MHMPP09FLRPG

Objednávka č. 8 Objednatele

Dílčí smlouva

Na základě Rámcové dohody o poskytování služeb technologické a aplikační podpory provozu ICT č. DOH/32/03/000160/2020 (dále jen „**Rámcová dohoda**") uzavřené dne 29. 6. 2020 mezi Hlavním městem Prahou, IČO: 00064581, se sídlem Praha – Staré Město, Mariánské náměstí 2/2, PSČ 11000 (dále jen „**Objednatel**") a společností **Operátor ICT a.s.**, IČO: 027 95 281, se sídlem Dělnická 213/12, 170 00 Praha 7 (dále jen „**Poskytovatel**") objednává Objednatel Služby specialistů dle článku 3.1.3. Rámcové dohody a Přílohy č. 3 Rámcové dohody dle níže uvedených požadavků, které byly stanoveny v souladu s odst. 6.5 Rámcové dohody.

Služby budou Poskytovatelem poskytnutu v rámci Služeb specialistů dle Rámcové dohody, a to v rozsahu a za podmínek níže uvedených a v souladu s Rámcovou dohodou.

1/ NÁPRAVNÁ OPATŘENÍ SPRÁVY SLUŽBY CERTIFIKAČNÍ AUTORITA

Specifikace Služeb

Předmětem činností je realizace požadavků nápravných opatření služby certifikační autority dle následující tabulky:

Nález	Řešení
Dlouhé odezvy systému CA při generování certifikátů na serveru srvSUBCA01	Výsledek: Funkční prostředí služby CA se standardní odezvou Součinnost: MHMP – garant CA
Nedostatečný monitoring služby CA	Budou definovány jednotlivé monitory pro dohledování služby CA. Ve spolupráci se správcem monitorovacího nástroje Zabbix Výsledek: Komplexní dohled služby CA • Monitoring OS • Služeb CA • CRL • Fronta requestů na vydání certifikátů • Platnost certifikátů jednotlivých CA • další... Součinnost: MHMP - garant CA Správce systému Zabbix
Chybějící procesy	Nasazení služby CA vyžaduje jasnou definici pravidel pro vydávání certifikátů tak i pro správu certifikátů a samotné služby CA. Zároveň musí být popsány postupy, které je nutné dodržovat při vydávání a správě certifikátů. Tyto informace

	bz měli být popsány ve standardizovaných dokumentech Certificate Policy /Certifikační Politika/ (zkratka CP) and Certificate Practice Statements /Certifikační prováděcí směrnice/ (zkratka CPS). Výsledek: V prostředí MHMP bude provozována služba CA dle pravidel, které zajistí bezpečné a důvěryhodné nasazení PKI. Součinnost: MHMP odbor BEZ
Neexistující DR plány	Správce CA vytvoří dokument popisující dokument popisující obnovu služby pomocí podporovaného postupu, který bude nezávislý na obnově serverů na úrovni virtualizační platformy VMware. Výsledek: Na základě vytvořeného dokumentu bude možné provést obnovu služby CA v případech havárie případně jiné události, která způsobí poškození nebo ztrátu serveru. Řešení bude splňovat požadavky interních směrnic MHMP Součinnost: MHMP - garant CA Správce systému zálohování Správce systému Vmware
Zálohování CA je prováděno pouze na lokální disk a následně je prováděna záloha virtuálního serveru	Bude provedena revize stávajícího stavu zálohování a připraveno rozšíření o pravidelnou zálohu konfigurace CA. Následně bude ve spolupráci se správcem systému zálohování navrženo a realizováno umístění záloh mimo prostředí CA a její virtuální servery. Výsledek: Pravidelné zálohování všech komponent služby CA, které budou zařazeny do centrálního systému zálohování v prostředí MHMP. Dostupnost záloh nebude závislá na platformě VMware. Řešení bude splňovat požadavky interních směrnic MHMP Součinnost: MHMP - garant CA Správce systému zálohování
Pro správu CA je definována v AD skupina ADCS_Admins. V této skupině jsou dva účty, z nichž jeden je disablovaný účet externího pracovníka	Odebrat disablovaný účet z administrační skupiny. Výsledek: Ve skupině *ADCS_Admins* budou pouze autorizované účty správců CA Součinnost: MHMP - Správce AD
Skupiny pro role správy certifikátů neobsahují žádné účty ADCS_Operators_Users/ADCS_Operators_Systems)	Nález má vazbu na definování procesní části CA, jejíž součástí je i definice administračního modelu. Bude dořešeno v návaznosti na dokumentů CP a CPS Výsledek: Členství v administračních skupinách bude v souladu s politikou CA a definovaného administračního modelu

