Smlouva

o poskytnutí SW pro monitorování funkčnosti aplikace Okamžitých plateb

uzavřená podle § 1746 odst. 2 a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník,
mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1

zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní

IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel")

a

Mainstream Technologies, s.r.o.
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 110101
Hvězdova 1734/2c
140 00 Praha 4

zastoupenou: Petrem Šetkou, jednatelem společnosti

IČO: 27404978
DIČ: CZ27404978
č. účtu: 2208802001 / 5500

(dále jen „poskytovatel")

Článek I
Předmět smlouvy

1. Poskytovatel se zavazuje dodat a implementovat software pro monitorování funkčnosti aplikace Okamžitých plateb v aplikacích CERTIS – AMOS (dále jen „SW řešení"), a to jak do testovacího, tak do produkčního prostředí objednatele, včetně integrace na systémové a aplikační prostředí objednatele. SW řešení musí splňovat veškeré technické požadavky objednatele uvedené v příloze č. 2 smlouvy, musí být plně kompatibilní se standardním systémovým prostředím objednatele, specifikovaným v příloze č. 3 smlouvy, nesmí vykazovat zranitelnosti při testování podle části 4 přílohy č. 3 smlouvy a musí být realizováno v souladu s návrhem technického řešení dle přílohy č. 1 smlouvy.
2. V případě rozporu návrhu technického řešení dle přílohy č. 1 smlouvy s technickými požadavky objednatele uvedenými v příloze č. 2 smlouvy nebo návrhu technického řešení

[redacted]

dle přílohy č. 1 smlouvy se standardním systémovým prostředím objednatele specifikovaným v příloze č. 3 smlouvy, je poskytovatel povinen při plnění této smlouvy postupovat přednostně dle požadavků uvedených v příloze č. 2 smlouvy a systémovým prostředím v příloze č. 3 smlouvy.

3. Součástí plnění dle odst. 1 tohoto článku je dále:

   a) Dodání administrátorské, uživatelské a technické dokumentace, každé v jednom vyhotovení v elektronické podobě v otevřeném a strojově čitelném formátu, a to v českém jazyce. Administrátorská dokumentace bude obsahovat zejména konfigurační postupy a činnosti administrátora a dále též postupy pro věcného správce aplikace, zejména parametrizace aplikace, správu přístupových oprávnění a rolí. Uživatelská dokumentace bude obsahovat zejména popis způsobu použití aplikace koncovým uživatelem. Technická dokumentace musí obsahovat popis datového a funkčního modelu SW řešení, včetně vzájemných vazeb.

   b) Dodání datového média s čitelným, nešifrovaným a kompletním zdrojovým kódem SW řešení.

   c) Dodání všech potřebných licencí třetích stran, pokud jsou pro dodané SW řešení potřebné a nejsou součástí standardního systémového prostředí objednatele popsaného v příloze č. 3 této smlouvy, a udržování těchto licencí po celou dobu platnosti a účinnosti této smlouvy od předání a převzetí SW řešení.

   d) Zaškolení 2 administrátorů ohledně věcné a technické správy SW řešení v rozsahu 1 pracovního dne, a to v sídle objednatele, nedohodnou-li se smluvní strany jinak.

   e) Základní uživatelské nastavení SW řešení,

   f) Poskytování podpory při testování v testovacím prostředí objednatele a při akceptačním testování v provozním prostředí objednatele.

4. Poskytovatel se dále zavazuje na žádost objednatele provádět úpravy SW řešení. Úprava musí odpovídat zadání objednatele, nenarušovat funkčnost SW řešení a podléhá akceptačnímu testování.

5. Poskytovatel se rovněž zavazuje k podpoře provozu SW řešení dle čl. VI smlouvy.

6. Poskytovatel bere na vědomí, že mu nebude umožněn vzdálený přístup k serverům objednatele, na kterých bude testováno a provozováno SW řešení.

7. Objednatel se zavazuje za poskytnuté plnění uhradit ceny dle této smlouvy.

Článek II
Lhůty a místo plnění

1. Dílo bude prováděno postupně v následujících lhůtách:

   a) Poskytovatel předá SW řešení spolu s administrátorskou a uživatelskou dokumentací k instalaci do testovacího prostředí objednatele nejpozději do 4 týdnů od podpisu této smlouvy.

   b) Objednatel provede testování dodaného SW řešení v testovacím prostředí. Testování bude prováděno po dobu 1 týdne.

c) Zaškolení administrátorů bude poskytovatelem provedeno nejpozději 3 pracovní dny před předáním SW řešení k akceptačnímu testování. O plánovaném datu zaškolení informuje poskytovatel objednatele nejméně 5 pracovních dnů předem. O provedení školení sepíše poskytovatel protokol obsahující den, čas a místo školení, jména školených osob a stručný popis obsahu školení, který bude podepsán pověřenými osobami obou smluvních stran.

d) Poskytovatel předá kompletní SW řešení k instalaci do provozního prostředí objednatele, a to bez vad zjištěných v rámci testování v testovacím prostředí, včetně datového média se zdrojovým kódem k akceptačnímu testování do 8 týdnů od podpisu smlouvy.

e) Objednatel provede akceptační testování dodaného SW řešení v provozním prostředí objednatele. Akceptační testování bude prováděno po dobu 2 týdnů.

f) Poskytovatel předá SW řešení bez vad zjištěných během testování, dokumentaci dle čl. I odst. 3 písm. a) a datové médium se zdrojovým kódem dle čl. I odst. 3 písm. b) objednateli nejpozději do 12 týdnů od podpisu této smlouvy. Nejpozději při předání provede poskytovatel také základní uživatelské nastavení SW řešení. O předání a převzetí plnění bude sepsán smluvními stranami protokol, jehož přílohou je protokol o akceptačním testování, který bude podepsán pověřenými osobami obou smluvních stran.

2. Místem plnění je sídlo objednatele na adrese Česká národní banka, Na Příkopě 28, 115 03 Praha 1, nestanoví-li dále tato smlouva nebo nedohodnou-li se pověřené osoby smluvních stran jinak.

3. Požadavek, nabídka a další komunikace bude probíhat e-mailem mezi pověřenými osobami smluvních stran, nebude-li to jejich povaha vylučovat, jinak zasíláním na adresu sídla objednatele Česká národní banka, Na Příkopě 28, 115 03 Praha 1, k rukám dohodnuté pověřené osoby objednatele, nebo zasláním na adresu Mainstream technologies, s.r.o., Hvězdova 1734/2c, Nusle, 140 00 Praha 4 k rukám dohodnuté pověřené osoby poskytovatele.

