# SMLOUVA O DÍLO A POSKYTNUTÍ LICENCE

Smluvní strany

**Teskalabs Ltd., odštěpný závod,**
IČO: 07957157
sídlo: Kodaňská 1441/46, Praha 10, 101 00
zastoupená Vladimírou Teskovou, director,
(dále jen „**Poskytovatel**“)

a

**Fakultní nemocnice Plzeň**
IČO: 00669806
sídlo: Edvarda Beneše 1128/13
zastoupena MUDr. Václav Šimánek, Ph.D.
(dále jen „**Klient**“)

(Klient a Poskytovatel dále společně jako „**Smluvní strany**“)

uzavřely níže uvedeného dne, měsíce a roku následující

**smlouvu o dílo a poskytnutí licence**

ve smyslu ustanovení § 2586 a násl. a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, v účinném znění (dále jen „**Smlouva**“):

## 1 PŘEDMĚT SMLOUVY

1.1 Poskytovatel se zavazuje umožnit Klientovi užití softwarového produktu SeaCat (dále jen "**Software**") a zajistit jeho implementaci, a to včetně implementace a podpory open source aplikace zScanner v souladu s nabídkou, tvořící přílohu č. 1 této Smlouvy (dále jen „**Nabídka**“). Není-li výslovně uvedeno jinak, Software zahrnuje také všechny aktualizace, opravy, nové verze

apod. Softwaru poskytnutém Poskytovatelem Klientovi.

1.2 Klient se zavazuje uhradit Poskytovateli odměnu v souladu s touto Smlouvou a Nabídkou.

## 2 LICENCE

2.1 Klient si je vědom toho, že Software je dílem chráněným autorským právem.

2.2 Poskytovatel poskytuje Klientovi právo užívat Software v rozsahu uvedeném dále (dále jen "**Licence**"). Licence se stává účinnou v okamžiku, kdy Klient řádně zaplatil odměnu uvedenou v článku 3 této Smlouvy.

2.3 Licence se uděluje na dobu dohodnutou mezi Smluvními stranami na základě specifikace v Nabídce. Licence je udělena bez jakéhokoli územního omezení (tj. celosvětově).

2.4 Licence se uděluje jako licence nevýhradní.

2.5 Klient je oprávněn na základě této Licence užít Software pouze pro účely, prostředky a v rozsahu ke kterým je Software určen. Klient není oprávněn zasahovat do Softwaru nebo měnit Software jakýmkoli způsobem, měnit jméno autora nebo Softwaru, sloučit Software s jiným dílem, zahrnout Software do kolektivního díla, nebo dokončit nedokončený Software (a to ani za pomoci třetí strany).

2.6 Počet uživatelů, kteří mohou užívat Software je 100, jedná se o licenci pro 100 koncových zařízení.

2.7 Klient není oprávněn poskytnout licenci k Softwaru třetí osobě (podlicence) bez písemného souhlasu Poskytovatele.

2.8 Klientovi je výslovně zakázáno zveřejnit či umožnit zveřejnění Softwaru, aby jej třetí osoby mohly kopírovat či jinak zneužít.

2.9 Podmínky užívání Softwaru stanovené v článku 2 této Smlouvy se obdobně použijí i na ostatní nehmotná aktiva tvořící součást Softwaru (zejména grafiku, texty apod.).

2.10 Smluvní strany vylučují veškerá volná užití či zákonné licence ve prospěch Klienta, které lze dohodou Smluvních stran vyloučit.

2.11 Klient je odpovědný za provoz Softwaru v souladu se všemi zákony a předpisy platnými a účinnými na území, ve kterém Klient provozuje Software, a také v souladu s jinými veřejnoprávními rozhodnutími a předpisy týkajícími se provozu Softwaru na takovém území. Klient je výhradně odpovědný za to, že provozování Softwaru Klientem (nebo třetí osobou, které Klient udělil

oprávnění užívat Software) je založeno na legitimním oprávnění (zejména je Klient odpovědný za zajištění všech potřebných licencí) po celou dobu používání Softwaru.

## 3 ODMĚNA

3.1 Klient se zavazuje zaplatit Poskytovateli za Licenci odměnu ve výši a za podmínek stanovených v Nabídce (dále jen "**Odměna**").

3.2 Odměna bude uhrazena na základě vystaveného daňového dokladu (faktury) Poskytovatelem. Splatnost faktury je stanovena na 30 dní od data jejího vystavení. Přílohou daňového dokladu je předávací protokol.

3.3 Platby na základě této Smlouvy budou provedeny Klientem převodem na bankovní účet Poskytovatele. Cena se považuje za zaplacenou dnem, kdy bude příslušná částka odpovídající ceně připsána na účet Poskytovatele.

3.4 V případě prodlení Klienta s placením Ceny je Poskytovatel oprávněn po Klientovi požadovat úroky z prodlení ve výši 0,05 % denně za každý, byť započatý, den prodlení, a to na základě písemné výzvy doručené Klientovi k jejímu uhrazení. Právo Poskytovatele na náhradu škody tímto není dotčeno.

## 4 PŘÍSTUP K SOFTWARU

4.1 Software je poskytován dle podmínek Nabídky.

4.2 Poskytovatel poskytne Klientovi přístup k nové verzi Softwaru. Poskytovatel je rovněž oprávněn označit novou verzi Softwaru za povinnou aktualizaci. V takovém případě je Klient povinen aktualizovat Software a nahradit původní verzi novou verzí Softwaru ve svých zařízeních ve lhůtě stanovené písemně Poskytovatelem. Lhůta pro standardní aktualizaci činní 6 měsíců, v případě urgentních bezpečnostních aktualizace pak lhůta záleží na jejich kritičnosti. Podmínky užívání nové verze Softwaru se řídí článkem 3 této Smlouvy.

## 5 DOKUMENTACE

5.1 Software může obsahovat softwarovou dokumentaci v jakémkoli formátu, zejména standardní příručky, technickou dokumentaci (datové modely a diagramy), analýzy nebo jiné specifikace funkcí Softwaru a jejich úplných nebo částečných kopií (dále jen "**Dokumentace**"). Podmínky použití Softwaru se řídí článkem 2 této Smlouvy.

