

Expert č. 1 - expert pre serverové technológie

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti navrhovania, inštalácie a konfigurovania a podporných služieb serverových technológií v pozícii experta pre serverové technológie; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát v oblasti navrhovania, inštalácie a konfigurovania ponúkaných serverových riešení.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosti a spôsobilosť s implementáciou serverovej infraštruktúry. Expert musí preukázať dostatočné profesionálne praktické skúsenosti v predmetnej oblasti, keďže bude z pohľadu kvality plnenia predmetu zákazky zodpovedať za kompletný návrh a realizáciu serverovej architektúry a jej integráciu do existujúceho prostredia, z čoho vyplýva aj požiadavka na predloženie certifikátu preukazujúceho spôsobilosť experta.

Expert č. 2 - expert pre technológie SAN prepínače

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti navrhovania, inštalácie a konfigurovania a podporných služieb v pozícii experta pre SAN prepínače; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát v oblasti navrhovania, inštalácie a konfigurovania ponúkaných SAN prepínačov.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosti a spôsobilosť s implementáciou a následnými podpornými službami po prevzatí implementácie obstarávateľom.

Expert musí preukázať dostatočné profesionálne praktické skúsenosti v predmetnej oblasti, keďže bude z pohľadu kvality plnenia predmetu zákazky zodpovedať za kompletný návrh a integráciu do existujúceho prostredia, z čoho vyplýva aj požiadavka na predloženie certifikátu preukazujúceho spôsobilosť experta.

Expert č. 3 - expert pre diskové polia

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti navrhovania, inštalácie a konfigurovania a podporných služieb diskových polí v pozícii experta pre diskové polia; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát v oblasti navrhovania, inštalácie a konfigurovania ponúkaných diskových polí.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosti a spôsobilosť s implementáciou diskových polí. Expert musí preukázať dostatočné profesionálne praktické skúsenosti v predmetnej oblasti, keďže bude z pohľadu kvality plnenia predmetu zákazky zodpovedať za kompletný návrh a realizáciu diskových polí a ich integráciu do existujúceho prostredia, z čoho vyplýva aj požiadavka na predloženie certifikátu preukazujúceho spôsobilosť experta.

Expert č. 4 - expert pre oblasť sieťovej infraštruktúry

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti navrhovania, inštalácie a konfigurovania a podporných služieb sieťovej infraštruktúry v pozícii experta pre sieťové infraštruktúry; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát na úrovni CCIE Routing and Switching alebo ekvivalent v oblasti návrhu, implementácie, validácie a riešenia chýb LAN a WAN existujúcej sieťovej infraštruktúry (CISCO).

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosti a spôsobilosť s implementáciou sieťovej infraštruktúry. Expert musí preukázať dostatočné profesionálne praktické skúsenosti v predmetnej oblasti, keďže bude z pohľadu kvality plnenia predmetu zákazky zodpovedať za integráciu do existujúceho prostredia, z čoho vyplýva aj požiadavka na predloženie certifikátu preukazujúceho spôsobilosť experta.

Expert č. 5 – expert pre oblasť bezpečnostnej sieťovej infraštruktúry (firewall)

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti bezpečnostnej sieťovej infraštruktúry v pozícii experta pre bezpečnostnú sieťovú infraštruktúru; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát v oblasti bezpečnostnej sieťovej infraštruktúry na úrovni CCNP Security, alebo ekvivalent pre existujúce riešenie bezpečnostnej sieťovej infraštruktúry (CISCO).

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosť navrhnuť a implementovať bezpečnostnú sieťovú infraštruktúru. Expert musí preukázať dostatočné profesionálne praktické skúsenosti v predmetnej oblasti, keďže bude z pohľadu kvality plnenia predmetu zákazky zodpovedať za integráciu do existujúceho prostredia, z čoho vyplýva aj požiadavka na predloženie certifikátu preukazujúceho spôsobilosť experta.

Expert č. 6 - expert pre oblasť serverovej virtualizácie

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti virtualizácie serverov v pozícii experta pre serverovú virtualizáciu; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát v oblasti navrhovania, inštalácie, konfiguráciu a administráciu existujúcej serverovej virtualizácii VMware na úrovni VMware Certified Professional Data Center Virtualization 2021 alebo ekvivalent.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosť navrhnuť, implementovať, konfigurovať a poskytovať podporné služby pre serverovú virtualizačnú technológiu.