Článek III
Testování

1. Při testování v testovacím a v provozním prostředí objednatele bude objednatelem ověřeno, zda SW řešení je funkční, splňuje veškeré stanovené požadavky a nevykazuje přítomnost zranitelností (viz část 4 přílohy č. 3 smlouvy).

2. Během testování je přítomen pracovník poskytovatele.

3. Vyskytne-li se během testování vada, která si vynutí přerušení testování, zejména že SW řešení je nefunkční nebo SW řešení ohrožuje bezpečnost objednatele, odstraní tuto vadu poskytovatel ve lhůtě určené objednatelem. Vyskytne-li se taková vada více než dvakrát nebo nebude-li v určené lhůtě odstraněna, je objednatel oprávněn od této smlouvy odstoupit. Testování se na dobu opravy vady přerušuje.

4. Vady zjištěné během testování v testovacím prostředí objednatele odstraní poskytovatel na místě, jinak bez zbytečného odkladu, nejpozději však do 1 týdne od jejich zjištění. Poté se testování opakuje a nejsou-li vady odstraněny, je objednatel oprávněn od smlouvy odstoupit; tím nejsou dotčeny lhůty podle čl. II smlouvy.

5. Vadám zjištěným během akceptačního testování bude přidělena kategorie podle čl. VI odst. 2; vady (technické zranitelnosti) zjištěné penetračním testováním a skenem známých zranitelností mají vždy kategorii A bez ohledu na znění čl. VI odst. 2. Akceptační testování je považováno za úspěšné, jsou-li zjištěny nejvýše 3 vady kategorie C a žádné vady kategorie A nebo B. Není-li akceptační testování úspěšné, je objednatel oprávněn od smlouvy odstoupit nebo, vyskytnou-li se nejvýše 3 vady jakýchkoliv kategorií, poskytnout poskytovateli lhůtu k jejich odstranění; budou-li vady odstraněny ve stanovené lhůtě, akceptační testování se opakuje.
6. O průběhu každého testování bude sepsán objednatelem protokol, který bude obsahovat soupis vad zjištěných, odstraněných a v případě akceptačního testování i neodstraněných a bude podepsán alespoň jednou pověřenou osobou za každou smluvní stranu.
7. O předání a převzetí díla bude sepsán objednatelem protokol, který bude případně obsahovat soupis vad kategorie C zjištěných během akceptačního testování a lhůty určené pro jejich odstranění. Protokol bude podepsán pověřenými osobami obou smluvních stran.

Článek IV
Pověřené osoby smluvních stran

1. Pověřenými osobami smluvních stran jsou:

   za objednatele:

   Ing. Zbyněk Jirovský, tel.: 724 938 987, e-mail: zbynek.jirovsky@cnb.cz;

   Ing. Vlastimil Fiala, tel.: 736 524 495, e-mail: vlastimil.fiala@cnb.cz;

   Ing. Bronislav Šmíd, tel.: 736 505 500, e-mail: bronisla.smid@cnb.cz;

   za poskytovatele:

   Eelko Truijens, tel.: +420 737201589, e-mail: Eelko.Truijens@mainstream.cz;

   Petr Šetka, tel.: +420603755434, e-mail: petr.setka@mainstream.cz.
2. V případě změny v osobě nebo údajích uvedených v odst. 1 tohoto článku jsou smluvní strany povinny nahlásit změnu následující pracovní den po provedení změny na e-mailové adresy pověřených osob druhé smluvní strany. Změna osob je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě.

Článek V
Cena a platební podmínky

1. Cena za dodávku a implementaci SW řešení podle čl. I odst. 1, včetně odměny za právo k užívání programového vybavení (licenci), činí 449 600 Kč bez DPH. K ceně bude připočtena DPH v sazbě platné v den uskutečnění zdanitelného plnění. Sjednaná cena zahrnuje veškeré náklady poskytovatele spojené s plněním uvedeným v tomto odstavci.
2. Cena za úpravu SW řešení dle čl. I odst. 4 bude stanovena jako součin hodinové sazby ve výši 2 200 Kč bez DPH a počtu hodin uvedených poskytovatelem v nabídce.

3. Cena za poskytování podpory dle čl. I odst. 5 bude stanovena jako součin hodinové sazby ve výši 2 470 Kč bez DPH a počtu skutečně odpracovaných hodin pracovníky poskytovatele na odstranění závady.

4. Daňové doklady na ceny podle odstavců 1 až 3 je poskytovatel oprávněn vystavit nejdříve v den předání a převzetí příslušného plnění. Přílohou daňového dokladu bude vždy příslušný protokol o předání a převzetí plnění, resp. o odstranění vady.

5. Doklad k úhradě (fakturu) zašle poskytovatel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel v analogové formě na adresu:

   Česká národní banka
   sekce rozpočtu a účetnictví
   odbor účetnictví
   Na Příkopě 28
   115 03 Praha 1

6. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován poskytovatelem (dále jen „určený účet"). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References), nebo číslo objednávky (ve formátu ISDOC v poli External_Order_ID ve skupině OrderReference), jsou-li objednávky v rámci smlouvy vystavovány. Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit poskytovateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

7. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřený pracovník poskytovatele povinen na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle předchozí věty.

8. Splatnost dokladu k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

9. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že je objednatel oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

Článek VI
Poskytování podpory SW řešení

1. Poskytovatel od okamžiku předání a převzetí SW řešení po celou dobu trvání smlouvy ručí za to, že SW řešení bude funkční a schopné použití ve standardním systémovém prostředí objednatele, v souladu s předanou dokumentací, a nebude vykazovat zranitelnost při periodickém testování podle části 4 přílohy č. 3 této smlouvy. Rozpor s popsaným stavem je považován za vadu SW řešení.
2. Vady SW řešení budou rozlišovány do kategorií A, B a C. Kategorii vady určuje objednatel.

   Vady kategorie A:

   - úplná nefunkčnost SW řešení jako celku nebo úplná ztráta funkcionality SW řešení;
   - použití dodaného SW řešení není bezpečné nebo vykazuje technikou zranitelnost při testování Qualys podle přílohy č. 3 části 4;
   - SW řešení vykazuje ztrátu nebo poškození dat;
   - SW řešení úplně nebo částečně neplní / přestalo plnit jakýkoliv požadavek objednatele, který má zasadní vliv na provoz SW řešení;
   - SW řešení zcela chybí naplnění požadavku objednatele, který má zasadní vliv na provoz SW řešení;
   - SW řešení ohrožuje provoz nebo dostupnost ostatních aplikací v provozním prostředí objednatele.

   Vadu kategorie A odstraní poskytovatel nejpozději do 3 pracovních dnů po jejím nahlášení, nedohodnopu-li se pověřené osoby smluvních stran jinak.

