FAKULTNÍ NEMOCNICE OLOMOUC

Níže uvedeného dne, měsíce a roku uzavřeli

Fakultní nemocnice Olomouc
státní příspěvková organizace zřízená Ministerstvem zdravotnictví ČR rozhodnutím ministra zdravotnictví ze dne 25.11.1990, č.j. OP-054-25.11.90
se sídlem: I. P. Pavlova 185/6, 779 00 Olomouc
IČ: 00098892
DIČ: CZ00098892
Zastoupená: prof. MUDr. Romanem Havlíkem, Ph.D., ředitelem
bankovní spojení: bankovní spojení: ČNB
číslo účtu: 36334811/0710

na straně jedné jako *„objednatel"*

a

Teskalabs Ltd., (zakládající zahraniční společnost),
se sídlem: F6s Accounting, Unit 6 Queens Yard, White Post Lane, London, England, E9 5 EN
IČ (Company ID No.): 8893495
prostřednictvím
Teskalabs Ltd., odštěpný závod,
Se sídlem: Kodaňská 1441/46, Praha 10, 101 00
IČ: 07957157,
DIČ: CZ684810425
zastoupená: Vladimírou Teskovou, vedoucí odštěpného závodu,
zapsaná v Obchodním rejstříku vedeném Městským soudem v Praze, pod spisovou značkou A 79133
bankovní spojení: PPF Banka a.s.
číslo účtu: 6063410004/6000

na straně druhé jako *„poskytovatel"*

(Uvedení zástupci obou stran prohlašují, že podle stanov nebo jiného obdobného organizačního předpisu jsou oprávněni tuto Smlouvu podepsat a k platnosti Smlouvy není třeba podpisu jiné osoby.)

tuto

Smlouvu o poskytnutí licence a služeb technické podpory a servisu

uzavřená dle § 1746 odst. 2 zák. č. 89/2012 Sb. občanského zákoníku v platném znění

I.
Úvodní ustanovení

1. Zúčastněné smluvní strany si navzájem prohlašují, že jsou oprávněny tuto smlouvu uzavřít a řádně plnit závazky v ní obsažené, a že splňují veškeré podmínky a požadavky stanovené zákonem a touto smlouvou.
2. Tato smlouva je uzavírána na základě výsledků zadávacího řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek v platném znění zahájeného objednatelem jako veřejným zadavatelem s názvem **„SW pro bezpečný přenos dat pro mobilní aplikace"**, evidenční číslo **VZ-2020-001074.** V případě, že je v této smlouvě odkazováno na zadávací dokumentaci, má se na mysli zadávací dokumentace vztahující se k uvedené veřejné zakázce. Smluvní strany se zavazují plnit podmínky obsažené v této smlouvě, přičemž za závazné se pro obě smluvní strany považuje rovněž zadávací dokumentace a nabídka, kterou poskytovatel předložil do zadávacího řízení.
3. Poskytovatel je povinen při realizaci předmětu smlouvy postupovat s řádnou odbornou péčí a chránit zájmy objednatele podle svých nejlepších profesních znalostí a schopností.
4. Poskytovatel je výrobcem nebo má od něj souhlas k distribuci, servisu a aktualizacím SW s názvem **TeskaLabs SeaCat** (dále jen „**Systém**") pro Fakultní nemocnici Olomouc (dále taky FNOL).

II.
Předmět smlouvy

1. Předmětem této smlouvy je:
   - poskytnutí SW licencí a implementace SW s názvem **TeskaLabs SeaCat** pro zabezpečenou komunikaci mezi mobilními zařízeními a serverem z hlediska požadavků na kybernetickou bezpečnost a ochranu dat pro mobilní aplikace ve zdravotnictví v souladu s platnou legislativou,
   - zajištění základní servisní technické podpory na 12 měsíců od předání Systému poskytovatelem k řádnému užívání objednatelem, v režimu 5x8 dle specifikace v Příloze č. 2 a Příloze č. 3 této smlouvy,
   - instalace programu na HW určený objednatelem dle specifikace v Příloze č. 2 smlouvy,
   - parametrizace programu v součinnosti s objednatelem,
   - dodávka SW bez omezení funkčnosti,
   - proškolení všech stanovených administrátorů objednatele přímými školiteli poskytovatele SW,
   - programové aktualizace (dodávka nových verzí, upgrade, update) včetně parametrizace programu v součinnosti se zadavatelem v případě, že ji nová aktualizace vyžaduje.
2. Dále je předmětem této smlouvy závazek poskytovatele poskytnout pro objednatele licence a zajistit služby technické podpory **Systému**, za podmínek stanovených v této smlouvě, v zadávací dokumentaci a SLA listech a závazek objednatele za poskytnutí licence a technické podpory platit cenu sjednanou v souladu s touto smlouvou, jakož i další závazky a práva smluvních stran z této smlouvy vyplývající.
3. Poskytovatel potvrzuje, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k poskytování služeb dle této smlouvy a že disponuje takovými odbornými znalostmi, které jsou k poskytování služeb nezbytné. Bude-li součástí poskytování služeb poskytnutí plnění, k němuž je nezbytné převedení vlastnického či jiného práva, garantuje poskytovatel, že takové plnění poskytuje se všemi právy nutnými k jeho řádnému a nerušenému nakládání a užívání objednatelem.
4. Poskytovatel garantuje po dobu platnosti smlouvy záruku za jakost jako shodu Systému s jeho dokumentací.
5. Poskytovatel se zavazuje poskytnout asistenci, analýzu a převod dat při přechodu objednatele na konkurenční SW jiného dodavatele za podmínek, stanovených smlouvou.
6. Poskytovatel prohlašuje, že poskytnuté SW řešení je již validované a je již využíváno pro zabezpečení jiných zdravotnických aplikací a je v souladu s platnou legislativou.

III.
Doba a místo plnění

1. Tato smlouva se uzavírá na dobu 12 měsíců od implementace a předání Systému k řádnému užívání. Platnou se stává dnem jejího podpisu oběma smluvními stranami a účinnou dnem zveřejnění v Registru smluv.

2. Poskytovatel se zavazuje poskytovat objednateli technickou podporu v rozsahu uvedeném v Příloze č. 2 a v Příloze č.3 této smlouvy.

3. Místem plnění je sídlo objednatele. Poskytovatel bere na vědomí, že v souladu s interními předpisy objednatele nese náklady související s vjezdem motorových vozidel do místa plnění za účelem plnění této smlouvy (dodávka, servis, údržba, jednání atp.).

