

SMLOUVA O DÍLO

Č.: 26SIT003

dále jen „**Smlouva**“ uzavřená v souladu s ust. § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „**Občanský zákoník**“) níže uvedeného dne, měsíce a roku mezi níže uvedenými smluvními stranami:

(1) **MITEL a.s.**, IČ 256 75 036, se sídlem Dobrušská 1797/1, 147 00 Praha 4, společnost zapsaná v obchodním rejstříku vedená u Městského soudu v Praze pod sp. zn. B 27511, za níž jedná Richard Mikeš, předseda představenstva, číslo účtu:  email: info@mitel.cz

(dále jen „**Obstaravatel**“)

(2) **Zaměstnanecká pojišťovna Škoda**, IČ 463 54 182, se sídlem Husova 302, 29301 Mladá Boleslav, zapsaná v obchodním rejstříku vedená u Městského soudu v Praze pod sp. zn. A 7541, za níž jedná Mgr. Gabriela Kadlecová, MBA, ředitelka, email: 
tel.: 

(dále jen „**Objednatel**“)

(Obstaravatel a Objednatel dále též jen společně jako „**Smluvní strany**“ nebo jednotlivě jako „**Smluvní strana**“)

PREAMBULE

(A) Tato Smlouva mezi uvedenými Smluvními stranami se uzavírá na základě poptávkového řízení s předmětem: **Penetrační testování aplikace Karta mého srdce**.

1. ÚVODNÍ USTANOVENÍ

- 1.1. Obstaravatel je akciovou společností s mnohaletou tradicí působící zejména v oblasti telekomunikací, kybernetické bezpečnosti, Audio/Video, IT Outsourcingu a budování datových sítí, dále pak v oblasti budování a konfigurací televizních a satelitních systémů a konfigurací systémů inteligentních domů. Další činností firmy je poskytování poradenství v oblasti telekomunikací.
- 1.2. Objednatel je zdravotní pojišťovnou s mnohaletou tradicí zejména v oblasti správy veřejného zdravotního pojištění, výběru pojistného a úhrady zdravotní péče pojištěncům dle platných právních předpisů.

2. PŘEDMĚT SMLOUVY

- 2.1. Předmět Smlouvy. Předmětem této Smlouvy je realizace penetračního testu aplikace Karta mého srdce (Android / iOS, WEB, Schvalovací aplikace, napojení na portál ZP, viz akceptovaná nabídka), zahrnující popis použité metodiky, konkrétní pracovní postupy, dohled nad průběhem testu a způsob řízení mimořádných událostí. Součástí je rovněž vymezení výjimek a omezení, na která bude při realizaci testu brán zřetel.
- 2.2. Splnění Díla. Obstaravatel se zavazuje splnit Dílo pro Objednatele dle čl. 2 odst. 2.1. této Smlouvy nejpozději do 31. 3. 2026. Obstaravatel po do dokončení díla předá výstupy, které jsou součástí Přílohy č.1, současně s předávacím protokolem, který je stvrzením fyzické předávky díla. Finanční plnění následně proběhne na základě potvrzení akceptačního protokolu

Objednavatelem, který je stvrzením nejen dodání díla, ale dodání díla v požadované kvalitě a bez výhrad Objednavatele.

- 2.3. Zaměření Díla. Dílo poskytované Obstaravatelem pro Objednatele dle čl. 2 odst. 2.1. této Smlouvy nezahrnují poskytování právních služeb.

3. CENA ZA POSKYTOVANÉ SLUŽBY A PLATEBNÍ PODMÍNKY

- 3.1. Cena. Objednatel se zavazuje uhradit za poskytnuté Dílo Obstaravateli částku uvedenou v Obchodní a cenové nabídce, jež tvoří Přílohu č. 1 této Smlouvy (dále jen „Cena“). Obstaravatel má povinnost vystavit na částku Ceny nebo jiné finanční plnění podle této Smlouvy řádný daňový doklad – fakturu, a to po předání předmětu této smlouvy a jeho akceptaci ze strany Objednatele s tím, že faktura bude zaslána do datové schránky ZPS (5kpadkp). Splatnost takového daňového dokladu bude alespoň 14 dní.
- 3.2. Ostatní objednávky. Smluvní strany si ujednávají, že v případě dalších požadavků Objednatele za Obstaravatelem budou prováděny prostřednictvím emailové komunikace zasílané na info@mitel.cz.