   Vady kategorie B:

   - SW řešení jako celek, jeho funkcionalita nebo jeho komponenta má omezenou funkčnost, která však nemá negativní vliv na funkčnost žádného požadavku objednatele dle přílohy č. 2;
   - SW řešení vykazuje / začalo vykazovat vadu u požadavku objednatele, který nemá zásadní vliv na provoz SW řešení;
   - SW řešení zcela chybí naplnění požadavku objednatele, který nemá zásadní vliv na provoz SW řešení.

   Vadu kategorie B odstraní poskytovatel nejpozději do 5 pracovních dnů po jejím nahlášení, nedohodnopu-li se pověřené osoby smluvních stran jinak.

   Vady kategorie C:

   - drobná vada, která nemá vliv na provoz SW řešení (např. gramatické nebo pravopisné vady v požadované dokumentaci, drobný konstrukční nedostatek SW řešení);
   - ostatní vady výše nepopsané.

   Vadu kategorie C odstraní poskytovatel nejpozději do 20 pracovních dnů po jejím nahlášení, nedohodnou-li se pověřené osoby smluvních stran jinak.

3. Objednatel nahlásí vadu včetně kategorie a jejího stručného popisu poskytovateli na tel: +420 733 708 223, a to v době od 9:00 do 17:00 hod., nebo zasláním e-mailu na e-mailovou adresu poskytovatele: helpdesk@mainstream.cz.
4. Poskytovatel potvrdí objednateli nahlášení vady nejpozději následující pracovní den, a to e-mailem zaslaným na e-mailovou adresu sdělenou při nahlášení vady nebo ze které byla vada nahlášena, popř. e-mailem zaslaným pověřeným osobám objednatele, nebudou-li předchozí způsoby potvrzení možné.
5. Poskytovatel bude odstraňovat nahlášené vady pouze v pracovní dny v době od 7:45 hod. do 16:15 hod.
6. Vady bude poskytovatel odstraňovat bez neodůvodněného přerušení od zahájení odstraňování až do úplného odstranění vady.
7. O odstranění vady bude vždy sepsán poskytovatelem protokol, který bude obsahovat alespoň charakteristiku vady, počet skutečně odpracovaných hodin na odstranění vady, datum a čas nahlášení vady a datum a čas odstranění vady, který podepíše za každou smluvní stranu alespoň jedna pověřená osoba.

Článek VII
Provádění úprav SW řešení

1. O potřebě úpravy SW řešení rozhoduje objednatel. Požadavek na úpravu SW řešení zašle pověřená osoba objednatele pověřené osobě poskytovatele. V požadavku bude uveden popis požadované úpravy a lhůta pro její provedení.
2. Poskytovatel zašle objednateli do 5 pracovních dnů od doručení požadavku nabídku, která bude obsahovat návrh technického řešení, rozpis pracnosti v hodinách a akceptaci lhůty navržené objednatelem nebo návrh jiné lhůty. Nedojde-li ohledně lhůty k dohodě, určí lhůtu objednatel s tím, že nebude kratší než 20 pracovních dnů. S realizací úpravy SW řešení může poskytovatel začít poté, co obdržel oznámení o akceptaci nabídky od pověřené osoby objednatele.
3. Součástí předání úpravy SW řešení je vždy předání čitelného, nešifrovaného a kompletního zdrojového kódu včetně aktualizované dokumentace, to vše v elektronické podobě.
4. U každé úpravy SW řešení proběhne testování, čl. III se použije obdobně vč. ustanovení o předání a převzetí, s tím, že délku testování určí objednatel, nejméně však v délce 3 dnů.

Článek VIII
Licenční ujednání

1. Poskytovatel poskytuje objednateli na dobu trvání majetkových práv k dílu nevýhradní a místně neomezenou licenci k užívání SW řešení (včetně dokumentace) a jeho úprav. Objednatel je oprávněn užívat vytvořené SW řešení a jeho úpravy (dále v tomto článku jen „SW“) všemi způsoby užití dle příslušných právních předpisů. Objednatel je zejména oprávněn:
   a) spojit SW nebo kteroukoliv jeho část s jiným autorským dílem, zařadit do jiného díla,

zařadit do díla souborného, a takto je užít způsoby dle této smlouvy,

b) zasahovat do kterékoliv části SW včetně zdrojových kódů, provádět úpravy a změny ve kterékoliv části SW včetně zdrojových kódů, a to jak sám, tak i prostřednictvím třetí osoby, a užívat takto změněný nebo upravený SW v rozsahu dle této smlouvy nebo i samostatně.

2. Objednatel se stane vlastníkem jakéhokoliv hmotného substrátu obsahujícího SW převzetím od poskytovatele. Objednatel si vyhrazuje právo zapůjčit SW třetí straně za účelem zajištění jeho údržby, provozu nebo rozvoje. Objednatel se dnem předání (poskytnutí) stává vlastníkem zdrojových kódů SW.
3. Licence umožňuje užívání SW bez omezení počtu současně pracujících uživatelů nebo kategorií uživatelského přístupu a rovněž bez omezení množství nebo typů počítačů objednatele nutných pro užívání SW řešení.
4. Za den poskytnutí příslušné licence se považuje vždy den, kdy je příslušné plnění poskytnuto objednateli k prvnímu užití.
5. Poskytovatel prohlašuje, že je licence a souhlasy dle tohoto článku objednateli oprávněn poskytnout a že na žádném z plnění dle této smlouvy neváznou žádná práva třetích osob, která by poskytnutí bránila. V případě porušení práv třetích osob chráněných autorským zákonem poskytovatel zajistí na své náklady náhradu škod uplatněných třetími osobami a nápravu vzniklého stavu tak, aby objednatel mohl SW řešení oprávněně užívat.
6. Objednatel není licence získané podle této smlouvy povinen užít.
7. Odměna za poskytnutí licencí podle této smlouvy je součástí cen podle čl. V této smlouvy.

Článek IX
Další ujednání

1. Poskytovatel se zavazuje zajistit, že jeho pracovníci, jakož i jiné osoby, které se budou podílet na plnění dle této smlouvy, zachovají mlčenlivost o všech skutečnostech, se kterými se po dobu plnění smlouvy seznámí a které nejsou veřejně dostupné. Uvádění podpory a údržby SW řešení dle této smlouvy poskytovatelem jako referenční zakázky tímto není dotčeno, vyjma případu, že by objednatel od této smlouvy odstoupil.
2. Závazek mlčenlivosti trvá i po skončení plnění podle této smlouvy.
3. Poskytovatel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 4 této smlouvy.
4. Použije-li poskytovatel při své činnosti poddodavatele, nahradí škodu jím způsobenou stejně, jakoby ji způsobil sám.
5. Poskytovatel je srozuměn s tím, že veškerá komunikace při plnění této smlouvy bude mezi poskytovatelem a objednatelem probíhat v českém jazyce.

