масу возила
- Највећа дозвољена осовинска оптерећења
- Датум прве регистрације
- Снагу мотора (за моторна возила)
- Запремину мотора (за моторна возила)
- Погонско гориво (за моторна возила)

Као прилог захтеву, запослени на систем поставља фотографије произвођачке плочице или налепнице, као и иностране саобраћајне дозволе.

Потврдом уноса, систем креира захтев/предмет у систему и прослеђује га на даљу обраду.

3.3.2 Обрада захтева и израда података о техничким карактеристикама

Поднети захтеви се налазе на систему. Овлашћена лица приступају систему и врше увид у пристигле захтеве. Овлашћено лице утврђује да ли захтев одговара опсегу посла којим који је у његовој надлежности. Уколико утврди да се захтев односи на опсег посла којим је у његовој надлежности, овлашћено лице „преузима“ обраду захтева на себе, што јасно назначавачу у систему.

Процес утврђивања тачности достављених података на захтеву и њихову проверу врши ван система. Овлашћено лице израђује податке о техничким карактеристикама ван система и прилаже је у предмет у систему.

Овлашћено лице у систему означава да је завршило рад на предмету, чиме се предмет прослеђује даље у пословни процес.

3.3.3 Провера издатих података

Издати подаци који нису верификовани од стране АБС се налазе у систему. Запослени АБС приступају систему и врше увид у пристигле податке. Запослени АБС означава да је преузео проверу података на себе.

Запослени АБС-а врши проверу издатих података. Евентуално додатно евидентирање података врши ван система.

Запослени завршава рад у овом кораку на један од следећа два начина:

- Потврдом исправности података чиме се пословни процес завршава, а запослени у лабораторији која је иницирала захтев добија обавештење о томе

- Захтевом за измену/дораду/допуну података – запослени АБС-а уноси разлоге због којих захтева измену/дораду/допуну података. Пословни процес се у овом случају наставља у кораку „Дорада потврде“.

3.3.4 Измена и дорада података

Овлашћено лице које је израдило податке добија задатак да измени/доради податке у складу са захтевом АБС-а. Након измене/дораде података пословни процес се враћа у корак „Провера издатих података“

3.3.5 Остали захтеви везани за аутоматизован пословни процес

3.3.5.1 Повлачење захтева

Запослени у лабораторији који је покренуо процес или Администратор лабораторије треба да имају могућност повлачења захтева уз унос разлога повлачења. Овом акцијом се пословни процес прекида уз слање е-маил обавештења свим дотадашњим учесницима.

3.3.5.2 Прерасподела задатака

Реално је могућ случај да запослени који је започео рад на предмету у неком кораку процеса буде спречен да га доведе до краја (нпр: одмор, боловање или друго одсуство са посла). У том случају Администратор лабораторије може да прерасподели задатак на неког од својих запослених. Супер администратор прерасподелу може да уради за запослене АБС и овлашћена лица.

3.3.5.3 Измена и дорада издатих података

Овлашћено лице за испитивање може извршити измену података након што је издат документ који садржи податке о техничким карактеристикама возила. Измењену потврду посебном акцијом ставља у исти предмет у коме су и иницијално издати подаци. Завршетком ове акције покреће се аутоматизован пословни процес у коме је први корак „Провера издатих података“. На даље се процес извршава на горе описан начин.