4. PRÁVA A POVINNOSTI

- 4.1. Poskytování Díla. Obstaravatel je povinen poskytovat Služby včas a v řádné kvalitě, při poskytování Služeb bude postupovat s náležitou odbornou péčí a profesionálně.
- 4.2. Součinnost. Smluvní strany se zavazují poskytovat si vzájemnou součinnost. Objednatel je oprávněn v průběhu poskytování služeb kontrolovat kvalitu, způsob poskytování služeb a soulad se zadáním ve Smlouvě a dílčí Objednávky.
- 4.3. Pověřené osoby. Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím osob pověřených za tímto účelem.
- 4.3.1. Pověřená osoba. Za Obstaravatele: 

- 4.3.2. Pověřená osoba. Za Objednatele: 

- 4.4. Odpovědnost za data. Objednatel bere na vědomí, že Obstaravatel nenese odpovědnost za obsah, množství a stav všech dat, zejména pak dokumentů Objednatele.

5. DALŠÍ USTANOVENÍ

- 5.1. Důvěrná informace. Každá Smluvní strana se zavazuje, že nezpřístupní, ani nepoužije žádnou informaci obchodní a/nebo výrobní povahy, se kterou se seznámí v souvislosti s plněním této Smlouvy, zejména nezpřístupní, ani nepoužije:
- Žádnou takovou informaci obsaženou v této Smlouvě,
 - Databázi zákazníků druhé Smluvní strany ani kontakty na ně,
 - Cenovou politiku druhé Smluvní strany,

- d) Marketingovou strategii druhé Smluvní strany,
- e) Informace o uzavřených smlouvách a dodavatelích druhé Smluvní strany,
- f) Způsob fungování podniku druhé Smluvní strany,
- g) Strategická rozhodnutí a podnikatelské záměry druhé Smluvní strany,
- h) Informace nabyté v souvislosti s poskytováním Služeb pro jakoukoliv třetí stranu.

(dále jen „**Důvěrná informace**“)

- 5.2. Výjimka mlčenlivosti. Povinnosti mlčenlivosti podle čl. 5. odst. 5.1. této Smlouvy platí s výjimkou případů, kdy:
- a) Druhá Smluvní strana udělila předchozí písemný souhlas s takovým zpřístupněním nebo použitím Důvěrné informace.
 - b) Právní předpis nebo veřejnoprávní orgán stanoví povinnost zpřístupnit nebo použít Důvěrnou informaci.
 - c) Takové zpřístupnění nebo použití Důvěrné informace je nezbytné pro realizaci této Smlouvy,
 - d) Je to podle jakékoliv smlouvy nebo dohody uzavřené mezi Smluvními stranami dovoleno.
- 5.3. Vyjmuté informace. Mezi Důvěrné informace nepatří žádné informace, které jsou v době jejich zpřístupnění nebo použití běžně dostupné veřejnosti.
- 5.4. Zveřejnění stran. Smluvní strany si tímto vzájemně dávají souhlas k tomu, aby je druhá Smluvní strana uváděla jako svého partnera.
- 5.5. Obchodní tajemství. Každá Smluvní strana bere na vědomí, že Důvěrné informace tvoří obchodní tajemství druhé Smluvní strany.
- 5.6. Ochrana a oznamování. Každá ze Smluvních stran je povinna vynaložit alespoň stejné úsilí k ochraně Důvěrných informací druhé Smluvní strany, jaké vynakládá ve vztahu ke svým vlastním informacím obdobné povahy, přičemž toto úsilí musí být vždy alespoň přiměřené. Jakékoli neoprávněné sdělení nebo ztráta Důvěrných informací sdělující Smluvní strany musí být této Smluvní straně okamžitě písemně oznámeno.
- 5.7. GDPR. Budou-li pro Objednatele nebo jeho jménem během poskytování Služeb zpracovávány osobní údaje ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „**Nařízení**“) a zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „**Zákon o zpracování osobních údajů**“), zavazuje se Obstaravatel i Objednatel postupovat v souladu s Nařízením i Zákonem o zpracování osobních údajů. Smluvní strany si poskytnou vzájemnou součinnost při plnění jakýchkoli povinností souvisejících s Nařízením a Zákonem o zpracování osobních údajů. Platnost tohoto ustanovení je vždy v souladu s platnou právní úpravou Nařízení a Zákonem o zpracování osobních údajů.
- 5.8. Platnost ustanovení. Tento čl. 5. této Smlouvy zůstane v platnosti po dobu deseti (10) let po uplynutí doby trvání nebo po ukončení této Smlouvy. Povinnost zachovávat důvěrnost ve vztahu k citlivým informacím a obchodnímu tajemství není časově omezena.
- 5.9. Zákaz poškozování. Smluvní strany se dále zavazují druhou Smluvní stranu či jeho spolupracující partnery, jakkoliv nepoškozovat, a to jak ve svém soukromém životě, tak i při další podnikatelské aktivitě.

