Dodatečné informace č. 20

Název veřejné zakázky:	**Dodávka a implementace informačního systému pro dohled nad hazardními hrami**
Uveřejněna:	Ve Věstníku veřejných zakázek dne 1.4.2016 pod evidenčním číslem 520768 a v Úředním věstníku Evropské unie pod značkou 2016/S 067-117416
Zadavatel:	Česká republika – Ministerstvo financí
Sídlo:	Letenská 15/525, Praha 1
IČO:	00006947
DIČ:	CZ00006947
Osoba oprávněná jednat za zadavatele:	Dipl.-Ing. Miroslav Hejna

Zadavatel v souladu s ustanovením § 49 zákona 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, poskytuje tyto dodatečné informace:

Dotaz č. 1

Zadávací dokumentace (Příloha smlouvy č. 1 „Technická dokumentace") specifikuje v „Tabulce 2 - Popis *elementů diagramu" v kapitole „4.1 Diagram komponent" (strana 14) modul „IdM provozovatelů" následovně:*

> *Modul, který slouží ke správě identit (IdM, Identity Management) provozovatelů.*
>
> *Pro přístup do Veřejného portálu budou provozovatelé využívat autentizaci pomocí systému datových schránek (ISDS).*
>
> *K zajištění důvěrnosti, integrity a nepopiratelnosti komunikace systému provozovatele s AISG (vystavené služby registrace, ztotožnění hráče atd., předávání herních dat) bude sloužit systém založený na správě a distribuci veřejných klíčů (PKI, Public Key Infrastructure).*

Tato dále neupřesněná specifikace vnáší do zadání nejasnosti a neurčitosti vedoucí k následujícím dílčím dotazům:

1. *Jaký je zadavatelem požadovaný identitní model poskytovatelů?*

Specifikace uvádí, že modul „slouží ke správě identit (IdM, Identity Management) provozovatelů.". Z dané specifikace ani z dalšího textu není zřejmá zadavatelem požadovaná podoba identitního modelu „Poskytovatelů" (ve smyslu provozovatelů hazardních her). Z textů zadávací dokumentace lze dovozovat, že předmětem správy jsou jednotliví poskytovatelé, kdy poskytovatelem hazardní hry může být jen Česká republika, nebo akciová společnost se sídlem v České republice, jiném členském státě Evropské unie nebo ve státě, který je smluvní stranou Dohody o Evropském hospodářském prostoru.

Zadávací dokumentace již nestanoví zejména, zda je model:

a. *Fakticky jednoúrovňový: jednomu poskytovateli (jakožto entitě) je přiřazena právě jedna identita (1:1). V technické rovině disponuje Provozovatele právě jedním účtem pro veškeré své přístupy k AISG.*
b. *Plně dvouúrovňový: jednomu poskytovateli (jakožto entitě) může být přiřazeno více identit (1:N). V technické rovině disponuje Provozovatel více účty pro přístup k AISG - např. pro různé systémy jednoho poskytovatele.*
c. *Víceúrovňový model: např. jednomu poskytovateli (jakožto entitě) může být přiřazeno více identit s tím, že každá identita může disponovat více sadami*

atributů (1:N:M). V technické rovině disponuje Provozovatel více identitami (např. pro různé systémy jednoho poskytovatele), z nichž každá může k AISG přistupovat více účty.

d. *Případně jiný typ modelu.*

Zadávací dokumentace též jednoznačně nestanoví, zda je v případě dvou a víceúrovňových modelů identitou informační systém provozovatele nebo též případně jiný subjekt (např. fyzická osoba v pozici pracovníka či statutárního zástupce provozovatele např. zasílající žádost/podnět/či oznámení do systému prostřednictvím ISDS).

Odpověď na dotaz 1/1:

Výše je uveden výraz poskytovatelé, který je v tomto kontextu nepřesně uveden. Nový zákon o hazardních hrách v § 6 stanovuje pojem „Provozovatel“ a uvádí výčet možných provozovatelů (ČR nebo právnická osoba). Pokud platí tento předpoklad Zadavatele, že uchazeč měl na mysli „provozovatele“, je znění odpovědi následující:

Předpokládáme dvouúrovňový systém, který naplňuje potřeby bezpečnosti a je v souladu se zákonem. Provozovatelé budou přistupovat do několika části AISG (veřejný portál ve správní části, dozorový batch část pro dodání herních a finančních dat, dozorová real-time část pro autentizaci a autorizaci). IdM modul bude tedy evidovat provozovatele hazardních her a pro každého jednu až několik sad přístupových údajů pro real-time část a zároveň identity jeho pracovníků pro přístup do privátní části veřejného portálu. IdM bude dále obsahovat údaj o datové schránce provozovatele.

