

Příloha:

Dodatečné informace, včetně přesného znění žádosti dodavatele o dodatečné informace

Pořadové číslo dodatečných informací: **09.**

ČÁST 1: Přesné znění žádosti dodavatele o dodatečné informace

Otázka č. 1:

PKI (infrastruktura veřejných klíčů)

- a) Mezi základními službami poskytovanými ISZR uvádíte PKI. Jaké jsou specifické požadavky na toto PKI? V obecném chápání PKI – infrastruktura veřejných klíčů – zajišťuje vydávání, správu, distribuci, ukládání a revokaci certifikátů. Tj., její nedílnou součástí je certifikační autorita. Je tedy požadavkem ISZR vybudovat vlastní certifikační autoritu? Jaké typy certifikátů a v jakém množství by měla taková CA vydávat? Měla by vydávat kvalifikované certifikáty? Měla by vydávat kvalifikované systémové certifikáty? Měla by být její součástí i služba časového razítka, a to i kvalifikovaného? Měla by CA vydávat i šifrovací certifikáty s možností odkrytí privátního klíče (key escrow)?
- b) Bez ohledu na to, zda budou certifikáty zajišťovány vlastní CA jako součástí ISZR PKI (viz předchozí otázka), předpokládá se užití kvalifikovaných systémových certifikátů pro agendové systémy (AIS)?

Otázka č. 2:

Katalog služeb

V dodatečných informacích poř. č. 06 otázka č. 1 uvádíte:

„Za dekompozici, orchestraci volání služeb a zpětnou kompozici výsledku z pohledu definice předpisu těchto pravidel a sledu aktivit odpovídá komponenta Katalog služeb a SLA, jejíž perzistenci zajišťuje RPP. Za provedení dekompozice, orchestrace volání služeb a zpětnou kompozici výsledku odpovídají procesy ISZR - Aplikační logika ISZR (Kapitola 1.3.1. Přílohy č. 1a ZD), která využívá obsahu Katalogu služeb a SLA k tomu, aby při zpracování služeb předem definovaná pravidla a sled aktivit dodržovala. Katalog služeb je tedy koncipován jako komponenta, za jejíž definici obsahu a perzistenci odpovídá RPP a za její užití, při zpracování komplexních služeb publikovaných na vnějším rozhraní systému základních registrů, odpovídá ISZR.“

Rozumí se katalogem služeb service repository ve smyslu SOA, tj. UDDI? Čím se tedy liší zodpovědnost tohoto Katalogu služeb jako součásti RPP od katalogů služeb, které je součástí ISZR?

V příloze 1a ZD se totiž uvádí:

Str. 15: „Katalog služeb základních registrů publikuje navenek pro potřeby veřejnosti i agendových systémů.“

Str. 23: „Z hlediska Agendových informačních systémů je systém základních registrů prezentován Web službami eGON publikovanými pomocí privátního Universal Description, Discovery, and Integration (UDDI) registru. Z hlediska ISZR jsou jednotlivé základní registry (RPP, ROB, ROS, RUIAN) a Převodník identifikátoru fyzických osob (ORG) prezentovány Web službami publikovanými v jednom společném UDDI registru. Tento společný katalog bude spravován Informačním systémem základních registrů.“

Str. 30:

„6.1. Základní východiska

- Katalog služeb veřejné správy obsahuje seznam služeb, ...”

„6.2. Cíle

Navrhnout katalog služeb ISZR, který zajistí: ...“

A řada dalších odkazů na Katalog služeb a UDDI jako součásti řešení ISZR v textu přílohy 1a ZD.

Což chápeme i ve shodě s diagramem na str. 23 přílohy 1a ZD, že ISZR provozuje dvě UDDI, jednu pro eGON služby a druhou pro služby ZR.

Bude tedy RPP provozovat třetí UDDI? Budou zde uvedené definice služeb používány pro tvorbu služeb vystavených na vnějším rozhraní?

Co jsou přesně artefakty, které budou definovány v RPP katalogu? Definice orchestrací? Definice služeb na vnějším rozhraní (WSDL) a jejich SLA? Definice služeb (WSDL) základních katalogů na vnitřním rozhraní? Nepochází k překryvu s oběma ISZR UDDI? Nebo se jedná jen o „slovní popis“ těchto služeb (resp. jejich specifikaci), který pak bude předán k technické implementaci? Popis, tak jak je uvedeno v příkladech v zadávací dokumentaci RPP, příloha 3, str. 3 a dále?

ČÁST 2: Dodatečné informace

K otázce č. 1:

PKI (infrastruktura veřejných klíčů)

- a) *Mezi základními službami poskytovanými ISZR uvádíte PKI. Jaké jsou specifické požadavky na tuto PKI? V obecném chápání PKI – infrastruktura veřejných klíčů – zajišťuje vydávání, správu, distribuci, ukládání a revokaci certifikátů. Tj., její nedílnou součástí je certifikační autorita. Je tedy požadavkem ISZR vybudovat vlastní certifikační autoritu? Jaké typy certifikátů a v jakém množství by měla taková CA vydávat? Měla by vydávat kvalifikované certifikáty? Měla by vydávat kvalifikované systémové certifikáty? Měla by být její součástí i služba časového razítka, a to i kvalifikovaného? Měla by CA vydávat i šifrovací certifikáty s možností odkrytí privátního klíče (key escrow)?*
- b) *Bez ohledu na to, zda budou certifikáty zajišťovány vlastní CA jako součástí ISZR PKI (viz předchozí otázka), předpokládá se užití kvalifikovaných systémových certifikátů pro agendové systémy (AIS)?*

Odpověď zadavatele:

Ano, požadavkem na ISZR je vybudování vlastní certifikační autority. Kvalifikované certifikáty může v principu vydávat pouze akreditovaná CA ve smyslu zákona o elektronickém podpisu. V rámci poptávky není tato akreditace požadována, do budoucna nicméně není tento požadavek vyloučen. Certifikáty budou určeny i pro šifrování.