## 6 OCHRANA PRÁV

6.1 Klient neodstraní žádné označení vlastnictví, autorská práva, ochranné známky nebo jiné označení ze Softwaru a/nebo Dokumentace. Klient nesmí usilovat o ochranu názvu Softwaru, používat název Softwaru jako ochrannou známku, ani jinak uplatňovat nároky z takového názvu.

6.2 Klient je povinen bez zbytečného odkladu informovat Poskytovatele o jakémkoli neoprávněném užití duševního vlastnictví, které bylo Klientovi zpřístupněno za podmínek uvedených v této Smlouvě, jakmile se o těchto okolnostech dozví. Klient souhlasí s tím, že Poskytovateli poskytne veškerou požadovanou podporu a spolupráci při vyšetřování a ochraně těchto práv duševního vlastnictví Poskytovatele.

6.3 Poskytovatel může na základě písemného oznámení doručeného Klientovi pozastavit Klientova práva a povinnosti vyplývajících z této Smlouvy (např. pozastavení práva k užití Softwaru) v případě, že:

a) Klient porušil povinnost stanovenou Smlouvou a neodstraní takové porušení v přiměřené lhůtě stanovené Poskytovatelem, ne kratší než 10 (deset) dnů,

b) Klient nebo třetí strana oprávněná Klientem užívat Software poruší práva duševního vlastnictví Poskytovatele,

c) nastanou závažné technické problémy s provozem softwaru (zejména závažné chyby v provozu Softwaru nebo nevyřešená bezpečnostní rizika)

d) existuje podezření, že Klient nebo třetí strany jednající na základě oprávnění Klienta užívají Software v rozporu s právními předpisy nebo Smlouvou, nebo

e) existují další závažné skutečnosti, způsobilé ovlivnit plnění Smlouvy nebo plnění Poskytovatele.

## 7 VADY A ŠKODY

7.1 Odpovědnost za vady a úrovni služeb (SLA) je specifikována dle Nabídky.

7.2 Poskytovatel neodpovídá za žádné škody, ledaže jde o nároky, kterých se Klient nemůže vzdát (např. úmyslné způsobení škody Poskytovatelem, škoda způsobená hrubou nedbalostí Poskytovatele).

## 8 DOBA BĚHU SMLOUVY

8.1 Poskytovatel začne poskytovat licenci a plnit předmět smlouvy ve lhůtě do 15 pracovních dnů od doručené výzvy Klienta k plnění. Délka trvání smlouvy je v souladu s nabídkou 3 měsíce od počátku plnění smlouvy. Po třech měsících se smlouva automaticky ukončuje.

8.2 Každá ze Smluvních stran je oprávněna od této Smlouvy bez dalšího odstoupit v případě vstupu do likvidace či pravomocného prohlášení konkurzu na majetek druhé Smluvní strany.

8.3 Každá Smluvní strana je oprávněna odstoupit od této Smlouvy v případě závažného porušení této Smlouvy druhou Smluvní stranou za předpokladu, že druhá Smluvní strana byla písemně informována o tomto porušení a byla ji poskytnuta přiměřená doba, nejméně deseti (10) pracovních dní k dodatečnému plnění.

8.4 Poskytovatel je oprávněn odstoupit od této Smlouvy

a) v případě prodlení Klienta se zaplacením faktury delším než jeden (1) měsíc od její splatnosti, za předpokladu, že byl Klient písemně informován o tomto prodlení a byla mu poskytnuta přiměřená lhůta, ne kratší než sedm (7) pracovních dní, k dodatečnému splnění,

b) v případě, že Klient trvá na poskytnutí výkonu podle zřejmě nevhodného příkazu nebo s použitím zřejmě nevhodné věci, ačkoli byl na tuto nevhodnost již dříve Poskytovatelem upozorněn.

8.5 Smluvní strany sjednávají, že v případě odstoupení od této Smlouvy, Poskytovatel nebude vracet doposud poskytnuté platby za poskytnutí Softwaru (nebo jeho části).

8.6 Po ukončení platnosti Smlouvy musí Klient vymazat všechny kopie Softwaru, které měl k dispozici, a ukončit veškeré užívání Softwaru.

## 9 OCHRANA INFORMACÍ

9.1 Smluvní strany prohlašují, že veškeré důvěrné podklady a důvěrné informace, které od sebe navzájem získají, budou použity výhradně pro potřebu přípravy a realizace Smlouvy. Tyto důvěrné informace nebudou poskytnuty v žádné formě třetím osobám ani nebudou použity smluvními stranami k žádnému dalšímu účelu, pokud nedojde k písemné dohodě, která by nakládání s informacemi tohoto charakteru upravila způsobem odlišným. Smluvní strany se zavazují po zde sjednanou dobu ochraňovat důvěrné informace obvyklým způsobem, přinejmenším však, jako by se jednalo o důvěrné informace jejich vlastní.

9.2 Za důvěrné podklady a důvěrné informace podle předchozího odstavce se bez ohledu na for-mu jejich zachycení považují veškeré podklady a informace, které byly některou ze smluvních stran označeny jako důvěrné, a které se týkají předmětu Smlouvy jejího plnění anebo podkladů a informací, které se týkají přímo některé ze smluvních stran (zejména obchodní tajemství, informace o činnosti, struktuře, hospodářských výsledcích, know-how, připravovaných projektech, technické specifikace a řešení apod.).

9.3 Smluvní strany se dále zavazují považovat za důvěrné podle tohoto ustanovení taktéž veškeré neveřejné informace, mající povahu obchodního tajemství, vzájemně získané ústním podáním některé ze smluvních stran.

9.4 Smluvní strany se dále zavazují považovat za důvěrné své know-how zahrnující dokumenty a postupy při realizaci předmětu Smlouvy. Zavazují se zachovávat mlčenlivost ohledně know-how, jakož i veškerých informací, které se dozví v průběhu plnění této Smlouvy (dále jen „Důvěrné infor-mace“), nezpřístupnit Důvěrné informace jakékoli třetí osobě, a nevyužívat Důvěrné informace ani pro svoji potřebu, s výjimkou plnění povinností vyplývajících z této Smlouvy. Zavazují se zajistit, aby povinnost mlčenlivosti dle tohoto článku plnili i jeho zaměstnanci, jakož i další osoby, které s nimi spolupracují na základě uzavřených smluv. Povinnost mlčenlivosti dle tohoto článku trvá v plném rozsahu i po ukončení této Smlouvy.

