

- **Vývojářskou dokumentaci** (včetně Pravidel vývoje a kódování software), která bude obsahovat zásady vývoje aplikací pro platformu mobilních zařízení. Dále bude zahrnovat popis platformy mobilního zařízení a mobilních služeb, referenční příručku aplikačního programového vybavení (API) platformy mobilního zařízení, popis sestavení dané verze aplikace a programátorský manuál. V případě nutnosti budou v dokumentu uvedeny odkazy na ostatní dokumenty i dokumenty třetích stran.

Prodávající dále zajistí **revizi a doplnění** výše uvedených dokumentů v souvislosti s vydávanými novými verzemi platformy mobilního zařízení, platformy mobilních služeb a mobilních aplikací po dobu trvání projektu.

Prodávající dále zhotoví:

- **Dokumentaci prostředí**, která bude obsahovat informace o nasazení a nastavení jednotlivých komponent dodaného řešení. Součástí bude popis umístění jednotlivých HW komponent a schéma globální architektury dodaného řešení znázorňující komunikaci mezi jednotlivými komponentami.
- **Technický projekt začlenění**, který bude obsahovat popis začlenění dodaného řešení do stávající ICT infrastruktury kupujícího.
- **Implementační plán (plán nasazení)**, který zahrne výčet a popis dílčích aktivit prováděných v rámci implementace, způsob (metodiku) vyhodnocení jejich úspěšnosti a časový harmonogram.
- **Výstupy analýzy a návrhu**, které budou obsahovat globální architekturu řešení, diagram požadavků, diagram případu užití, diagram tříd, diagram perzistence, diagram komponent a diagram nasazení tak, jak je uvedeno v kapitole 13.1.2. Analýza a vývoj SW.
- **Výstupy z přípravy a provedení testování**, které budou obsahovat testovací plán, testovací scénáře, testovací skripty. Dále pak protokoly o provedení testů a dokument Správa neshod.
- **Podklady pro školení**, které budou ve formě prezentace.
- **Dokumenty** vyplývající ze Zadávací dokumentace související s návrhem procesů a opatření pro životní cyklus mapových služeb, životní cyklus lokací, životní cyklus aplikací, konfigurace a verzování, životní cyklus uživatelů, životní cyklus práv a skupin uživatelů, životní cyklus log managementu a životní cyklus služeb pro verzování.

Dokumenty, které vzniknou v rámci zajištění bezpečnosti, jsou uvedeny v kapitole 13.1.1.4.1. Bezpečnostní analýza a dokumentace.

13.1.7. Záruka a servis

Prodávající zajistí, že na dodané plnění bude z jeho strany poskytnuta kupujícímu záruka a servis v souladu s uzavřenou kupní smlouvou. Prodávající bude odpovídat za to, že dodané zboží bude mít vlastnosti uvedené v dodané technické dokumentaci a z hlediska bezpečnosti provozu bude odpovídat platným předpisům ČR a technickým normám.

Záruční doba začne běžet dnem předání zboží kupujícímu a nepoběží po dobu, po kterou Kupující nebude moci užívat zboží pro jeho vady, za které bude odpovídat Prodávající. Záruční doba na zboží bude stanovena v době trvání 36 měsíců od splnění dodávky, kterým se rozumí odevzdání a uvedení zboží do provozu v místě plnění, převzetí zboží osobami zmocněnými kupujícím a dodání všech dokladů nutných k jeho provozování podle právních předpisů a technických norem ČR.

O předání a převzetí zboží bude mezi prodávajícím a kupujícím sepsán předávací protokol ve čtyřech vyhotoveních. V případě zjištěných zjevných vad zboží bude Kupující oprávněn odmítnout jeho

převzetí, což řádně i s důvody potvrdí na příslušném dokladu. Při převzetí zboží proběhne v místě plnění provozní zkouška, které budou přítomny osoby pověřené kupujícím.

Veškeré vady zboží bude kupující povinen uplatnit u prodávajícího bez zbytečného odkladu poté, kdy vadu zjistí, a to formou písemného oznámení o vadě nebo emailem. Na písemné oznámení vad bude Prodávající povinen odpovědět do jednoho pracovního dne ode dne doručení. Pokud tak neučiní, bude se mít za to, že souhlasí s termínem odstranění vad uvedených v oznámení. V případě, že kupující nesdělí při vytknutí vady či vad zboží v rámci záruční doby prodávajícímu jiný požadavek, bude prodávající povinen vytkané vady odstranit bez zbytečného odkladu, nejpozději ve lhůtě do 30 pracovních dnů vlastním nákladem odstranit, nedohodnou-li se smluvní strany v reklamačním protokolu jinak. Bude-li pro prodávajícího technicky proveditelné a nikoliv nepřiměřeně zatěžující, bude povinen provést odstranění vady v místě určeném kupujícím.

Prodávající současně zajistí servisní služby na dodané zboží u kupujícího, bude-li to pro prodávajícího technicky proveditelné a nikoliv nepřiměřeně zatěžující, příp. ve výrobním závodě či v servisních organizacích se smluvním závazkem na provádění servisních prací. Prodávající bude ručit za kvalitu a termínový průběh servisních služeb, ať budou poskytovány výrobním závodem nebo smluvním partnerem.

Prodávající rovněž zajistí záruční servis zařízení dle dohody přímo u kupujícího mobilní servisní službou nebo ve výrobních prostorách u prodávajícího na základě písemného, telefonického, faxového, popř. emailového oznámení kupujícího. Servisní skupina vyjede k odstranění vážné poruchy do 24 hodin po písemném nahlášení závady. Vážná porucha bude definována jako porucha znemožňující bezpečné použití zboží. Porucha bude odstraněna nejpozději do 10 pracovních dnů od převzetí k odstranění poruchy. Pokud oprava bude vyžadovat více než 10 dní, bude po dohodě s uživatelem stanoven závazný harmonogram provedení opravy.

Prodávající na žádost kupujícího po dobu záruky a po jejím skončení povolí provádění záručních prohlídek, revizí a oprav zboží autorizované osobě (nebo způsobilé fyzické osobě), kterou Kupující určí. Této osobě Prodávající poskytne náhradní díly (v ceně obvyklé v místě prodávajícího), přičemž bude oprávněn ji přiměřeně kontrolovat. Kupující zajistí, že autorizovaná osoba bude souhlasit s kontrolou prodávajícího. V případě, že Prodávající bude disponovat servisním místem pro provádění servisních prací na území České republiky, bude možno určení autorizované osoby podle tohoto bodu smlouvy kupujícím po dobu záruky vyloučit.

Uznané reklamace, které nebudou moci být odstraněny opravou, budou řešeny výměnným způsobem vadného dílu za díl nový na náklady prodávajícího.

13.2. Popis nabízeného řešení

Vlastní řešení se sestává z pohledu prodávajícího z následujících klíčových částí:

- Platforma mobilního zařízení (PMZ) – vytváří framework a poskytuje základní služby pro běh zabezpečených aplikací na mobilních zařízeních.
- Platforma mobilních služeb (PMS) – vytváří adekvátní framework na serverové straně a nabízí sdílené služby platformám mobilních zařízení a v nich realizovaných aplikací.
- Referenční aplikace – používá obě výše definované platformy a dodává funkcionalitu lustrace a messaging.
- Integrované lokalizační služby - poskytuje jednotný způsob práce s lokalizačními informacemi pro potřeby PČR. Pro zobrazení budou primárně využity mapové podklady z GIS PČR v režimu on-line i off-line v závislosti na typu koncového uživatelského zařízení.

- Infrastruktura – poskytuje nezbytné HW a SW infrastrukturní elementy pro běh serverových komponent řešení.

Výše uvedené části jsou dále popsány v jednotlivých kapitolách ve větším detailu.

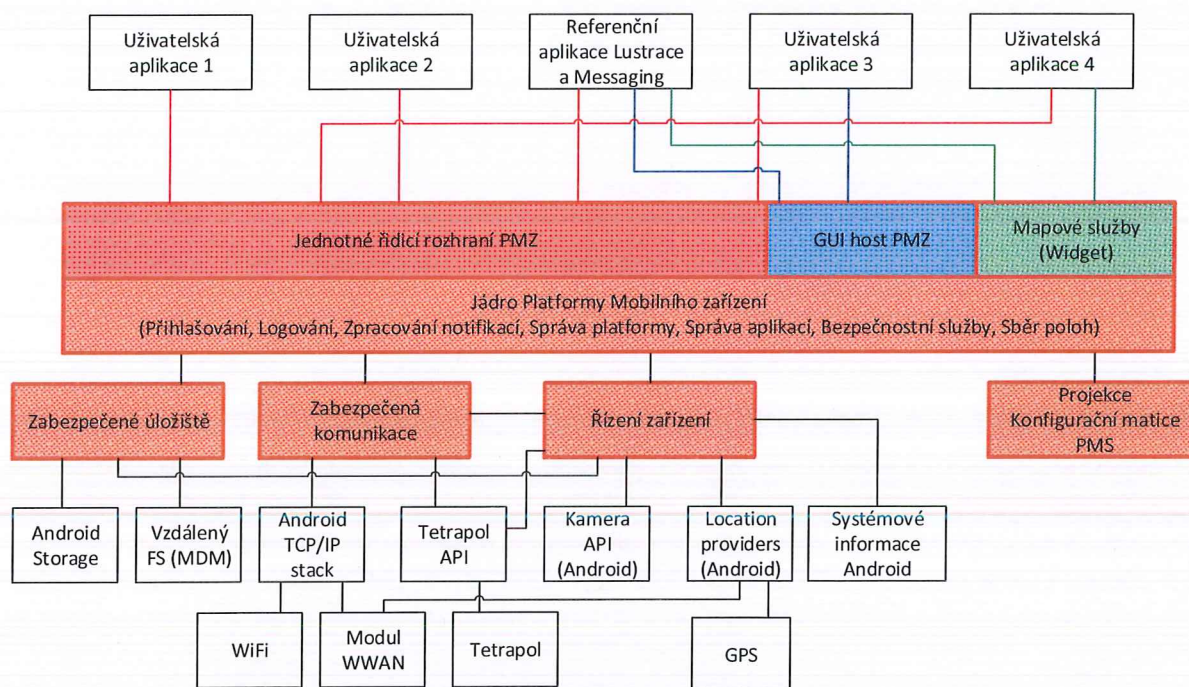
13.2.1. Platforma mobilního zařízení

Platforma mobilního zařízení je v podstatě mobilním klientem Platformy mobilních služeb. Primárně je vyvinuta pro operační systém Google Android s možností portace na ostatní mobilní platformy.

Platforma mobilního zařízení slouží především pro zajištění:

- běhu uživatelských aplikací a zajišťování vymezených služeb pro uživatelské aplikace (hlavní vlastnost tzv. Middleware),
- jednotného systému přenosu aplikačních dat (vícekanálového, zabezpečeného, odolného a robustního),
- jednotného bezpečného a spolehlivého uložení aplikačních dat,
- jednotného uživatelského přístupu k funkcionalitám uživatelských aplikací, platformy mobilních služeb a centrálních systémů PČR,
- jednotného systému auditu a logování pro všechny podřízené aplikace i funkce platformy,
- jednotného přístupu k periferním zařízením (jako je GPS, kamera, atd..) pro platformu i pro její uživatelské aplikace,
- jednotného systému přístupu k mapovým podkladům a vrstvám bodů zájmu a dalších vektorových dat,
- jednotného systému sběru informací o poloze,
- jednotné správy všech konfiguračních parametrů, katalogu uživatelských aplikací.

Z pohledu aplikační architektury je aplikace logicky členěna do několika úrovní:



Aplikační architektura PMZ

- jádro aplikace PMZ zajišťuje všechny základní požadované funkce platformy,
- jednotné řídicí rozhraní PMZ slouží pro komunikaci uživatelských aplikací s platformou,

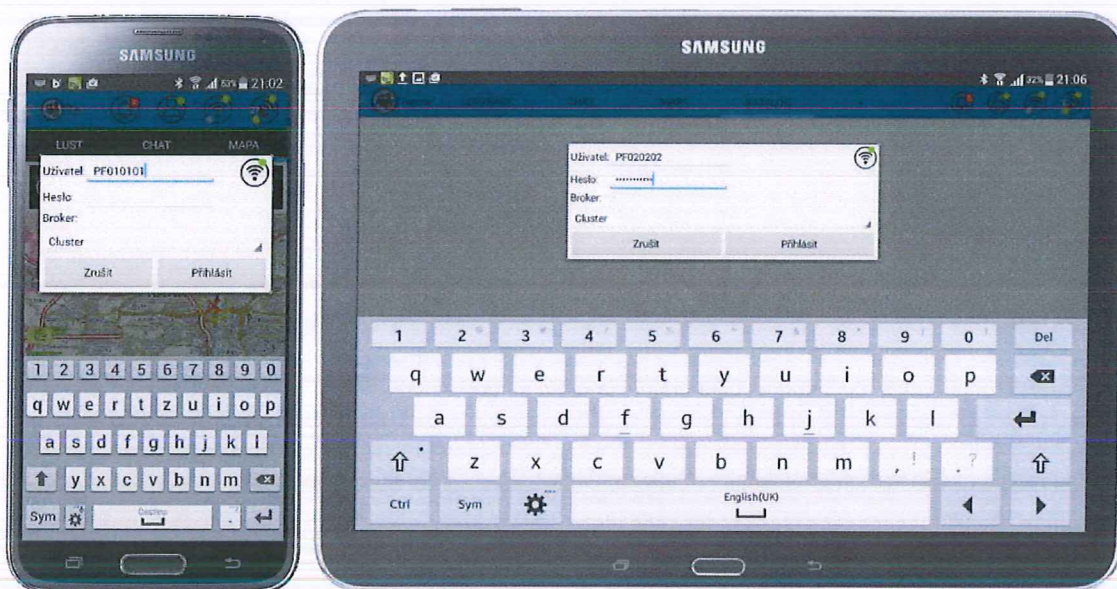
- GUI host PMZ zajišťuje běh uživatelských aplikací, které jsou vytvořeny formou tzv. Widgetu PMZ, tedy jsou spuštěny přímo v GUI aplikace PMZ, dále v textu též tzv. Miniaplikace,
- mapové služby jsou využívány jako interní modul PMZ (obrazovka Mapa), též je ale lze použít jako tzv. Widget pro uživatelské aplikace (zobrazení mapy v kontextu externí uživatelské aplikace).

Konkrétní implementace Platformy mobilního zařízení vychází z nativního jádra a nativní nadstavby pro OS Google Android. Jedná se tedy o plnohodnotný „těžký“ klient, který využívá těchto základních stavebních bloků:

- Android aplikace kombinovaná s Android službou, která je spuštěna trvale na pozadí operačního systému a její prezentovaná část je aktivována na popředí. Aplikace má hlavní aktivitu, která poskytuje uživatelské funkce Přihlášení, Členění na obrazovky, Menu aplikace, Stavové indikátory.
- Systémové úložiště souborů (private store), souborový systém mobilního zařízení včetně kontejneru PMZ na vyjímatelných médiích.
- Technologie relační databáze SQLite (konkrétní implementace použití v rámci PTX Mobile Kit, viz dále).
- Systémové služby OS Google Android.

Základem Platformy mobilního zařízení je standardizovaný modul PTX Mobile Kit, který poskytuje základní funkce pro uložení dat, komunikaci, logování, ovládání periférií, mapových služeb, lokalizace a konfigurace.

Ukázka aplikace Platformy mobilního zařízení:



Ukázka PMZ

Aplikace PMZ (resp. její základní uživatelské rozhraní, tzv. GUI host) je členěna na tzv. obrazovky (zde Lustrace, Chat, Mapa, Katalog), které jsou konfigurovatelné na úrovni Konfigurační matice PMZ. Na těchto obrazovkách jsou pak spouštěny jednotlivé „Miniaplikace“ platformy.



Horní titulkový pruh zobrazuje vedle (nebo nad) seznamem obrazovek indikátory:

- nevyřízených notifikací,
- stavu uživatele,
- stavu a dostupnosti síťového připojení,
- stav a přesnost systému sběru poloh (zjišťování polohy).

Aplikace PMZ poskytuje tzv. SSO (single sign on) mechanismus, který umožňuje využít jednotné přihlášení do PMZ pro všechny uživatelské aplikace.

Stavový panel přehledně a jednoduše zprostředkovává uživateli informace o módu aplikace a důležitých událostech, jako jsou:

- Notifikace (informuje uživatele o příchozích zprávách a požadavcích).
- Status uživatele (informuje uživatele, zda je připojen k serveru a je pro ostatní uživatele systému viditelný jako aktivní).
- Stav připojení (informuje uživatele o stavu komunikačního kanálu a dostupnosti serveru systému).
- Poloha (informuje uživatele o stavu zjišťování a sdílení aktuální polohy s uvedením přesnosti v metrech).

13.2.1.1. Typy uživatelských aplikací

V rámci PMZ rozeznáváme dva hlavní typy Uživatelských aplikací:

- Aplikace spuštěná v rámci GUI platformy jako tzv. **Miniaplikace** Platformy mobilního zařízení, využívající technologii tzv. speciálního Widgetu. Jedná se o preferovaný způsob.
- **Samostatná aplikace** pro OS Google Android (nativní nebo v HTML5 v nativním kontejneru) s vlastním APK a vlastním GUI, která povinně využívá jednotné řídicí rozhraní PMZ pro komunikaci, ukládání dat, logování a další funkce publikované PMZ.

Předtím, než bude aplikace umístěna do aplikačního katalogu, musí být validována, zda splňuje všechny požadavky předepsané pro funkčnost a bezpečnost uživatelských aplikací PMZ a podepsána (code signing) platným elektronickým podpisem na bázi certifikátu správce platformy (PČR).

Každá aplikace se při spuštění musí autentizovat Platformě mobilního zařízení, přičemž je kontrolována mimo jiné také platnost její certifikace.

Doporučením pro běh uživatelských aplikací je nastavení interního Firewallu pomocí MDM tak, aby jediná přípustná síťová komunikace z Uživatelských aplikací byla komunikace s PMZ.

Informace o běhu uživatelských aplikací budou zaznamenávány do logu PMZ a odesílány na PMS. A to včetně statistických informací o využití aplikace, doby práce s ní, atd. V případě kritické chyby v aplikaci je zaznamenána chyba a proveden restart uživatelem. PMZ udržuje informaci o spuštěných miniaplikacích a jejich viewstate. Po restartu PMZ je viewstate obnoven včetně UA.

Systémový monitoring využití zdrojů aplikací realizuje PMZ pouze pro aplikace třídy „Miniaplikace“, pro samostatné aplikace využívá služeb MDM.

13.2.1.2. Jednotné řídicí rozhraní

Jedná se o rozhraní (API) mezi Uživatelskými aplikacemi a Platformou mobilního zařízení. Veškeré služby PMZ budou aplikacím poskytovány přes toto rozhraní formou tzv. IPC (Inter-proces communication). K rozhraní PMZ je možno přistupovat přes lokální socket (TCP/IP) a to výhradně definovaným komunikačním protokolem, jehož popis bude součástí vývojářské dokumentace PMZ. Předpokládá se, že Uživatelské aplikace se připojí na jednotné řídicí rozhraní v okamžiku startu a ukončí spojení přes řídicí rozhraní v okamžiku ukončení činnosti. Typický pracovní cyklus komunikace UA s Jednotným řídicím rozhraním je složen z těchto částí:

- spojení (socket connect) UA->PMZ,
- příkaz k autentizaci UA (součástí je i prezentace elektronického podpisu UA),
- ověření UA na PMZ a aktivace povolených funkcí (komunikace, úložiště),
- push aktuální konfigurace UA ze strany PMZ,
- jednotlivé operace UA vs. PMZ (příjem dat, odeslání dat, práce s úložištěm, logování, atd..),
- uložení změn v konfiguraci UA,
- ukončení spojení,
- ukončení UA.

13.2.1.3. Modul zabezpečené komunikace

Spolehlivý a bezpečný přenos dat mezi mobilním zařízením a systémy v zázemí kupujícího (včetně vlastní Platformy mobilních služeb) je základním stavebním kamenem celého řešení.

