SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

Opis predmetu zákazky

Názov predmetu zákazky: „Univerzálny komunikačný systém s kryptovacím modulom pre centrálny zber a prenos medicínskych dát“

Obsah

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

Názov predmetu zákazky

Univerzálny komunikačný systém s kryptovacím modulom pre centrálny zber a prenos medicínskych dát

Opis predmetu zákazky

Zámerom projektu je vývoj jednotného komunikačného systému a šifrovacieho modulu softvérového charakteru za účelom zberu a prijímania dát, s dôrazom na zachovanie integrity, bezpečnú výmenu osobných údajov a citlivých informácii zo zdrojov hardvérového, ako aj softvérového typu do centrálneho systému v prostredí telemedicínskych a ambulantných systémov.

Príkladom použitia je zber dát z elektronicky riadeného dávkovača liekov, kedy sú dáta zariadením zozbierané a bezpečne odoslané s unikátnym identifikátorom pacienta na centrálny systém, následne dešifrované a kategorizované pre ďalšie spracovanie inými telemedicínskymi systémami prostredníctvom RESTful API.

Elektronicky riadený dávkovač liekov je zariadenie schopné z hľadiska svojej funkcionality pomôcť pacientom pripomínať čas kedy si majú dať svoje lieky. Zároveň je po stlačení tlačidla schopné odoslať informáciu o tom, že si pacient svoje lieky zobral. Informácia o spotrebe, čase a unikátnom identifikátore pacienta sú po zbere dát prenesené šifrovanou formou na centrálny systém a ďalej spracované externými telemedicínskymi systémami. Odtiaľ môže lekár taktiež využiť údaje napríklad na analýzu odozvy organizmu na daný liek (pri súbežnom využití s iným telemedicínskymi zariadeniami napr. EKG holter, tlakomer atď.) Takúto informáciu využijú najmä zdravotné poisťovne, opatrovatelia, rodinní príslušníci či samostatní pacienti na kontrolu či si dali svoje lieky.

Ďalším základným použitím je prijímanie a zber medicínskych dát zo systémov tretích strán. Zber dát bude realizovaný formou dotazu „GET", kedy sa systém aktívne dotazuje na konkrétne dáta pacienta podľa stanoveného unikátneho kľúča, dáta vyhodnotí, kategoricky modifikuje a v zašifrovanej forme uloží na ďalšie spracovanie.
Podporované bude taktiež bezpečne prijímanie dát metódou „PUSH", kedy sú dáta rôznorodého charakteru spracovávané v reálnom čase, bez predchádzajúcej požiadavky systému. Dáta systém kategorizuje podľa stanovených štruktúr a v šifrovanej forme uloží na základe prijatých kľúčov.

Modul zabezpečí obojsmernú šifrovanú komunikáciu medzi koncovými zariadeniami a centrálnym systémom, ako aj medzi koncovými zariadeniami navzájom, za pomoci centrálneho systému a to na úrovni transportnej, relačnej, prezentačnej, ako aj aplikačnej vrstvy.

Systém zabezpečí zber, prijímanie, šifrovaný prenos a spracovanie prijímaných dát aj z hardvérových zariadení medicínskeho charakteru akými sú:

- dávkovač liekov
- tlakomer, pulzný oxymeter (Omron, Beurer, …)
- Holter, IoTemp
- smart váha
- mobilný telefón
- A iné

Taktiež prenos dát zo smart zariadení prostredníctvom systémov tretích strán, napríklad:

- Garmin Cloud Connect
- Samsung Cloud
- Suunto Partner API
- Google Fit
- a iné

Systém taktiež zabezpečí kategorizáciu dát a ponúkne webové rozhranie s podporou REST API pre ďalšie spracovanie zozbieraných dát inými telemedicínskymi systémami.

Systém ako celok je navrhnutý flexibilne a umožňuje systém v budúcnosti rozširovať o zber dát z ďalších typov zariadení a tiež o komunikáciu s inými systémami.

Systém bude postavený s dôrazom na bezpečnosť, rýchlosť a škálovateľnosť. Všetky použité prvky a komponenty systému bude možné individuálne auditovať pre potreby identifikácie zraniteľností, nevyhnutných aktualizácii a 0-day útokov.

Predmetom zákazky je jednotný komunikačný systém, koncový šifrovací modul, Webové rozhranie RESTful API, ako aj prvky centrálneho systému s výnimkou fyzickej, či virtualizačnej infraštruktúry a ich sieťových prvkov.

Popis riešenia

Prístupové REST API jednotného komunikačného systému so šifrovacím modulom zabezpečuje spojenie medzi koncovými zariadeniami užívateľa a centrálnym systémom.

Koncové medicínske zariadenia sa v prvom kroku pripájajú technológiou Bluetooth/Bluetooth Low Energy (BLE) na zariadenia zabezpečujúce komunikáciu, tie prostredníctvom sieťových rozhraní WiFi, prípadne 4G komunikujú priamo na jednotné RESTful API, kde je vo finálnom kroku zabezpečené spracovanie dát, ich kategorizácia, prípadná modifikácia a ukladanie pre ďalšie spracovanie.

Na strane servera sa bude využívať softvérový kryptovací modul, ktorý zabezpečí verifikáciu, integritu dát a dešifrovanie údajov pre ich následné ďalšie spracovanie.

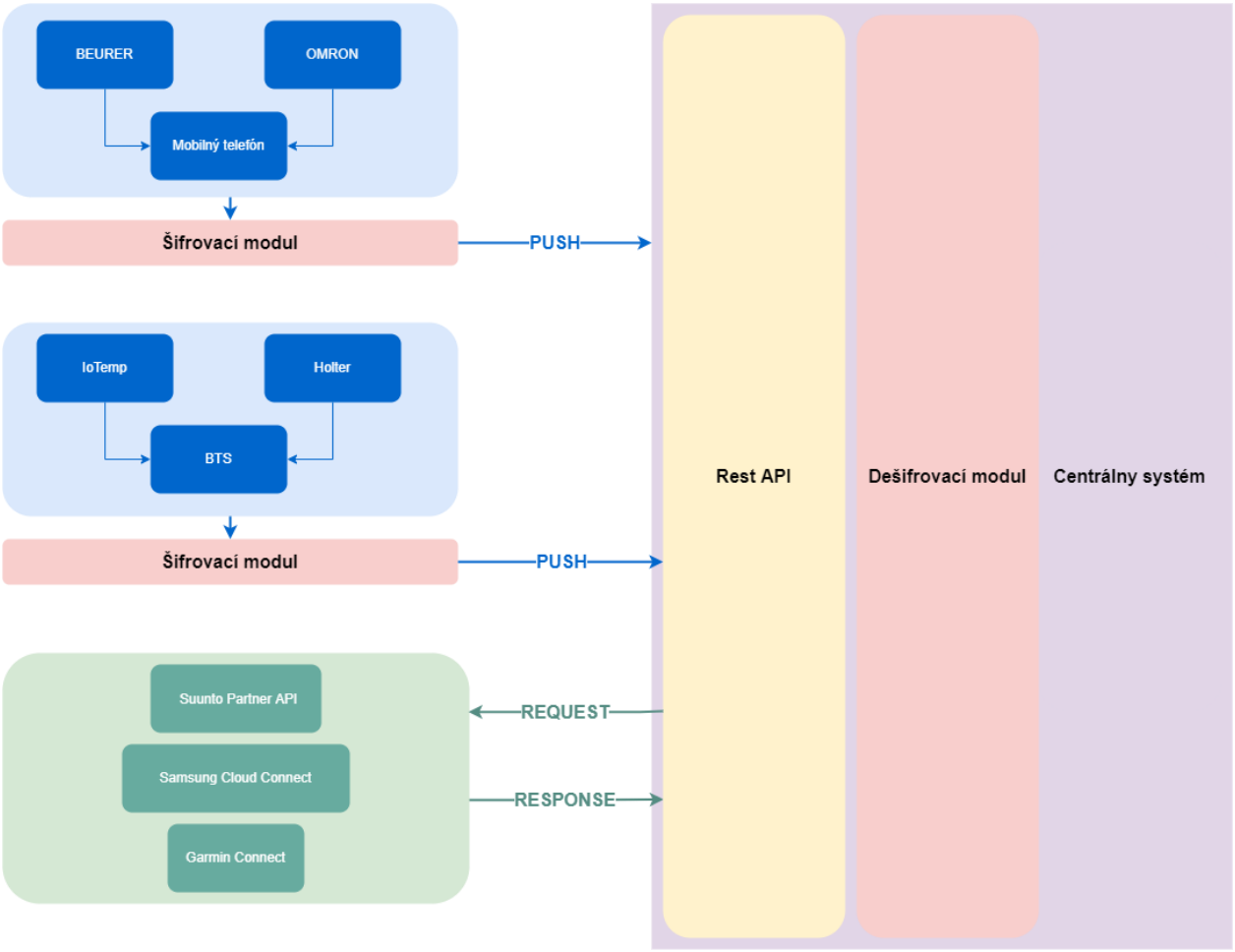
Systémy tretích strán sa pripájajú priamo na zabezpečené webové rozhrania REST API jednotného komunikačného systému, bez využitia lokálneho zberu dát prostredníctvom Bluetooth/Bluetooth Low Energy.

