Otázka č.1:

Proof Of Concept (PoC) – Na základe požiadaviek vyplývajúcich zo súťažných podkladov (SP) vyplýva požiadavka na realizáciu PoC v súvislosti s MKAM-SW. SP však nepojednávajú o predmete PoC, čo má byť cieľom a predmetom PoC, čo a aké varianty konkrétne má preskúmať. Žiadame upresniť zadanie na PoC, čo presne má byť v rámci PoC realizované.

Odpoveď č.1:

Poukazujeme na to, že upravená časť projektu ESO1-D musí súbežne zabezpečiť funkcionalitu systému, ktorý bol rozvrhnutý tak na HW a krabicové riešenie tak na mobilno- softvérovú časť, ktorá mala priniesť určitý pilot.

Zmenovým konaním, ale musel byť z projektu vyňatý HW čím sa preniesla obrovská váha na SW riešenie a keďže niektoré časti a ich riešenia budú až výsledkom PoC. Na základe týchto objasnení bude pripravovaný finálny návrh architektúry a jej komponentov.

Projekt ESO1-D nedefinuje presné požiadavky na vytvorenie diela, ale definuje požiadavky pre dodanie riešenia, ktoré má naplniť hodnoty a požadované KPI a na tieto účely a potreby je v projekte prierezovo definovaný PoC - P3, P21, P70, P74, P81, P82 a P87.

Doplňujúca otázka k odpovedi č. 1:

Z uvedenej odpovede nie je možné určiť presný scope dodávky, naplánovať práce na jej realizáciu a v konečnom dôsledku stanoviť jej cenu. Aj v prípade realizácie PoC je minimálne žiadúce ohraničiť jednotlivé požadované alternatívy a prostredia (vrátane HW), ktoré majú byť skúmané. V opačnom prípade môže dôjsť k nepredvídateľnému nárastu nákladov pri realizácii takéhoto PoC. Žiadame upresniť zadanie na PoC, čo presne má byť v rámci PoC realizované, aké konkrétne varianty majú byť preskúmané a aké sú konkrétne očakávané výstupy PoC.

Doplňujúca odpoveď k odpovedi č.1:

Zadávateľ viacnásobne v odpovediach definoval a objasňoval, že dané zadanie nepojednáva o opise a stanovení parametrov pre dielo. Uchádzač na základe definovaných rozhraní a požiadaviek má priniesť riešenia k projektu.

Viď. 5.1.Objednávateľ požaduje dodať riešenie pozostávajúce z niekoľkých logických častí systému, ktoré budú implementovať spoločné, ale aj špecifické požiadavky popísané pre jednotlivé moduly (riešenia). Objednávateľ má za to a nevidí dôvod na vzdelávanie budúceho zhotoviteľa ohľadom procesného nastavenia PoC a jeho realizácie a následne ešte aj jeho finančnej politiky v definovaní ceny.

Objednávateľ definoval požiadavky na riešenie. Vysvetlenie PoC prechádza celým opisom a požiadavkami na riešenie. Budúci zhotoviteľ v rámci riešenie, ktoré chce dodať bude musieť vhodnosť a naplnenie logických časti systému preukázať PoC, 4.2 KPI pre hodnotenie PoC.

Otázka č.5:

KPI pre hodnotenie PoC definuje KPI „Kompatibilita MKAM-SW pre rôzne (mobilné) platformy (Android, iOS, Microsoft, Linux, Unix, iné)“ s cieľovou hodnotou 95%. Predpokladáme, že v rámci PoC bude stanovená obmedzená množina podporovaných platforiem (napr. mobilné platformy a konkrétna platforma pre dedikované zariadenie). Žiadame upresniť akým spôsobom bude tento parameter vyhodnocovaný a za akých podmienok možno dosiahnuť požadovanú hodnotu 95%.

Odpoveď č.5:

Máme za to že, kompatibilita pre platformy a operačné systémy bola zadefinované viacej širokospektrálne, ale keďže nepojednávame o presnej definícií diela, ale určujeme smer na naplnenia požiadavky riešenia, tak v tomto smere nevidíme problém.