9.5 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opomenutím strana přijímající dle Smlouvy důvěrnou informaci,
- měla přijímající strana legálně k dispozici před uzavřením Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo informacemi třetí strany, bez ohledu na to zda obsahuje důvěrné informace či nikoli,
- po podpisu této dohody poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem

9.6 Smluvní strany se dále pro případ každého jednotlivého prokázaného porušení povinnosti ochrany důvěrných informací dle Smlouvy dohodly na smluvní pokutě ve výši 100.000,- Kč. Smluvní pokuta je splatná na základě faktury zaslané poškozenou smluvní stranou druhé smluvní straně. Jejím zaplacením není dotčen nárok poškozené smluvní strany na náhradu škody, jež by jí takovýmto

porušením smluvní povinnosti vznikla.

## 10 ZÁVĚREČNÁ USTANOVENÍ

10.1 Tato Smlouva nabývá platnosti a účinnosti uveřejněním v registru smluv.

10.2 Tato Smlouva a právní poměry z ní vyplývající se řídí právním řádem České republiky.

10.3 Pokud je kterékoli ustanovení této Smlouvy nebo její část neplatné či nevykonatelné nebo se takovým v budoucnu stane, nebude mít tato neplatnost či nevynutitelnost vliv na platnosti či vynutitelnost ostatních ustanovení této Smlouvy nebo jejich částí, pokud nevyplývá přímo z obsahu této Smlouvy, že toto ustanovení nebo jeho část nelze oddělit od dalšího obsahu. V případě uvedeném v ustanovení předchozího odstavce tohoto článku se Smluvní strany zavazují neúčinné či neplatné ustanovení nahradit novým ustanovením, které je svým účelem a hospodářským významem co nejbližší ustanovení, jež má být nahrazeno.

10.4 Změny a doplnění této Smlouvy je možné provádět pouze písemnými, vzestupně číslovanými, oběma stranami podepsanými dodatky.

10.5 Žádná ze Smluvních stran nemá právo postoupit na třetí osobu tuto Smlouvu či její část bez předchozího souhlasu druhé Smluvní strany.¨

10.6 Žádná ze smluvních stran není oprávněna postoupit jakoukoliv svoji pohledávku vyplývající z této smlouvy bez předchozího souhlasu druhé smluvní strany.

10.7 Tato Smlouva nahrazuje veškeré předchozí písemné i ústní dohody a ujednání vztahující se k předmětu Smlouvy.

10.8 Tato Smlouva je vyhotovena ve dvou vyhotoveních, z nichž každá Smluvní strana obdrží po jednom.

10.9 Smluvní strany si Smlouvu přečetly, souhlasí s celým jejím obsahem a na důkaz toho připojují své podpisy.

10.10 Každá strana má právo vypovědět smlouvu ve lhůtě 1 měsíc. Tato lhůta počíná běžet prvního dne měsíce následujícího po doručení písemné výpovědi druhé straně. V případě ukončení smlouvy výpovědí bude poskytovatelem vrácena alikvotní zaplacená částka za dobu nevyužití předmětu smlouvy.

_____

**Teskalabs Ltd,**
Zastoupená
Vladimírou Teskovou, director

_____

**Fakultní nemocnice Plzeň**
MUDr. Václav Šimánek, Ph.D
ředitel


**Příloha 1. ke smlouvě:**

**TeskaLabs FN Plzeň 200128-Licenční smlouva_v01**

# Obsah

# zScanner

zScanner je mobilní aplikace pro klinickou a lékařskou fotodokumentaci. zScanner umožňuje lékařům pořizovat snímky zdravotních záznamů pacientů a zranění pacientů, a nahrávat je do nemocničního informačního systému.

## Bezpečnost a ochrana dat v aplikaci zScanner

Tato část obsahuje specifické informace týkající se ochrany dat, vyžádané FN Plzeň.

### Identifikace pacienta při odeslání fotky

Rodné číslo, či kód pacienta, je zadán pouze při výběru pacienta. Dále aplikace pracuje pouze s databázovým identifikátorem Medicalc. Při odeslání fotky je s ní odeslán pouze tento identifikátor.

### Přístup dodavatele k datům na serveru

Na serverové straně bude implementována pouze jedna softwarová komponenta - SeaCat Gateway, která žádná data neukládá, plní pouze funkci tzv. proxy/aplikačního firewall. Detailní popis komponenty SeaCat Gateway je k dispozici v sekci Technologie SeaCat níže.

### Možnost nahrání fotografie uložené v paměti telefonu

Varianta zScanner upravená dle požadavků FN Plzeň **neobsahuje** možnost nahrát fotografie uložené v galerii telefonu.

Fotografie dále není možné ukládat, a jsou přítomny v paměti pouze po dobu procesu uploadu. Pokud si provozovatel přeje, je možné pořizovat fotky jen v online režimu.

### Ověření uživatelského jména a hesla

Uživatelské jméno a heslo se odešle do Medicalc (přes šifrované, vzájemně authentikované TLS spojení), v aplikaci zScannner k ověření nedochází.

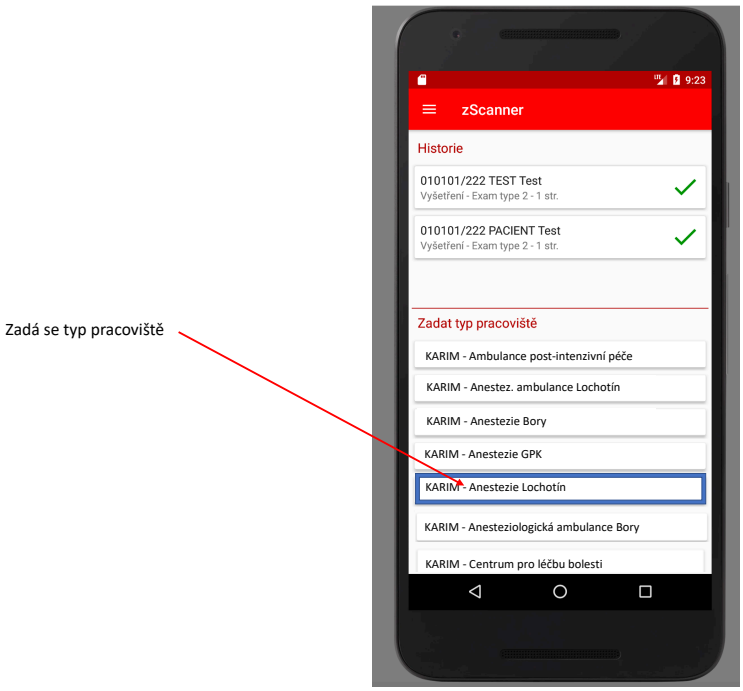
MediCalc za správný login vydá access_token, který se používá (spolu s privátním klíčem uloženým v HSM telefonu) k autentikaci volání API MediCalcu.