2. *Jaký je zadavatelem požadovaný model resp. způsob využití PKI?*

Specifikace uvádí, že „K zajištění důvěrnosti, integrity a nepopiratelnosti komunikace systému provozovatele s AISG (vystavené služby registrace, ztotožnění hráče atd., předávání herních dat) bude sloužit systém založený na správě a distribuci veřejných klíčů (PKI, Public Key Infrastructure).". Z dané specifikace ani z dalšího textu není zřejmý zadavatelem požadovaný model resp. způsob použití PKI.

Zadávací dokumentace zejména nestanoví:

a. *zda má být komunikace mezi systémem provozovatele a AISG na úrovni PKI zajištěna pouze v reálném čase, kdy se navazuje a realizuje (v technické rovině např. použití protokolů na bázi TES), nebo zda má být zpětně prokazatelná (zejména z hlediska neodmítnutelnosti odpovědnosti) též kdykoli později (v technické rovině např. výměna šifrovaných a elektronicky podepisovaných datových struktur).*
b. *zda má být (zejména v případě ochrany komunikace v reálném čase) na bázi PKI ověřována pouze identita systému AISG (v technické rovině např. použití protokolů na bázi anonymního TES se serverovými certifikáty AISG), nebo zda má být na bázi PKI též ověřována identita přistupujícího systému (v technické rovině např. použití protokolů na bázi neanonymního ILS se serverovými certifikáty AISG a klientskými certifikáty systému poskytovatele).*
c. *jaké PKI procesy mají být podporovány (např. zneplatnění případného klientského certifikátu či vystavení následného certifikátu) a případně jaké vlastnosti mají být podporovány (např. požadavky na obsah případných serverových a klientských certifikátů či doby jejich platnosti)*

Odpověď na dotaz č. 1/2:

Předpokládané zabezpečení XML komunikace se systémem provozovatele je na úrovni HTTPS. Předávané XML zprávy budou podepsány certifikátem provozovatele nebo certifikátem AISG dle standardu WS-security nebo obdobným způsobem. Všechny používané certifikáty budou ve formátu X.509 a budou registrovány v IdM. Provozovatel bude mít

zajištěnu externí certifikační autoritu CA tak, aby do aplikace přistupoval s definovanou rolí a nastavením autorizace a autentizace. Budou užívány certifikáty od certifikovaných subjektů uznávané pro celou EU, tj. nikoliv jen pro ČR. Podpora PKI na straně dodavatele zahrnuje použití certifikátů a příslušných klíčů pro výše uvedené zabezpečení komunikace a kontrolu CRL.

3. ***Jaký je zadavatelem požadovaný účel/způsob využití autentizace prostřednictvím ISDS?*** *Specifikace uvádí, že „Pro přístup do Veřejného portálu budou provozovatelé využívat autentizaci pomocí systému datových schránek (ISDS).“. Zadávací dokumentace (zejména Příloha smlouvy č. 2 „Analytická dokumentace", kapitoly 3.3 a 4.2) v některých pasážích zmiňuje interakci provozovatele s AISG prostřednictvím DS. Z těchto textací nicméně není jednoznačně zřejmé:*