3.3.5.4 Обавештења

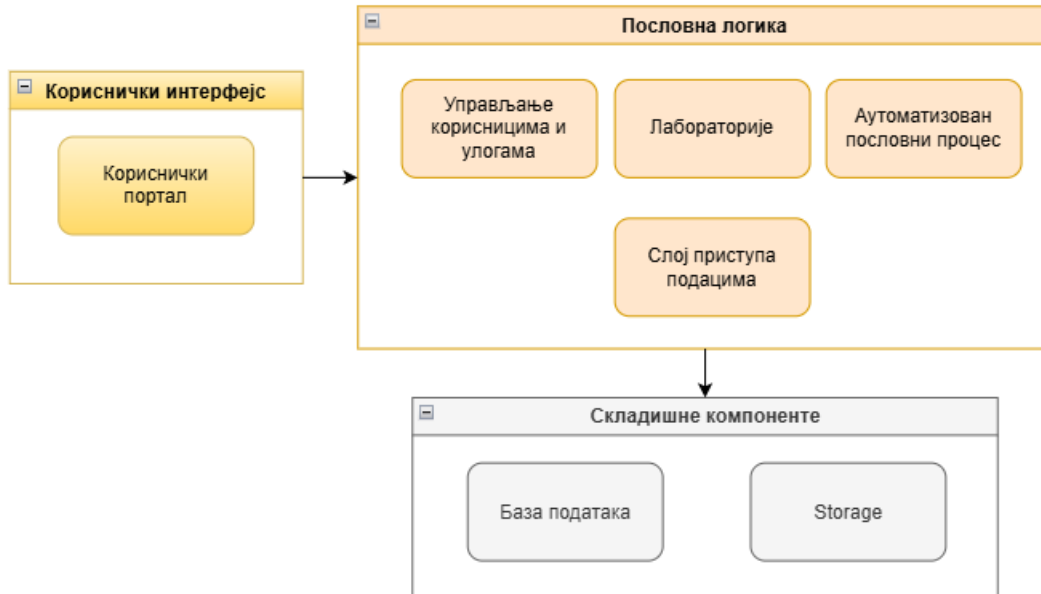
Систем треба да шаље аутоматска е-маил обавештења учесницима у процесу:

- Приликом преласка у наредни корак пословног процеса обавештење се шаље потенцијалним извршиоцима наредног корака пословног процеса
- Након завршетка пословног процеса обавештење се шаље подносиоцу захтева

4 Технички захтеви система

4.1 Архитектура система

На следећем дијаграму дата је high-level архитектура система.



Илустрација 2 high-level архитектура система

Кориснички портал намењен је корисницима система који учествују у пословном процесу. Приступ овом порталу ће имати искључиво ауторизовани корисници система. Комуникација која се одвија преко портала мора бити заштићена применом TLS протокол. Из технолошке перспективе, овај слој треба да буде развијен коришћењем React.js framework-а.

Слој пословне логике имплементира комплетну пословну логику система. Он служи као медијатор између корисничког портала и слоја података. Ово је централно место на коме су имплементирана пословна правила, калкулације и алгоритми. Овај слој врши проверу и валидацију података обезбеђујући проверу испуњености свих услова пре него што се подаци даље процесирају. Он имплементира и извршава пословна правила која дефинишу како се подаци креирају, складиште и мењају. Слој треба имплементирати као скуп засебних модула који као целину чине систем. Сваки модул покрива одређени скуп функција независно од другог. Ово треба да учини апликацију лако за управљање, тестирање или скалирање. Из технолошке перспективе, овај слој треба да буде развијен као скуп Rest API сервиса користећи .NetCore framework. За коришћење сваког Rest API сервиса потребан је токен за аутентификацију са важећим информацијама о кориснику.

Складишне компоненте су системска компоненте које чине база података и storage.

4.2 Скалабилност

Систем мора бити дизајниран са високим степеном скалабилности. У ту сврху систем мора бити развијен применом сервисно оријентисане архитектуре (SOA). Архитектура мора бити раздвојена барем на три слоја: Слој корисничког интерфејса, Слој пословне логике, Слој приступа подацима.

Потребно је да се у имплементацији, у максимално могућој мери, тежи примени microservice архитектуре. Имплементирани сервиси треба да буду грануларни и у што већој мери независни једни од других.

Све компоненте система морају бити container-ready и спремне за хостовање на Kubernetes.

Систем мора да буде развијен тако да омогућава независно скалирање сервиса, без утицаја на доступност апликација као целине.

4.3 Висока доступност

Систем мора радити у режиму високе доступности. Компоненте система морају имати више инстанци које ће гарантовати високу доступност система.

Висока доступност мора да буде подржана и применом CI/CD алата који омогућавају брзо и сигурно увођење нових функција и исправки у окружење наручиоца.