IV.
Cena a platební podmínky

1. Cena technické podpory **Systému** je stanovena formou paušálu za fakturační období, který je složen z:
   a) Implementace SW;
   b) paušálu za využívané licence;
   c) dostupnosti služeb za podmínek stanovených SLA listy;
   d) aktualizací **Systému** z důvodu vylepšování, odstraňování závad v rámci záruky za jakost, technologického rozvoje, zvyšování bezpečnosti, zajištění souladu Systému s legislativními změnami
2. Podrobný popis služeb a způsob jejich poskytování je popsán v Příloze č. 2 Příloze č. 3 této smlouvy.
3. Objednatel se zavazuje po dobu platnosti této smlouvy platit poskytovateli za služby dle čl. IV.1 cenu stanovenou dohodou ve výši: **16 667,00 Kč bez DPH**, DPH 3 500,07 Kč, **20 167,07 Kč včetně DPH** za fakturační období.
4. Cena je stanovena jako pevná a nejvýše přípustná, závazná a platná po celou dobu platnosti smlouvy a nemůže být navýšena ani v případě zvýšení sazby DPH. Cena zahrnuje veškeré náklady, jejichž vynaložení je nutné na řádné a včasné splnění předmětu smlouvy, zejména náklady na dopravu, předání a veškeré náklady související. Poskytovatel bere na vědomí, že v souladu s interními předpisy objednatele nese náklady související s vjezdem motorových vozidel do místa plnění.
5. Fakturačním obdobím se rozumí kalendářní měsíc.
6. Objednatelem vyžádané služby při řešení poskytovatelem nezaviněných havarijních stavů Systému nebo obnovy poskytovatelem nezaviněné ztráty dat Systému budou řešeny samostatnými objednávkami na základě nabídky poskytovatele.
7. Všechny smlouvou dohodnuté ceny zahrnují veškeré náklady spojené s činnostmi, dopravou a materiálem pro zajištění služeb.
8. Podkladem pro zaplacení je daňový doklad (faktura) vystavený poskytovatelem.
9. Daňový doklad (faktura) bude poskytovatelem vystaven v souladu s ustanovením zákona č.235/2004 Sb. o dani z přidané hodnoty ve znění pozdějších předpisů vždy k prvnímu dni příslušného kalendářního měsíce, na který se poplatek vztahuje. Poskytovatel se zavazuje takto vystavenou fakturu předat objednateli nejpozději do 10 dnů od začátku fakturačního období.
10. Splatnost faktury je stanovena na 60 dní od data prokazatelného doručení faktury objednateli. Každá jednotlivá faktura vystavená v rámci smluvního vztahu založeného touto smlouvou musí obsahovat identifikátor veřejné zakázky **VZ-2020-001074.**
11. Cena se považuje za zaplacenou v okamžiku jejího odeslání z účtu objednatele na účet poskytovatele.
12. Poskytovatel je oprávněn vystavit první daňový doklad dle této smlouvy teprve po ukončení implementace Systému a předání SW licencí k řádnému užívání objednateli. Výše paušálu za toto první fakturační období se stanoví jako alikvot počtu kalendářních dnů v daném měsíci.

V.
KOMUNIKACE

1. **Kontaktní údaje** pro komunikaci při plnění služeb technické podpory Systému z této smlouvy jsou.
   - Dispečink objednatele:
     tel: +420588444516
     email: informatika@fnol.cz

- Dispečink poskytovatele:
  Hotline v pracovní době: +420 604 806 483
  Hotline mimo pracovní dobu: +420 604 806 483
  email: support@teskalabs.com

2. **Odpovědnými osobami** pověřenými jednat jménem smluvních stran při plnění a výkladu závazků z této smlouvy ve věcech technických jsou:
   - za objednatele: náměstek informačních technologií zastupuje: vedoucí Odboru informatiky
     tel: [redacted] Tel: [redacted]
     email: uis@fnol.cz e-mail: informatika@fnol.cz
   - za poskytovatele: [redacted] zastupuje:
     tel: tel:
     email: [redacted]

3. **Technický zástupce objednatele** je pracovník objednatele, který je oprávněn žádat a přebírat technickou podporu poskytovatele, resp. užívat služby Hotline poskytovatele.

4. **Konzultant poskytovatele** je pracovník poskytovatele, který má oprávnění přebírat požadavky objednatele a poskytovat služby technické podpory.

5. Pokud má být konzultantovi poskytovatele umožněn **vzdálený přístup**, musí poskytovatel předložit doklady zavazující konzultanta k mlčenlivosti dle odstavce X.5 této smlouvy. Přístup zajistí odpovědná osoba objednatele na základě písemné žádosti odpovědné osoby poskytovatele. Odebrání přístupu se bude provádět obdobným postupem.

6. Jakákoli komunikace mezi smluvními stranami ve věcech obchodních může být učiněna osobně nebo písemně.

7. O změnách v obsazení v odpovědných osobách jsou strany povinny se vzájemně bezodkladně písemně informovat.

8. Smluvní strany se dohodly, že běžné technické a organizační konzultace týkající se plnění této smlouvy odpovědnými osobami mohou být prováděny i telefonicky. Tyto konzultace v čase do 15 minut bude poskytovatel poskytovat bezplatně.

9. Pokud je ve smlouvě zmíněná **písemná** komunikace, pak se za ni považuje:
   a) Zaslání listinného dokumentu poštou nebo doručené kurýrem
   b) Zaslání elektronického dokumentu elektronicky podepsaným emailem
   c) Zaslání elektronicky podepsaného dokumentu emailem

VI.
ZÁKLADNÍ PODMÍNKY SPOLUPRÁCE STRAN

1. Poskytovatel se zavazuje zajišťovat objednateli technickou podporu řádně, včas a s náležitou odbornou péčí v souladu s příslušnými právními a technickými předpisy a dohodnutými podmínkami této smlouvy.

2. Poskytovatel bere na vědomí, že vlastníkem dat vložených objednatelem je objednatel, že data v databázi jsou pro objednatele nepostradatelná a ztrátou přístupu k nim nebo nemožností jejich zpracování by objednateli vznikla škoda značného rozsahu.

3. Objednatel se v této souvislosti zavazuje případné ztrátě dat předcházet cestou pravidelného zálohování databází a transakčních logů tak, aby se minimalizovaly případné ztráty dat pouze na krátké časové období.

4. Dojde-li k významné ztrátě dat zaviněnou poskytovatelem, potom:
   a) objednatel je povinen poskytnout poskytovateli neprodleně data ze zálohy tak, aby mohl poskytovatel provést rekonstrukci ztracených dat;
   b) poskytovatel provede rekonstrukci dat na svoje náklady;
   c) pokud by i po rekonstrukci trvala významná ztráta dat, je poskytovatel povinen objednateli uhradit škodu, která vznikla obnovou dat zaměstnanci objednatele s tím, že objednatel vyčíslí poskytovateli tyto náklady položkově, a to počtem hodin a počtem zaměstnanců k obnově dat nutných. Hodinová sazba se pro tyto účely stanovuje ve výši 350 Kč. Poskytovatel se zavazuje tuto škodu uhradit ve lhůtě do 30 dnů od odeslání vyúčtování objednatelem.

5. Dojde-li ke změně vlastníka nebo změně obchodního názvu společnosti na straně poskytovatele, je poskytovatel povinen tuto skutečnost s dostatečným předstihem objednateli oznámit.

6. Poskytovatel se zavazuje, že data objednatele, která jsou svým obsahem citlivá, nebudou poskytovatelem *šířena mimo servery objednatele. Za citlivá data se považují všechny osobní údaje dle specifikace nařízení* GDPR a ta data, která objednatel označí jako citlivá formou písemného sdělení poskytovateli.

7. Objednatel se zavazuje, že data označená jako citlivá nebude poskytovateli jakoukoliv formou zasílat (případně zaslané osobní údaje vždy anonymizuje). Pokud k tomu přesto dojde, provede poskytovatel neprodleně výmaz (skartaci) těchto dat (u osobních údajů v nezbytných případech z důvodu plnění požadovaných služeb provede poskytovatel jejich anonymizaci) a informuje o tom neprodleně písemně odpovědnou osobu objednatele.

8. Před ukončením této smlouvy, a to i v případě jednostranné výpovědi:
   - poskytovatel poskytne na vyžádání objednatele bezplatně (z databáze **Systému)** úplný export dat vložených objednatelem tak, aby je mohl objednatel sám dle potřeby kdykoliv použít, a to v otevřeném formátu (např. CSV, XML, XLS) do transparentní struktury vhodné pro další zpracování. Úplností dat se rozumí veškerý obsah dat z databáze, který umožní zpracování veškerých informací v databázi uložených, zejm. musí být umožněna kompletní rekonstrukce dat bez ztráty jakýchkoliv informací.
   - Objednatel má pak právo takto vyexportovaná data bezplatně poskytnout třetí straně za účelem jejich dalšího zpracování ve prospěch objednatele (zejm. analýza, validace, transformace, migrace dat).