## Specifikace funkcionalit

| **Funkcionalita** | **Popis** |
|---|---|
| Přihlášení | zScanner umožňuje přihlášení pomocí jména a hesla, nebo pomocí biometrické autentizace, jako je například otisk prstu.<br>Uživatelské jméno a heslo je odesláno do Medicalc (přes šifrované, vzájemně authentikované TLS spojení), kde dojde k ověření. V aplikaci zScannner k ověření nedochází.<br>MediCalc za správný login vydá access_token, který se používá (spolu s privátním klíčem uloženým v HSM telefonu) k autentikaci volání API MediCalcu. |
| Výběr pracoviště | Z Medicalc je načten seznam pracovišť, ke kterým má daný uživatel přístup. Z těchto pracovišť si uživatel vybere. |

| | |
|---|---|
| Výběr pacienta | Identita pacienta je zadána buď pomocí rodného čísla, nebo pomocí naskenování čárového kódu. |
| Fotografování | zScanner umožňuje vytvořit více fotografií v rámci jedné události, a ke každé fotografii přidat popisek.<br>Po každém vytvoření fotografie se uživateli zobrazí náhled, aby zkontroloval kvalitu pořízené fotografie. V případě, že uživatel není spokojen s fotografií má možnost fotografovat znovu. |
| Zadání typu události | Po dokončení fotografování zScanner zobrazí typy událostí, které jsou relevantní danému oddělení. |
| Zadání specifikace události | V případě, že se událost má nejen typ, ale i specifikaci, zScanner zobrazí typy specifikací, které jsou relevantní dané události. |

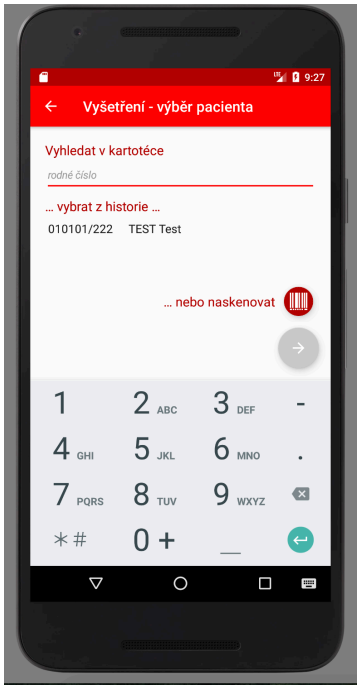
Funkcionality jsou ilustrovány na níže přiložených screenshotech z aplikace.



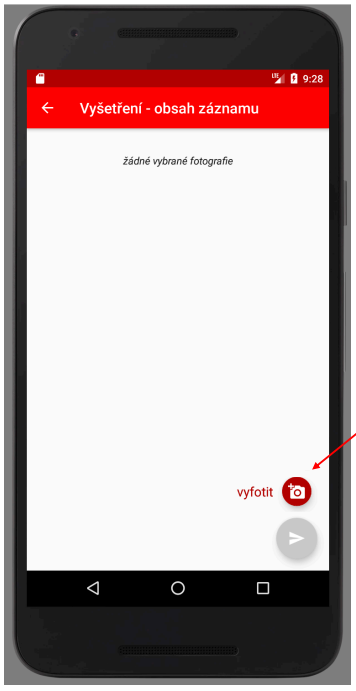

Obrázek 1: Výběr pracoviště

Zadá se identita pacienta, buď pomocí rodného čísla, nebo pomocí načtení čárového kódu.

Po zadání rodného čísla či čárového kódu se zobrazí jméno pacienta pro ověření identity.