4.4 Безбедност и заштита података

Систем мора имплементирати највише стандарде заштите података и приватности.

Подаци у транзиту морају бити заштићени применом TLS протокола како би се осигурало да сви подаци који пролазе кроз комуникационе канале буду шифровани и заштићени од пресретања.

Систем мора имплементирати механизме строге контроле приступа који укључују аутентификацију и ауторизацију корисника система.

Систем мора обезбедити израду и чување резервних копија података.

Понуђени систем мора да задовољи техничке захтеве из области безбедности информационих система, са фокусом на заштиту критичне инфраструктуре и апликација које су изложене интернету. У савременим ИТ окружењима, кључни сервиси све чешће користе web а технологије, што их чини посебно рањивим на нападе попут злоупотребе web рањивости и волуметријских DDoS напада. Потребно је обезбедити високу доступност и интегритет система кроз имплементацију cloud-native решења за Web Application Firewall (WAF) и DDoS заштиту.

4.4.1 Cloud Web Application Firewall (WAF)

WAF решење мора бити понуђено као cloud сервис уз високу доступност и скалабилност, и мора првенствено штитити апликације и изложене API-је од OWASP Top 10 напада.

Минимални технички захтеви:

1. Deployment и интеграција:
 - a. Могућност једноставне интеграције путем DNS преусмеравања (reverse proxy)
 - b. Решење мора да обезбеди могућност додавања више апликација и домена
2. Заштита од OWASP Top 10 напада:
 - a. Решење мора да обезбеди заштиту од следећих типова напада:
 - i. A01: Broken Access Control
 - ii. A02: Cryptographic Failures
 - iii. A03: Injection (SQL, LDAP, OS Command...)
 - iv. A04: Insecure Design
 - v. A05: Security Misconfiguration

- vi. A06: Vulnerable and Outdated Components
- vii. A07: Identification and Authentication Failures
- viii. A08: Software and Data Integrity Failures
- ix. A09: Security Logging and Monitoring Failures
- x. A10: Server-Side Request Forgery (SSRF)
- b. Решења треба да обезбеди следеће функционалности:
 - i. Virtual patching – заштита од познатих рањивости без измене кода.
 - ii. Bot detection i rate limiting – за спречавање аутоматизованих напада
- 3. Заштита изложених API сервиса:
 - a. Валидација API захтева према спецификацији.
 - b. Rate limiting и детекција не стандардних образаца коришћења

4.4.2 DDoS заштита

Систем за заштиту мора да омогући cloud-based заштиту од DDoS волуметријских напада, уз ослањање на локалне WAF компоненте за додатну инспекцију и контролу саобраћаја.

Минимални технички захтеви:

1. Врсте напада које сервис мора да спречи:
 - a. Волуметријски напади: UDP flood, TCP SYN flood, ICMP flood, DNS amplification, NTP amplification.
2. Модел заштите:
 - a. Cloud scrubbing centar који филтрира саобраћај пре уласка у мрежу корисника.
 - b. Могућност једноставне интеграције путем DNS преусмеравања
 - c. Интеграција са WAF решењем као додатни слој за детаљну L7 инспекцију
3. Перформансе и капацитет
 - a. Cloud DDoS заштита са глобалним капацитетом од 1 Gbps.
 - b. WAF инспекција саобраћаја треба да подржи минимално 200 Mbps протока

4.5 Остали захтеви

Параметарски подаци система морају бити дефинисани кроз конфигурационе фајлове. На овај начин се омогућава Администраторима да врше лаку промену вредности параметара и да на тај начин у одређеној мери врше прилагођавања система.

Кориснички интерфејс мора бити израђен на Српском језику, коришћењем ћириличног и латиничног писма.

Систем мора подржати рад великог број корисника. Очекивани број корисника система је 150.

Очекивани прираштај броја докумената на годишњем нивоу је 540.000, просечне величине 0.5 MB.

Дизајн апликације треба да буде оптимизован за приказ на различитим врстама уређаја (десктоп рачунар, лаптоп, таблет...).