Systém bude pri prijímaní a následnom spracovaní podporovať rôzne typy vstupnej komunikácie (Single point of data collection). Podporované budú metódy PUSH, kedy koncový zdroj dáta zasiela bez predchádzajúcej výzvy systému v štruktúrovanej a neštruktúrovanej forme, ako aj REQUEST&GET kedy sa systém dotazuje na špecifické dáta v stanovených intervaloch a v štruktúrovanej forme.

Je nevyhnutné zabezpečiť podporu spracovania rôznorodých dát z heterogénnych zdrojov hardvérového, ako aj softvérového pôvodu. Systémová kategorizácia a formát štruktúrovania dát bude dynamicky konfigurovateľný, s podporou zápisu do relačných aj nerelačných databázových platforiem.

Kompletná komunikácia medzi bezpečnostným komunikačným modulom a centrálnym úložiskom je chránená proti odpočúvaniu a zneužitiu údajov. Rovnako je komunikácia zabezpečená aj proti ich modifikácii a zároveň poskytuje ochranu ďalším prvkom po celej prenosovej trase (domáci router, poskytovateľ internetu,…).

Kryptovací modul má charakteristiku univerzálneho prvku pre šifrovanie dátovej komunikácie z rôznorodých hardvérových, softvérových zariadení a iných zdrojov.


BEURER
OMRON
Mobilný telefón
Šifrovací modul
PUSH
IoTemp
Holter
BTS
Šifrovací modul
PUSH
Suunto Partner API
Samsung Cloud Connect
Garmin Connect
REQUEST
RESPONSE
Rest API
Dešifrovací modul
Centrálny systém

Technická špecifikácia

Systém pozostáva z nasledujúcich častí:

- Univerzálny softvérový kryptovací modul - Základný prvok šifrovanej komunikácie
- Centrálny systém - servery pre komunikáciu a archiváciu údajov, ktoré je súčasťou inej časti projektu
- RESTful API pre WEB
- RESTful API pre Mobilné aplikácie
- RESTful API pre externé systémy
- RESTful API pre Ambulantný softvér
- RESTful API pre poisťovne
- RESTful API pre lekárnický softvér
- RESTful API pre NCZI
- Kognitívny modul

Každá z týchto častí je detailnejšie popísaná v ďalšej časti tohto dokumentu.

Pojmy

ID	SKRATKA	POPIS
	USKM	Univerzálny softvérový kryptovací modul
	KTS	Kardiologický telemedicínsky systém

Univerzálny softvérový kryptovací modul

Základná bezpečnosť komunikácie a integrita prenášaných údajov bude zabezpečená technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať obstarávateľ.

Štandardné komunikačné kanály však nepredstavujú dostatočnú ochranu voči napr. man-in-the-middle útokom (MITM).

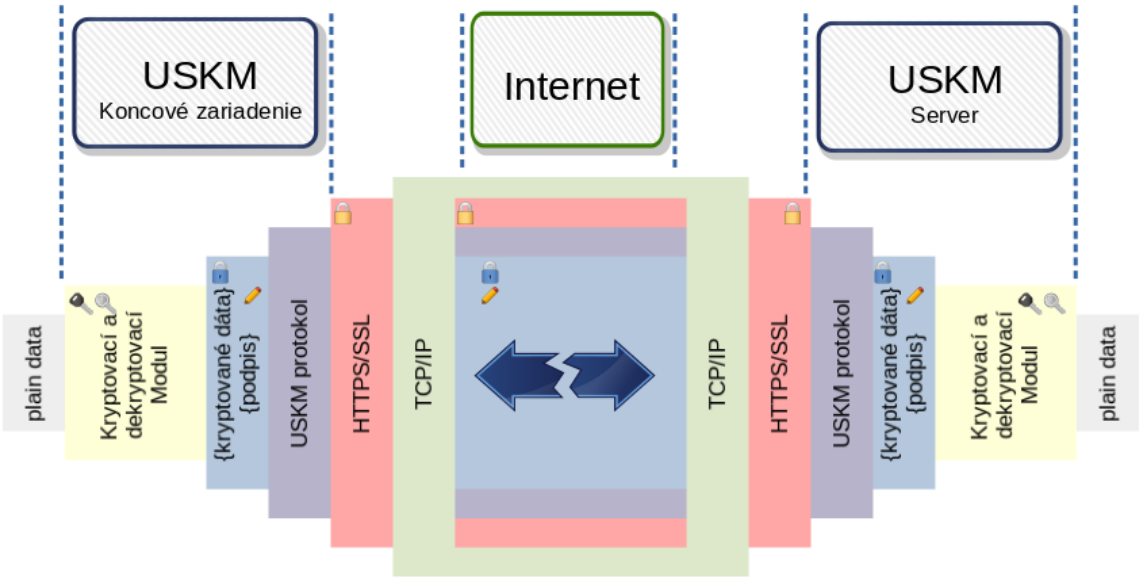
Vzhľadom na povahu prenášaných údajov je možné vybrané komunikačné kanály vybaviť dodatočnou vrstvou zabezpečenia, tvorenou univerzálnym softvérovým kryptovacím modulom (USKM).

USKM dopĺňa zabezpečenie transportnej vrstvy o dodatočné kryptovanie dát v aplikačnej vrstve. Modul využíva technológiu RSA na kryptovanie a Diffie–Hellman alebo Elliptic-curve Diffie–Hellman na bezpečnú výmenu kľúčov. Vďaka použitiu metódy privátneho a verejného kľúča je možné dáta nielen kryptovať, ale aj podpisovať a zabezpečiť tým možnosť overenia autenticity odosielateľa.

USKM pozostáva z nasledujúcich častí:

- modul pre koncové zariadenie
- modul pre centrálny server

Modul pre koncové zariadenie predstavuje softvérový balík, umožňujúci nadviazanie spojenia so serverom a vytvorenie kryptovaného kanálu, transparentného pre aplikácie tretích strán.



Na strane servera je inštalovaný softvérový balík, ktorý umožňuje bezpečnú komunikáciu súčasne so všetkými registrovanými klientami pri dodržaní vysokej úrovne zabezpečenia a verifikácie autenticity údajov. Modul si udržiava databázu aktuálne platných verejných kľúčov jednotlivých zariadení ako aj databázu všetkých svojich privátnych kľúčov. Tento balík sprístupňuje API rozhranie pre komunikáciu s koncovými zariadeniami vybavenými modulom USKM. A umožňuje tak vytvoriť vysoko bezpečný komunikačný tunel.

Každý modul si riadi generovanie kľúčov autonómne a s využitím interného protokolu (USKM protokol) a sprístupneného API je zabezpečená výmena verejných kľúčov ako aj koordinácia ich aktivácie.

Aplikácie tretích strán využívajú pre obojsmernú komunikáciu plain data rozhranie modulu USKM. Aplikácia sa môže rozhodnúť či bude posielať požiadavku len s podpisom alebo aj s plnúm kryptovaním dát. K privátnemu kľúču v systéme USKM má prístup len samotný USKM modul, externé aplikácie tento prístup nemajú a nemôžu ani ovplyvniť generovanie nových kľúčových párov.

USKM modul pre centrálny server je určený pre architektúru x86_32, x86_64. USKM modul pre koncové zariadenie je určený pre architektúry x86_32, x86_64 a ARM.

Nadviazanie zabezpečeného spojenia na SSL/TLS vrstve

Vzhľadom na to, že systém využíva ako prvotnú ochranu SSL/TLS vrstvu, prebieha nadviazanie spojenia nasledovne:

1. Klient odošle požiadavku na vytvorenie spojenia na server (napr. https://kts-server.sk) s identifikáciou podporovaných verzií TLS (min. podporovaná verzia je 1.2, voliteľne 1.3), šifrovacích algoritmov a kompresných algoritmov. Súčasťou tejto správy je aj náhodné číslo.
2. Server odošle klientovi zvolenú verziu TLS, šifrovacieho algoritmu, kompresného algoritmu a náhodné číslo. Zároveň odošle klientovi aj svoj certifikát, obsahujúci aj identifikáciu servera a certifikačnej autority. Server si zároveň môže vyžiadať od klienta jeho certifikát.
3. Klient overí platnosť certifikátu:
    - overí či uvedená certifikačná autorita patrí k dôveryhodným - klient USKM umožňuje striktné nastavenie dôveryhodných certifikačných autorit (nezávisle od certifikačných autorít akceptovaných operačným systémom), vrátane použitia vlastnej certifikačnej autority pre vydávanie a podpisovanie certifikátov v rámci systému

- pomocou verejného kľúča certifikačnej autority overí digitálny podpis certifikačnej autority vo verejnom kľúči servera
- overuje sa tiež časová platnosť certifikátu
- porovnáva sa tiež dns názov servera s názvom v certifikáte

4. Klient odpovie serveru zaslaním tajného kľúča a svojho verejného kľúča.
5. Na základe odpovede a náhodných čísel vypočíta klient aj server hash pomocou zvolenej funkcie a tento hash sa stáva kľúčom pre symetrické kryptovanie v ďalšej komunikácii na SSL/TLS vrstve.