- 5.10. Rozsah povinnosti. Uvedená povinnost se vztahuje i na zaměstnance Objednatele či jiné osoby, které by se na poskytování služeb podíleli nebo měli z jednání či opomenutí Objednatele přístup k takovým informacím.

6. ODPOVĚDNOST ZA ŠKODU

- 6.1. Odpovědnost za škodu. Obstaravatel odpovídá Objednateli za škodu způsobenou vadnou Službou.
- 6.2. Předcházení škodám. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
- 6.3. Vyšší moc. Smluvní strany neodpovídají za prodlení způsobené nepředvídatelnými okolnostmi nebo příčinami ležícími mimo jejich vliv v souladu s ustanovením § 2913 odst. 2 Občanského zákoníku. Za okolnost vylučující odpovědnost se považuje překážka, jež nastala nezávisle na vůli povinné strany a brání jí ve splnění její povinnosti, jestliže nelze rozumně předpokládat, že by povinná strana tuto překážku nebo její následky odvrátila nebo překonala a dále, že by v době vzniku překážky předvídala. Účinky vylučující odpovědnost jsou omezeny však pouze po dobu, co trvá překážka, s níž jsou tyto povinnosti spojeny. V případě, že je některá ze Smluvních stran v prodlení dle tohoto bodu Smlouvy déle než 20 dní a nezjedná nápravu ani do 20 dnů od doručení písemného upozornění druhé Smluvní strany, je druhá Smluvní strana oprávněna vypovědět Smlouvu jako celek, a to s okamžitou účinností ke dni doručení písemné výpovědi druhé Smluvní straně. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

7. SMLUVNÍ POKUTY

- 7.1. Porušení mlčenlivosti. V případě, že Smluvní strana poruší jakoukoliv svou povinnost mlčenlivosti uvedenou v čl. 5. této Smlouvy, zavazuje se tato vydat veškerý prospěch z tohoto porušení druhé Smluvní straně a zaplatit druhé Smluvní straně smluvní pokutu ve výši 150.000,- Kč za každé jednotlivé porušení uvedené povinnosti. Uhrazením smluvní pokuty není vyloučeno právo požadovat náhradu škody či újmy.
- 7.2. Pokuta z prodlení. V případě porušení povinnosti Objednatele dle čl. 3 odst. 3.1. této Smlouvy včas uhradit Fakturu, je Objednatel povinen Obstaravateli zaplatit smluvní pokutu ve výši 0,5 % z Ceny za každý den prodlení.
- 7.3. Pokuta z prodlení. V případě neposkytnutí Služeb Obstaravatelem ve stanoveném termínu v souladu s čl. 2 odst. 2.2. této Smlouvy je Obstaravatel povinen uhradit Objednateli smluvní pokutu z prodlení ve výši 0,5 % z Ceny za každý den prodlení.
- 7.4. Splatnost a náhrada škody. Smluvní pokuta, na kterou vzniká nárok podle této Smlouvy, je splatná do 10 pracovních dnů od data doručení písemné výzvy k platbě jednou Smluvní stranou adresovanou druhé Smluvní straně. Uhrazením smluvní pokuty není vyloučeno právo požadovat náhradu škody či újmy.