V rámci a po zhodnotení PoC bude stanovená množina a presné zadefinovanie "pracovnej stanice" na ktorom bude ZPr. vidieť výstup z NZIS a tak isto aj presné zadefinovanie "mobilného zariadenia" a to po stránke operačnej a technickej. Týmto spôsobom sa zadefinuje určitá modelová, operačná rada a verzie mobilných zariadení s OS na ktoré bude dané riešenie implementované a tým pádom vyhovujúcim týmto požiadavkám. V danom prípade nevidíme budúcu diskrepanciu pre nedosiahnutie požadovanej hodnoty 95%.

Doplňujúca otázka k odpovedi č. 5:

Vzhľadom na uvedené, t.j. že kompatibilita pre platformy a operačné systémy bola zadefinované viacej širokospektrálne, ale Objednávateľ nepojednáva o presnej definícií diela, ale určuje len smer, vstupujú do prípravy ponuky neznáme faktory, ktoré len ťažko možno vopred odhadnúť. Pre plánovanie vývoja SW je kľúčové poznať podmienky prostredia, pre ktoré má byť vyvíjaný. Aj v prípade realizácie PoC je minimálne žiadúce ohraničiť jednotlivé požadované alternatívy a prostredia , ktoré majú byť skúmané. V opačnom prípade môže dôjsť k nepredvídateľnému nárastu nákladov pri realizácii takéhoto PoC. Žiadame upresniť zadanie na PoC, čo presne má byť v rámci PoC realizované, aké konkrétne varianty a prostredia majú byť preskúmané a aké sú konkrétne očakávané výstupy PoC.

Doplňujúca odpoveď k odpovedi č.5:

Objednávateľ má za to, že prostredie a vysvetlenie celej definície diela je v SU -MD -su_127. SU spolu s požiadavkami na dodanie riešenia k projektu a KPI vymedzujú dostatočne kľúčové podmienky na základe ktorých zhotoviteľ má predstaviť a priniesť riešenie na dané požiadavky. Áno Objednávateľ z dôvodu zmenového konania definoval určité časti viacej širokospektrálne, ale má za to, že v podobe vyššie uvedených dokumentov a parametrov určil pre budúci zhotoviteľ dostatočné faktory pre jeho patričné vypracovanie požiadaviek.

Pokiaľ má budúci zhotoviteľ za to, že má v prípade jeho navrhovaného riešenia a PoC dôjsť k nepredvídateľnému nárastu nákladov, či už pri SW alebo HW, tak potom riešenie pre naplnenie daného projektu nie je v rovinách definície súťažných podkladov. Ďalšie rozdefinovanie podmienok prostredia nevníma Objednávateľ ako žiadúcu a potrebnú požiadavku, a to ani v podobe minimálneho definovania.

Otázka č.6:

Požiadavka P68 SP definuje požiadavky riešenia na aplikačnú časť mobilnej autentifikácie, pričom ako prvý bod požiadavky uvádza: „Aplikácia bude vytvorená a publikovaná pod NCZI pre rôzne (mobilné) platformy (Android, iOS, Microsoft, Linux, Unix...)“. Zároveň posledný bod požiadavky uvádza „Využívať mobilné zariadenia na platformách Android a iOS pre verzie platné a používané v roku 2018 a vyššom“. Uvedené predstavuje nekonzistenciu v požiadavkách a navyše Microsoft, Linux, Unix nie sú mobilné platformy. Žiadame o vysvetlenie prípadne úpravu požiadavky na tak, aby aplikácia pre mobilnú autentifikáciu bola implementovaná iba pre platformy Android a iOS.

Odpoveď č.6:

V prvotnom zadefinovaný OS pojednávame o viacerých, ale v rámci požiadaviek pre riešenie zároveň pridávame časovú indikáciu, o ktorú by sa mal budúci zhotoviteľ a riešiteľ opierať, keďže v stave a čase implementácie projektu budú mobilné zariadenia z technologického hľadiska v úplne iných verziách.

Máme za to, že definovanie minimálnej hodnoty platných a používaných verzií OS pre mobilné zariadenia je na mieste a nie o „nekonzistenciu“, keďže posledný bod uvádza, že v prípade aplikácie pre platformu Android alebo iOS musí byť táto kompatibilná s verziou takéhoto OS vydaného minimálne v roku 2018 a nie staršom, zároveň upozorňujeme na všeobecnú definíciu mobilného zariadenia, ktorá pojednáva, že mobilným zariadením môže byť akýkoľvek mobilný počítač alebo množstvo ďalších elektronických zariadení, ktoré vykazujú prenosnú funkciu.