    a. *zda se poskytovatel prostřednictvím ISDS přihlašuje a provádí vybrané operace typu „Vydání základního povolení", „Změna základního povolení", „Ohláška hazardní hry" či „Změna místního povolení" přímo v systému AISG, nebo zda prostřednictvím ISDS pouze předává do AISG datovou zprávu*
    b. *zda vytváří svá „podání" (v případě elektronické verze předání) pro výše uvedené typy operací dle bodu a. v rámci AISG, nebo v jiných systémech, neboť zadávací dokumentace hovoří v textových pasážích pouze o formulářích na webu či webu MF, nikoli např. veřejném portále AISG*
    c. *zda v případě, že se poskytovatel prostřednictvím ISDS přihlašuje a provádí výše uvedené typy operací dle bodu a. v systému AISG, pod jakou identitou (v technické rovině pod jakým přístupovým účtem) tyto operace provádí, zejména pravděpodobně nepůjde o identitu používanou pro přístup jeho systémů k AISG, ale o jinou identitu daného provozovatele a případně zda těchto identit může provozovatel používat více.*
    d. *Zda a případně jak může poskytovatel sledovat stav svých podání - např. pouze na základě datových zpráv zasílaných provozovateli ze strany AISG či po přihlášení k některému z rozhraní AISG.*

Pro efektivní návrh řešení a optimální stanovení ceny nabídky je nutná jednoznačná specifikace/požadavky zadavatele z hlediska uchazečem kladených výše uvedených dílčích dotazů. Vzhledem k vysokým požadavkům na propustnost a SLA může mít daná specifikace zásadní vliv na technické řešení a jeho cenu. Upřesní zadavatel v daném smyslu zadávací dokumentaci?

Odpověď na dotaz 1/3:

Výše je uveden výraz poskytovatelé, který je v tomto kontextu nepřesně uveden. Nový zákon o hazardních hrách v § 6 stanovuje pojem “Provozovatel“ a uvádí výčet možných provozovatelů (ČR nebo právnická osoba). Pokud platí tento předpoklad Zadavatele, že uchazeč měl na mysli „provozovatele“, je znění odpovědi následující:

Ad a) Veřejný portál AISG bude podporovat přípravu příslušných podání, které budou následně doručovány datovou zprávou do datové schránky Zadavatele.

Ad b) Ano, provozovatel si v AISG vytváří své vlastní podání, do kterého vyplní údaje, které budou pro vydání základního nebo místního povolení nezbytné.

Ad c) Toto navazuje na odpověď k otázce č. 1. Zadavatel požaduje vybudovat alespoň dvouúrovňový systém, aby výše popsané, bylo zajištěno.

Ad d) Stav svých podání bude moci provozovatel zjistit pouze na základě dotazu. AISG nebude zasílat či evidovat žádné automatizované notifikace o stavu řízení.

Dotaz č. 2

Zadávací dokumentace (příloha smlouvy č. 2 „Analytická dokumentace", kapitola 4.4 „Nefunkční požadavky", požadavky RT3; příloha zadávací dokumentace č. 3 „Tabulka", list „nefunkční požadavky", požadavky RT3) kladou požadavek elektronického podpisu s popisem „MF zajistí certifikáty; AISG musí být schopno komunikovat s externí certifikační autoritou".

Zadávací dokumentace (Příloha smlouvy č. 1 „Technická dokumentace", kapitola 4.1 „Diagram komponent", „Tabulka 2 - Popis elementů diagramu", položka modul „IdM provozovatelů" na straně 14) dále okrajově jednou větou zmiňuje PKI.

Tato dále neurčitá specifikace nestanoví k jakým účelům má být v rámci AISG elektronického podpisu používáno. Zejména nestanoví:

a. *zda a která data či dokumenty nebo jejich typy mají být opatřována elektronickým podpisem*
b. *zda a které komponenty či kteří uživatelé AISG mají elektronický podpis vytvářet*
c. *zda a u kterých dat či dokumentů nebo jejich typů má být ověřován elektronický podpis*
d. *zda a kterékomponenty či kteří uživatelé AISG mají provádět ověřování elektronického podpisu*
e. *je-li podpora elektronického podpisu v rámci systému AISG požadována, jaké jsou požadavky zadavatele na prostředky k jejich vytváření a ověřování*
f. *jaká je vazba elektronického podpisu na jiné externí systémy typu spisová služba zadavatele.*

Mimo jiné též s ohledem na vysoké požadavky na propustnost a SLA řešení AISG má přesná specifikace požadavků zadavatele ve výše uvedené oblasti zásadní vliv na technické řešení a jeho cenu. Upřesní zadavatel v daném smyslu zadávací dokumentaci tak, aby mohl uchazeč zpracovat efektivní návrh řešení a optimální stanovení ceny nabídky?