	Součinnost: MHMP - Správce AD
EFS recovery agent – v GPO je nastaven certifikát účtu Administrátor, který má exspirovaný certifikát v roce 2005. V dokumentaci je uvedena poznámka, že je nutné distribuovat platný veřejný EFS certifikát z nové CA, k čemu doposud nedošlo. Dle dokumentace došlo ke generování certifikátu pro EFS RA, ale veřejný certifikát není publikován v AD	Ověření klíče EFS Recovery Agenta, který je bezpečně uložen v prostředí MHMP. Následně bude zajištěno publikování veřejné části EFS certifikátu v AD. Výsledek: V AD bude publikován platný EFS certifikát, tak aby v případě používání šifrování souborů pomocí EFS byl k dispozici recovery klíč EFS Součinnost: MHMP – Správce AD Správce služby Active Directory (GPO)
Není prováděna aktualizace OS kořenové CA	V rámci pravidelného spouštění kořenové CA, která je provozována v režimu offline, bude definován postup údržby a kontroly systému jehož součástí bude i provádění aktualizace OS v intervalu minimálně 1x ročně Výsledek: Aktualizovaný OS k datu spuštění serveru kořenové CA Součinnost: MHMP – držitel Bitlocker klíče
Není definována komunikační matice pro službu CA. Není jasné, kdo je držitelem jednotlivých rolí, kontakty na držitele certifikátů KRA a EFS RA, klíč Root CA atd	Definovat komunikační matici, která bude obsahovat všechny zainteresované subjekty s vazbou na službu CA Výsledek: Jasný popis komunikace mezi subjekty. Kontaktní informace. Součinnost: MHMP - garant CA
V KL09 je definováno udržování provozní dokumentace (Postupy pro provoz a správu služby CA a Postupy pro obnovu služby CA ze záloh) tuto dokumentaci jsme neobdrželi	Zrevidovat existující dokumentaci popisující proces správy CA a doplnit chybějící části. Dokumentace musí zohledňovat popis služby definovaný v dokumentech CP a CPS. Popis obnovy služby CA bude řešen v rámci nápravných kroků v části týkající se DRP. Výsledek: Zajištění dokumentace popisující postupy správy služby CA na jednotlivých úrovních a dokumentace postupů DR Součinnost: MHMP - garant CA
V dokumentaci je vedeno zabezpečení disku pomocí systému Bitlocker. Nejsou uvedeny informace, kdo je držitelem recovery klíčů. V průběhu tranzice bylo zjištěno, že k dispozici je pouze Recovery Key pro spuštění serveru srvROOTCA01 .	Bude provedena změna/reset hesla pro spuštění OS chráněného pomocí šifrování nástrojem Bitlocker. Následně bude provedena i změna Bitlocker Recovery Key. Nově vygenerovaná hesla a obnovovací klíče budou bezpečně předány zástupci MHMP. Výsledek: MHMP bude výhradní držitelem hesla pro spuštění serveru kořenové CA a obnovovacího klíče Bitlocker Součinnost: MHMP - garant CA
Na úrovni CA je nastaveno podrobné auditování událostí. Tyto informace nejsou vyhodnocovány a kontrolovány	Servery CA jsou napojeny na systém SIEM, ale neprobíhá vyhodnocování auditních informací.

