Dodatečné informace č. 36

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

Zadavatel v Dodatečných informacích č. 20 v odpovědi na dotaz č. 1/1 oproti zadávací dokumentaci rozšiřuje původní zadání včetně zavedení identity pracovníků provozovatele.
Současně nově uvádí možnost přístupu k systému AISG - konkrétně přístup pracovníků provozovatele k privátní části veřejného portálu AISG. Nicméně tento přístup není v souladu se specifikací uvedenou Zadávací dokumentací (Příloha smlouvy č. 1 „Technická dokumentace", kapitola 4 „Popis rozhraní a komunikace", tabulka 2 „Popis elementů diagramu", element „Veřejný portál", strana 15), která stanoví, že privátní část je určena pro přístup úředníků obcí prostřednictvím JIP/KAAS.
Taktéž jiná dokumentace neobsahuje jakékoli další informace k přístupům pracovníků provozovatele. Zadávací dokumentace (Příloha smlouvy č. 2 „Analytická dokumentace", kapitola 4.2 „Diagram datových toků", tabulka 3 „Popis elementů diagramu") bez dalšího upřesnění pouze zmiňuje „ID pracovníka", který provádí registraci/autorizaci/aktualizaci hráče a to pouze jakožto údaj v rámci obousměrné online komunikace systému provozovatele a AISG.
Zadávací dokumentace též nestanoví postupy či požadavky a pravomoci na zavedení/registraci, změny, zrušení/blokaci uživatele typu „pracovník provozovatele".
*Zadavatel dále v Dodatečných informacích č. 20 v odpovědi na dotaz č. 4 uvádí „Nefunkčnost systémů JIP/KAAS a ISDS má dopad pouze na správní část AISG a navíc znemožňuje přístup uživatelů k AISG.", **n**icméně součástí dozorové části AISG je též minimálně analytický engine/subsystém, který využívají zejména pracovníci Zadavatele, kteří pravděpodobně budou identifikování a autentizováni také s využitím **JIP/KAAS.***
Uchazeč žádá zadavatele o řádné, ucelené a konzistentní doplnění a úpravu zadávací dokumentace v oblasti požadavků na AIM a to zejména tak, aby byl ze Zadávací dokumentace zřejmý:

- *výčet typů entit interagujících s AISG (provozovatel, obec, MF, CÚ, a další)*
- *výčet typů identit interagujících s AISG pro jednotlivé entity (např. pro provozovatele IS provozovatele, pracovník provozovatele, a případně další). Pro jednotlivé identity stanovit:*
  - *části/funkcionality systému, ke kterým mají přistupovat/které mají využívat a role resp. jejich pravomoci/odpovědnosti*

- *požadavky na způsob identifikace, autentizace (Certifikát, uživatelské jméno/ID a heslo, ISDS, a další) a autorizace a specifikování, které systémy mají být pro tyto účely použity (ISDS, JIP/KAAS, interně AISG, případně jiné)*

- *Požadavky na procesy/postupy zavedení/registrace/rušení/změny jednotlivých identit pro AISG a to zejména ve vztahu k informačním systémům a pracovníkům provozovatelů.*

Odpověď

Zadavatel považuje popis interakcí mezi provozovateli a jejich informačními systémy a AISG specifikovaný v Zadávací dokumentaci a v dosud poskytnutých dodatečných informacích za dostatečný pro zpracování nabídek v požadované míře detailu, přičemž terminologická nepřesnost v odpovědi na dotaz č. 1/1 z DI č.20 byla vysvětlena v odpovědi na dotaz č.2 v DI č.32. Základní rozdělení přístupů provozovatelů k AISG je tedy následující: veřejný portál ve správní části, dozorová batch část pro dodání herních a finančních dat, dozorová real-time část pro ověření / registraci hráčů. V prvním případě bude autentizace provozovatele založena na ISDS, ve zbylých případech se bude jednat o komunikaci s využitím HTTPS. Z legislativního hlediska není důležité, který konkrétní pracovník provozovatele přistupuje k AISG. Veškerá odpovědnost za předávání dat a dodržení ostatních pravidel dle zákona je na provozovateli jako právnické osobě. ID pracovníka a ID provozovny jsou pouze poskytnuté údaje ze strany provozovatele jako součást předávaných dat a nemají vliv na způsob autentizace provozovatele. Detailní popis způsobů identifikace, autentizace a autorizace a procesů správy identit provozovatelů a jejich informačních systémů bude zpracován v Etapě 1A.

