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.

Otázka č.2:

Nie je jasne zadefinované, aké zariadenia sa myslia pod označením CPE. Vo vysvetlivkách sa konkrétne píše: „„CPE“ tiež „MKAM“ je Customer-premises equipment s mobilno - komunikačným autentifikačným modulom (MKAM-SW) bežiacim ako samostatný softvérový prvok implementovaný na (mobilnom) zariadení zdravotníckeho pracovníka za účelom komunikácie s NZIS.“ Vo vysvetlivkách sa pri MKAM-SW píše „Komunikačno-autentifikačný modul - časť softvér. Ide o sadu aplikácií a modulov, ktoré ako celok budú bežať na pracovnej stanici ZPr a na dedikovanom mobilnom hardvéri ZPr - CPE. Spôsob použitia a prípadné technické obmedzenia overí krok dodávky ďalej označený ako PoC“. V SP kap. 5.6 „Požiadavky riešenia na MKAM-SW“ sa ďalej píše „Softvér pre pracovnú stanicu - mobilné zariadenie ZPr alebo dedikovaný hardvér CPE“.

Bolo by dobré:

- Zjednotiť terminológiu pri použití označenia CPE

- Upresniť aké konkrétne typy zariadení sú myslené pod označením CPE (napr. mobilný telefón ZPr, dedikovaný hardvér v ambulancii ZPr, PC lekára, ...)

- Definovať použitie jednotlivých typov zariadení vo vzťahu k predpokladaným scenárom použitia, t.j. či sa má používať v ambulancii pri štandardnom poskytovaní zdrav. starostlivosti, v teréne (záchranná služba), atď.

Ospravedlňujem sa, ale nevidím otázku. Pokiaľ sa jedná o upozornenia, tak áno samozrejme relevantné zhodnotenie a usmernenia berieme na vedomie:

Odpoveď č.2a: <u>Zjednotiť terminológiu pri použití označenia CPE</u>

V tomto prípade, rozumieme pripomienke - keďže sa jedná customer - premises equipment, môže sa jednať o akékoľvek koncové zariadenie na strane užívateľa.

Odpoveď č.2b: Upresniť aké konkrétne typy zariadení sú myslené pod označením CPE (napr. mobilný telefón ZPr, dedikovaný hardvér v ambulancii ZPr, PC lekára, ...)

V projekte pri využitý HW a krabicového riešenia sa predpokladalo a rátalo s tým, že toto riešenie sa bude napájať na rôznu zmes "počítačov“ umiestnených v zdravotných ambulanciách a to po stránke rôznych myslíme z pohľadu operačného programu, rýchlosti pripojenia alebo technickej vyspelosti daného zariadenie. Pri SW riešení, ale s úplnou presnosťou nevieme exaktne definovať rozsah týchto parametrov, preto možno nastala menšia disproporcia a o daných zariadeniach pojednávame taktiež ako o CPE.

Odpoveď č.2c: Definovať použitie jednotlivých typov zariadení vo vzťahu k predpokladaným scenárom použitia, t.j. či sa má používať v ambulancii pri štandardnom poskytovaní zdrav. starostlivosti, v teréne (záchranná služba), atď.

Z pohľadu projektu, nie je prínosnou stránkou, definovať rozsah jednotlivých typov zariadení, ale priniesť možnosť mobilnej autentifikácie a autorizácie, ktorou sa má odstrániť nutnosť statického prihlasovania a verifikovania kartou. V budúcnosti by mohlo byť v postupných krokoch nahradené mobilnou autentifikáciou a pre ZPr. by bola toto hlavná forma prihlásenia do NZIS-u. Definovať jednotlivé zariadenie a ich typológiu je súčasťou požiadavky na dodanie riešenia.

Otázka č.3:

MKAM-SW – vzhľadom na predchádzajúcu otázku žiadame

• upresniť pre aké konkrétne typy zariadení má byť MKAM-SW vyvinutý,

• uviesť v akých konkrétnych nasadeniach v praxi má byť použitý (ambulancia, lekáreň, záchranná služba, vizity, ...) a to pre každý požadovaný typ CPE

• predpokladaný rozsah úkonov v danom nasadení (napr. ambulantné PC – plný rozsah, záchranná služba s aplikáciou e Zdravie v mobile s prístupom na vybrané funkcie eZdravie)

Odpoveď č.3a: upresniť pre aké konkrétne typy zariadení má byť MKAM-SW vyvinutý,

Zodpovedané v predošlej pripomienke.

