Приложение №3

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ
за „Разработване на иновативна билинг платформа за кратки текстови съобщения: Изграждане и тестване на прототип на иновативна билинг платформа за кратки текстови съобщения“

по проект BG16RFPR001-1.001-0218-C01
„Иновативна билинг платформа за кратки текстови съобщения“

1. ПРЕДМЕТ НА ПОРЪЧКАТА: „Възлагане на разработване на иновативна билинг платформа за кратки текстови съобщения: Изграждане и тестване на прототип на иновативна билинг платформа за кратки текстови съобщения“

Изпълнителят следва да извърши научноизследователска дейност, включваща изграждане, изпитване и валидация на прототип на иновативна услуга за билинг платформа за кратки текстови съобщения.

2. ЕТАПИ

Дейността включва минимум следните етапи:

Изпълнителят следва да осъществи минимум следните етапи:

Етап 1: Разработка и тестване на прототип:

- Създаване на базова версия на платформата, която включва основните функционалности за ценообразуване и управление на пакетите.
- Интеграция с SMS шлюзове/доставчици на съобщения за автоматично обновяване на цените.
- Тестване на функционалностите за динамично определяне на оператора и автоматични промени в тарифите.

Етап 2: Демонстрация в операционна среда

- Пилотно изпълнение: Реализиране на прототипа в реална операционна среда.
- Събиране на обратна връзка и оптимизация: Анализ на резултатите от пилотното изпълнение, събиране на обратна информация от потребителите и внедряване на подобрения в системата.
- Документиране и финализиране: Създаване на детайлни документи за крайните потребители и технически наръчници.

Този документ е създаден с финансовата подкрепа на програма „Конкурентоспособност и иновации в предприятията“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „Омнилинкс“ ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Етап 3: Тестване и оценка на нивото на технологична готовност

- Валидация на технологията: Тестване и оценка на функционалностите, стабилността и ефективността на платформата в реална операционна среда

3. МИНИМАЛНИ ИЗИСКВАНИЯ

Прототипа на Иновативната билинг платформа за кратки текстови съобщения трябва да е структуриран около четири ключови функционалности:

- управление на пакети;
- тарифиране;
- обработване на данни за промяна на тарифите на доставчици маршрутизиране на съобщения;

Архитектурата да поддържа, както синхронни, така и асинхронни потоци на данни - от заявки в реално време за изпращане на SMS до фонови процеси за актуализация на тарифи.

Основните компоненти които да съдържа софтуерната архитектурата са:

1. **API Gateway – KrakenD.**

Платформата да използва KrakenD, като централизиран API Gateway, който служи като единствена входна точка за всички външни заявки от уеб интерфейса

Основни функции и отговорности на **API Gateway**:

- маршрутизиране на заявките - да преобразува единен външен endpoint (напр. POST /api/v1/packages) в заявки към съответните микросървиси (напр. Account Billing Service). Маршрутизирането се дефинира чрез декларативни YAML конфигурации, които са версионирани в Git и прилагани чрез CI/CD pipeline. Това да позволява промени в маршрутизацията без промяна в кода;
- аутентикация и ауторизация - всяка входяща заявка да се проверява за валиден JWT Access Token, издаден от централизирания Keycloak Authentication Server. KrakenD:

- валидира подписа на токена чрез публичния JWKS endpoint на Keycloak;
- проверява срок на валидност, issuer и audience;
- извлича потребителските роли и скоупове от claims-овете,
- прилага endpoint-базиран RBAC — например, само потребители с роля admin могат да достъпят /api/v1/providers.

- филтриране и трансформация на данни - да поддържа селективно включване/изключване на полета, както в заявките към бекенда, така и в отговорите към клиента:

Този документ е създаден с финансовата подкрепа на програма „Конкурентоспособност и иновации в предприятията“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „Омнилинкс“ ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- агрегация на отговори (Response Aggregation) - за сложни клиентски нужди, API gateway-а е нужно да може да изпрати паралелни или последователни заявки към няколко микросървиса и да обедини отговорите в единен отговор.

2. Сървис за интеграция с SMS доставчици (SMS Provider Integration Service)

Този сървис да управлява цялата комуникация с външните SMS доставчици (агрегатори и телекомуникационни оператори).

Основни отговорности на SMS Provider Integration Service:

- поддържане CSV файлове на множество SMS доставчици и формати на данни;
- нормализиране на данни за цени от различни формати на доставчици – преобразува специфични за доставчика структури в унифициран вътрешен модел, който може да бъде използван от SMS Billing Service;

3. Сървис за тарифиране на SMS (SMS Billing Service)

SMS Billing Service да бъде централният компонент, отговарящ за цялата логика, свързана с ценообразуването и управлението на тарифи в платформата. Да функционира като „мозъкът“ на билинг модела и осигурява точност, прозрачност и гъвкавост при определяне на крайните цени за клиентите.

Основни отговорности на SMS Billing Service:

- изчисляване на клиентски тарифи въз основа на актуалните цени от SMS доставчиците и приложими бизнес правила, например, марж, минимална цена и др.;
- прилагане на конфигурации за надценка;
- управление на история на тарифите и дати на влизане в сила – всяка промяна в тарифата да се записва, като нова версия с ясно дефинирана дата на активиране, което позволява точна проследяемост;
- изпълнение на автоматични актуализации на тарифи – при промяна в разходите от страна на доставчиците (получени чрез Provider Integration Service), системата автоматично да преизчислява клиентските цени и подготвя нова версия на тарифите според зададени правила;

4. Сървис за управление на клиентски билинг (Account Billing Service)

Account Billing Service да управлява всички аспекти, свързани с клиентските профили, техните финансови настройки и баланс, както и контрол върху използването на SMS услуги. Account Billing Service да действа, като финансов шлюз в архитектурата — не просто да съхранява данни, а активно да участва в одобрението на всяка транзакция, като гарантира спазването на бизнес правилата и финансовата устойчивост на платформата.