Článek X
Smluvní pokuty, úrok z prodlení

1. V případě prodlení poskytovatele v kterékoliv lhůtě stanovené v čl. II odst. 1 písm. a), c), d) nebo e) nebo čl. VII odst. 2 je objednatel oprávněn požadovat smluvní pokutu ve výši

1 500 Kč za každý den prodlení.

2. V případě prodlení poskytovatele ve lhůtě pro odstranění vady kategorie A dle čl. VI odst. 2 je objednatel oprávněn požadovat smluvní pokutu 500 Kč za každý pracovní den prodlení.
3. V případě prodlení poskytovatele ve lhůtě pro odstranění vady kategorie B dle čl. VI odst. 2 je objednatel oprávněn požadovat smluvní pokutu 200 Kč za každý pracovní den prodlení.
4. V případě prodlení poskytovatele ve lhůtě pro odstranění vady kategorie C dle čl. VI odst. 2 je objednatel oprávněn požadovat smluvní pokutu 100 Kč za každý pracovní den prodlení.
5. Je-li telefonická linka pro nahlášení vady podle čl. VI odst. 3 nefunkční po dobu delší než 48 hodin, je objednatel oprávněn požadovat smluvní pokutu 1 500 Kč za každý pracovní den nefunkčnosti telefonické linky (včetně prvních 48 hodin).
6. V případě, že poskytovatel nepotvrdí objednateli nahlášení vady ve lhůtě podle čl. VI odst. 4 nebo je v určené hodiny nefunkční telefonická linka pro nahlášení vady podle čl. VI odst. 3 při současné nedostupnosti e-mailu pro nahlášení vady, je objednatel oprávněn požadovat smluvní pokutu ve výši 1 500 Kč za každý takový případ.
7. V případě prodlení objednatele s úhradou daňového dokladu je poskytovatel oprávněn požadovat úrok z prodlení podle předpisů občanského práva.
8. Smluvní pokuty a úrok z prodlení jsou splatné do 14 dnů ode dne doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu.
9. Ujednáními o smluvní pokutě není dotčeno právo smluvních stran na náhradu škody.

Článek XI
Trvání smlouvy, ukončení smlouvy, odstoupení od smlouvy

1. Smlouva se uzavírá na dobu neurčitou.
2. Smlouvu lze ukončit písemnou výpovědí, a to nejdříve po 4 letech od předání a převzetí SW řešení, přičemž výpovědní lhůta činí 3 měsíce a počíná běžet prvním dnem měsíce následujícího po doručení výpovědi druhé smluvní straně.
3. V případě, že některá ze smluvních stran podstatným způsobem poruší smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit.
4. Odstoupení od smlouvy je účinné doručením písemného oznámení o odstoupení druhé smluvní straně.
5. Za podstatné porušení smluvní povinnosti se považuje:

   a) ze strany poskytovatele:

   - prodlení ve lhůtě pro odstranění vady kategorie A podle čl. VI odst. 2 delší než 10 pracovních dnů;
   - prodlení ve lhůtě pro odstranění vady kategorie B podle čl. VI odst. 2 delší než

15 pracovních dnů;

- prodlení ve lhůtě pro odstranění vady kategorie C podle čl. VI odst. 2 delší než 60 pracovních dnů;
- opakovaná nefunkčnost telefonické linky pro nahlášení vady podle čl. VI odst. 3 při současné nedostupnosti e-mailu pro nahlášení vady;
- nefunkčnost telefonické linky pro nahlášení vady podle čl. VI odst. 3 po dobu delší než 10 pracovních dnů;
- opakované prodlení poskytovatele ve lhůtě podle čl. VII odst. 2.

b) ze strany objednatele:

- prodlení s úhradou daňového dokladu delší než 30 dnů.

Článek XII
Uveřejnění smlouvy a dalších souvisejících skutečností

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků, a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ"), uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.
3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejnění bude provedeno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XIII
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední ze smluvních stran.
2. Smlouvu lze měnit nebo doplňovat pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak.
3. Závazkový vztah založený touto smlouvou se řídí českým právním řádem, zejména občanským zákoníkem a dále rovněž příslušnými ustanoveními zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
4. Smlouva je vyhotovena ve třech stejnopisech, z nichž objednatel obdrží dva a poskytovatel jeden stejnopis.

Přílohy:

č. 1 – Návrh technického řešení (volně připojená příloha)

č. 2 - Technické požadavky objednatele na SW
č. 3 - Systémové prostředí a související požadavky objednatele
č. 4 - Bezpečnostní požadavky objednatele

V Praze dne: 03 -07- 2019 .....

Za objednatele:

[redacted]

.....

Ing. Milan Zirnsák
ředitel sekce informatiky

[redacted]

.....

Ing. Zdeněk Virius
ředitel sekce správní

[redacted]

ČNB ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1
48

V Praze dne: 3.7.2019

Za poskytovatele:

[redacted]

Petr Šetka
jednatel

[redacted]

Příloha č. 2

Technické požadavky objednatele na SW řešení

1. POŽADAVKY

1.1 Požadavky na funkcionalitu poptávaného SW produktu

Okamžité platby mají charakter synchronního zpracování dat a tudíž i nepatrné výpadky mohou být vnímány na obou stranách (ČNB – externí subjekt/banka) v porovnání se současně provozovaným asynchronním způsobem. Hlavním cílem aplikace SKOP je rozpoznat, jestli je závada na přenosové trase, nebo v systému ČNB.

Aplikace SKOP, umožní nestranné zobrazení funkčnosti aplikace Okamžitých plateb na straně ČNB.

Aplikace **SKOP, neslouží pro analýzu příčiny nedostupnosti, zda jde o výpadek připojení, či vlastní aplikace.** Cílem je určit subjekt odpovědný za řešení výpadku. SKOP je pouze pasivní pozorovatel funkčnosti, neúčastní se vlastního fungování okamžitých plateb a není pro něj nezbytně nutný.

Vyplývající požadavky:

1. ČNB dodá 2 samostatné servery na platformě Intel x86 s operačním systémem RedHat Linux ver. 6 nebo 7 (případně Oracle Linux) nebo s operačním systémem MS Windows 2016. Servery budou umístěny v primárním a záložním výpočetním středisku. ČNB zajistí zálohy těchto serverů.
2. Dodavatel dodá a následně bude udržovat aplikaci pro monitorování funkčnosti Okamžitých plateb.
3. Systém by měl být co nejjednodušší, s minimálními požadavky na instalace SW třetích stran.

1.1.1 Topologické umístění v síti

SKOP je umístěný v DMZ tak, aby napodobil komunikaci „fiktivní" banky, z pohledu firewallů jde o externí prostředí, a tudíž není závislý na interní síti, ani na interních systémech, webových, aplikačních či databázových serverech.

