Otázka č. 1:

Obstarávateľ vyžaduje kompatibilitu riešenia s jeho infraštruktúrou (kubernetes kontajnery a uvádza zoznam operačných systémov). Pre jednoznačnosť žiadame o potvrdenie, že licencie/subscription pre samotnú kontajnerizačnú platformu a OS nie sú súčasťou dodávky. (Referencia: Príloha č. 18 - Katalóg požiadaviek - CEP, REQ_PR_26).

Odpoveď č. 1:

Ak uchádzač vo svojom riešení potrebuje softvér/softvérové prvky, ktoré nie sú súčasťou prierezových požiadaviek verejného obstarávateľa (napríklad OS Windows alebo špecifický aplikačný server) je potrebné, aby licencie, vyžadované na prevádzku týchto softvérových prvkov boli súčasťou dodávaného riešenia a ocenené v Štruktúrovanom rozpočte zákazky. Súčasti, ako kontajnerizačné a virtualizačné platformy v rozsahu definovanom vo zverejnených dokumentoch/prílohách k súťažným podkladom, sú dostupné v existujúcom alebo pripravovanom prostredí verejného obstarávateľa.

Licencie/subscription kontajnerizačnej platformy nie sú súčasťou dodávaného riešenia. Koncepčná architektúra infraštruktúry je súčasťou dokumentu Prístup k projektu, zverejnenom na link-u: Verejné pripomienkovanie k pripravovanému projektu Modernizácia Platformy pre rozvoj a riešenie prioritných životných situácií (SVK 3.0 stream 4) v časti „Projektová dokumentácia SVK 3.0 stream 4“.

Otázka č. 2:

Obstarávateľ požaduje poskytnutie APV, vrátane ,,zabezpečenia, aby zhotovené APV poskytovalo automatizovaný monitoring SLA parametrov dodaných koncových a aplikačných služieb, ak relevantné". Je požadované aj dodanie SW pre vizualizáciu týchto parametrov, alebo postačuje poskytnutie monitorovacieho rozhrania (API), ktoré Obstarávateľ začlení do svojich existujúcich systémov? (Referencia: Súťažné podklady, s. 7)

Odpoveď č. 2:

APV pre vizualizáciu nie je verejným obstarávateľom požadované. Poskytnutie rozhrania a možnosti replikovania / streamovania týchto informácií je pre verejného obstarávateľa postačujúce.

Otázka č. 3:

V rámci požiadavky ,,Riešenie poskytne remote sealing aj s využitím SAM (signature activation module) pre HSM a na potrebnej úrovni zabezpečenia autentifikácie." je potrebné dodržať kompatibilitu s konkrétnym typom SAM? (Referencia: Príloha č. 18 - Katalóg požiadaviek - CEP, REQ_CEP_21)

Odpoveď č. 3:

Verejný obstarávateľ má zakúpené konkrétne HSM moduly typu nShield Solo XC od výrobcu Entrust, ktoré plánuje využiť v rámci infraštruktúry Centrálnej elektronickej podateľne 3.0. Verejný obstarávateľ zároveň plánuje obstarať rozširujúci SAM modul k týmto HSM modulom, konkrétne Qualified Signature and Seal Creation Device (QSCD) Entrust Signature Activation Module (predpokladane verzia 1.0.4).

Otázka č. 4:

Obstarávateľ požaduje dodržanie kompatibility s rôznymi historickými formátmi podpisov (ZEPf, XAdES_ZEP), vo formátoch k rôznej účinnosti. Ďalej požaduje kompatibilitu s rôznymi atypickými situáciami. Poskytne pre tieto prípady príslušné testovacie dáta? (Referencia: Príloha č. 18 - Katalóg požiadaviek - CEP, REQ_CEP_14, REQ_CEP_23, REQ_CEP_52.)

Odpoveď č. 4:

Verejný obstarávateľ v rámci súčinnosti poskytne budúcemu dodávateľovi testovacie vzorky, ktoré má k dispozícii pre rôzne historické formáty a atypické situácie, pre ktoré požaduje dodržanie kompatibility. V prípade, že verejný obstarávateľ nebude vedieť poskytnúť budúcemu dodávateľovi testovaciu vzorku (napríklad vzhľadom na nemožnosť upravovať údaje v produkčných TSL), verejný obstarávateľ takúto situáciu popíše vrátane možnosti a podmienok realizácie testovania.

Otázka č. 5:

Obstarávateľ vyžaduje „realizáciu minimálne dvoch zmlúv, ktorých predmetom bolo poskytovanie služieb podpory prevádzky informačného systému poskytujúceho pečatenie elektronických dokumentov kvalifikovanou elektronickou pečaťou v mene minimálne 50 rôznych právnych subjektov (organizácií) a zároveň poskytovanie funkcie prevodu na archívnu formu PDF s minimálne 500 000 volaniami aspoň v jednom kalendárnom mesiaci." Túto požiadavku považujeme za diskriminačnú a neprimeranú.

