Smlouva
o dodávce řešení proxy serveru

uzavřená podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník"), mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Vladimírem Mojžíškem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČ: 48136450
DIČ: CZ48136450

(dále jen „objednatel" nebo „ČNB")

a

T-Mobile Czech Republic a.s.
Tomíčkova 2144/1
148 00 Praha 4 – Chodov
zastoupenou: Ing. Petrem Malimánkem, Corporate & Public Sales Director, na základě pověření, uvedeného v příloze č. 12 této smlouvy
a
Ing. Petrem Žáčkem, Senior manažerem prodeje segmentu bankovnictví a financí, na základě pověření, uvedeného v příloze č. 12 této smlouvy
IČO: 64949681
DIČ: CZ64949681
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 3787

(dále jen „zhotovitel").

Preambule

Objednatel umožnuje prostřednictvím řešení proxy serveru svým zaměstnancům pro plnění jejich pracovních povinností zabezpečený přístup (URL browsing) do Internetu. Současná instalace tohoto řešení se již blíží konci své morální a fyzické použitelnosti a objednatel jej musí nahradit novým řešením proxy serveru, které bude dlouhodobě do budoucnosti provozně podporované.

Objednatel očekává, že nabízené řešení proxy serveru bude provozně spolehlivé a optimalizované pro bezpečný přístup zaměstnanců objednatele do Internetu, a dále umožní jeho průběžný rozvoj, včetně na něm provozovaných programových prostředků (např. patchování, upgrade na podporované verze výrobce řešení) v dlouhodobé perspektivě (minimálně po dobu 5 let).

Řešení proxy serveru bude standardní, na trhu dostupné a dodávané zařízení/systém včetně služby jeho provozní podpory, nebude se jednat o specializované zařízení/systém vytvořený/é jednorázově pouze pro potřeby objednatele.

Vzhledem k důležitosti předmětného řešení proxy serveru pro plnění pracovních úkolů zaměstnanců objednatele a zabezpečení jeho interních informačních systémů, stanovuje objednatel dále uvedené požadavky, lhůty, platební podmínky, smluvní pokuty a další smluvní ujednání, které z této důležitosti pro objednatele vycházejí.

Článek I
Předmět plnění

1) Předmětem této smlouvy je povinnost zhotovitele dodat objednateli a v jeho prostředí implementovat, zkonfigurovat a zprovoznit řešení proxy serveru, vypracovat dokumentaci skutečného stavu implementace a konfigurace řešení proxy serveru a zaškolit odborné pracovníky objednatele (dále též „dílo").

   Dodávka řešení proxy serveru a jeho implementace bude realizována v souladu s přílohou č. 1, a dále musí splňovat funkční požadavky objednatele uvedené v příloze č 2 této smlouvy. Dodávka řešení proxy serveru včetně implementace řešení proxy serveru musí být realizována také v souladu s návrhem technického řešení zhotovitele (příloha č. 7 této smlouvy). Základní požadavky na řešení proxy serveru jsou následující:

   a) Řešení proxy serveru bude zahrnovat technické („HW") a programové prostředky („SW") včetně navazujících služeb pro zabezpečený přístup současně pro minimálně 1500 uživatelů (zaměstnanců objednatele) a případně dalších zařízení (např. pracovní stanice, server - minimálně 100 ks) z vnitřní sítě objednatele do Internetu. Řešení proxy serveru bude obsahovat zejména následující bezpečnostní funkce/služby (podrobný výčet viz příloha č. 2):

      - kategorizace webových stránek s funkcí URL filteringu,
      - detekce narušení sítě (Intrusion Prevention Systém – IPS),
      - ochrana před škodlivým kódem Malware (Antivir, Antispyware, Antimalware),
      - rozpoznání a analýza aplikací na základě jejich L7 otisku (Aplication Control),
      - AntiBot,
      - inspekce předmětných protokolů včetně šifrovaných variant (zejména HTTPS) z hlediska výše uvedených bezpečnostních funkcí,
      - ochrana proti Zero Day útokům a neznámým hrozbám (SandBoxing).

   b) Toto řešení bude realizováno ve formě dvou vzájemně se zálohujících instalací implementovaných ve dvou geograficky vzdálených lokalitách (viz místa plnění v čl. II odst. 2) a umístěných na perimetru objednatele. Obě instalace budou propojeny tak, aby v případě výpadku systému v jedné instalační lokalitě objednatele bylo automatizovaně aktivováno připojení uživatelů a zařízení do Internetu přes druhou instalaci ve druhé instalační lokalitě.

   c) Řešení proxy serveru musí dále zajistit (v obou lokalitách plnohodnotně) centrální řízení a konfigurace tohoto řešení proxy serveru a uchovávání záznamů o přístupech

(uživatelů a zařízení) na cíle v Internetu (po dobu minimálně 13 měsíců) včetně možnosti jejich třídění, vyhledávání v nich a reportování.

2) Součástí předmětu plnění je také dodání uživatelské dokumentace výrobce technických prostředků, dokumentace programových prostředků obsažených v řešení proxy serveru a jejich konfigurace včetně jejího funkčního popisu.

3) Plnění podle odst. 1 a 2 tohoto článku smlouvy bude realizováno v níže definovaných etapách, které budou předmětem akceptace podle čl. III a zahrnují:

1. etapa: Realizační studie

První etapa je zaměřena na detailní analýzu požadavků objednatele (příloha č. 2) s cílem ověřit realizovatelnost nabízeného technického řešení proxy serveru (příloha č. 1 a 7) v podmínkách objednatele, ověřit a rozpracovat soulad s požadavky objednatele a identifikovat případné technické problémy či dosud neidentifikované změny a požadavky, které by vznikly v souvislosti implementací řešení proxy serveru do prostředí objednatele.

Výstupem této etapy bude podrobná realizační studie, která bude vycházet z šablony realizační studie (příloha č. 10). Ve studii budou dále navrženy akceptační testy, upřesněný harmonogram realizace a způsob zaškolení odborných pracovníků objednatele.

Ze studie musí být objednatel schopen ověřit, že navrhované řešení proxy serveru splňuje požadavky objednatele, vyhovuje jeho potřebám, jeho provozním zvyklostem a je implementovatelné ve lhůtách uvedených v této smlouvě. Dále u případně nově identifikovaných požadavků či změn souvisejících s implementací řešení proxy serveru v prostředí objednatele neuvedených v příloze č. 1 a 7 této smlouvy musí realizační studie obsahovat vypořádání takových požadavků či změn, které je smluvními stranami odsouhlaseno.

První etapa se bude sestávat z následujících činností (týká se obou instalačních lokalit a činnosti zabezpečuje zhotovitel v místě plnění (ne vzdáleně), není-li stanoveno jinak):

a) provedení workshopů mezi odbornými pracovníky objednatele a zhotovitele v rozsahu min. 2 dny s cílem získat potřebné informace a zafixovat a podrobně popsat technické řešení proxy serveru a procesy jeho instalace / aktivace / zprovoznění v prostředí objednatele,

b) vytvoření realizační studie,

c) ve spolupráci obou smluvních stran akceptaci realizační studie.

Akceptovaná realizační studie je pro zhotovitele závazná a stává se volně připojenou přílohou č. 11 této smlouvy.

2. etapa: Instalace a zprovoznění řešení proxy serveru v obou instalačních lokalitách ČNB

Druhá etapa je zaměřena na instalaci a aktivaci kompletního nového řešení proxy serveru v prostředí objednatele a převod uživatelů a zařízení nejdříve v omezeném počtu pro ověření funkčnosti (všech požadovaných funkcionalit dle přílohy č. 2 této smlouvy) nového řešení proxy serveru a později všech zaměstnanců objednatele pro ověření výkonnosti a kapacitní propustnosti nabízeného řešení proxy serveru. V závislosti na postupu implementace řešení v prostředí objednatele bude probíhat průběžná dodávka a aktivace potřebných licencí pro řešení proxy serveru (software, služby, aktivace služeb či komponent řešení proxy serveru atd.).

Výstupem je nové plně funkční řešení proxy serveru.

Druhá etapa zahrnuje následující činnosti (týká se obou instalačních lokalit a činnosti zabezpečuje zhotovitel v místě plnění (ne vzdáleně), není-li stanoveno jinak):

a) dodávka technických prostředků řešení proxy serveru (servery/výpočetní jednotky/appliance, diskové kapacity, komponenty pro interní komunikační propojení komponent řešení proxy serveru včetně propojovací kabeláže a komunikační interface pro externí komunikaci řešení proxy serveru prostřednictvím LAN (datová, management/monitoring) atd.) v souladu se specifikací uvedenou v příloze č. 1,

b) fyzická instalace výpočetních a diskových kapacit řešení proxy serveru do racků objednatele včetně jejich vzájemného komunikačního propojení a připojení na napájení,

c) konfigurace komunikačního propojení řešení proxy serveru do Internetu i do vnitřní sítě objednatele (datové propojení, propojení pro management, monitoring a sandboxing atd.), konfigurace firmware/BIOS, instalovaných výpočetních a diskových kapacit,

d) instalace/aktivace a konfigurace programových prostředků řešení proxy serveru v aktuálních verzích včetně dostupných servisních balíků či patchů, tj. zejména:

   i) operační systém,

   ii) aplikační software řešení proxy serveru,

   iii) software pro bezpečnostní funkce,

   iv) software pro administraci a monitoring řešení,

   v) napojení řešení proxy serveru na služby systémového prostředí objednatele (adresářové služby (AD), zálohování, SIEM, DNS, NTP, monitoring (např. SNMP), emailové notifikace (např. SMTP) apod.,

e) ve spolupráci s objednatelem instalace/aktivace programových prostředků na klientských zařízeních zaměstnanců objednatele a aktivace použití nového řešení proxy serveru pro cca 100 uživatelů, a dále pro cca 10 zařízení (např. server).

   Po realizaci výše uvedené instalace a zprovoznění řešení proxy serveru bude objednatelem proveden funkční test dle přílohy č. 3 za účelem ověření, že nabízené řešení nevykazuje provozní chyby, umožňuje zálohovaný provoz v rámci obou instalačních lokalit objednatele („High Availability řešení") a zároveň budou odzkoušeny bezpečnostní funkce požadované objednatelem,

f) ve spolupráci s objednatelem instalace/aktivace programových prostředků na klientských zařízeních zaměstnanců objednatele a aktivace použití nového řešení proxy serveru pro všechny zbývající uživatele a zařízení objednatele a další funkce (např. stahování patchů pro servery objednatele).