Expert č. 7 – expert pre oblasť operačných systémov Microsoft

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 2 profesionálne praktické skúsenosti v oblasti inštalácie, konfigurácie a administrácie existujúcich riešení Microsoft Windows Server systémov; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,

2) získaný a platný certifikát v oblasti návrhu, inštalácie, konfiguráciu a administrácie existujúcich riešení Microsoft Windows Server systémov na úrovni:

1 expert s certifikáciou Microsoft Certified Solutions Expert Core Infrastructure

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosť navrhnuť, implementovať, konfigurovať a poskytovať podporné služby pre operačné systémy Microsoft.

Expert č. 8 - expert pre oblasť zálohovania

Expert preukáže svoju odbornú spôsobilosť nasledovne:

1) minimálne 2 profesionálne praktické skúsenosti v oblasti inštalácie, konfigurácie a administrácie existujúceho zálohovacieho systému Veeam; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,

2) získaný a platný certifikát v oblasti návrhu, inštalácie, konfiguráciu a administrácie existujúceho zálohovacieho systému Veeam na úrovni Veeam Certified Architect alebo Veeam Certified Engineer alebo ekvivalent.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosť navrhnuť, implementovať, konfigurovať a poskytovať podporné služby pre zálohovací systém.

Expert č. 9 - expert pre oblasť zálohovania = Disaster recovery

Expert preukáže svoju odbornú spôsobilosť nasledovne:

1) minimálne 2 profesionálne praktické skúsenosti v oblasti inštalácie, konfigurácie a administrácie existujúceho systému HPE StoreOnce, túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,

2) získaný a platný certifikát v oblasti návrhu, inštalácie, konfiguráciu a administrácie existujúceho systému na úrovni HPE StoreOnce 3XXX and 5XXX Service and Solution Qualification - alebo certifikát HPE Master Accredited Solutions Expert - Storage Solutions Architect V3 alebo ekvivalent.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosť navrhnuť, implementovať, konfigurovať a poskytovať podporné služby pre systém HPE StoreOnce.

Expert č. 10 – manažér zodpovedný za implementáciu projektu

Expert preukáže svoju odbornú spôsobilosť nasledovne:

1) minimálne 2 profesionálne praktické skúsenosti v riadení projektov v oblasti informačno-komunikačných technológií; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,

2) získaný a platný certifikát PRINCE 2 Practitioner alebo IPMA B alebo PMI alebo PMP a ITIL Foundation certifikát pre IT služby na odbornú spôsobilosť pre riadenie projektov alebo ekvivalentný certifikát.

Verejný obstarávateľ akceptuje aj rovnocenné certifikáty vydané certifikačnými organmi z členských štátov EÚ.

Zdôvodnenie: Verejný obstarávateľ požaduje preukázať schopnosti a spôsobilosť s riadením projektu.

Expert č. 11 – Hlavný expert pre oblasť bezpečnosti IT a ochrany osobných údajov

– osoba zodpovedná za činnosti zabezpečujúce ochranu IS a jeho zložiek proti bezpečnostným hrozbám a nepriateľským aktivitám, ktorých cieľom je krádež informácií, financií, zničenie dát, znefunkčnenie činnosti IS, prípadne iné činnosti s negatívnym dopadom, realizované prostredníctvom IS alebo na IS

Expert preukáže svoju odbornú spôsobilosť nasledovne:

- 1) minimálne 5 ročnú odbornú prax/skúsenosti v oblasti bezpečnosti informačných technológií a ochrany osobných údajov v nich v pozícii špecialistu pre oblasť bezpečnosti. Túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
- 2) získaný a platný certifikát pre oblasť bezpečnosti, napr. CISA a CISM, CISSP alebo ekvivalent daného certifikátu od inej akreditovanej autority (preukáže platným certifikátom alebo odkazom na URL adresu na register akreditovanej autority, kde je možné overiť platnosť certifikácie/certifikátu)