Doplňujúca otázka k odpovedi č. 6:

Tzn. Objednávateľ (napr. pre záchranné služby a iné použitie v teréne) zvažuje aj custom mobilné zariadenia? Keďže na trhu sú rozšírené takmer výhradne mobilné zriadenia s OS Android a iOS, aké iné mobilné zariadenia má Objednávateľ na mysli? Zvažuje sa aj špeciálny HW s OS napr. Linux, Unix, ...? A je tento HW, ktorý Objendávateľ zvažuje, vybavený napr. skenerom QR kódov?

Doplňujúca odpoveď k odpovedi č.6:

Objednávateľ v rámci požiadavky na dodávku riešenia k projektu definoval mobilné zariadenia, nepojednáva a ani nezvažuje custom mobilné zariadenie. V nadväznosti na hlavnú odpoveď opätovne uvádzame, že aplikácia má byť vytvorená pre mobilné zariadenia v rozsahu všeobecnej definície, komerčne dostupné, ktorých OS bude v dobe implementácie stále podporovaný. Objednávateľ pojednáva v tejto rovine iba o požiadavke a to, že pokiaľ sa budú používať mobilné zariadenia na platformách Android a iOS, tak stanovujeme požiadavku na verzie platné a používané v roku 2018 a vyššom.

Otázka č.8:

SP, v kap. 5.5 Požiadavky na riešenie Mobilnej autentifikácie, uvádzajú: „Centralizované riešenie pre bezpečné uloženie a centralizovaný manažment kryptografických kľúčov vybraných ZPr, sprístupnenie kryptografických kľúčov ZPr prostredníctvom samostatnej aplikácie mobilného zariadenia, pomocou ktorej bude ZPr vykonávať požadované operácie v systéme eZdravie, a zároveň úprava existujúceho IAM o nový typ kryptografického kľúča uloženého v centrálnom bezpečnom úložisku využívajúcom certifikované kryptografické zariadenia pre úschovu kľúčov ZPr s rovnakým atribútom použitia ako kľúče uložené na jeho ePZP karte s možnosťou spárovania mobilného zariadenia s kryptografickými kľúčmi ZPr uloženými v centrálnom bezpečnostnom úložisku a následnom plnohodnotnom využívaní služieb identifikácie a autentifikácie bez potreby využívania čítačky ePZP kariet“. Otázka: aká konkrétna certifikácia kryptografického zariadenia je požadovaná? Resp. keďže predmetom dodávky nie je hardvér, poskytne objednávateľ pre účely projektu certifikované kryptografického zariadenia spĺňajúce dané podmienky? Aký typ zariadenia Objednávateľ poskytne a koľko kusov bude k dispozícii? Aký je výkon kryptografických zariadení poskytovaných Objednávateľom napr. v počte podpisov za sekundu pri RSA algoritme o dĺžke kľúča 2048 bitov a pri ECDSA algoritme o dĺžke kľúča 256 bitov?

Odpoveď č.8:

V tomto prípade sa jedná o princíp, na ePZP karte sú uložené certifikáty resp. kryptografické kľúče – rozpísané aj v SU -MD -su_127. Dodávateľ musí navrhnúť bezpečnú alternatívu ako narábať s týmito kľúčmi. Používa sa samozrejme PKI infraštruktúra eZdravie. PKI-> Crypto Controller -> IAM -> NZIS.

Doplňujúca otázka k odpovedi č. 8:

Áno, avšak Objednávateľ požaduje použitie „centrálneho bezpečného úložiska využívajúceho certifikované kryptografické zariadenia pre úschovu kľúčov ZPr“. Takýmito zariadeniami sú hardvérové security moduly (HSM). Keďže predmetom dodávky nie je hardvér, pýtame sa, akými zariadeniami disponuje Objednávateľ, resp. aké zariadenia vie pre tento účel zabezpečiť?

Doplňujúca odpoveď k odpovedi č.8:

Autentifikačné a šifrovacie certifikáty sú pridelené k definovanej karte a priamo sa viažu na túto kartu. Ďalší popis je obsiahnutý v design manuály IAM, ktorý je interným bezpečnostným dokumentom NZIS. Pridelenie RSA kľúčov a proces registrácie používateľa a mobilného zariadenia a spárovania daného mobilného zariadenia s kryptografickými kľúčmi ZPr uloženými v centrálnom bezpečnostnom úložisku nie je „požiadavkou“ ale definovaním postupu, keďže budú prebiehať rovnakým atribútom použitia ako kľúče uložené na jeho ePZP karte.