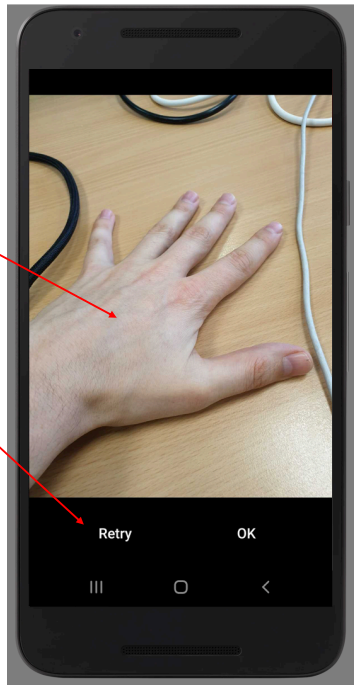



Obrázek 2: Zadání identity pacienta

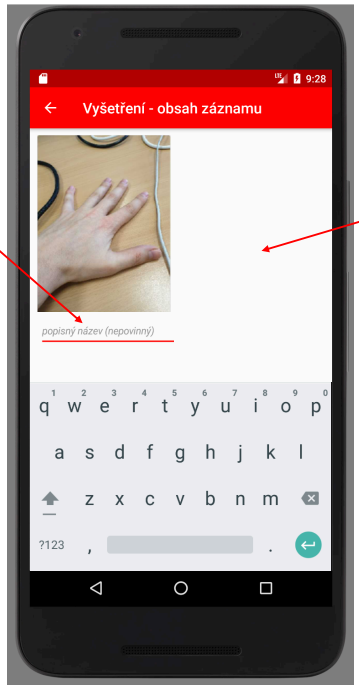



Kliknout pro vytvoření fotografie

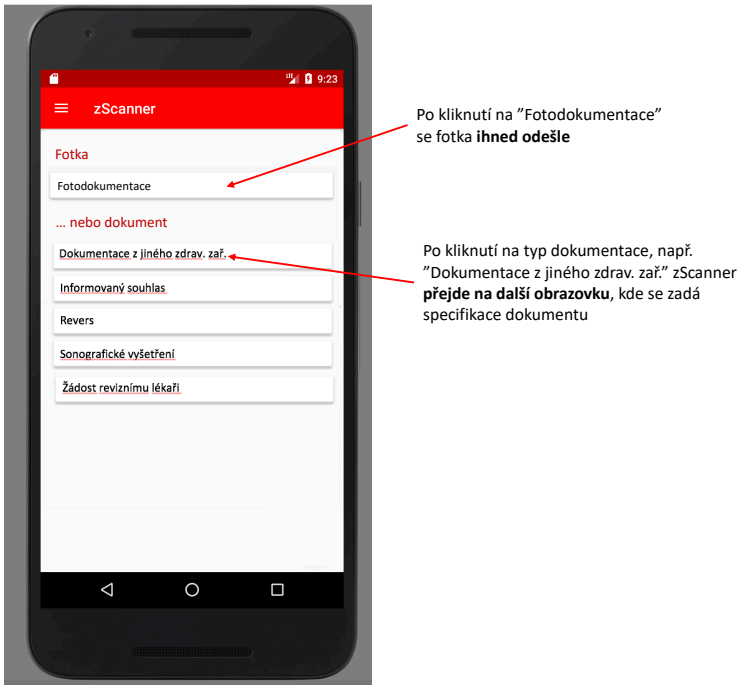
Obrázek 3: Vytvořit fotografii



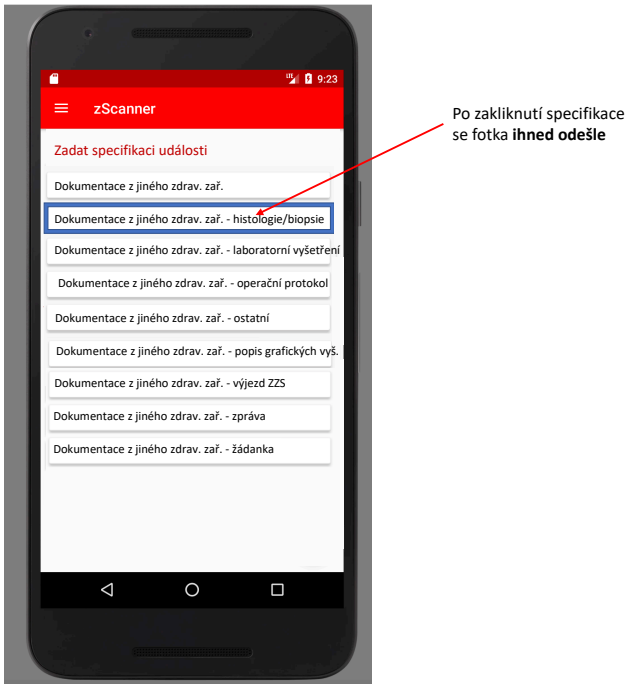

Obrázek 4: Tvorba fotografie




Obrázek 5: Popisek fotografie

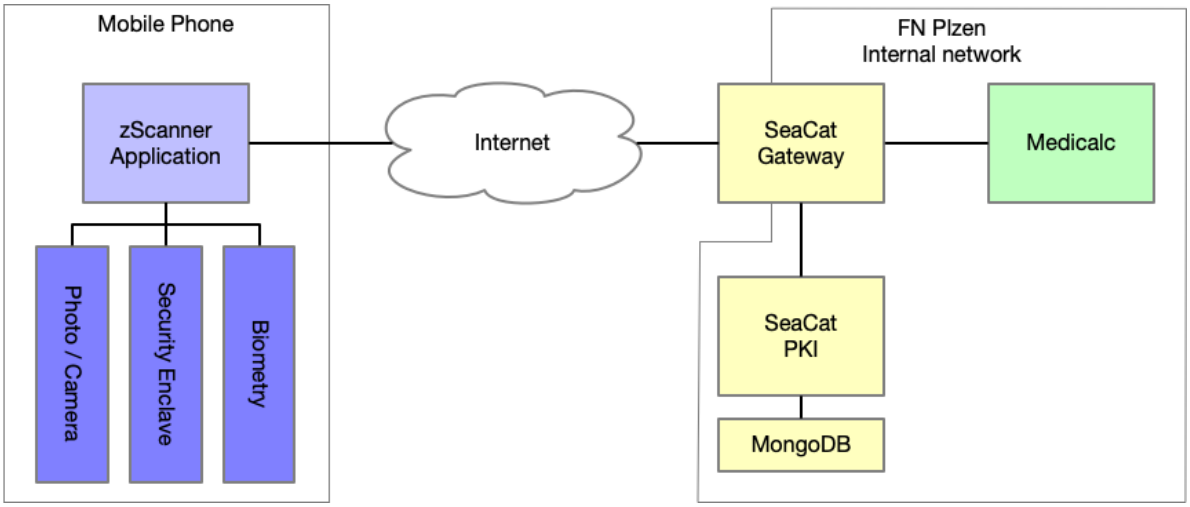



Obrázek 6: Zadání typu fotografie




Obrázek 7: Zadání podtypu fotografie

## Architektura aplikace




## Specifikace

| **Obecné** | |
|---|---|
| Podporované platformy OS | Android<br>iOS |
| Podporované formáty fotografií | JPG, PDF |
| Zdrojové kódy Android | https://github.com/ikem-cz/zscanner-android |
| Zdrojové kódy iOS | https://github.com/ikem-cz/zScanner-iOS |
| **API** | |
| Typ API | HTTPS / REST |
| **Jednotlivá volání** | |
| /v3.1/departments | Získá seznam oddělení, přiřazených danému uživateli. |
| /v3.1/documenttypes | Získá seznam typů událostí a specifikací událostí, přiřazených danému oddělení |
| /v3.1/folders/search | Vyhledá pacienta na základě rodného čísla. |
| /v3.1/folders/decode | Spáruje rodné číslo s internal ID Medicalc |
| /v3.1/documents/summary | Nahraje popis dokumentu, který bude nahrán. |
| /v3.1/documents/page | Nahraje jednotlivé stránky dokumentu |
| Detailní popis volání | https://zscannermedicalc.docs.apiary.io/#reference/0 |

# Technologie SeaCat

SeaCat provides the strong security for applications used on different types of endpoint devices (e.g. mobile phones, smart IoT/M2M devices, handhelds, tablets, computers). It provides secure endpoint connectivity over public networks and protects application backends from cyber threats. As such SeaCat-based solutions reduce the attack surface of these environments and devices.