Přenosový protokol navržený pro platformu je unikátní kombinací nejnovějších poznatků z mobilního světa a souhrnem dosavadních zkušeností prodávajícího s provozem obdobných systémů, zohledňující i specifický model způsobu činnosti kupujícího.

Modul zabezpečené komunikace využívá pro přenos dat základní komunikační jednotku, tzv. **zprávu** (message) a svým realizovaným pojetím se podobá tzv. komunikačnímu brokeru. Zpráva má vždy tyto základní atributy:

- odesílatele a příjemce,
- data a časy vytvoření, doručení, zpracování v cílové aplikaci,
- prioritu,
- preferenci komunikačního kanálu (např. přenášet pouze Tetrapol, přenášet jen po WiFi, atd.),
- základní obsah,
- binární přílohy.

Příkladem dat posílaných jako zprávy jsou například:

- požadavek na přihlášení uživatele / odpověď na požadavek na přihlášení uživatele,
- požadavek na provedení lustrace / odpověď s výsledky lustrace,
- notifikace,
- přenos vrstvy (přílohou je soubor s obsahem vrstvy),
- přenos bodu zájmu mapy,
- systémová zpráva (například obraz konfigurační matice PMS pro přihlášeného uživatele a konkrétní zařízení).

Mechanismus přenosu zpráv využívá principu inteligentní alokace komunikačních kanálů. Před vlastním zahájením komunikace je načtena definice povolených komunikačních kanálů a ověření jejich aktuální dostupnosti (zařízení připojeno k: WiFi, Mobilním datům, Tetrapol). V závislosti na

typu přenášených dat je připravená zpráva předána jednotlivým poskytovatelům komunikačních kanálů k přenosu. V praxi to znamená, že systém na základě inteligentní matice přenosu vypočítá, pro kterou zprávu má alokovat který komunikační kanál a ten pro přenos využije. Pro kritická data může systém přenosu dat alokovat více komunikačních kanálů naráz. V některých případech může odeslat zprávu jedním kanálem a její přílohu například druhým kanálem. Vše záleží na nastavení konfigurační matice PMS. V případě nedostupnosti některých komunikačních kanálů nebo jejich dočasnému přetížení, může systém jeho využití dočasně potlačit.

Pro velká data (například mapové podklady) není systém zpráv zcela vyhovující a proto je přenos dat realizován prostřednictvím tzv. Streamu. Ovládání přenosu dat je řízeno systémovými zprávami (žádost o publikaci dat, zpráva o otevření publikace, ukončení publikace).

Pro vlastní přenos dat využívá modul tři základní poskytovatele komunikačních kanálů:

- TCP/IP + UDP pro zprávy (spojení je navazováno a udržováno vždy z mobilního zařízení směrem k serveru) – poskytovatel se využívá pro síť WiFi a Mobilní data.
- Tetrapol UDP – pro síť standardu Tetrapol. Předpokládá se sériové spojení s RDST síť PEGAS. Spojení je možno navázat oběma směry (server-klient i klient-server). Mechanismus server-klient využívá RFSI RDST pro PUSH přenos.
- TCP/IP stream (HTTPS) pro velká data (například pro mapové podklady) – spojení vždy zahajuje klient, řízení přenosu dat probíhá přes systémové zprávy.

Mechanismy podporující přenos dat v rámci Modulu zabezpečené komunikace jsou především:

- PUSH mechanismus – vlastní implementace procesu PUSH mezi PMS a PMZ. Proces doručení zprávy nevyžaduje externího poskytovatele PUSH komunikace (například Google Cloud Messaging) a je plně autonomní. Mechanismus není implementován na principu tzv. pollingu, kdy klient neustále oslovuje server, neboť tento způsob je zcela nevhodný jak ke komunikačnímu kanálu, tak ke kapacitě baterií mobilního zařízení. Mechanismus navrhovaný v popsaném řešení využívá kombinace TCP/UDP spojení, které je udržováno s velmi malými nároky na objem dat a výdrž baterie. V případě poskytovatele Tetrapol je PUSH přenos nativně realizován navázáním spojení ve směru Server->Klient.
- Komprese dat v komunikačním kanále – všechna data jsou před šifrováním komprimována a je potlačena komprese na dalších přenosových komponentách (komprese šifrovaných dat je již neúčinná).
- Fragmentace dat a odesílání po částech – větší data jsou fragmentována (rozdělena na části) jednotlivými poskytovateli komunikačních kanálů, přičemž je podporován opakovaný přenos bloků (při výpadku spojení), transakčnost přenosu (zajištění kompletního a konzistentního výsledku přenosu na obou stranách) a rychlost (nepřenáší se redundantně data).

13.2.1.3.1. Proces personalizace mobilního zařízení (aktivace PMZ)

Proces personalizace mobilního zařízení probíhá následovně:

- inicializace zabezpečeného úložiště PKI PMZ (nastavení PIN, vytvoření kontejnerů, atd.) – v závislosti na vybavení mobilního zařízení může být úložiště buď v rámci OS, nebo externí (např. HSM ve formě paměťové karty, nebo HSM na SIM kartě, a podobně),
- nahrání certifikátu root certifikační autority do zabezpečeného úložiště mobilního zařízení,
- generování klíčového páru AK_DEV1^{PRIV} a AK_DEV1^{PUB} v zabezpečeném úložišti,
- generování první žádosti o certifikát CERT_DEV1,

- odeslání žádosti bezpečnou cestou na CA PMS (detaily je nutné definován v rámci definice životního cyklu, který bude navržen s ohledem na procesy kupujícího a dodávajícího část A - MDM),
- instalace vydaného certifikátu CERT_DEV1 do zařízení (detaily je nutné definován v rámci definice životního cyklu, který bude navržen s ohledem na procesy kupujícího a dodávajícího část A -MDM).

13.2.1.3.2. Prerekvizity zabezpečené komunikace

Prerekvizity zabezpečené komunikace jsou následující:

- root CA (CERT_CA) nahráno v zabezpečeném úložišti zařízení,
- platný certifikát mobilního zařízení (CERT_DEV1) včetně přístupu k privátnímu klíče (AK_DEV1^{PRIV}) v zabezpečeném úložišti zařízení,
- platný certifikát CERT_PMS vydaný společnou CA PMS na straně platformy mobilních služeb,
- pro asymetrickou kryptografii předpokládáme využití algoritmů RSA s délkou klíčů 2048 a 4096 bit,
- pro symetrickou kryptografii předpokládáme využití algoritmů AES s délkou klíče 256bit,
- pro elektronické podepisování obsahu předpokládáme využití hash funkce SHA256 a RSA algoritmů,
- obě strany komunikace znají předsdílené tajemství (tzv. sůl), tato je součástí binárního kódu PMS i PMZ.

13.2.1.3.3. Jednotlivé fáze komunikace PMZ vs. PMS

Vlastní fáze komunikace mezi PMZ a PMS jsou následující:

- connect / reconnect [ověření zařízení]-> Iniciální fáze ustavení komunikačního kanálu. Cílem je ověření mobilního zařízení vůči PMS, ověření pravosti PMS pro mobilní zařízení, výměna komunikačních klíčů a ustavení síťového propojení.

V rámci této fáze mobilní zařízení vygeneruje pomocí PNG (Prime Numbers Generator) první část jednorázového komunikačního klíče (SK_COMM_part1) a tento kryptuje (společně se solí) pomocí veřejného klíče serverové části PMS (AK_PMS1^{PUB}). K požadavku přidá také UID zařízení. Celý požadavek na navázání komunikace podepisuje svým soukromým klíčem k autentizačnímu certifikátu (AK_DEV1^{PRIV}). Následně je požadavek ve formě zprávy odeslán vybranými komunikačními kanály.

PMS ověří elektronický podpis požadavku na connect (pomocí AK_DEV1^{PRIV}) a ověří registraci mobilního zařízení podle UID a zkontroluje revokaci jeho certifikátu CERT_DEV1. Pokud je identita zařízení považována za prokázanou a platnou, vygeneruje server svou část jednorázového komunikačního klíče (SK_COMM_part2) a tuto společně se solí kryptuje veřejným klíčem mobilního zařízení (AK_DEV1^{PUB}), k obsahu přidá další řídicí data (např. část konfigurační matice PMS relevantní pro zařízení, certifikát CERT_PMS pokud je potřeba) a celý obsah podepíše svým privátním klíčem (AK_PMS1^{PRIV}). Celou zprávu odešle vybranými komunikačními kanály.

PMZ po přijetí ověří validitu odpovědi (ověření elektronického podpisu pomocí řetězce důvěry CERT_CA -> CERT_PMS a veřejného klíče PMS (AK_PMS1^{PUB}) a pomocí (AK_DEV1^{PRIV}) dekoduje druhou část komunikačního klíče (SK_COMM_part2).

Tímto krokem jsou obě strany komunikačního řetězce ověřeny a znají dočasný kompletní komunikační klíč SK_COMM a také je na straně PMZ nahrána aktivní část konfigurační matice PMS. V závislosti na nastavení konfigurační matice PMS je proces connect/reconnect opakován (nastavená expirace klíče SK_COMM).

- login [ověření uživatele]-> Je odeslána aktuální sada pověření uživatele (přihlašovací jméno, hash hesla, doplňkové údaje) ve formě zprávy. Zpráva je šifrována prostřednictvím klíče SK_COMM. Na straně PMS je provedena autentizace uživatele a vygenerována sada autorizačních pověření a doplňková část konfigurační matice PMS vztahující se k uživateli (povolené aplikace, povolené komunikace, parametry běhu, atd..). Návratová hodnota je odeslána jako šifrovaná zpráva vybranými kanály na mobilní zařízení (PMZ) kde je provedena aplikace politik, autorizace uživatele k službám PMZ a aplikace konfigurace.
- příjem / odesílání aplikačních a systémových zpráv -> za běhu aplikace dochází k odesílání zpráv z fronty na zabezpečeném úložišti na mobilním zařízení a k příjmu zpráv z PMS a jejich uložení do zabezpečeného úložiště pro zpracování v PMZ nebo v uživatelských aplikacích. V podstatě všechna aplikační data s výjimkou velkých dat (data uživ. aplikací, logy, nastavení, atd.) jsou předávána touto formou.
- načítání velkých dat -> PMS zašle systémovou zprávou seznam dostupných dat (seznamy mapových podkladů, vrstev, atd. dostupných uživateli). PMZ na základě vnitřní logiky vyhodnotí, které součásti potřebuje využívat a požádá PMS o stream přístup k těmto datům. PMS odpoví systémovou zprávou se seznamem otevřených HTTPS streams k žádaným součástem. PMZ otevírá dle potřeby streams a stahuje požadovaná data a ukládá je do Zabezpečeného úložiště dat.
- logout -> je odeslána zpráva o odhlášení uživatele.

13.2.1.3.4. Konfigurace zabezpečené komunikace

Mimo jiné, jsou pomocí Konfigurační matice PMS předávány také konfigurační parametry, které jsou zohledňovány v modulu zabezpečené komunikace. Jedná se především o tyto parametry:

- **názvy povolených APN bodů pro mobilní datové připojení,**
Pokud není UDT připojen na jeden z povolených APN bodů, je uživateli signalizován problém s komunikací a PMZ ani nezahajuje komunikaci s PMS.
- **názvy povolených SSID pro bezdrátové WiFi sítě a povolené autentizační mechanismy,**
Pokud platforma detekuje nepovolený aktivní WiFi přístupový bod, odmítne komunikaci, případně vyžádá přechod na mobilní datové připojení, rovněž pokud zabezpečení WiFi neodpovídá nastavené konfiguraci, komunikace není přes tento kanál povolena.
- **priorita použití komunikačních kanálů pro přenášená data.**
Pro jednotlivé typy přenášených dat (např. data lustrace, data chatu, atd.) je v obrazu konfigurační matice PMS pro aktuální kombinaci zařízení, uživatele a aplikace nastaveno, jaká data s jakou prioritou, mají být přenášena jakým kanálem. Například:
 - data lustrace preferovaně kanálem TETRA POL, nouzově GSM,
 - data messaging preferovaně kanálem WiFi, poté GSM, poté TETRA PO,
 - fotografie – náhledy přes GSM, plné rozlišení jen od LTE výše (LTE a WiFi),
 - atd.

13.2.1.3.5. Vzájemná komunikace mezi moduly a Uživatelskými aplikacemi

Modul zabezpečené komunikace realizuje také interní komunikaci na PMZ. Na základě obrazu Konfigurační matice PMS. Uživatelské aplikace (UA) mezi sebou komunikují výhradně přes Komunikační modul PMZ, nikoli spolu napřímo. Veškerá komunikace je logována v závislosti na nastavení Konfigurační matice PMS.

Komunikace probíhá přes Jednotné řídicí rozhraní PMZ (JŘR). Zdrojová UA vyžádá přenos dat do cílové UA pomocí volání rozhraní JŘR, PMZ vyhodnotí, zda je požadovaná komunikace možná a v případě, že je povolena, provede notifikaci cílové UA a přenos dat prostřednictvím modulu Zabezpečeného úložiště nebo přímo.

13.2.1.3.6. Sběr dat pro QoS moduly

Každá zahájená komunikace je statisticky sledována a PMZ v reálném čase dopočítává úspěšnost přenosu dat přes jednotlivé komunikační kanály v obou směrech a jejich dostupnost. Tato data pak buďto na vyžádání PMS nebo v nastavených intervalech (dle aktuálního obrazu Konfigurační matice) odesílá na PMS pro další vyhodnocení.

Statistika QoS je vyhodnocována i lokálně a pokud je tato funkcionality nastavena v konfigurační matici PMS, může být na základě lokální analýzy QoS na některém kanále, tento kanál pro přenos dat dočasně potlačen.

13.2.1.4. Zabezpečené úložiště dat

Zabezpečené úložiště dat (ZUD) poskytuje univerzální a bezpečný způsob ukládání dat pro aplikace Platformy Mobilního Zařízení i pro platformu samotnou. Zabezpečené úložiště dat může být vytvořeno v interním paměťovém prostoru mobilního zařízení nebo na vložené paměťové kartě.

Pokud se jedná o ZUD v interním paměťovém prostoru, je tato ZUD vytvořena v tzv. private storage aplikace Platformy mobilního zařízení. Tím je zajištěno, že uživatel ani operační systém nemá žádným způsobem možnost přístupu k datům jednotlivých ZUD.

V případě ZUD na vloženém paměťovém médiu dojde při vložení ke kontrole, zda některá z aplikací, případně sama platforma vyžaduje ukládání dat na externí média. Pokud je požadavek na využití tohoto typu úložiště, provedou se inicializační kroky k inicializaci média. Úložiště bude tzv. „spárováno s mobilním zařízením“. Proces inicializace je spojen s formátováním média a zápisem elektronického podpisu zařízení na médium. Inicializované úložiště lze vyjmout a vložit znovu bez ztráty dat.

Úložiště má vždy svého vlastníka a to buď aplikaci PMZ nebo PMZ samotné. Ve spolupráci s Konfigurační maticí Platformy mobilních služeb je možné nastavit limit velikosti dat, která je možné uložit jednotlivými aplikacemi. Všechna data v ZUD jsou šifrována a autentizována.

ZUD je pro uživatelské aplikace přístupné výhradně prostřednictvím Jednotného řídicího rozhraní Platformy Mobilního Zařízení. Platforma Mobilního Zařízení zajišťuje při zprostředkování služeb Zabezpečeného úložiště řízený přístup k úložišti nejen na úrovni aplikace, ale i uživatele. V závislosti na určení dat (specifikuje konfigurační matice PMS, přetěžuje uživatelská aplikace), jsou data buď sdílená platformě (dostupná všem vyjmenovaným aplikacím), sdílená v aplikaci (dostupná všem uživatelům konkrétní aplikace), sdílená aplikacím (dostupná konkrétnímu uživateli ve více aplikacích) nebo dedikovaná (dostupná pouze konkrétnímu uživateli konkrétní aplikace).

Platforma Mobilního Zařízení poskytuje přehled o všech využitých zdrojích v rámci Zabezpečeného úložiště dat.

Zabezpečené úložiště dat poskytuje možnost pro každý ukládaný záznam přidat tzv. „doplňkové klíče“, podle kterých je úložiště indexováno. Pro každý datový kontejner je možné tyto klíče definovat dynamicky (tedy jejich význam ve smyslu klíč-hodnota pomocí slovníku).

13.2.1.4.1. Dočasné zabezpečené úložiště dat

Dočasné ZUD je určeno převážně k ukládání dat, která jsou určena k odeslání na Platformu mobilních služeb. Nad dočasným ZUD běží garbage collector, který zajišťuje odstranění nepotřebných dat a tím uvolnění prostoru pro nová data. Pokud i přesto pro nová data již není prostor, je uložení dat odmítnuto.

13.2.1.4.2. Permanentní zabezpečené úložiště dat

Permanentní ZUD je určeno převážně k ukládání konfiguračních dat jednotlivých aplikací i samotné Platformy mobilních služeb. Do permanentního ZUD jsou také ukládána data s větším objemem, aby nedošlo k jejich výmazu. Nad tímto typem úložiště neběží garbage collector, takže nedochází k odstranění dat, pokud již nejsou potřebná.

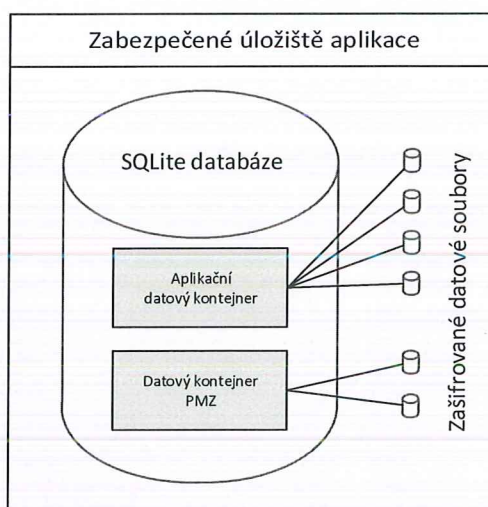
13.2.1.4.3. Služby poskytované Zabezpečeným úložištěm dat

Zabezpečené úložiště dat poskytuje následující služby:

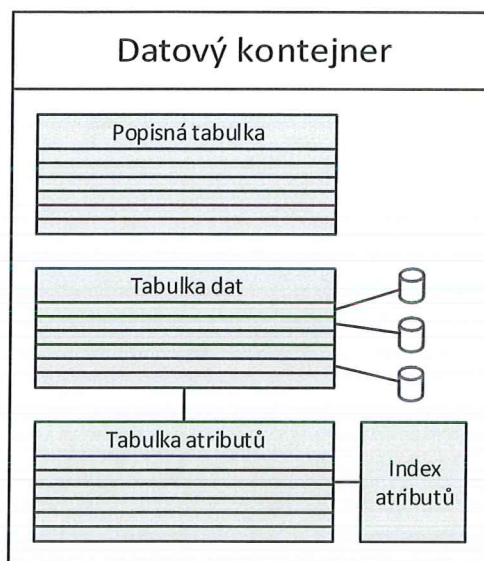
- Zápis dat uživatelskou aplikací nebo platformou. Data jsou zapisována do ZUD, které je specifické pro uživatelskou aplikaci nebo Platformu. Při zápisu dat je kontrolováno překročení povolené maximální velikosti dat.
- Čtení dat uživatelskou aplikací.
- Automatické čištění úložiště dat (garbage collector).
- Automatické čištění úložiště dat na bázi událostí PMZ .
- Transparentní šifrování všech dat.
- Výmaz všech dat v úložišti jako reakce na externí požadavek PMS nebo interní událost PMZ.
- Notifikace o nových datech a to jak pro PMZ, tak pro uživatelskou aplikaci (např. „přijaty nové zprávy“).
- Komunikace mezi PMZ a Aplikacemi PMZ.