Co se týká key escrow, neexistuje v ČR na tuto metodiku žádná platná legislativa, takže o této možnosti neuvažujeme.

Množství certifikátů závisí na požadavcích jednotlivých ZR (kolik certifikátů budou potřebovat), na vnitřních požadavcích ISZR a na požadavcích AIS (kolik AIS bude se ZR komunikovat). Rámcově lze očekávat desetitisíce až statisíce certifikátů.

AIS pro komunikaci se ZR budou využívat certifikáty vydávané CA popsanou výše.

K otázce č. 2:

Katalog služeb

V dodatečných informacích poř. č. 06 otázka č. 1 uvádíte:

„Za dekompozici, orchestraci volání služeb a zpětnou kompozici výsledku z pohledu definice předpisu těchto pravidel a sledu aktivit odpovídá komponenta Katalog služeb a SLA, jejíž perzistenci zajišťuje RPP. Za provedení dekompozice, orchestrace volání služeb a zpětnou kompozici výsledku odpovídají procesy ISZR - Aplikační logika ISZR (Kapitola 1.3.1. Přílohy č. 1a ZD), která využívá obsahu Katalogu služeb a SLA k tomu, aby při zpraco-

vání služeb předem definovaná pravidla a sled aktivit dodržovala. Katalog služeb je tedy koncipován jako komponenta, za jejíž definici obsahu a perzistenci odpovídá RPP a za její užití, při zpracování komplexních služeb publikovaných na vnějším rozhraní systému základních registrů, odpovídá ISZR.

Rozumí se katalogem služeb service repository ve smyslu SOA, tj. UDDI? Čím se tedy liší zodpovědnost tohoto Katalogu služeb jako součásti RPP od katalogů služeb, které je součástí ISZR?

V příloze 1a ZD se totiž uvádí:

Str. 15: „Katalog služeb základních registrů publikuje navenek pro potřeby veřejnosti i agendových systémů.”

Str. 23: „Z hlediska Agendových informačních systémů je systém základních registrů prezentován Web službami eGON publikovanými pomocí privátního Universal Description, Discovery, and Integration (UDDI) registru. Z hlediska ISZR jsou jednotlivé základní registry (RPP, ROB, ROS, RUIAN) a Převodník identifikátoru fyzických osob (ORG) prezentovány Web službami publikovanými v jednom společném UDDI registru. Tento společný katalog bude spravován Informačním systémem základních registrů.”

Str. 30:

„6.1. Základní východiska

- Katalog služeb veřejné správy obsahuje seznam služeb, ...”

„6.2. Cíle

Navrhnout katalog služeb ISZR, který zajistí: ...“

A řada dalších odkazů na Katalog služeb a UDDI jako součásti řešení ISZR v textu přílohy 1a ZD.

Což chápeme i ve shodě s diagramem na str. 23 přílohy 1a ZD, že ISZR provozuje dvě UDDI, jednu pro eGON služby a druhou pro služby ZR.

Bude tedy RPP provozovat třetí UDDI? Budou zde uvedené definice služeb používány pro tvorbu služeb vystavených na vnějším rozhraní?

Co jsou přesně artefakty, které budou definovány v RPP katalogu? Definice orchestrací? Definice služeb na vnějším rozhraní (WSDL) a jejich SLA? Definice služeb (WSDL) základních katalogů na vnitřním rozhraní? Nedochozí k překryvu s oběma ISZR UDDI? Nebo se jedná jen o „slovní popis“ těchto služeb (resp. jejich specifikaci), který pak bude předán k technické implementaci? Popis, tak jak je uvedeno v příkladech v zadávací dokumentaci RPP, příloha 3, str. 3 a dále?

Odpověď zadavatele:

Pro zamezení směřování pojmů uvádíme následující výklad:

Každá eGON služba poskytovaná na externím rozhraní ISZR se skládá z několika částí:

1. Vnější reprezentace služby jako web service – dle specifikace SOA popis služby směrem k uživateli služby využitím WDSL.
2. Vnitřní „workflow služby“ – popisuje sekvenci volání interních služeb, transformací a procesů, které je nutné vykonat pro realizaci služby.
3. Používané interní služby – na jakých službách základních registrů je služba závislá a jak mají být tyto služby volány v rámci realizace konkrétní služby.
4. Používané služby externích AIS – na jakých službách externích AIS je služba závislá a jak mají být tyto služby volány v rámci realizace konkrétní služby.
5. Slovní popis služby – zveřejněný katalog služby v textové formě – pro tvůrce AIS jako podklad pro výběr web služeb základních registrů.

Z tohoto popisu je zřejmé, že nedochází k tvorbě třetího UDDI katalogu v rámci RPP. Dále je zřejmé, že tento katalog služeb jako datovou strukturu udržuje a spravuje RPP. Zajišťuje publikaci do eGON UDDI katalogu (příslušné části katalogu služeb) a předává ISZR workflow služby pro její vykonávání.

Konkrétní návrh orchestrace – body 2,3 navrhnete. Konkrétní způsob konstrukce SLA – z bodů 2,3 a 4.