	Budou definovány události, které je z pohledu bezpečného provozování služby CA vhodné vyhodnocovat. Bude vydefinováno jakým způsobem monitorovat i provoz služby CA ve virtualizovaném prostředí (např. provozování kořenové CA v offline režimu)
Roli CA operátora zastává jedna osoba a neexistuje zastupitelnost na této úrovni. Je řešeno zástupem na úrovni správce CA, což je v rozporu s návrhem administračního modelu CA a popsaným pravidlům uvedených v dokumentaci pro CA	Je nutné zajistit provoz služby CA v takovém režimu, kde je zajištěna zastupitelnost na jednotlivých úrovních správy CA. Zastupitelnost je možná jak zajištěním personální kapacit pro jednotlivé úrovně nebo je možné řešit zastupitelností z jiných úrovní správy za předpokladu, že tento režim nebude v rozporu s administračním modelem a dokumenty CP a CPS. Výsledek: Funkční zastupitelnost v souladu s technickým řešením a bezpečnostní politikou CA Součinnost: MHMP - garant CA
Na podřízených CA jsou publikovány certifikační šablony, které nejsou v prostředí používány (vydány)	Zrevidovat požadavky na typy certifikátů, které budou jednotlivé vydávající CA poskytovat. Služba CA musí obsahovat pouze šablony, které jsou schváleny pro vydávání, a to včetně definice pravidel/konfigurace šablony. Šablony pro certifikáty, které služba CA nevydává nesmí být publikovány. Výsledek: Služba CA poskytuje certifikáty, které jsou definovány v dokumentech CP a CPS Součinnost: MHMP - garant CA
Na serverech podřízených CA jsou publikovány šablony certifikátů, které nejsou popsány v dokumentaci. (např MHMP Web Client and Server, MHMP Domain Controller 3R). Dle těchto šablon jsou vydány certifikáty.	Zrevidovat požadavky na typy certifikátů, které budou jednotlivé vydávající CA poskytovat. Služba CA musí obsahovat pouze šablony, které jsou schváleny pro vydávání, a to včetně definice pravidel/konfigurace šablony. Výsledek: Služba CA poskytuje certifikáty, které jsou definovány v dokumentech CP a CPS Součinnost: MHMP - garant CA
Server srvOCSP01 a srvROOTCA01 jsou provozovány s 4 GB RAM. V dokumentaci je uvedena hodnota 8GB RAM u obou serverů	Aktualizace údajů v dokumentaci Výsledek: Aktuální informace o sizingu serverů CA a návazných systémů
Nejsou k dispozici přihlašovací údaje pro servisní účet *svc_ADCS*	Provést analýzu využití servisního účtu *svc_ADCS* a naplánovat reset hesla v AD. Následně bude provedeno rekonfigurace všech služeb navázaných na uvedený účet (naplánované úlohy a případně další služby) Výsledek: Provedení resetu hesla servisního účtu svc_ADCS a jeho bezpečné uložení. Součinnost: MHMP – garant AD MHMP – Držitel přihlašovacích údajů CA

Nefunkční odesílani e-mailů v prostředí CA	Výsledek: Funkční e-mailové notifikace služby CA

Požadovaný termín zahájení a ukončení poskytování Služeb

Termín zahájení činností

8.2.2021

Termín ukončení činností

8.8.2021

Předpokládaný rozsah plnění a předpokládaná cena za Služby

Cena za skutečně poskytnuté Služby bude uhrazena postupem dle Rámcové dohody (viz odst. 12.3. Rámcové dohody).

Rozsah plnění a předpokládané služba vychází z nabídky NÁPRAVNÁ OPATŘENÍ SPRÁVY SLUŽBY CERTIFIKAČNÍ AUTORITA, která je přílohou této dílčí smlouvy.

Služby budou poskytovány od následujících členů realizačního týmu:

Role	02 - 08/2021
Projektový manažer	20 MD
IT specialista na OS Microsoft Windows Server – Active Directory	40 MD
Specialista architekt řešení	15 MD
Specialista řízení IT služeb	15 MD

Celková cena je 717 000 Kč bez DPH.

Akceptační kritéria

Akceptace proběhne písemným schválením výkazu plnění za poskytnuté Služby.

Případně další požadavky v rozsahu a dle potřeb Objednatele

Objednatel nestanovuje další požadavky.