Princíp komunikácie

Komunikácia v USKM je chránená asymetrickým šifrovaním, kde sa pre šifrovanie používa kľúčový pár verejný/privátny kľúč. Účastník spojenia USKM môže kedykoľvek vygenerovať nový kľúčový pár (privátny/verejný kľúč). Každý kľúčový pár získava interné číslovanie v podobe 4-bitového čísla. Číslo kľúčového páru je pri vygenerovaní automaticky zvýšené o 1. Pri dosiahnutí čísla 15 sa začína číslovanie opäť od jednotky. Číslo nula je v tomto prípade rezervované pre dlhodobý kľúčový pár. Nový verejný kľúč je následne odoslaný protistrane, pričom tento kľúč je podpísaný aktuálne platným privátnym kľúčom. Doba platnosti kľúčového páru je v systéme nastaviteľná, rovnako ako aj minimálny interval pre generovanie nového kľúčového páru. Overenie platnosti kľúčového páru servera sa vykonáva na základe podpisu certifikátu certifikačnou autoritou. Pre vyššiu flexibilitu je v systéme využívaná vlastná certifikačná autorita.

Identifikácia aktuálne platného, resp. použitého kľúčového páru sa nachádza v hlavičke dátového balíka. Hlavička dátového balíka obsahuje tiež nasledujúce informácie:

- **packet_id** - 16 bit int – poradové číslo balíčka, automaticky inkrementované s ďalším balíčkom
- **packet_part_id** – 16 bit int – poradové číslo časti balíčka v prípade že množstvo dát v balíčku vyžaduje rozdelenie na viacero častí
- **my_key_id** – 4 bit int – poradové číslo privátneho kľúča, použitého pre podpisovanie
- **your_key_id** – 4 bit int – poradové číslo verejného kľúča, použitého pre kryptovanie obsahu
- **data_encr** – 4 bit – 1 bit identifikuje či sú dáta zakryptované alebo len podpísané, ďalšie 3 bity sú rezerva pre budúce účely
- **data_type –** 4 bit int – typ odosielaných dát (potvrdenie prijatia, nový verejný kľúč, zamietnutie, používateľské dáta,...)

Za hlavičkou nasledujú prenášané dáta, ktoré môžu byť buď len podpísané, alebo podpísané a zároveň aj kryptované.

Príklad výmeny kľúčov a následnej komunikácie:

Východiskový stav: klient používa kľúčový pár s id=2, server používa kľúčový pár s id=6. Klient vygeneruje nový kľúčový pár, tento kľúčový pár dostane id=3, ale ešte nie je známy v systéme, takže verejný kľúč musí oznámiť serveru

1. Klient odošle nový verejný kľúč s identifikátorom id=3, tento podpíše privátnym kľúčom s id=2
2. Server prijme dáta, overí podpis pomocou verejného kľúča klienta s id=2
3. Server vytvorí potvrdenie prijatia a akceptáciu nového kľúča s id=3. Toto potvrdenie podpíše svojim privátnym kľúčom s id=6 a odošle klientovi
4. Klient overí podpis servera pomocou verejného kľúča servera s id=6

5. Klient zakryptuje dáta pomocou verejného kľúča servera s id=6 a podpíše ich svojim privátnym kľúčom s id=3
6. Server overí podpis klienta pomocou verejného kľúča klienta s id=3 a dekryptuje dáta pomocou svojho privátneho kľúča s id=6
7. Server v ďalšej komunikácii používa pre kryptovanie a overenie podpisu klienta certifikát s id=3

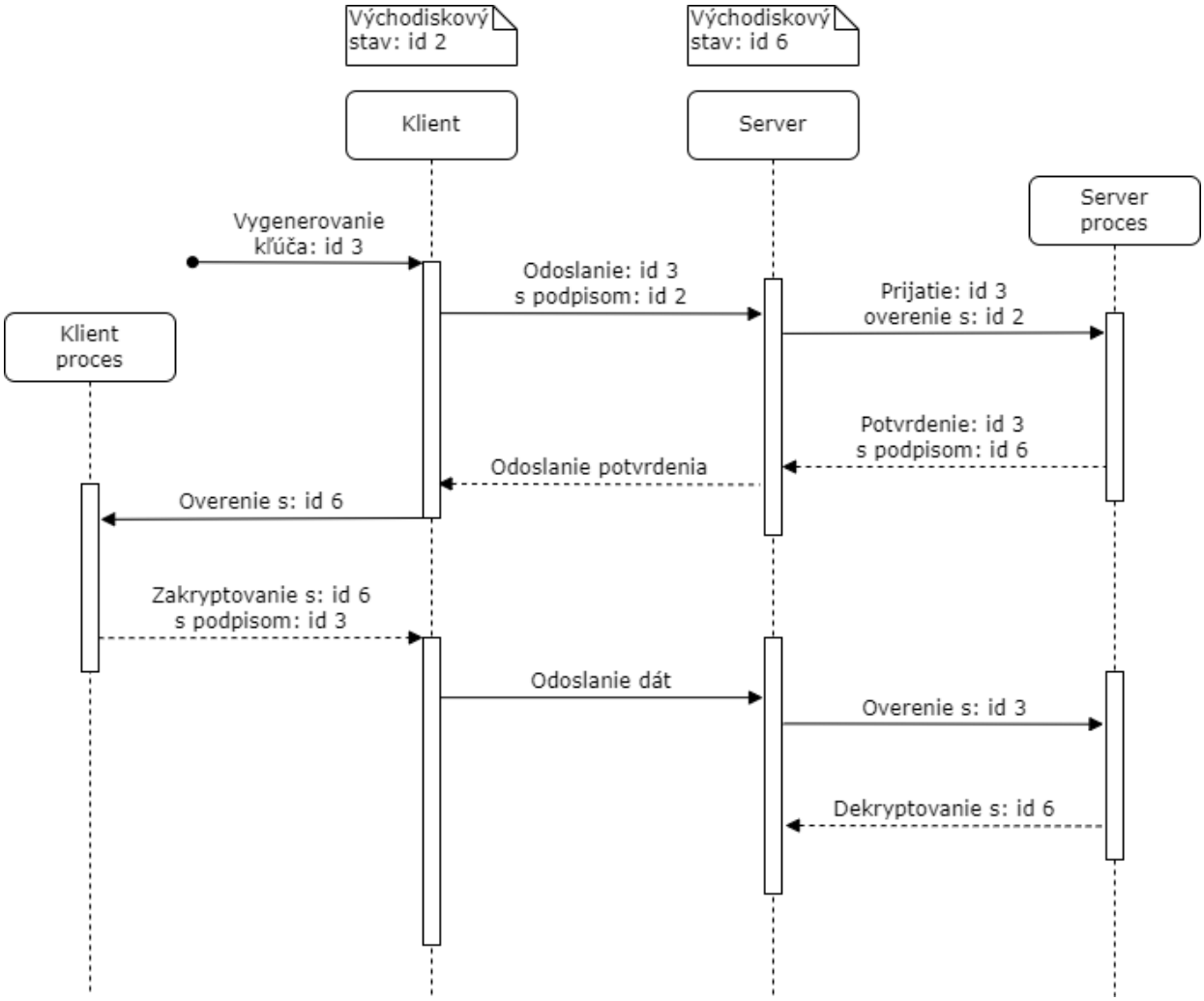


Diagram výmeny kľúčov pre uvedený príklad

USKM - nadviazanie spojenia

Pre nadviazanie spojenia a zabezpečenie autenticity systém využíva tzv. dlhodobé kľúčové páry. Tieto kľúčové páry majú verejný kľúč podpísaný certifikačnou autoritou systému a slúžia len pre nadviazanie komunikácie so systémom v prípade vypršania platnosti krátkodobých kľúčových párov.

USKM – výmena kľúčov

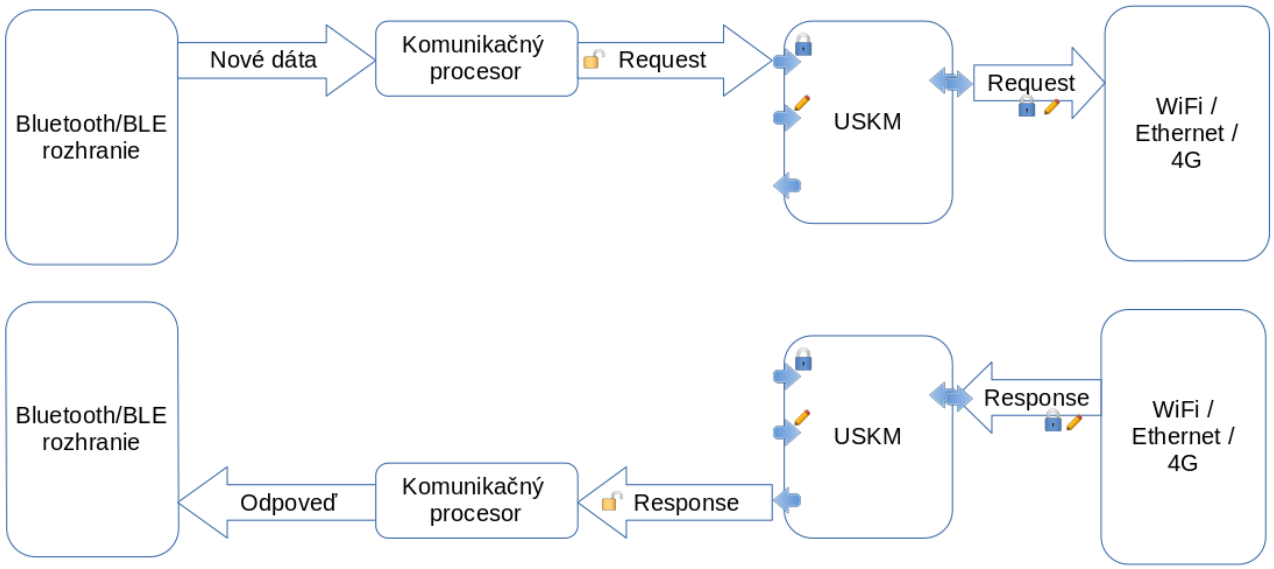
Výmena/aktualizácia kľúčov sa vykonáva vždy pred vypršaním časovej platnosti predchádzajúceho, resp. aktuálne platného kľúča, alebo pri požiadavke na túto výmenu. Medzi účastníkmi sú vymieňané len verejné kľúče. Nový verejný kľúč je vždy pred odoslaním podpísaný aktuálne platným privátnym kľúčom. Po prijatí

nového verejného kľúča si druhý účastník overí platnosť podpisu a následne tento nový verejný kľúč zaradí do svojho zoznamu kľúčov pre komunikáciu s odosielateľom kľúča. Potvrdenie prijatia a akceptácie tohto kľúča je oznámené odosielateľovi, pričom táto správa je ešte kryptovaná pomocou pôvodného verejného kľúča. Odosielateľ následne v najbližšej komunikácii začne pre podpisovanie používať nový privátny kľúč.