Máme za to, že ak uchádzač poskytuje napríklad služby vzdialeného podpisu, je rovnako, ak nie viac kvalifikovaný, ako ak poskytuje služby pečatenia, nakoľko v prípade vzdialeného podpisu je vyžadovaný vyšší stupeň kontroly nad podpisovacím kľúčom. Túto požiadavku považujeme za neprimeranú aj vzhľadom na počet subjektov v SR, ktoré vykonávajú pečatenie pre viac ako 50 organizácií a majú na to dve zmluvy.

Ďalej máme za to, že odbornú spôsobilosť uchádzača nijako nezvyšuje to, či služby podpory prevádzky na pečatenie kvalifikovanou elektronickou pečaťou a na prevod PDF do archívnej formy poskytuje v rámci jednej zmluvy („a zároveň") alebo v rámci rôznych zmlúv. Obzvlášť v kontexte toho, že ide o služby podpory, nie samotnú implementáciu. (Referencia: SP CEP 3.0 NASES, Technická a odborná spôsobilosť 3.1 d)

Požiadavku navrhujeme odstrániť alebo upraviť v súlade s vyššie uvedenými pripomienkami.

Odpoveď č. 5:

Verejný obstarávateľ vzhľadom na predmet zákazky „Centrálna elektronická podateľňa 3.0" t. j. centrálny komponent verenej správy, ktorého jednou z kľúčových funkcionalít je pečatenie elektronických dokumentov kvalifikovanou elektronickou pečaťou, trvá na požiadavke na referenciu tak, ako je uvedená v súťažných podkladoch.

Požiadavku na referenciu môže uchádzač dokladovať aj zmluvami, realizovanými v rámci v iných štátov.

Otázka č. 6:

Obstarávateľ pre pozíciu ,,Kľúčový expert č. 3 - business analytik'' požaduje ,, minimálne jedna (1) profesionálna praktická skúsenosť v oblasti analýzy a návrhu automatizovaných procesov v elektronickej podateľni prevádzkovanej podľa § 10 odsek 2 alebo odsek 14 zákona č. 305/2013 Z. z. (zákon o e-Governmente) alebo obdobnej legislatívy v iných štátoch, pričom elektronická podateľňa poskytuje pečatenie elektronických dokumentov kvalifikovanou elektronickou pečaťou v mene min. 50 rôznych právnych subjektov (organizácií)". Túto požiadavku považujeme za diskriminačnú a neprimeranú.

V zmysle argumentácie vyššie máme za to, že má skúsenosti v oblasti analýzy a návrhu služieb vzdialeného podpisu, je rovnako, ak nie viac kvalifikovaný, ako ak poskytuje služby pečatenia, nakoľko v prípade vzdialeného podpisu je vyžadovaný vyšší stupeň kontroly nad podpisovacím kľúčom. Túto požiadavku považujeme za neprimeranú aj vzhľadom na počet subjektov v SR, ktoré vykonávajú pečatenie pre viac ako 50 organizácií a majú na to dve zmluvy. (Referencia: SP CEP 3.0 NASES, Technická a odborná spôsobilosť 3.2)

Odpoveď č. 6:

Verejný obstarávateľ vzhľadom na predmet zákazky „Centrálna elektronická podateľňa 3.0" t. j. centrálny komponent verenej správy, ktorého jednou z kľúčových funkcionalít je pečatenie elektronických dokumentov

kvalifikovanou elektronickou pečaťou, trvá na požiadavke na praktickú skúsenosť tak, ako je uvedená v súťažných podkladoch.

Požiadavku na praktickú skúsenosť môže uchádzač dokladovať aj zmluvami, realizovanými v rámci v iných štátov.

Verejný obstarávateľ má za to, že aj v rámci Slovenskej republiky existujú orgány verejnej moci (riadiace orgány, VÚC a pod.), ktorých elektronické podateľne spĺňajú parametre tejto požiadavky, a z tohto dôvodu nepovažuje požiadavku za diskriminačnú.

Otázka č. 7:

Obstarávateľ pre pozíciu „Kľúčový expert č. 6 – špecialista na bezpečnosť IT / Bezpečnostný manažér" kombinuje viacero špecializovaných rolí, a to požiadavkou na predloženie certifikátov a odborných skúseností v troch rôznych oblastiach – bezpečnosti informačných systémov (CISSP, CISM, CISA, ISO27001), ochrany osobných údajov (DPO) a zabezpečenia kontinuity podnikania (BCM). Týmto vzniká potreba kombinovať tri vysoko špecializované oblasti do jednej osoby.