9. V případě nesplnění výše uvedených závazku poskytovatele z odstavce VI.8 má objednatel právo bezplatně poskytnout přímý přístup třetím stranám do databáze k datům vložených objednatelem, tj. na takové případy se nebude vztahovat mlčenlivost ujednaná ve smlouvě v čl. X.

VII.
PRÁVA A POVINNOSTI OBJEDNATELE

1. Objednatel se zavazuje zajišťovat poskytovateli součinnost nezbytnou k plnění této smlouvy.

2. Objednatel se zavazuje, že zajistí pracovníkům poskytovatele fyzický přístup s doprovodem do všech prostor dotčených pro nezbytné plnění této smlouvy (pracovní dny 07:00 – 15:30 hod).

3. Objednatel se pro zajištění technické podpory poskytovatele zavazuje:
   a) poskytnout vzdálený přístup pro spravovaná prostředí;
   b) zabezpečit nezbytnou součinnost poskytovateli pro výkon poskytovaných služeb.

VIII.
SMLUVNÍ SANKCE

1. Odpovědnost za škodu se řídí příslušnými ustanoveními občanského zákoníku.

2. V případě prodlení poskytovatele s plněním svých závazků reakční doby ve lhůtách stanovených v Příloze č. 3 této smlouvy, je objednatel oprávněn žádat a poskytovatel povinen zaplatit smluvní pokutu takto:
   a) *neposkytnutí aktualizace - ve výši 90% aktuálního měsíčního paušálu;*
   b) neuvolnění otestované verze aktualizace nejpozději ke dni účinnosti legislativní změny - ve výši 50% aktuálního měsíčního paušálu.

3. V případě prodlení poskytovatele s jakýmikoli jeho dalšími závazky dle této smlouvy je objednatel oprávněn žádat a poskytovatel povinen zaplatit smluvní pokutu ve výši 0,5% hodnoty předmětu plnění za každý započatý den prodlení, nedohodnou-li se smluvní strany jinak.

IX.
UKONČENÍ SMLOUVY

1. Smlouva může být ukončena písemnou dohodou stran nebo odstoupením ze zákonných důvodů. Oznámení o odstoupení musí být písemné a musí být doručeno druhé straně na adresu uvedenou v této smlouvě.

2. Poskytovatel má právo odstoupit od smlouvy v případě prodlení objednatele s úhradou faktur poskytovatele překračujícím o 60 dnů termín splatnosti. Poskytovatel v rámci této doby písemně vyzve k úhradě splatného závazku.
3. *Objednatel má právo smlouvu vypovědět, a to i bez uvedení důvodu s jednoměsíční výpovědní dobou, která* počíná běžet od prvního dne měsíce následujícího po doručení výpovědi.
4. Poskytovatel má právo smlouvu vypovědět, a to i bez uvedení důvodu se tříměsíční výpovědní dobou, která počíná běžet od prvního dne měsíce následujícího po doručení výpovědi.
5. Kterákoliv ze smluvních stran je oprávněna tuto smlouvu vypovědět s okamžitou platností v případě, že druhá smluvní strana hrubě poruší nebo opakovaně porušuje své smluvní závazky vyplývající z této smlouvy a přes písemnou výzvu odmítá odstranit vady svého jednání, anebo nečiní žádné kroky k nápravě vzniklého vadného stavu, nebo v případě, že druhá smluvní strana vstoupí do likvidace anebo bude vůči ní prohlášen konkurs.

X.
MLČENLIVOST

1. Smluvní strany se zavazují zachovávat vůči třetím osobám mlčenlivost o informacích, které získají v průběhu plnění této smlouvy vyjma situací, kdy obdrží od druhé strany písemné svolení.
2. Za důvěrnou informaci se pro účely této smlouvy považují všechny informace, které jedna strana získala v průběhu plnění smlouvy od druhé strany, a to i když se nejedná o obchodní tajemství dle občanského zákoníku, stejně tak i know-how, kterým se rozumí všechny poznatky obchodní, výrobní, technické a ekonomické povahy související s činností druhé strany, které mají skutečnou nebo alespoň potencionální hodnotu.
3. Poskytovatel je povinen zavázat povinností mlčenlivosti všechny osoby, které se budou podílet na poskytování služeb dle této smlouvy včetně osob třetích stran, které mohou být přizvány po předchozím písemném souhlasu objednatele.
4. Poskytovatel před podpisem této smlouvy předloží doklady zavazující jeho zaměstnance, kteří se budou podílet na plnění předmětu smlouvy k mlčenlivosti o informacích získaných u objednatele. Totožný doklad je poskytovatel povinen předložit i v případě, kdy pověří nového zaměstnance plněním předmětu této smlouvy.
5. Komunikace vztahující se k této smlouvě bude probíhat pouze prostřednictvím osob oprávněných dle čl. V. odst. 2. jednat jménem smluvních stran.
6. Trvání mlčenlivosti není omezeno trváním této smlouvy a trvá i po jejím zániku.
7. Smluvní strany souhlasně prohlašují, že předmětem této smlouvy není přenos či zpracování osobních údajů. Nicméně poskytovatel se zavazuje v souvislosti s předmětem plnění této smlouvy, že pověření pracovníci, kteří i přesto přijdou do styku s osobními/citlivými údaji ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění, učiní veškerá opatření, aby nedošlo k jejich neoprávněnému užití, změně, zcizení, ztrátě, zničení nebo neoprávněným přenosům.
8. Pokud poskytovatel poruší svoji povinnost mlčenlivosti, je objednatel oprávněn požadovat po poskytovateli smluvní pokutu, a to jednorázově ve výši 30.000,- Kč. Smluvní pokutu, sjednanou touto smlouvou, zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé straně škoda, kterou lze vymáhat samostatně.

XI.
ZÁVĚREČNÁ USTANOVENÍ

1. Neplatnost některého smluvního ustanovení nemá za následek neplatnost celé smlouvy, pokud se nejedná o skutečnost, se kterou zákon spojuje takové účinky. Pokud dojde ke změně obecně závazných právních předpisů, bude příslušné ustanovení této smlouvy, kterého se změna týká upraveno v souladu s touto změnou, přičemž ostatní smluvní ujednání zůstávají v platnosti, pokud by z dohody smluvních stran, nebo z povahy změny nevyplývalo něco jiného.
2. Poskytovatel souhlasí se zveřejněním této smlouvy včetně všech jejích náležitostí.

3. Tato smlouva je vyhotovena ve dvou exemplářích, z nichž každý má sílu originálu. Objednatel obdrží jeden a poskytovatel jeden exemplář smlouvy.
4. Tuto smlouvu nelze dále postupovat, jakož ani pohledávky z ní vyplývající. Kvitance za částečné plnění a *vracení dlužních úpisů s účinky kvitance se vylučují.*
5. Změny této smlouvy mohou být provedeny pouze písemnou dohodou smluvních stran.
6. Tato smlouva se řídí českým právním řádem. Nepodaří-li se případné spory vyřešit smírem, bude je rozhodovat soud místně příslušný dle sídla objednatele.
7. Poskytovatel i objednatel souhlasí s tím, že veškeré přílohy smlouvy jsou její nedílnou součástí.
   - Příloha č. 1 – Položkový seznam a technická specifikace
   - Příloha č. 2 – Požadavky na SW pro kybernetickou bezpečnost a ochranu dat pro mobilní aplikace ve zdravotnictví.
   - Příloha č. 3 – Podrobný popis služeb (SLA)
8. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že rozumí jejímu obsahu, souhlasí s ním, a dále prohlašují, že tuto smlouvu neuzavřely v tísni, ani za jiných nápadně nevýhodných podmínek.