SeaCat is designed for enterprise environments to secure large-scale B2C (business-to-consumer), B2B (business-to-business) and B2E (business-to-employee) applications and large-scale IoT applications.

SeaCat consists of following main components:

- SeaCat SDK
- SeaCat Gateway

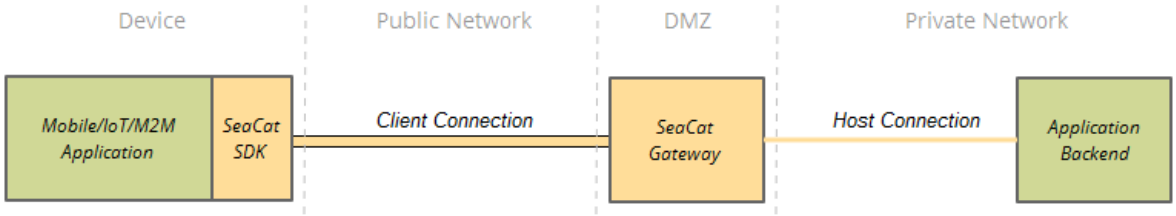



Figure 2.1: High-level diagram of SeaCat [7]

Note: in following texts terms user and client are used with following the meaning. The client is an application containing SeaCat SDK; the user is a user of the application.

## SeaCat SDK

SeaCat SDK is a software library, which is designed to be integrated into the protected mobile, IoT or M2M Application. SeaCat SDK secures the client connection between the application and its respective backends.

SeaCat SDK provides:

- Unique client identification due to its integrated certificate authority and PKI [up 4] support;
- FIPS 140-2 compliant encryption support on all devices, independent of operating system capabilities (e.g. mobiles with the old cryptographic library, IoT/M2M devices) thanks to OpenSSL cryptographic module integration;
- Endpoint data security (e.g. key pairs, application data) owing to local secure permanent storage;
- Secure data transport between an application and a SeaCat Gateway over unsecured public networks;
- Secure client onboarding sequence.

## SeaCat Gateway

SeaCat Gateway is a server software that acts as a security gate between a public network and a private network and to orchestrate clients. It is typically deployed in the demilitarized zone [up 1] as a cloud or on-premise appliance. It forwards valid and authorized client requests to respective application backends via HTTP, MQTT [up 2] and other protocols. It is built using POSIX standard and runs on various Linux and Apple Mac OS X operating systems.

SeaCat Gateway provides:

- Protection from cyber-attacks (e.g. volumetric DDoS [up 3], robots probing, ports scanning) thanks to isolating application backends from public networks;
- Protection from unauthorized access to application backend due to inbound client connections authentication;
- High availability of application backends thanks to the redundancy of all used components;
- Load resistance by traffic load-balancing between Clients and SeaCat Gateways;
- High data throughput thanks to easy scalability (e.g. hundreds of thousands of concurrent client connections);
- Support for disaster recovery plans and requirements;
- Access rights management;
- Certificate authority;
- Audit log to connect to the security information and event management (SIEM) or network security center;
- Application Programming Interface (API).

## Client connection

Client connection is a network link similar to Secure Socket Layer Virtual Private Network (SSL VPN) between a SeaCat Gateway and a SeaCat SDK (typically in a public network). It ensures confidentiality, integrity, authenticity and non-repudiation of transferred data.

Client connection provides:

- Protection from interception or other data traffic manipulation by SSL mutual authentication;
- Increase in communication speed due to reduced http protocol overhead and client connection persistency;
- Server pushing ability thanks to client connection persistency and MQTT support;
- High security thanks to TLS 1.2, FIPS 140-2 compliant encryption.
- SeaCat Gateway ensures that each client is connected to one application backend for the whole session. The pinning is active until the client connection timed out.

## Host connection

Host connection is a network link between a SeaCat Gateway and an application backend (typically in a private network).

Host connection provides:

- Support for HTTP, HTTPS and MQTT protocols;
- Sticky session by virtue of pinning to a particular SeaCat Gateway and an application backend instance;
- Load resistance by traffic load balancing between SeaCat Gateways and application hosts.

## Diagram of secure communication

Common communication flow between application and application backend look as on the Figure 2.2 (for HTTP traffic as an
example):

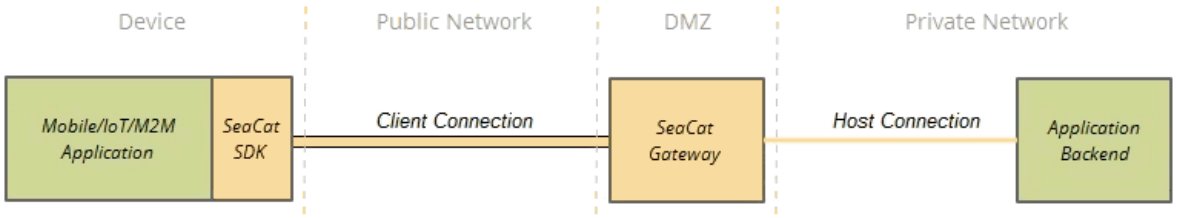



Figure 2.2: Communication flow between application and application backend [7]

1. Application generates an HTTP request
2. SeaCat SDK intercepts the HTTP request
3. SeaCat SDK pass the HTTP request to SeaCat Gateway via client connection
4. SeaCat Gateway verify client certificate and authorize client to communicate with application backend
5. SeaCat Gateway takes the HTTP request and pass it to application backend
6. Reply from application backend is similar but in reverse order
7. Client connection is established until client inactivity timed out