8. ZÁVĚREČNÁ USTANOVENÍ

- 8.1. Oznámení. Veškerá doručování, oznámení, úkony a jinou komunikaci mezi Stranami v souvislosti s touto Smlouvou budou Strany činit písemně a elektronicky v českém jazyce a budou doručována na adresu Strany uvedenou v záhlaví této Smlouvy.
- 8.2. Úplná dohoda. Tato Smlouva se řídí mimo svůj obsah také zákonem č. 89/2012 Sb. „Občanský zákoník“.
- 8.3. Dodatky. Tuto Smlouvu lze měnit a doplňovat pouze písemně odsouhlasenými a podepsanými dodatky.
- 8.4. Účinnost. Tato Smlouva nabývá platnosti dnem jejího podpisu všemi Smluvními stranami a účinnosti dnem zveřejnění Smlouvy v registru smluv v souladu s čl. 8 odst. 8.6. této Smlouvy.
- 8.5. Stejnopisy. Tato Smlouva je vyhotovena ve dvou (2) stejnopisech, z nichž každý z účastníků Smlouvy obdrží po jednom (1) stejnopisu.
- 8.6. Zveřejnění Smlouvy. Obstaravatel prohlašuje, že Smlouva neobsahuje informace, která nelze poskytovat podle právních předpisů upravujících svobodný přístup k informacím. Obstaravatel bere na vědomí, že Objednatel coby povinná osoba ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákona o registru smluv), ve znění pozdějších předpisů, je povinna Smlouvu zveřejnit v registru smluv. Objednatel se zavazuje, že zašle tuto Smlouvu správci registru smluv k uveřejnění prostřednictvím registru smluv bez zbytečného odkladu, nejpozději však do 20 dnů od podpisu této Smlouvy. Tato skutečnost nebrání Obstaravateli, aby z jeho strany došlo k uveřejnění této Smlouvy. Obě Smluvní strany jsou povinny nejpozději do 25 dnů ode dne podpisu této Smlouvy provést kontrolu, zda je smlouva uveřejněna v registru smluv. V případě, že Obstaravatel zjistí, že tato Smlouva uveřejněna v registru není, je povinen neprodleně písemně informovat kontaktní osobu Objednatele anebo smlouvu sám uveřejnit.
- 8.7. Přílohy. Všechny následující přílohy jsou nedílnou součástí této Smlouvy.

PŘÍLOHA 1: Obchodní a cenová nabídka 26VHM001

Podpisy. Strany shodně prohlašují, že si tuto Smlouvu před jejím podpisem přečetly, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísní za nápadně nevýhodných podmínek a na důkaz toho připojují své vlastnoruční podpisy.

V


za MITEL a.s.,
Richard Mikeš, předseda představenstva



za Zaměstnaneckou pojišťovnu Škoda
Mgr. Gabriela Kadlecová, MBA, ředitelka

Příloha č. 1 – Obchodní a cenová nabídka (vč. Předmětu plnění)



Předmět cenové nabídky

Tato nabídka popisuje realizaci penetračního testu mobilní aplikace (Android / iOS), zahrnující popis použité metodiky, konkrétní pracovní postupy, dohled nad průběhem testu a způsob řízení mimořádných událostí. Součástí nabídky je rovněž vymezení výjimek a omezení, na která bude při realizaci testu brán zřetel. Dokument slouží jako podklad pro oboustranné odsouhlasení rozsahu, formy a kvality poskytované služby.

Cíl testu

Identifikovat bezpečnostní slabiny klientské mobilní aplikace a její interakce se serverovými rozhraními tedy také serverovou částí proti které aplikace v cloudu komunikuje, ověřit jejich reálný dopad a navrhnout doporučená nápravná opatření.

Použitá metodika

Test bude proveden v souladu s doporučenou metodikou OWASP Mobile Application Security Verification (MASTG) se zaměřením na kategorie zranitelností uvedené v OWASP Mobile Top 10. V testu budou kombinovány statické i dynamické techniky, včetně analýzy binárních souborů, analýzy zdrojového kódu (pokud je k dispozici), reverse-engineeringu a testování na reálných i upravených zařízeních.

Rozsah prací

Analýza struktury aplikace, konfigurací (např. AndroidManifest.xml) a webového rozhraní (část pro pojištění a část pro referenty, tzv. Schvalovací aplikace).

Otestování Portálu ZP v souvislosti s přihlašování (Autentizace a autorizace).

Statická analýza binárních artefaktů a zdrojových kódů (kde dodány).

Dynamické testování na „čistých“ i root/jailbreak zařízeních a na vybraných starších verzích OS (podle dohody).

Analýza lokálních úložišť, komunikace (TLS/SSL, pinning) a správy autentizace/tokenů.

Testy proti OWASP Mobile Top 10 a ověření ochranných mechanismů (obfuskování, detekce debugu, tamper-detekce).

Dokumentace důkazů (screenshoty, logy, výstupy nástrojů) a kroků k reprodukcii.

Dohled nad průběhem testu a komunikace

Test bude prováděn pod aktivním dohledem odpovědného testovacího týmu. Před zahájením bude dohodnut kontaktní list pro rychlou komunikaci a eskalaci. V průběhu testu bude pro zadavatele k dispozici určená kontaktní osoba, které budou neprodleně (i v průběhu testování) hlášena nalezená kritická zjištění ohrožující bezpečnost společnosti.