V Olomouci dne: 28. 12. 2020 V Praze dne: 22. 12. 2020

[redacted]

Příloha číslo 1 smlouvy
Položkový seznam a technická specifikace

Aplikace (SW): TeskaLabs SeaCat

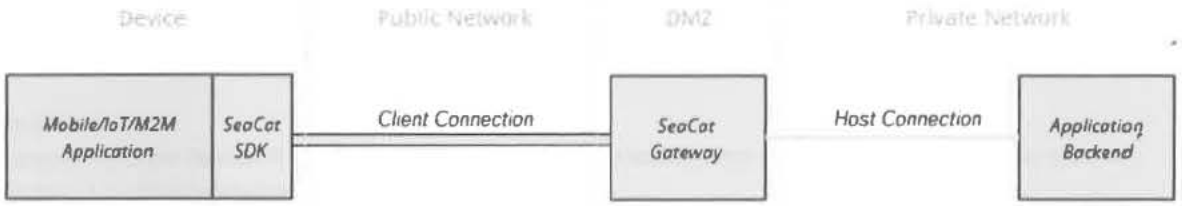
Licence: Licence TeskaLabs SeaCat pro jednu mobilní aplikaci pro období 12 měsíců

Produkt SeaCat

SeaCat poskytuje vysokou míru zabezpečení aplikací na široké škále zařízení (např. mobilní telefony, chytré IoT/M2M přístroje, tablety, počítače). Zajišťuje zabezpečené připojení koncových zařízení k veřejným sítím a chrání aplikace před kybernetickými hrozbami. Systémy s implementovaným SeaCat-em eliminují zranitelné části těchto prostředí a zařízení.

SeaCat je navržen k fungování ve velkých společnostech k zabezpečení objemných B2C (business-to-consumer), B2B (business-to-business) a B2E (business-to-employee) aplikací a velkých IoT aplikací.
SeaCat je tvořen těmito hlavními součástmi:

- SeaCat SDK
- SeaCat Gateway



Obrázek 1: Architektura SeaCat-u

Poznámka: v následujících textech jsou použity pojmy uživatel a klient, přičemž jejich význam je následující: klient je aplikace s integrovaným SeaCat SDK; uživatel je uživatel aplikace.
SeaCat SDK
SeaCat SDK je softwarovou knihovnou, která je určena k integraci do dané mobilní, IoT nebo M2M aplikace. SeaCat SDK zabezpečuje klientské připojení mezi aplikací a jejími příslušnými backendy.
SeaCat SDK poskytuje:

- Identifikaci každého jedinečného klienta díky integrované certifikační autoritě a podpoře PKI;
- Podpora FIPS 140-2 šifrování na všech zařízeních, nezávislé na vlastnostech operačního systému (např. mobilní telefony se starou šifrovací knihovnou, IoT/M2M zařízení) díky integraci Open SSL kryptografického modulu;
- Zabezpečení dat na koncovém zařízení (např. páry klíčů, data aplikací) vzhledem k místnímu zabezpečenému trvalému úložišti;
- Bezpečný přenos dat mezi aplikací a SeaCat Gateway i přes nezabezpečené veřejné sítě;
- Bezpečná adaptační sekvence klienta.

SeaCat Gateway
SeaCat Gateway je serverový software, který slouží jako bezpečnostní Gateway mezi veřejnou sítí a sítí soukromou, a k orchestraci klientů. Je většinou vložen do demilitarizované zóny v cloudové či on-premise infrastruktuře. Přeposílá platné a ověřené klientské žádosti do příslušných aplikačních backendů skrze HTTP, MQTT a dalších protokolů. Je navržen s použitím POSIX standardu a běží na různých Linux a Apple Mac OS X operačních systémech.

SeaCat Gateway poskytuje:

- Ochranu před kybernetickými útoky (např. volumetrický DDoS, strojový probing, skenování portů) díky izolaci backendů aplikací od veřejných sítí;
- Ochranu před neoprávněným přístupem k aplikačním backendům z důvodu ověřování příchozích klientských připojení;
- Jednoduchý přístup k backendům aplikací díky velkému množství použitých součástí;

- Odolnost vůči náporu vzniklému při vyvažování objemu provozu mezi klienty a SeaCat Gateway;
- Možnost velkého průtoku dat díky jednoduché škálovatelnosti (např. stovky tisíc souběžných klientských připojení);
- Podporu tzv. „disaster recovery" plánů
- Správu přístupových práv;
- Certifikační autoritu;
- Revizní protokol k připojení k bezpečnostním informacím a správu událostí (SIEM) nebo centru síťového zabezpečení;
- Rozhraní pro programování aplikací (API).

Připojení Klienta

Připojení Klienta je realizováno pomocí síťového spojení s podobnými vlastnostmi jako Secure Socket Layer Virtual Private Network (SSL VPN) mezi SeaCat Gateway a SeaCat SDK (většinou v prostředí veřejné sítě). Zaručuje soukromí, integritu, autenticitu a zabraňuje pozměnění přenesených dat.

Připojení klienta poskytuje:

- Ochranu před zachycováním nebo jiným ovlivňováním přenosu dat díky vzájemnému SSL ověření;
- Zvýšení rychlosti komunikace díky zredukovanému HTTP protokolovému overheadu a trvalému připojení klienta;
- Možnost tzv. „server pushing" díky trvalému připojení klienta a MQTT podpoře;
- Vysokou úroveň zabezpečení díky šifrování vyhovující úrovním TLS 1.2/1.3, FIPS 140-2;
- SeaCat Gateway zabezpečuje, že každý klient je připojený k jednomu aplikačnímu backendu během celé relace. Ověřování (pinning) je aktivní až do odpojení klienta.

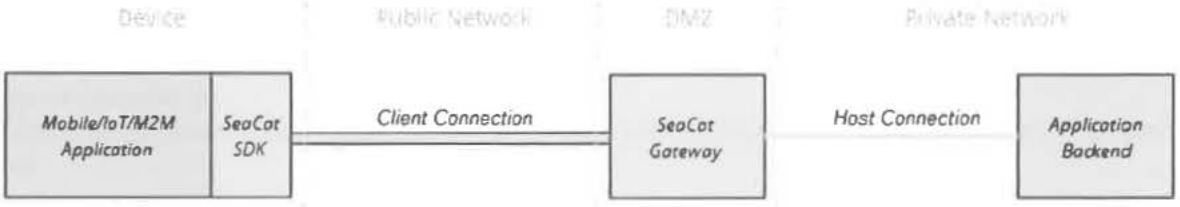
Připojení hostitele

Připojení hostitele je síťové spojení mezi SeaCat Gateway a backendem aplikace (většinou v soukromé síti). Připojení hostitele poskytuje:

- Podporu HTTP, HTTPS a MQTT protokolů;
- „Sticky" relaci na základě pinning-u k dané SeaCat Gateway a backendu konkrétní aplikace;
- Odolnost vůči náporu díky rozdělení provozu mezi SeaCat Gateway a hostitele (aplikace).

