Veřejná zakázka

Jednotný informační systém práce a sociálních věcí – Provozní integrační prostředí

Ev.č.: 498306

Zadavatel veřejné zakázky:

Česká republika – Ministerstvo práce a sociálních věcí

se sídlem Na Poříčním právu 1/376, 128 01 Praha 2

IČO: 00551023

(dále jen „**zadavatel**“ nebo „**MPSV**“)

Dodatečné informace k zadávacím podmínkám č. XVI

dle § 49 odst. 1 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**ZVZ**“).

MPSV, jako zadavatel shora uvedené veřejné zakázky, obdrželo dne 4. 2. 2015 žádost o poskytnutí dodatečných informací k zadávacím podmínkám.

Na níže uvedené dotazy poskytuje zadavatel následující odpovědi:

Dotaz č. 1:

V zadávací dokumentaci a doplňujících dotazech byly opakovaně řešeny otázky týkající se migrace objektů Active Directory do nově navrženého prostředí. Z dosavadního vyplývá, že Zadavatel požaduje:

- vybudovat novou (nebo nové) doménu (nebo domény) Active Directory pro uživatelské objekty, pracovní stanice a servery
- do této domény (nebo do těchto domén) migrovat uživatelské identity a skupiny se zachováním původních SIDů do atributu sIDHistory
- Zadavatel negarantuje možnost získání administrátorských oprávnění pro dodavatele ve zdrojových doménách x1.mpsv.cz až x4.mpsv.cz

Pokud výše uvedené platí současně, nelze migraci v rámci dané technologie realizovat tak, jak požaduje Zadavatel. SIDy objektů lze migrovat pouze v režimu online (propojené domény pomocí vztahu důvěry) a s využitím administrátorských oprávnění ve zdrojové doméně (vyplývá z vysoké úrovně zabezpečení těchto údajů v rámci Active Directory). Export a import SIDů v offline režimu nebo bez administrátorských oprávnění ke zdroji není možný. V tomto případě by byly nově vytvořené objekty v nových doménách vytvořené na základě exportovaných dat bez jakékoli vazby na objekty původní.

Připouští tedy Zadavatel skutečnost, že za současné platnosti všech výše uvedených požadavků, není možné splnit zadání beze zbytku?

Odpověď zadavatele:

Zadavatel poskytne potřebnou součinnost při migraci SID. Pokud Zadavatel nebude schopen zajistit takovou součinnost, nebude se jednat o nesplnění požadavků na straně Uchazeče.

Úvod k dotazům 2 – 4

KONTEXT DOTAZU UCHAZEČE

2.4.2 CERTIFIKAČNÍ AUTORITA A ČIPOVÉ KARTY

Požadavek MPSV je implementace jediné certifikační autority provozované na bázi produktu Microsoft. Certifikační autorita bude určena zejména k vydávání certifikátů:

- Certifikáty pro servery (a aplikace na nich provozované)
- Certifikáty pro uživatele
- Certifikáty pro stanice
- Certifikáty užité pro účely interního elektronického podpisu (případně časového razítka)
- Certifikáty užité pro šifrování elektronické pošty (email)

- Certifikáty užité pro šifrování dokumentů

Certifikáty budou používat algoritmus SHA-2 a budou délky 2048 bitů. Pokud vyplyne z analýzy nutnost zachovat ještě po omezenou dobu certifikáty s algoritmem SHA-1, bude zřízena druhá CA s tímto algoritmem.

Odpovědi na dotazy uchazeče k veřejné zakázce JIS-PIP, Dodatečné informace k zadávacím podmínkám č. 1

Původní dotaz č. 8:

Je požadována jediná CA, která tedy bude zároveň kořenová (self-signed). Předpokládáme, že bude mít např. pro servery aplikovánu politiku automatického vydávání certifikátů a pro uživatele politiku off-line vydávání certifikátů prostřednictvím certifikačních autorit. Může toto Zadavatel potvrdit?

Odpověď zadavatele:

Ano, Zadavatel toto potvrzuje.