   Po dokončení instalace a zprovoznění řešení proxy serveru bude opakován funkční test dle přílohy č. 3 za účelem ověření, že nabízené řešení nevykazuje provozní chyby a zároveň bude ověřena dostatečná výkonnostní kapacita a celková propustnost nového řešení proxy serveru požadované objednatelem dle požadavků objednatele,

g) provádění průběžného zaškolení maximálně 4 odborných zaměstnanců objednatele (2x role administrátor/operátor řešení proxy serveru, 2x bezpečnostní architekt) v délce, kterou určí zhotovitel (minimálně však 2 dny) tak, aby vyškolení zaměstnanci objednatele byli schopni zajišťovat běžný provoz a údržbu včetně konfigurace dodaných technických a programových prostředků řešení proxy serveru. Popis

jednotlivých školení bude uveden v realizační studii (první etapa projektu), termín školení bude oznámen zhotovitelem vždy nejméně 5 pracovních dnů před jeho uskutečněním. Další požadavky na zaškolení jsou:

i) skupina operátorů/administrátorů řešení proxy serveru nemůže být z provozních důvodů školena najednou (z tohoto důvodu objednatel předpokládá 2 školení, každé v rozsahu minimálně 2 dny),

ii) objednatel preferuje realizovat školení v prostorech objednatele v instalační lokalitě 1. Školení může být realizováno i v prostorách zajištěných zhotovitelem mimo prostory objednatele, avšak takové prostory musí být na území Hlavního města Prahy a pro pracovníky objednatele musí být dosažitelné z instalační lokality 1 prostřednictvím MHD do 30 minut,

iii) školícím jazykem bude čeština,

iv) zhotovitel zajistí případné potřebné školící materiály (český jazyk).

h) vypracování či kompletace dokumentace v českém jazyce s využitím na Internetu obecně dostupných manuálů či schémat atd., jejichž seznam je uveden níže:

i) zpracování popisu finálního stavu implementovaného řešení proxy serveru, který musí obsahovat všechny nezbytné informace pro instalaci technických a programových prostředků nad rámec jejich defaultního nastavení (skutečný stav zapojení, nastavení/konfigurace, postupů při provozu, nastavení účtů či bezpečnostních opatření/funkcí, clustering – high availability, zálohování/obnova atd.),

ii) základní dokumentace dodávaná výrobcem řešení proxy serveru typicky např. Admin Guide, Implementation Guide, Licensing Guide apod. (může být po dohodě dodáno i v anglickém jazyce),

iii) zápisy z jednání a protokolů o implementaci, nastavení a předání funkčních celků řešení proxy serveru objednateli,

iv) zpracování zápisů/protokolů o zaškolení zaměstnanců objednatele,

v) dokumentace pro podporu provozu řešení proxy serveru, není-li již obsažena výše:

(1) postupy pro vypnutí/zapnutí řešení proxy serveru pro případ řízeného odstavení, tj. popis postupu řízeného vypnutí lokality tak, aby byl zajištěn provoz ve druhé instalační lokalitě,

(2) havarijní postupy pro případ výpadku některých komponent dodaného řešení proxy serveru (obvyklé/očekávané závady), tj. pro operátory/administrátory popis řešení, co mají zajistit v případě výpadku některé z komponent na řešení proxy serveru v jedné instalační lokalitě (troubleshooting),

(3) doporučené provozní postupy, tj. doporučení pro operátory/administrátory, jaké činnosti/kontroly by měly provádět rutinně denně/týdně/měsíčně na implementovaném řešení proxy serveru. Jedná se o popis postupu komunikace s externí podporou řešení proxy serveru zhotovitelem, tj. komu/kdy/jak hlásit provozní závady (nesmí být v rozporu s přílohou č. 5 smlouvy),

vi) základní popis procesů a cyklů patchování (upgrade, update), tj. uvedení standardní četnosti, proces jejich aplikace s rozdělením odpovědností (co zajišťuje objednatel, co zhotovitel, výrobce řešení proxy serveru aj.).

3. etapa: Ověřovací provoz nového řešení proxy serveru

Třetí etapa je zaměřena na ověření funkční a provozní spolehlivosti v delším časovém horizontu 2 měsíců nabízeného nového řešení proxy serveru a procesů provozní podpory tohoto řešení zhotovitelem. Na závěr bude dokončena finální verze dokumentace.

Třetí etapa bude sestávat z následujících činností (týká se obou instalačních lokalit a činnosti zabezpečuje zhotovitel v místě plnění (ne vzdáleně), není-li stanoveno jinak):

a) provoz, monitoring a průběžné odstraňování případných vad vzniklých při provozu řešení proxy serveru v souladu s postupy dle této smlouvy a dokumentace dle bodu g) druhé etapy projektu,

b) případná aktualizace dokumentace dle bodu g) druhé etapy projektu.

4) Zhotovitel zodpovídá za to, že provoz programového vybavení instalovaného na implementovaném řešení proxy serveru je ve všech fázích implementace v souladu s licenčními podmínkami použitého software či služeb.

5) Činnosti uvedené v odst. 3 tohoto článku se realizují v pracovní dny během standardní pracovní doby objednatele (7:45 až 16:15 - časové pásmo místa plnění), pokud se objednatel a zhotovitel nedohodnou jinak.

6) Součástí díla je poskytování provozní podpory a bezpečnostních služeb po dobu provádění 2. a 3. etapy díla, a to podle odstavce 7 a podle přílohy č. 5 smlouvy.

7) Předmětem této smlouvy je dále závazek zhotovitele poskytovat pro finálně akceptované řešení proxy serveru provozní podporu podle přílohy č. 5 smlouvy. Provozní podpora zejména zahrnuje:

a) servis a opravu technických prostředků řešení proxy serveru (HW),

b) odstraňování závad programových prostředků řešení proxy serveru (SW),

c) informování objednatele o nových update a upgrade pro jednotlivé komponenty řešení proxy serveru a na výzvu objednatele poskytnutí update, upgrade a patch včetně jejich implementace v prostředí objednatele, a to v souladu s obchodními a licenčními podmínkami výrobce,

d) zajištění bezpečnostních služeb (např. stahování signatur antiviru, IPS, kategorizace URL apod.).

8) Předmětem této smlouvy je dále závazek zhotovitele poskytovat případnou přímou pomoc a konzultační podporu objednateli ohledně implementovaného řešení proxy serveru ohledně jeho dalšího rozvoje, možné automatizace či napojení na interní informační systémy objednatele. Plnění dle tohoto odstavce je zhotovitel povinen poskytnout nejpozději do 14 dní od obdržení požadavku objednatele, nedohodnou-li se smluvní strany jinak.

9) Předmětem této smlouvy je dále závazek zhotovitele poskytnout objednateli produkty či služby zajišťující zvyšování výkonnosti řešení proxy serveru a rozšiřování jeho bezpečnostních funkcionalit včetně provozní podpory, které byly vymezeny jako tzv. vyhrazená změna závazku v zadávacím řízení. Postup při uzavření dodatku k této smlouvě na uvedené služby se bude řídit pravidly pro jednací řízení bez uveřejnění dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

10) Zhotovitel bere na vědomí, že mu v rámci implementace řešení proxy serveru v prostředí objednatele ani později v rámci podpory implementovaného řešení nebude umožněn vzdálený přístup k tomuto řešení ani k jiným serverům objednatele.

11) Objednatel se zavazuje poskytnout zhotoviteli potřebnou součinnost a za poskytnuté plnění uhradit cenu dle čl. IV.

Článek II
Lhůty a místa plnění

1) Zhotovitel se zavazuje předat plnění dle článku I odst. 1 až 2 nejpozději do 7 měsíců od podpisu smlouvy, přičemž první etapa projektu musí být dokončena do 2 měsíců od podpisu smlouvy a druhá etapa projektu musí být dokončena do 5 měsíců od podpisu smlouvy.

2) Místem plnění jsou prostory výpočetních středisek v objektech objednatele:
   - instalační lokalita č. 1: Na Příkopě 28, 115 03 Praha 1;
   - instalační lokalita č. 2: Strojírenská 175, 155 21 Praha 5.

3) Poskytování provozní podpory dle článku I odst. 7 zahájí zhotovitel první kalendářní den po závěrečné akceptaci řešení proxy serveru.

4) Objednatel se zavazuje umožnit zhotoviteli vykládku a úschovu prostředků nového řešení proxy serveru dle čl. I odst. 3 (2. etapa, písm. a)) v prostorách objednatele určených k instalaci v termínu (tj. určí konkrétní den a čas), o kterém byl zhotovitelem informován nejméně tři pracovní dny předem. Objednatel převezme prostředky do úschovy a zajistí jejich bezpečné uskladnění do zahájení instalace.

5) Zhotovitel prohlašuje, že technické prostředky řešení proxy serveru budou nové a nepoužité, vyjma výrobních procesů jako např. testy funkčnosti, nebo ověření funkčnosti v rámci případné kompletace řešení proxy serveru výrobcem či zhotovitelem před jejich dodáním (tyto však budou typově totožné, jako finální).

Článek III
Akceptace, ověřovací provoz, předání a převzetí plnění

1) Zhotovitel umožní objednateli kontrolovat průběh implementace řešení proxy serveru a za tím účelem poskytne objednateli potřebnou součinnost.

2) Akceptační řízení bude prováděno pro každou etapu uvedenou ve článku I odst. 3, a to podle přílohy č. 3 smlouvy. Akceptační řízení začne předložením potřebných podkladů zhotovitelem k příslušnému předmětu akceptace.

3) Zhotovitel je oprávněn zahájit další etapu až poté, co objednatel akceptoval předchozí etapu.

4) O ukončení každého akceptačního řízení bude sepsán akceptační protokol, který vyhotovuje zhotovitel. V případě akceptace s výhradami bude přílohou protokolu seznam zjištěných vad, stručný popis způsobu jejich odstranění včetně termínu pro realizaci jejich nápravy. K akceptačnímu protokolu se vyjádří objednatel nejpozději do 3 pracovních dnů po jeho obdržení. Akceptační protokoly podepisují pověřené osoby uvedené v čl. V odst. 10 (postačuje jedna z nich za každou smluvní stranu).