Přístup do dozorové části AISG bude v případě úředníků veřejné správy též probíhat s využitím JIP / KAAS. Ohledně implementace mechanismů minimalizujících vliv nefunkčnosti zde platí odpověď na dotaz č.4 z DI č.20, tedy že Zadavatel toto po Dodavateli nepožaduje.

Dotaz č. 2

Zadavatel v Dodatečných informacích č. 20 uvedl (pravděpodobně chybou opisu) chybné znění bodu 2. dotazu č. 2, když v bodech „a" a „b", uvedl „např. použití protokolů na bázi TES", „např. použití protokolů na bázi anonymního TES" a „např. použití protokolů na bázi neanonymního ILS" namísto správné textace zaslaného dotazu uchazeče „např. použití protokolů na bázi TLS", „např. použití protokolů na bázi anonymního TLS" a „např. použití protokolů na bázi neanonymního TLS".

V odpovědi na dotaz č. 1/2 Zadavatel doplňuje zadání o použití protokolu HTTPS, jehož prostřednictvím jsou předávány XML zprávy, které mají (na základě doplnění zadání zadavatelem) nově opatřené elektronickým podpisem (kterážto funkcionalita vyžaduje na straně IS provozovatele nakládat s podpisovým certifikát a svázanými prostředky pro vytváření elektronického podpisu).

Uchazeč žádá zadavatele o doplnění jeho odpovědi ve smyslu původního dotazu, tedy zda požaduje použití anonymního HTTPS nebo zda požaduje použití neanonymního HTTPS (v takovém případě bude nutno držet na straně IS provozovatele druhý „autentizační" klientský certifikát a příslušný klíčový materiál).

Odpověď

Zadavateli stačí použití anonymního HTTPS při dodržení ostatních požadavků uvedených v DI č.20.

Zadavatel se omlouvá za chyby v přepisu u DI č.20, nicméně tento fakt neměl žádný vliv na znění odpovědí.

Dotaz č. 3

Zadavatel v Dodatečných informacích č. 20 v odpovědi na dotaz č. 3 doplňuje zadání o požadavek, který stanoví, že „Přenos herních a finančních dat a dat k ověření/ registraci hráčů mezi systémem provozovatele a AISG by měl být vždy šifrován".
Uchazeč žádá zadavatele o doplnění jeho odpovědi v tom smyslu, zda požaduje/zda z jeho strany postačuje šifrování na úrovni HTTPS protokolu (samozřejmě při volbě vhodných kryptografických parametrů příslušných protokolů) nebo zda požaduje také šifrování v rámci avizovaných podepisovaných XML zpráv nebo jejich částí.

Odpověď

Šifrování na úrovni HTTPS protokolu postačuje.

Dotaz č. 4

Zadavatel v Dodatečných informacích č. 20 v odpovědi na dotaz č. 2 neuvádí odpověď na základní položené dotazy pro které dokumenty/data a kterými uživateli/komponentami mají být vytvářeny a ověřovány elektronické podpisy. Ve své odpovědi uvádí, že „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.".
Z dané odpovědi není zřejmé, zda problematiku vytváření a ověřování elektronických podpisů řeší EPD, nebo zda ji řeší AISG, nebo zda je použito nějaké jiné kombinace typu s podpisy nakládá EPD a AISG je povinen pracovat se službami EPD (např. pro odeslání dokumentu) či atributy EPD typu „dokument v EPD je opatřen platným podpisem". Stejně tak není stanoveno, kterých dokumentů by se daná věc měla týkat.
V již výše zmiňované odpovědi na dotaz č. 1/2 Zadavatel nově doplňuje požadavky zadávací dokumentace o podepisování (a nepřímo ověřování podpisů) vybraných XML zpráv předávaných mezi IS provozovatele a AISG v rámci dozorové části.