Diagram zabezpečené komunikace

Komunikace mezi aplikací a backendem aplikace obecně vypadá jako na obrázku 2 (s HTTP provozem jako příkladem):



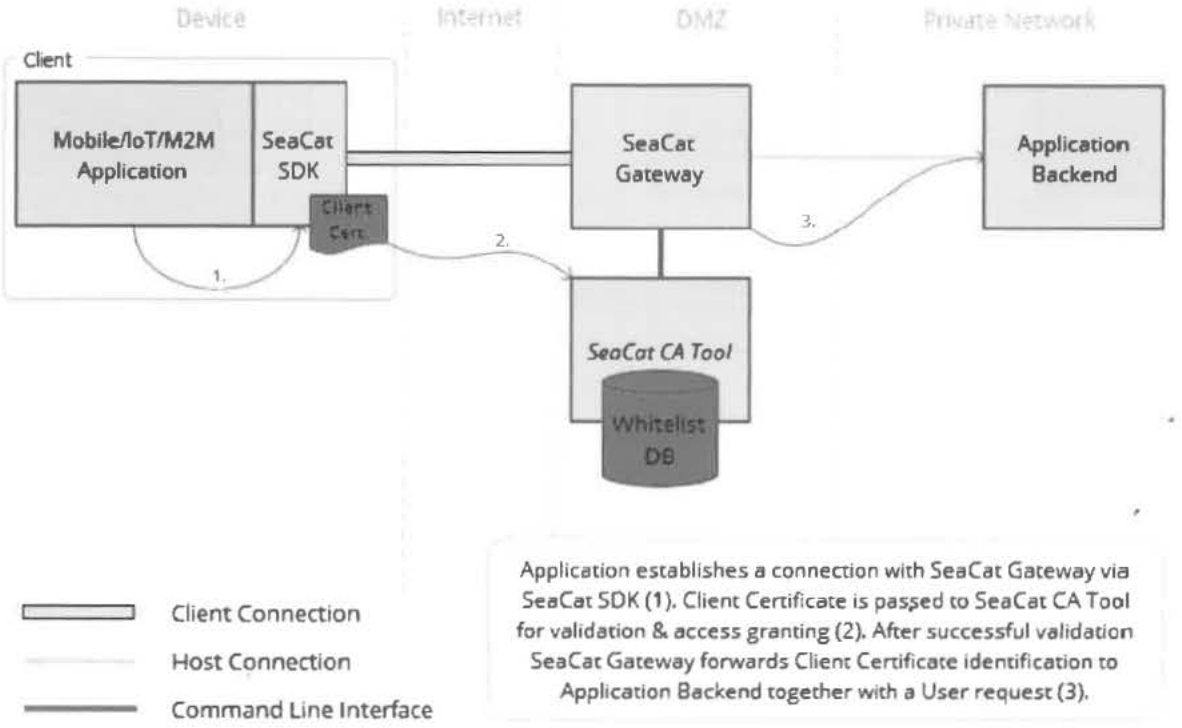
Obrázek 2: Komunikace mezi aplikací a backendem aplikace

1. Aplikace vytvoří http request
2. SeaCat SDK zachytí HTTP request
3. Skrze klientské připojení SeaCat SDK předá HTTP request SeaCat Gateway
4. SeaCat Gateway ověří klientský certifikát a oprávní klienta ke komunikaci s backendem aplikace
5. SeaCat Gateway převezme HTTP request a předá ji backendu aplikace
6. Odpověď od backendu je podobná, akorát v převráceném pořadí
7. Klientské spojení běží, dokud je klient aktivní

Správa Identit

Jedinečná identita každé konkrétní aplikace (např. mobilní aplikace nainstalovaná na zařízení) je založena na privátních a veřejných klíčích. Tuto dvojici klíčů generuje SeaCat SDK na místním zařízení během prvního spuštění aplikace a je vázána ke konkrétní aplikaci. Nazýváme ji Klient. Poté, co je Klient autorizován SeaCat Gateway, obdrží klient Klientský Certifikát ověřený Certifikační Autoritou ze SeaCat Gateway.

Ochranu Klientského privátního klíče zabezpečuje SeaCat SDK. Pokud je ve verzi operačního systému začleněný Secure Enclave nebo Andriod Keystore, může být Klientský privátní klíč chráněn těmito technologiemi.
V případě potřeby je k dispozici nadstavbová uživatelská ochrana Klientského privátního klíče za použití pokročilých šifrovacích technik (např. ochrana Heslem/PIN; NFC hardwarové tokeny apod.).
SeaCat Gateway ověřuje klientskou identitu během vytváření Klientského Připojení. SeaCat Gateway zprostředkovává propojení mezi klientem a příslušným Backendem Aplikace. Na základě whitelistu Klientských Certifikátů pak umožňuje či blokuje přístup k Backendu Aplikace. Administrátorský panel spravuje Klientské ověřování (existenci Klientského Certifikátu na whitelistu).



Klientské ID

Klientská identifikace je SHA-384 miniaturou (hash) Klientského veřejného klíče zvaná Klientské ID. Klientské ID poskytuje globální identifikaci Klienta. Klientské ID je hexadecimální vlákno o 96 znacích (povolené znaky jsou a-f0-9). Je používáno SeaCat-em pro všechny vnitřní procesy. Klientské ID abstrahuje ze všech polí Certifikátu.

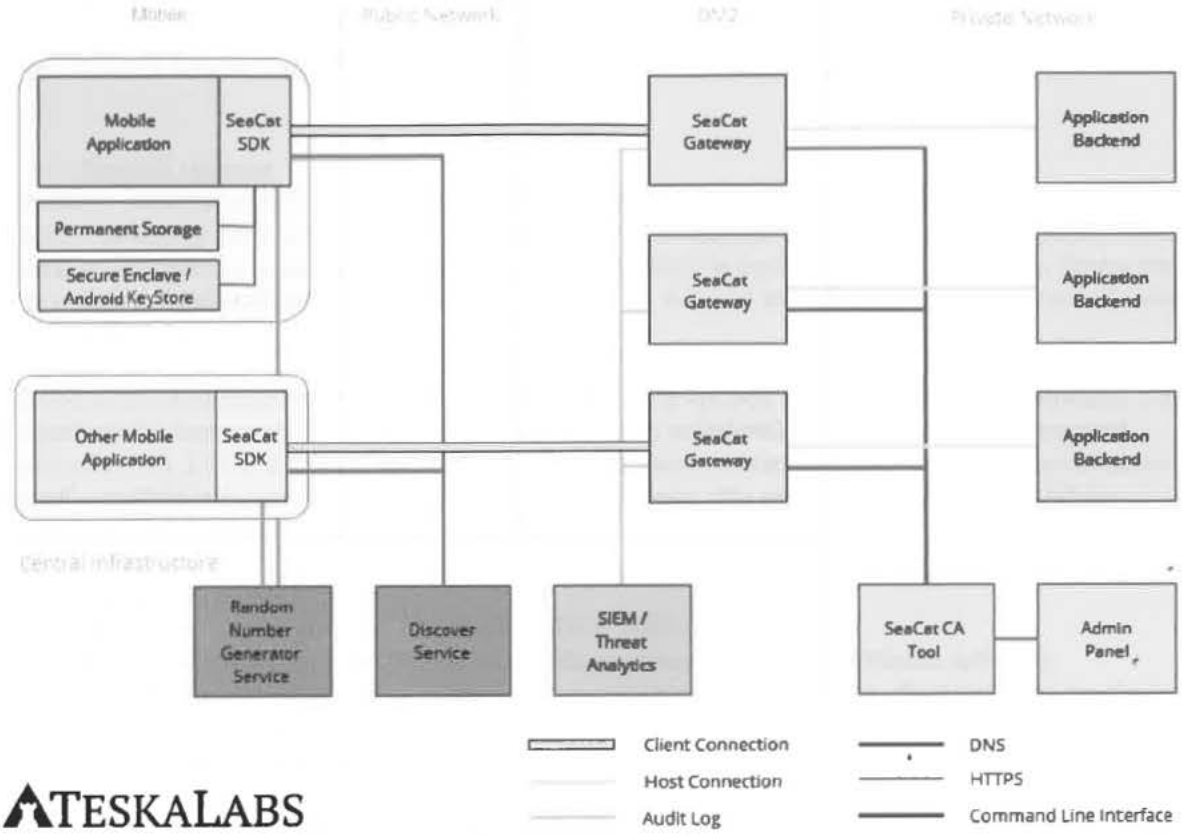
Příklad Klientského ID:
4ffe3b6cc5a5340fbac48345e7582aab1af8400e4838c9a97018809915ba1c1b9060006e6dbe4b597c612a854807e212

Uživatelská Identita a Správa Přístupů (IAM)
SeaCat identifikační proces používá Klienty jako koncové entity. Díky unikátnímu Klientskému ID má SeaCat Gateway podrobné informace o každém jednotlivém komunikujícím Klientovi, a to i v případě, když Uživatel neposkytne žádné charakteristiky nebo Aplikace žádné nevyžaduje. Identifikace Klienta je provedena ihned po začátku komunikace Aplikace se SeaCat Gateway a Backendem Aplikace. Díky tomuto postupu je schopna SeaCat Gateway zaručit:

- Identifikaci Aplikací nezávisle na čase;
- Mapování Uživatelských zvyků a pracovních postupů v rámci Aplikace;
- Statistiky o použití Aplikace;
- Automatické akce (např. zamítnutí přístupu do Backendu Aplikace pro konkrétního Uživatele) v případě detekce podezřelé aktivity;
- Vzdálený přístup ke každému Klientovi.