# Identity Management

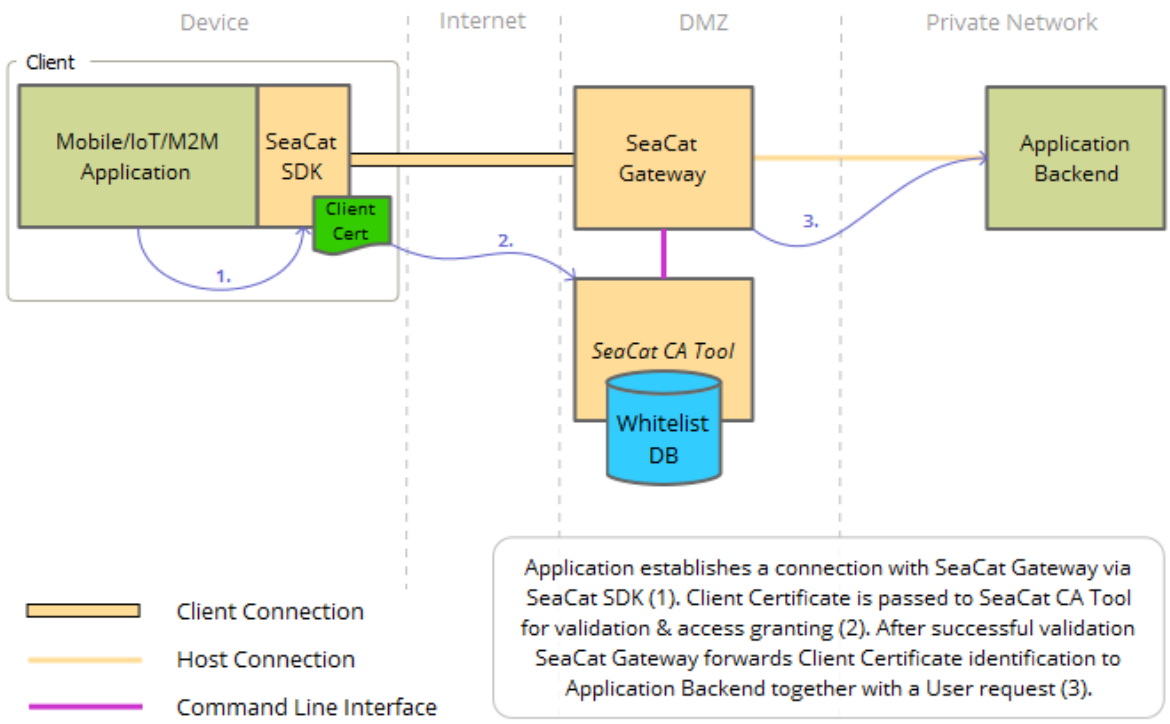
A unique identity of each Application instance (e.g. mobile Application installed on the particular device) is based on the private and public keys. This key pair is generated locally on the device by SeaCat SDK during a first launch of the Application and it is bound to the particular Application instance. We call it Client. After Client is authorized on SeaCat Gateway, Client receives Client Certificate signed by Certificate Authority from SeaCat Gateway.

For more details regarding Client onboarding procedure go to Workflows chapter. Certification authority functions and deployment scenarios are described in Certificate Authority chapter.

The protection of Client private key is up to SeaCat SDK. If operating system version has Secure Enclave or Android Keystore integrated Client private key can be protected by these technologies. Optionally, additional User protection of Client private key is available by use of advanced cryptographic techniques (e.g. Password/PIN protection, NFC HW tokens, etc.)

For more details about private key protection go to Key Management chapter.

SeaCat Gateway checks Client identity during establishing of Client Connection. SeaCat Gateway mediates access between Client and respective Application Backend. It refuses or grants access to Application Backend based on a whitelist of the Client Certificates. Admin Panel manages Client authorization (presence of Client Certificate in the whitelist).




## Client ID

Client identification is an SHA-384 hash of Client public key called Client ID. Client ID provides a globally unique identification of a Client. Client ID is represented by 96 characters long hexadecimal string (allowed characters are a-f0-9). It is used by SeaCat for all internal processes. Client ID abstracts from all Client Certificate fields.

Client ID example:
4ffe3b6cc5a5340fbac48345e7582aab1af8400e4838c9a97018809915ba1c1b9060006e6dbe4b597c612a854807e212

## User Identity and Access Management (IAM)

SeaCat identification process uses Clients as an end entity. Thanks to unique Client ID, SeaCat Gateway has detailed information of every single communicating Client even if the User provide no credential or Application requires no credential. Client identification is made immediately after Application starts communication with the SeaCat Gateway and Application Backend. Thanks to this approach, SeaCat Gateway provides the following:

- Unique time-independent Application identification;
- Application User behavior and workflows trace;
- Statistics of Application usage;

- Automatic actions (e.g. refuse access to Application Backend for particular User) in a case of suspicious activity is detected;
- Remote access to every Client.

SeaCat identification is invisible to Application and it can coexist with any built-in authentication method. By SeaCat SDK integration existed built-in User authentication mechanism is not altered. Application developers have absolute freedom regarding built-in User authentication mechanism inside the Application.

Client identification in cooperation with Client authentication on SeaCat Gateway can extend or replace built-in User authentication mechanism. It can be the only User authentication mechanism if Application has no built-in authentication implemented.

## SeaCat Identification Integration

Integration of SeaCat identification to Application differs for applications with built-in authentication and applications without it.

### Application with Built-in Authentication

Integration of SeaCat identification to Application enhances the information about Client/User ID provided by SeaCat Gateway. For single-User Application (e.g. Application for the personalized digital access card, Instant messaging Application linked with phone number), Client identity is directly linked to User. Every Client than represents the particular User which results in the following functionalities:

- Client is extended by User identity in the access management;
- A list of User devices is created.

For multi-User Application it results in the following functionalities:

- A list of User devices is created.
- A list of devices shared by more than one User is created.