V prípade že server obdrží nový verejný kľúč s identifikátorom rovným nule sa jedná o žiadosť klienta o podpis nového dlhodobého verejného certifikátu. V tomto prípade server vykoná podpísanie tohto kľúča systémovou certifikačnou autoritou a takto podpísaný certifikát odošle späť klientovi. Doba platnosti dlhodobých kľúčov je taktiež nastaviteľná ako parameter systému.

Odoslanie zakryptovanej požiadavky

Odoslanie zakryptovanej požiadavky predstavuje najvyššiu úroveň ochrany dát a je určená pre dáta, ktoré by mohli obsahovať osobné údaje, konfiguračné údaje alebo inak citlivé údaje. Na obrázku je znázornený príklad keď aplikácia tretej strany – v tomto prípade zariadenie, vykonávajúce zber dát a ďalšiu komunikáciu s rôznymi Bluetooth/BLE zariadeniami, odosiela dáta získané zo zariadení do centrálneho systému.



Komunikačný procesor prečíta dáta a tieto dáta s použitím svojho interného protokolu, nezávislého od USKM, ich zapíše na kryptovací vstup modulu USKM [nekryptovaný Request]. Modul USKM okrem zakryptovania dát aktuálne platným verejným kľúčom prijímateľa (servera) tieto dáta následne aj podpíše svojim privátnym kľúčom. Takto zakryptované a podpísané dáta sú následne odoslané na server [kryptovaný a podpísaný request].

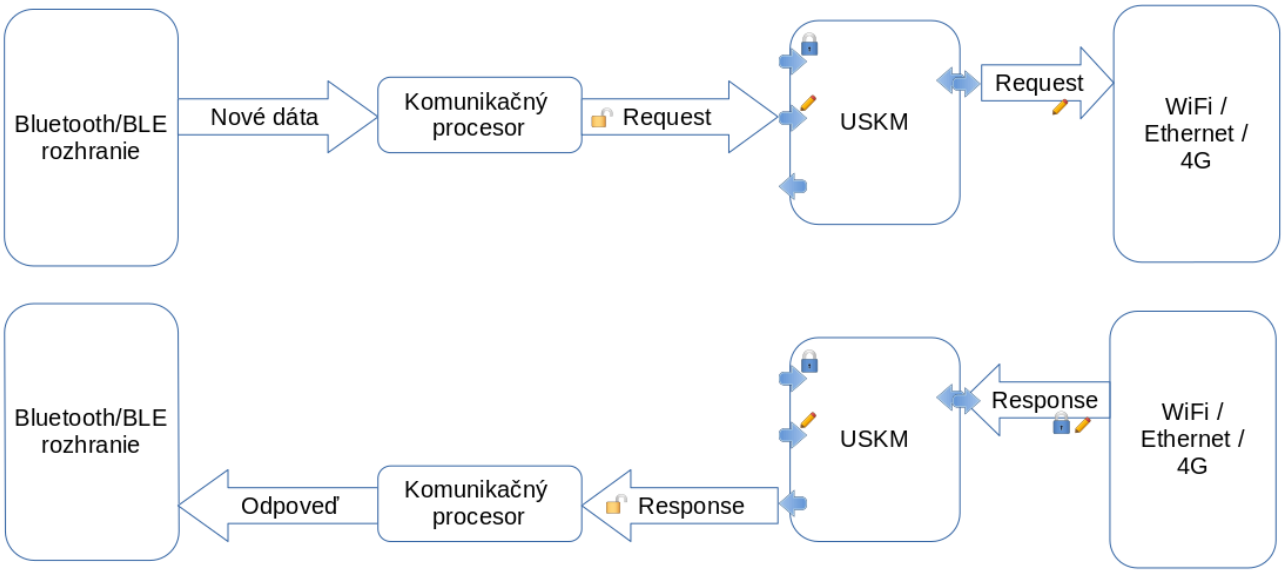
Serverový modul overí správnosť podpisu a vykoná dekryptovanie správy. Dekryptované dáta následne odovzdá procesu, ktorý sa stará o spracovanie dát zo zariadení (ukladanie do databázy a ďalšie spracovanie, notifikácie,…). Odpoveď tohto procesu server zakryptuje verejným kľúčom prijímateľa a podpíše svojim privátnym kľúčom. Takáto správa je následne doručená do modulu USKM zariadenia, kde sa vykoná overenie podpisu, dekryptovanie a odovzdanie dát komunikačnému procesoru.

Komunikačným procesorom môže byť ľubovolný proces, využívajúci socketovú komunikáciu.

Odoslanie podpísanej požiadavky

Podpísaná požiadavka umožňuje odosielať informácie, ktoré nevyžadujú kryptovanie, avšak je potrebné garantovať ich autenticitu, resp. autenticitu ich odosielateľa. Môže ísť napr. o údaje anonymného alebo anonymizovaného charakteru.

Komunikačný modul zapíše svoje dáta do modulu USKM, tentokrát však na port, ktorý je určený len pre podpisovanú komunikáciu. Modul USKM tieto dáta podpíše svojim privátnym kľúčom a odošle ich na server.



Server overí platnosť podpisu pomocou verejného kľúča používateľa a dáta rovnako ak v predchádzajúcom prípade odošle na ďalšie spracovanie.

Proces spracovania a vyhodnotenia odpovede je rovnaký. Modul USKM automaticky overí či sú dáta len podpísané alebo aj kryptované a postará sa o ich konverziu do „čistej" – nezakryptovanej podoby.

Odosielanie požiadaviek len s podpisom je výrazne menej náročné na výpočtový výkon zariadení a špeciálne pre zariadenia napájané z batérie predstavuje predĺženie doby prevádzky.

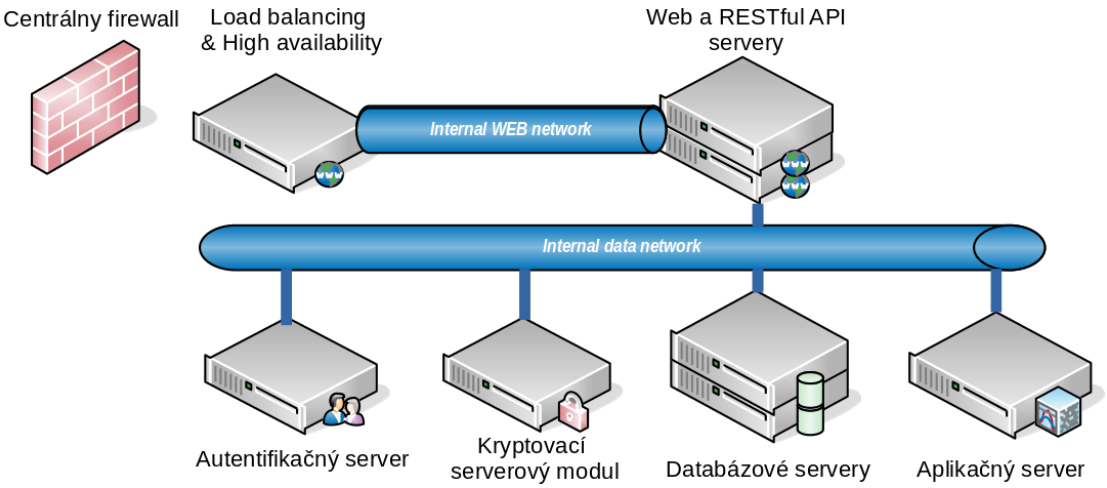
V prípade, že je podpis z nejakého dôvodu neplatný, prípadne sú dáta poškodené, nie sú takéto dáta doručované komunikačnému procesoru.

Centrálny systém

Centrálny systém je tvorený skupinou virtuálnych serverov, prevádzkovaných na hardvérovej infraštruktúre obstarávateľa. Fyzické servery ani virtualizačná platforma nie sú súčasťou tejto dodávky.

Odporúčaná virtualizačná platforma je KVM/QEMU, prípadne Vmware. Vo všeobecnosti je pre všetky virtualizované servery systému KTS odporúčaný operačný systém GNU/Linux v aktuálnej verzii s Long Term Support plánom.

Štruktúra virtualizovanej infraštruktúry je zobrazená na nasledujúcom obrázku.