5) Dílo bude zhotovitelem předáno a objednatelem převzato po úspěšném ověřovacím provozu na základě závěrečného akceptačního protokolu, který podepíší pověřené osoby obou smluvních stran pokud:
   a) řešení proxy serveru bylo implementováno v souladu s přílohami 1, 2 a 7 této smlouvy a akceptovanou realizační studií,

b) byly splněny podmínky akceptace dle přílohy č. 3,

c) byly aktivovány bezpečnostní služby,

d) zhotovitel dodal aktuální požadovanou dokumentaci dle čl. I odst. 3 (3. etapa, písm. b)),

e) zhotovitel poskytl veškeré potřebné licence pro správný a bezproblémový provoz řešení proxy serveru. Poskytnuté licence odpovídají licenčním ujednáním dle čl. VI.

6) Zhotovitel garantuje, že:

a) dodané a implementované řešení proxy serveru je schopno rutinního provozu ve standardním systémovém prostředí objednatele (příloha č. 6), a to i za pravidelného nasazování aktualizací (update/upgrade/patch/hotfix) komponent systémového prostředí objednatele,

b) dodané a implementované řešení proxy serveru je funkční dle předané finální dokumentace,

c) řešení proxy serveru bude podporované a provozuschopné včetně jeho průběžného rozvoje minimálně po dobu 5 let od převzetí objednatelem.

Článek IV
Ceny plnění a platební podmínky

1) Cena plnění podle čl. I odst. 1 a 2 činí celkem 4.425.172,- Kč bez DPH, z toho činí cena školení 54.261,- Kč bez DPH. Podrobná specifikace této ceny plnění je obsažena v příloze č. 8 této smlouvy.
2) Cena za provozní podporu dle čl. I odst. 7 činí:
    1. v prvním roce provozu 135.912,- Kč bez DPH za rok,
        i. z toho cena za HW činí 40.692,- Kč bez DPH,
        ii. z toho cena za SW činí 40.692,- Kč bez DPH,
        iii. z toho cena za bezpečnostní služby činí 40.692,- Kč bez DPH,
        iv. z toho cena za službu HelpDesk činí 13.836,- Kč bez DPH,
    2. v druhém roce provozu 135.912,- Kč bez DPH za rok,
        i. z toho cena za HW činí 40.692,- Kč bez DPH,
        ii. z toho cena za SW činí 40.692,- Kč bez DPH,
        iii. z toho cena za bezpečnostní služby činí 40.692,- Kč bez DPH,
        iv. z toho cena za službu HelpDesk činí 13.836,- Kč bez DPH,
    3. ve třetím roce provozu 135.912,- Kč bez DPH za rok,
        i. z toho cena za HW činí 40.692,- Kč bez DPH,
        ii. z toho cena za SW činí 40.692,- Kč bez DPH,
        iii. z toho cena za bezpečnostní služby činí 40.692,- Kč bez DPH,
        iv. z toho cena za službu HelpDesk činí 13.836,- Kč bez DPH,
    4. ve čtvrtém roce a v dalších letech provozu 196.968,- Kč bez DPH za rok,
        i. z toho cena za HW činí 61.044,- Kč bez DPH,
        ii. z toho cena za SW činí 61.044,- Kč bez DPH,
        iii. z toho cena za bezpečnostní služby činí 61.044,- Kč bez DPH,
        iv. z toho cena za službu HelpDesk činí 13.836,- Kč bez DPH.
3) Cena za konzultační podporu dle čl. I odst. 8 bude účtována podle skutečného počtu hodin poskytnuté konzultační podpory a hodinové sazby, která činí 848,- Kč bez DPH za hodinu.

4) Na cenu díla poskytne objednatel zhotoviteli

   a) první zálohu ve výši ceny realizační studie uvedené v příloze č. 8, nejvýše však 50 000,- Kč,

   b) druhou zálohu ve výši ceny druhé etapy projektu uvedené v příloze č. 8. Výše zálohy nepřesáhne 70 % celkové ceny plnění podle čl. IV odst. 1.

   Zálohovou fakturu je zhotovitel oprávněn vystavit nejdříve v den podpisu akceptačního protokolu o ukončení první či druhé etapy plnění.

5) Daňový doklad na cenu díla dle článku IV odst. 1, ve kterém budou vyúčtovány poskytnuté zálohy, je zhotovitel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu oběma smluvními stranami.

6) Daňový doklad na cenu roční provozní podpory dle článku I odst. 7 je zhotovitel oprávněn vystavit nejdříve následující pracovní den po převzetí díla; v dalších letech vždy nejdříve ve výroční den zahájení poskytování podpory.

7) Daňový doklad na cenu konzultační podpory dle článku I odst. 8 je zhotovitel oprávněn vystavit po poskytnutí konzultací. Přílohou daňového dokladu bude časový a věcný rozpis konzultací podepsaný pověřenou osobou objednatele.

8) V případě, že účinnost smlouvy skončí před uplynutím předplaceného ročního období, vrátí zhotovitel objednateli alikvotní část zaplacené ceny podpory.

9) K cenám plnění bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. V cenách jsou zahrnuty veškeré náklady zhotovitele spojené s plněním této smlouvy.

10) Daňový doklad či zálohová faktura vedle údajů podle § 435 občanského zákoníku obsahovat i evidenční číslo smlouvy ČNB. Daňový doklad bude nadto obsahovat náležitosti stanovené zákonem o DPH. V případě, že doklad bude postrádat některou ze stanovených náležitostí, nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit zhotoviteli. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu. Daňový doklad či zálohová faktura bude dále obsahovat evidenční číslo smlouvy ČNB, popis realizovaných činností a jako příloha bude připojena kopie příslušného podepsaného akceptačního protokolu.

11) Doklady zasílá zhotovitel elektronicky na adresu faktury@cnb.cz, přičemž musí být vložen jako příloha mailové zprávy ve formátu PDF. Mimo vlastní fakturu může být přílohou mailu jedna až tři přílohy k faktuře ve formátech PDF, DOC, DOCX, XLS, XLSX. Nebude-li možné doklad zaslat elektronicky, zašle zhotovitel doklad v analogové formě na adresu objednatele:

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

12) Splatnost dokladů činí 14 dnů ode dne jejich doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu zhotovitele.

13) V případě, že zhotovitel zajišťuje část podpory dle čl. I odst. 7 u zahraničního výrobce, je kterákoliv smluvní strana oprávněna navrhnout úpravu aktuální ceny za podporu, jestliže se změní průměrný měsíční kurz CZK k zahraniční měně, za kterou zhotovitel část podpory pořizuje, o více než 5 %. Porovnávat se bude průměrný měsíční kurz z poslední

cenové úpravy s průměrným měsíčním kurzem za měsíc předcházející měsíci, ve kterém bude vystaven daňový doklad na cenu roční podpory. Při první změně ceny se bude vycházet z měsíčního průměru devizového kurzu vyhlášeného ČNB za kalendářní měsíc, v němž uplyne lhůta pro podání nabídky, tj. 25,452 CZK / EUR. Upravena bude ta část ceny, které se změna uvedeného kurzu dotýká.

14) Smluvní strany se ve smyslu občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za zhotovitelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce zhotovitele za objednatelem, ať splatné či nesplatné.

15) Ke konci kalendářního roku, nejpozději však do 31. 12., je zhotovitel povinen písemně sdělit objednateli, jakou část z uhrazené roční ceny podpory tvoří cena nových verzí představujících technické zhodnocení SW, nebo že k žádnému technickému zhodnocení v daném roce nedošlo.

Článek V
Práva, povinnosti a součinnost smluvních stran

1) Zhotovitel se zavazuje, že bude po celou dobu trvání této smlouvy disponovat minimálně dvěma vzájemně zastupitelnými, výrobcem certifikovanými specialisty na dodávané produkty řešení - realizaci plnění dle této smlouvy. Zhotovitel se dále zavazuje, že plnění dle této smlouvy budou provádět pouze takto certifikovaní specialisté na dodané produkty a že jejich certifikáty budou po celou tuto dobu platné. Zhotovitel se zavazuje, že plnění dle této smlouvy bude poskytováno minimálně těmito specialisty:

   a) hlavní technik: Jan Bártl, mob.: 603 605 303, e-mail: jan.bartl@t-mobile.cz,

   b) zástupce hlavního technika: Ing. Attila Tóth, mob.: 603 607 002, e-mail: attila.toth@ t-mobile.cz.

   Doklady (certifikáty) prokazující odbornou způsobilost hlavního technika a jeho zástupce tvoří přílohu č. 9 této smlouvy.

2) Změna v osobách uvedených v odst. 1 tohoto článku, může být provedena pouze se souhlasem objednatele, a to po prokázání splnění kvalifikačních požadavků objednatele ve stejném rozsahu, jaký byl stanoven v zadávací dokumentaci veřejné zakázky na poskytování služeb uvedených v této smlouvě. Odsouhlasení změny osoby bude provedeno e-mailem alespoň jednou kontaktní osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě.

3) Zhotovitel je oprávněn provádět i část plnění dle této smlouvy prostřednictvím poddodavatele. Pokud zhotovitel v rámci veřejné zakázky na výběr zhotovitele dle této smlouvy prokazoval kvalifikaci prostřednictvím poddodavatele, musí se takový poddodavatel podílet na plnění předmětu této smlouvy, a to v takovém rozsahu, v jakém prokazoval za zhotovitele splnění kvalifikace. Zhotovitel je oprávněn vyměnit poddodavatele za jiného pouze se souhlasem objednatele. Objednatel udělí souhlas se změnou poddodavatele za předpokladu, že nový poddodavatel prokáže objednateli kvalifikaci minimálně ve stejném rozsahu, v jakém kvalifikaci prokázal původní poddodavatel. Splnění podmínek technické kvalifikace je objednatel oprávněn ověřit před udělením souhlasu. Zhotovitel a poddodavatel jsou v rozsahu činností prováděných poddodavatelem odpovědni společně a nerozdílně. Za plnění poskytovaná poddodavatelem je zhotovitel odpovědný jako by toto plnění poskytoval sám. Zhotovitel se zavazuje, že poskytne objednateli, pokud bude i část plnění poskytována poddodavatelem, seznam kontaktních údajů na osoby provádějící plnění za poddodavatele. Objednatel je oprávněn průběh plnění realizovaný poddodavatelem řešit

napřímo s jeho pracovníky a zhotovitel není oprávněn tuto komunikaci s poddodavatelem či jeho pracovníky jakkoliv omezovat nebo mařit.

4) Zhotovitel se zavazuje, že jeho zaměstnanci se budou pohybovat v místech plnění pouze ve vyhrazených prostorách za přítomnosti oprávněné osoby objednatele.