Odpoveď č.3b: uviesť v akých konkrétnych nasadeniach v praxi má byť použitý (ambulancia, lekáreň, záchranná služba, vizity, ...) a to pre každý požadovaný typ CPE

Presné rozloženie a zadefinovanie zariadení je rozpracované v SU -MD -su_127. Po rozsahovej stránke sa určenie cieľovej skupiny ani jej rozsah nezmenil, iba technologický prevedenie projektu prešlo úplne na plecia SW riešenia.

Odpoveď č.3c: predpokladaný rozsah úkonov v danom nasadení (napr. ambulantné PC – plný rozsah, záchranná služba s aplikáciou e Zdravie v mobile s prístupom na vybrané funkcie eZdravie)

Rozpracované v SU -MD -su_127 aj s opisom pristupovania pre záchranné služby.

Otázka č.4:

Potvrdenie prítomnosti pacienta v mobilnom zariadení ZPr a dedikovanom HW zariadení – súťažné podklady definujú požiadavku na MKAM, aby umožnil „Vygenerovať a priložiť k požiadavke token potvrdenie prítomnosti pacienta“. Potvrdenie prítomnosti pacienta sa vykonáva prostredníctvom Aplikácie pre PPP, ktorú poskytuje MVSR. Pre aké platformy je aplikácia PPP dostupná?

V prípade prevádzky MKAM-SW na mobilných zariadení ZPr by mala byť dostupná min. pre Android a iOS a v prípade dedikovaného HW pre OS, na ktorom bude daný dedikovaný HW bežať. V prípade mobilných zariadení by k zariadeniu navyše musela byť pripojená externá čítačka kontaktného čipu občianskeho preukazu. Prosíme upresniť, v ktorých prípadoch a na ktorých typoch zariadení má byť potvrdenie prítomnosti pacienta podporované.

Odpoveď č.4a: Pre aké platformy je aplikácia PPP dostupná?

MS Windows, Mac OS, GNU/Linux 32 bit (x86) a GNU/Linux 64 bit (x86_64).

Odpoveď č.4b: V prípade mobilných zariadení by k zariadeniu navyše musela byť pripojená externá čítačka kontaktného čipu občianskeho preukazu.

V prípade mobilných zariadení sa neráta s pripojením externej čítačky a verifikovanie občianskeho preukazu. Mobilné verifikácie má priniesť možnosť mobilnej verifikácie pre ZPr. ako náhrada pre ePZP, ktorí momentálne slúži ako identifikačný predmet zdravotníckeho pracovníka pri prístupe k službám NZIS.

Odpoveď č.4c: Prosíme upresniť, v ktorých prípadoch a na ktorých typoch zariadení má byť potvrdenie prítomnosti pacienta podporované.

Rozpracované v SU -MD -su_127.

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%.

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.

Otázka č. 7:

SP uvádzajú: „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 (pričom SW a OS pre CPE variant a jeho implementácia do mobilného zariadenia lekárov a internetové pripojenie nie je predmetom dodania v rámci tohto Diela)“. Požiadavka uvádza, že SW nie je predmetom dodania Diela v prípade CPE variantu. Aký SW sa tým myslí? Čo presne je CPE variant? Aké ďalšie varianty sú?

Odpoveď č.7:
Z nášho pohľadu sa jedná o zlú kompozíciu vety a áno miernu disproporciu v rámci ponímania označenia CPE, na ktorú je naviazaná Vaša otázka č.2. Predmetom dodania a ani požiadavkou na riešenie nie je operačný systém, ktorý dané mobilné zariadenie obsahuje ani jeho iné SW vybavenie, rovnako zabezpečenie internetového pripojenia nie je súčasťou tohto projektu.
Tak isto vnímame pracovné stanice, cez ktoré bude ZPr. vstupovať do NCIS, že nie sú súčasťou tohto riešenia a dodávky pre tento projekt.

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.

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.