Centrálny firewall zabezpečuje základnú ochranu serverov pred potenciálnymi útokmi a nie je súčasťou riešenia. Na tento účel bude využitá existujúca infraštruktúra obstarávateľa. Pravidlá centrálneho firewallu umožňujú pripojenie zo siete internet len na oficiálne vypublikované TCP porty Load balancing & High availability servera.

Load balancing & High availability server – Virtuálny server na plaforme Linux, ktorý ako jediný zabezpečuje prístup k službám systému z verejnej internetovej siete. Vypublikované služby (dostupné z verejnej siete) sú:

- Webové rozhranie na porte 443/tcp (https)
- RESTful API:
  - Pre webové rozhranie
  - Pre mobilné aplikácie
  - Pre ambulantný softvér
  - Pre NCZI
  - Pre zdravotné poisťovne
  - Pre lekárenský softvér

Jednotlivé RESTful API služby môžu byť dostupné na rôznych TCP portoch, tento údaj nemá žiadny vplyv na komplexnosť systému a bude upresnený dodatočne.

Všetky verejne dostupné služby budú chránené technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať vlastník projektu.

Tento server bude požiadavky následne preposielať jednotlivým webovým serverom v systéme podľa nastavených kritérií pre rozdeľovanie záťaže.

Server bude vybavený automatickým monitoringom dostupnosti a v prípade problému sa musí pokúsiť o automatický reštart kritických služieb.

Web a RESTful API servery – minimálne dva virtuálne servery na platforme Linux, kde ktorýkoľvek z nich dokáže poskytovať potrebné služby:

- Webové rozhranie na porte 80/tcp (http)

- RESTful API:
  - Pre webové rozhranie
  - Pre mobilné aplikácie
  - Pre ambulantný softvér
  - Pre NCZI
  - Pre zdravotné poisťovne
  - Pre lekárenský softvér
  - RESTful API pre externé systémy

Poskytované služby môžu byť implementované s využitím technológií PHP, Python, Java, JavaScript, HTML 5.0, CSS, SCSS, detailnejšia špecifikácia je uvedená pri jednotlivých moduloch ďalej v tomto dokumente. Požiadavky na inú ako uvedenú technológiu, je potrebné vopred vyšpecifikovať. Jednotlivé služby môžu byť inštalované ako samostatné balíky so zabezpečením aktualizácie, prípadne ako microservices alebo kontajnerové riešenie.

Autentifikačný server – virtuálny server s nainštalovaným LDAP, prípadne Active Directory pre autentifikáciu používateľov pri prihlasovaní. Platforma Linux Server LTS (preferované) alebo Windows Server.

Kryptovací server – minimálne jeden Linux server, ktorý zabezpečuje kryptovanie a dekryptovanie správ v rámci USKM. Požiadavku na kryptovanie/dekryptovanie server dostáva od serverov „Web a RESTful API". Kryptovací server využíva vlastnú internú databázu pre udržiavanie kryptovacích kľúčov. Podrobnejšie je funkcia systému USKM popísaná v časti Univerzálny softvérový kryptovací modul.

Databázové servery – minimálne dva virtuálne servery s nainštalovaným SQL serverom v konfigurácii Master/Slave s nastavenou replikáciou. Pre ukladanie neštruktúrovaných dát bude využitá noSQL databáza. Použité riešenie musí taktiež umožňovať load balancing a pridávanie ďalších serverov bez dodatočných nákladov na licencie.

Aplikačný server – minimálne jeden virtuálny server s konektivitou na databázu, ktorý umožňuje prevádzku Kognitívneho modulu a vytváranie anonymizovaných exportov a ďalších operácií s databázou systému. Anonymizované exporty dát umožňujú vytváranie analytických výstupov bez rizika úniku osobných informácií.

Virtualizované riešenie umožní rýchly monitoring vyťaženosti prostriedkov a následné dynamické prideľovanie prostriedkov, prípadne pridávanie virtuálnych serverov v prípade vysokej záťaže alebo rozširovania systému.

Riešenie bude prevádzkované na serverovej infraštruktúre obstarávateľa.

Rozhranie pre lekárov a lekárnikov pre registráciu zariadenia

Pre lekárov a lekárnikov bude dispozícií moderné, responzívne používateľské rozhranie určené pre definíciu a párovanie zariadení k pacientovi. Rozhranie tiež umožní prístup k dôležitým informáciám v systéme, ktoré bude dostupné z akéhokoľvek zariadenia, ktoré bude disponovať webovým prehliadačom:

- Google Chrome ver. 96 a vyššej
- Mozilla Firefox ver. 95 a vyššej
- Microsoft Edge ver. 96 a vyššej
- Safari ver. 15 a vyššej
- A ďalšie kompatibilné s vyššie uvedenými

Rozhranie môže byť implementované s využitím technológií PHP, Python, Java, JavaScript, HTML 5.0, CSS, SCSS. Požiadavky na inú ako uvedenú technológiu, je potrebné vopred vyšpecifikovať a musí byť schválená verejným obstarávateľom.

Rozhranie musí byť optimalizované a testované minimálne pre nasledujúce rozlíšenia:

- Desktopové prehliadače
  - 1280x768
  - 1366x768
  - 1440x900
  - 1920x1080
- Mobilné prehliadače a tablety
  - 540x960
  - 720x1280
  - 604x966

Rozhranie bude využívať technológiu pre doručovanie PUSH notifikácií (Firebase FCM alebo ekvivalentné riešenie), prípadne využije technológiu HTML SSE (Server-Sent Events). Pre dynamický update obsahu bude toto rozhranie využívať RESTful API pre Web.

Detailná špecifikácia funkcionalít a dizajnu webového rozhrania vzíde z Analýzy a dizajnu riešenia, časť: Zber požiadaviek, analýza, návrh a architektúra rozhrania pre lekára a lekárnika, návrh obrazoviek a workflow.

Bezpečnosť komunikácie a integrita prenášaných údajov bude zabezpečená technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať obstarávateľ projektu.

Zdravotnícky pracovník (ZPr) môže v tomto rozhraní vykonávať nasledujúce operácie

- Prihlásenie/Odhlásenie
- Zobrazenie prehľadu pridelených pacientov
- Vyhľadávanie pacientov
- Zobrazenie zoznamu priradených zariadení pacienta
  - Správa priradených zariadení
  - Priradenie nového zariadenia

Prihlásenie/Odhlásenie

Prihlásenie do rozhrania je vykonané prihlásením ZPr do systému KTS

Prehľad pacientov

Zdravotnícky pracovník má k dispozícii prehľad pridelených pacientov aj so zobrazením oprávnení na každého konkrétneho pacienta.

Vyhľadanie pacienta

Táto funkcia je určená primárne pre pracovníkov lekárne, ktorí nemusia mať priradeného žiadneho pacienta, ale potrebujú priradiť monitorovacie zariadenie konkrétnemu pacientovi, aby bolo možné namerané údaje z

tohto zariadenia korektne zaradiť. Funkciu tiež môže použiť iný ZPr, ktorý potrebuje požiadať o prístup k údajom pacienta (napr. pri konzultácii pacienta u iného odborného lekára).

Pre vyhľadanie pacienta, ktorý nie je priradený prihlásenému zdravotníckemu pracovníkovi slúži funkcia na vyhľadávanie podľa jednoznačného identifikátora (vzhľadom na skutočnosť, že momentálne sa pacient v lekárni identifikuje rodným číslom, uvažuje sa s týmto identifikátorom). Pracovník zadá rodné číslo do vyhľadávacieho poľa a ak sa v centrálnom úložisku systému nachádza zodpovedajúci pacient, bude mu zobrazený jeho zoznam zariadení s informáciami a funkciami zodpovedajúcimi priradeným oprávneniam aktuálneho zdravotníckeho pracovníka.

Zoznam zariadení pacienta

Zoznam zariadení pacienta je zobrazenie informácií o zariadeniach priradených konkrétnemu pacientovi v KTS. Zobrazenie zohľadňuje oprávnenia prihláseného ZPr a na základe týchto oprávnení umožňuje vykonávať operácie pridávania a odoberania zariadení.

V prípade lekárnika je zobrazené len pole pre pridanie nového zariadenia, ktoré umožňuje zadať unikátny identifikátor zariadenia, prípadne zoscanovať identifikátor vo forme čiarového alebo QR kódu.

V prípade lekára (ZPr) s vyššími oprávneniami sú zobrazené všetky zariadenia s možnosťou zmeny ich parametrov alebo odobratia zariadenia.

RESTful API pre WEB

RESTful API bude implementované na základe Swagger API špecifikácie. Finálna verzia tejto špecifikácie bude súčasťou analýzy a dizajnu riešenia časť: Špecifikácia a návrh modulu RESTful API pre WEB.

implementácia volaní v rozsahu:

Volanie	Typ volania	Stručný popis/účel
auth	POST, GET, PUT	Prihlásenie používateľa, manažment autentifikačných tokenov
account	GET, PUT, DELETE	Správa konta KTS, vyžiadanie údajov, zmena hesla, odstránenie
users	GET	Zoznam používateľov/pacientov s oprávneniami
userinfo	GET, PUT, DELETE	Detailné informácie o používateľovi, pridanie používateľa, zmena používateľských dát
devices	GET	Zoznam registrovaných zariadení
device	PUT, GET, DELETE	Detailné informácie o zariadení (napr. pri dávkovači liekov o jeho naplnení a pravidlách pre vydávanie liekov)
sharing	POST, GET, PUT, DELETE	Správa zdieľania informácií o zariadení
push	PUT, GET, DELETE	Manažment tokenov pre PUSH notifikácie
history	GET	Vyžiadanie dát s určením rozsahu pomocou filtrov
scheduler	GET, PUT, DELETE	Intervaly užívania liečiv alebo plánované spúšťanie meraní
message	GET, PUT	Odoslanie / prijatie textovej správy
messages	GET	Textové správy medzi používateľmi

Bezpečnosť komunikácie a integrita prenášaných údajov bude zabezpečená technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať obstarávateľ.