5) Zhotovitel je oprávněn požadovat po objednateli po dobu trvání této smlouvy poskytnutí nezbytných informací, podkladů a dokladů nutných k plnění předmětu této smlouvy.

6) Zhotovitel je povinen písemně upozornit objednatele na nedostatečnou součinnost pověřených pracovníků objednatele, pokud z tohoto důvodu vznikne riziko nedodržení termínů stanovených touto smlouvu nebo poskytnutí vadného plnění. Stejnou povinnost má zhotovitel i v případě, kdy nedostatečná součinnost pověřených pracovníků objednatele byla příčinou nedodržení stanovených termínů nebo poskytnutí vadného plnění a přitom nebylo možné objednatele upozornit předem.

7) Objednatel si vyhrazuje právo písemně upozornit zhotovitele na nedostatečnou součinnost pověřených pracovníků zhotovitele, pokud z tohoto důvodu hrozí, že dojde k ohrožení termínů a kvality plnění dle této smlouvy.

8) Objednatel se zavazuje vytvořit zhotoviteli potřebné podmínky k plnění smlouvy, zejména:

   a) poskytnout zhotoviteli k nahlédnutí orientační plán stávajícího zapojení na perimetru, propojení instalačních lokalit, případně plán používaných konvencí pro tvorbu jejich označování, používané konvence pro označování LAN, síťových hostnamů atd.;

   b) umožnit prohlídky obou míst plnění s ohledem na fyzické umístění dodávaných technických prostředků řešení proxy serveru;

   c) zajistit potřebné rekonfigurace všech technických a programových systémů dotčených přechodem na dodávané řešení proxy serveru (konfigurace klientských zařízení, konfigurace prvků LAN);

   d) přidělit IP adresy pro dodávané prostředky řešení proxy serveru, pro potřeby jeho managementu a dalších komponent řešení;

   e) zajistit přístup odborných pracovníků zhotovitele na příslušná pracoviště objednatele.

9) Zhotovitel se zavazuje dodržovat bezpečnostní požadavky objednatele uvedené v příloze č. 4.

10) Pověřenými zaměstnanci pro technická jednání, akceptaci a k předání a převzetí plnění (včetně konzultační podpory) jsou:

   a) za objednatele: Ing. Petr Puchmeltr, tel. 224 412 883,
   e-mail: petr.puchmeltr@cnb.cz,
   Jiří Matějka, tel.: 224 412 390,
   e-mail: jiri.matejka@cnb.cz,

   b) za zhotovitele: Honza Petřík, tel.: 603 423 669,
   e-mail: jan.petrik@t-mobile.cz,
   Martin Šimonek, tel.: 603 418 615,
   e-mail: martin.simonek@t-mobile.cz.

11) Pověřenými zaměstnanci pro jednání ohledně změn této smlouvy jsou:

a) za objednatele: Ing. Petr Puchmeltr, tel. 224 412 883,
e-mail: petr.puchmeltr@cnb.cz,
Ing. Robert Lederer, tel.: 224 412 669,
e-mail: robert.lederer@cnb.cz,

b) za zhotovitele: Honza Petřík, tel.: 603 423 669,
e-mail: jan.petrik@t-mobile.cz,
Ing. Lukáš Marhoul, tel.: 724 095 710
e-mail: lukas.marhoul@t-mobile.cz.

12) Smluvní strany se zavazují ohlásit změnu pověřených osob dle odst. 10 a 11 tohoto článku bez zbytečného odkladu. Ohlášení je možné provést písemně či elektronickou poštou a nepovažuje se za změnu smlouvy.

Článek VI
Přechod nebezpečí škody a vlastnické právo, licenční ujednání

1) Vlastnictví k technickým prostředkům a právo užívání programových prostředků řešení proxy serveru včetně všech potřebných licencí dle této smlouvy přechází na objednatele dnem podpisu závěrečného akceptačního protokolu.
2) Po dobu úschovy prostředků přechází nebezpečí škody na těchto prostředcích na objednatele.
3) Zhotovitel poskytuje objednateli nevýhradní, nepřevoditelnou, nedělitelnou, časově a územně neomezenou licenci umožňující užívat poskytnutý SW pouze pro potřebu objednatele dle této smlouvy.
4) Objednatel není povinen licenci využít.
5) Součástí licence je příslušná dokumentace v elektronické podobě.
6) Zhotovitel prohlašuje, že práva, která touto smlouvou poskytuje, mu náleží bez jakéhokoliv omezení, a odpovídá za škodu, která by objednateli vznikla, pokud by toto prohlášení bylo nepravdivé.
7) Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace programového vybavení řešení proxy serveru (tj. update/upgrade/patch/hotfix atd.).
8) Zhotovitel umožní objednateli užívání programových prostředků dle této smlouvy již v průběhu druhé a třetí etapy s tím, že licence podle tohoto článku objednatel nabývá dnem podpisu závěrečného akceptačního protokolu.
9) Licenční ujednání podle tohoto článku se vztahují i na případná plnění provedená zhotovitelem dle čl. I odst. 9, nebude-li v konkrétním případě dohodnuto jinak.

Článek VII
Smluvní pokuty, úrok z prodlení

1) V případě prodlení zhotovitele ve lhůtě pro provedení jednotlivé etapy nebo ve lhůtě pro předání a převzetí plnění stanovené ve článku II odst. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000,- Kč za každý den prodlení.

2) V případě, že se v průběhu 2 let od podpisu závěrečného akceptačního protokolu prokáže, že zhotovitelem nebyl splněn jakýkoliv z povinných požadavků objednatele uvedených v příloze č. 2 smlouvy a zhotovitel nezajistí splnění takového požadavku nejpozději do 2 měsíců od doručení výzvy objednatele, je objednatel oprávněn požadovat smluvní pokutu ve výši 100 000,- Kč za každý jednotlivý nesplněný požadavek. Tím není dotčeno právo objednatele odstoupit od smlouvy ani požadovat náhradu vzniklé škody.

3) V případě prodlení zhotovitele ve lhůtě pro odezvu dle přílohy č. 5 smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 500,- Kč za každou hodinu prodlení.

4) V případě prodlení zhotovitele ve lhůtě pro odstranění vady/vyřešení problému dle přílohy č. 5 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 2 000,- Kč za každou hodinu prodlení u priority Vysoká, 1 000,- Kč za každou hodinu prodlení u priority Střední a 500,- Kč za každou hodinu prodlení u priority Nízká.

5) V případě prodlení zhotovitele se splněním smluvní povinnosti ve stanovené lhůtě dle čl. XI odst. 2 smlouvy se poskytovatel zavazuje zaplatit objednateli smluvní pokutu ve výši 500,- Kč za každý den prodlení.

6) V případě prodlení objednatele nebo zhotovitele v úhradě daňového dokladu má zhotovitel právo požadovat úrok z prodlení podle příslušných ustanovení předpisů občanského práva.

7) V případě porušení povinnosti mlčenlivosti pracovníky zhotovitele dle čl. IX má objednatel právo požadovat smluvní pokutu ve výši 20 000,- Kč za každý jednotlivý zjištěný případ porušení této povinnosti.

8) Smluvní pokutou není dotčen nárok na náhradu škody. Případná odpovědnost zhotovitele za škodu způsobenou neplněním povinností vyplývajících z této smlouvy je omezena celkovou částkou ve výši 20 000 000,- Kč, kterou smluvní strany považují za předvídatelnou škodu.

Článek VIII
Trvání a výpověď smlouvy, odstoupení od smlouvy, zrušení smlouvy zaplacením odstupného

1) Smlouva se v části poskytování provozní a konzultační podpory uzavírá na dobu neurčitou.

2) Smlouvu lze v části týkající se poskytování podpory ukončit písemnou výpovědí bez uvedení důvodu, která musí být doručena druhé smluvní straně nejpozději 6 měsíců ze strany objednatele a 9 měsíců ze strany zhotovitele přede dnem uplynutí předplacené doby podpory. Smlouva v tomto případě zaniká skončením předplacené doby podpory.

3) Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek zhotovitele vypovědět tuto smlouvu, a to ve 14 denní výpovědní lhůtě, která počíná běžet dnem následujícím po doručení písemné výpovědi zhotoviteli. V případě, že účinnost smlouvy skončí před koncem účtovacího období, vrátí zhotovitel objednateli alikvotní část předplacené ceny podpory od zhotovitele.

4) Smluvní strany si v souladu s ustanovením 1992 občanského zákoníku sjednávají, že objednatel je oprávněn zrušit smlouvu zaplacením odstupného ve výši 50 000,- Kč, a to kdykoliv před ukončením první etapy plnění podle článku I odst. 3 smlouvy. Zrušení smlouvy bude účinné zaplacením sjednaného odstupného na bankovní účet zhotovitele vedeného u Komerční banky a.s., č.ú.: 19-2271190247/0100. Oznámení o využití práva zrušit smlouvu zaplacením odstupného oznámí objednatel písemně.

5) Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to prostřednictvím písemného odstoupení. Takové odstoupení bude platné a nabude účinnosti dnem jeho doručení druhé smluvní straně.

6) Za podstatný způsob porušení smlouvy strany považují zejména tyto případy:

   a) objednatel bude více než 30 dnů v prodlení s úhradou sjednané zálohy nebo ceny,

   b) dodané řešení proxy serveru, nebo některá jeho komponenta, nebude splňovat veškeré požadavky dle této smlouvy,

   c) předmět plnění není způsobilý plnit svou funkci v rámci systémového prostředí objednatele na perimetru včetně geoclusteru (High Availability) - např. není plně kompatibilní s prostředím bezpečnostních bran na tomto perimetru,

   d) zhotovitel nedodá dokumentaci skutečného provedení implementace řešení proxy serveru v požadovaném rozsahu,

   e) zhotovitel bude v prodlení v kterékoliv lhůtě uvedené v článku II odst. 1 této smlouvy delším než 30 dnů,

   f) v průběhu 365 po sobě jdoucích dnů jsou objednatelem uplatněny k nápravě minimálně 3 závady s prioritou „Vysoká" nebo 5 závad s prioritou „Střední"

   g) zhotovitel nebude plnit předmět plnění výrobcem certifikovanými specialisty dle čl. V i přes výzvu k nápravě objednatele.

Článek IX
Mlčenlivost

Zhotovitel se zavazuje zajistit, že jeho pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele v průběhu plnění seznámí, a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.