Uchazeč žádá zadavatele o řádné, ucelené a konzistentní doplnění a úpravu zadávací dokumentace v oblasti požadavků na používání elektronického podpisu a to zejména tak, aby bylo ze Zadávací dokumentace zřejmé:

- *zda má systém AISG zajišťovat vytváření elektronického podpisu dokumentů či dat jiných, nežli nově uváděných vybraných XML zpráv předávaných mezi IS provozovatele a AISG, a pakliže ano, jaký je výčet typů těchto dokumentů/dat a kteří uživatelé/komponenty jej mají vytvářet.*
- *zda má systém AISG zajišťovat ověřování elektronického podpisu dokumentů či dat jiných, nežli nově uváděných vybraných XML zpráv předávaných mezi IS provozovatele a AISG, a pakliže ano, jaký je výčet typů těchto dokumentů/dat a kteří uživatelé/komponenty mají podpis ověřovat.*

Odpověď

Problematiku vytváření a ověřování elektronických podpisů u dokumentů bude kompletně řešit EPD (při příjmu i při odeslání), tedy správní část AISG s podpisy pracovat nebude. Detailní specifikace všech vstupních a výstupních dokumentů všech procesů podporovaných AISG bude realizována v rámci Etapy 1A, jak již bylo uvedeno v DI č.26.

Podepisování jednotlivých XML zpráv bude řešeno při komunikaci s provozovateli – viz odpovědi na DI č.20 a dotazy č.2 a 3 těchto DI.

Komunikace s dalšími IS bude řešena následovně:

- ISZR (vč. kompozitních služeb) – dle platných pravidel pro napojení na ISZR
- spisové služby MF a FÚ (EPD, ADIS) – popis rozhraní byl specifikován v DI č.3, autentizace bude řešena jménem a heslem

- IS Celní správy (Aplikace Mobilní dohled a její spisová služba EPP) – jak již bylo uvedeno v DI č.3, je plánován rozvoj těchto IS dle potřeb AISG. Pro účely nabídek předpokládejte stejný princip jako u spisových služeb MF a FÚ.
- IS SDSL - autentizace bude řešena jménem a heslem.

Dotaz č. 5

Zadavatel v Dodatečných informacích č. 20 v odpovědi na dotaz č. 5 neuvádí na síťové úrovni žádnou podporu antivirové ochrany (uvádí pouze DoS, DDoS, IPS, IDS, síťový firewalling, WAF).

Konstatuje tímto Zadavatel, že infrastruktura SPCSS nedisponuje/nebude poskytovat pro potřeby řešení AISG žádné služby antivirové (případně antispamové) ochrany na úrovni výkonných hraničních prvků infrastruktury? Typicky se jedná o specializované doplňky, pluginy či rozšiřující komponenty výkonných FW či ADC řešení s cílem omezit negativní vlivy antivirové kontroly na efektivní šířku pásma centrálních komunikačních kanálů (zejména z/do prostředí Internet).

Odpověď

Zadavatel jednoznačně specifikoval služby SPCSS v této oblasti v odpovědi na dotaz č.5 v DI č.20. Žádné další služby SPCSS nabízet nebude. Platí tedy, že primární úroveň antivirové ochrany je na aplikační úrovni a je zajišťována Dodavatelem.

Dotaz č. 6

Zadavatel v Dodatečných informacích č. 20 v odpovědi na dotaz č. 6 uvádí, že „Dodavatel bude mít přístup k incidentům registrovaným v ServiceDesku za účelem získání informace o incidentu. Časy SLA běží od momentu oznámení incidentu Dodavateli.".

Nicméně zadavatel požaduje garanci vysokého SLA, která vyžaduje též preventivní/prediktivní přístup k monitoringu a dohledu - tedy zejména sledovat průběžně stav jednotlivých komponent a součástí řešení a generovaných událostí, tak aby bylo možno včasně předcházet vniku nežádoucích provozních stavů.

Poskytne Zadavatel v rámci svého dohledového a monitorovacího systému pro potřeby podpory provozu Uchazeči takovýto typ přístupu (resp. přístup k tomuto typu informací)?

Odpověď

Nástroje monitoringu budou spravovány a používány SPCSS, primární nástroj pro komunikaci s Dodavatelem je ServiceDesk SPCSS. V rámci přípravy provozní dokumentace budou ve spolupráci Dodavatele a SPCSS navrženy detailní postupy řešení problémů, analýzy stavu AISG apod. a následného předávání potřebných informací.

V Praze dne 14.7. 2016

Ing. Božena Zděnková

Digitálně podepsal Ing. Božena Zděnková
DN: c=CZ, cn=Ing. Božena Zděnková, o=Česká republika - Ministerstvo financí, ou=12299, ou=Letenská 15, 118 10 PRAHA 1, ou=Ministerstvo financí, title=ředitel odboru, serialNumber=ICA - 10343555
Datum: 2016.07.14 14:48:28 +02'00'

v.z. .....

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