Přílohy

Příloha č.1 - NABÍDKA: NÁPRAVNÁ OPATŘENÍ SPRÁVY SLUŽBY CERTIFIKAČNÍ AUTORITA

Za Ob[redacted]e

..... [redacted] ..... 05 -02- 2021

Mgr.
ředit[redacted]nformatické infrastruktury

Přijal za Poskytovatele: 8.2.2021

[redacted]

Michal Fišer, MBA
předseda představenstva

[redacted]

JUDr. Matej Šandor, Ph.D.
místopředseda představenstva

OPERÁTOR ICT

V Praze dne 21.01.2021

NABÍDKA: NÁPRAVNÁ OPATŘENÍ SPRÁVY SLUŽBY CERTIFIKAČNÍ AUTORITA

K rukám:
Mgr. Jiří Károly
odbor informatické infrastruktury
Magistrát hl. m. Prahy

NABÍZEJÍCÍ: OPERÁTOR ICT, A.S.

Operátor ICT, a.s. je městskou společností, která pro Hlavní město Prahu zajišťuje odborné služby ICT a realizaci ICT projektů pro městské části a další městské společnosti.

PŘEDMĚT NABÍDKY

Předmětem této nabídky je realizace požadavků objednatele a nápravných opatření služby certifikační autority.
Seznam nápravných opatření je obsahem přílohy.

CENOVÁ NABÍDKA

Maximální předpokládaný rozsah plnění nápravných opatření:

Název pozice/role	Sazba / J bez DPH	Jednotka (J)*	Počet J	Sazba celkem bez DPH
Projektový manažer	8.160,-	MD	20	163.200,-
IT specialista na OS Microsoft Windows Server – Active Directory	6.000,-	MD	40	240.000,-
Specialista architekt řešení	11.920,-	MD	15	178.800,-
Specialista řízení IT služeb	9.000,-	MD	15	135.000,-
Celková cena				717.000,-

*MD = man-day, člověko-den, práce pro jednoho člověka na jeden pracovní den (8 h)

Maximální cena služeb činí **717.000,- bez DPH**

Fakturace bude probíhat měsíčně na základě výkazu skutečně odpracovaných hodin.

SOUČINNOST

Součinnost je popsána u jednotlivých návrhů nápravných opatření nebo bude dohodnuta v rámci oboustranné dohody objednatele a dodavatele. U poskytování součinnosti se bude jednat zejména o poskytnutí vstupních informací a odpovídání na dotazy v písemné podobě.

Doba plnění

Realizace činnosti bude provedena do 6 měsíců od podpisu objednávky. Platnost nabídky: do 31.01.2021

Tato nabídka má pouze informativní charakter a není závazným návrhem k uzavření smlouvy.

KONTAKT

Operátor ICT, a.s.
www.operatorict.cz
IČO:02795281,
DIČ:CZ02795281

JUDr. Matej Šandor, Ph.D.
Digitálně podepsal JUDr. Matej Šandor, Ph.D.
Datum: 2021.01.21 09:21:35 +01'00'

JUDr. Matej Šandor, Ph.D.
Ředitel úseku projektového řízení a fondů

[redacted]

PŘÍLOHA

Nález	Řešení
Dlouhé odezvy systému CA při generování certifikátů na serveru srvSUBCA01	Výsledek: Funkční prostředí služby CA se standardní odezvou Součinnost: MHMP – garant CA
Nedostatečný monitoring služby CA	Budou definovány jednotlivé monitory pro dohledování služby CA. Ve spolupráci se správcem monitorovacího nástroje Zabbix Výsledek: Komplexní dohled služby CA • Monitoring OS • Služeb CA • CRL • Fronta requestů na vydání certifikátů • Platnost certifikátů jednotlivých CA • další... Součinnost: MHMP - garant CA Správce systému Zabbix
Chybějící procesy	Nasazení služby CA vyžaduje jasnou definici pravidel pro vydávání certifikátů tak i pro správu certifikátů a samotné služby CA. Zároveň musí být popsány postupy, které je nutné dodržovat při vydávání a správě certifikátů. Tyto informace bz měli být popsány ve standardizovaných dokumentech Certificate Policy /Certifikační Politika/ (zkratka CP) and Certificate Practice Statements /Certifikační prováděcí směrnice/ (zkratka CPS). Výsledek: V prostředí MHMP bude provozována služba CA dle pravidel, které zajistí bezpečné a důvěryhodné nasazení PKI. Součinnost: MHMP odbor BEZ