Odpověď

Pro správní část AISG platí, že elektronická komunikace bude probíhat primárně přes spisovou službu MF (EPD) s využitím ISDS. Pokud je na MF doručen elektronicky podepsaný dokument emailem, je zanesen do EPD obdobně jako v případě, že by dorazil s využitím ISDS.

Zadavatel požaduje po Dodavateli postupovat v souladu se Zákonem č. 227/2000 Sb., o elektronickém podpisu a Vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, od 1. 7. 2016 i s Prováděcím rozhodnutím Komise č. 2014/148/EU, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu. Případné dopady způsobené předpokládaným přijetím vládního návrhu zákona o službách vytvářejících důvěru pro elektronické transakce budou řešeny v rámci Etapy 1A.

V případě dozorové části platí pravidla uvedená v odpovědi na dotaz č.1/2.

Dotaz č. 3

Zadávací dokumentace (příloha smlouvy č. 2 „Analytická dokumentace", kapitola 4.4 „Nefunkční požadavky", požadavky RT2; příloha zadávací dokumentace č. 3 „Tabulka", list „nefunkční požadavky", požadavky RT2) kladou požadavek šifrování s popisem „Vyhláška NBÚ viz výše; musí být v souladu" (vyhláškou míněna „úroveň významný systém -> zákon o kybernetické bezpečnosti; provádějící vyhláška NBÚ (316 a 317)").

Zadávací dokumentace (Příloha smlouvy č. 1 „Technická dokumentace", kapitola 4.1 „Diagram komponent", „Tabulka 2 - Popis elementů diagramu", položka modul „IdM provozovatelů" na straně 14) dále okrajově jednou větou zmiňuje důvěrnost komunikace mezi systémy provozovatelů a AISG.

Tato dále neurčitá specifikace nestanoví za jakých okolností a která data či informace mají být šifrováním chráněny.

Přesná specifikace požadavků zadavatele ve výše uvedené oblasti má vliv na technické řešení a jeho cenu. Upřesní zadavatel v daném smyslu zadávací dokumentaci tak, aby mohl uchazeč zpracovat efektivní návrh řešení a optimální stanovení ceny nabídky?

Odpověď

Přenos herních a finančních dat a dat k ověření / registraci hráčů mezi systémem provozovatele a AISG by měl být vždy šifrován.

Viz odpovědi výše na dotaz č. 1.

Dotaz č. 4

*Zadávací dokumentace (Příloha smlouvy č. 1 „Technická dokumentace") specifikuje v „Tabulce 2 - Popis elementů diagramu" v kapitole „4.1 Diagram komponent" (strana 14) modul **„AM veřejná správa"** následovně:*

Modul, který slouží k řízení přístupu (AM, Access Management) uživatelů z veřejné správy. Ke správě identit a přístupových údajů uživatelů z veřejné správy a jejich rolí v AISG, stejně jako k autentizaci a autorizaci, bude sloužit výhradně systém JIP/KAAS. Modul „AM veřejná správa" bude sloužit pro integraci s JIP/KAAS a pro správu oprávnění rolí definovaných v AISG.

Současně zadávací dokumentace (příloha smlouvy č. 5 „Servisní služby a Služby rozvoje", kapitola 1.2 „Vymezení Servisních služeb Dodavatele", 4. odstavec) specifikuje „1/ případě dopadu nefunkčnosti spolupracujících externích systémů na funkčnost AISG je výsledné omezení provozu vyloučeno z SLA Dodavatele. Dodavatel je nicméně povinen v rámci návrhu a implementace systému definovat a implementovat mechanismy, které minimalizují vliv nefunkčnosti spolupracujících externích systémů na funkčnost AISG (ošetření chybových stavů, využití nakešovaných informací apod.) a dáte je povinen v průběhu poskytování Servisních služeb tyto mechanismy dále rozvíjet a upravovat na základě provozních zkušeností.".

Případná nefunkčnost spolupracujících externích systémů JIP/KAAS a ISDS je pro provoz AISG zcela zásadní. Implementace a provoz mechanismů, které by minimalizovali tuto nefunkčnost v prostředí s vysokými požadavky na propustnost, redundanci a SLA může být náročná a zejména nákladná (v extrémním případě se může jednat až o replikaci chování JIP/KAAS a části ISDS). Současně je nutno zvažovat též přípustnost a věcně-bezpečnostní aspekty a rizika případného využití „kešovaných" autentizačních informací při nefunkčnosti těchto systémů.