Vyplývající požadavky:

1. ČNB určí seznam monitorovaných IP adres, DNS server v tomto prostoru není k dispozici.
2. SKOP bude monitorovat aplikace na určených IP adresách a portech.

1.1.2 Výstupy

SKOP si lze představit jako „radar", který monitoruje výše uvedené IP adresy a porty, případně adresy URL v pravidelných intervalech (např. 60 sec). Zjištěné stavy zaznamenává do souboru (databáze) pro pozdější využití při reklamacích.

Vyplývající požadavky:

1. SKOP zaznamenává dostupnosti podle jednotlivých IP adres v pravidelných intervalech a tyto hodnoty uchovává minimálně 40 dní pro potřeby případných reklamací.
2. Aplikace disponuje funkcí reportu výsledků monitorování za určené období (např. den, týden, měsíc) za jednotlivý subjekt anebo celkově.
3. SKOP umožňuje operátorům v ČNB zjišťovat stav.
4. Spojení uživatele s aplikací SKOP probíhá pomocí webového prohlížeče protokolem HTTPS s ověřením platného jména a hesla uživatele.

1.1.3 Testované banky

SKOP testuje funkčnost aplikací všech bank, které se účastní na Okamžitých platbách včetně ČNB. Využívá k tomu speciální funkci „no operation (NOP)", která je součásti aplikace a která nemá žádnou výkonnou funkčnost. V ideálním případě by toto volání mohlo prověřit i konektivitu vůči databázi. Funkce NOP je provedena v hlavní smyčce aplikace, která vykonává požadavky v architektuře web services serveru. SKOP tedy funguje jako web service klient. Testované banky jsou určeny v souboru parametrů, kde každý řádek obsahuje jméno banky a URL web service, pomocí kterého je volána funkce NOP a další parametry.

Vyplývající požadavky:

1. Aplikace SKOP funguje jako Web Service Client, tj. navazuje HTTPS spojení na jednotlivé web services, které si zrealizují externí subjekty včetně ČNB samy.
2. Vstupem pro aplikaci bude soubor testovaných bank, kde jednotlivé řádky budou představovat URL web service pro volání funkce NOP.
3. Aplikace SKOP bude pro přihlášení na web service používat speciální účet.

1.1.4 Metoda testování

SKOP v určitých intervalech volá v architektuře web service klient funkci NOP v každé bance. Interval je uveden v sekundách v souboru parametrů u každé banky. Pokud není uveden, tak ve výchozím stavu, např. po 1 minutě. V souboru parametrů je taky u každé banky uveden limit na úspěšnou odpověď a limit maximálního čekání na odpověď. Pokud limity nejsou pro banku uvedeny, využije SKOP nastavené výchozí hodnoty. Výsledek testu banky je tedy buď zelená (vše v limitu), nebo oranžová (banka odpovídá, ale mimo stanovený limit), nebo červená (SKOP se nedočkal odpovědi).

Vyplývající požadavky:

1. SKOP zaznamenává průběh monitorování do souboru/databáze pro pozdější reklamaci.
2. Vstupním souborem je seznam subjektů s URL web services a parametry očekávaných odezev.
3. SKOP rozlišuje 3 stavy:

a. Plně funkčí (odezvy jsou ve stanoveném limitu, „zelená“)
b. Funkční, ale mimo stanovené limity („oranžová“)
c. Nefunkční (bez odezvy, „červená“)

1.1.5 Stavy banky

SKOP zobrazuje stav výsledku posledního testování každé banky.

1.1.6 SMS alerty a log

SKOP při změně stavu banky (k lepšímu i horšímu) zasílá SMS alert odpovědnému zaměstnanci banky. Čísla, na která jsou SMS zasílány, jsou v konfiguračním souboru pro každou banku. Každá banka může mít více čísel, na která chce aletry zasílat. Počítač, kde je SKOP provozován, nevyužívá SMS bránu ve vnitřní síti ČNB, ale umí zasílat SMS v rámci své konfigurace. Každá změna stavu je zároveň logována do souboru.

Vyplývající požadavky:

1. ČNB dodá SMS bránu a příslušené API pro zasílání SMS.
2. SKOP zasílá alerty na určená telefonní čísla s informací o změně stavu.

1.1.7 Správa SKOP

SKOP spravuje technický správce v ČNB. Má k počítači, kde je provozován SKOP, vzdálený přístup, aby mohl instalovat upgrady aplikace a operačního systému. Kromě toho provádí registraci certifikátů pro vzájemnou autentizaci SSL.

Vyplývající požadavky:

1. SKOP umožní autorizovaným uživatelům stahovat reporty.

1.2 Ostatní požadavky

V technické specifikaci nabízeného SW řešení musí být uveden způsob aktualizace.

1.3 Hardwarové a softwarové nároky aplikace

Poskytovatel SW řešení dodá takový produkt, který je plně kompatibilní se standardním prostředím ČNB, které je uvedeno v příloze č. 3 této smlouvy - Standardní prostředí ČNB a související požadavky objednatele.

2. SLOVNÍK POJMŮ

Výraz	Význam
SKOP	Stavová konzole okamžitých plateb
SEPA	Single European Payment Area - jednotná oblast pro platby v eurech.
SEPA CT	Soubor pravidel a technických norem pro provádění SEPA plateb.
SWIFT	Společnost pro celosvětovou mezibankovní finanční komunikaci.

Příloha č. 3

Systémové prostředí a související požadavky objednatele

3. SYSTÉMOVÉ PROSTŘEDÍ ČNB

SW musí akceptovat standardní systémové prostředí ČNB a musí být snadno do tohoto prostředí implementovatelný.

3.1 Serverová část

Serverové prostředí je tvořeno:

- HW platformou x86/x64 serverů s OS MS Windows Server 2008R2/2012/2016, RedHat Linux v6 nebo v7, případně Oracle Linux jako alternativní prostředí,
- virtualizovanými verzemi serverů na platformách VMWare vSphere nebo Oracle VM.

Pokud bude SW dodán s využitím těchto platforem, zajistí licence ČNB. Bude-li dodán s využitím jiných platforem, je poskytovatel zavázán dodat i potřebné licence.

3.2 Klientská část

Klientská část je založena na OS:

- MS Windows 7 Professional nebo Windows 10 (64bit) + aktuální aktualizace, nebo
- na publikovaném vDesktopu prostřednictvím Citrix XenApp 6.5 na MS Windows 2008 Server R2 (virtuální desktop využívající MS terminálové služby).

