Produktové informace

zScanner zabezpečený platformou SeaCat

Obsah

Manažerské shrnutí

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. zScanner je open source aplikace vyvinutá a používaná Institutem Klinické a Experimentální Medicíny (IKEM), významnou českou nemocnicí, a největším centrem klinické a experimentální medicíny v České republice.

SeaCat je platforma kybernetické bezpečnosti pro mobilní zdravotnické aplikace vyvinutá TeskaLabs. SeaCat umožňuje firmám provozovat aplikace spolehlivým, škálovatelným a bezpečným způsobem. Poskytuje cenné informace o provozu aplikace v kombinaci se silnou ochranou dat. SeaCat umožňuje rozpoznat, vyřešit či zmírnit všechny druhy bezpečnostních a provozních incidentů dříve, než ohrozí provozovatele aplikace či koncové uživatele.

TeskaLabs nabízí aplikaci zScanner, zabezpečenou platformou SeaCat jako out-of-box produkt. TeskaLabs také nabízí profesionální služby zajišťující implementaci a podporu aplikace.

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.

zScanner je snadno použitelný pro lékaře, bezpečný, v souladu se zdravotními předpisy a kompatibilní s nemocničními informačními systémy. zScanner plně podporuje zásady Bring-Your-Own-Device a může být instalován jak na osobních zařízeních lékařů tak i na zařízeních ve vlastnictví nemocnice / kliniky.

zScanner funkcionality

Přihlášení

zScanner umožňuje lékaři přihlásit se pomocí jména a hesla, nebo pomocí biometrické autentizace, jako je například otisk prstu.

Výběr pacienta

Po přihlášení lékaře vybere příslušného pacienta buď naskenováním čárového kódu, nebo vyhledáním pacienta v databázi nemocničního informačního systému.

Vložení platnosti vyšetření

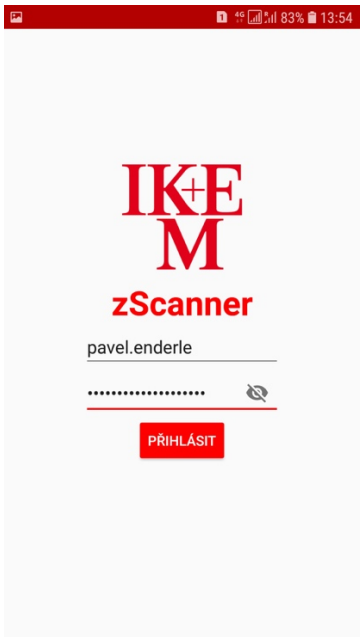
Lékař může rychle vložit datum platnosti vyšetření, které je pak zapsáno do příslušného foto záznamu.

Výběr typu vyšetření nebo typu dokumentu

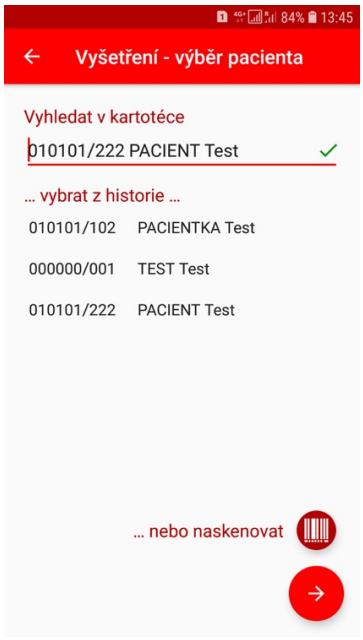
zScanner umožňuje lékaři vybrat typ vyšetření z předem definovaného seznamu, aniž by trávil čas tvorbou písemné specifikace. Lékař může také doplnit své vlastní poznámky, které budou následně propojeny s příslušnou fotodokumentací.