SeaCat identifikace je pro Aplikaci neviditelná a může fungovat spolu s jakoukoliv vestavěnou ověřovací metodou. Integrací SeaCat SDK není narušen žádný vestavěný mechanismus pro ověřování Uživatele. Vývojáři Aplikace tak mají naprostou svobodu při výběru a užití mechanismů pro ověřování Uživatelů v Aplikaci.

Identifikace Klienta v kombinaci s Ověřením Klienta na SeaCat Gateway může rozšířit či úplně nahradit dedikovaný způsob ověřování Klientů. Tato kombinace může být jediným mechanismem pro ověřování, když žádný vestavěný není použit



ATESKALABS

Obrázek 3. Architektura

FAKULTNÍ NEMOCNICE OLOMOUC

Příloha číslo 2 smlouvy

Požadavky na SW pro kybernetickou bezpečnost a ochranu dat pro mobilní aplikace ve zdravotnictví.

Zkratky:

SW Software (program)
FNOL Fakultní nemocnice Olomouc
GDPR General Data Protection Regulation - Obecné nařízení o ochraně osobních údajů

1. Předmět smlouvy

Předmětem smlouvy je splnění požadavků na poskytnutí SW licencí pro zabezpečenou komunikaci mezi mobilními zařízeními a serverem z hlediska požadavků na kybernetickou bezpečnost a ochranu dat pro mobilní aplikace ve zdravotnictví v souladu s platnou legislativou. Součástí je implementace poskytnutého SW na HW a SW prostředky objednatele a následná (servisní) podpora na dobu 12 měsíců od předání Systému k řádnému užívání v režimu 5x8.

Následně uvedené požadavky jsou základním předpokladem pro vysokou bezpečnost datové komunikace, a to jak z pohledu tzv. best-practice, tak pro naplnění regulatorních požadavků v oblasti zákona o kybernetické bezpečnosti (§ 10, § 17 až § 27), tak z pohledu evropské regulace o ochraně osobních dat - GDPR (autentizace uživatelů a zajištění přístupu k datům pouze pro oprávněné osoby, dále pak ochrana před kybernetickým útokem a neautorizovanému získání osobních dat apod.).

2. Požadavky na klientskou část

Poskytnutý SW bude na straně klienta (mobilního zařízení) zajišťovat:

- trvalou, jednoznačnou a nepřenosnou identifikaci komunikačního bodu (klienta, aplikace);
- *znalost rizikovosti prostředí, ve kterém se komunikační bod nachází (jak je cílové prostředí důvěrné);*
- silnou klientskou autentizaci pomocí nejméně dvou faktorů;
- silnou kryptografii pro vytváření unikátních přístupových kódů.

3. Požadavky na stranu poskytovatele služby (aplikačních serverů)

Poskytnutý SW bude na straně poskytovatele služby (aplikačních serverů) zajišťovat:

- podrobné logování činnosti klientů (tzv. auditní stopu);
- dostupnost poskytovaných služeb pouze pro autorizované osoby/aplikace/klienty;
- vysokou dostupnost poskytovaných služeb s rozkládáním zátěže a bez Single Point of Failure (SPoF);
- možnost integrace s dohledovými nástroji typu Log Management a Security information and event management (SIEM).

4. Požadavky na bezpečný komunikační kanál

Poskytnutý SW bude v této oblasti zajišťovat:

- využívání kryptografických funkcí a řešení kompatibilních se standardem min. FIPS 140-2;
- oddělení kritického datového toku od dalších typů datové komunikace;
- vzájemné ověření komunikujících stran pomocí mutual SSL/TLS authentication;
- naplnění přístupu least privilege (princip minimálního přístupu), security by design a security by default (architektonický návrh a koncepce tvořená s ohledem na zajištění vysoké bezpečnosti);
- nezávislost na přenášených datech a použitých komunikačních protokolech.

5. Požadavky na dvoufaktorové přihlašování

Poskytnutý SW bude umožňovat:

- využití biometrie mobilního telefonu pro dvou-faktorové přihlašování do webové aplikace (v souladu s tzv. Zero-trust policy) a
- bez nutnosti používat k přihlašování jméno a heslo.

6. Požadavky na kontinuální bezpečnostní updaty

Aby bylo zajištěno, že bezpečnost je neustále aktuální, dodavatel bude:

- monitorovat zranitelnosti, které se týkají využitých bezpečnostních komponent a v případě kritické události vydá do 3 dnů bezpečnostní update;
- zajišťovat aktualizaci komponent dle vývoje v oblasti bezpečnostních technologií pro všechny kryptografické součásti (kryptografické knihovny, šifrovací sady).

7. Požadavky na vlastnosti SW (specifika)

Vlastnost	Popis
Bezpečnost	• bezpečný přenos dat • certifikovaná a schválená kryptografie (RSA-4096, vzájemná autorizace SSL / TLS, AES-256, ...) • zabezpečené úložiště na mobilním zařízení silná úroveň zabezpečení i na staré verzi operačního systému (Android, iOS) • soukromý klíč uložený v HSM (Hardware Security Module), pokud je přístrojem podporován • automatizované rozpoznávání, které detekuje, zda mobilní zařízení obsahuje modul HSM (Hardware Security Module) • audit trail
Autentifikace a on-boarding nových uživatelů	• přizpůsobitelné ověření uživatele • bezproblémové propojení s existujícími uživatelskými účty • kompatibilní s LDAP, Active Directory • biometrické ověřování • ověření dvou faktorů (2FA) • jednoduchý on-boarding proces, plně automatizovaný pro uživatele
Správa aplikací	• fungování i na mobilních zařízeních bez nutnosti MDM či VPN • vzdálená správa aplikací (např. odmítnutí přístupu k citlivým informacím v případě ztráty zařízení) • přístup i přes internet, nejen v interní síti
Uživatelská přívětivost	• bezproblémová obsluha uživatele • určeno pro použití zaměstnanci, lékaři a / nebo pacienty • bez narušení bezpečnostní technikou • bez dopadu na produktivitu • bez dopadu na rychlost • sdílení obrazovky a technologie vzdáleného přístupu • nástroj pro sdílení obrazovky pro technickou / zákaznickou podporu
Regulations compliance	• GDPR compliant
Výkon	• vysoká škálovatelnost • vyrovnávání zatížení, vysoká dostupnost • nízká režie síťové komunikace
Nasazení	• možnost nasazení do veřejných i soukromých cloudových úložišť • možnost nasazení on-premise • aplikace mohou být distribuované prostřednictvím veřejných App stores

8. Kvalifikační požadavky

Poskytovatel má aktuálně platnou Certifikaci ISO 9001:2015 pro vývoj a poskytování softwarových produktů pro kybernetickou bezpečnost. Tuto skutečnost doložil elektronickou kopií certifikátu.