13.2.1.4.4. Implementace Zabezpečeného úložiště dat

Vlastní implementace úložiště je realizována jako hybridní mechanismus šifrovaných binárních souborů se stream přístupem a více logicky propojených databázových souborů SQLite Lite. Každému aplikačnímu úložišti odpovídá jeden databázový soubor SQLite a sada šifrovaných souborů, které obsahují data větší velikosti. Seznam všech úložišť a informace o nich jsou uloženy ve zvláštním databázovém souboru SQLite. Aplikační úložiště obsahuje datové kontejnery. Jeden datový kontejner slouží pro ukládání vlastních dat aplikace, druhý pro komunikaci mezi PMZ a aplikací. PMZ sem ukládá zprávy určené pro aplikaci, které úložiště patří. Po uložení dat PMZ je vygenerován event, který signalizuje aplikaci, že v datovém kontejneru jsou uložena nová data. V kontejneru pro vlastní data aplikace je rozlišeno, zda uložená data patří některému z uživatelů, nebo jsou platná v kontextu celé aplikace.



Struktura zabezpečeného úložiště dat



Struktura datového kontejneru

Tabulka atributů	
Klíč	Řetězec klíč:hodnota

Struktura tabulky atributů

Tabulka dat								
Klíč	Uloženo	Expirace	Uživatel	IV	Zašifrovaná JSON data	Integrovní součet	Umístění zašifrovaného souboru	Délka zašifrovaného souboru

Struktura tabulky dat dočasného zabezpečeného úložiště

Tabulka dat								
Klíč	Uloženo	Uživatel	IV	Zašifrovaná JSON data	Integrovní součet	Umístění zašifrovaného souboru	Délka zašifrovaného souboru	

Struktura tabulky dat dočasného permanentního úložiště

13.2.1.4.5. Způsob šifrování Zabezpečeného úložiště dat

Zabezpečení úložiště dat zajišťuje ochranu uložených dat šifrováním, s transparentním přístupem pro nadřazené vrstvy (PMZ, uživatelské aplikace) a to jak pro „transakční“ data uložená v interní paměti, tak pro „velká“ data uložená na externím úložišti.

Data v úložišti se šifrují klíčem SSEK (Secure Storage Encryption Key) a autentizují klíčem SSAK (Secure Storage Authentication Key). Pro derivaci těchto klíčů se použije neveřejný algoritmus derivace klíče. Jeho vstupy jsou sériové číslo mobilního zařízení a master klíč, který je známý pouze serveru PMS. Použití master klíče je zvoleno, kvůli možnosti odšifrování dat vytvořených aplikacemi Platformy i Platformou samotnou mimo mobilní zařízení (např. pro forenzní účely). Klíče vytváří server PMS a jsou distribuovány na zařízení v rámci šifrovaného přenosu dat.

Data aplikací, která se šifrují, přichází z aplikací nebo vlastní Platformy ve formátu JSON (JavaScript Object Notation). Pro každý záznam je vygenerován inicializační vektor IV. Pomocí IV a šifry AES256 v modu CFB (Cipher Feedback) je vstupní JSON string zašifrován. Z klíče ukládaného záznamu, IV, a šifrovaného textu se vypočte HMAC (Hash Message Authentication Code). Pokud jsou součástí ukládaných dat i „velká“ data, která se ukládají externě do zašifrovaného souboru, je pointer na jejich umístění přidán do výpočtu HMAC. Všechny tyto části jsou potom uloženy do záznamu tabulky dat datového kontejneru.

V případě, kdy jsou součástí dat i „velká“ data, jsou tato data ukládána do souboru. Je vygenerován inicializační vektor IV. Pomocí IV a šifry AES256 v modu CFB, jsou „velká“ data zašifrována a uložena

včetně IV do souboru. Současně se šifrováním se provádí také výpočet HMAC. Vstupem je HMAC příslušného záznamu v tabulce dat datového kontejneru, (který byl vytvořen výše popsaným postupem), IV a zašifrovaný obsah souboru. HMAC je připojen na konec zašifrovaného souboru. Je zjištěna kompletní délka uloženého souboru, která je následně zapsána do záznamu v tabulce dat datového kontejneru. Tento údaj je potom využíván k výpočtu velikosti obsazeného prostoru úložiště.

13.2.1.5. Správa platformy

Správu platformy zajišťuje jádro PMZ. Základním konfiguračním prvkem je obraz Konfigurační matice Platformy mobilních služeb replikovaný na mobilním zařízení a uložený v zabezpečeném úložišti. Základní hodnoty Konfigurační matice jsou distribuovány také společně s instalačním balíkem PMZ, pro účely prvotního nastavení kritických parametrů než dojde k vytvoření plného obrazu Konfigurační matice prostřednictvím Zabezpečené komunikace – stažením parametrů z PMS. Konfigurační maticí se řídí všechny komponenty PMZ ve všech ohledech a to včetně Uživatelských aplikací.

Jádro platformy zajišťuje nastavení chování PMZ podle hodnot jednotlivých parametrů a také distribuci konfigurací jednotlivých uživatelských aplikací a to včetně notifikací o změnách. Uživatelské aplikace přistupují ke své konfiguraci prostřednictvím Jednotného řídicího rozhraní. Stejně tak, jako uživatelské aplikace prostřednictvím JŘR svou konfiguraci na PMZ aktualizují (pouze části, které jsou povoleny aplikaci aktualizovat).

Modul poskytuje informace a aktuální konfiguraci (jak platformy, tak UA) na vyžádání také Platformě mobilních služeb, pro účely vyhodnocování, statistik a technické podpory.

13.2.1.6. Sběr poloh

Jednou ze základních vlastností Platformy mobilního zařízení je sběr informací o poloze. Chování modulu Sběr poloh je plně řízeno dle Konfigurační matice PMS. Pro zjišťování aktuální polohy mobilního zařízení jsou použity tyto poskytovatele polohy (location providers):

- GPS provider (přesnost desítky až jednotky metrů) – využívá vestavěnou GPS,
- GSM location provider – využívá polohu z buněk sítě, v případě tzv. intranetového režimu, s vypnutou WiFi může být poloha silně nepřesná (přesnost několik kilometrů až desítky metrů). Součástí dodávky jsou konzultace pro tým infrastruktury kupujícího pro správné nastavení prostupů intranet -> Internet pro přesnější zjišťování polohy (využití lokalizačních služeb Google), v případě, že Kupující tuto službu povolí,
- MATRA location provider – využívá přibližnou polohu ze sítě buněk TETRAPOL, slouží pouze k orientačnímu určení kraje, případně části kraje (přesnost desítky kilometrů).

Platforma mobilního zařízení využívá vlastní geo-kodér (převod GPS souřadnic na přibližnou adresu) na bázi mapového podkladu OpenStreetMap, který funguje bez potřeby připojení PMZ a PMS k Internetu.

Každý z poskytovatelů polohy má v konfigurační matici vlastní konfiguraci, jak často se má poloha zjišťovat (krok vzdálenosti, krok času) v závislosti na stavu baterie a použití zařízení. Pokud je to v konfiguraci matice povoleno, lze některé parametry měnit i uživatelsky (uživatel může dočasně zakázat sběr nebo odesílání polohy).

Modul provádí inteligentní odesílání polohy do Platformy mobilních služeb, opět v závislosti na nastavení konfigurační matice a to zvlášť pro jednotlivé poskytovatele polohy.

Nastavení sběru a odesílání polohy může být provedeno například v takovéto kombinaci:

- sbírat polohu z GPS kontinuálně (krok 0 sec, 0 min) a zároveň
 - odeslat binární soubor s logem polohy 1x za 10 minut s nízkou prioritou,
 - odeslat 1x za 10 sec. při pohybu o více než 5m nejlepší polohu za posledních 10 sec. s vysokou prioritou (sdílení polohy uživatele).
- sbírat kontrolní polohu z GSM a
 - odeslat 1x za minutu.

Modul dále zajišťuje distribuci informací o poloze také Uživatelským aplikacím prostřednictvím Jednotného řídicího rozhraní.

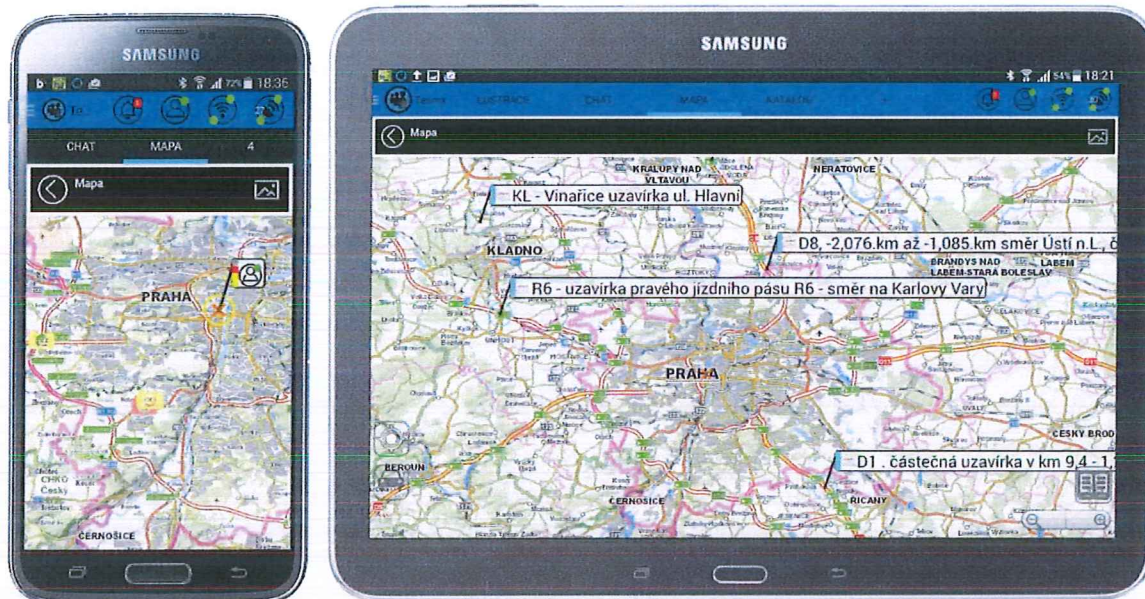
13.2.1.7. Poskytování mapových služeb

Modul zprostředkovává zobrazení rastrových map a přístup k nim, je jedním z několika modulů v rámci PMZ, které mají vlastní grafické uživatelské rozhraní. Modul je realizován víceúrovňově a plně využívá dalších submodulů PMZ. Pro načítání mapových dat využívá Modulu zabezpečené komunikace, přičemž dávkové načítání mapových dat probíhá pouze při dostupnosti komunikačního kanálu s větší šířkou přenosového pásma (WiFi, LTE). Načítání dat je optimalizováno a probíhá tzv. „rozdílovým způsobem“. Zdrojem mapových dat je vždy modul Evidování mapových podkladů PMS (EMP). Modul obecně umožňuje tzv. online přístup (stahování dlaždice mapy tzv. „on demand“ v terénu z modulu EMP, mapové dlaždice průběžně ukládá do zabezpečeného úložiště, případně lze mapy na zařízení replikovat (tzv. offline přístup). Dle konfigurace EMP na konfigurační matici jsou na mobilním zařízení zpřístupněny pouze konkrétní mapové podklady a jejich části (vybrané území, vybrané vrstvy atd.).

Pro uložení mapových dat na mobilním zařízení využívá modul samozřejmě Zabezpečeného úložiště dat.

Modul zajišťuje především tyto služby:

- stahování a ukládání mapových podkladů z PMS do PMZ,
- vykreslování mapy uživateli (mapové podklady),
- vykreslování vektorových dat uživateli (body zájmu, mapové vrstvy, objekty, atd.),
- interakci s uživatelem (vytvoření bodu zájmu, editace, atd.).



Ukázka zobrazení mapových pokladů v modulu Poskytování mapových služeb

Modul Poskytování mapových služeb umožňuje tyto operace se zobrazenou mapou:

- výběr mapového podkladu (pokud je dostupných více podkladů) : kartografická mapa, ortofoto, atd.,
- zobrazení ovládacích prvků mapy na kliknutí,
- přiblížení / oddálení (zoom) pomocí gest, dvojitého poklepání a tlačítek + a −,
- posun mapy podržením a potažením (scroll),
- centrování mapy na aktuální polohu uživatele,
- automatickou volbu měřítka podle rychlosti uživatele,
- navigační mód mapy (udržuje na mapě stále zobrazený cíl a aktuální polohu) – automaticky nastavovaný zoom,
- výběr zobrazených vrstev na mapě s nastavením:
 - zobrazení značky v barvě vrstvy (pokud je znám směr pohybu, značka obsahuje i indikátor směru, pokud je známa přesnost polohového údaje, po kliknutí na značku je zobrazen kruh přesnosti),
 - zobrazení vlajky s rozlišením (ikona vrstvy a barevný pruh),
 - zobrazení textového popisu (např. označení uživatele, volací znak, atd.),
- „otisk“ mapy do schránky PMZ pro další zpracování (např. zakres do mapy jako do fotografie, odeslání snímku mapy modulem Messaging, atd.).

V rámci GUI PMZ je přístupná také volba Uživatelských nastavení, kde může uživatel (pokud k tomu má příslušná oprávnění), nastavit své preference stahování mapových podkladů.

Další funkce modulu Poskytování mapových služeb jsou také popsány v rámci kapitoly Způsob splnění požadavků kupujícího (dle Přílohy č. 2 k ZD).

13.2.1.8. Zpracování notifikací

Modul Zpracování notifikací využívá pro přenos notifikací službu PUSH modulu zabezpečené komunikace. V případě, že je na zařízení dostupná TCP/IP konektivita služba PUSH udržuje stálé TCP/IP spojení s PMS. Konektivita TETRAPOL používá pro službu PUSH nativní protokol navázání spojení server-> stanice. Tím je zajištěna komunikace ve směru PMS->PMZ s minimálními nároky na

objem přenášených dat bez nutnosti periodické kontroly stavu PUSH dat ve směru PMZ->PMS. V případě, že notifikaci není možné okamžitě doručit z důvodu nedostupnosti zařízení, jsou notifikace ukládány v PMS. Po připojení zařízení k PMS jsou všechny nashromážděné notifikace odeslány.

Notifikace se přenášejí ve formátu JSON, kde jsou v jednotlivých položkách uložena všechna potřebná data:

- Adresa příjemce
- Odesílatel
- Priorita
- Platnost notifikace
- Obsah notifikace
- Doplnkové atributy (lze definovat dynamicky klíč/hodnota)

Kompletní obsah notifikace je doručen do PMZ prostřednictvím služby PUSH modulu Zabezpečená komunikace. Notifikace je uložena do Datového kontejneru notifikací v ZUD PMZ. Další zpracování probíhá podle nastavení v poli Adresa příjemce.

Pokud je notifikace adresována modulu nebo aplikaci, je tato notifikace uložena do Datového kontejneru PMZ v ZUD aplikace nebo modulu, kterému je notifikace adresována. Na základě toho je pro aplikaci vygenerován event o zápisu dat do Datového kontejneru PMZ. Další reakce je již na konkrétní aplikaci nebo modulu. Po zpracování notifikace modulem nebo aplikací, je voláním API potvrzeno přijetí a zpracování notifikace. Volání API vygeneruje Potvrzení o přečtení a uloží ho do ZUD PMZ. Odtud je standardním způsobem odesláno do PMS. Zároveň dojde k výmazu zpracované notifikace z Datového kontejneru PMZ příslušné aplikace.

Zprávy, které jsou adresovány uživatelům, jsou ukládány pouze do Datového kontejneru notifikací v ZUD PMZ. Další zpracování pak zajišťuje samotná PMZ.

Zobrazení notifikace řídí PMZ. Pokud je uživatel přihlášen, zobrazí se mu seznam přijatých notifikací okamžitě po jejich přijetí, na základě jejich uložení do datového kontejneru notifikací ZUD PMZ. Po každém přihlášení uživatele je datový kontejner notifikací prohledán, jestli v něm existují notifikace, které jsou označeny jako nepřečtené. Výsledný seznam se zobrazí uživateli. Po přečtení notifikace je vygenerováno potvrzení o přečtení a je uloženo do ZUD PMZ. Odtud je standardním způsobem odesláno do PMS. Existence nepřečtené notifikace je vždy signalizována prostředky notifikace operačního systému.

Všechny notifikace jsou uloženy v Datovém kontejneru notifikací ZUD PMZ. Uživatel má možnost zobrazit uložená data notifikací a provádět jejich filtrování. Filtrování je možné provádět nad všemi atributy notifikací. Přístup je řízen nastavením práv v konfigurační matici PMS.

13.2.1.9. Logování

Systém logování je založen na Zabezpečeném úložišti dat, tím je zajištěno, že data logu jsou zašifrována. Existuje pouze jedno centrální ZUD pro logy. ZUD pro logy zakládá a obsluhuje Jádro Platformy mobilního zařízení. Funkce logu jsou přístupné uživatelským aplikacím přes Jednotné řídicí rozhraní PMZ. Vlastní zápis do logu provádí Jádro Platformy Mobilního zařízení, které do logu zapisuje i vlastní zprávy. Promazávání logu je zajištěno garbage collectorem Zabezpečeného úložiště dat.

Do logu se zapisují záznamy v JSON formátu definované struktury. Jsou definovány povinné položky, které musí aplikace nebo platforma vyplnit při zápisu do logu. Do záznamu lze doplnit další položky, které generuje zapisující aplikace dynamicky. Tím je umožněno jednoduché rozšíření struktury logovaných dat. Jádro Platformy Mobilního zařízení při zápisu do logu automaticky přidává položky o čase zápisu záznamu do logu a kdo (jaká aplikace) zápis do logu provedl. Položky, podle kterých je možné filtrovat záznamy logu pro jejich odesílání, jsou uloženy také jako atributy jednotlivých záznamů.

Parametry (např. maximální velikost) nastavení logu se přebírají z Konfigurační matice PMS. Aktuální velikost logu je zjistitelná z informací zabezpečeného úložiště dat. Při zápisu záznamů do logu se provádí selekce záznamů, které se skutečně do logu zapíší. Selekce se provádí na základě informací v zapisovaném záznamu a nastavení pravidel v Konfigurační matici PMS. Uživatel má možnost nastavit pravidla, která budou nadřizena nastavení v Konfigurační matici PMS. Uživatel může pouze zvýšit úroveň logování oproti nastavení v Konfigurační matici PMS. Přístup k této funkcionalitě je umožněn na základě přidělených práv v Konfigurační matici PMS. Toto nastavení je také zapisováno do logu. Uživatel má také možnost záznamy logu filtrovat a prohlížet přímo v mobilním zařízení. Filtrování probíhá přes doplňkové atributy jednotlivých záznamů. Pro použití této funkcionality je třeba mít přidělena práva v Konfigurační matici PMS. Přístup k logu je také logován.

Záznamy logu se prostřednictvím procesů Jádra Platformy mobilního zařízení a Zabezpečené komunikace odesílají na server Platformy mobilních služeb. Rozsah odesílaných záznamů je definován v Konfigurační matici PMS. Platforma mobilních služeb si může vzdáleně vyžádat odeslání záznamů z logu podle nastavených kritérií. Tyto záznamy jsou potom postupně odesílány kanálem Zabezpečené komunikace.

13.2.1.10. Bezpečnostní služby

Certifikáty a privátní klíče jsou uloženy v Permanentním zabezpečeném úložišti dat PMZ nebo v HSM modulu vloženém do mobilního zařízení. Symetrické klíče jsou uloženy v Permanentním zabezpečeném úložišti dat PMZ nebo v HSM modulu vloženém do mobilního zařízení. Instalace nových certifikátů a klíčů do Permanentního ZUD PMZ nebo HSM probíhá kanálem Zabezpečená komunikace příkazy správy klíčů.

Platnost certifikátu (resp. jeho odvolání) je kontrolována vůči online službě, kterou vystavuje PMS. Každý certifikát má u sebe informaci o poslední kontrole. Před každým použitím certifikátu nebo privátního klíče, který s ním tvoří klíčový pár je zjišťováno, před jakou dobou byla ověřena platnost certifikátu. Pokud tato doba přesáhne nastavený limit, je ověřena platnost certifikátu vůči ověřovací službě PMS. Limit je nastaven v Konfigurační matici PMS.