Upřesní zadavatel v případě modulu „AM veřejná správa" a spolupracujících externích systémů JIP/KAAS a ISDS, zda se jeho požadavek na implementaci mechanismů minimalizujících vliv jejich nefunkčnosti vztahuje i na tyto případy a pakliže ano, potom v jakém rozsahu?

Odpověď

Nefunkčnost systémů JIP/KAAS a ISDS má dopad pouze na správní část AISG a navíc znemožňuje přístup uživatelů k AISG. V tomto případě Zadavatel nepožaduje po Dodavateli, aby implementoval mechanismy minimalizující vliv jejich nefunkčnosti.

Dotaz č. 5

Zadavatel ve své odpovědi na nezodpovězený dotaz č. 1 z Dodatečných informací č. 13 (zodpovězený v rámci Dodatečných informací č. 14) uvádí: „Antivir na aplikační úrovni včetně licencí dodává Dodavatel, SPCSS zajistí ochranu na úrovni sítí. ".

Specifikace rozsahu a technologií antivirové ochrany poskytnuté pro ochranu na úrovni sítí ze strany SPCSS je podstatná pro správné navázání návrhu řešení uchazeče na cílové prostředí zadavatele.

Upřesní zadavatel rozsah (jaké typy antivirové ochrany a na jakých síťových komponentách/službách jsou nasazeny) a případně použité technologie antivirové ochrany poskytnuté pro ochranu na úrovni sítí ze strany SPCSS?

Odpověď

SPCSS zajišťuje na úrovni sítí ochranu proti DoS a DDoS útokům, ochranou proti síťovým útokům (IPS, IDS) a dále se jedná o ochranu síťovými firewally a prostřednictvím webového aplikačního firewallu (WAF). Síťová infrastruktura SPCSS je plně integrována do monitoringu infrastruktury a bezpečnostního dohledu SPCSS.

Primární úroveň antivirové ochrany je na aplikační úrovni a je zajišťována Dodavatelem.

Dotaz č. 6

Zadávací dokumentace specifikuje požadavky na provozní a bezpečnostní monitoring AISG. Tyto požadavky se soustřeďují na implementaci příslušných funkcionalit, jejich integraci na dohledové systémy SPCSS, součinnost při jejich „nastavení" a součinnost při řešení následných incidentů a událostí.

Velmi vysoké požadavky zadavatele na SLA si nicméně s ohledem na smluvní povinnosti a odpovědnosti uchazeče, vyžadují intenzivní zejména technický dohled/monitoring uchazeče nad provozem AISG. Tento stav vede v principu na dva možné přístupy:

a. *Zadavatel poskytne uchazeči (dodavateli) plnohodnotný (nejlépe vzdálený) uživatelský přístup ke všem dohledovým nástrojům provozovaným ze strany SPCSS v souvislosti se systémem AISG.*
b. *Uchazeč (dodavatel) bude muset vytvořit vlastní dohledový systém pro své potřeby napojený na AISG s tím, že zadavatel umožní a zajistí přístup takovéhoto dohledového systému k AISG.*
c. *Případný jiný přístup.*

Upřesní zadavatel (vzhledem k dopadu na návrh a stanovení ceny nabízeného řešení), které z daných přístupů jsou pro něj akceptovatelné a v jakém rozsahu - zejména co bude v jejich rámci k dispozici uchazeči (dodavateli)?

Odpověď

Dodavatel bude mít přístup k incidentům registrovaným v ServiceDesku za účelem získání informace o incidentu. Časy SLA běží od momentu oznámení incidentu Dodavateli.

Dotaz č. 7

Dotaz k ZD, kapitola 9 Jistota:

Dle ZVZ a zadávací dokumentace musí být jistota platná po celou dobu zadávací lhůty, a to nejpozději od skončení lhůty pro podávání nabídek. S ohledem na to, že zadávací lhůta se může stavět (a tedy může trvat po předem nepředvídatelnou dobu), chceme se zadavatele dotázat, jakým způsobem má být postupováno v případě jistoty formou bankovní záruky (tj. a) má být tato vystavena na mnohem delší dobu než aktuálně vychází konec zadávací lhůty nebo b) bude možné v průběhu ZŘ předložit prodloužení BZ)?