Odpovědi na dotazy uchazeče k veřejné zakázce JIS-PIP, Dodatečné informace k zadávacím podmínkám č. 5

Původní dotaz č. 15:

Příloha 6 – Kapitola 2.4.2

Očekává Zadavatel v rámci implementace vybudování nové kořenové Certifikační Autority? Pokud ano, bude požadováno pro ochranu klíče HW ochrana pomocí HSM modulu? Pokud ano, bude požadována implementace kořenové CA z pohledu procesní ochrany na určeném typu HW (PC, fyzický server, virtuální server …)?

Odpověď zadavatele:

Ano, Zadavatel očekává v rámci Implementace vybudování nové kořenové Certifikační Autority

Zadavatel přepokládá využití HSM modulu z důvodu zajištění potřebné bezpečnosti. Umístění kořenové CA (virtuální server, fyzický server) bude výstupem Bezpečnostního projektu.

Původní dotaz č. 18:

Příloha 6 – Kapitola 2.4.2

Jsou stávající CA clusterovány přes obě datová centra? Jaký je přibližně průměrný počet vydaných certifikátů denně?

Odpověď zadavatele:

Ano, stávající CA jsou clusterovány přes obě datová centra. Zadavatel ze stávající statistiky odhaduje průměrný počet vydaných certifikátu denně na 200 ks.

Odpovědi na dotazy uchazeče k veřejné zakázce JIS-PIP, Dodatečné informace k zadávacím podmínkám č. 6

Původní dotaz č. 13:

Má být řešení koncipované tak aby:

a) Splňovalo v maximální možné míře implementované možnej miere implementovanie bezpečné

podnikové certifikační autority?

B) Splňuje podmínky na akreditaci ve smyslu zákona 227/2000 Sb.?

Odpověď zadavatele:

A) Ano

B) Ano

Původní dotaz č. 14:

Má být součástí řešení zdokumentování procesů správy a vydávání certifikátů? Tzn. má být součástí dodávky vypracování „certificate policy" resp. pravidel na výkon certifikačních činností („certificate practice statement")?

Odpověď zadavatele:

Ano

Původní dotaz č. 15:

Má být v rámci řešení implementovaná služba časových razítek (TSA)? (pozn. Microsoft nemá produkt který by implementoval TSA konformní s RFC 3161), řešení je však možné doplnit o produkt třetí strany (komerční resp. FOSS).

Odpověď zadavatele:

Ano, v rámci řešení má být implementována služba časových razítek.

Odpovědi na dotazy uchazeče k veřejné zakázce JIS-PIP, Dodatečné informace k zadávacím podmínkám č. 9

Původní dotaz č. 1:

Příloha 6 – kapitola 2.4.2

V zadání se požaduje vydávání interních časových razítek.

Otázka:

Předpokládá Zadavatel použití svých stávajících nástrojů na generování časových razítek, nebo má

být součástí implementace také dodávka a implementace nástroje generování časových razítek?

Odpověď zadavatele:

Zadavatel odkazuje na odpověď č. 13 v Dodatečných informacích č. V a odpověď č. 15 v rámci Dodatečných informací č. VI.

Původní dotaz č. 2:

Příloha 6

Hardware Security modul – HSM

Otázka:

Předpokládá Zadavatel použití svých vlastních HSM modulů nebo má být součástí implementace také dodávka HSM modulů?

Odpověď zadavatele:

Zadavatel odkazuje na odpověď č.15 Dodatečných informací V.

Konec kontextu dotazu

Z výše uvedených dotazů vyplývají dle názoru uchazeče následující skutečnosti:

a) Původní požadavek zadavatele, vyjádřený v Příloze č. 6 Funkční a technické požadavky k veřejné zakázce JIS-PIP v odstavci 2.4.2 byl následující: **Požadavek MPSV je implementace jediné certifikační autority provozované na bázi produktu Microsoft.**

b) Původní požadavek zadavatele, vyjádřený v Příloze č. 6 Funkční a technické požadavky k veřejné zakázce JIS-PIP v odstavci 2.4.2 požadoval vydávat certifikáty užité pro účely interního elektronického podpisu (případně časového razítka), **nikoli vydávat vlastní časová razítka** (časové razítko není certifikát, certifikát slouží k ověření časového razítka). Požadavek na vydávání časových razítek není v kapitole 2, příloha č. 6 zadávací dokumentace uveden, a současně informace uvedené v kapitole 1 přílohy č. 6 netvoří soubor požadavků kladených na poptávané systémy. Pokud bylo záměrem Zadavatele vydávat časová razítka prostřednictvím certifikační autority provozované na bázi produktu Microsoft, pak tento požadavek ani splnit nelze, neboť příslušná certifikační autorita časová razítka nevydává.