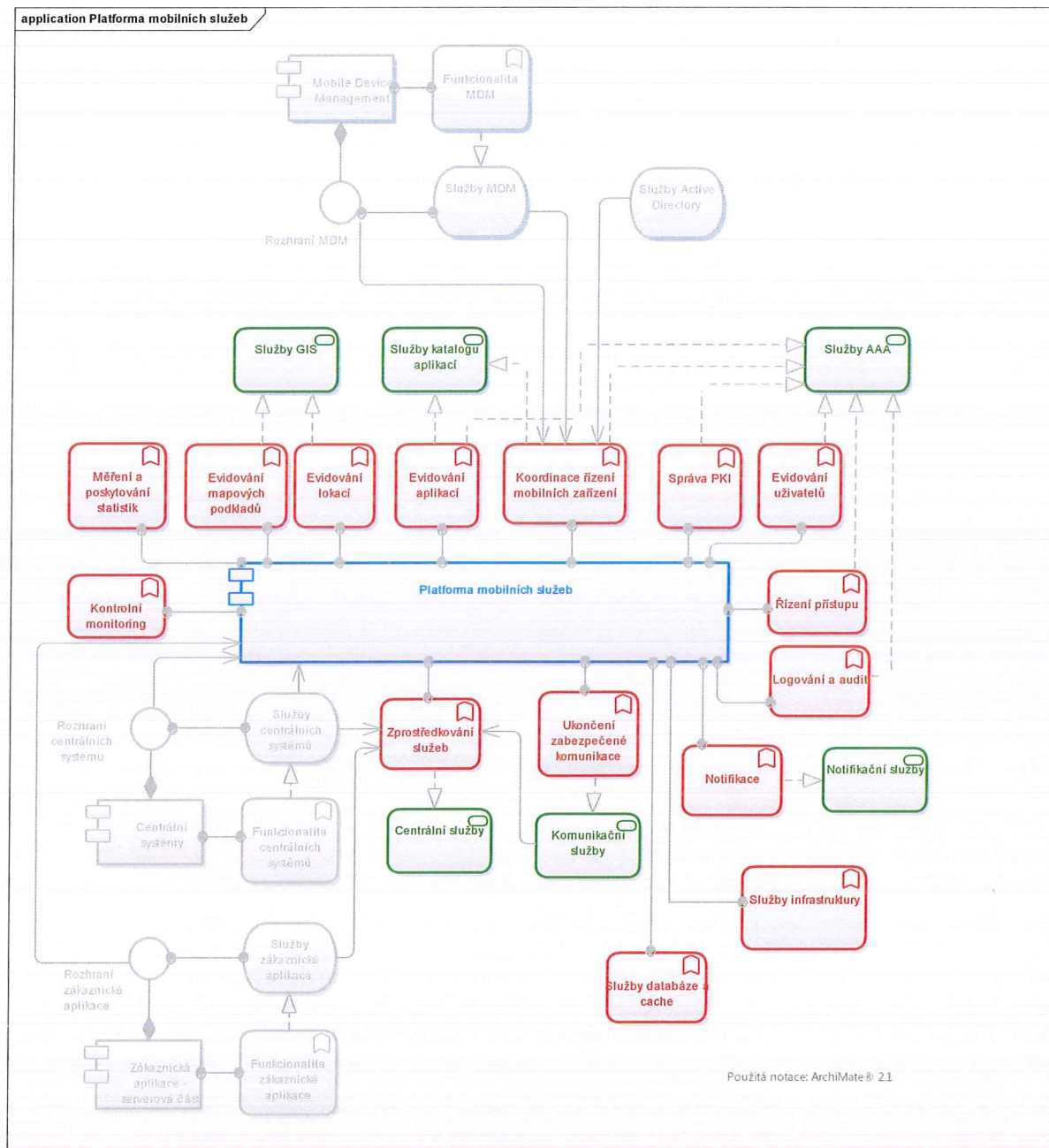
PMZ je schopna reagovat na příkazy správy klíčů zasílaných z PMS:

- Přechzení certifikátů přítomných na zařízení.
- Nastavení symetrického klíče.
- Nastavení cizího certifikátu (např. certifikát PMS).
- Vygenerování nového asymetrického klíčového páru a odeslání požadavku na vystavení certifikátu.
- Nastavení certifikátu jako výsledku na požadavek o vystavení certifikátu pro nově generovaný klíčový pár.

Veškeré činnosti týkající se bezpečnostních služeb jsou logovány.

13.2.2. Platforma mobilních služeb

Obecný pohled na platformu mobilních služeb vychází ze zadání kupujícího a je rozšířen o Služby databáze a cache (kapitola 13.2.5.7.) a Ostatní infrastrukturní služby (kapitola 13.2.5.8.). Celkové schéma včetně okolních služeb systémů kupujícího vypadá následovně:

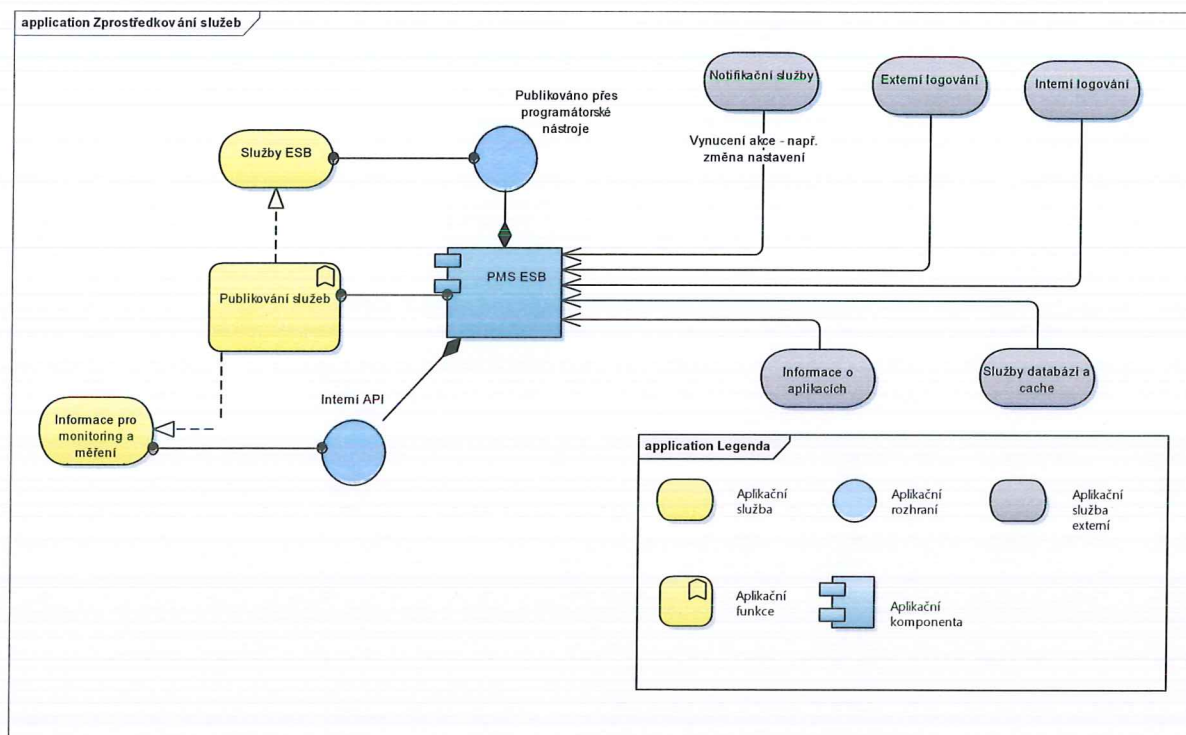


Služby a funkce Platformy mobilních služeb

V následujících kapitolách jsou popsány jednotlivé moduly do většího detailu. Cílem je popsat základní principy a služby, které moduly poskytují. Toto je zobrazeno ve velké míře abstrakce - jsou zobrazeny vybrané závislosti tak, aby byly pokryty klíčové vazby a přitom zůstala diagramy přehledné.

13.2.2.1. Zprostředkování služeb

Komponenta realizuje vlastní integrační platformu a zpřístupňuje vybranou funkcionalitu primárně z centrálních systémů PČR a MVČR. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na modul Zprostředkování služeb

Požadovaná funkcionalita je založena na následujících principech:

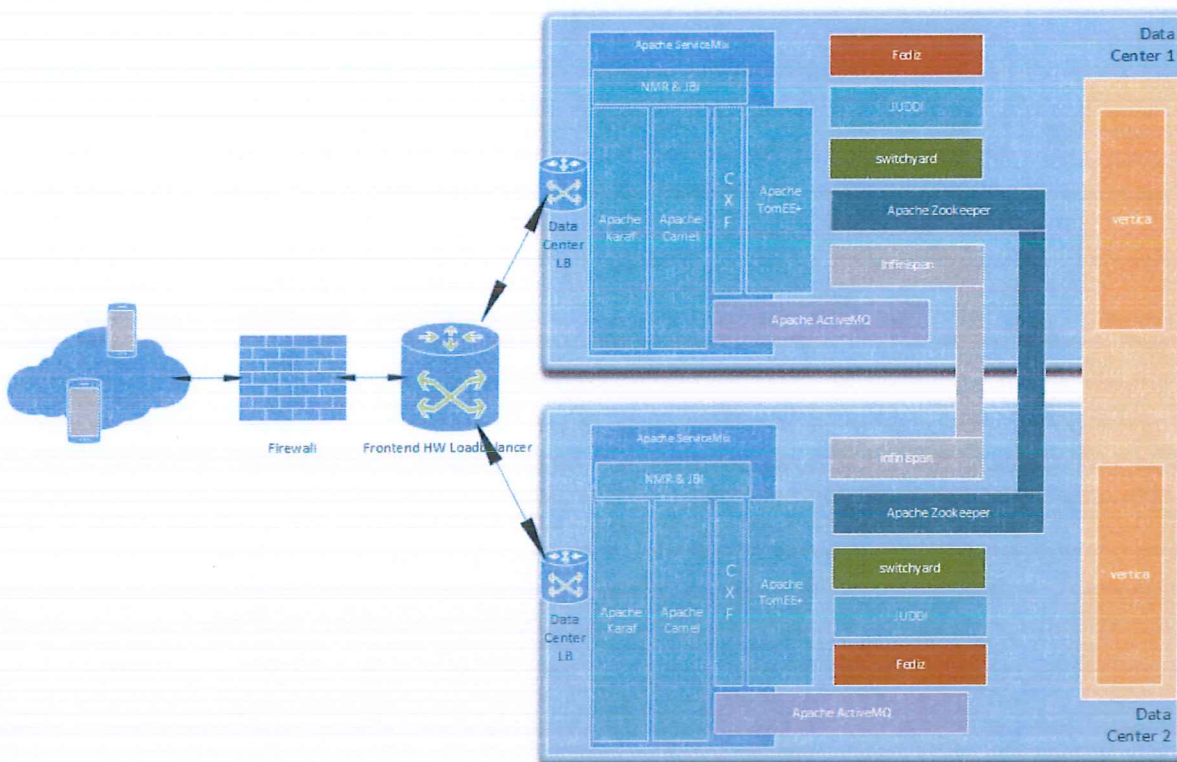
- Základem je vlastní řešení pro ESB – viz dále.
- Notifikace bude použita v případě informování o změně nastavení – aby mohla být na straně mobilního zařízení provedena odpovídající operace.
- Extensivně se používá distribuovaná konfigurace přes Apache Zookeeper.
- Distribuovaná cache není popsána v rámci tohoto modulu, ale je definována v rámci kapitoly 13.2.5.7. Služby databáze a cache
- Komponenta Evidence aplikací dodává povolenou mapu komunikace.
- Logování bude realizováno za pomoci komponenty Logování a audit, kdy bude logování provedeno do lokálního syslog rozhraní nebo případně přes interní rozhraní a to bude dále předáno.

Služby nabízené touto komponentou jsou následující:

- Služby ESB dostupné vývojářům systému – pomocí těchto služeb bude možné při dodržení definovaných standardů publikovat služby pro použití platformou mobilního zařízení a zde běžících aplikací.
- Informace pro monitoring a měření dostupné interní API – budou poskytovat informace o základních statistikách – jako je velikosti front, počet zpracovaných zpráv.

13.2.2.1.1. ESB řešení

Platforma pro zprostředkování služeb bude koncipována na modelu „active-active“ ve dvou datových centrech, které fyzicky spojuje jeden hardwarový loadbalancer. Výhodou tohoto modelu je možnost odpojit jedno z center pro účel restartu serverů nebo upgradu aplikací bez výpadku, pouze za degradace jednotlivých služeb.



Architektura ESB pro zprostředkování služeb

V jednotlivých centrech budou použity lokální loadbalancery, které budou rozkládat zátěž v rámci centra na příslušné služby. Tento obecný model dovoluje rozšířit a škálovat služby v případě potřeby opět bez jakéhokoliv výpadku.

Samotné ESB bude postaveno na open source technologiích Apache. Základem bude Apache ServiceMix, který integruje Apache Karaf, Apache Camel, framework webových služeb Apache CXF, JBI integrační technologie pro SOA, Apache ActiveMQ a Apache Tomcat. Celý systém bude doplněn o databázi pro logování a audit, dále o Infinispan pro cachování, replikaci nebo distribuci dat, Apache ZooKeeper pro centrální konfiguraci a synchronizaci služeb. Pro úložiště, verzování a jmennou službu použije Prodávající Apache Juddi. Zabezpečení a přístupy k jednotlivým aplikacím budou navrženy na principu SSO, kde IDP bude realizován aplikací Fediz. Vývoj a implemetace bude realizována v prostředí Eclipse, pro modelování služeb a toků zpráv použije Prodávající SwitchYard. Níže jsou rozebrány jednotlivé komponenty v detailech.

Apache ServiceMix – integrační kontejner.

Apache Karaf – poskytuje prostředí pro běh OSGi rutin, umožňuje.

- Hot deployment (instalaci/reinstalaci balíčků za běhu kontejneru bez nutnosti restartu serveru).
- Dynamická konfigurace služeb za jejich běhu.
- Centralizované logování (podpora Log4J formátů).

- OS integrace (Karaf může být integrován do operačního systému jako služba).
- Shell konzole (Karaf podporuje velké množství příkazů, které můžeme spouštět z příkazové konzole).
- Vzdálený přístup (podpora vzdálené správy kontejneru přes ssh).
- Zabezpečení (podpora JAAS).
- Monitoring a správa aplikací (Karaf poskytuje jednoduché rozhraní pro správu aplikací).

Apache Camel – slouží pro routování zpráv nebo požadavků mezi různými systémy včetně transformace mezi protokoly. Konfigurace probíhá pomocí DSL nebo XML.

Apache CXF – framework pro webové služby (SOAP, WS-I Basic Profile, WSDL, WS-Addressing, WS-Policy, WS-ReliableMessaging, WS-Security, WS-SecurityPolicy, WS-SecureConversation, WS-Trust), poskytuje knihovny pro vytváření služeb (JAX-WS, JAX-RS) a podporuje různé komunikační protokoly (SOAP, XML/HTTP, RESTful HTTP, CORBA) na různých transportech (HTTP, JMS, JBI).

NMR – „Normalized Message Routing“ rozhraní, podporuje Camel messaging a CXF messaging a umožňuje celému ESB být nezávislé na různých přenosových technologiích.

Apache ActiveMQ – aplikační server založený na JMS specifikaci, vhodný pro spolehlivé doručování dat, disponuje vysokým výkonem, dostupností a podporou různých topologií a konfigurací. Aplikace je dodávána s webovým rozhraním pro monitoring, správu a konfiguraci jednotlivých destinací.

Apache TomEE – webový server servlet kontejner, plně podporuje Java EE specifikaci.

Infinispan – slouží jako distribuované úložiště/cache. Java aplikace k úložišti přistupují přes knihovny, pro ostatní umí Infinispan vystavit svou funkcionalitu jako službu.

Apache Zookeeper – distribuovaný systém pro konfiguraci a synchronizaci služeb.

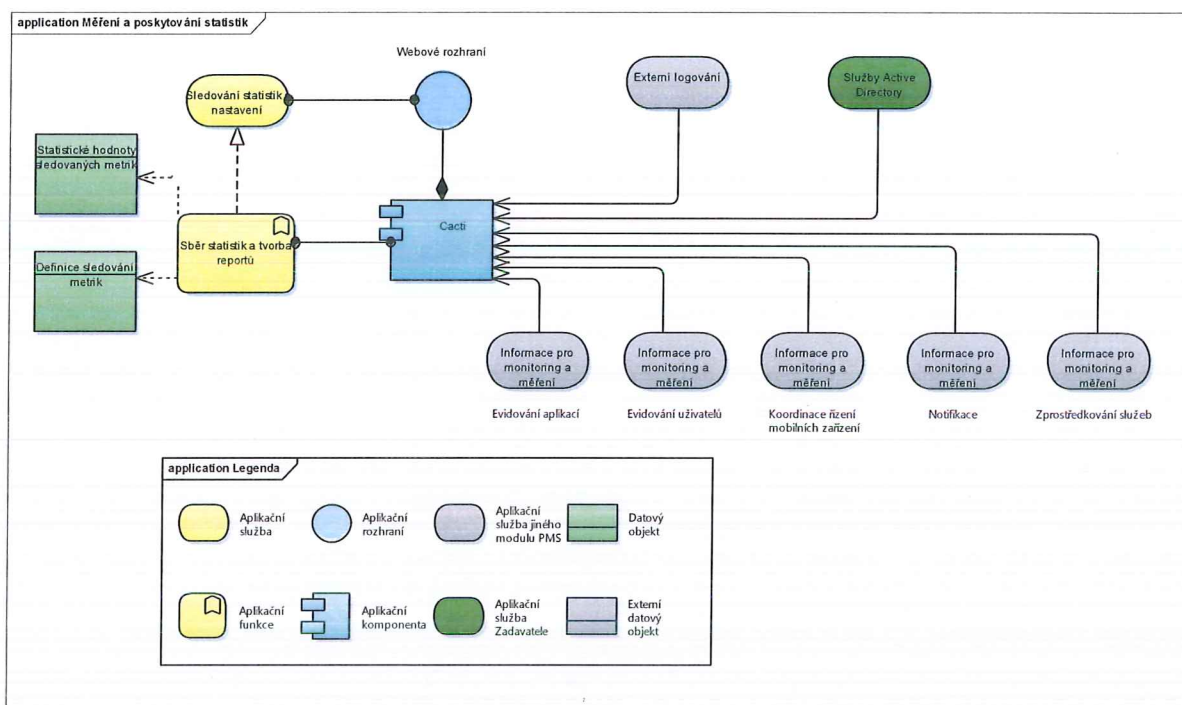
Apache Fediz – slouží pro zabezpečení přístupu k aplikacím, deleguje autentifikaci a autorizaci na IDP server, podporuje SSO a model „Federated Security“, pracuje na principu „SAML tokens“.

Apache Juddi – primárně slouží jako „web service registry“.

SwitchYard – vývojářský framework založený na modelování jednotlivých komponent a cest mezi službami.