Článek X
Uveřejnění smlouvy, výše skutečně uhrazené ceny a seznamu poddodavatelů

1) Zhotovitel 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) Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

5) Zhotovitel se v souladu s ust. § 105 odst. 3 ZZVZ zavazuje poskytnout objednateli identifikační údaje všech poddodavatelů, kteří nebyli identifikováni dle věty první uvedené v § 105 odst. 3 ZZVZ a kteří se následně zapojí do plnění předmětu dle této smlouvy, a to nejpozději před zahájením plnění předmětu dle této smlouvy poddodavatelem.

Článek XI
Ostatní ujednání

1) Zhotovitel je povinen mít po dobu účinnosti této smlouvy uzavřeno pojištění pro případ vzniku odpovědnosti za škodu způsobenou v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 5 000 000 Kč (slovy: pět milionů korun českých) a jeho spoluúčast nepřevyšuje 5 %.
2) Zhotovitel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy, a do 5 pracovních dnů od výzvy objednatele je zhotovitel povinen toto objednateli prokázat.
3) Zhotovitel se zavazuje, že nebude využívat plnění pro objednatele (resp. označení České národní banky) jako veřejně dostupnou referenci bez předchozího písemného souhlasu objednatele.

Článek XII
Závěrečná ustanovení

1) Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2) Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě stanoveno jinak.
3) Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě nebo jejímu plnění bude probíhat v českém jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
4) Smluvní strany se dohodly, že tato smlouva a právní vztahy s ní související se řídí zákonem č. 89/2012 Sb., občanský zákoník, a ostatními souvisejícími platnými právními předpisy.
5) Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
6) Smlouva je vyhotovena ve třech vyhotoveních s platností originálu, z nichž objednatel obdrží dvě a zhotovitel jedno vyhotovení.

Přílohy:
- č. 1 – Specifikace technických a programových prostředků řešení proxy serveru dodávaných zhotovitelem
- č. 2 – Požadavky objednatele na řešení proxy serveru
- č. 3 – Akceptace – kritéria, proces
- č. 4 – Bezpečnostní požadavky objednatele
- č. 5 – Provozní podpora, SLA podpory od zhotovitele a od výrobce
- č. 6 – Standardní systémové prostředí objednatele
- č. 7 – Technický návrh řešení proxy serveru

č. 8 – Podrobná specifikace cen
č. 9 – Doklady prokazující odbornou způsobilost hlavního technika a jeho zástupce
č. 10 – Šablona realizační studie
č. 11 – Realizační studie (volně připojená příloha)
č. 12 – Pověření k zastupování

V Praze dne: 28.2. 2018

Za objednatele:

[redacted]

Ing. Vladimír Mojžíšek
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní

[redacted]

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

V Praze dne: 28.2. 2018

Za zhotovitele:

[redacted]

Ing. Petr Malimánek
Corporate & Public Sales Director

[redacted]

Ing. Petr Žáček
Senior manažer prodeje segmentu bankovnictví a financí

Příloha č. 1

Specifikace technických a programových prostředků řešení proxy serveru dodávaných zhotovitelem

FG – 1000D-BDL-950-60	**Fortinet, FortiGate, FortiGate 1000D, HW+24x7 Protection 5YR**
FAZ-1000E	**Fortinet, FortiAnalyzer, FortiAnalyzer 1000E, HW only**
FC-10-L1005-247-02-60	**Fortinet, FortiAnalyzer, FortiAnalyzer 1000E, 24x7 FortiCare 5YR**
FSA – 1000D-BDL-970-60	**Fortinet, FortiSandbox, FortiSandbox-1000D, HW+24x7 FortiCare plus AV, IPS, Web Filtering, File Query and SandBox 5YR**
FSA – 1000D-UPG	**Fortinet, FortiSandbox, FortiSandbox-1000D, Licence upgrade**
FC1-15-EMS01-158-02-60	**Fortinet, FortiClient, FortiClient Enterprise Management Software, Server License for 100 clients 5YR**
FMG-VM-Base	**FortiManager VM**

Příloha č. 2

Požadavky objednatele na řešení proxy serveru

Níže v kapitolách 1.x jsou uvedeny základní věcné funkční požadavky na poptávané řešení proxy serveru. Z pohledu objednatele se jedná o nejdůležitější požadavky, které mají umožnit splnit cíle uvedené v preambuli této smlouvy.

U každého požadavku je uveden jak jeho název definice dle objednatele, tak i popis tohoto požadavku. Dále jsou pak případně uvedeny konkrétní komponenty či produkty, které by dle objednatele umožňovaly splnění daných požadavků[1)].

U všech požadavků se jedná o závazné požadavky.

1. Věcné požadavky

1.1. Vysoká dostupnost řešení proxy serveru

ID	Název	Popis požadavku
1.	Vysoká dostupnost (HA – High Availability)	Řešení proxy serveru musí pracovat v režimu vysoce dostupného geoclusteru typu primární-sekundární s automatizovaným přepínáním mezi jednotlivými instalačními lokalitami. Jeden člen clusteru je nastaven jako aktivní/primární a druhý/sekundární je průběžně synchronizován s tím, že je připraven automatizovaně bezvýpadkově převzít funkci prvního (a naopak při automatizovaném přepnutí geoclusteru zpět).
2.	Duální napájení	Veškerá (jednotlivá) zařízení dodaná v rámci řešení budou obsahovat duální napájecí zdroje zapojitelné do samostatných napájecích okruhů.

1.1.1. Definice „Vysoké dostupnosti":

1.1.1.1. Zajištění kontinuity provozu řešení

Řešení proxy serveru bude navrženo pro bezodstávkový provoz a to jak pro plánované rutinní činnosti, tak i pro neplánované události.

Plánovanými rutinními činnostmi se rozumí možnost SW záplatování, výměna vadných HW komponent nebo jejich doplnění. Neplánovanými událostmi se rozumí poruchy jedné komponenty v rámci redundantní skupiny (např. disk v rámci diskového pole, síťové rozhraní v rámci skupiny, serverová nebo dílčí jednotka v rámci dvojice apod.).

Z toho vyplývá, že řešení proxy serveru musí být navrženo jako soběstačné fault-tolerantní řešení, tedy bez tzv. *single-point-of-failure*. Veškeré důležité komponenty pro běh řešení musí být zdvojeny. Řešení proxy serveru musí obsahovat vhodný SW a konfiguraci pro zajištěna kontinuity provozu.

1.1.1.2. Zajištění provozu v případě výpadku jedné lokality

Řešení proxy serveru musí být dále navrženo tak, aby byl v případě výpadku celého řešení v jedné instalační lokalitě zajištěn automatizovaný převod provozu do druhé lokality. Při přechodu do provozu do druhé lokality nedojde k přerušení session/komunikace uživatelů do Internetu.

Zhotovitel předpokládá, že při normálním provozu budou jedna instalační lokalita nastavena jako aktivní, druhá jako pasivní/záložní. Dle potřeby objednatele lze tyto role (aktivní/pasivní) jednotlivých lokalit přehodit. Řešení musí umožnit toto přehození rolí do 15 minut.

Řešení v každé instalační lokalitě musí být kapacitně navrženo tak, aby zvládlo provoz a zátěž vyvolanou všemi uživateli (požadavek ID 24) a zařízeními (požadavek ID 22) objednatele.

Pro přenos dat řešení mezi jednotlivými instalačními lokalitami bude využita počítačová síť se dvěma nezávislými šifrovanými optickými trasami, každá s přenosovou kapacitou 10 Gbps. Tato komunikační kapacita je sdílena s ostatním datovým provozem objednatele mezi instalačními lokalitami.

[1)] Výčet není úplný a vychází z aktuálních znalostí pracovníků objednatele či informací získaných z průběžného monitoringu rozvoje technologií v dané oblasti.

1.1.2. Možná realizace:

Požadavky objednatele naplňují na HW úrovni např. zdvojení HW komponent a Hot-Plug technologie, osazení N+1 nezávislých napájecích zdrojů, lokální zabezpečení dat na discích technologií RAIDx atd.

1.2. Soulad se standardním systémovým prostředím objednatele

ID	Název	Popis požadavku
3.	Soulad se standardním systémovým prostředím	Řešení proxy serveru bude implementováno do již existujícího systémového prostředí objednatele. Řešení musí být tedy kompatibilní s jeho komponentami.

1.2.1. Definice kompatibility se systémovým prostředím:

V příloze č. 6 je uvedena definice základních komponent standardního systémového prostředí objednatele a nové řešení musí být s tímto prostředím kompatibilní. Objednatel nechce v souvislosti s tímto projektem zavádět další jiné platformy již existujících produktů. Maximálně je možné instalovat či aktivovat vyšší verze již existujících produktů (např. verze u Windows operačních systémů).

Při nasazení komponent objednatel požaduje, aby komponenty řešení proxy serveru byly pro tyto produkty systémového prostředí certifikovány výrobcem řešení proxy serveru.

Stejně tak nové řešení proxy serveru musí respektovat existující provozní zvyklosti s provozováním komponent systémového prostředí objednatele a jeho provozní podpory – systém přístupových práv, automatizace provozních činností, automatizace instalace software na PC v MS doméně apod.

Pokud je pro provoz nového řešení proxy serveru navrhováno doplnění tohoto systémového prostředí o další komponentu či aplikaci, je zhotovitel kromě její implementace povinen zajistit i její plnou provozní podporu (monitoring, zálohování, upgrady/updaty, řešení vad v dohodnutých časech atd.)

1.2.2. Možná realizace:

Pro nové řešení proxy serveru je možné využít produkty osvědčených výrobců – viz NSS LAB SVM pro rok 2017.

Při instalacích SW na klientská zařízení bude použito automatizovaných bezobslužných instalací (MS balíčky v rámci instalace prostřednictvím GPO objektů Active Directory objednatele).

1.3. Obecné požadavky

ID	Název	Popis požadavku
4.	Hodnocení výrobce nabízeného řešení proxy serveru NSS LABS SVM 2017	Nadprůměrné umístění výrobce nabízeného řešení proxy serveru pro přístup do Internetu v testu NSS LABS NGFW Security Value Map (SVM) za rok 2017 v obou sledovaných parametrech – blíže viz www.nsslabs.com (cena za chráněný megabit provozu, efektivita/účinnost bezpečnostních funkcí).
5.	Instalace v bankovním sektoru	Zhotovitelem nabízené řešení má v České republice prokazatelně minimálně 2 další instalace této technologie u úvěrových institucí (tj. banky, stavební spořitelny a družstevní záložny), investičních společností nebo investičních fondů ve stejné nebo podobné konfiguraci – Proxy pro přístup do Internetu v geoclusteru s funkcionalitami uvedenými v kapitole 1.1 a 2. této přílohy – požadavky ID 1, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 25, 26, 27 (in-house, propustnost min 1 Gbps), 28, 31, 32, 33, 34, 39, 41.
6.	Omezení součinnosti objednatele	Vyžadovaná součinnost objednatele při implementaci a následném provozu řešení proxy serveru nesmí překročit 80 člověkodní (dále jen "čld") (celkem za projekt) při implementaci a 80 čld (celkem za rok) pro provozní podporu.