Poskytovatelem dříve zabezpečená zdravotnická mobilní aplikace prošla nezávislým přezkoumáním soudním znalcem pro obor kybernetické bezpečnosti v oboru zdravotnictví. Tuto skutečnost Zhotovitel doložil elektronickou kopií výstupu přezkoumání, které obsahuje minimálně následující (či obdobná) tvrzení:

- "Aplikace zabezpečuje uchovávané osobní údaje (...). Způsob zabezpečení odpovídá metodice „Privacy and Data Protection by Design" Evropské agentury pro informační bezpečnost a sítě (ENISA)."
- „Znalec konstatuje, že s ohledem na provedená zjištění Aplikace naplňuje požadavky GDPR. Aplikace postupuje podle zásad záměrné i standardní ochrany osobních údajů."
- "Aplikace s ohledem na požadované funkce zajišťuje vysokou bezpečnost přenášených a uchovávaných dat v několika stupních ochrany s využitím nativních funkcí operačního systému mobilního zařízení (HSM) i externí PKI dle standardu RFC 5280. Aplikace využívá jak symetrickou, tak asymetrickou kryptografii."

Poskytovatel pro zabezpečení dodá již validované řešení, které je již využíváno pro zabezpečení jiných zdravotnických aplikací, a které je v souladu s platnou legislativou.

9. Požadavky na služby

Poskytnutý SW bude poskytovat:

- možnost 24/7 dohledu nad provozem mobilní aplikace vlastními silami objednatele;
- možnost automatické i manuální reakce na bezpečnostní události vlastními silami objednatele;
- bezodkladnou aktualizaci komponent dle vývoje v oblasti bezpečnostních technologií pro všechny kryptografické součásti (kryptografické knihovny, šifrovací sady) ze strany poskytovatele;
- automatickou správu a řízení životnosti certifikátů (PKI a Certification Authority) ze strany poskytovatele;
- možnost telefonických či e-mailových konzultací k programovým funkcím u poskytovatele;
- řešení chybových stavů poskytovatelem;
- programové aktualizace (dodávka nových verzí, upgrade, update poskytovatelem) včetně parametrizace programu v součinnosti s objednatelem v případě, že ji nová aktualizace vyžaduje.

10. Požadavky na HW a systémové prostředky

SW musí být provozovatelný na HW prostředcích a databázích objednatele:

- na virtuálním serveru s min. parametry:
  - Operační systém min. Ubuntu 18.04 LTS server
  - 2 GB RAM
  - 2 CPU cores
  - 64 GB HDD
  - Network connectivity
  - Public IP

11. Požadavky na implementaci

Obsah implementace:

- součástí poskytnutí SW licence je instalace SW včetně operačního systému na virtuální server dodaný objednatelem;
- parametrizace programu v součinnosti s objednatelem;
- součástí dodávky je proškolení stanovených administrátorů objednatele. Školení provedou přímý *školitelé poskytovatele SW;*
- implementace zahrnuje dodávku SW bez časového omezení funkčnosti;
- v případě potřeby ze strany objednatele bude poskytovatel ve spolupráci s objednatelem řešit integraci na straně mobilní aplikace.

Poskytovatel implementuje SW v plné míře výše uvedených požadavků a funkcionalit nejpozději do 1 měsíce od oboustranného podpisu této smlouvy.

Příloha č. 3 – Podrobný popis služeb (SLA)

Definice pojmů

1. **Technická podpora** je činnost poskytovatele, kterou zajišťuje:
   a) Poradenství k Systému.
   b) Diagnostiku a řešení problémů při užívání Systému.
   c) Asistenci při aktualizaci Systému.
2. **Aktualizace** je služba zajišťující instalaci nových verzí **Systému** nebo jeho částí.
3. **Provozní doba služby** je doba, po kterou je stanovena její dostupnost.
4. **Legislativní změnou** se rozumí realizace úprav **Systému** k zajištění jeho souladu s legislativními požadavky, s právními předpisy orgánů státní moci.
5. **Incidentem** se rozumí nesoulad chování a skutečných vlastností **Systému** s jeho dokumentací nebo specifikací.
   Za **oprávněný incident** není možno považovat:
   a) nesprávné nebo nepovolené používání **Systému**,
   b) jakékoliv modifikace **Systému**, mimo modifikace, které poskytovatel standardně umožňuje v rámci dodávaného **Systému**,
   c) jakékoliv modifikace struktur Databáze, mimo modifikace, které poskytovatel standardně umožňuje v rámci dodávaného **Systému**
   d) propojení **Systému** nebo Databáze s jinými programy či systémy bez použití dodaných nástrojů poskytovatele,
   e) nesprávné nastavení **Systému** provedeného objednatelem nebo dle chybných pokynů objednatele,
   f) závady nebo chyby v softwaru, hardwaru, rozvodné síti, komunikačním, periferním či jiném zařízení dodaném třetími stranami
   g) opomenutí objednatele zajistit pravidelnou údržbu hardware a/nebo software třetích stan, na kterých je **Systém** funkčně závislý,
   h) provedení změn v IT infrastruktuře negativně ovlivňujících funkčnost **Systému**,
   i) používání zastaralých verzí **Systému**, které již nejsou podporovány,
   j) odstraňování ochranných prvků nebo technologií chránících integritu **Systému**.
   k) negarantované funkce **Systému**
6. **Odstraňováním incidentů** se rozumí činnost vykonávaná za účelem plného zprovoznění **Systému** a odstranění příčiny incidentu nebo problému nebo za účelem aplikace náhradního řešení (WorkAroundu) – tím se rozumí z pohledu uživatele přijatelná cesta, jak problém obejít; tato cesta může být softwarová nebo organizační.
7. **Kategorie incidentu** je klasifikace závažnosti dopadu incidentu na uživatele a jsou následující:
   a) Havárie = Systém jako celek nebo jeho funkce nejsou pro uživatele dostupné a nelze pokračovat v užívání. Celková ztráta funkcionality, kdy není k dispozici žádné dočasné řešení problému.
   b) Závada velká = Systém jako celek nebo jeho funkce jsou pro uživatele významně omezeny, problém způsobuje závažnou ztrátu funkcionalit. V používání lze pokračovat pouze omezeně, některé z klíčových funkcionalit nelze použít. Není k dispozici žádné přijatelné náhradní řešení.
   c) Závada malá - Systém jako celek nebo jeho funkce jsou pro uživatele dostupné, problém způsobuje omezení funkcionalit. V používání lze pokračovat. Není ohroženo používání služby pro uživatele.
8. **Paušál** - je předplacený objem poskytovaných služeb (vyjmenované služby, hodiny, legislativa atd.).

<u>S01 Aktualizace Systému</u>

1) Popis služby

a) Aktualizace **Systému** realizuje Upgrade/Update aplikačního vybavení včetně verzí nové generace (technologické a funkční změny **Systému**, které jsou iniciovány poskytovatelem) a vlastní instalace jsou v ceně služby.
b) V případě upgrade, který bude vyžadovat změnu systémových prostředků ICT, je poskytovatel povinen konzultovat s úsekem IT FNOL min. 3 měsíce před plánovaným nasazením takového upgrade.
c) Aktualizace provádí buď poskytovatel, nebo sám objednatel.
d) Objednatel provádí aktualizaci dle požadovaného vybraného scénáře v příslušných prostředích provozu **Systému**.
e) Bezodkladná aktualizace komponent dle vývoje v oblasti bezpečnostních technologií pro všechny kryptografické součásti (kryptografické knihovny, šifrovací sady) ze strany poskytovatele.
f) Automatická správa a řízení životnosti certifikátů (PKI a Certification Authority) ze strany poskytovatele.