13.2.2.2. Měření a poskytování statistik

Komponenta bude realizovat získávání údajů o činnosti platformy a jejich statistické vyhodnocování. Nad vybranými statistikami bude poskytovat základní reporty. Funkcionalitu bude realizovat v těsné spolupráci s jednotlivými komponentami řešení, které jí budou poskytovat odpovídající naměřené ukazatele. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na modul Měření a poskytování statistik

Požadovaná funkcionalita je založena na následujících principech:

- Funkcionalita je zajištěna primárně pomocí nástroje Cacti, který je dostupný pod GNU General Public licencí, jedná se o kompletní řešení pro sběr a následné sledování monitorovaných dat v čase (viz dále).
- Data jsou poskytována a mohou být využívána z následujících zdrojů (pokud jsou publikována přes interface srozumitelný z pohledu nástroje – např. přes SNMP protokol):
 - Na míru připravené hodnoty v rámci platformy (např. počet zpracovaných požadavků v rámci modulu zprostředkování služeb, množství evidovaných bodů zájmu, počet uživatelů nebo počet aplikací a jejich instalací).
 - Data dostupná z používaných nástrojů (např. velikost databáze, VMware informace).
 - Data dostupná na úrovni operačního systému (např. velikost místa, zatížení).
 - Data dostupná z dodaných HW komponent (např. server, enclosure).
 - Data dostupná externě – např. informace ze síťových prvků ale např. i z volaných systémů.
- Cílem je vytvořit jednotné místo, ze kterého bude možné sledovat stav řešení v čase a navrhnout odpovídající změny – tvoří tak jeden z klíčových vstupů do Capacity management kupujícího. Díky tomu Kupující bude moci:
 - Zvýšit efektivitu výdajů a realizovat úspory nákladů (možnost odložit investice na pozdější dobu = ekonomicky efektivní poskytování služeb).
 - Rozhodnout o nasazení změn v aplikacích – např. zda je možné dodat novou aplikaci, která bude využívat zdroje platformy kupujícího.
 - Zvýšit dostupnosti služeb proaktivní eliminací příčin vzniku incidentů z důvodu nedostatečné kapacity infrastruktury a zdrojů IT.
- Naměřená data jsou ukládána ve formátu RRD (Round Robin Database), který umožňuje zajistit fixní velikost databáze, která v čase ztrácí přesnost (tedy u starších událostí ukládá průměry za delší období).

- Cacti potřebuje pro svůj běh nástroje RRDTool, MySQL, PHP a web server Apache, které budou instalovány společně s Cacti na jednom serveru, vysoká dostupnost bude zajištěna prostředky pole (data budou kopírována na druhou lokalitu), prostředky VMware a předpokládá se běh nástroje na obou lokalitách (buď v identické konfiguraci, nebo asymetrické – tedy sběr dat na lokálních serverech bude častější než na druhé lokalitě).
- Uživatelé jsou primárně spravováni v Active Directory kupujícího, v rámci nástroje jsou přiřazována přístupová práva.
- Logování je realizováno za pomoci komponenty Logování a audit, kdy je logování provedeno do lokálního syslog rozhraní a to je dále předáno.

Služby nabízené touto komponentou budou následující:

- Sledování statistik a nastavení přes webové rozhraní – vybraným uživatelům budou zde dostupné statistiky a grafy o vybraných sledovaných ukazatelích a to zejména formou grafů. Uživatelé v roli administrátorů budou mít možnost dále nastavovat nové nebo upravovat již nastavené definice sběru monitorovaných atributů.

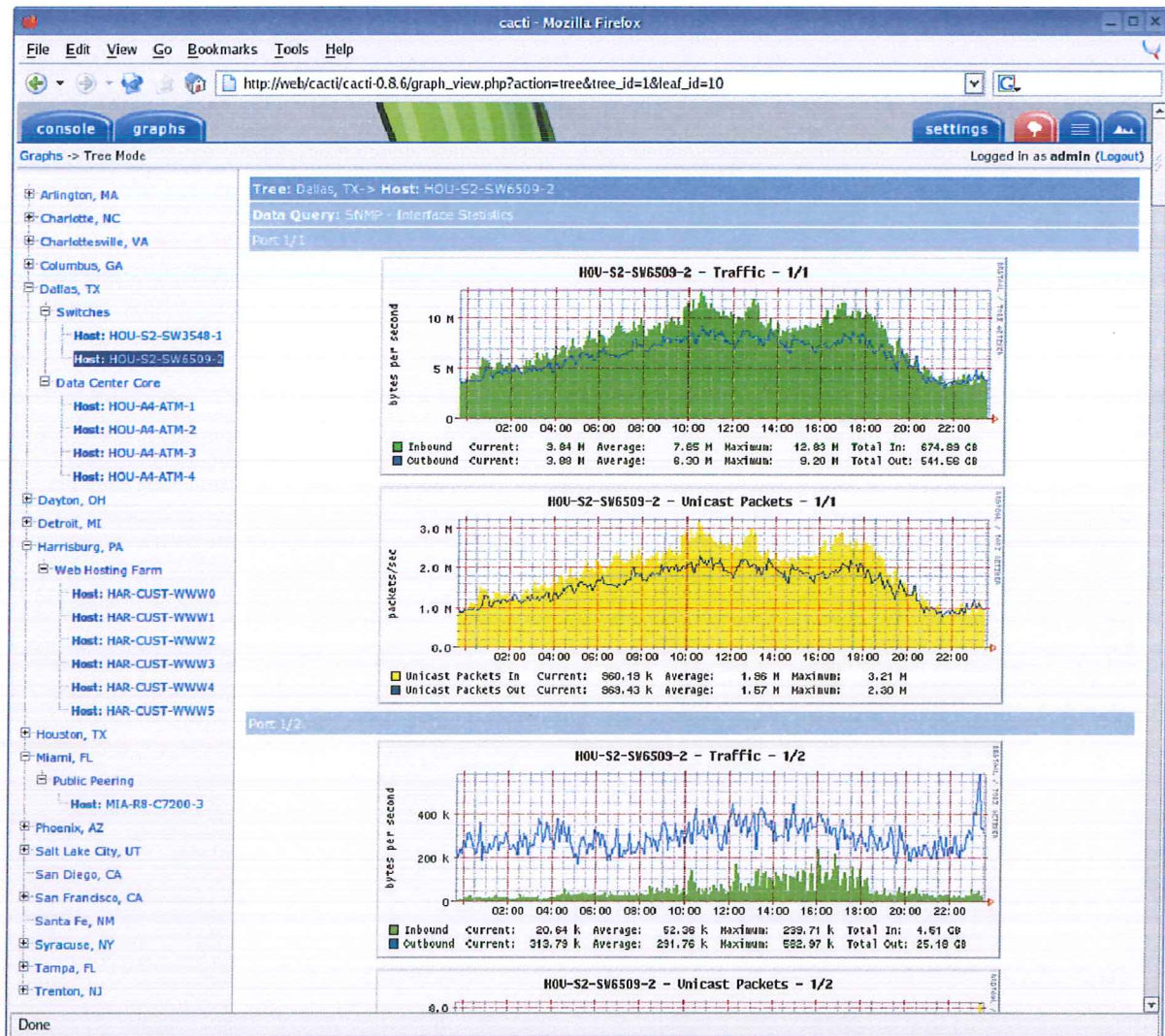
Hlavní datové objekty spravované v rámci komponenty budou následující:

- Statistické hodnoty sledovaných metrik – to jsou vlastní naměřené hodnoty uložené v databázi a z nichž se generují ad-hoc reporty.
- Definice sledování metrik – určují, jak často jsou vybrané ukazatele sledovány a jejich hodnoty ukládány.

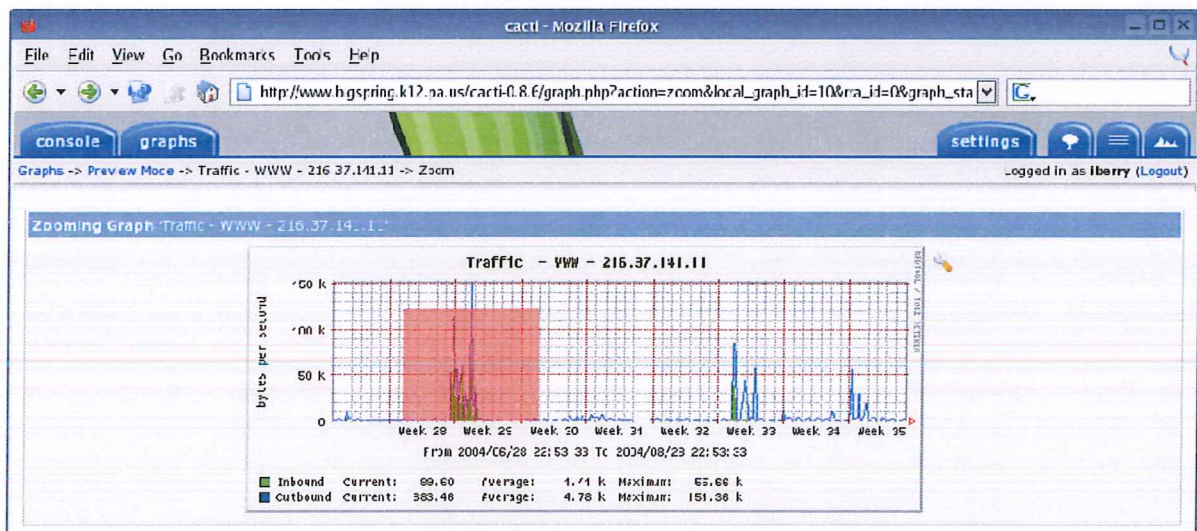
13.2.2.2.1. Nástroj Cacti

Nástroj Cacti je nástroj pro monitorování IT systémů a aplikací. Je určen ke sběru statistik, a to jak systémových a technologických (např. využití procesoru, paměti, zaplněnosti filesystému, zatížení portů, teplotě diskových jednotek atp.), tak uživatelských (statistiky z aplikací nebo i externí ukazatele jako je např. teplota nebo počet srážek). Umožňuje monitorovat větší množství zařízení a hodnot. Na zjištěné hodnoty umí upozornit např. zasláním emailové notifikace.

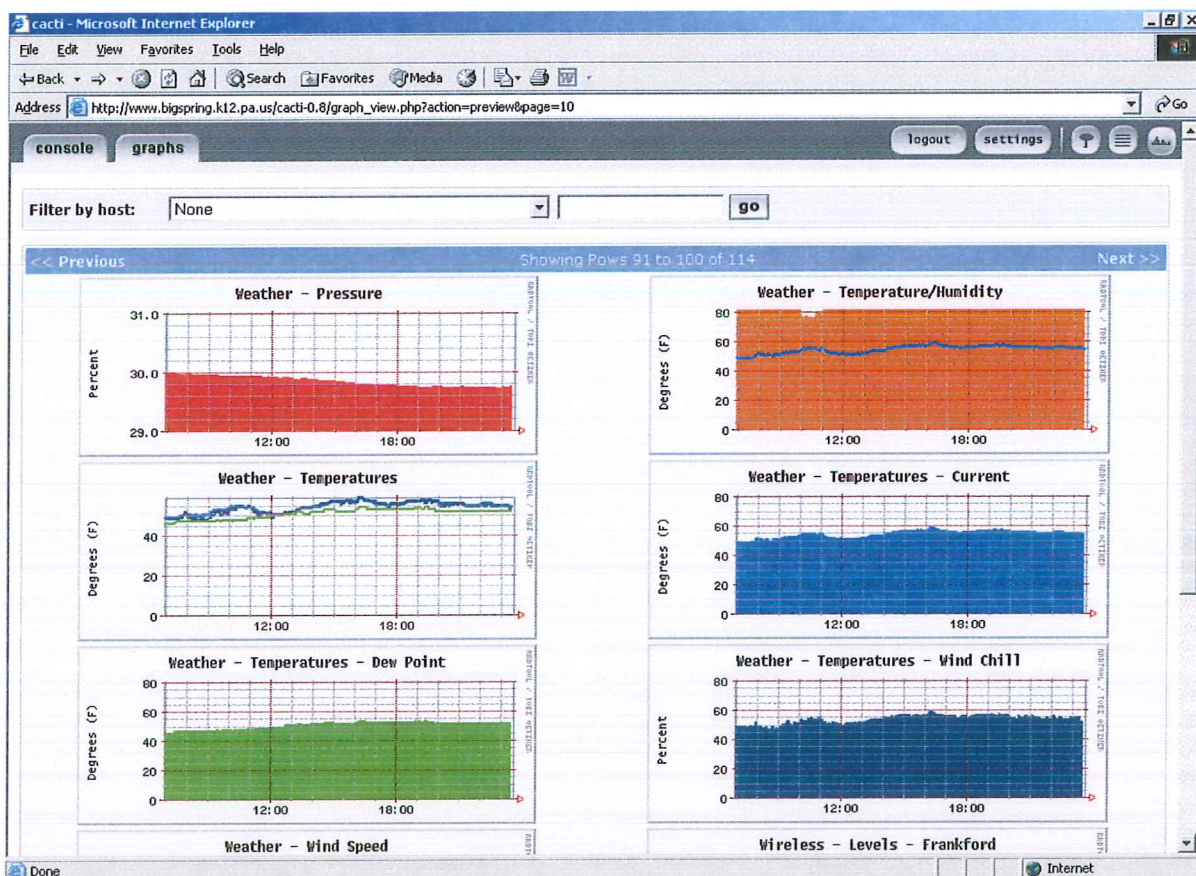
Výhodou nástroje Cacti je přehledné webové rozhraní, široká dostupnost pluginů rozšiřující standardní funkcionalitu, tvorba šablon, otevřenost pro vlastní získávání dat a tvorbu grafů a statistik. Lze využít již předdefinovaných šablon nebo definovat své vlastní. Šablony jsou také k dispozici ke stažení na internetu. Monitoring probíhá přes protokol SNMP a také formou skriptů (je tak možné sledovat např. data přes JMX). Cacti umožňuje spustit skript pro získání informací o monitorovaném prostředí. Spouštění skriptů je vhodné pro zařízení, které nepodporují SNMP protokol.



Obrazovka nástroje Cacti



Zoom v grafu v rámci nástroje Cacti



Zobrazení více grafů v rámci nástroje Cacti

Vlastnosti nástroje Cacti:

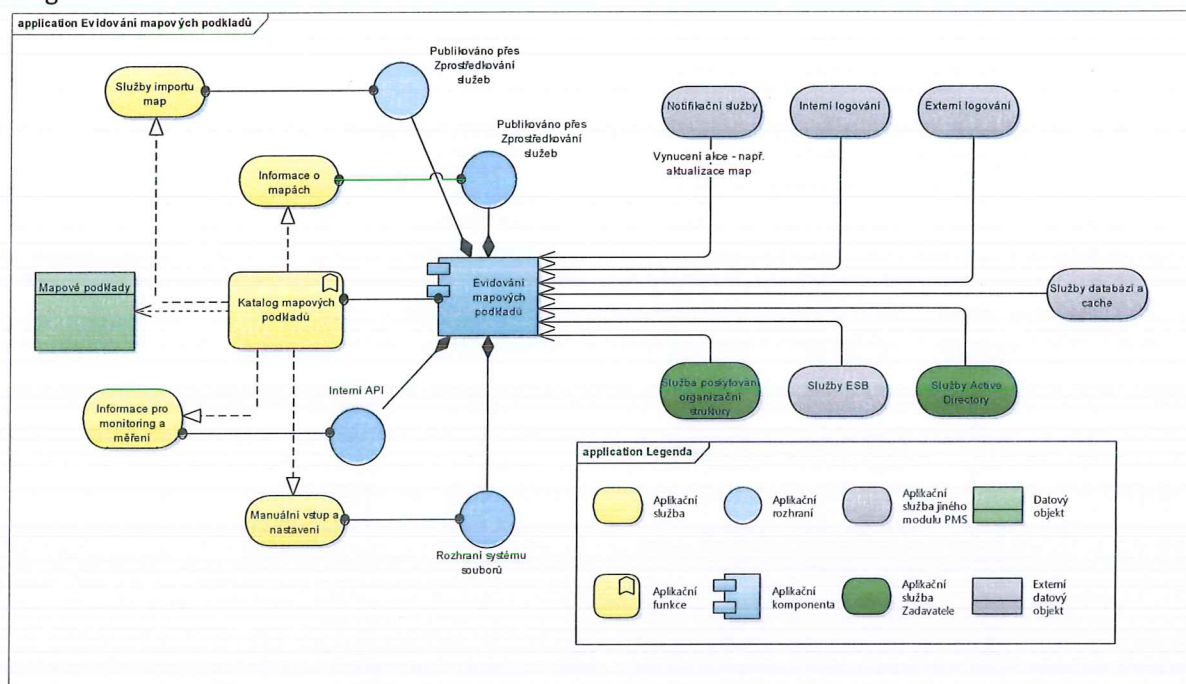
- Tvorba neomezeného množství grafů.
- Lze nastavit pravidla pro archive (degradování) dat v čase.
- Umožňuje zasílat emailové notifikace.
- Grafy lze sdružovat do přehledů a ty pak dle období zobrazovat.
- Kromě grafů jsou k dispozici i informace o maximální, minimálních a celkových hodnotách.
- Na grafech je možné provádět „zoom“ – tedy zobrazení přesnějšího detailu v čase.
- Lze importovat a exportovat soubory s naměřenými daty.
- Lze vytvářet nové šablony nebo importovat existující.
- Umožňuje přidělovat práva koncovým uživatelům pro prezentaci naměřených hodnot a to až na úrovni graf na uživatele.
- Uživatelé si mohou nastavit vlastní atributy grafů.
- Dostupnost pluginů rozšiřující jeho funkcionalitu.

Pomocí volně dostupných pluginů lze rozšířit jeho funkcionalitu např.

- **Backup** – umožňuje zálohovat konfiguraci a data Cacti nástroje.
- **Discovery** – vyhledá v síti zařízení používající SNMP a umožní přidání do monitoringu Cacti.
- **Threshold** – umožňuje vytvořit, nastavit a monitorovat prahové hodnoty (tzv. thresholdy). Na základě prahových hodnot umí nástroj posílat e-mailové upozornění s přílohou daného grafu při překročení nebo navrácení hodnoty do normálu. Lze nastavit, zda má upozorňovat při prvním překročení prahové hodnoty nebo až po několikátém.

13.2.2.3. Evidování mapových podkladů

Komponenta realizuje funkcionalitu evidování mapových podkladů (typicky rastrových map kupujícího). Tedy zajišťuje správu mapových podkladů, jejich aktualizaci a případně i notifikace platformy mobilního zařízení a participuje při vlastní distribuci mapových podkladů do mobilních zařízení. Vstupem mapových podkladů jsou přímo systémy kupujícího. Data jsou nahrávána buď pomocí manuálního vstupu, nebo automatizovaně. Základní schéma je zobrazeno na následujícím diagramu.



Základní pohled na Evidování mapových podkladů

Požadovaná funkcionalita je založena na následujících principech:

- Součástí dodávky je rozhraní pro nahrávání mapových podkladů z aktuálních zdrojů kupujícího. Předpokládá se načítání mapových podkladů ve formátu ESRI Compact Cache (dlaždice rastru). Komponenta kromě základního mapového podkladu v rastrové podobě umožňuje také načíst některá vektorová data statických vrstev, typicky plošných (správní celky, územní působnosti, atd.), jako tzv. Shape. Ostatní vektorová data (typicky polygony, linie, body) budou načítány v rámci modulu Evidování lokací (kapitola 13.2.2.4.).
- Aplikační serverová komponenta zdrojový formát vždy převádí automaticky do vlastního optimalizovaného formátu platformy mobilních služeb, který je především:
 - rozdělitelný na územní jednotky pro jednodušší řízení nahrávání na různé skupiny mobilních zařízení,
 - rozdělený na jednotlivá měřítka (Layers), korespondující se zdrojovými daty, s možností řízení, která měřítka se replikují na která zařízení,
 - optimalizovaný pro rychlost načítání na mobilním zařízení (vlastní indexace platformy mobilních služeb),
 - šifrovaný (zabezpečený, chráněný tak proti zneužití) mechanismy ochrany dat Platformy mobilních služeb (využitý algoritmus AES 256 bit),
 - úsporný (velikost ukládaných a následně přenášených dat v rámci Platformy mobilních služeb je prioritní částí návrhu),
 - efektivní pro zobrazení vektorových dat.

- Řízená aktualizace dat (požadavek PMS8) je primárně řešena na straně platformy mobilního zařízení, z pohledu serverové strany se jedná zejména o odesílání adekvátních notifikací v případě změny mapových podkladů.
- Úvodní nahrání mapových podkladů (požadavek PMS9) bude řešeno v návaznosti na analýzu a definici procesů aktivace mobilního telefonu a také s ohledem na možnosti MDM řešení poptávaného kupujícím v části A. Možnou alternativou (kromě kontrolovaného ožívování mobilního zařízení na lokalitách s dobrou dostupností sítě) je i distribuce podkladů přes MDM spolu s dalšími aplikacemi instalovanými při ožívování mobilních zařízení.
- Komponenta je založena na standardním řešení a pouze malá část bude vytvořena pomocí zákaznického vývoje (např. distribuce na platformu).
- Logování je realizováno za pomoci komponenty Logování a audit.