Informácie akými zariadeniami disponuje Objednávateľ a celkovo podrobnejšie informácie tohto charakteru nad rámec SU -MD -su_127 nie sme oprávnení poskytovať.

Objednávateľ by zároveň ale rád poukázal na informácie, že v definovaní požiadaviek na dodanie riešenia k projektu je vznikom nového spôsobu autentifikácie prostredníctvom mobilnej aplikácie implementovaná nová služba pre získanie OAuth tokenu. Prípadné vyvolané

nevyhnutné úpravy súčasného riešenia IAM NZIS pre integráciu s autentifikačným OAuth serverom nie sú predmetom dodávky a Objednávateľ ich zabezpečí vo vlastnej réžii.

Otázka č.9:

Požiadavka SP č. P69 stanovuje požiadavky riešenia na centrálne podpisovanie, pričom jedna z požiadaviek znie: „Riešenie musí byť navrhnuté tak, aby umožnilo vykonať paralelné podpisové operácie vykonávané ZPr pre 2000 požiadaviek, z ktorých každá musí skončiť do 5 sekúnd“. Keďže predmetom dodávky nie je hardvér, poskytne objednávateľ pre účely projektu dostatočne výkonné kryptografického zariadenia, ktoré budú poskytovať dostatočný výkon umožňujúci splniť danú požiadavku?

Odpoveď č.9:

Nie, kryptografia má byť riešená softvérovo.

Doplňujúca otázka k odpovedi č. 9:

Ak má byť kryptografia riešená softvérovo, žiadame v tomto zmysle upraviť požiadavky SP. T.j. odstrániť z kap 5.5 požiadavku na použitie „centrálneho bezpečného úložiska využívajúceho certifikované kryptografické zariadenia pre úschovu kľúčov ZPr“.

Navyše dopĺňame otázku, či si je Objednávateľ vedomý, že požiadavka na použitie bezpečného hardvéru pre kryptografické operácie v systéme Server Signing vyplýva z normy STN EN 419241-1, na ktorú sa objednávateľ v požiadavkách P26 a P58 odvoláva.

Doplňujúca odpoveď k odpovedi č.9:

Objednávateľ v kapitole 5.5 pojednáva o požiadavkách na riešenie mobilnej autentifikácie a sprístupnenie kryptografických kľúčov ZPr prostredníctvom samostatnej aplikácie mobilného zariadenia, ktoré bude ďalej riešiť problematiku prihlásenia a kryptografie softvérovo. ePZP aktuálne obsahuje sadu certifikátov, ďalšiu funkcionalitu zabezpečia RSA kľúče prislúchajúce k autentifikačnému certifikátu, šifrovaciemu certifikátu a certifikátu pre elektronický podpis.

V popise požiadavky na riešenie definujeme proces registrácie používateľa a mobilného zariadenia a spárovania daného mobilného zariadenia s kryptografickými kľúčmi ZPr uloženými v centrálnom bezpečnostnom úložisku, rovnako ako jeho napojenie v rámci funkcionality podpisovania a šifrovania a na strane NCZI - IAM NZIS. Preto požiadavka na odstránenie predmetného úložiska je neopodstatnená.
Objednávateľ si je vedomý a pojednáva o riešení pomocou nového centrálneho komponentu nasadeného v NZIS pomocou server-signing technológie, ktorá je definovaná vo všeobecných a bezpečnostných požiadavkách.

Prípadné vyvolané nevyhnutné úpravy súčasného riešenia IAM NZIS pre integráciu s autentifikačným OAuth serverom nie sú predmetom dodávky – viď SP – 5.5

Otázka č.13:

SP v kap. 5.2 uvádzajú požiadavky na harmonogram nasledovne

- Riešenie podľa Opisu PZ vrátane jeho uvedenia do prevádzky bude zrealizované najneskôr do 12 mesiacov od nadobudnutia účinnosti Zmluvy o dielo,
- V rámci etapy Testovanie prebehne najneskôr v 10. mesiaci od nadobudnutia účinnosti Zmluvy ukončenie testovania PoC (CPE, MKAM-SW a Serverové riešenie). Objednávateľ podľa dodaných štruktúrovaných výstupov z etapy Testovanie rozhodne akou formou softvérových riešení (MKAM-SW) v zmysle požiadaviek uvedených v tomto opise PZ a SU sa bude pokračovať.
- Doba na dodanie finálnej verzie server signing komponentov je 18 mesiacov od účinnosti zmluvy
- V ďalšom období trvania Zmluvy, t.j. nasledujúcich 14. mesiacov až do ukončenia celého projektu ESO1-D, Zhotoviteľ zabezpečí nasadenie- Deployment, resp. podporu pri spustení do prevádzky vybraného variantu CPE a MKAM-SW pre ambulantných lekárov
- Predpokladané trvanie hlavných aktivít je 26 mesiacov.

Otázky:

- Ak v 10tom mesiaci bude ukončené PoC a až následne sa len určí „akou formou softvérových riešení (MKAM-SW) v zmysle požiadaviek uvedených v tomto opise PZ a SU sa bude pokračovať“, potom dodanie riešenia a jeho sprevádzkovanie už v 12tom mesiaci, t.j. len dva mesiace po ukončení PoC sa zdá byť nereálne. Žiadame prehodnotiť túto požiadavku a poskytnúť väčší časový priestor na dodanie finálneho riešenia, napr. v 18tom mesiaci spolu s finálnou verziou Server Signingu.

Odpoveď č. 13a:

V danej požiadavke došlo k redakčnej chybe a zameneniu numerického definovania mesiacov.:

- riešenie podľa Opisu PZ vrátane jeho uvedenia do prevádzky bude zrealizované najneskôr do 18 mesiacov od nadobudnutia účinnosti Zmluvy o dielo – maximálne do 30.6.2023...
- V rámci etapy Testovania najneskôr v 10. mesiaci, pričom harmonogram autorizovaný vo vzťahu ku termínu ukončenia 30.6.2023. Odkaz na testovanie PoC je redakčnou chybou, nakoľko PoC musí byť jedným z hlavných výstupov častí Analýza a dizajn.
- Doba na dodanie finálnej verzie server signing komponentov je 18 mesiacov...
- V ďalšom období trvania Zmluvy, t.j. po 4. mesiacoch nasledujúcich, až do ukončenia celého projektu ESO1-D, Zhotoviteľ zabezpečí nasadenie - Deployment...
- Predpokladané trvanie hlavných aktivít je 26 mesiacov – zadefinovanie časového rozhrania sa uskutočnilo v čase prípravy. Časové trvanie hlavných aktivít bude samozrejme upravené od podpísania zmluvy s víťazným uchádzačom a to maximálne do 30.6.2023.
- Odpoveďou na Vami položenú otázku, je doba realizácie najneskôr do 18 mesiacov od nadobudnutia účinnosti Zmluvy o dielo – maximálne do 30.6.2023.

Doplňujúca otázka k odpovedi č. 13a:

Ďakujeme za vysvetlenie. Napriek tomu nám v SP chýba významne detailnejší rozpis míľnikov dodávky a to najmä vo vzťahu k očakávaným konkrétnym výstupom dodávky pre jednotlivé míľniky. Uvedené má totiž značný vplyv na faktory vstupujúce do prípravy ponuky, najmä na plánovanie realizácie, alokáciu ľudských zdrojov ako aj ďalšie odhady týkajúce sa dodávky. Žiadame preto Objednávateľa o doplnenie týchto informácií resp. požiadaviek do SP.

Doplňujúca odpoveď k odpovedi č.13a:

Objednávateľ má za to, že rozpis míľnikov dodávky a ich vzájomné napojenie na jednotlivé úseky a trvania je dostačujúce, keďže primárnym faktorom vstupujúcim do plánovania realizácie je vyhotovenie a naplnenie požiadaviek pre riešenie a dodanie diela na základe týchto požiadaviek a definovaného harmonogramu.

Objednávateľ by rád poukázal na to, že pokiaľ zhotoviteľ ponúkne konštruktívne riešenie a implementáciu k projektu, tak automaticky bude vedieť splniť komplexné záležitosti a to rozdefinovať ponúkané riešenie z pohľadu finančného, technického, rovnako aj alokácie ľudských zdrojov a to všetko pri dodržaní definovaných časových hodnôt tak aj plánu realizácie.