Fotografování a nahrávání dokumentů

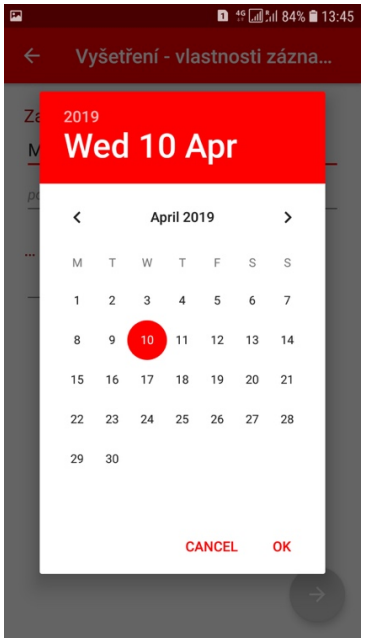
zScanner umožňuje lékaři pořizovat více fotografií lékařských dokumentů a zranění pacientů. Když lékař dokončí fotodokumentaci, zScanner nahraje fotografie do nemocničního informačního systému.



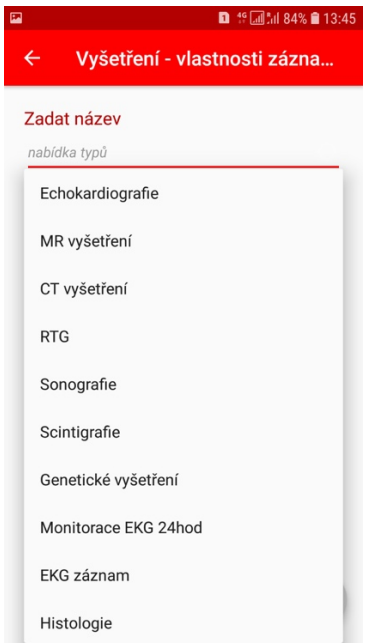
Přihlášení



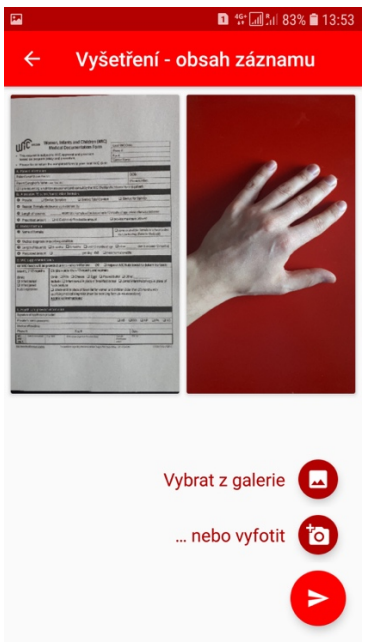
Výběr pacienta



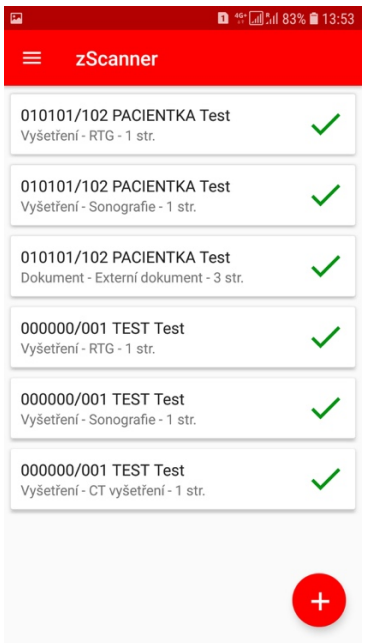
Vložení platnosti vyšetření



Výběr typu vyšetření

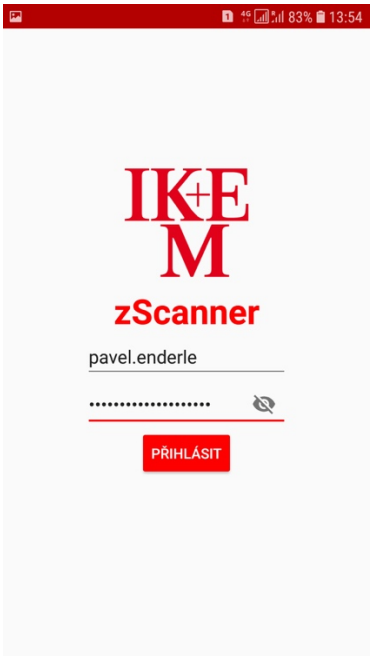


Fotografování



Nahrávání foto dokumentace

Případová studie – zScanner v nemocnici IKEM



Mobilní aplikace zScanner používaná v nemocnici IKEM

IKEM je významnou českou nemocnicí a největším centrem klinické a experimentální medicíny v České republice.

IKEM potřeboval vyřešit dlouhotrvající problém: pacienti již několik let prezentovali lékařům kritické zdravotní záznamy v tištěné podobě. Tyto dokumenty pak musely být ručně nahrány do nemocničního informačního systému IKEM. Lékaři čelili dvojímu dilematu: neměli čas na plnění těchto úkolů, a přesto museli mít k těmto důležitým informacím o pacientech rychlý přístup.

Další problém byl, že současné lékařské postupy vyžadují, aby lékaři vytvořili fotodokumentaci zranění pacientů. IKEM tuto problematiku dříve řešil pracným způsobem: lékař musel použít fotoaparát, pořídit si fotografii a později nahrát fotografii z fotoaparátu do počítače a poté ji nahrát z počítače do nemocničního informačního systému. To bylo časově náročné, a často i předmětem chyb.

Pro vyřešení tohoto problému vyvinula nemocnice IKEM zScanner, mobilní aplikaci pro klinickou a lékařskou fotodokumentaci. zScanner umožňuje lékařům používat jedno zařízení k vytváření digitálních kopií lékařských záznamů o pacientech, snímků zraněních pacientů, a jejich jednoduché a rychlé nahrání do nemocničního informačního systému.