Služby nabízené touto komponentou jsou následující:

- Služby importu lokací map publikované jako služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné importovat mapy automatizovaně.
- Informace o mapách publikované jako služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné získávat mapy na platformu mobilního zařízení při zohlednění filtrovacích kritérií a práv. Součástí jsou také služby participující na řízené aktualizaci dat (požadavek PMS8) a také služby úvodního nahrání podkladů (požadavek PMS9).
- Informace pro monitoring a měření dostupné interní API – poskytují informace o základních statistikách – jako je například počet podkladů.
- Manuální vstup a nastavení dostupné přes rozhraní systému souborů – umožňuje nahrávání dat pomocí manuálního vstupu a umožňuje realizovat vlastní nastavení (např. přístupová práva, preference jakým uživatelům se mají podklady nabízet a nastavování platnosti v čase). Přístup k aplikaci je omezen pomocí skupin v Active Directory kupujícího.
- Žádosti o aktualizaci map dostupné přes webové rozhraní – umožňuje požádat o aktualizace lokace mobilního zařízení (viz požadavek EMP7).

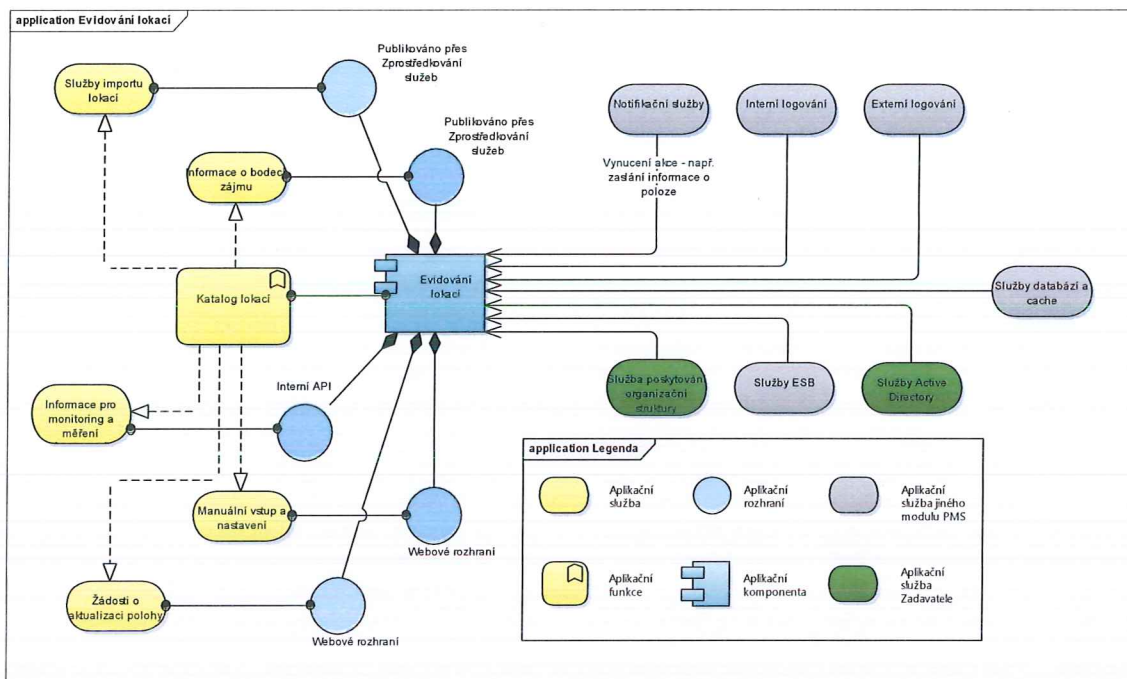
Hlavní datové objekty spravované v rámci komponenty jsou následující:

- Mapové podklady – spravované importované mapové podklady, kromě vlastního podkladu jsou u nich udržované další atributy jako:
 - nastavení práv,
 - preference jakým uživatelům se mají dané podklady nabízet,
 - definice platnosti v čase.

13.2.2.4. Evidování lokací

Komponenta realizuje poskytování a získávání informací o lokalizaci míst zájmu, včetně vedení katalogu statických míst zájmu a dynamických katalogů. Součástí je i základní uživatelské prostředí pro nastavení atributů a uživatelských práv a pro import sad bodů zájmu. Tuto funkcionalitu realizuje poskytováním služeb nad řešením popsáním v kapitole 13.2.4. Integrované lokalizační služby.

Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Evidování lokací

Požadovaná funkcionalita je založena na následujících principech:

- Komponenta nabízí služby řešení popsaného v rámci kapitoly 13.2.4. Integrované lokalizační služby.
- Zajistí integraci všech systémů poskytujících lokalizační data pro potřeby PČR (PEGAS AVL, PEGAS MDG, CarControl, Princip, Positrex). Údaje budou ukládány v jednotném formátu do perzistentního úložiště.
- Přístup k aplikaci (služby Manuální vstup a nastavení) se řídí pomocí skupin uživatelů uložených v Active Directory kupujícího.
- Komponenta je založena na standardním řešení a pouze malá část bude vytvořena pomocí zákaznického vývoje (např. realizování žádosti o aktualizace polohy).
- Logování je realizováno za pomoci komponenty Logování a audit.

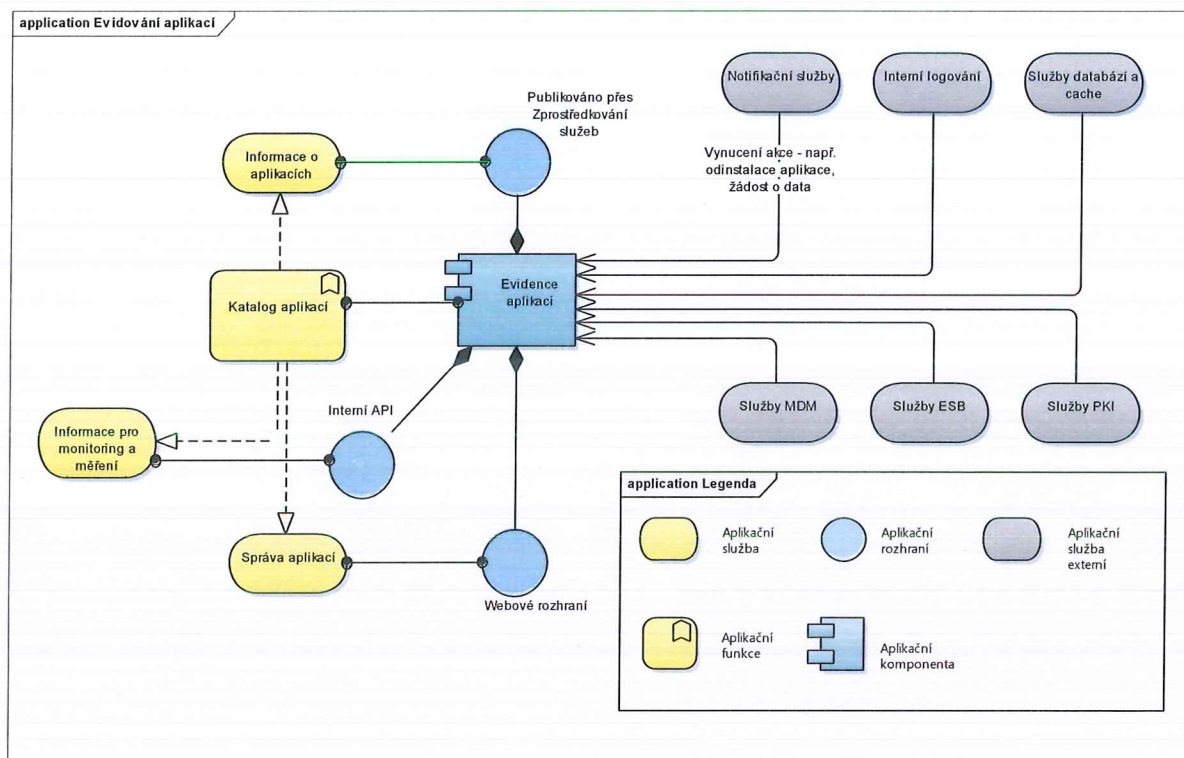
Služby nabízené touto komponentou jsou následující:

- Služby importu lokací publikované jako služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné zadávat body zájmu a to buď přímo z platformy mobilního zařízení (např. na základě přijatých notifikací, na žádost zákaznických aplikací, vytvořené v uživatelském rozhraní) nebo z dalších zdrojů lokací PČR (PEGAS AVL, PEGAS MDG, CarControl, Princip, Positrex).
- Informace o bodech zájmu publikované jako služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné získávat na platformě mobilního zařízení informace o bodech zájmu a to při zohlednění filtračních kritérií a práv.
- Informace pro monitoring a měření dostupné interní API – poskytují informace o základních statistikách – jako je počet evidovaných lokací, počet pohybů za časový okamžik.
- Manuální vstup a nastavení dostupné přes webové rozhraní – umožňuje nahrávání dat pomocí manuálního vstupu (a to včetně konverzí z obecně používaných formátů) a umožňuje realizovat vlastní nastavení (např. přístupová práva).

- Žádosti o aktualizaci polohy dostupné přes webové rozhraní – umožňuje požádat o aktualizace lokace mobilního zařízení (viz požadavek EVL11).

13.2.2.5. Evidování aplikací

Komponenta realizuje evidenci aplikací a zajišťuje vedení katalogu aplikací. Tuto funkcionalitu realizuje v těsné spolupráci s MDM. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Evidování aplikací

Požadovaná funkcionalita je založena na následujících principech:

- Aplikace jsou primárně spravovány v rámci MDM, v rámci modulu se udržují pouze případné atributy a data, které není možné v rámci MDM spravovat – např. defaultní konfigurace, povolené verze, definice omezení komunikace a další restrikce.
- Spolupráce s MDM je také potřebná v případě realizace požadavků na odebrání aplikací (např. při zrušení nebo aktualizaci).
- Notifikace bude použita v případě informování o změně verze nebo odebrání aplikace z katalogu – aby mohla být na straně mobilního zařízení provedena odpovídající operace. Toto nebude použito, pokud bude možné danou operaci požadovat přes MDM.
- Komponenta Evidence aplikací bude vytvořena pomocí zákaznického vývoje.
- Logování je realizováno za pomoci komponenty Logování a audit.

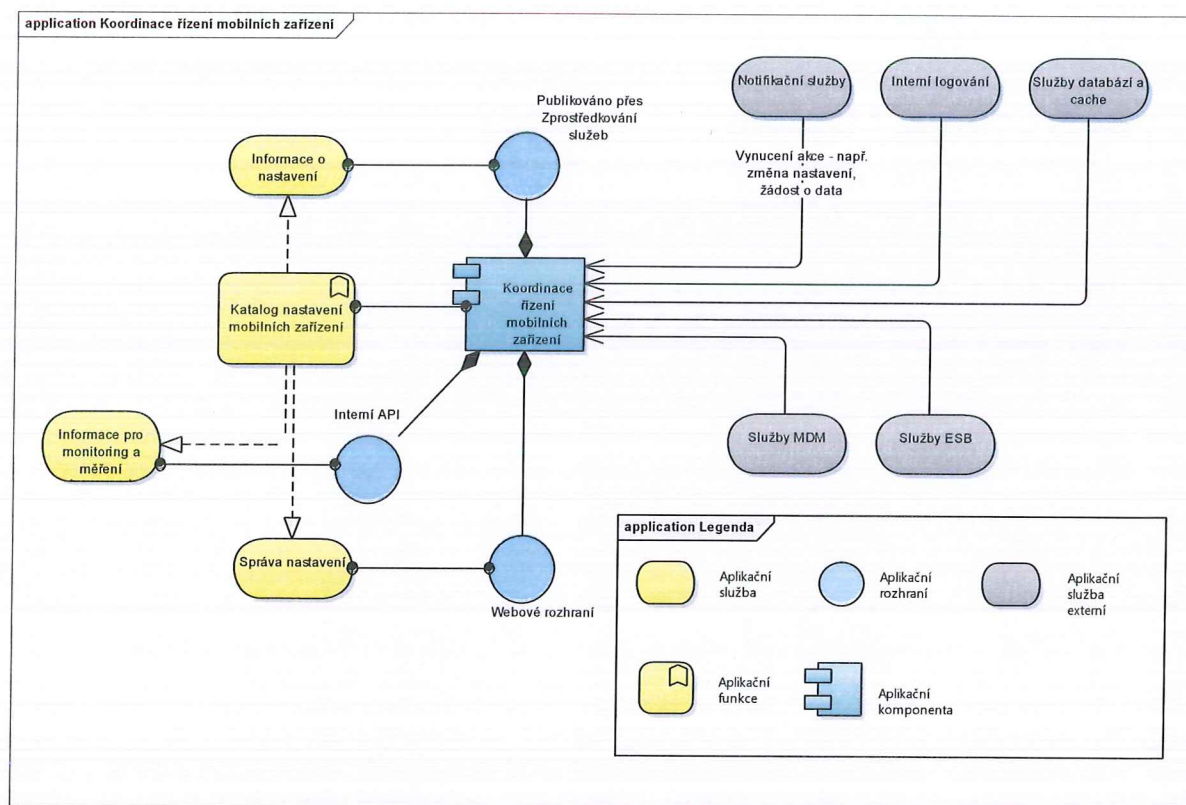
Služby nabízené touto komponentou jsou následující:

- Informace o aplikacích publikované jako služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné získávat na platformě mobilního zařízení informace o aplikacích, verzích a také umožní registrovat informace nutné pro základní statistiky (např. o instalaci nebo puštění aplikace).

- Informace pro monitoring a měření dostupné interní API – poskytují informace o základních statistikách – jako je počet aplikací, instalací, puštění. Tyto informace jsou získávány také ve spolupráci s MDM.
- Správa aplikací dostupná přes webové rozhraní – umožní přístup k nastavení atributů aplikací. Data jsou ukládána do MDM (přes odpovídající rozhraní), další data nutná pro běh platformy jsou uložena přímo v ní za pomoci modulu Služby databáze a cache (kapitola 13.2.5.7.). Navrhované rozhraní bude primárně určené pro administrátory znalé pravidel a to pro zajištění větší flexibility nastavení (týká se především konfigurace, nastavení povolené mapy spojení atd.)

13.2.2.6. Koordinace řízení mobilních zařízení

Komponenta realizuje řízení mobilních zařízení z pohledu konfigurace a zajišťuje vedení katalogu těchto nastavení. Tuto funkcionalitu realizuje v těsné spolupráci s MDM. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Koordinaci řízení mobilních zařízení

Požadovaná funkcionalita je založena na následujících principech:

- Mobilní zařízení jsou primárně spravována v rámci MDM, v rámci modulu se udržují pouze případné atributy a data, které není možné v rámci MDM spravovat – např. obecná nastavení, definice omezení a další atributy.
- Vlastní získání nastavení je víceúrovňová operace kombinující nastavení platná na více úrovních (globální, skupinová a uživatelská) – viz dále v kapitole 13.2.2.6.1. Proces nastavení jako víceúrovňová operace.

- Notifikace bude použita v případě informování o změně nastavení – aby mohla být na straně mobilního zařízení provedena odpovídající operace. Toto nebude použito, pokud bude možné danou operaci požadovat přes MDM.
- Komponenta Koordinace řízení mobilních zařízení bude vytvořena pomocí zákaznického vývoje.
- Logování je realizováno za pomoci komponenty Logování a audit.

Služby nabízené touto komponentou jsou následující:

- Informace o nastavení publikované jako služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné získávat na platformě mobilního zařízení informace o nastavení celé platformy a to jednak v obecném kontextu tak i v kontextu jednotlivých uživatelů a také umožní registrovat informace nutné pro základní statistiky (např. o instalaci nebo puštění aplikace).
- Informace pro monitoring a měření dostupné interní API – poskytují informace o základních statistikách – jako je počet mobilů pod správou platformy. Tyto informace mohou být získávány také ve spolupráci s MDM.
- Správa nastavení dostupná přes webové rozhraní – umožní přístup k nastavení atributů platformy a to jak obecně, tak pro jednotlivá mobilní zařízení. Data jsou ukládána do MDM (přes odpovídající rozhraní), další data nutná pro běh platformy jsou uložena přímo v ní. Navrhované rozhraní bude primárně určené pro administrátory znalé pravidel, a to pro zajištění větší flexibility nastavení (týká se především konfigurace, nastavení restrikcí atd.).

13.2.2.6.1. Proces nastavení jako víceúrovňová operace

Pro získání vlastního nastavení platného pro danou platformu a i přihlášeného uživatele je nutné uvažovat změny parametrů a jejich vzájemné přepisování na více úrovních. Každý parametr si kromě vlastní hodnoty nastavení nese i příznak o typu (ten kromě vlastního typu atributu – jako např. text může definovat i to zda je atribut povinný a musí být definován na nižších úrovních) a zejména příznak, zda je možné jej na nižších úrovních měnit. Díky tomuto mechanismu bude snadné realizovat například následující operace:

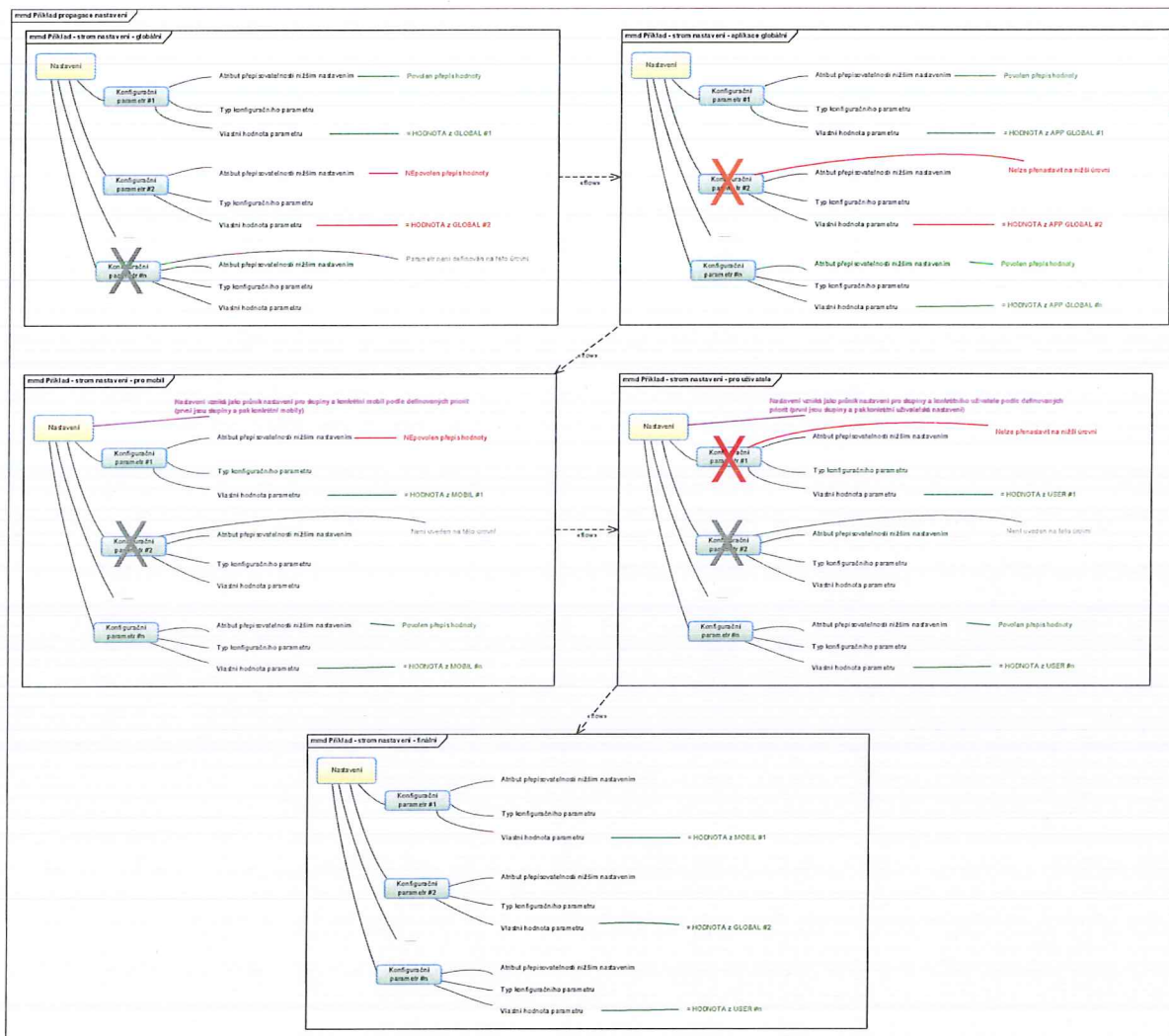
- Definovat různá nastavení na více úrovních – např. vytvářet konfigurace pro jednotlivé aplikace.
- Měnit nastavení na globální úrovni a zabránit jeho přepisu na nižších úrovních – tedy např. globálně zakázat komunikaci po vybraném kanálu, nebo zakázat přístup ke kameře telefonu.
- Nastavovat parametry pouze relevantní pro danou úroveň – tedy např. ignorovat přenosové parametry platformy na úrovni uživatele.