Řízení mimořádných událostí

Při zjištění zranitelnosti s bezprostředním vysokým dopadem na dostupnost, integritu nebo citlivost dat test přerušíme a neprodleně informujeme kontaktní osoby zadavatele. Dále navrhujeme řešení či dočasná opatření a pokračujeme po odsouhlasení zadavatele a implementaci opravy či dočasného opatření dle rozhodnutí zadavatele retestem opravených komponent.

Výstupy

Executive summary pro vedení.

Technická zpráva s detailně popsány výstupy, reprodukčními kroky, důkazy a odhadem rizikovosti.

Seznam doporučených nápravných opatření a prioritizace.

Checklist provedených testů a možnost retestu po odstranění zjištěných problémů (dle dohody).

Výjimky a omezení

Testování bude prováděno výhradně v dohodnutém produkčním prostředí;

Root/jailbreak testy a testy na zastaralých verzích OS budou provedeny pouze s předchozím souhlasem zadavatele.

Sociální inženýrství, útoky na fyzický přístup nebo jiné aktivity mimo předem odsouhlasený rozsah nejsou součástí nabídky, pokud není uvedeno jinak.

Test nezahrnuje vytváření a distribuci exploitů či škodlivého kódu mimo účely interního ověření a důkazních materiálů.

Právní a etické záruky

Všechny činnosti budou provedeny eticky a v souladu s platnou legislativou. Před zahájením testu bude uzavřena písemná dohoda definující rozsah, odpovědnosti, autorizace a kontakty pro řešení incidentů.

Používané nástroje

Všechny používané nástroje splňují několik základních kritérií, které obecně zajišťují vyšší bezpečnost a důvěryhodnost prováděných testů a omezují rizika vznikající při testování produkčních systémů.

Všechny nástroje jsou důkladně testovány na vlastním polygonu s cílem ověřit jejich správné fungování, skutečně vykonávané funkce a možné dopady na testované i okolní části systému.

Všechny klíčové nástroje jsou analyzovány a kompilovány pracovníky dodavatele. Nástroje, u kterého toto není možné, jsou zvýšenou měrou testovány a používají se pouze pro detekční účely, a ne ve fázích vytváření nebo udržování přístupu do testovaného systému.

V případě potřeby použití speciálního kódu na využití existující slabiny (tzv. exploit) jsou vždy preferovány vlastní programy nebo ty, u kterých je možné provést kontrolu zdrojového kódu a otestovat jejich funkčnost na polygonu.

Většina uvedených nástrojů nemá žádný, nebo jen minimální škodlivý dopad na vlastní testované systémy. U nástrojů, kde existuje vyšší riziko, ale kde kvalita a přidaná hodnota nástroje nelze nahradit žádným bezpečnějším způsobem, je toto uvedeno. Použití těchto nástrojů je vždy plánováno na dobu, ve které nejsou produkční systémy příliš využívány.

Mezi hlavní nástroje využívané v prostředí klienta patří:

- Nessus Professional,
- Hydra,
- Terrascan,
- Metasploit.
- BurpSuite Pro,
- Nessus,
- Acunetix

Závěrečná zpráva

Z bezpečnostního testu bude zpracována závěrečná zpráva v předpokládané následující struktuře (finální struktura může být testerem upravena tak, aby lépe odrážela výsledky testu).

- manažerské shrnutí zahrnující souhrn zjištění a doporučení k přijetí opatření s indikací prioritizace opatření,
- základní informace o testu včetně časového rámce, cílů, rozsahu, technických údajů, údajů o testovacím týmu, omezeních testu apod.,
- metodika testu popisující fáze testu i použité metriky tak, aby bylo možné test periodicky opakovat, případně ověřit výsledky,
- výsledky testu se statistickým vyhodnocením a podrobným popisem zjištěných nálezů v testovaném rozsahu systémů, sítí apod.

Doba plnění

Předpokládaný termín: do 14ti od objednání

Cena návrhu

Penetrační test mobilní aplikace	179 000,- Kč
Test odolnosti mobilní aplikace iOS	179 000,- Kč
Test odolnosti mobilní aplikace android	
Webová aplikace (část pro pojištěnce, část pro referenty)	
Interní aplikace	

Všechny ceny jsou uvedeny bez DPH v českých korunách (CZK).

Na základě akceptace jednotlivých etap je oprávněn uchazeč vystavit daňový doklad / fakturu na dílčí plnění. Splatnost faktur je 21 dní.