2. Funkční a technické požadavky

2.1. Bezpečnostní funkce řešení

V rámci implementovaného řešení proxy serveru budou zhotovitelem implementovány a objednatelem následovně využívány níže uvedené bezpečnostní funkce.

ID	Název	Popis požadavku
7.	Proxy	Řešení musí plnit funkci proxy serveru pro přístup z vnitřní sítě do Internetu. Včetně NAT.
8.	Firewall	Řešení musí plnit funkci bezpečnostní brány s možností bezpečně řídit datovou komunikaci mezi vnitřním (privátním) prostředím datové sítě a Internetem. Dále musí umožňovat vytvořit minimálně 3 oddělené demilitarizované zóny a bezpečně řídit datovou komunikaci do/z nich. Všechna prostředí (Internet, vnitřní síť, jednotlivé demilitarizované zóny) musí být na samostatných fyzických portech zařízení – proxy.
9.	URL filtering	Řešení musí podporovat funkci kategorizace webových stránek (URL filtering) a detekci aplikací (na L7).
10.	Kategorizace webových stránek	Kategorizace webových stránek vychází z výrobcem průběžně aktuálně udržované databáze webových stránek, podporující české internetové prostředí. K dispozici jsou desítky kategorií, pro které může administrátor řešení volit různé akce: Povolení přístupu (na webovou stránku z dané kategorie), Povolení podmíněného přístupu (přístup s varováním a vědomím souhlasem uživatele), Zákaz přístupu. Dále lze definovat maximální časovou povolenou lhůtu (pro přístup k vybraným kategoriím webových stránek) na daného uživatele. Jednotlivá URL webových stránek je též možné nezávisle ověřit na stránkách výrobce technologie řešení.
11.	Výjimky URL	Řešení musí umožňovat výjimky z kategorizace URL (white/black listing). Dle kategorie, URL, IP adresy.
12.	HTTPS inspekce	Řešení musí poskytovat funkci dešifrování HTTPS provozu a následnou automatizovanou inspekci na přítomnost a ochranu před malware. Inspekci lze provádět selektivně (např. pro kategorie URL, dle výčtového seznamu apod.).
13.	Web proxy	Explicitní i transparentní proxy musí umožňovat manipulaci s http hlavičkami (odstranění vybraných hlaviček např. kvůli HPKP a HSTS), i při ssl inspekci v protokolu HTTPS).
14.	AntiMalware ochrana	Řešení musí poskytovat funkci detekce a restriktivní ochrany před škodlivým kódem – malware (Antivir).
15.	IDS/IPS	Řešení bude poskytovat detekční i restriktivní ochranu proti zneužití zranitelností typu IDS i IPS (restriktivní).
16.	Zero Day (sandboxing)	Řešení musí poskytovat restriktivní ochranu proti Zero Day útokům a neznámým hrozbám (včetně emulace v sandbox prostředí – v prostředí objednatele) v preventivním - restriktivním módu (včetně prvního výskytu neznámého souboru). Sandbox platforma musí být obousměrně propojená s web proxy, musí obsahovat mininimálně 8 virtuálních strojů pro emulaci, musí obsahovat API rozhraní a interface pro napojení endpoint SW.
17.	Bot detekce (Antibot)	Řešení musí poskytovat funkční detekce a blokace komunikace na C&C centra.
18.	Definice cílů v bezpečnostní politice	V bezpečnostní politice řešení proxy serveru je možné cíle komunikace definovat jako hostname, IP adresu, nebo URL.

2.2. Administrace řešení

ID	Název	Popis požadavku
19.	Centralizovaná administrace	Celé řešení proxy serveru musí být možné centrálně řídit (i u jednotlivých funkcionalit). Bezpečnostní pravidla pro provoz (funkce explicitní proxy) a ochranné profily (antivirus, L7 analýza aplikací) musí být konfigurovatelné z jednoho místa v GUI Autentizace administrátorů ke konfiguračnímu rozhraní proxy musí být zabezpečená a umožněná prostřednictvím certifikátů. K tomuto rozhraní musí být také možný přístup pouze v režimu read-only.
20.	Centrální správa	Řešení musí plnit roli centralizované správy bezpečnostní politiky, funkci analýzy logů a generování reportů na jedné platformě (pro celé dodané řešení).
21.	Zálohování	Řešení musí umožňovat zálohování (automatizované i manuální) konfigurace všech bezpečnostních komponent.

2.3. Kapacitní nastavení řešení

ID	Název	Popis požadavku
22.	Propustnost	Propustnost konektivity řešení do Internetu (včetně všech požadovaných a aktivovaných bezpečnostních funkcionalit) je aktuálně limitována připojením 1 Gbps (v každé lokalitě) reálného provozu (v prostředí objednatele), na kterou musí být řešení minimálně dimenzováno. Dále musí být propustnost řešení (včetně všech požadovaných a aktivovaných bezpečnostních funkcionalit) dimenzována na obsluhu oddělených demilitarizovaných zón (do každé připojení minimálně 1 Gbps). Datová propustnost řešení proxy serveru musí být (v každé lokalitě) u uvedených funkcionalit (s ohledem na předpokládaný růst datových toků do Internetu) v reálném provozu a s maximálním průměrným vytížením CPU 70%: • Firewall 4 Gbps. • SSL inspekce 4 Gbps. • Ochrana proti hrozbám (IPS, L7 kontrola aplikací, ochrana před škodlivým kódem) 4 Gbps. • Zařízení musí být vybaveno alespoň 16 GB operační paměti RAM. • Zařízení musí odbavit minimálně 10 milionů současných spojení.
23.	Síťová rozhraní	Síťová rozhraní dodávaných zařízení (např. proxy, log servery) v rámci předmětu plnění budou v dostatečném počtu, o minimální kapacitě 1GbE, konektor typu RJ-45, případně 10GbE a SFP+. Každý proxy server musí mít minimálně samostatná (oddělená) fyzická rozhraní do Internetu , do vnitřní sítě a jednotlivých demilitarizovaných zón ČNB.
24.	Uživatelé, administrátoři, servery	Řešení musí umožňovat řízený přístup do Internetu minimálně pro 1500 současně pracujících uživatelů. Současně s tím musí umožňovat přístup do Internetu dalším minimálně 100 současně pracujícím zařízením (serverům). Vyžaduje-li řešení licence pro jednotlivé Administrátory (RW přístup) či Auditory (RO přístup), potom musí být dodány neomezené licence pro tyto přístupy.

2.4. Provozní požadavky na řešení

ID	Název	Popis požadavku
25.	Podporované protokoly	Řešení musí poskytovat plnou podporu komunikačních protokolů HTTP a HTTPS. Musí umožňovat i řízený přesun komunikace těmito protokoly na jiný TCP port. Podpora IPv4 (výhledově i IPv6).
26.	Podporované síťové služby	Řešení musí být napojitelné na: časové služby NTP (synchronizace času), jmenné služby DNS, adresářové služby.
27.	Kontrola prováděna In house	Kontrola (inspekce) dat bude prováděna lokálně v prostředí ČNB (data nebudou odesílána ke kontrole např. do cloudu v Internetu).

28.	QoS	Řešení musí umožňovat definování maximální šířky pásma pro určitý typ komunikace: browsing / business aplikace/URL kategorie a pro specifické uživatelské skupiny v rámci definovaných pravidel bezpečnostní politiky.
29.	Garance provozu aplikací	Uživatelský browsing nesmí nijak negativně (zejména z hlediska bezpečnosti a dostupnosti) ovlivňovat komunikaci business aplikací do/z Internetu – týká se především použití sdílených technických prostředků.
30.	Garance řešení	Řešení (HW, SW, služby) budou ze strany zhotovitele/výrobce podporovány minimálně po dobu 5 let od podpisu smlouvy. Po tuto dobu budou na řešení poskytovány aktuální verze, bezpečnostní záplaty a aktuální signatury (SW, služby) a náhradní díly na HW.
31.	Zařízení bez defaultní brány	V síti objednatele existují zařízení (servery), kteří nemají nastavenu defaultní bránu do Internetu (protože běžně nepřistupují do Internetu). Řešení jim musí umožňovat (na základě identifikace jejich IP adresy) přístup na konkrétní zdroje pro aktualizace v Internetu (např. Redhat, Akamai).

2.5. Uživatelé/zařízení

ID	Název	Popis požadavku
32.	Identifikace uživatelů (PC)	Řešení musí umožňovat řídit politiky přístupu do Internetu a logovat tyto přístupy na základě identit uživatelů z MS AD. (Autentizace uživatelů při browsingu vůči MS AD musí probíhat prostřednictvím standardního uživatelského účtu, případně servisního účtu služby - bez privilegovaných oprávnění.) Požadované metody autentizace jsou: Kerberos a napojení na doménový řadič MS AD. Autentizace musí být možná na uživatelské jméno a/nebo IP adresu či zařízení.
33.	Identifikace Citrix klientů (vPC)	Řešení musí umožňovat řídit politiky přístupu do Internetu a logovat tyto přístupy na základě identit uživatelů Citrix klientů z MS AD. (Autentizace uživatelů při browsingu vůči MS AD musí probíhat prostřednictvím standardního uživatelského účtu, případně servisního účtu služby - bez privilegovaných oprávnění.) Požadované metody autentizace jsou: Kerberos a napojení na doménový řadič MS AD. Autentizace musí být možná na uživatelské jméno a/nebo IP adresu či zařízení.
34.	Výjimky identifikace	Řešení musí umožňovat vyjmutí konkrétní IP komunikujících zařízení z povinné autentizace uživatelů – komunikace bude (ve zdůvodněných případech) umožněna na základě identifikace zařízení (dle jeho IP adresy), nikoliv na základě identity uživatele.
35.	Uživatelská transparentnost	Z hlediska uživatelů musí probíhat jejich identifikace i bezpečnostní kontroly transparentně. Autentizace uživatelů musí zohledňovat každé spojení zvlášť (tzv. session base), a také akceptovat systém práce některých uživatelů na terminálových serverech (skupina uživatelů sdílí stejnou IP adresu).