Aplikace zScanner obsahuje velmi citlivá data, a proto je kybernetická bezpečnost velmi důležitým prvkem. IKEM se rozhodl zabezpečit zScanner pomocí platformy kybernetické bezpečnosti SeaCat. SeaCat pokrývá všechny požadavky na kybernetickou bezpečnost a regulační požadavky, a navíc se velmi snadno integruje.

Dnes zScanner používají desítky lékařů v nemocnici IKEM. Dle tvrzení lékařů tato aplikace významně zvyšuje efektivitu a značně šetří čas při provádění administrativních prací.

Institut klinické a experimentální medicíny (IKEM)

Institut klinické a experimentální medicíny je největší superspecializované klinické a vědeckovýzkumné pracoviště v České republice. Už více než 45 let se zaměřuje na léčbu kardiovaskulárních chorob, transplantace orgánů a diabetologii se spádovostí celé České republiky. Výzkumnou základnu institutu tvoří Centrum experimentální medicíny (CEM), které se zaměřuje na výzkum molekulární biologie a genetiky a studium experimentálních patofyziologických a fyziologických modelů v oblasti výzkumu všech tří odborných center Institutu – Kardiocentra, Transplantcentra, Centra diabetologie.

Kontakt pro média:

Mgr. Šárka Nevoralová, tisková mluvčí IKEM

+ 420 734 236 325

sarka.nevoralova@ikem.cz

SeaCat

SeaCat je platforma kybernetické bezpečnosti pro mobilní zdravotnické aplikace vyvinutá společností TeskaLabs. SeaCat umožňuje firmám provozovat aplikace spolehlivým, škálovatelným a bezpečným způsobem. Poskytuje cenné informace o provozu aplikace, v kombinaci se silnou ochranou dat. SeaCat umožňuje rozpoznat, vyřešit či zmírnit všechny druhy bezpečnostních a provozních incidentů dříve, než ohrozí provozovatele aplikace či koncové uživatele.