Vlastní nastavování pak probíhá na následujících úrovních:

- Globální – nejvyšší úroveň, parametry označené jako nepřepisovatelné nelze již měnit. Typicky obsahuje nastavení platná pro celou platformu, které se mění pouze výjimečně.
- Globální na úrovni aplikace – další úroveň, je relevantní pouze v případě, že se zjišťuje nastavení pro aplikaci, není použit v případě vlastní platformy.
- Nastavení na úrovni mobilu (platformy) – platí v kontextu mobilu a není závislý na tom, zda a jaký je přihlášený uživatel. Nastavení vzniká jako průnik nastavení pro skupiny a konkrétní mobil podle definovaných priorit (první jsou skupiny a pak konkrétní mobily).
- Nastavení na úrovni uživatele (přihlášeného) – platí v kontextu přihlášeného uživatele (obsahuje typicky jeho personalizaci). Nastavení vzniká jako průnik nastavení pro skupiny a

konkrétního uživatele podle definovaných priorit (první jsou skupiny a pak konkrétní uživatelská nastavení).

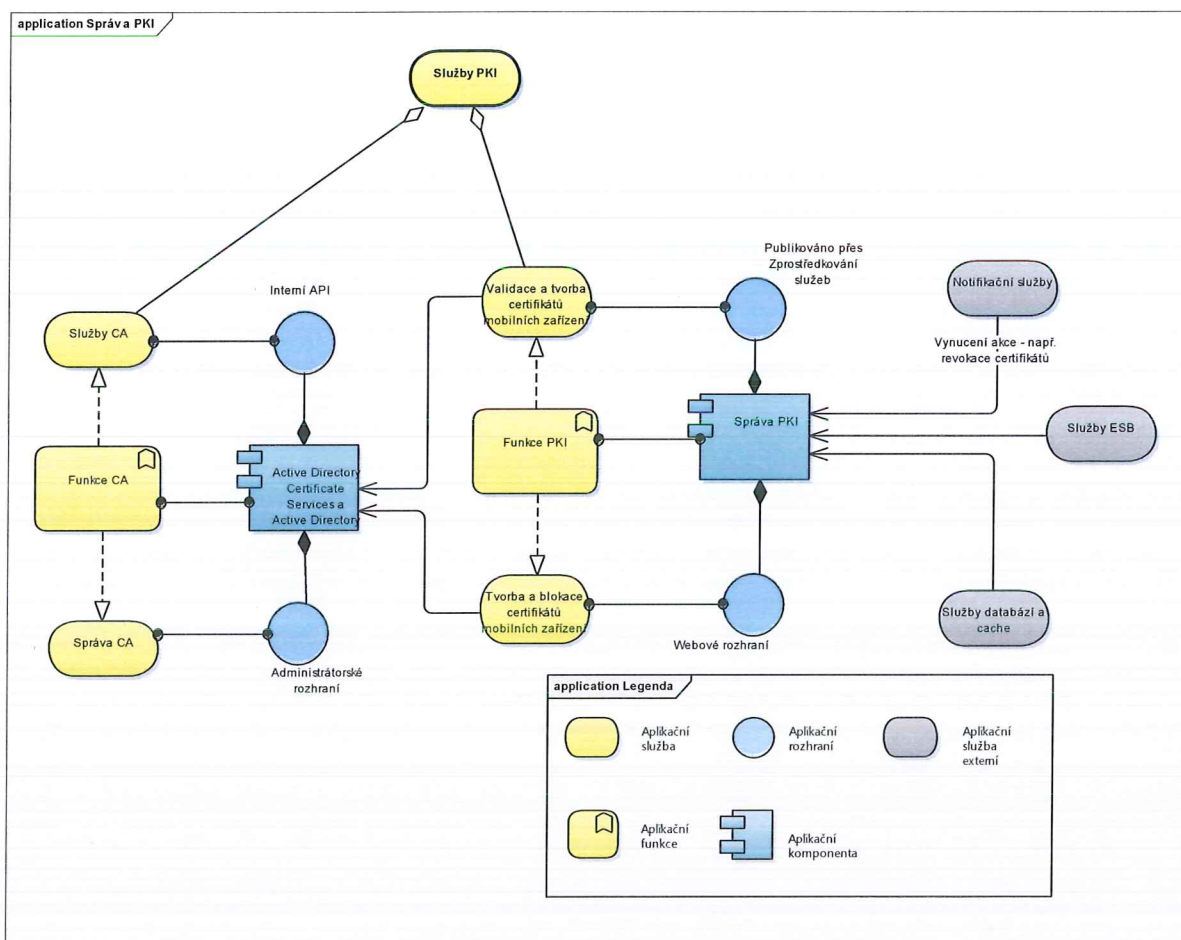
Příklad propagace nastavení a zjištění jaká hodnota parametru je platná, je uveden na následujícím schématu:



Příklad propagace nastavení

13.2.2.7. Správa PKI

Tato komponenta realizuje vedení evidence a zajištění životního cyklu digitálních certifikátů pro potřeby identifikace zařízení (respektive platformy mobilního zařízení), identifikace zákaznických aplikací pro mobilní platformu a serverů platformy mobilních služeb. Tuto funkcionalitu realizuje nad Active Directory Certificate Services. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Správu PKI

Požadovaná funkcionální je založena na následujících principech:

- Základní služby PKI budou založené na Active Directory Certificate Services (standardní součást dodávaného operačního systému Windows 2012).
- Vlastní pravidla pro žádosti o certifikáty mobilních zařízení bude vypracován v analýze a v rámci modulu vzniknou dedikované služby umožňující realizovat tuto funkcionální.
- PKI bude založené na tříúrovňovém hierarchickém modelu CA (viz dále v kapitole 13.2.2.7.1. PKI – součástí řešení).
- Notifikace bude použita v případě informování o změně platnosti certifikátu a při žádosti o informaci o certifikátech na platformě – aby mohla být na straně mobilního zařízení provedena odpovídající operace.
- Logování je realizováno za pomoci komponenty Logování a audit.

Služby nabízené touto komponentou jsou následující:

- Validace a tvorba certifikátů mobilních zařízení přes modul Zprostředkování služeb – pomocí těchto služeb bude možné validovat certifikáty, aktivně participovat při jejich vytváření a také získat seznam nevalidních certifikátů (případně bude použit Online Certificate Status Protocol – viz dále).
- Tvorba a blokáce certifikátů mobilních zařízení dostupná přes webové rozhraní – slouží k blokaci certifikátů a také participuje při vlastní tvorbě certifikátů (pokud nebude v rámci

analýzy definováno jinak – např. iniciace bude ze strany zařízení nebo externího nástroje). Součástí je také komponenta umožňující vyžádat stav certifikátu na mobilním zařízení (viz požadavek BES6).

- Služby CA dostupné přes interní API – standardní funkcionality Active Directory Certificate Services dostupná přes API.
- Správa CA dostupná přes administrátorské rozhraní – standardní administrace CA v rámci Active Directory Certificate Services.

13.2.2.7.1. PKI – součástí řešení

Public Key Infrastructure (PKI) je framework sestávající se z pravidel (policies), služeb a šifrovacího software, které společně poskytují odpovídající zabezpečení pro transport dat a validaci jednotlivých stran. Hlavní funkce jsou následující:

- Správa klíčů – umožňuje tvorbu nových, kontrolu stávajících, ukončování platnosti (revokaci) a spravuje vlastní hierarchii důvěry.
- Publikování klíčů – nabízí dobře definované procesy a nástroje pomocí kterých je možné lokalizovat a stáhnout veřejné klíče a informaci, zda daný klíč je validní. Bez této možnosti (stáhnout a validovat) nemohou uživatelé PKI služby používat.
- Užití klíčů – PKI umožňuje jednoduché použití klíčů ve formě knihoven a aplikací, které provádí kryptografické operace a tím je umožněno zabezpečení celého řešení. V žádném případě to není jen o přesouvání klíčů.

Vlastní navrhovaná infrastruktura se sestává z certifikačních autorit (CA - Certification Authority), registračních autorit (RA - Registration Authority), adresářových služeb (Directory services) a vlastních aplikací, které certifikáty spravované v rámci PKI používají.

13.2.2.7.1.1. CA – certifikační autorita

Certifikační autorita (CA) je hlavní komponenta PKI. CA je důvěryhodná třetí strana, která je odpovědná za vydávání certifikátů a jejich správu v průběhu jejich životního cyklu. Digitální certifikáty obsahují veřejný klíč (uživatele, zařízení, serveru a dalších evidovaných objektů) a specifické informace o nich. Tento certifikát je nepozměnitelný nemůže být falšován. CA při vydání tohoto certifikátu potvrzuje, že subjekt je tím nebo čím za koho se vydává (podobně jako při vydání pasu orgány veřejné správy).

13.2.2.7.1.2. RA – registrační autorita

Registrační autorita je entita, která je odpovědná za registraci subjektů a přijímá požadavky na certifikáty. Vlastní proces pro jednotlivé subjekty bude definován v průběhu projektu. V současné době se počítá s registrací zejména následujících subjektů:

- Mobilních zařízení – při prvotní instalaci platformy je vydán certifikát pro dané zařízení.
- Servery platformy – generováno při jejich instalaci serveru.

13.2.2.7.1.3. Adresářové služby

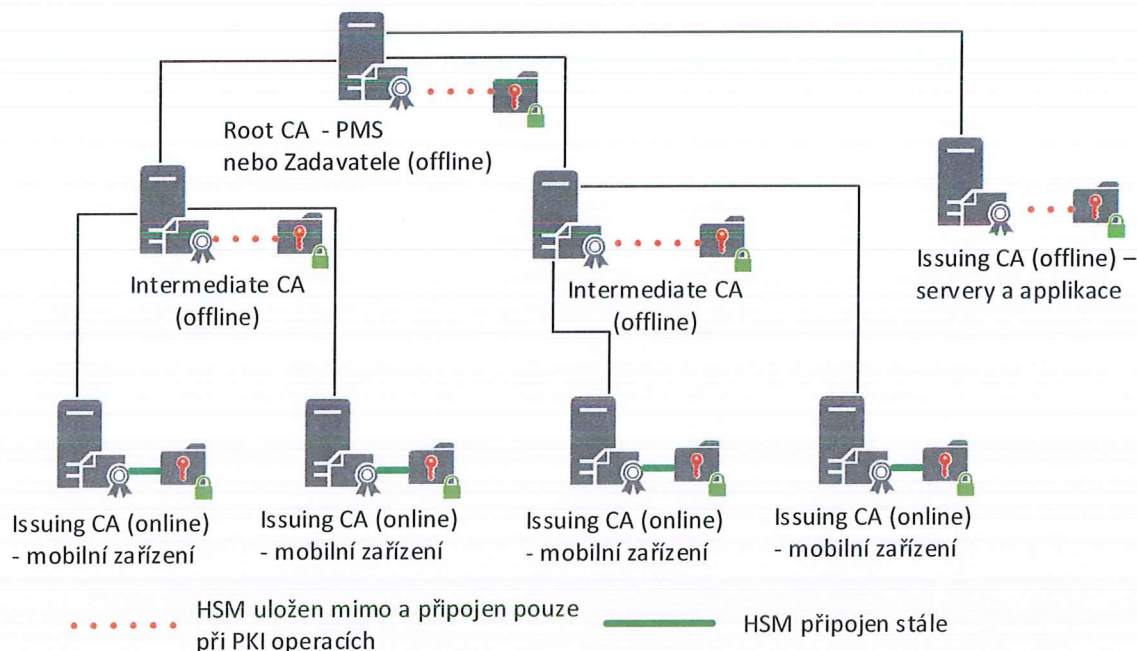
Adresářové služby (Directory services) jsou služby zodpovědné za ukládání klíčů, certifikátů a udržování aktuální listu zneplatněných certifikátů - Certificate Revocation Lists (CRLs). V našem případě jsou tyto služby postaveny na Microsoft Active Directory.

13.2.2.7.2. PKI architektura

Pro použití v rámci platformy navrhujeme použít dvou nebo tříúrovňový hierarchický model podle výsledků analýzy. V každém případě nedoporučujeme jednoúrovňový model, který nesplňuje obecné

požadavky na bezpečnost (může být použit pouze v rámci neprodukčních prostředí). Součástí jsou také HSM moduly (Hardware Security Module), které zvýší zabezpečení celého řešení.

Diagram řešení je na následujícím obrázku, kde je návrh tříúrovňové hierarchie, případný dvouúrovňový model nebude obsahovat Intermediate CA:



PKI architektura

Zobrazené komponenty plní následující role

- **Root CA** – jedná se o kořenovou CA a je postavená nejvýše v hierarchickém modelu. Tato Root CA je tzv. self-signed Certificate Authority (tedy vydala a podepsala certifikát sama sobě) a vydává, podepisuje pro CA o úroveň níže (Intermediate CA). V normální stavu je v produkci tato CA offline – tedy vypnutá aby nemohlo dojít k jejímu napadení a je zapínána pouze ve výjimečných případech – např. obnova certifikátů podřízených CA. S ohledem na bezpečnost je její privátní klíč uložen na HSM modulu, který je uložen v zabezpečeném úložišti a který je připojen pouze v případě potřeby podle postupů definovaných v rámci projektu. Root CA bude založena na Active Directory Certificate Services. V případě požadavku na využití Root CA kupujícího bude tato užita, jako náhrada Root CA PMS.
- **Intermediate CA** – je na druhé úrovni v hierarchickém modelu a je také někdy pojmenovávána policy-based CA. Tato CA vydává a podepisuje certifikáty jednotlivým Issuing CA, které vydávají vlastní certifikáty pro koncové použití. Výhodou zapojení těchto CA je vyšší flexibilita a škálovatelnost PKI infrastruktury. Předpokládá se, že každá bude na jiné lokalitě. V normální stavu je v produkci tato CA offline – tedy vypnutá aby nemohlo dojít k jejímu napadení a je zapínána pouze ve výjimečných případech – např. obnova certifikátů nebo participace při tvorbě nebo revokaci certifikátů pomocí Certificate Revocation Listu (CRLs). S ohledem na bezpečnost je její privátní klíč uložen na HSM modulu, který je uložen v zabezpečeném úložišti a který je připojen pouze v případě potřeby podle postupů

definovaných v rámci projektu.

Intermediate CA bude opět založena na Active Directory Certificate Services.

- Issuing CA (online) - mobilní zařízení – z pohledu koncových zařízení se jedná o nejvíce zatíženou komponentu, která vydává a zpravuje certifikáty pro koncové subjekty (v tomto případě mobilní zařízení). S ohledem na denní zatížení je HSM modul připojen permanentně, ale kontrolovaně. Vydávání bude zajištěno tak, aby byly certifikáty pokud možno rozprostřeny rovnoměrně mezi jednotlivými CA.

Tyto CA budou založeny na Active Directory Certificate Services, Active Directory (kde jsou uloženy certifikáty) a na zákaznickém vývoji (poskytování služeb v rámci platformy).

- Issuing CA (offline) – servery a aplikace – tato CA je oproti předchozí používána výrazně méně a proto bude většinou vypnutá a z pohledu bezpečnosti bude HSM opět uložen mimo a připojován jen při operacích vydávání certifikátu pro servery a v případě certifikace aplikace. Pokud se v rámci bezpečnostního projektu ukáže, že je nutné funkcionality pro podepisování kódu oddělit bude připraven další uzel PKI infrastruktury dedikovaný pro tuto část.

Na schématu je také tato CA podřízena přímo pod Root CA, nicméně je možné, že bude přiřazena pod Intermediate CA.

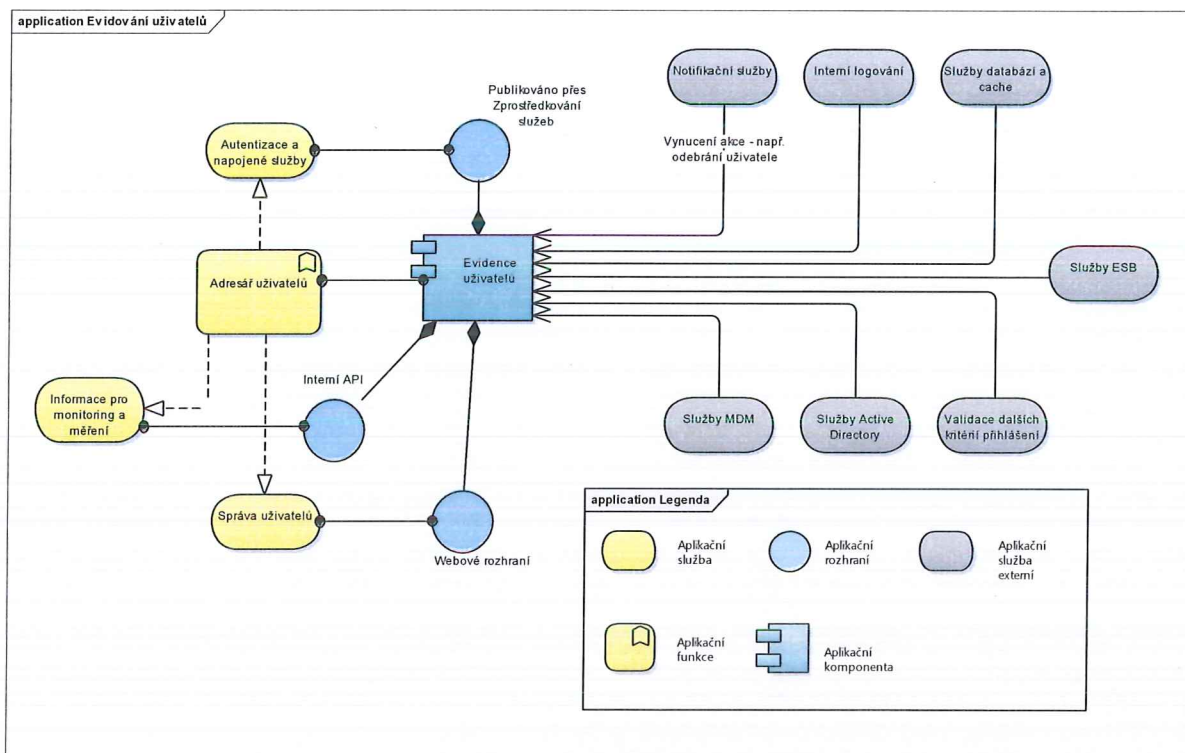
Na diagramu nejsou zobrazeny služby spojené s vedením Certificate Revocation Listu, který je nedílnou součástí řešení. Pokud se v rámci analýzy ukáže, jako nezbytné, je případně možné používat i Online Certificate Status Protocol. Tento protokol slouží k ověření stavu X.509 certifikátu, zejména zda certifikát nebyl revokován (zneplatněn). OCSP je definován v RFC 6960 a nahrazuje starší CRL (Certificate Revocation List). OCSP komunikace probíhá na bázi dotaz-odpověď přes HTTP, načež serverům provozujícím OCSP se obecně říká OCSP Responder, který by provozovala certifikační autorita (CA), jež vystavila X.509 certifikát. Hlavní výhodou OCSP oproti CRL jsou výrazně nižší nároky na data, protože odpověď responderu zpravidla obsahuje méně informací. Variantně se může použít kombinace.