2.6. Logy

ID	Název	Popis požadavku
36.	Logy	V řešení musí být v každý okamžik dostupné záznamy o všech přístupech prostřednictvím této proxy brány do Internetu 13 měsíců průběžně zpětně, kapacita diskového pole logovací platformy je požadována minimálně 20 TB (v RAID 5). Řešení logovací platformy musí umět zpracovat minimálně 15tis. událostí za sekundu a 500 GB logů za den.
37.	Export logů	Export logů musí být možný do textového formátu (ASCII/UTF8).
38.	Syslog	Logování musí být možné do externího Syslogu (napojení na SIEM - HP Arcsight).
39.	Obousměrná kompatibilita	Logovací a reportovací platforma musí být z důvodu obousměrné kompatibility přenosu dat od stejného výrobce, který ji bude garantovat.

2.7. Reporting

ID	Název	Popis požadavku
40.	Reporting	Řešení musí umožňovat tvorbu vlastních reportů. Nebo export záznamů do prostředí Oracle, kde jsou následně zpracovány ve stávajícím reportovacím řešení. Periodicita zpracování reportů musí být minimálně jednou denně. Záznamy / reporty musí obsahovat všechny následující údaje (u každého záznamu): kdo (jméno uživatele – jedná-li se o uživatele, jméno zařízení, IP adresu), kdy (čas a datum), kam (URL, IP adresu) přistoupil a jaký přenesl objem dat. Tyto údaje musí být možné zobrazovat (filtrovat) souhrnně dle: zařízení, jednotlivého uživatele, organizačních útvarů objednatele, volitelného časového období (plus jsou předdefinovány denní, týdenní, měsíční), dle jednotlivých kategorií cílů v Internetu a dle jednotlivých URL. A musí být možné kombinace uvedených filtrů.
41.	Reporting per uživatel	Řešení musí umožňovat pro jednotlivé uživatele vytvářet reporty o jejich provozu do Internetu. Musí být možná volitelná periodicita (denní / týdenní / měsíční / vlastní).
42.	Reporting podle role	Nadřízení uživatelů mají náhled do reportů o provozu do Internetu svých podřízených (jednotlivě i souhrnně). Role je určena příznakem v MS AD.
43.	Práce s incidenty	Logovací a reportovací nástroj musí být vybaven funkcí správy vzniklých incidentů (vznik incidentu, zachycení události systémem, automatizované založení incidentu na základě předpřipravených nebo vlastních filtrů, zobrazení předmětných vzorků síťového provozu a následným řešení administrátorem). Tyto incidenty bude následně možné exportovat do systému SIEM.

Příloha č. 3

Akceptace – kritéria, proces

1. Akceptace první etapy projektu – realizační studie

Akceptační řízení započne nejpozději 3 týdny před termínem dle článku II odst. 1 pro první etapu projektu. Akceptace je zahájena tak, že zhotovitel předloží objednateli realizační studii v elektronické formě ve formátech Office 2010 a vyšší (Word, Excel).

Objednatel si vyhrazuje nejméně 5 pracovních dní od obdržení studie k akceptaci na její prostudování a zaslání případných připomínek zhotoviteli. Zhotovitel bez zbytečného odkladu připomínky vypořádá a zašle objednateli další verzi studie k akceptaci. Ten se k ní opět bez zbytečného odkladu vyjádří.

Závažnou chybou bránící akceptaci se v tomto případě rozumí:

1. chybějící část textové dokumentace nebo nevyplněná či nevypracovaná část realizační studie (šablona viz příloha č. 10),
2. textová část studie neodpovídá skutečnosti popisované entity (např. procesu, systému, chybové zprávě apod.) nebo popisované řešení proxy serveru ve studii není v souladu se všemi požadavky objednatele uvedenými v této smlouvě,
3. navrhované řešení proxy serveru nelze jednoduše implementovat do systémového prostředí objednatele a vyžaduje neúměrné zásahy či změny tohoto prostředí či vyžaduje výrazné změny v provozních standardech a zvyklostech objednatele,
4. požadavky na součinnost a kapacity objednatele výrazně převyšují limity uvedené v požadavcích v příloze č. 2.

Ostatní chybou, kdy objednatel může podmíněně akceptovat realizační studii, se rozumí např. nejednoznačnost textové části, případně gramatické chyby.

Realizační studii lze akceptovat pouze v případě, že neobsahuje chyby bránící akceptaci (viz výše).

2. Akceptace druhé etapy projektu

Akceptace druhé etapy je rozdělena na 2 samostatné akceptační celky.

a. Funkční test s omezeným počtem uživatelů a zařízení.

Tento akceptační celek je zaměřen na prověření provozních i bezpečnostních funkcí nového řešení proxy serveru v provozu s omezeným počtem uživatelů (max. 100 jmenovitých/současných uživatelů + max. 2 servery komunikující do Internetu).

Testy z hlediska uživatelů budou prováděny na samostatných klientských stanicích (Win7 či Win10 - PC) a současně na virtuálních klientských stanicích (publikovaný desktop prostřednictvím Citrix XenApp 6.5 hostovaný na Win2008R2 Serveru - vPC)

- Předpoklady testu:
    - Nové řešení proxy serveru je plně nainstalováno a všechny komponenty řešení proxy serveru jsou navzájem komunikačně a konfiguračně správně propojeny a jsou současně všechny aktivní v restriktivním módu a jsou nastaveny dle bezpečnostních požadavků objednatele.
    - Jsou aktivovány potřebné funkce, licence a služby potřebné pro provoz nového řešení proxy serveru.

- V případě potřeby je na klientské straně u testujících uživatelů nainstalováno potřebné programové vybavení formou automatické vzdálené instalace prostřednictvím služby Windows Installer a GPO objektů v AD (PC), manuální instalace (vPC).
- Jsou aktivovány služby (Autentizace uživatelů, HTTPS inspekce, Antivir, IPS, URL Filtering atd.) na proxy serveru.
- Jsou aktivní služby a servery pro zajištění centrální administrace řešení proxy serveru, pro zajištění sběru logů a jejich následné vyhodnocování, jsou připraveny a nakonfigurovány reportovací nástroje.
- Všechny komponenty řešení proxy serveru nevykazují ve svých provozních logách chyby či varování.

b. Popis testu – provoz po dobu 1 týdne

Test spočívá v reálném provozu řešení a testovacích uživatelů, přičemž jsou sledovány případné chyby tohoto řešení a jsou cíleně uživateli či administrátory realizovány minimálně níže uvedené testy.

Při testech se zejména kontroluje:

- bezpečnostní funkce (kategorizace (freemail, warez, hry, anonymizační proxy),
- odmítnutí nebezpečných stránek,
- detekce hrozeb (antivir),
- autentizace uživatelů a porušení bezpečnosti,
- ověření reportů a jejich hierarchie (1 zaměstnanec, 1 vedoucí zaměstnanec, 1 organizační útvar, celá banka; v časovém členění za den, týden a volitelné období).

Testy - typické scénáře:

- Kontrola provozních funkcí
  - Přepnutí mezi lokalitami v geoclusteru
    - Za provozu je jsou vypnuta zařízení (Proxy, Log server,...) v primárním středisku CVS (vypínačem, simuluje se výpadek napájení), musí proběhnout plně automatické převedení provozu a plné funkcionality do druhé lokality ZVS. Při následném zapnutí zařízení v primární lokalitě CVS musí proběhnout plně automatizovaně převedení provozu a plné funkcionality zpět.
- Kontrola bezpečnostních funkcí
  - Kategorizace webových stránek s funkcí URL filteringu
    - Bude proveden přístup na běžné webové stránky v českém prostředí Internetu (idnes, ihned, seznam, mapy, youtube, skype...). Stránky musí být v logu správně zakategorizovány. Též bude proveden pokus o přístup (HTTP i HTTPS protokolem) na stránky s podmíněným přístupem a stránky zakázané a musí korektně proběhnout definovaná akce.
  - Detekce narušení sítě

- Pomocí libovolného nástroje (např. Metasploit) je generován pokus o síťový útok, zařízení je schopno tento útok detekovat a eliminovat.

- Ochrana před škodlivým kódem
  - Zařízení je schopno detekovat testovací vzorek škodlivého kódu staženého ze stránek eicar.org v šifrované i nešifrované podobě (protokoly HTTP a HTTPS), i v archivu zip.
- Rozpoznání a analýza aplikací na základě jejich L7 otisku
  - Testovací uživatel započne pomocí webového prohlížeče (MS IE 11 či Edge, Firefox, Chrom) komunikaci na vybrané služby v Internetu (FB, Dropbox, Google Drive, LinkedIn), zařízení je schopno správně rozpoznat použité aplikace a zalogovat je.
- Inspekce předmětných protokolů včetně šifrovaných variant (HTTPS)
  - Testovací uživatel provede přihlášení do FreeMailu (Seznam, Gmail) a provede stažení unikátní přílohy. Mail i přílohu musí být možné otevřít a přečíst (přílohu lokálně uložit). Zařízení musí provést antivirovou kontrolu komunikace, správně zakategorizovat a zalogovat tuto akci.
  - Zařízení je schopno odebrat hlavičky webové komunikaci (např. hlavička Public-Key-Pins, Strict-Transport-Security) – ověřit regulérním přístupem např. na stránky FB.

- Kontrola autentizace uživatelů
  - Přihlášený uživatel (na PC i vPC) je transparentně ověřován při přístupu do Internetu – test bude proveden přihlášením stejného uživatele na PC i vPC – správná identita uživatele (jméno, příjmení a uživatelské jméno) a uskutečněné jeho přístupy do Internetu včetně množství přenesených dat musejí být jednoznačně viditelné v logách (reportech).
- Kontrola vyhodnocovacích nástrojů
  - Kontrola logování a reportingu
    - Jsou provedeny testovací přístupy uživatelů (alespoň pěti) a současně je možné sledovat v administrátorském rozhraní tyto přístupy a jejich zalogování.
  - Kontrola nástroje pro práci s incidenty
    - Je simulován vznik incidentu (např. stažení vzorku škodlivého kódu ze stránky eicar.org), nástroj pro práci s incidenty detekuje incident, administrátor je schopen detaily tohoto incidentu (vzorky síťové komunikace), incident lze doplnit komentářem, lze ho označit jako vyřešený.

c. Funkční test s plným počtem uživatelů (1500) a servery (max. 5).