Další SW na klientské části je:

- TCP/IP síťové služby (DHCP klient, SNMP klient),
- MS .NET Framework verze 4.0 a vyšší,
- MS Office 2010 Professional Plus CZ + Service Pack 2,
- MS Internet Explorer 10 CZ (aktuální SP),
- Adobe Acrobat Reader 10 CZ – prohlížeč souborů ve formátu PDF,
- Java JRE 8.x,
- Symantec EndPoint Protection v.12.1 - antivirový program.

Instalace další provozní platformy na klientskou stanici není preferována. Instalace programového vybavení na klientskou stanici je prováděna především prostřednictvím vzdálené automatické instalace. Instalace musí být kompatibilní se službou MS Installer (standardní služba operačního systému). Instalace programového vybavení na vDesktop je prováděna centrálně pomocí tzv. image z provisioning serverů.

Není přípustné ukládat na klientskou stanici/vDesktop data trvalé hodnoty, taková data je nutno ukládat na centrální diskové kapacity. Na klientské stanici nesmí být prováděno dávkové zpracování dat IS.

Na klientské stanici a vDesktop pracuje uživatel standardně pod právy přidělené skupině „Users".

Při realizaci IS je nutné zajistit, aby programové komponenty realizovaného SW nebyly v rozporu s komponentami dalších provozovaných IS. Realizovaný SW tedy musí být provozovatelný v systémovém prostředí ČNB a současně nesmí narušovat funkčnost ostatních IS.

3.3 Datová síť

- Servery jsou připojeny typicky rychlostí 1 Gb 1000Base-T.
- Mezi servery a klientskými stanicemi je pouze L3 konektivita, mezi servery možná L2 nebo L3 konektivita.
- Adresace dle RFC 1918 (10.x.y.z 172.16-31.y.z, 192.168.y.z).
- Datová síť je plně přepínaná s redundantním jádrem.

3.4 Systémové služby

Synchronizace času

Čas na všech komponentách sítě ČNB mimo stanic uživatelů je synchronizován se zdrojem přesného času (pro zajištění správného vyhodnocení auditních záznamů).

4. BEZPEČNOST IT

Servery a na nich instalované SW produkty jsou pravidelně monitorovány a skenovány produktem QUALYS (http://www.qualys.com/). Pokud jsou nalezeny zranitelnosti u instalovaných produktů hodnoty 4 a vyšší (hodnoty výstupu ze systému Qualys), jsou neprodleně odstraněny, a to formou aplikací patchů či jiným doporučeným postupem.

Součástí akceptace systému je provedení penetračního testu a skenu známých zranitelností, přičemž systém nesmí obsahovat technické zranitelnosti dle seznamů OWASP Top 10 a CWE/SANS top 25. Testována jsou rozhraní dostupná z internetu, interním uživatelům i případná další (propojení s jinými systémy).

Všechna datová média (především pevné disky) použitá v informačním systému jsou před přemístěním mimo prostory ČNB bezpečně smazána nebo zničena.

K funkcím pro správu, změny, diagnostiku apod. systému je přístup pouze ze sítě ČNB (příp. prostřednictvím běžného vzdáleného přístupu zaměstnance ČNB do této sítě.) Poskytovatelé nemají ze svých sítí jiný přístup k systému než veřejnost.

Příloha č. 4

Bezpečnostní požadavky ČNB

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB") budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu schváleném ČNB (dále jen „seznam"). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam poskytovatel předloží ČNB nejpozději den před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků poskytovatele. Poskytovatel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu obecného nařízení o ochraně osobních údajů - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR"). Poskytovatel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že poskytovatel předá jejich osobní údaje v rozsahu: jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1 v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do budovy ČNB z důvodu ochrany majetku a osob a správy přístupového systému ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči poskytovateli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese poskytovatel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle bodu 2. nahradí poskytovatel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků poskytovatele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Při příchodu do objektů ČNB pracovníci poskytovatele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny v seznamu, nebudou do objektů ČNB vpuštěny.
6. Schválení pracovníci poskytovatele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci poskytovatele budou do prostor ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní

policie ČNB.

7. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB, a dále instrukcemi vyhlašovanými vnitřním rozhlasem ČNB.
8. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
9. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
10. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
11. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací dozorujícího zaměstnance ČNB. Dále se pracovníci poskytovatele musí zdržet poškozování či odcizování majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
12. Pracovníci poskytovatele uvedení v seznamu se musí před započetím výkonu práce v objektech ČNB seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifiky daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka poskytovatele uvedeného na seznamu ohledně dodržování těchto předpisů a ustanovení.

92-083-19

Příloha č. 1

1. Úvod

Tato část dokumentu představuje popis technické části implementace. Kromě předpokládaných technologií popisuje také myšlenky implementace a hlavní implementační kroky.

Společnost Mainstream Technologies má rozsáhlé zkušenosti v této oblasti z prostředí velkých zákazníků na území České Republiky.

Děkujeme za možnost předložit tuto nabídku a rádi bychom Vás ujistili, že jsme připraveni ji prezentovat či upravit dle Vašich požadavků.

2. Technologie

Dodavatel (Mainstream Technologies, s.r.o.) využije pro implementaci řešení SKOP dále popsané technologie.

Microsoft System Center Operations Manager

Produkt Microsoft System Center Operations Manager (dále SCOM) je součástí infrastruktury ČNB a je vhodným řešením pro využití v implementaci SKOP. Pro tuto implementaci poskytuje nativní prostředky (například dohled IP adres, cílových portů či URL adres).

Technický popis využití SCOM

Dodavatel využije dva nové servery se systémem Windows Server 2016 implementované v zóně DMZ:

1. **ČNB provede implementaci dvou nových serverů v zóně DMZ. Operační systém těchto serverů bude Windows Server 2016.**
2. **ČNB povolí na firewallu mezi DMZ a interní síti, ve které se nacházejí servery SCOM s rolí Management Server, komunikaci 5723/TCP, a to ve směru z DMZ (může být izolováno až na IP adresy oněch dvou serverů) do interní sítě na servery SCOM (role Management Server).**
3. **Na tyto servery v DMZ provede dodavatel instalaci agenta dohledového řešení SCOM. Implementace těchto agentů vyžaduje certifikát spolu s privátním klíčem (certifikát vystavený na název serveru) pro oba servery a certifikát pro samotný server SCOM, případně další servery SCOM s rolí managment server. Certifikáty spolu s privátními klíči zajití ČNB (postačí certifikáty z interní infrastruktury PKI).**
4. **Dodavatel spolu s ČNB si potvrdí funkčnost těchto nových serverů v roli agentů SCOM. Podmínkou implementace další konfigurace je plná funkčnost těchto agentů (tj. komunikace s rolemi SCOM Management server).**
5. **Na serverech SCOM provede dodavatel konfiguraci dohledu webové služby formou funkčnosti *Web Application Trasaction Monitoring*. Tato konfigurace má zdroj (to budou ony dva servery v DMZ), cíl (to bude adresa webové služby každé banky), a způsob dohledu (to bude definice účtu a způsobu jeho ověření pro každou webovou službu, dále adresa URL, obsah hlavičky požadavku, případně definice SOAP dotazu, definice času pro odpověď služby). Interval dohledu bude 60 sekund. Oba vzniklé objekty dohledu (pro každou webovou službu, protože jsou dva zdroje) budou následně zkombinovány do jednoho tak, že lepší stav každého objektu určuje stav objektu (tato konfigurace zamezí červenému stavu objektu v případě, že bude mít potíže jeden ze serverů, ze kterých se dohled provádí). Ke všem uvedeným krokům budou využity nativní prostředky dohledového řešení SCOM.**
6. **Vzniklé objekty (pro každou webovou službu dva plus kombinovaný objekt) budou standardně vidět v běžné konzole pro správu řešení SCOM (Operations Console) a nelze je odtud skrýt, tato konzola však nebude primární konzolou pro vyhodnocování stavu SKOP.**