Oddelenie týchto rolí nie je len bežné, ale z viacerých dôvodov sa ako best practice často výslovne neodporúča. Ich kombinovanie môže viesť k potenciálnym konfliktom záujmov, najmä medzi požiadavkami na ochranu osobných údajov (ako vyžaduje rola DPO) a opatreniami v oblasti kybernetickej bezpečnosti (ako vyžaduje rola CISM alebo CISSP), čo môže spôsobovať konflikt pri rozhodovaní a zníženie objektivity.

Pre dosiahnutie rovnováhy medzi ochranou údajov a správnou implementáciou bezpečnostných opatrení môže byť potrebné nezávislé posúdenie, čo je v prípade jednej osoby ťažko dosiahnuteľné. Namiesto spájania týchto rolí je efektívnejšie a flexibilnejšie rozdeľovať tieto zodpovednosti medzi viacerých odborníkov, ktorí sa môžu zamerať na konkrétnu oblasť a zabezpečiť kvalitný výkon.

Požiadavka, aby jedna osoba mala všetky tieto certifikáty a skúsenosti, je neprimeraná a môže viesť k preťaženiu jednotlivca, ktorý nebude schopný efektívne vykonávať všetky tieto úlohy. Tento prístup môže mať negatívny vplyv na kvalitu služieb poskytovaných v rámci verejného obstarávania.

Navrhujeme, aby sa požiadavka na Kľúčového experta č. 6 upravila a rozdelila na samostatné role pre každú z uvedených oblastí (IT bezpečnosť, ochrana osobných údajov, kontinuita podnikania). Tým sa zabezpečí vyššia kvalita poskytovaných služieb a predíde sa preťaženiu jednotlivca, čo by mohlo negatívne ovplyvniť výkonnosť a efektívnosť celého projektu.

Tento prístup zároveň zvýši transparentnosť verejného obstarávania, keďže sa umožní širšiemu okruhu odborníkov prihlásiť sa na jednotlivé špecializované oblasti, čím sa podporí konkurencia a zlepší kvalita dodaných služieb. (Referencia: SP CEP 3.0 NASES, Technická a odborná spôsobilosť 3.2)

Odpoveď č. 7:

Kľúčový expert č. 6 – špecialista na bezpečnosť IT / Bezpečnostný manažér – má byť zastúpený minimálne jednou osobou za stranu dodávateľa diela.

Verejný obstarávateľ v súťažných podkladoch uviedol, že každý kľúčový expert má byť zastúpený minimálne jednou fyzickou osobou. Podmienky účasti majú za cieľ zabezpečiť dosiahnutie výberu takého dodávateľa, ktorý za vynaložené prostriedky poskytne najlepšie a najefektívnejšie plnenie predmetu zákazky. Z našich skúseností, týkajúcich sa aplikácie zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a prislúchajúcej vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, resp. jej novelizovanej verzie – vyhlášky NBÚ č. 264/2023, ktorou sa mení a dopĺňa vyhláška NBÚ č. 362/2018 Z. z., máme za to, že požiadavka na Kľúčového experta č. 6 – špecialista na bezpečnosť IT / Bezpečnostný manažér je pre nás relevantná pre naplnenie cieľov a predmetu nášho projektu, ktoré sú popísané v Opise predmetu zákazky a Katalógu požiadaviek v súlade so znením Zmluvy o poskytnutí prostriedkov mechanizmu na podporu obnovy a odolnosti č. 929/2024 a podpornou dokumentáciou k tejto zmluve (Produktový zoznam požiadaviek, Plán práce projektového tímu).

Koncentrovaná požiadavka pri Kľúčovom expertovi č. 6 na platný certifikát v oblasti ochrany osobných údajov (DPO) a na platný certifikát v oblasti zabezpečenia kontinuity funkčnosti systému Business Continuity Manager (BCM) vyplýva z predpokladu verejného obstarávateľa, že dodanie diela „Centrálna elektronická podateľňa 3.0“ môže byť realizované aj v časovej tiesni vzhľadom na potrebu splnenia míľnika programu Slovensko 3.0 a dodanie požadovanej funkcionality pre použitie v životných situáciách orgánmi verejnej moci. V rámci zrealizovania predmetu zákazky je kľúčové, aby dodávateľ disponoval kvalifikovaným expertom – špecialistom na bezpečnosť IT / Bezpečnostným manažérom, ktorý chápe komplexnosť dodávaného diela a je kompetentný zvládnuť náročné úlohy modelovania systému požadovanej náročnosti integrácie na systémy ÚPVS v kontexte nielen ochrany osobných údajov ale aj zabezpečenia kontinuity prevádzkovaných služieb a teda verejný obstarávateľ na základe vyššie uvedeného má za to, že stanovené podmienky účasti na pozíciu kľúčového experta č. 6 – špecialista na bezpečnosť IT / Bezpečnostný manažér sú primerané danej pozícii.