c) V odpovědi na dotaz č. 15 v dokumentu Dodatečné informace k zadávacím podmínkám č. 5 Zadavatel přepokládá využití HSM modulu z důvodu zajištění potřebné bezpečnosti. Tento požadavek není v Zadávací dokumentaci uveden, a tudíž mění a rozšiřuje Zadávací dokumentaci.

d) V odpovědi na dotaz č. 18 v dokumentu Dodatečné informace k zadávacím podmínkám č. 5 Zadavatel upřesňuje, že stávající CA jsou clusterovány přes obě datová centra. Z této odpovědi není jasné, zdali se požaduje vytvořit cluster CA i v novém systému.

Dotaz č. 2:

Potvrzuje Zadavatel změnu zadávacích podmínek rozšířením zadávací dokumentace o požadavek na vybavení certifikační autority provozované na bázi produktů Microsoft o HSM?

Odpověď zadavatele:

Ne, Zadavatel nepotvrzuje změnu zadávacích podmínek.

Zadavatel se dále vyjadřuje k uchazečem uvedeným skutečnostem b) – d):

Ad b):

Zadavatel požaduje v příloze č. 6 – bod 2.4.2 implementaci certifikační autority a uvádí:

Požadavek MPSV je implementace jediné certifikační autority provozované na bázi produktu Microsoft. Certifikační autorita bude určena zejména k vydávání certifikátů:

- *Certifikáty užité pro účely interního elektronického podpisu (**případně časového razítka**)*

Výše uvedeným Zadavatel vznesl požadavek na funkcionalitu časových razítek v rámci vlastní CA. Zadavatel shledává závěr uchazeče za nesprávný, neboť v rámci certifikační autority Microsoft lze zajistit službu časového razítka softwarem třetí strany.

Ad c:

Zadavatel uvedl u otázky číslo 15 Dodatečných informací V, že **předpokládá** využití HSM modulu pro zajištění potřebné bezpečnosti. Zadavatel uvedl pouze předpoklad (nikoliv požadavek). Je na zvážení Uchazeče, zdali z důvodu zajištění potřebné bezpečnosti specifikované v rámci zadávací dokumentaci HSM modul použije nebo využije jiné alternativy (např. ukládání klíčů na šifrovaném úložišti) bez užití HSM modulu.

Ad d:

Zadavatel v odpovědi na dotaz č. 18 Dodatečných informací č. V pouze odpověděl na dotaz Uchazeče směřující ke **stávajícímu řešení CA**, nicméně v rámci zadávací dokumentace není zmíněn požadavek na CA cluster a CA cluster není tedy vyžadován.

Dotaz č. 3:

Potvrzuje Zadavatel, že požaduje cluster certifikačních autorit provozovaných na bázi produktů Microsoft přes obě datová centra?

Odpověď zadavatele:

Zadavatel odkazuje na odpověď č. 2 těchto Dodatečných informací.

Dotaz č. 4:

Potvrzuje Zadavatel změnu zadávacích podmínek rozšířením zadávací dokumentace o požadavek na vydávání časových razítek?

Odpověď zadavatele:

Zadavatel odkazuje na odpověď č. 2 těchto Dodatečných informací.

Úvod k dotazům 5 a 6

V odpovědi na dotaz č. 13 v dokumentu Dodatečné informace k zadávacím podmínkám č. 6 Zadavatel požaduje, aby řešení splňovalo podmínky na akreditaci podle zákona 227/2000 Sb. Uchazeč upozorňuje, že tento nově vznesený požadavek, kromě podstatného rozšíření původních požadavků, má podstatné souvislosti, na které upozorňuje:

a) Splnění podmínek pro akreditaci tvoří komplexní soubor organizačních, personálních, technických, provozních a implementačních činností, jejichž rozsah a náklady jsou podle

zkušeností stávajících akreditovaných poskytovatelů certifikačních služeb srovnatelné s odhadovanou cenou celé zakázky.