To ensure the functionalities, SeaCat Gateway needs to know which User works with Application. Pair User with the Client can be done by:

- SeaCat SDK
- SeaCat Gateway
- integration with internal systems (e.g. identity management) via an API

SeaCat Gateway maintains the pair list regardless Client/User ID pair origin. Description of Client/User ID pair processes regarding origin follows:

### SeaCat SDK

For a User/Client ID pair, any unique User identifier (e.g. User name, some ID, etc.) need to be passed from Application to SeaCat SDK. SeaCat SDK is responsible for manipulating with Client Certificate Signing Request, so after Application passes the unique User identifier to SeaCat SDK, SeaCat SDK added User identifier to Client Certificate Signing Request and send it to SeaCat

Gateway. Dedicated Client Certificate field reserved for TeskaLabs purposes is used for that, so all other fields are available for developers for any purpose.

### SeaCat Gateway

SeaCat Gateway can be used as an origin of User/Client ID pair only if Application requests contains unique User identifier. Than, User identification is gathered by SeaCat Gateway from Application request syntax. Client ID is available to SeaCat Gateway naturally. User/Client ID pair is done by a combination of Client ID and unique identifier from the Application request.

### Internal Systems Integration

SeaCat Gateway can forward Client ID string to Application Backend for future processing in XFF header. Afterwards, Application Backend has knowledge about both User and Client ID for the future pairing. User/Client ID pairs are available to SeaCat Gateway via Application Backend API or by any other API which has available User/_Client_ID pairs (e.g. Identity management).

### Application without Built-in Authentication

For Application without built-in authentication, Client ID represents one and only identification created by SeaCat SDK automatically with all the benefits described in User Identity and Access Management paragraph.

## Services

Additional services besides the main functionalities are Random Number Generator Service, Discover Service and Admin Panel. Random Number Generator Service is used when there is not enough entropy to generate a cryptographic tools such as a private key (e.g. on virtual machines). Admin panel is a management tool which enables operators of a mobile application to have control over them. Discover Service is a DNS-based service which provides mobile apps equipped with SeaCat client with information to which SeaCat Gateway they should connect.

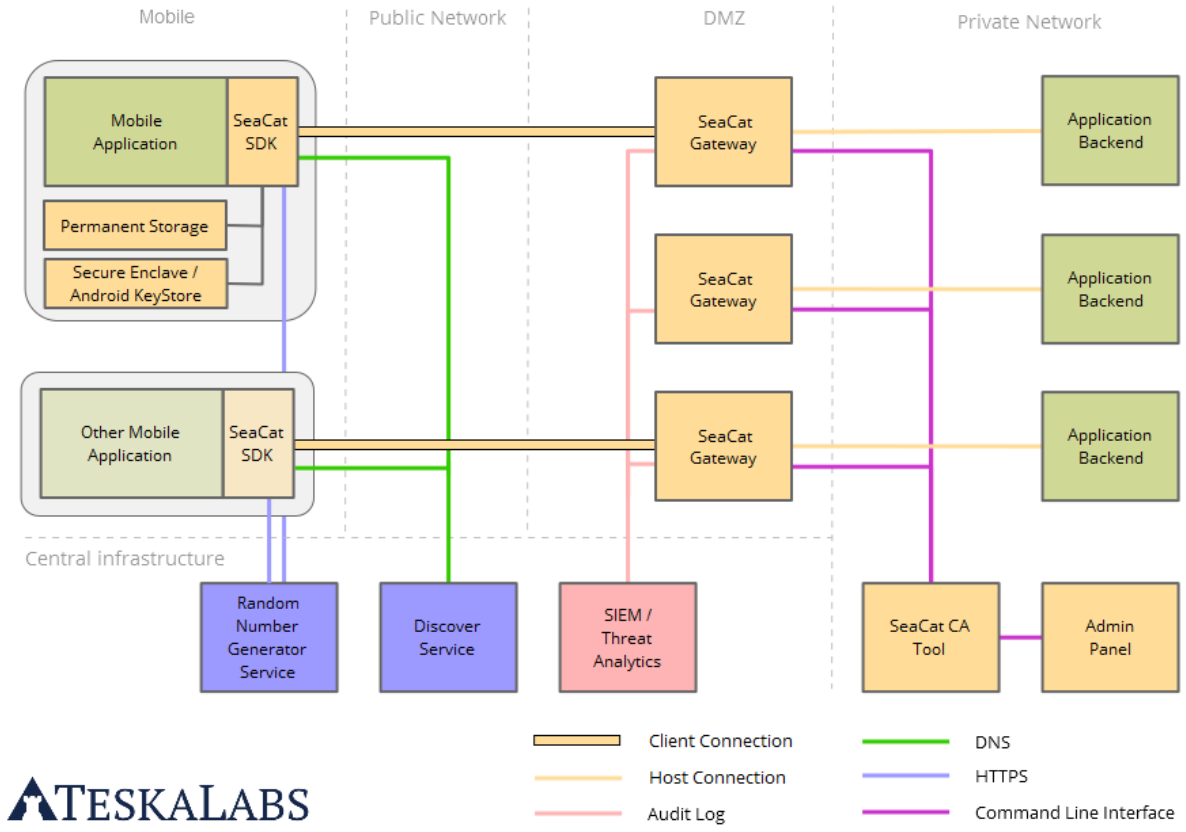



Figure 2.5: SeaCat components and interactions for SeaCat Mobile Secure Gateway [7]

# Cena

***V případě zakoupení následné roční licence, bude její cena snížena o 40 000 Kč (sleva se týká prvního roku používání)**

| **Pilotní nasazení aplikace zScanner zabezpečené platformou SeaCat** | | |
|---|---|---|
| Produkt | Typ platby | Cena |
| Pilotní nasazení aplikace zScanner zabezpečené SeaCat<br>▪ Setkání s uživateli pro optimalizaci aplikace pro využití ve FN Plzeň<br>▪ Implementace pro platformu Android<br>▪ Implementace pro platformu iOS<br>▪ Integrace se systémem Medicalc<br>▪ Licence SeaCat pro pilotní nasazení na tři měsíce pro 100 uživatelů | Jednorázově | 79 990 Kč* |

| | | |
|---|---|---|
| ▪ Basic support, emailová podpora 5/8 v české pracovní době (od 8:00 do 16:00) | | |

*V případě zakoupení následné roční licence, bude její cena snížena o 40 000 Kč (sleva se týká prvního roku používání)

Uvedené ceny jsou bez DPH.

Platnost nabídky: 10. 7. 2020