API pre WEB umožňuje Webovému rozhraniu systému KTS pristupovať k štruktúrovaným aj neštruktúrovaným dátam v Centrálnom úložisku.

RESTful API pre Mobilné aplikácie

Toto RESTful API slúži pre implementáciu komunikácie s mobilnou aplikáciou pre používateľov - pacientov systému KTS.

RESTful API bude implementované na základe Swagger API špecifikácie. Finálna verzia tejto špecifikácie bude súčasťou analýzy a dizajnu riešenia časť: Špecifikácia a návrh modulu RESTful API pre Mobilné aplikácie.

Predbežne sa uvažuje s implementáciou volaní v rozsahu:

Volanie	**Typ volania**	**Stručný popis/účel**
auth	POST, GET, PUT	Prihlásenie používateľa, manažment autentifikačných tokenov
account	GET, PUT, DELETE	Správa konta, vyžiadanie údajov, zmena hesla, odstránenie
devices	GET	Správa registrovaných zariadení
device	PUT, GET, DELETE	Detailné informácie o zariadení (napr. pri dávkovači liekov o jeho naplnení a pravidlách pre vydávanie liekov)
sharing	POST, GET, PUT, DELETE	Správa zdieľania informácií o zariadení
push	PUT, GET, DELETE	Manažment tokenov pre PUSH notifikácie
history	GET	Vyžiadanie dát s určením rozsahu pomocou filtrov
scheduler	GET, PUT, DELETE	Intervaly užívania liečiv alebo plánované spúšťanie meraní
message	GET, PUT	Textové správy medzi používateľmi
messages	GET	Textové správy medzi používateľmi

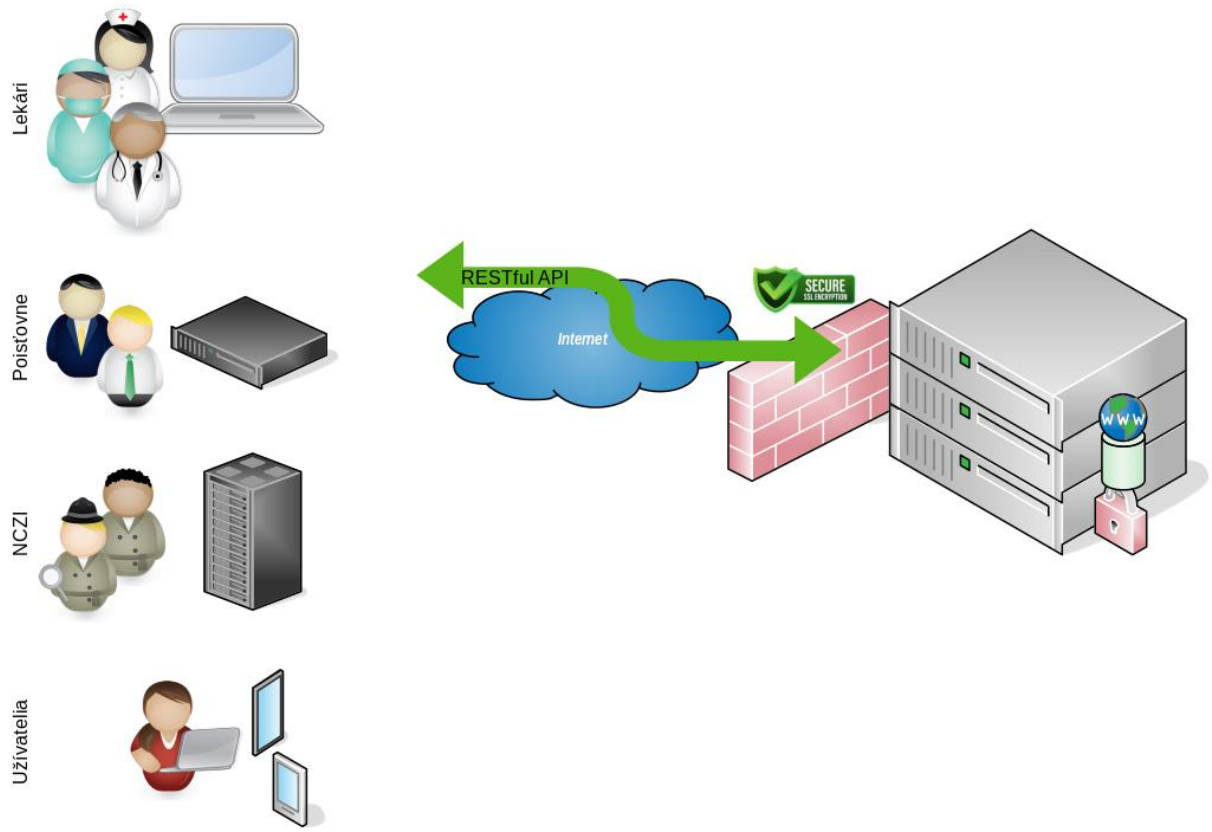
Bezpečnosť komunikácie a integrita prenášaných údajov bude zabezpečená technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať vlastník projektu.

RESTful API pre externé systémy

Systém bude disponovať samostatným RESTful API rozhraním, ktoré umožní priamu integráciu zo strany ambulantných softvérov, systémov poisťovne a systémov NCZI (eZdravie).

Pre všetky RESTful API bude k dispozícii dokumentácia v Swagger API formáte. Táto dokumentácia musí byť zohľadnená aj pri tvorbe FAT a SAT testovacích scenárov.

Všetky RESTful API rozhrania pre externé systémy musia byť dodané so zdrojovým kódom a licenciou umožňujúcou obstarávateľovi vykonávať úpravy, prípadne dopĺňať nové funkcionality.



RESTful API pre Ambulantný softvér

Toto rozhranie slúži na sprístupnenie vybraných informácií z centrálneho systému KTS pre ambulantné softvéry a umožní tvorcom ambulantných softvérov integráciu a vizualizáciu týchto informácií. Rozhranie nie je viazané na konkrétny ambulantný softvér.

Implementácia RESTful API pre Ambulantný softvér bude zdokumentovaná v analýze a dizajne riešenia časť: RESTful API pre Ambulantný softvér.

Pre jednoduchú integráciu do softvérov tretích strán bude k dispozícii Swagger API špecifikácia tohto rozhrania.

Predbežne sa uvažuje s implementáciou volaní v rozsahu:

Volanie	**Typ volania**	**Stručný popis/účel**
auth	POST, GET, PUT	Prihlásenie používateľa, manažment autentifikačných tokenov
account	GET, PUT, DELETE	Správa konta KTS, vyžiadanie údajov, zmena hesla, odstránenie
users	GET	Zoznam používateľov/pacientov s oprávneniami
userinfo	GET, PUT, DELETE	Detailné informácie o používateľovi, pridanie používateľa, zmena používateľských dát
devices	GET	Zoznam registrovaných zariadení
device	PUT, GET, DELETE	Detailné informácie o zariadení (napr. pri dávkovači liekov o jeho naplnení a pravidlách pre vydávanie liekov)

sharing	POST, GET, PUT, DELETE	Správa zdieľania informácií o zariadení
push	PUT, GET, DELETE	Manažment tokenov pre PUSH notifikácie
history	GET	Vyžiadanie dát s určením rozsahu pomocou filtrov
scheduler	GET, PUT, DELETE	Intervaly užívania liečiv alebo plánované spúšťanie meraní
message	GET, PUT	Odoslanie / prijatie textovej správy
messages	GET	Textové správy medzi používateľmi

Ambulantný softvér – podľa miery využitia poskytnutého API umožní prihlásenie do systému, stiahnutie zoznamu dát sprístupnených zo zariadení s identifikátorom pacienta, príjem PUSH notifikácií, správu nastavenia užívania liekov, plánovanie meraní a prehľad histórie užívania liekov, histórie nameraných údajov. Umožňuje tiež odosielanie krátkych textových správ s odporúčaniami pacientovi.

Bezpečnosť komunikácie a integrita prenášaných údajov bude zabezpečená technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať vlastník projektu.

RESTful API pre poisťovne

Toto rozhranie slúži na sprístupnenie vybraných údajov z centrálneho systému projektu KTS pre systémy zdravotnej poisťovne. Zdravotná poisťovňa vďaka systému eRecept a ďalším napojeniam na NZIS už disponuje informáciami o predpísanej medikácii pre pacienta a tiež informáciami o odobratých liekoch. Momentálne však ZP nemá informácie o reálnom užívaní liekov – pravidelné užívanie, dodržiavanie intervalov užívania atď. Vytvorené RESTful API rozhranie umožní poisťovni tieto informácie zo systému KTS získavať a ďalej ich spracovávať vlastnými informačnými systémami.

Implementácia RESTful API pre Zdravotné poisťovne bude zdokumentovaná v analýze a dizajne riešenia časť: RESTful API pre Zdravotné poisťovne.

Pre jednoduchú integráciu do softvérov tretích strán bude k dispozícii Swagger API špecifikácia tohto rozhrania.