Otázka č. 14

Verejný obstarávateľ má pri kľúčovom expertovi č. 7 Bezpečnostný expert nasledovné požiadavky na preukázanie kvalifikácie:
minimálne 3-ročná odborná prax v oblasti bezpečnostných incidentov
minimálne 5-ročná odborná prax v oblasti návrhu alebo posudzovania informačných systémov, riešenia bezpečnostných incidentov alebo bezpečnostných auditov
minimálne 1-ročná odborná prax v oblasti zachytávania digitálnych stôp a forenznej analýzy
platný certifikát CISSP alebo CISA alebo ekvivalent daného certifikátu od inej akreditovanej autority; túto podmienku účasti uchádzač preukáže prostredníctvom kópie certifikátu;
platný certifikát CHFI alebo GCFE alebo GCFA. túto podmienku účasti uchádzač preukáže prostredníctvom kópie certifikátu

Nakoľko sa ale v súťažních podkladoch nikde nenachádza požiadavka foréznej analýzy na zachytávanie ddigitálnej stopy ani požiadavka na dodávku SIEM (security information and event management) alebo SOC (security operation center), bude pri expertovi 7 postačovať peukázanie kvalifikácie okrem požiadaviek na odbornú prax len certifikátom CISSP alebo CISA alebo ekvivalentom daného certifikátu?

Odpoveď č. 14

Verejný obstarávateľ poukazuje na podrobný opis predmetu zákazky v súťažných podkladoch. Predmetom zákazky je vytvorenie bezpečnej platformy pre realizáciu **Národného projektu Zabezpečenia efektívneho používania služieb ESO1** poskytovateľmi zdravotnej starostlivosti na celom území SR (ESO1-D). Projekt je zameraný na prístup všetkých aktérov

zdravotnej starostlivosti do procesov elektronického zdravotníctva v Slovenskej republike, známom ako eZdravie.
Systém elektronického zdravotníctva eZdravie je prevádzkovaný od 1. januára 2017. Do systému eZdravie sa pracovníci v zdravotníctve (ďalej len „ZPr“) prihlasujú cez svoje vlastné informačné systémy v pozícii poskytovateľov zdravotnej starostlivosti a pristupujú doň výhradne prostredníctvom elektronického preukazu zdravotníckeho pracovníka (ďalej len „ePZP“), pre ktorý je nevyhnutné, aby bol počas práce s IS eZdravie stále vložený v čítačke ePZP. Uvedené riešenie predstavuje obmedzenie prístupu do eZdravie významnej skupine zdravotníckych pracovníkov, ktorí využívajú, pracujú a zapisujú zdravotné záznamy pacientov v teréne, veľakrát v akútnych situáciách alebo mimo pripojenia do IS eZdravie. Ďalším zámerom je nutnosť odbremeniť ZPr od riešenia technických problémov eZdravie a aby neboli pre neho zdržaním alebo inou prekážkou v práci so systémom eZdravie. Cieľom implementácie a riešenia projektu je teda rozšíriť a doplniť elektronické služby, doplniť nové komponenty a minimalizovať problematické oblasti pri používaní elektronických služieb systému eZdravie v sektore zdravotníctva.
Súčasťou projektu je Mobilno-Komunikačno-Autentifikačný modul-MKAM-SW a CPE, ktorý zabezpečí presunutie centrálnych aplikačných komponentov eZdravie ako ovládačov, klientský SW a CryptoController mimo hardwarových komponentov ZPr do softwarovej časti CPE tak, aby všetky komponenty mohol verejný obstarávateľ spravovať vzdialene (off-site) a primárne bez potreby komunikácie so ZPr alebo IT podpory na strane PZS. Týmto spôsobom sa bude vedieť implementovať online monitoring MKAM-SW a CPE, v ktorom bežia MKAM-SW a aplikačné komponenty tak, aby verejný obstarávateľ v prípade prevádzkového incidentu vedel v čo najskoršom čase vzdialene zasiahnuť.
V zmysle vyššie uvedeného stručného opisu predmetu zákazky je nesporné, že súčasná a požadovaná platforma/riešenie pre efektívne používanie služieb ESO1 poskytovateľmi zdravotnej starostlivosti na celom území SR, získava, pracuje a bude pracovať s citlivými údajmi o zdravotnom stave pacientov, bude tieto uchovávať a spätne poskytovať ZPr pre účely efektívnej a rýchlej zdravotnej starostlivosti.
Verejný obstarávateľ zdôrazňuje, že zákon č. 576/2004 Z. z. o zdravotníckej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a zmene a doplnení niektorých zákonov v znení neskorších predpisov **výslovne ustanovuje** konkrétne osoby, oprávnené nahliadať do zdravotnej dokumentácie. Osobné/zdravotné údaje pacientov sú **hlavným zdrojom informácií pre liečbu pacientov**, preto pri ich získavaní, spracovávaní a uchovávaní, je nevyhnutné akceptovať tiež zákon NR SR č.18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov.
Riešenie obsahuje aj serverovú časť pre neobmedzené používanie centrálnej časti modulov na dobu neurčitú tak, aby bolo možné serverovú časť diela nasadiť aj v inom prostredí určenom verejným obstarávateľom s využitím certifikovaných služieb vládneho cloudu.