Otázka č.10:

SP, v kap. 5.5 Požiadavky na riešenie Mobilnej autentifikácie, uvádzajú: „ePZP aktuálne obsahuje nasledovné certifikáty a zodpovedajúce súkromné kľúče:

X.509 certifikáty:

• Autentifikačný certifikát zdravotníckeho pracovníka

• Certifikát pre elektronický podpis zdravotníckeho pracovníka

• Jednorazový šifrovací certifikát zdravotníckeho pracovníka“

Otázka: čo sa myslí pod pojmom jednorazový? Aký je životný cyklus takého certifikátu? Kedy vzniká a zaniká? Na aký účel, v akých scenároch je využívaný?

Odpoveď č. 10:

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. Životný cyklus, informácie a účel momentálne používaného certifikátu, je súčasťou aktuálne používaného prihlasovacieho a verifikačného protokolu a preto podrobnejšie informácie nad rámec SU -MD -su_127 nie sme oprávnení poskytovať.

Otázka č.11:

SP, v kap. 5.5 Požiadavky na riešenie Mobilnej autentifikácie, uvádzajú: „Funkcionalita podpisovania a šifrovania, ktorú zabezpečovali zodpovedajúce certifikáty bude riešená pomocou nového centrálneho komponentu nasadeného v NZIS pomocou server-signing technológie“. Uvedené certifikáty ZPr budú teda uložené centrálne Server Signing systéme. SP však nepojednávajú o certifikačnej autorite (CA), ktorá bude dané certifikáty vydávať. Disponuje objednávateľ už príslušnou PKI infraštruktúrou, ktorá bude vydávať certifikáty používateľom Server Signingu a vie túto infraštruktúru poskytnúť pre účely projektu?

Odpoveď č.11:

SP podklady nepojednávajú o certifikačnej autorite, keďže projekt ESO1-D je v plnej kompetencií zadávateľa t.j. NCZI a ako verejný obstarávateľ riešenia berieme ako samozrejmosť, že pre dodania plnohodnotného riešenia je samozrejmosťou, že už patričnou infraštruktúrou disponujeme.

eZdravie má vlastnú PKI infraštruktúru a ak SU -MD -su_127 neurčila inak, je použiteľná na zámery tohto projektu.

Otázka č.12:

SP v kap. 5.2 uvádzajú požiadavku: „V rámci etapy Testovanie prebehne najneskôr v 10. mesiaci od nadobudnutia účinnosti Zmluvy ukončenie testovania PoC (CPE, MKAM-SW a Serverové riešeni).“ Čo sa v tomto prípade myslí pod serverovým riešením? Žiadame upresniť predmet a ciele PoC a upresniť v rámci SP zadanie na jeho realizáciu.

Odpoveď č.12:

Serverové riešenie, je popísané v SU -MD -su_127 tak ako v kapitole 5. Požiadavky na dodanie riešenia k Projektu. SU -MD -su_127: „Z pohľadu používateľov nie sú zmeny zásadné, výhodou je, že karta ePZP nebude musieť byť vložená v čítačke celý čas a pribudne možnosť prihlásenia sa do systému eZdravie aj cez mobilné zariadenie. Rovnako štúdia predpokladá, že vzhľadom na vývoj mobilných služieb, prístup do eZdravie prostredníctvom mobilného zariadenia budú využívať aj takí ZPr, ktorí nepracujú v teréne.“

Predmetom a cieľmi PoC je vypracovanie detailnej funkčnej, technickej a bezpečnostnej špecifikácie ako podklad pre budúce riešenie. Detailný popis požiadavky pre riešenia a vypracovanie PoC sa nachádza v požiadavke číslo tri. (P3). Predmetom a cieľmi PoC sa ďalej zaoberajú požiadavky P3, P21, P70, P74, P81, P82 a P87.

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.

Otázka č.14:

Požiadavka SP č. P94 stanovuje požiadavku „na monitoring a sledovanie chýb koncových zariadení a komponentov či aplikácií ZPr s centrálnym zberom a vyhodnocovaním“.

• Aké „zariadenia a komponenty či aplikácie ZPr“ má obstarávateľ na mysli?

Odpoveď č.14:

Zariadenia - časť otázky zodpovedané v otázke č.2, komponenty a aplikácie súvisiace s vykonávaním autentifikácie a autorizácie. Ide o monitoring všetkých zariadení komunikujúcich s NZIS.