b) Akreditovány mohou být pouze kvalifikované služby, což není použitelné pro většinu certifikátů uvedených v požadavku **2.4.2 CERTIFIKAČNÍ AUTORITA A ČIPOVÉ KARTY**

c) MPSV nemůže být akreditováno podle zákona o elektronickém podpisu, neboť nesplňuje požadavky zákona (kromě jiného §10 odst. (2) b).

d) Přímo vykonatelné Nařízení Evropského parlamentu a Rady č. 910/2014, ze dne 23.7. 2014 (tzv. eIDAS) zrušilo směrnici 1999/93/ES, na jejímž základě byl zaveden Zákon o elektronickém podpisu a související legislativa v členských státech EU, speciálně český zákon 227/2000 Sb. v platném znění a související vyhlášky a akreditace kvalifikovaných poskytovatelů certifikačních služeb. Nařízení EIDAS definuje rámec pro tzv. důvěryhodné služby v oblasti identifikace, autentizace, elektronického podpisu, elektronického doručování a ověřování webových stránek, účinnost většiny opatření EIDAS nastává 1. 7. 2016. Požadavek na akreditaci dle zákona 227/2000 Sb. je tudíž pro nový systém irelevantní.

Dotaz č. 5:

Potvrzuje Zadavatel změnu zadávacích podmínek rozšířením zadávací dokumentace, ve smyslu požadavku aby řešení splňovalo podmínky na akreditaci podle zákona 227/2000 Sb.?

Odpověď zadavatele:

Zadavatel uvádí, že došlo vinou nesrozumitelně položeného původního dotazu Uchazeče č. 13 DI VI k mylnému pochopení kontextu dotazu ze strany Zadavatele a následné mylné interpretaci odpovědi Zadavatele Uchazečem. Zadavatel v kontextu otázky a) u otázky b) předpokládal, že jde o dotaz směřující k otázce, zda řešení má být koncipováno tak, aby „Splňovalo v **maximální možné míře** implementované možnej miere implementovanie bezpečné podnikové certifikační autority“ podmínky na akreditaci ve smyslu zákona 227/2000 Sb.

Pro upřesnění - pokud Uchazeč původním dotazem č. 13 DI VI měl na mysli, zda Zadavatel **striktně** požaduje, aby celé řešení „**splňovalo**“ ve smyslu zákona 227/2000 Sb. podmínky pro akreditaci, pak Zadavatel uvádí, že nikoliv.

Dotaz č. 6:

Pokud Zadavatel trvá na dodatečném požadavku, aby řešení splňovalo podmínky na akreditaci podle zákona 227/2000 Sb., přestože Zadavatel nemůže být akreditován a současně zákon 227/2000 nebude od 1. 7. 2016 relevantní, žádáme o doplnění informací, které povinnosti kvalifikovaného poskytovatele certifikačních služeb uvedené v zákonu 227/200. Sb. a ve vyhlášce 378/2006 Sb. požaduje zadavatel splnit?

Odpověď zadavatele:

Vzhledem k odpovědi na dotaz č. 5 těchto dodatečných informací je tento dotaz irelevantní.

Dotaz č. 7:

Příloha č. 6 kapitola 1.2.5.1 Popis zobrazených systémů

- Jakým serverům bude poskytovat vzdálenou správu systém centrální distribuce aplikací?

- Kde jsou tyto servery umístěné?

- Je požadováno, aby tyto servery byly migrovány podobně jako stanice?

- O jaké aplikace, jejichž vzdálenou distribuci má systém zajistit, se jedná?

Odpověď zadavatele:

Zadavatel upozorňuje Uchazeče, že kapitola 1 přílohy č. 6 zadávací dokumentace, ze které ve svém dotazu primárně vychází, pouze poskytuje kontext globální architektury JISPSV za účelem vyjasnění role poptávaného řešení. Požadavky na poptávané řešení jsou sumarizovány v kapitole 2 přílohy č. 6 zadávací dokumentace. Dotaz uchazeče je proto irelevantní.

Dotaz č. 8:

Příloha č. 6 Kapitola 2.4.1.1 Active Directory

- Bude pro migraci umožněno přímé propojení stávajícího a budovaného systému?

- Bude pro potřeby migrace umožněno vytvoření obousměrného vztahu důvěry (trust) s existujícími adresáři AD?