Podmienky účasti:

Referencie na 2 realizované zákazky v porovnateľnom rozsahu ako je hodnota zákazky

Osobné postavenie ... v zmysle zákona

Ekonomická a finančná spôsobilosť = zábezpeka podľa rozhodnutia obstarávateľa

Technická a odborná spôsobilosť = referencie, experti

Certifikát/potvrdenie od výrobcu preukazujúci schopnosť poskytnúť služby spojené s inštaláciou a zároveň dodávkou záručného a pozáručného servisu ponúkaných zariadení = obchodné a servisné partnerstvo s výrobcom/výrobcami ponúkaných technológií

Certifikát systému riadenia kvality podľa ISO 9001.

Certifikát systému manažmentu bezpečnosti informácií ISO 27001.

Certifikát Systém environmentálneho manažmentu ISO 14001.

Certifikát Systém manažérstva BOZP ISO 45001

Certifikát ISO 50001 pre oblasť Riadenie projektov, Helpdesk, Vzdialená správa a dohľad.

Poistka .. vo výške podľa rozhodnutia obstarávateľa

Definícia krajiny :

1. Pre minimalizáciu rizík, súvisiacich s geopolitickými faktormi, verejný obstarávateľ požaduje, aby všetky hardvérové komponenty pochádzali od výrobcov z jurisdikcií, ktoré sú členmi Európskej únie alebo iných dôveryhodných partnerov EÚ, s cieľom zabezpečiť ochranu prevádzkovanvej IKT infraštruktúry a produkčného prostredia verejného obstarávateľa pred potenciálnymi bezpečnostnými hrozbami, vrátane únikov citlivých informácií mimo Európu.
2. Verejný obstarávateľ preferuje hardvérové komponenty od výrobcov z krajín, ktoré sú:
 - členmi Európskej únie (EÚ) – krajiny, ktoré sú členmi EÚ, sú automaticky považované za dôveryhodné jurisdikcie, keďže podliehajú jednotným pravidlám a bezpečnostným štandardom únie,

- súčasťou Európskeho hospodárskeho priestoru (EHP) – krajiny ako Nórsko, Island a Lichtenštajnsko, ktoré nie sú členmi EÚ, ale sú súčasťou EHP, sú tiež považované za dôveryhodných partnerov, pretože dodržiavajú veľkú časť pravidiel EÚ vrátane bezpečnostných štandardov,
- členmi NATO – členovia Severoatlantickej aliance sú považovaní za strategických partnerov v oblasti bezpečnosti a obrany, vrátane krajín ako USA, Kanada, Spojené kráľovstvo (aj po Brexite), Turecko a ďalších spojencov.
- partnermi EÚ v súlade so schémou Trusted Connectivity EÚ – EÚ vyvíja iniciatívy na rozšírenie dôveryhodných partnerstiev s krajinami, ktoré zdieľajú podobné hodnoty, ako je ochrana osobných údajov, kybernetická bezpečnosť a technologická suverenita. Takými partnermi sú napríklad Japonsko, Južná Kórea, Austrália a Nový Zéland, ktoré majú obchodné a technologické dohody s EÚ,
- partnermi EÚ v súlade s Politikou obchodných dohôd EÚ – krajiny, s ktorými má EÚ uzavreté obchodné dohody, môžu byť považované za dôveryhodných partnerov, pokiaľ dohody obsahujú prvky týkajúce sa ochrany osobných údajov, bezpečnosti a geopolitických rizík. Tieto dohody často zahŕňajú ustanovenia o ochrane proti geopolitickým rizikám.

Oficiálne informácie o partnerstvách a dohodách EÚ je možné čerpať z nasledujúcich zdrojov:

- web stránka Európskej komisie – obsahuje informácie o obchodných dohodách a geopolitických partnerstvách EÚ,
- European External Action Service (EEAS) – agentúra EÚ pre zahraničnú a bezpečnostnú politiku poskytuje aktuálne informácie o strategických partnerstvách,
- Stratégia digitálnej a kybernetickej bezpečnosti EÚ – v tomto dokumente nájdete pravidlá a partnerstvá týkajúce sa digitálnej suverenity a bezpečnosti kritických technológií.