Predbežne sa uvažuje s implementáciou volaní v rozsahu:

Volanie	**Typ volania**	**Stručný popis/účel**
auth	POST, GET, PUT	Prihlásenie klientskeho sw, manažment autentifikačných tokenov
push	PUT, GET, DELETE	Manažment tokenov pre PUSH notifikácie
med_usage	GET	História užívania liečiv

Rozhranie uvažuje s vytvorením jedného používateľa pre každú klientsku aplikáciu zdravotnej poisťovne, pričom prístup k API môže byť navyše limitovaný na IP adresy jednotlivých ZP. V rámci komunikácie prostredníctvom RESTful API si poisťovňa na základe identifikácie pacienta vyžiada štatistiku užívania liečiv. Návratová hodnota je JSON pole s údajmi o identifikácii pacienta, predpísanom čase užitia, identifikácie liečiva a reálnom čase užitia.

Prihlasovacie kontá pre zdravotné poisťovne budú spravované interne v systéme KTS a budú vydané na základe autorizovanej požiadavky zo strany Zdravotnej poisťovne.

RESTful API pre lekárnický softvér

Toto rozhranie slúži na komunikáciu so softvérmi lekární, hlavne za účelom registrácie nových zariadení do systému KTS a ich priradenia k pacientovi.

Predbežne sa uvažuje s implementáciou volaní v rozsahu:

Volanie	**Typ volania**	**Stručný popis/účel**

auth	POST, GET, PUT	Prihlásenie používateľa, manažment autentifikačných tokenov
account	GET, PUT, DELETE	Správa konta KTS, vyžiadanie údajov, zmena hesla, odstránenie
userinfo	GET	Vyhľadanie používateľa na základe identifikátora a zobrazenie detailných informácií o používateľovi (limitované údaje).
device	PUT, GET	Priradenie zariadenia k používateľovi, Zrušenie priradenia zariadenia

Bezpečnosť komunikácie a integrita prenášaných údajov bude zabezpečená technológiou SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať verejný obstarávateľ.

RESTful API pre NCZI

Toto rozhranie slúži na sprístupnenie vybraných údajov z centrálneho systému projektu KTS pre systémy NCZI. Jedná sa napr. o informácie o pravidelnosti užívania predpísaných liekov.

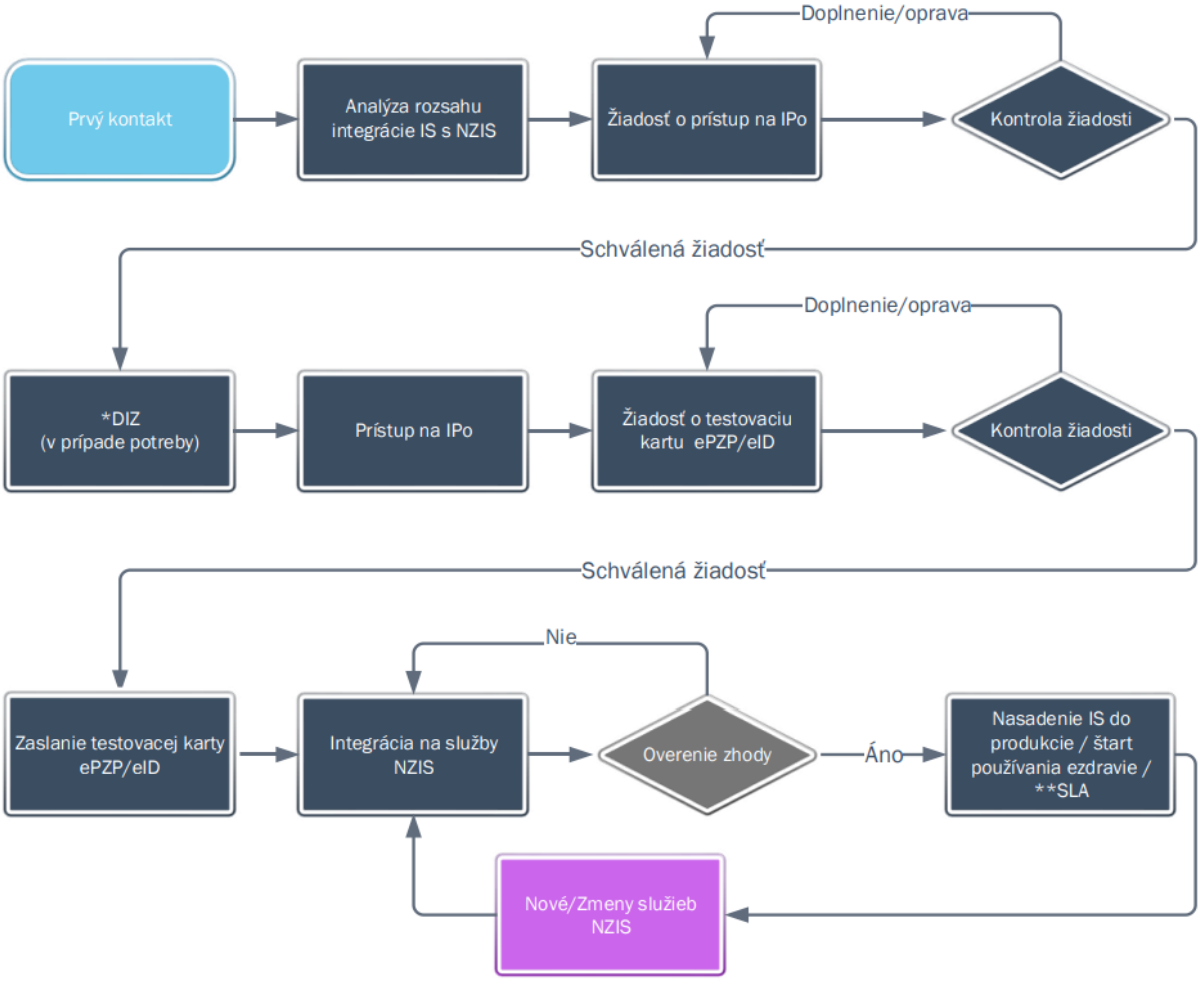
Implementácia RESTful API pre NCZI bude zdokumentovaná v analýze a dizajne riešenia časť: RESTful API pre NCZI. Podmienky a metodika pre integráciu informačných systémov sú dostupné na oficiálnej stránke https://www.ezdravotnictvo.sk/sk/-/dodavatel-integracia-informacnych-systemov

Predpokladaná implementácia je v minimálne rozsahu:

- overovania užívateľa/pacienta
- čítanie zo systému eRecept (predpísané lieky, výber z lekárne)
- sprístupnenie informácií o užití lieku

Detailná špecifikácia rozhrania bude súčasťou Analýzy a dizajnu riešenia časť: Špecifikácia a návrh modulu prepojenia s NCZI. Špecifikácia RESTful API bude vo formáte Swagger API.

V zmysle platnej metodiky je proces integrácie nasledovný:



Systémy, pripájajúce sa do systému eZdravie / NZIS musia prejsť procesom overenia zhody. Overenie zhody určuje zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme, v znení neskorších predpisov. Proces overenia zhody sa vykonáva v sídle Národného centra zdravotníckych informácií (NCZI).

Aktuálne podmienky ako aj postup overenia zhody informačného systému sú dostupné na https://www.ezdravotnictvo.sk/sk/-/dodavatel-overenie-zhody-informacnych-systemov

Bezpečnosť komunikácie a integritu prenášaných údajov bude zabezpečovať technológia SSL/TLS (Secure Sockets Layer / Transport Layer Security) s certifikátom podpísaným akceptovanou certifikačnou autoritou, ktorý bude administrovať a obnovovať verejný obstarávateľ vlastník projektu.

Kognitívny modul

Kognitívny modul v systéme KTS predstavuje rozhranie, ktoré umožní vykonávať rôzne analýzy získaných informácií, pričom sa v budúcnosti uvažuje s integráciou ďalších typov zariadení, ako sú napr. tlakomery, prenosné zariadenia na meranie tepu, teploty a podobne. Vďaka svojmu priamemu prístupu k anonymizovaným dátam KTS bude možné navrhovať a vytvárať aplikácie, ktoré budú schopné analyzovať tieto dáta, vyhľadávať nezrovnalosti a korelácie. Za týmto účelom bude možné implementovať rôzne algoritmy strojového učenia, spúšťať tieto algoritmy v rámci kognitívneho modulu a získavať štatisticky významné informácie, ktoré by napr. mohli pomôcť pri ďalšom zohľadnení medikácie, prípadne predikovať rôzne stavy.

Anonymizácia údajov musí byť vykonaná v súlade s ISO 25237:2017 Health informatics — Pseudonymization.

Implementácia tohto modulu spočíva vo vytvorení minimálne jedného virtuálneho servera s prístupom k anonymizovaným údajom KTS. Systém musí podporovať akceleráciu AI algoritmov pomocou GPU alebo TPU.

Dizajn infraštruktúry pre prevádzkovateľa

Zhotoviteľ vypracuje dizajn infraštruktúry z pohľadu hardvéru, softvéru, sieťovej topológie, bezpečnosti a spoľahlivosti. Dizajn infraštruktúry bude realizovaný na základe konzultácií s prevádzkovateľom so zohľadnením aktuálneho stavu a plánovaného rozširovania na strane prevádzkovateľa.