Výhody

Silná kybernetická bezpečnost

SeaCat chrání před všemi běžnými kybernetickými útoky. SeaCat je platforma pro kybernetickou bezpečnost, kterou vytvořili bezpečnostní odborníci, a která obsahuje všechny bezpečnostní funcionality pro ochranu aplikace a ochranu osobních údajů se kterými aplikace pracuje.

Rychlé nasazení

Nasazení SeaCat je jednoduché a bezproblémové. SeaCat zvyšuje úroveň zabezpečení okamžitě, bez nutnosti vlastního vývoje.

Rozumná investice

Budování bezpečné mobilní aplikace může být obtížná a nákladná cesta. SeaCat zajišťuje velmi vysokou úroveň kybernetické bezpečnosti, za zlomek nákladů vlastního vývoje.

Spolehlivá technologie

SeaCat je využíván každý den na desítkách tisíc zařízení. SeaCat chrání aplikace v oblasti telekomunikací, maloobchodu, zdravotnictví, automobilového průmyslu a dalších.

Bezproblémová uživatelská zkušenost

Kybernetická bezpečnost by neměla být na úkor zkušenosti uživatelů. SeaCat nevyžaduje žádné otravné konfigurace nebo postupy ze strany uživatele; SeaCat využívá všechny moderní funkce kybernetické bezpečnosti, jako jsou biometrické autorizační moduly a moduly zabezpečení hardwaru.

Otevřená platforma

SeaCat je platforma pro kybernetickou bezpečnost, která vám umožní těžit z nejnovějších pokroků v oblasti kybernetické bezpečnosti, zatímco Vy se zaměřujete na funkce Vaší aplikace. SeaCat je otevřená platforma bez vendor-locku či jakýchkoli jiných omezení.

Features

Feature	**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	Funguje i na mobilních zařízeních bez MDM Vzdálená správa aplikací (např. odmítnutí přístupu k citlivým informacím v případě ztráty zařízení)

Uživatelská zkušenost	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 CatVision.io pro technickou / zákaznickou podporu
Regulations compliance	GDPR compliant HIPAA 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 Podporuje všechny hlavní mobilní operační systémy (iOS, Android, Windows Phone) a platformy (Xamarin, PhoneGap a další) Kompatibilní se všemi politikami podnikové mobility (např. BYOD, COPE)