- Bude pro potřeby migrace stanic možné získat přístup úrovně doménového administrátora do zdrojových domén?

- Požaduje zadavatel migrovat uživatelská hesla?

Odpověď zadavatele:

Zadavatel odkazuje na odpověď č. 25 v rámci dodatečných informací č. VI.

Dotaz č. 9:

Příloha č. 6 Kapitola 2.4.1.2 Microsoft Exchange

- V jaké formě budou data poskytnuta?

- Bude možné přímé propojení stávajícího a nově budovaného systému?

- Bude možné pro potřeby migrace exchange mailboxů a veřejných složek získat přístup úrovně exchange ogranization administrators do zdrojové Exchange organizace?

Odpověď zadavatele:

Zadavatel požaduje migraci nezbytných dat, zejména se jedná o obsah datových schránek uživatelů a veřejné složky. Data budou poskytnuta ve formě exportních PST souborů nebo obdobným způsobem.

Zadavatel nemůže garantovat propojení stávajícího a nově budovaného systému.

Zadavatel nemůže garantovat přístup se zmíněnými právy do zdrojové Exchange organizace.

Dotaz č. 10:

Příloha č. 6 Kapitola 2.4.6.1 SCCM – Microsoft System Center Configuration manager

Jaké příslušné dohledové nástroje požaduje zadavatel implementovat a integrovat do JIS?

Odpověď zadavatele:

Zadavatel přepokládá maximální využití Microsoft SCCM. Stanovení příslušných dohledových nástrojů proběhne v rámci Návrhu realizace.

Dotaz č. 11:

Příloha č. 6 kapitola 2.4.6.3 Správa koncových stanic a mobilních zařízení.

Je myšleno rozčleněním systému do jednotlivých částí také jeho fyzické geografické rozčlenění?

Odpověď zadavatele:

Zadavatel považuje položený dotaz za nesrozumitelný, resp. připouštějící rozdílný výklad, proto nelze na Zadavateli požadovat, aby na něj kvalifikovaně odpověděl. Zadavatel nerozumí v kontextu otázky pojmu fyzické geografické rozčlenění.

Dotaz č. 12:

Příloha č. 6 kapitola 2.5.1.19 Kontaktní místo Uchazeče.

- Předpokládá zadavatel integraci aplikací Service Desk Zadavatele a Uchazeče?

- Pokud ano, jakou aplikaci pro Service Desk Zadavatel provozuje?

Odpověď zadavatele:

Zadavatel odkazuje na odpověď č. 20 Dodatečných informací XII.

Dotaz č. 13:

Příloha č. 6, kapitola 2.3.1 Obecné požadavky

- Je požadována implementace File a Print serverů ve vzdálených lokalitách?

- Pokud ano, ve kterých lokalitách budou provozovány, a je požadována implementace nových nebo budou migrovány stávající?

- V jakém prostředí tyto servery poběží (virtuální nebo fyzický server)?

Odpověď zadavatele:

Ne, Zadavatel nepožaduje implementaci File a Print serverů ve vzdálených lokalitách.

Dotaz č. 14:

Příloha 6, kapitola 2.4.6.3 Správa koncových stanic a mobilních zařízení.

- Je požadována implementace WSUS serverů ve vzdálených lokalitách?

- V případě, že ano, budou implementovány nové nebo použity stávající a v jakém prostředí poběží (virtuální nebo fyzický server)?

- V kolika lokalitách budou umístěny a jaký bude celkový počet WSUS serverů?

Odpověď zadavatele:

Zadavatel nepředjímá rozmístění instalace WSUS serverů, to je součástí Návrhu realizace s přihlédnutím k ostatním podmínkám (počet stanic v dané lokalitě, kapacita komunikační infrastruktury) a návrhu architektury Uchazeče.

Dotaz č. 15:

Bude umožněno pro zajištění vysoké dostupnosti poskytovaných služeb využívat vysokou dostupnost virtualizovaných serverů včetně jejich disků v rámci i mezi oběma datovými centry (Hyper-V live migration a replikace na úrovni diskového pole)?

Odpověď zadavatele:

Zadavatel nepředjímá návrh architektury Uchazeče.

V Praze dne 10. 2. 2015