Veškerá data určující chování dohledu (tj. jeho konfigurace), stejně jako data ze samotného průběhu dohledu, jsou uložena v databázích dohledového řešení SCOM. V samotných monitorovací počítačích jsou tyto informace uloženy pouze krátkou chvilku dočasně (do naplnění mezipaměti agenta dohledu, poté se informace přepisují).

Savision LiveMaps

Savision Live Maps od společnosti Savision je řešení třetí strany rozšiřující funkčnost řešení SCOM v několika oblastech. Pro tento případ je konkrétně využitelná prezentační vrstva.

Dodavatel toto řešení využije následujícím způsobem:

1. **Provede implementaci Savision Live Maps na určený SCOM Management Server. Součástí implementace je také webová konzola.**
2. **Vytvoří stránku (tzv. dashboard) graficky zobrazující stav webové služby každé banky (zelený, žlutý, červený) a dále zobrazující přehled aktivních alertů. Alerty se generují, dojde-li ke změně stavu webové služby směrem k horším (zelený -> žlutý, zelený -> červený, nebo žlutý -> červený) a automaticky se zavírají v okamžiku, kdy „špatný" stav objektu pomine a vrátí se do zdravého, zeleného.**
3. **Dodavatel dále vytvoří tzv. *Business application* aplikovanou na výše pospaný dashboard. *Business application* nepřinese žádný nový pohled ani informaci a bude nakonfigurována nad rámec požadavků pro SKOP. Poskytne možnost definovat cílovou dostupnost (například 99,9 %) a sledovat její plnění prostřednictvím webové stránky pro oprávněné uživatele.**
4. **Dodavatel poskytne ČNB adresu URL vytvořeného dashboardu a Business application**
5. **Dodavatel spolu s ČNB nakonfiguruje ve SCOM oprávnění pro požadované uživatele (přístup na jakoukoli webovou stránku na předaných URL – viz bod 4 výše – vyžaduje ověření jménem a heslem doménového uživatele).**

Řešení pro zprávy SMS

Dohledové řešení SCOM umí spustit proces notifikace na základě vzniku alertu či zániku chybového stavu monitorované služby, jehož výsledkem je zpráva SMS. Existuje-li již nyní nakonfigurované notifikace formou zpráv SMS z dohledového řešení SCOM, pak jej dodavatel doplní o notifikace spojené se změnami stavu dostupnosti webových služeb.

Není-li notifikační řešení pomocí SMS v dohledu SCOM nakonfigurováno, pokusí se dodavatel tento kanál do dohledu SCOM naimplementovat dle instrukcí dodaných zákazníkem.

Možnosti, kdy bude notifikace generována, jsou uvedeny v následující tabulce.

Tabulka 1 Popis generování notifikací

Situace	Notifikace/komu
Chyba koncového bodu (například webová služba na straně komerční banky)	E-mail a SMS na odpovědnou osobu za danou banku (osob může být i více)
Chyba koncového bodu na straně ČNB	E-mail a SMS na odpovědnou osobu na straně ČNB (osob může být i více)
Vrácení koncového bodu u komerční banky do zeleného stavu	E-mail a SMS na odpovědnou osobu za danou banku (osob může být i více)
Vrácení koncového bodu na straně ČNB do zeleného stavu	E-mail a SMS na odpovědnou osobu za danou banku (osob může být i více)

Informace poskytované prezentační vrstvou řešení

Prezentační vrstva řešení vznikne implementací oblastí pospaných v odstavcích výše – Microsoft System Center Operations Manager, Savision LiveMaps a Řešení pro zprávy SMS – a bude poskytovat informace uvedené v následující tabulce.

Tabulka 2 Informace z prezentační vrstvy řešení

Situace	Způsob prezentace	Poznámka
Stav webové služby konkrétní banky se změní ze zdravého na nezdravý	Změna barvy objektu webové služby na dashboardu, vygenerování alertu, odeslání notifikace pomocí SMS.	Alert je aktivní (viditelný) na dashboardu, jedním z jeho parametrů je čas jeho vzniku. Čas vzniku alertu se v případě montoringu stavu služby 1x za 60 sekund nemusí shodovat se skutečným časem výpadku, nebude se ale lišit o více, než 60 sekund.
Stav webové služby se změní zpět na zdravý (zelený)	Změna barvy objektu webové služby na dashboardu na zelenou, zavření odpovídajícího alertu.	Po zavření alert mizí z dashboardu.
Jeden z serverů považuje webovou službu za funkční, druhý za nefunkční	Žádná změna v dohledu, stav objektu webové služby je zelený.	Dohled je nastaven tak, že bere vždy lepší variantu z použitých dvou serverů.
Požadavek na zobrazení stavu služby za uplynulé období (např. Q1 kalendářního roku)	Tento report není k dispozici na dashboardu, musí jej generovat správce dohledového řešení SCOM. Report lze zobrazit až do úrovně jednotlivých hodin, tj. došlo-li k výpadku služby mezi 10. a 11. hodinou, bude na část této časové úsečky zobrazena červeně a bude u ní uvedena skutečná dostupnost v dané hodině (například 86,7 %).	Tyto reporty lze pravidelně generovat a ukládat do složky na interním serveru, nebo je automaticky odesílat e-mailem na stanovenou e-mailovou adresu.
Jeden ze serverů provádějící dohled přestane fungovat	Žádná změna v dohledu, stav monitorovaných objektů webových služeb je nadále monitorován druhým serverem, který tak určuje stav objektů.	Výpadek monitorovacího uzlu (tzv. watcher) neovlivňuje zobrazený stav monitorovaného objektu.
Oba servery provádějící dohled přestanou současně fungovat	Stav monitorovaných objektů bude zobrazen šedou barvou. Pro obsluhu je toto informace, že dohled řešení není funkční. Stav monitorovaného objektu bude v reportu dostupnosti veden jako *Unmonitored* a tento výpadek nebude standardně (tj. bez další konfigurace) počítán do nedostupnosti služby.	Tento stav je nutné řešit na úrovni správy dohledového řešení SCOM. Příčinou ale také může být například změna konfigurace firewallu, která způsobí přerušení komunikace ze serverů v DMZ na SCOM Management servery.
Přestane fungovat dohledové řešení SCOM	Objekty monitorovaných webových služeb buď změní svoji barvu na šedou (viz popis situace o řádek výše), nebo zůstanou	