V nadväznosti na uvedenú vecnú argumentáciu je teda nesporné, že príprava a realizácia vládneho projektu v rezorte zdravotníctva je mimoriadne významným riešením, ktorý v nadväznosti na súvisiacu právnu úpravu, charakter a význam spracúvaných informácií si nevyhnutne vyžaduje, ako súčasť predmetu zákazky, riešenie bezpečnosti požadovaného riešenia. Verejný obstarávateľ zdôrazňuje, že predmet zákazky nie je požiadavkou na

jednoduché technologické riešenie procesov a výkonu interných potrieb jednej zo štátnych organizácií, ktorou je NCZI,<>b ale ide o národný projekt s dosahom primárne na občanov Slovenskej republiky a všetkých poskytovateľov zdravotnej starostlivosti pre účely zlepšenia zdravotnej starostlivosti.
Masívne vládne riešenia si vyžadujú mimoriadnu pozornosť rovnako ako vecné riešenia účelu národných projektov. Forenzné vyšetrovanie hackingu je nevyhnutnou súčasťou projektu pre odhaľovanie hackerských útokov a získavania dôkazov a pre vykonávanie auditov s cieľom zabrániť budúcim útokom. Cieľovou skupinou certifikácie pre forenzné vyšetrovanie hackingu sú práve, okrem iných, aj správcovia systémov, vládne organizácie.
Z uvedených dôvodov je v nadväznosti na predmet zákazky nielen požadované ale nevyhnutné realizovať predmet zákazky expertmi, ktorí disponujú overenými znalosťami, zručnosťami a schopnosťami vykonávať typické vyšetrovania incidentov, forenzné analýzy, hlásenia a získavania dôkazov. Za účelom ochrany získania kvalitného riešenia sa zo strany verejného obstarávateľa objektívne vyžaduje, aby požadovaný expert prispel v riešení projektu svojimi znalosťami o pokročilých scenároch riešenia incidentov, vrátane narušenia interného a externého údajov, pokročilých perzistentných hrozbách, anti-forenzných technikách používaných útočníkmi a komplexných digitálnych forenzných prípadoch.
Verejný obstarávateľ súhlasí s tvrdením žiadateľa, že stanovené náročné podmienky na experta sú primerané v zákazkách, ktorých predmetom sú služby a plnenia priamo súvisiace s bezpečnosťou informačných systémov, pretože predmet zákazky si vyžaduje maximálnu bezpečnosť. Verejný obstarávateľ však nemôže súhlasiť s názorom žiadateľa, že z opisu predmetu zákazky absentuje súvis tejto podmienky účasti so samotným predmetom zákazky. Na základe analýzy verejného obstarávateľa o dostupnosti požadovanej služby forenzného vyšetrovania hackingu prostredníctvom na to určených a v znalostiach overených expertov, je len v rámci Slovenskej republiky dostupných cca 15 expertov. Analýza dostupnosti bola overovaná v certifikačných autoritách napr. EC – Councilom, GIAC - Global Information Assurance Certification , ktoré pôsobia na SK viac ako 20 rokov Verejný obstarávateľ tvrdí, že je jeho primárnou úlohou predchádzam v rámci projektov takým situáciám ako sa nedávno medializovali, v prípade útoku hackerov do IS eHranica, kedy sa objavili dve vážne zraniteľnosti v štátnych systémoch.