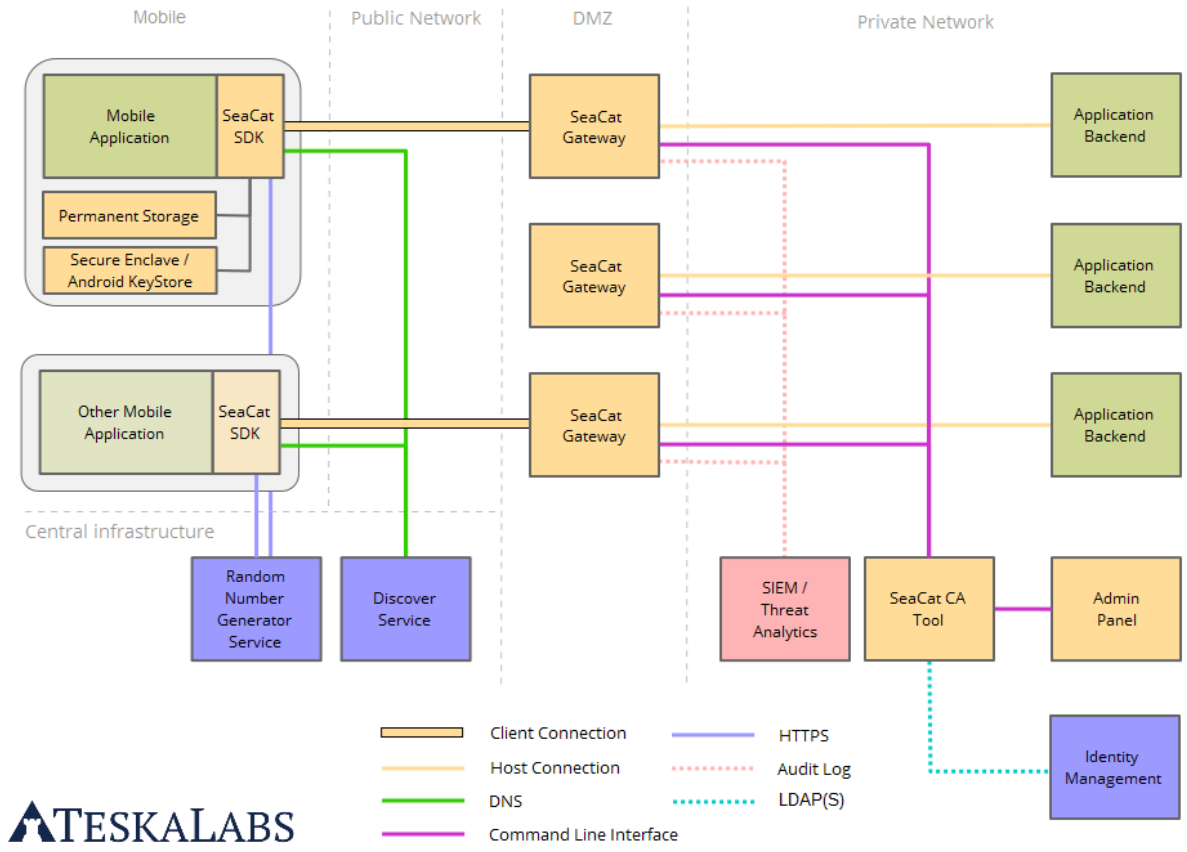
Technická specifikace

Technologie SeaCat se skládá ze SeaCat SDK, která je přidána do mobilní aplikace, a SeaCat Gateway, která je instalována do demilitarizované zóny (DMZ) před backend aplikace. SeaCat je navržen tak, aby byl transparentní pro vývojáře mobilní aplikací, snadno provozovatelný administrátory, a aby poskytoval maximální viditelnost lidem zodpovědným za kybernetickou bezpečnost.

SeaCat je kompatibilní se všemi hlavními mobilními operačními systémy a platformami.

Architektura

SeaCat komponenty jsou popsány v následujícím diagramu:



TESKALABS

Dokumentace

SeaCat dokumentace je k dispozici na: https://teskalabs.com/docs

O TeskaLabs

We, at TeskaLabs, believe that the digital world has to be safe. Today, as enterprises move toward mobile and Internet of Things (IoT), we help them build and operate mobile and IoT applications securely.

TeskaLabs is an award-winning product company committing to creating the world's most comprehensive application security technology for mobile and IoT apps. We are a proud member of Microsoft BizSpark Plus, a strategic partner of O2 Czech Republic, and a Cisco Preferred Solution Partner.

TeskaLabs operates from the headquarters in London, United Kingdom and an additional office in Prague, Czech Republic.

Kontakt

Obchodní dotazy	**Technické dotazy**
Pavel Enderle Sales Executive +420 731 211 381 pavel.enderle@teskalabs.com	Ales Teska CEO +420 731 624 038 ales.teska@teskalabs.com
TeskaLabs Ltd., odštěpný závod	
Adresa	Kodaňská 1441/46 Praha 10, 101 00
IČO	079 57 157
Vedeno u Městského soudu v Praze pod spisovou značkou A 79133	
TeskaLabs Ltd.	
Address	TeskaLabs LTD Unit 6 Queens Yard, London, E9 5EN United Kingdom
Company Identification Number	08893495
VAT Number	GB242432143

Certified by the Registrar of Companies for England and Wales.