Situace	Způsob prezentace	Poznámka
	v poslední aktuální barvě. Nebude ale funkční dohled, tj. například nedojde ke změně na červenou barvu, pokud by webová služba vypadla, nebo z červené na zelenou, pokud by služba začala po předchozím výpadku fungovat.	

Souhrn technického řešení dle sktruktury Přílohy 2 poptávkového dokumentu

Tato část shrnuje výše poskytnuté informace do struktury požadované poptávkovým dokumentem.

1.1 Požadavky na funkcionalitu poptávaného SW produktu

Dodavatel využije dva servery se systémem Windows Server 2016.

Dodavatel dodá a bude udržovat řešení (aplikaci) pro monitorování funkčnosti Okamžitých plateb. Toto řešení bude využívat interní monitorovací řešení SCOM, přidá k němu pouze prezentační vrstvu tvořenou produktem Savision Live Maps.

1.1. Topologické umístění v síti

Servery, které budou fyzicky provádět dohled, budou umístěny v DMZ. Služba DNS není pro řešení požadována. Z DMZ do interní sítě musí existovat potřebný prostup (být povolen provoz protokolu TCP na portu 5723, aby mohly tyto dva nové agenty komunikovat s dohledovým řešením SCOM.

SW Savision Live Maps bude nainstalován na interní server SCOM Management Server, na kterém bude i webová konzola pro zobrazení aktuálního stavu dohledu a alertů. SKOP bud monitorovat koncové body pomocí dotazů na webovou službu pomocí protokolu HTTP (IP adresy a porty dodá ČNB).

1.1.2 Výstupy

1. Informace o stavu koncového bodu (webové služby) se monitorují v intervalu 60 sekund. Zpětně jsou informace o stavu dostupné po dobu existující retence datového skladu SCM (výchozí hodnota je 13 měsíců, má-li ji ČNB změněnu, pak bude nastavena na minimálně 40 dnů. To samé platí pro uchování vzniklých alertů.

2. Reporting stavu jednotlivých monitorovaných koncových bodů je dostupný zpětně v intervalu popsaném ve větě bezprostředně výše, informace se dají rozpadnou až na jednotlivé hodiny dne. Reporty bude generovat přímo řešení SCOM a zasílat je e-mailem nebo je ukládat do sdílené složky. Na vyžádání je generuje operátor SCOM, který má k takovému kroku udělená oprávnění. Běžní uživatelé tyto reporty generovat nemohou.

3. SKOP umožní uživatelům v ČNB zobrazit aktuální stav jednotlivých koncových bodů (webových služeb). Uživatel musí disponovat potřebnými přístupovými oprávněními, aby si mohl dashboard se stavem těchto bodů zobrazit.

4. Uživatelé se k dashboardu SKOP připojují prostřednictvím webového prohlížeče pomocí protokolu HTTP nebo HTTPS (záleží na konfiguraci).

1.1.3 Testované banky

1. Řešení SKOP testuje dostupnost aplikací každé banky pomocí dotazu na webovou službu. K tomu použije adresu dodanou IP a port, specifické informace v hlavičce požadavku, případně definovaný SOAP dotaz, aby byla využita funkce NOP. Definici těchto informací dodá ČNB.

2. Každá banka bude mít reprezentována vlastní webovou službou. Informace v souboru dodané ČNB přepíše Dodavatel do monitorovací logiky dohledového řešení SKOP ručně, stejně jako ke každé bance vytvoří stavový objekt na dashboardu. Automatické zpracování informací ve smyslu soubor -> SKOP není možné.

3. Ověření požadované webovými službami (jméno/heslo) je podmínkou konfigurace takového dohledu v dohledovém řešení SKOP a bude realizováno nativními prostředky existujícího dohledového řešení SCOM.

1.1.4 Metoda testování

1. Informace z dohledu se ukládají do databáze dohledového řešení SCOM. Řešení SKOP nepoužívá žádnou svoji databázi. Informace z této databáze lze zpětně získat pomocí reportů (přehled generovaných alertů, nebo stav jednotlivých webových služeb).

2. Vstupní soubor je důležitý pro Dodavatele, který informace z něj použije v konfiguraci dohledu. Neexistuje možnost, že by se dohled konfiguroval automaticky podle takového souboru.

3. SKOP bude rozlišovat pro každou webovou službu tři stavy: Funkční (zelený), Warning (žlutý), nebude.li odpověď vrácena v požadovaném limitu (tento limit určí ČNB, a červený (Critical), nebude-li webová služba odpovídat nebo nebude-li vracet očekávané informace.

1.1.5 Stavy banky

SKOP zobrazuje při aktuálním pohledu stav každého objektu (webové služby) zjištěný při posledním dotazu (dotazy probíhají v minutových intervalech).

1.1.6 SMS alerty a log

V rámci implementace dohledu dodavatel nakonfiguruje zasílání zpráv SMS na definované příjemce (ty dodá ČNB) při každé změně stavu monitorované webové služby.

1.1.7 Správa SKOP

SKOP umožní generovat a stáhnout report uživatelům, kteří mají potřebná oprávnění a umí pracovat s nástroji dohledu SCOM. Pro uživatele, kteří tato oprávnění nemají, nebo neumějí pracovat s nástroji dohledového řešení SCOM, může reporty zasílat e-mailem, nebo je po ně ukládá do sdílené složky, do které mají přístup. Reporty jsou v takovém případě ve formátu PDF nebo XLSX (ČNB si vybere jeden z těchto formátů).

1.2 Ostatní požadavky

Aktualizaci řešení (produktu Savision Live Maps) provádí dodavatel v souladu se smlouvou v následujících případech:

- Aktualizace obsahuje opravu kritických chyb zabezpečení

Aktualizaci provede dodavatel ručně.

1.3 Hardwarové a softwarové nároky aplikace

Dodaný produkt (Savision Live Maps a dohledová logika) v rámci dodávky SKOP je plně kompatibilní se standardním prostředím ČNB specifikovaným v Příloze 3 zadávací dokumentace.