Požiadavky na jednotlivé informačné systémy

Univerzálny softvérový kryptovací modul

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_51	Funkčná požiadavka	USKM	Komunikácia	Registrácia komunikačného partnera/zariadenia v USKM. - Zaregistrovanie verejného kľúča partnera - Odoslanie verejného kľúča servera USKM
ID_52	Funkčná požiadavka	USKM	Komunikácia	Je implementovaná bezpečná výmena kľúčov medzi klientom a serverom USKM
ID_53	Funkčná požiadavka	USKM	Komunikácia	Je možná obojsmerná komunikácia medzi serverom a klientom vo forme kryptovaných a podpísaných dát
ID_54	Funkčná požiadavka	USKM	Komunikácia	Je možná obojsmerná komunikácia medzi serverom a klientom vo forme podpísaných dát
ID_55	Technická požiadavka	USKM	Komunikácia	Systém USKM si udržiava lokálnu databázu verejných kľúčov jednotlivých klientov za účelom kryptovania a verifikácie podpisov
ID_56	Technická požiadavka	USKM	Komunikácia	Systém USKM si interne zabezpečuje generovanie nových párov verejný-privátny kľúč a distribúciu verejných kľúčov

Viď príloha UTSKA_...

Centrálny systém

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_98	Technická požiadavka	Centrálny systém	Všeobecné	Systém je vybavený load ballancing serverom pre verejne dostupné služby s možnosťou pridávania ďalších serverov na rozloženie záťaže
ID_99	Technická požiadavka	Centrálny systém	Všeobecné	Všetky vypublikované služby sú chránené minimálne SSL/TLS technológiou
ID_100	Technická požiadavka	Centrálny systém	Všeobecné	Prevádzkovateľ má možnosť meniť a aktualizovať certifikát pre SSL

ID_101	Technická požiadavka	Centrálny systém	Všeobecné	Systém disponuje minimálne dvomi servermi pre prevádzku vypublikovaných WEB a RESTful API služieb
ID_102	Technická požiadavka	Centrálny systém	Všeobecné	Autentifikačný server umožňuje vykonávanie CRUD operácii na užívateľoch
ID_103	Technická požiadavka	Centrálny systém	Všeobecné	Je inštalovaný minimálne jeden kryptovací server s funkčným modulom USKM
ID_104	Technická požiadavka	Centrálny systém	Všeobecné	Sú inštalované minimálne dva servery s SQL databázou
ID_105	Technická požiadavka	Centrálny systém	Všeobecné	Použité SQL databázové servery majú nastavenú replikáciu
ID_106	Technická požiadavka	Centrálny systém	Všeobecné	Je inštalovaný minimálne jeden aplikačný server s prístupom na databázu systému

RESTful API pre WEB

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_57	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre prihlásenie požívateľa a výmenu autentifikačných tokenov - Prihlásenie menom a heslom - Získanie auth tokenu - Výmena auth tokenov po vypršaní platnosti
ID_58	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre správu používateľských údajov (zmena hesla, kontaktných údajov v KTS,…)
ID_59	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre vyžiadanie zoznamu lekárov alebo pacientov - zoznam pacientov ku ktorým má prihlásený používateľ určité oprávnenie
ID_60	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre vyžiadanie informácií o lekárovi alebo pacientovi a ich správu
ID_61	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre vyžiadanie zoznamu zaregistrovaných zariadení
ID_62	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre detailné informácie o zariadení a ich správu - Detaily o zariadení - Pridanie zariadenia a jeho priradenie k pacientovi - Odobratie zariadenia pacientovi - Deaktivácia zariadenia v systéme
ID_63	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre správu zdieľania údajov a informácií o zariadení
ID_64	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre manažment tokenov pre PUSH notifikácie - Odoslanie tokenu - Deaktivácia starého/zneplatneného tokenu

ID_65	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre vyžiadanie dát s určením rozsahu pomocou filtrov - Obmedzenie podľa používateľa - Obmedzenie časového obdobia - Výber typu dát
ID_66	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre definíciu/zistenie naplánovaných udalostí (intervaly užívania liečiv alebo plánované spúšťanie meraní)
ID_67	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre odoslanie / prijatie textovej správy - odoslanie textovej správy inému používateľovi - vyžiadanie konkrétnej textovej správy na základe id (po prijatí push notifikácie)
ID_68	Funkčná požiadavka	API-WEB	Všeobecné	RESTful API volanie pre vyžiadanie textových správ s možnosťou filtrovania účastníkov a časového intervalu

RESTful API pre Mobilnú aplikáciu

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_69	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre prihlásenie požívateľa a výmenu autentifikačných tokenov - Prihlásenie menom a heslom - Získanie auth tokenu - Výmena auth tokenov po vypršaní platnosti
ID_70	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre správu používateľských údajov (zmena hesla, kontaktných údajov v KTS,…)
ID_71	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre vyžiadanie zoznamu zaregistrovaných zariadení
ID_72	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre detailné informácie o zariadení a ich správu - Detaily o zariadení
ID_73	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre správu zdieľania údajov a informácií o zariadení
ID_74	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre manažment tokenov pre PUSH notifikácie - Odoslanie tokenu - Deaktivácia starého/zneplatneného tokenu
ID_75	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre vyžiadanie dát s určením rozsahu pomocou filtrov - Obmedzenie podľa používateľa - Obmedzenie časového obdobia - Výber typu dát
ID_76	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre definíciu/zistenie naplánovaných udalostí (intervaly užívania liečiv alebo plánované spúšťanie meraní)

ID_77	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre odoslanie / prijatie textovej správy - odoslanie textovej správy inému používateľovi - vyžiadanie konkrétnej textovej správy na základe id (po prijatí push notifikácie)
ID_78	Funkčná požiadavka	API-MA	Všeobecné	RESTful API volanie pre vyžiadanie textových správ s možnosťou filtrovania účastníkov a časového intervalu

RESTful API pre ambulantný softvér

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_79	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre prihlásenie požívateľa a výmenu autentifikačných tokenov - Prihlásenie menom a heslom - Získanie auth tokenu - Výmena auth tokenov po vypršaní platnosti
ID_80	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre správu používateľských údajov (zmena hesla, kontaktných údajov v KTS,…)
ID_81	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre vyžiadanie zoznamu lekárov alebo pacientov - zoznam pacientov ku ktorým má prihlásený používateľ určité oprávnenie
ID_82	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre vyžiadanie informácií o lekárovi alebo pacientovi a ich správu
ID_83	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre vyžiadanie zoznamu zaregistrovaných zariadení
ID_84	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre detailné informácie o zariadení a ich správu - Detaily o zariadení - Pridanie zariadenia a jeho priradenie k pacientovi - Odobratie zariadenia pacientovi - Deaktivácia zariadenia v systéme
ID_85	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre správu zdieľania údajov a informácií o zariadení
ID_86	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre manažment tokenov pre PUSH notifikácie - Odoslanie tokenu - Deaktivácia starého/zneplatneného tokenu
ID_87	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre vyžiadanie dát s určením rozsahu pomocou filtrov - Obmedzenie podľa používateľa - Obmedzenie časového obdobia - Výber typu dát
ID_88	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre definíciu/zistenie naplánovaných udalostí (intervaly užívania liečiv alebo plánované spúšťanie meraní)

ID_89	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre odoslanie / prijatie textovej správy - odoslanie textovej správy inému používateľovi - vyžiadanie konkrétnej textovej správy na základe id (po prijatí push notifikácie)
ID_90	Funkčná požiadavka	API-EXT-AMB	Všeobecné	RESTful API volanie pre vyžiadanie textových správ s možnosťou filtrovania účastníkov a časového intervalu

RESTful API pre zdravotné poisťovne

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_91	Funkčná požiadavka	API-EXT-ZP	Všeobecné	RESTful API volanie pre prihlásenie sw poisťovne a výmenu autentifikačných tokenov - Prihlásenie menom a heslom (pridelené systémom KTS) - Získanie auth tokenu - Výmena auth tokenov po vypršaní platnosti
ID_92	Funkčná požiadavka	API-EXT-ZP	Všeobecné	RESTful API volanie pre manažment tokenov pre PUSH notifikácie - Odoslanie tokenu - Deaktivácia starého/zneplatneného tokenu
ID_93	Funkčná požiadavka	API-EXT-ZP	Všeobecné	RESTful API volanie pre vyžiadanie dát o užívaní liekov s určením rozsahu pomocou filtrov

RESTful API pre lekárenský softvér

ID POŽIADAVKY	KATEGÓRIA POŽIADAVKY	OBLASŤ POŽIADAVKY	NÁZOV POŽIADAVKY	POPIS POŽIADAVKY
ID_94	Funkčná požiadavka	API-EXT-LEK	Všeobecné	RESTful API volanie pre prihlásenie požívateľa a výmenu autentifikačných tokenov - Prihlásenie menom a heslom - Získanie auth tokenu - Výmena auth tokenov po vypršaní platnosti
ID_95	Funkčná požiadavka	API-EXT-LEK	Všeobecné	RESTful API volanie pre správu používateľských údajov (zmena hesla, kontaktných údajov v KTS,…)
ID_96	Funkčná požiadavka	API-EXT-LEK	Všeobecné	RESTful API volanie pre vyžiadanie informácií o pacientovi
ID_97	Funkčná požiadavka	API-EXT-LEK	Všeobecné	RESTful API volanie pre priradenie zariadenia k používateľovi, prípadne zrušenie priradenia zariadenia