Otázka č.15:

Požiadavka P98, bod 1 „Prepojenie na centrálny portál CMS (integrácia)“ – skratka CMS nie je vysvetlená.

Odpoveď č.15:

Content management systém, skr. CMS: Systém (softvér), ktorý manažuje (riadi), t.j. spravuje, archivuje a pod. a často aj pomáha zostavovať obsah a dáva tento obsah k dispozícii na prezentovanie, a to nie nevyhnutne len na web; "obsahom" sa myslí ľubovoľný elektronický obsah, t.j. záznamy, dáta, metadáta, dokumenty, webové stránky, obrázky, zvukové súbory a pod. V danej požiadavke myslené interné NCZI CMS – IBM Servicedesk.

Otázka č.16:

Požiadavka P98, bod 5 „predmetom nie je dodávka licencií pre softvér a agentov na koncové systémy a zariadenia umiestnené alebo inštalované na pracovisku ZPr“ – má objednávateľ k dispozícii už zakúpené licencie pre softvér a agentov pre koncové systémy a zariadenia? O aký softvér a agentov sa jedná.

Odpoveď č. 16:

Koncovými zariadeniami a v tomto prípade rozumejú "pracovná stanica" na ktorom bude ZPr. vidieť výstup z NZIS a "mobilné zariadenie ZPr." slúžiace na autorizáciu a autentifikáciu daného ZPr., licencie a softwér na týchto zariadeniach nie sú súčasťou ani štúdie ani požiadavkou v rámci dodávky riešenia v tohto projektu. Tak isto, objednávateľ nedisponuje takýmto druhom monitoringu a preto nie sú k dispozícii žiadne SW licencie a agenty. Tento projekt má riešiť podľa požiadaviek monitoring tohto typu a preto je potrebné navrhnúť riešenie zo strany dodávateľa.

Otázka č.17:

V kapitole 5.5 časť P64 je uvedené „prihlásenie sa na registračný portál (využitie SAML autentifikačného tokenu)“ avšak v časti P66 je uvedené “... eZdravie z mobilných zariadení bude nevyhnutná autentifikácia prístupovým tokenom. Prístupový token bude získavaný z

novej OAuth služby eZdravie a na jeho získanie bude nevyhnutné sa autentifikovať z mobilného autentifikačného zariadenia...“ a „... Služby riešenia API rozhrania je potrebné technologicky navrhnúť tak, aby boli využiteľné mobilnými zariadeniami bez ePZP (preferujeme REST) s využitím OAuth autentifikácie a umožňujúce vzdialené podpisovanie správ určených pre zápis,....“

Prosíme upresniť súvis SAML autentifikačného tokenu v súvislosti s ďalej uvedenou OAuth autentifikáciou.

Odpoveď č.17:

SAML autentifikačný token bude používaný pre vytvorenie/registráciu konta na mobilnom zariadení s NZIS v nadväznosti na OAuth autentifikáciu, ktorá bude používaná na komunikáciu cez mobilné rozhranie. Našim cieľom bolo zadefinovať pre budúce riešenie nutnosť nepoužiť rovnaký protokol na registráciu a zároveň na prihlasovanie sa do aplikácie. Rovnako ako pri iných odpovediach, chceme poukázať na to, že pojednávame o požiadavkách na riešenie a je potrebné ich technologicky navrhnúť. Návrh úspešného uchádzača, či už v podobe vyššie opísaného riešenia alebo obdobného mechanizmu, bude musieť samozrejme prejsť cez naše security oddelenie.

Otázka č.18:

V kapitole 5.7, časť P87 je uvedené „... CPE musí zabezpečiť trusted execution environment pomocou zabezpečenia celej reťaze hardware – firmware – operačný systém – aplikácia, napr. pomocou mechanizmu secure boot alebo obdobného mechanizmu....“. Je zadávateľovi zrejmé, že takúto požiadavku spĺňa z pohľadu operačného systému iba MS Windows a hardvér s TPM čipom?

Odpoveď č.18:

Zadávateľ v rámci požiadavky pre riešenie sieťovej vrstvy definoval trusted execution environment a to napríklad pomocou secure boot alebo obdobného mechanizmu. Zadávateľ má za to, že secure boot chain (alebo jemu obdobný mechanizmus) technológia je dostupná a implikovaná tak pre Android aj pre iOS.