Този документ е създаден с финансовата подкрепа на програма „Конкурентоспособност и иновации в предприятията“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „Омнилинкс“ ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Основни отговорности на **Account Billing Service**:

- съхраняване на клиентски профили и конфигурации - активни пакети и ограничения;
- управление на billing session - създаване и валидиране на billing session при всяка заявка за изпращане на SMS.

5. HLR Service (Home Location Register Lookup Service)

HLR Service е специализиран микросървис, отговорен за съхранението на текущия мобилен оператор на даден телефонен номер.

Основни отговорности:

- съхранение на текущия мобилен оператор, както и други данни на даден телефонен номер:
- интеграция с Provider Integration Service и SMS Billing Service – предоставя актуална информация за оператора на получателя

6. Уеб портал

Чрез уеб портала потребителите да могат да:

- създават, редактират и деактивират SMS пакети с пълен набор от параметри (държава, мрежа, брой съобщения, цена, срок на валидност);
- наблюдават текущите тарифи от доставчиците и клиентските цени в реално време;
- управляват правила за маржове и динамично ценообразуване;
- генерират отчети за употреба, приходи и рентабилност по пазари, клиенти или пакети;

Уеб интерфейсът трябва да е реализиран, като самостоятелно frontend приложение, изградено с Vue.js 3

Всички заявки към бекенда трябва да се изпращат през API Gateway, който да служи като единствена входна точка и да осигурява маршрутизиране, rate limiting и security enforcement. Комуникацията да се осъществява чрез RESTful API с JSON payload и стриктна валидация на входните данни.

Порталът да следва принципите на ролево-базиран контрол на достъпа (RBAC). Автентикацията да се осъществява чрез OIDC (OpenID Connect), като е избран Authorization Code Flow with PKCE (Proof Key for Code Exchange) – съвременен и сигурен стандарт, препоръчан за SPAs (Single-Page Applications). Този подход предотвратява атаки като code interception и осигурява защита дори при липса на backend secret. Сесиите се управляват чрез краткотрайни JWT access токени и refresh токени с възможност за отдалечен logout.

Този документ е създаден с финансовата подкрепа на програма „Конкурентоспособност и иновации в предприятията“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „Омнилинкс“ ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

7. Authentication Server – Keycloak (OIDC Identity Provider)

Системата да включва централизиран Authentication Server, реализиран чрез Keycloak в конфигурация cluster от 3 нода, разположени във високо-достъпна (HA) среда. Този избор осигурява отказоустойчивост, балансиране на натоварването и непрекъснатост на услугата дори при отказ на един от нодовете. Keycloak да служи като единен източник на истина за идентичността и правата на всички потребители и системи, взаимодействащи с платформата — от човешки оператори до машинни клиенти (микросървиси и външни интеграции).

Стандартизиран подход: OpenID Connect (OIDC) и OAuth 2.0

Keycloak да е конфигуриран, като OIDC Identity Provider (IdP), използвайки OpenID Connect — слой върху протокола OAuth 2.0.

Всички клиенти на платформата да са регистрирани като OIDC clients в Keycloak, с ясно дефинирани права, редирект URI-та и flow-ове.

Валидацията на JWT токъните да се извършва:

- В API Gateway - преди заявката да бъде насочена към съответния микросървис, API Gateway проверява:

- валидност на подписа (чрез публичния ключ от Keycloak JWKS endpoint);
- срок на валидност;
- audience и issuer.

Ако токенът е невалиден, заявката се отхвърля с HTTP 401.

Микросървисите на прототипа да се интегрират с наличните Event Bus, Сървис за нотификации (Notification Service) и Слой за съхранение на данни (Data Storage Layer)

Слоя за съхранение на данни (Data Storage Layer) към които да се интегрира прототипа да се състой от следните типове бази данни:

- **Релационна база данни – PostgreSQL**

- Да се използва логическо разделяне на схеми по микросървиси (напр. account_billing, sms_billing), което осигурява изолация и независимост при миграции;

- **Документно-ориентирано хранилище – MongoDB**

MongoDB да се използва за съхранение на полу-структурирани и динамични данни, където схемата често се променя или варира между записи. Това включва конфигурации, справочници и метаданни, които изискват гъвкавост и бързо четене.

Този документ е създаден с финансовата подкрепа на програма „Конкурентоспособност и иновации в предприятията“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „Омнилинкс“ ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Интеграцията със Сървиса за нотификации (Notification Service) ще се използва за уведомяване на заинтересовани страни за промени в тарифите – както вътрешни екипи (продукт, финанси), така и външни клиенти, когато това е договорено;

4. ИЗИСКВАНИЯ КЪМ РЕЗУЛТАТИТЕ

1. Да бъде изграден работещ прототип на билинг платформа за кратки текстови съобщения;
2. Да се представи детайлна документация за крайния потребител и технически наръчници
3. Да се тестват и оценят функционалностите, стабилността и ефективността на платформата в реална операционна среда.

Този документ е създаден с финансовата подкрепа на програма „Конкурентоспособност и иновации в предприятията“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от „Омнилинкс“ ЕООД и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.