Výše popsané řešení počítá s vytvořením kompletně nezávislé PKI infrastruktury, nicméně je možné ji napojit i další CA kupujícího (tzv. „Cross-Certification Trust“) nebo přímo použít Root CA kupujícího.

Celý systém je dimenzován jako vysoce škálovatelný a může sloužit jako CA i pro další použití bude použit i pro poptávané MDM v rámci části A. V případě přidání dalších prvků (servery) je samozřejmě možné i další užití.

13.2.2.8. Evidování uživatelů

Komponenta realizuje evidenci uživatelů a zajišťuje vedení a správu adresáře uživatelů mobilní platformy a jejich přístupových údajů s možností vyhodnocení doplňujících faktorů při autentizaci uživatele. Funkcionality realizuje v těsné spolupráci s Active Directory(AD) kupujícího dostupné přes LDAP. Základní schéma je zobrazeno na následujícím diagramu.



Základní pohled na Evidování uživatelů

Požadovaná funkcionalita je založena na následujících principech:

- Uživatelé jsou primárně spravováni v Active Directory kupujícího, v rámci modulu se udržují pouze případné atributy a data, které není možné v rámci AD spravovat.
- Spolupráce s AD je také potřebná v případě realizace požadavků na blokaci uživatele a dodání doplňkových informací (např. zda je nutné měnit heslo).
- Validace dalších kritérií přihlášení (dle požadavku PAR2, EVU3, EVU4) je realizováno pomocí volání odpovídající webové služby připravené kupujícím.
- Uzamknutí účtu je učiněno po definovaném množství (konfigurovatelné) neúspěšných pokusů na straně serveru (dle požadavku PAR9).
- Aby byl zajištěn požadavek PAR7 (Heslo a další citlivé údaje použité pro autorizace nejsou nikdy odesílány v otevřené podobě a vždy musí být posílán jejich hash) bude pro autentizaci v Active Directory použita autentizační metoda Simple Authentication and Security Layer (SASL), které je užívána v rámci Lightweight Directory Access Protocol (LDAP) a definována v Request for Comments (RFC) 2222.
- Kontrola mobilního zařízení (požadavek EVU3 - je zařízení z pohledu MDM korektně zpravováno a podle nastavení i přiřazeno uživateli) je realizováno voláním odpovídající služby MDM.
- Tato komponenta nezajišťuje autentizaci ani autorizaci pro „interní“ informační systémy kupujícího. Ty musí případné požadavky realizovat pomocí vlastních funkcí (viz požadavek INB2). Nicméně není problém předávat identifikace uživatele a přiřazené skupiny, tak jak ji ověřil tento modul a modul Evidování uživatelů. V případě potřeby je možné dopsat odpovídající funkcionalitu např. za pomoci protokolu Kerberos pro jednotlivé další aplikace (podobně jak se plánuje pro potřeby dodávané Referenční aplikace).

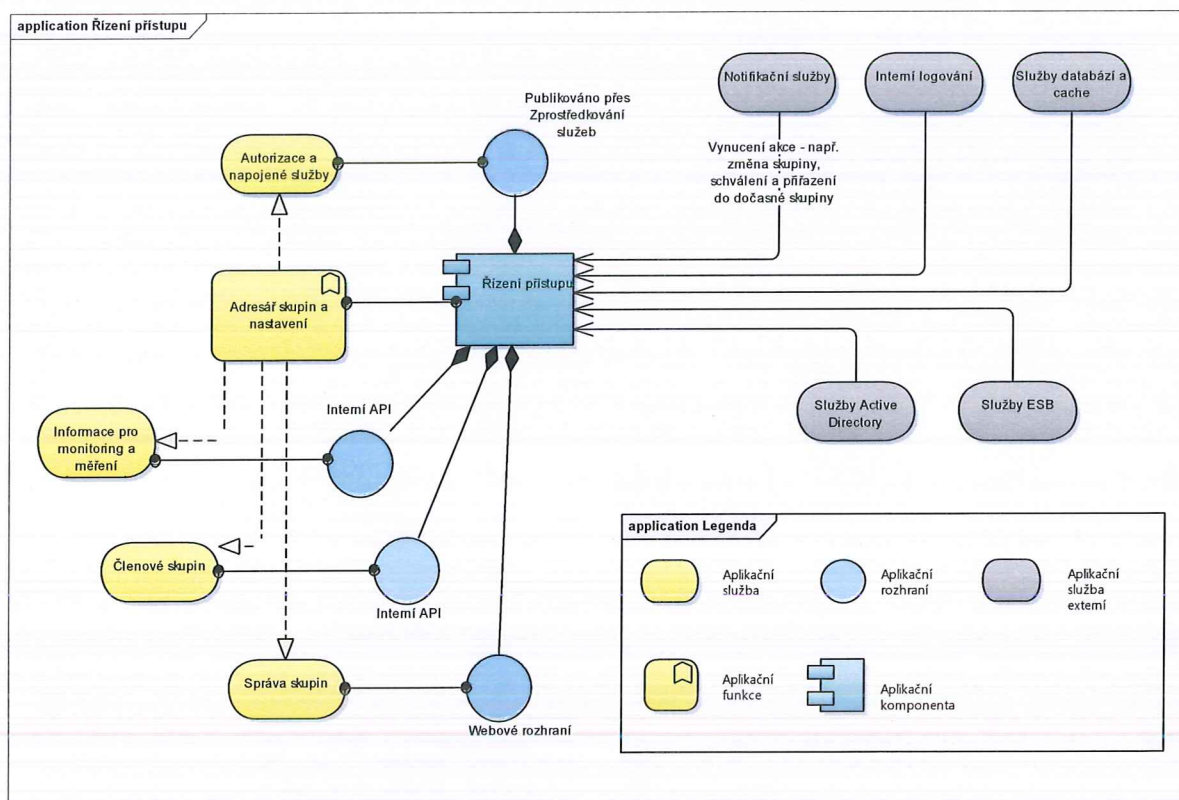
- Notifikace bude použita v případě informování o odebrání uživatele z adresáře, nebo jeho blokaci – aby mohla být na straně mobilního zařízení provedena odpovídající operace.
- Komponenta Evidence uživatelů bude vytvořena pomocí zákaznického vývoje.
- Logování je realizováno za pomoci komponenty Logování a audit.

Služby nabízené touto komponentou jsou následující:

- Autentizace a napojené služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné autentizovat uživatele a získat doplňkové informace v rámci odpovědi (např. zda je nutné měnit heslo, stav účtu). Vlastní autentizace je přes LDAP a SASL.
- Informace pro monitoring a měření dostupné interní API – poskytují informace o základních statistikách – jako je počet uživatelů.
- Správa aplikací dostupná přes webové rozhraní – umožní přístup k adresáři uživatelů a umožní jejich blokaci.

13.2.2.9. Řízení přístupu

Komponenta realizuje evidenci uživatelů a zajišťuje vedení a správu adresáře skupin uživatelů užívaných v rámci mobilní platformy. Tuto funkcionalitu realizuje v těsné spolupráci s Active Directory (AD) kupujícího dostupné přes LDAP (kde získává skupiny uživatelů), interně udržuje pouze tzv. dočasné skupiny. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Řízení přístupu

Požadovaná funkcionalita je založena na následujících principech:

- Skupiny uživatelů jsou primárně spravovány v Active Directory kupujícího, v rámci modulu se udržují pouze případné atributy a data, které není možné v rámci AD spravovat a pak tzv. dočasné skupiny.

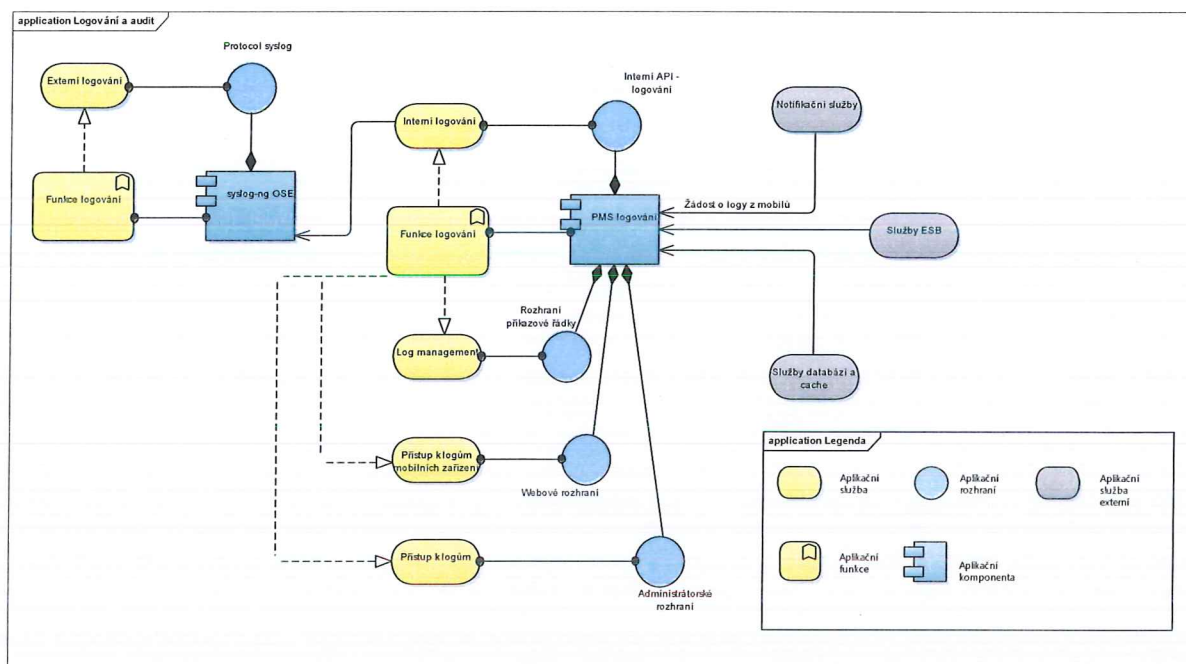
- V rámci modulu je možné evidovat tzv. dočasné skupiny, které umožní vytvářet ad-hoc skupiny bez odpovídající skupiny v AD. Nastavení je dostupné pouze pro administrátory a přiřazení do skupiny může vyžadovat schválení na straně uživatele (v rámci platformy mobilního zařízení).
- Realizace validace doplňkových pravidel – např. času, umístění, použitého komunikačního kanálu, zda jsou certifikáty uloženy v interním úložišti telefonu apod., je realizováno v rámci aplikace funkcionalitou napsanou na zakázku (PAR2).
- Dodatečná pravidla (dle požadavku PAR4) jsou realizována pomocí uložení nastavení v kontextu skupin (pokud je uživatel členem skupiny, pro kterou jsou definována další nastavení je toto reflektováno při odesílání celkového nastavení – je tak možné např. definovat, že pokud je uživatel členem vybrané skupiny, není mu umožněna komunikace přes některé kanály).
- Tato komponenta nezajišťuje autentizaci ani autorizaci pro „interní“ informační systémy kupujícího. Ty musí případné požadavky realizovat pomocí vlastních funkcí (viz požadavek INB2). Nicméně není problém předávat identifikace uživatele a přiřazené skupiny, tak jak ji ověřil tento modul a modul Evidování uživatelů (kapitola 13.2.2.8). V případě potřeby je možné dopsat odpovídající funkcionalitu např. za pomoci protokolu Kerberos pro jednotlivé další aplikace (podobně jak se plánuje pro potřeby dodávané Referenční aplikace (kapitola 13.2.3.)).
- Notifikace bude použita v případě změny skupin a jejich nastavení, schválení a přiřazení do dočasné skupiny.
- Komponenta Řízení přístupu bude vytvořena pomocí zákaznického vývoje.
- Logování je realizováno za pomoci komponenty Logování a audit.

Služby nabízené touto komponentou jsou následující:

- Autorizace a napojené služby přes modul Zprostředkování služeb – pomocí těchto služeb bude možné autorizovat uživatele a získat informace o právech a nastavení v rámci odpovědi. Vlastní skupiny jsou získávány přes LDAP z AD a v rámci modulu (dočasné skupiny).
- Členové skupin dostupné přes interní API – poskytují informace o jednotlivých uživateli v skupinách např. pro potřeby modulu Notifikace.
- Informace pro monitoring a měření dostupné přes interní API – poskytují informace o základních statistikách – jako je počet skupin.
- Správa aplikací dostupná přes webové rozhraní – umožní přístup k adresáři skupin (a to včetně dočasných) a nastavení.

13.2.2.10. Logování a audit

Zprostředkování služeb – budou přes to publikovat služby (ukládání logů z mobilu) – asi nová služba na diagramuKomponenta realizuje vysoce spolehlivé ukládání auditních a logovacích informací pocházejících jak ze samotné mobilní platformy, tak i z jednotlivých aplikací. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Logování a audit

Požadovaná funkcionalita je založena na následujících principech:

- Cílovou destinací logů je primárně databáze, která umožňuje pokročilý přístup k těmto datům a jejich následné vytěžení, pro méně důležité informace a pro provozní logy bude použit souborový systém.
- Interní logování (vytvořené zakázkovým vývojem) bude nabízet služby pomocí interního API, aby byla zajištěna konzistence informací a jejich následné uložení.
- Přístup externím systémům protokolem Syslog je umožněn za pomoci nástroje syslog-ng OSE, který pak předá relevantní informaci přes interní API a to je pak uloženo do databáze. Logové informace s nižší důležitostí mohou být rovnou uloženy do souborů, které mohou být dále využívány a případně kopírovány na další lokalitu.
- Ostatní komponenty platformy logují primárně přes výše uvedená rozhraní, v případě že používají vlastní logy, tyto logy plní požadavky uvedené v zadání a jedná se jen o dílčí části, jejichž logy jsou primárně potřebné pro technické účely.
- Komponenta PMS logování bude vytvořena pomocí zákaznického vývoje, komponenta syslog-ng OSE je založena na obecně rozšířeném nástroji šířeným pod LGPL+GPL licencí (jádro programu syslog-ng OSE je šířeno pod licencí GNU Lesser General Public License Version 2.1 a zbytek programů tvořící celý nástroj je licencovaný pod GNU General Public License Version 2 license).

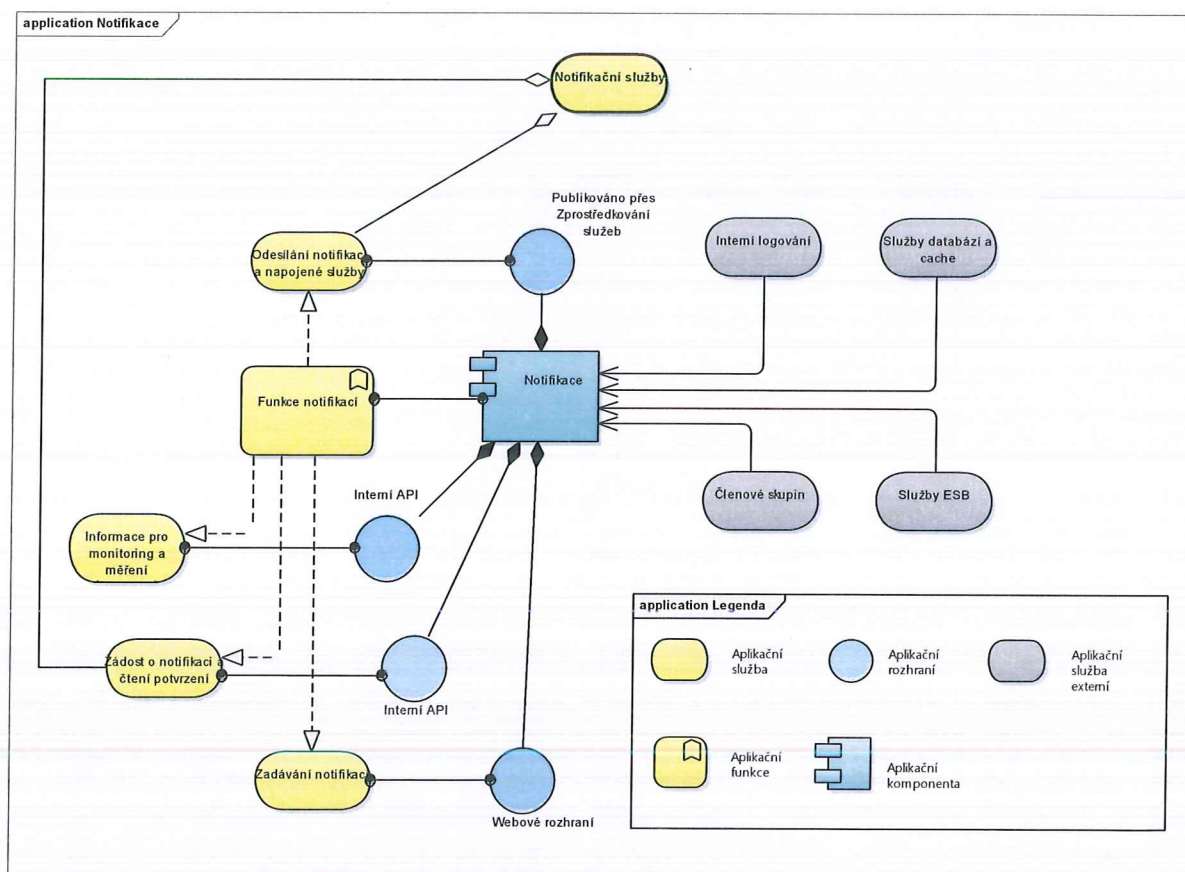
Služby nabízené touto komponentou jsou následující:

- Interní logování přes interní API – primární rozhraní pro logování a audit, využíváno všemi dalšími moduly platformy pro garanci konzistentních informací.
- Externí logování přes protokol syslog – rozhraní zejména pro externí komponenty řešení, které nemohou použít interní API. Zde logované informace budou primárně ukládány na souborový systém, pro události z vysokou důležitostí budou přes dedikovanou a distribuovanou ActiveMQ frontu ukládány pomocí interního API.

- Log management dostupný přes rozhraní příkazové řádky – řeší základní procesy log managementu a to rotaci logů, jejich retenci a archivaci. Jednotlivé příkazy je možné volat buď ad-hoc v případě potřeby a budou také součástí pravidelně vykonávaných příkazů pomocí scheduleru.
- Přístup k logům mobilních zařízení pomocí webového rozhraní – umožní přístup k historickým logům na mobilních zařízeních. Pomocí rozhraní dostupného administrátorům systémů bude možné zadat request, který bude odeslán na mobilní zařízení (pomocí služeb Notifikace), a z něj pak budou odeslány zpět do platformy mobilních služeb, kde jsou dostupné administrátorům pomocí standardních nástrojů.
- Administrátorský přístup k logům přes administrátorské rozhraní – výsledné logy jsou dostupné administrátorům a pracovníkům podpory buď přes sdílené databázové pohledy (pokud je finální destinací databáze) nebo pomocí systémových nástrojů operačního systému, pokud je cílovou destinací souborový systém.

13.2.2.11. Notifikace

Komponenta realizuje odesílání notifikací a nabízí služby spojené s jejich správou a ve spolupráci s databází zajišťuje persistenci neodeslaných notifikací. Funkcionalitu realizuje v těsné spolupráci s modulem Ukončení zabezpečené komunikace pro zajištění optimálního využití dostupných komunikačních kanálů. Základní schéma je zobrazeno na následném diagramu.



Základní pohled na Notifikace

Požadovaná funkcionalita je založena na následujících principech:

- Existují primárně dva typy notifikací – systémové a uživatelské (viz požadavky ZPN3 a ZPN4).