Odpověď

Není třeba, aby uchazeč při stanovování délky platnosti záruční listiny zohledňoval rezervu z důvodu

- případné budoucí situace, kdy by:
  - zadávací lhůta byla uchazeči prodloužena dle § 43 odst. 3 ZVZ, či
  - neběžela dle § 43 odst. 4 ZVZ,
- případné situace dle § 43 odst. 4 ZVZ, která sice před ukončením lhůty pro podání nabídek již nastala, avšak zadavatel využil implicitní oprávnění dle ZVZ o této situaci dodavatele neinformovat.

Uchazeč bude i po uplynutí lhůty pro podání nabídek oprávněn prodloužit délku platnosti záruční listiny, pokud uchazečem ve lhůtě pro podání nabídek předložená záruční listina nepokrývá celou zadávací lhůtu v důsledku:

- prodloužení zadávací lhůty uchazeči dle § 43 odst. 3 ZVZ, nebo
- posunutí zadávací lhůty dle § 43 odst. 4 ZVZ.

V jiných případech zadávací podmínky nezakládají oprávnění uchazeče prodloužit délku platnosti záruční listiny.

Zadavatel nicméně upozorňuje, že zajištění platnosti nepeněžní formy záruky po celou dobu zadávací lhůty je zákonnou povinností uchazeče. Pokud tedy uchazeč zvolí nepeněžní formu jistoty, bude na něm, aby aktivně přistupoval k naplňování této zákonné povinnosti. Jestliže uchazeč nesplní povinnost uloženou mu ustanovením § 67 odst. 5 ZVZ, je zadavatel povinen takového uchazeče vyloučit z další účasti v zadávacím řízení pro neposkytnutí jistoty.

Dotaz č. 8

Dotaz k ZD, kapitola 6.3 Pojištění:

Citace ze ZD: "…Vybraný uchazeč je povinen před uzavřením smlouvy na realizaci veřejné zakázky předat zadavateli originál nebo úředně ověřenou kopii pojistné smlouvy uzavřené v rozsahu a za podmínek specifikovaných v čl. 12.4 Závazného návrhu smlouvy. Nepředání originálu či úředně ověřené kopie pojistné smlouvy před uzavřením smlouvy na realizaci veřejné zakázky bude považováno za neposkytnutí řádné součinnosti potřebné k uzavření smlouvy dle § 82 odst. 4 ZVZ." Dotaz: pojišťovna, u které máme sjednánu pojistnou smlouvu, jejímž předmětem je pojištění za škodu způsobenou naší společností třetí osobě, považuje tuto pojistnou smlouvu za obchodní tajemství, proto nemůžeme předložit její ověřenou kopii. Bude zadavatel považovat za dostatečné, pokud prokážeme existenci požadovaného pojištění předložením certifikátu pojistného brokera, potvrzující typ pojištění a jeho výši?

Odpověď

Obdobný dotaz byl již zodpovězen v Dodatečných informacích č. 14 z 18. 5. 2016, v části VIII.: Nezodpovězené dotazy z Dodatečných informací č. 12: *„Ano, je možné předložit certifikát, jak plyne z dikce odst. 12.4 Smlouvy (v dotazu chybně uvedeno 14.4): ´Dodavatel je povinen předat kopii pojistného certifikátu (pojistné smlouvy)…´“.*

V Praze dne 22. 6. 2016

Dipl.-Ing.
Miroslav Hejna

Digitálně podepsal Dipl.-Ing. Miroslav Hejna
DN: c=CZ, cn=Dipl.-Ing. Miroslav Hejna, o=Česká republika - Ministerstvo financí, ou=15195, ou=Letenská 15, 118 10 PRAHA 1, ou=Ministerstvo financí, title=Náměstek pro řízení sekce, serialNumber=ICA - 10366748
Datum: 2016.06.22 14:50:29 +02'00'

.....

Dipl.-Ing. Miroslav Hejna
náměstek pro řízení sekce 09