Neexistující DR plány	Správce CA vytvoří dokument popisující dokument popisující obnovu služby pomocí podporovaného postupu, který bude nezávislý na obnově serverů na úrovni virtualizační platformy VMware. Výsledek: Na základě vytvořeného dokumentu bude možné provést obnovu služby CA v případech havárie případně jiné události, která způsobí poškození nebo ztrátu serveru. Řešení bude splňovat požadavky interních směrnic MHMP Součinnost: MHMP - garant CA Správce systému zálohování Správce systému Vmware
Zálohování CA je prováděno pouze na lokální disk a následně je prováděna záloha virtuálního serveru	Bude provedena revize stávajícího stavu zálohování a připraveno rozšíření o pravidelnou zálohu konfigurace CA. Následně bude ve spolupráci se správcem systému zálohování navrženo a realizováno umístění záloh mimo prostředí CA a její virtuální servery. Výsledek: Pravidelné zálohování všech komponent služby CA, které budou zařazeny do centrálního systému zálohování v prostředí MHMP. Dostupnost záloh nebude závislá na platformě VMware. Řešení bude splňovat požadavky interních směrnic MHMP Součinnost: MHMP - garant CA Správce systému zálohování
Pro správu CA je definována v AD skupina ADCS_Admins. V této skupině jsou dva účty, z nichž jeden je disablovaný účet externího pracovníka	Odebrat disablovaný účet z administrační skupiny. Výsledek: Ve skupině *ADCS_Admins* budou pouze autorizované účty správců CA Součinnost: MHMP - Správce AD
Skupiny pro role správy certifikátů neobsahují žádné účty ADCS_Operators_Users/ADCS_Operators_Systems)	Nález má vazbu na definování procesní části CA, jejíž součástí je i definice administračního modelu. Bude dořešeno v návaznosti na dokumentů CP a CPS Výsledek: Členství v administračních skupinách bude v souladu s politikou CA a definovaného administračního modelu Součinnost: MHMP - Správce AD
EFS recovery agent – v GPO je nastaven certifikát účtu Administrátor, který má exspirovaný certifikát v roce 2005. V dokumentaci je uvedena poznámka, že je nutné distribuovat platný veřejný EFS certifikát z nové CA, k čemu doposud nedošlo. Dle dokumentace došlo ke generování certifikátu pro EFS RA, ale veřejný certifikát není publikován v AD	Ověření klíče EFS Recovery Agenta, který je bezpečně uložen v prostředí MHMP. Následně bude zajištěno publikování veřejné časti EFS certifikátu v AD. Výsledek: V AD bude publikován platný EFS certifikát, tak aby v případě používání šifrování souborů pomocí EFS byl k dispozici recovery klíč EFS Součinnost: MHMP – Správce AD Správce služby Active Directory (GPO)

Není prováděna aktualizace OS kořenové CA	V rámci pravidelného spouštění kořenové CA, která je provozována v režimu offline, bude definován postup údržby a kontroly systému jehož součástí bude i provádění aktualizace OS v intervalu minimálně 1x ročně Výsledek: Aktualizovaný OS k datu spuštění serveru kořenové CA Součinnost: MHMP – držitel Bitlocker klíče
Není definována komunikační matice pro službu CA. Není jasné, kdo je držitelem jednotlivých rolí, kontakty na držitele certifikátů KRA a EFS RA, klíč Root CA atd	Definovat komunikační matici, která bude obsahovat všechny zainteresované subjekty s vazbou na službu CA Výsledek: Jasný popis komunikace mezi subjekty. Kontaktní informace. Součinnost: MHMP - garant CA
V KL09 je definováno udržování provozní dokumentace (Postupy pro provoz a správu služby CA a Postupy pro obnovu služby CA ze záloh) tuto dokumentaci jsme neobdrželi	Zrevidovat existující dokumentaci popisující proces správy CA a doplnit chybějící části. Dokumentace musí zohledňovat popis služby definovaný v dokumentech CP a CPS. Popis obnovy služby CA bude řešen v rámci nápravných kroků v části týkající se DRP. Výsledek: Zajištění dokumentace popisující postupy správy služby CA na jednotlivých úrovních a dokumentace postupů DR Součinnost: MHMP - garant CA
V dokumentaci je vedeno zabezpečení disku pomocí systému Bitlocker. Nejsou uvedeny informace, kdo je držitelem recovery klíčů. V průběhu tranzice bylo zjištěno, že k dispozici je pouze Recovery Key pro spuštění serveru srvROOTCA01 .	Bude provedena změna/reset hesla pro spuštění OS chráněného pomocí šifrování nástrojem Bitlocker. Následně bude provedena i změna Bitlocker Recovery Key. Nově vygenerovaná hesla a obnovovací klíče budou bezpečně předány zástupci MHMP. Výsledek: MHMP bude výhradní držitelem hesla pro spuštění serveru kořenové CA a obnovovacího klíče Bitlocker Součinnost: MHMP - garant CA
Na úrovni CA je nastaveno podrobné auditování událostí. Tyto informace nejsou vyhodnocovány a kontrolovány	Servery CA jsou napojeny na systém SIEM, ale neprobíhá vyhodnocování auditních informací. Budou definovány události, které je z pohledu bezpečného provozování služby CA vhodné vyhodnocovat. Bude vydefinováno jakým způsobem monitorovat i provoz služby CA ve virtualizovaném prostředí (např. provozování kořenové CA v offline režimu)