2) **Dostupnost služby**
   On-line služba dostupná v režimu 7x24
3) **Úhrada služby**
   Služba je poskytovaná v rámci paušálu.

S02 Zajištění souladu Systému s legislativními požadavky

1) **Plán uvolnění verze Systému**
   Poskytovatel zašle objednateli písemně oznámení o plánu uvolnění verze Systému, ve které bude řešena plánovaná legislativní změna.
2) **Nasazení verze Systému**
   Poskytovatel uvolní otestovanou verzi včetně aktualizované dokumentace nejpozději ke dni účinnosti legislativní změny.
3) **Úhrada služby**
   Služba je poskytovaná v rámci Paušálu.

S03 Hot-line - běžné telefonické konzultace

1) **Popis služby**
   Poskytování telefonických konzultací konzultanty poskytovatele (krátké telefonické konzultace do 15 minut).
2) **Dostupnost služby**
   Konzultace dostupná v pracovní dny v čase od 8.00 hod do 16.00 hod na dispečinkovém telefonním čísle dle odstavce V.1
3) **Úhrada služby**

Služba je hrazena v rámci paušálu.

S04 Hotline – havárie a závady

1) **Popis služby**

Poskytnutí komunikačního centra dostupného s garantovanou reakcí ze strany poskytovatele. Cílem je zabezpečit jedinou evidenci zadávání servisních požadavků odpovědných zástupců objednatele, evidenci průběhu jejich řešení, stavu a schvalování/uzavírání těchto požadavků na straně poskytovatele. Služba Hotline bude realizována prostřednictvím kontaktů dle čl. V.1. této smlouvy.

A) **Iniciace incidentu objednatelem**

- Incident hlásí pověřený pracovník objednatele na Hotline poskytovatele nebo na dispečinkové kontakty dle odstavce V.1 s tím, že provede primární klasifikaci incidentu.
- Objednatel se zavazuje využít všech technických prostředků k nahlášení incidentu pro případ, kdy by byly některé technické cesty nefunkční nebo pokud by selhalo doručení z jiného důvodu.
- Pro vyloučení pochybností o určení lhůt je technický zástupce objednatele povinen nahlásit incident explicitním označením „Havárie", „Závada velká" a „Závada malá".
- V případě zadání události označením „Havárie" nebo „Závada velká" na Hotline poskytovatele emailem je nutné objednatelem ověřit přijetí hlášení poskytovatelem telefonicky na číslo dle čl. V.1. této smlouvy.
- Popis „Havárie" nebo „Závady velké" musí obsahovat důležité informace o vzniklé situaci, zejména konkrétní popis nefunkčnosti a popis provedených zásahů, které by mohly mít souvislost se vznikem havárie. Objednatel je v případě Havárie povinen stanovit Dispečera havárie, který bude za objednatele s pověřeným pracovníkem poskytovatelem průběžně řešit diagnostiku, nápravu a uvedení Systému zpět do provozuschopného stavu.
- Před nahlášením „Havárie" nebo „Závady velké" je objednatel povinen zajistit zejména:
  - vzdálený přístup poskytovatele k technickým prostředkům objednatele;
  - dostatečná přístupová práva poskytovatele k technickým prostředkům objednatele, která jsou nutná pro efektivní řešení havárie;
  - součinnost formou okamžité dostupnosti kontaktní osoby pověřené řešením Havárie ze strany objednatele.
  - veškeré informace a podklady, které jsou nutné pro diagnostiku příčin havárie a její následné řešení.

B) **Registrace incidentu poskytovatelem**

- Každý zaslaný incident je označen poskytovatelem jednoznačným identifikátorem a je neprodleně registrován ve formě požadavku na Hotline poskytovatele.
- V případě incidentu typu „Havárie" je poskytovatel povinen stanovit Dispečera havárie, který bude za poskytovatele s pověřeným pracovníkem objednatele průběžně řešit diagnostiku, nápravu a uvedení Systému zpět do provozuschopného stavu.
- V případě incidentu typu „Havárie" nebo „Závady velké" je poskytovatel povinen vést o každé operaci provedené při řešení incidentu evidenci včetně času provedení operace.
- V případě, kdy není mezi poskytovatelem a objednatelem shoda v kategorizaci požadavku (poskytovatel neshledal důvod požadavek vést jako oprávněný incident), postoupí se řešení na úroveň odpovědných osob poskytovatele a objednatele.

C) **Řešení incidentu**

- Řešení nahlášených incidentů zahájí poskytovatel v předepsané lhůtě dle typu klasifikace, v případě „Havárie" nebo „Závady velké" pokračuje v jejím řešení bez neodůvodněného přerušení až do ukončení.
- Nástupem k řešení incidentu se rozumí zahájení prací na lokalizaci a odstranění závady nebo poskytnutí přijatelného náhradního řešení.
- *Lhůta začíná poskytovateli běžet od okamžiku prokazatelného doručení oznámení o incidentu v pracovní* dobu.
- Lhůta se poskytovateli přerušuje v případech:
  - pokud došlo k překážkám v plnění, za které poskytovatel neodpovídá – o této skutečnosti informuje poskytovatel objednatele písemně;
  - při neposkytnutí požadované součinnosti objednatele poskytovateli – o této skutečnosti informuje poskytovatel objednatele písemně;
  - rozhodnutím odpovědné osoby objednatele, poskytnuté poskytovateli v písemné formě;
  - předáním písemné výzvy poskytovatelem k převzetí incidentu objednateli, pokud není vyřešení incidentu objednatelem akceptováno, pokračuje lhůta okamžikem písemného doručení zdůvodněného odmítnutí akceptace;
  - poskytovatelem zaslanou písemnou informací objednateli o uvolnění opravné verze. Po dobu do instalace opravné verze se lhůta přerušuje. Pokud po nasazení opravné verze objednatel prokáže, že opravná verze závadu neodstranila, pokračuje lhůta okamžikem písemného doručení zdůvodněného odmítnutí akceptace opravné verze.
- Pracovník objednatele je oprávněn se dohodnout s řešitelem poskytovatele na jiném termínu vyřešení incidentu, než je stanoven v této smlouvě. Tento termín pak bude zohledněn při výpočtu případných sankcí.

2) *Lhůty řešení dle kategorie Incidentů*

a) **Havárie**

Nástup na řešení:	nejpozději další pracovní den od nahlášení havárie.
Odstranění havárie:	do 48 hodin od nahlášení havárie.

b) **Závada velká**

Nástup k řešení:	do 2 pracovních dnů od nahlášení závady.
Odstranění závady:	do 4 pracovních dnů od nahlášení závady.

c) **Závada malá**

Nástup k řešení:	do 2 pracovních dnů od nahlášení závady.
Odstranění závady:	do 10 pracovních dnů od nahlášení závady.

3) Dostupnost služby

Telefonický kontakt:	dostupnost v pracovních dnech 08:00-16:00 hod
Elektronická pošta:	dostupnost 24x7 řešení v pracovních dnech 08:00-16:00 hod

Odstraňování havárie a závady velké bude probíhat bez přerušení a to i mimo pracovní dobu v režimu 24x7.

Odstraňování závady malé bude probíhat pouze v pracovní dny.

4) Úhrada služby

a) Pokud během řešení incidentu poskytovatel jednoznačně prokáže, že příčinou incidentu není vada Systému (např. v případech, kdy je příčinou porucha HW, SW třetích stran, chyba obsluhy apod.),

nebudou aplikovány sankce a prokazatelné náklady na řešení incidentu budou vyúčtovány samostatnou úhradou dle odstavce IV.6.

b) Pokud byla příčinou havárie vada Systému je služba hrazena v rámci paušálu.