Roli CA operátora zastává jedna osoba a neexistuje zastupitelnost na této úrovni. Je řešeno zástupem na úrovni správce CA, což je v rozporu s návrhem administračního modelu CA a popsaným pravidlům uvedených v dokumentaci pro CA	Je nutné zajistit provoz služby CA v takovém režimu, kde je zajištěna zastupitelnost na jednotlivých úrovních správy CA. Zastupitelnost je možná jak zajištěním personální kapacit pro jednotlivé úrovně nebo je možné řešit zastupitelností z jiných úrovní správy za předpokladu, že tento režim nebude v rozporu s administračním modelem a dokumenty CP a CPS. Výsledek: Funkční zastupitelnost v souladu s technickým řešením a bezpečnostní politikou CA Součinnost: MHMP - garant CA
Na podřízených CA jsou publikovány certifikační šablony, které nejsou v prostředí používány (vydány)	Zrevidovat požadavky na typy certifikátů, které budou jednotlivé vydávající CA poskytovat. Služba CA musí obsahovat pouze šablony, které jsou schváleny pro vydávání, a to včetně definice pravidel/konfigurace šablony. Šablony pro certifikáty, které služba CA nevydává nesmí být publikovány. Výsledek: Služba CA poskytuje certifikáty, které jsou definovány v dokumentech CP a CPS Součinnost: MHMP - garant CA
Na serverech podřízených CA jsou publikovány šablony certifikátů, které nejsou popsány v dokumentaci. (např MHMP Web Client and Server, MHMP Domain Controller 3R). Dle těchto šablon jsou vydány certifikáty.	Zrevidovat požadavky na typy certifikátů, které budou jednotlivé vydávající CA poskytovat. Služba CA musí obsahovat pouze šablony, které jsou schváleny pro vydávání, a to včetně definice pravidel/konfigurace šablony. Výsledek: Služba CA poskytuje certifikáty, které jsou definovány v dokumentech CP a CPS Součinnost: MHMP - garant CA
Server srvOCSP01 a srvROOTCA01 jsou provozovány s 4 GB RAM. V dokumentaci je uvedena hodnota 8GB RAM u obou serverů	Aktualizace údajů v dokumentaci Výsledek: Aktuální informace o sizingu serverů CA a návazných systémů
Nejsou k dispozici přihlašovací údaje pro servisní účet *svc_ADCS*	Provést analýzu využití servisního účtu *svc_ADCS* a naplánovat reset hesla v AD. Následně bude provedeno rekonfigurace všech služeb navázaných na uvedený účet (naplánované úlohy a případně další služby) Výsledek: Provedení resetu hesla servisního účtu svc_ADCS a jeho bezpečné uložení. Součinnost: MHMP – garant AD MHMP – Držitel přihlašovacích údajů CA
Nefunkční odesílani e-mailů v prostředí CA	Výsledek: Funkční e-mailové notifikace služby CA