V případě korektních výsledků předchozích testů pokračuje v nakonfigurovaném prostředí řešení proxy serveru testování s plným počtem současně pracujících uživatelů a max. 5 serverů komunikujících do Internetu. Cílem je jednoznačně prokázat dostatečnou komunikační propustnost řešení proxy serveru a výkonnostní kapacitu pro zvládnutí požadovaných bezpečnostních funkcí, logů a jejich vyhodnocování v prostředí objednatele.

Při testech se zejména kontroluje:

- Dtto jako u předchozího testu.
- Zobrazení typických stránek do max. 5 sekund od vyvolání požadavků na jejich zobrazení uživatelem (neplatí pro případ SandBox kontroly).
- Nedochází k chybám zobrazování stránek (obsah zobrazen jen částečně) nebo nedojde k neidentifikovatelným nebo chybovým stavům – např. nezobrazení stránky („stránku nelze zobrazit apod.") – z důvodu chyby funkčnosti proxy serveru.

Testy - typické scénáře:

- Dtto jako u předchozího testu jen ve větším počtu uživatelů.

Akceptace této etapy

Tato etapa bude úspěšně akceptována v případě, že řešení proxy serveru bude splňovat provozní i bezpečnostní požadavky při plném zatížení v prostředí objednatele. Dále bude dodána požadovaná dokumentace skutečného provedení v prostředí objednatele a obsluha řešení proxy serveru byla zaškolena pro jeho provoz dle požadavků objednatele z této smlouvy.

Etapa nemůže být akceptována, pokud se vyskytnou zejména následující závažné vady či nedostatky:

- Řešení proxy serveru bylo implementováno odlišně od akceptované realizační studie a tato odchylka nebyla schválena oběma smluvními stranami.
- Budou detekovány závažné chyby např.:
    - plná či částečná nefunkčnost požadovaných provozních i bezpečnostních funkcí,
    - komponenty proxy serveru vykazují chyby do svých provozních logů, chyby typu warning mohou být akceptovány podmíněně,
    - nedodána požadovaná dokumentace dle této smlouvy.

3. Akceptace třetí etapy projektu - Ověřovací provoz

Cílem této etapy projektu a akceptace je detekovat případné problémy spojené s provozem plně nakonfigurovaného řešení proxy serveru pod plným provozním zatížení v dlouhodobějším časovém horizontu, které nebyly odhaleny v průběhu akceptačních testů v předchozí etapy. Dále budou prověřeny postupy zhotovitele v oblasti provozní podpory řešení proxy serveru.

Délka trvání této etapy je minimálně 2 měsíce.

Testy - typické scénáře:

Kromě sledování provozních a bezpečnostních funkcí bude v souladu se smlouvou realizován a prověřen proces:

- Opatchování všech komponent řešení proxy serveru a jejich případný dopad na HA funkci tohoto řešení.
- Verifikace procesu zadání a vypořádání servisního požadavku zadaného objednatelem do ServiceDeskového systému zhotovitele.

Akceptace této etapy

Tato etapa bude úspěšně akceptována v případě, že řešení proxy serveru bude minimálně po nepřerušovanou dobu 2 týdnů splňovat provozní i bezpečnostní požadavky při plném zatížení v prostředí objednatele a řešení bude po tuto dobu bez závad.

Další podmínkou akceptace je, že objednateli byla dodána případná aktualizace dokumentace dle skutečného stavu v prostředí objednatele.

Etapa nemůže být akceptována, pokud se vyskytnou zejména závažné vady či nedostatky provozu proxy serveru a nebyla tak splněna doba minimálně 2 týdnů nepřetržitého bezproblémového provozu.

Příloha č. 4

Bezpečnostní požadavky objednatele

1) Zhotovitel odpovídá za to, že do objektů objednatele (dále jen „ČNB") budou vstupovat nebo vjíždět pouze jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu schváleném ČNB (dále jen „seznam"). Tato povinnost se vztahuje i na posádky vozidel zhotovitele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam zhotovitel předloží ČNB nejpozději v den podpisu smlouvy.

2) Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti pracovníků zhotovitele. Součástí seznamu je „Prohlášení o poučení subjektů osobních údajů" o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOÚ") a 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 („GDPR"). Zhotovitel v něm prohlásí a nese odpovědnost za to, že jeho pracovníci uvedení v seznamu byli poučeni:

   a) o tom, že zhotovitel 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 zhotoviteli a ČNB, zejména o právu právo na přístup k osobním údajům, které jsou o nich zpracovávány, právo na námitku proti zpracování osobních údajů, požadovat nápravu situace, která je v rozporu s právními předpisy, zejména formou zastavení nakládání osobními údaji, jejich opravou, doplněním či odstraněním a právem podat stížnost k Úřadu pro ochranu osobních údajů.

3) Zhotovitel si je vědom povinností vyplývajících pro správce osobních údajů z GDPR, které nabývá účinnosti 25. května 2018, a obsah poučení upraví tak, aby požadavky tohoto nařízení ode dne jeho účinnosti splňoval.

4) Požadavky na případné doplňky a změny schváleného seznamu pracovníků zhotovitele je nutno neprodleně oznámit ČNB. Případné doplňky a změny 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 zhotovitele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny na seznamu, nebudou do objektu ČNB vpuštěny.

6) Schválení pracovníci zhotovitele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci zhotovitele budou do prostorů 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 zhotovitele musí řídit pokyny bankovních policistů nebo dozorujícím zaměstnancem ČNB, a dále instrukcemi vyhlašovanými vnitřním rozhlasem.

8) Pracovníci zhotovitele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom co je a není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.

9) ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka zhotovitele, 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 zhotovitel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací, dozorujícího zaměstnance ČNB. Dále se pracovníci zhotovitele musí zdržet poškozování či zcizení majetku ČNB, a dále zdržet se nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.

12) Pracovníci zhotovitele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifikami 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 zhotovitele uvedeného na seznamu z dodržování těchto předpisů a ustanovení.

Příloha č. 5

Provozní podpora, SLA podpory od zhotovitele

1. Obecné náležitosti provozní podpory

1. Provozní podpora bude poskytována v obou instalačních lokalitách objednatele.
2. Služby poskytované zhotovitelem musí vyhovovat technickým a softwarovým specifikacím a požadavkům výrobce příslušného řešení proxy serveru.
3. Zhotovitel je srozuměn s tím, že veškerá komunikace při hlášení a řešení závad bude mezi objednatelem a technickými pracovníky zhotovitele probíhat v českém (nebo po vzájemném odsouhlasení pro daný případ v anglickém jazyce).
4. O klasifikaci nahlášených závad rozhodují pracovníci objednatele.
5. Detekované závady mohou být dočasně vyřešeny nebo jejich důsledky mohou být potlačeny také například pomocí dočasného řešení – workaround. Pracovníci objednatele rozhodují, zda workaround splňuje požadavek na dočasné vyřešení či potlačení důsledků závady umožňující další provoz řešení proxy serveru.
    a. Akceptovaný workaround splňuje závazek zhotovitele opravit nahlášenou závadu.
    b. Bez ohledu na akceptovaný workaround pokračuje zhotovitel v procesu nalezení systémového řešení trvale odstraňující / opravující nahlášenou závadu.
6. Zhotovitel se zavazuje převzít od objednatele vyměněné vadné díly řešení proxy serveru.
7. Zhotovitel souhlasí s tím, že při výměně vadného disku či média pro uchovávání dat budou na vadném disku či médiu smazána data tzv. degausserem (označováno též jako „magnetická pec"). Smazání dat na disku zajišťují zaměstnanci objednatele. Jiné komponenty umožňující trvalý záznam dat nemagnetického charakteru (např. SSD, Flash apod.) objednatel nevrací a zajistí sám jejich bezpečné smazání a likvidaci.

2. Popis služby Helpdesk

Detaily autorizace a popis komunikace

Problém, závadu nebo požadavek na konzultaci ohlašuje oprávněná osoba objednatele na HelpDesk zhotovitele.

Hlášení problému/závady/požadavku na konzultaci musí obsahovat

1. datum a čas hlášení
2. instalační lokalitu a jméno kontaktní osoby, která problém nahlásila
3. stručný popis problému/požadavku

Problém se hlásí na HelpDesk zhotovitele:

- Telefon: 800 73 73 11 (v pracovních dnech od 8:00 – 18:00 hod.)
  800 73 73 11 (mimo pracovní dobu)
- Email: dohled@t-mobile.cz

Problémy/závady/požadavky na konzultaci jsou hlášeny pouze oprávněnými osobami objednatele:

Jméno a příjmení	E-mail	Telefon	Mobil
Milan Zirnsák	milan.zirnsak@cnb.cz	224 414 334	736 524 489
Petr Puchmeltr	petr.puchmeltr@cnb.cz	224 412 883	731 597 041
Jiří Matějka	jiri.matejka@cnb.cz	224 412 390	731 597 094
Karel Weiss	karel.weiss@cnb.cz	224 413 571	736 524 465
Milan Vácha	milan.vacha@cnb.cz	224 413 442	736 265 285

Provozní doba služby Helpdesk

Provozní doba pro hlášení problémů/závad/požadavků na konzultaci na HelpDesk zhotovitele je v pracovní dny od 8:00 do 18:00. Provozní doba pro plnění této služby a interval pro počítání měřených parametrů je v pracovní dny od 8:00 do 18:00

Cíle služby Helpdesk, termíny a standardní měřené parametry

Zhotovitel vyvine maximální úsilí, které lze spravedlivě požadovat, k odstranění problému/požadavku.

Standardní měřené parametry jsou:

- doba odezvy
- množství řešených /vyřešených incidentů

Priorita	Doba odezvy	Čas s vyvinutím maximálního úsilí k odstranění problému do
Vysoká	1 hodina	4 hodin
Střední	1 hodina	16 hodin
Nízká	1 hodina	30 hodin

Pravidla pro určení priority a dopadu

V požadavku na službu objednatel specifikuje její prioritu pro jednotlivá zařízení v mezích dle níže uvedené tabulky

Priorita	Popis	Příznaky
Vysoká	Závada se týká prvků sítě nebo bezpečnostního prvku, jejichž výpadek způsobuje, že významná část uživatelů má znemožněn přístup z/do sítě LAN/WAN/DMZ/Internetu a neexistuje postup pro náhradní řešení problému.	▪ nefunkční centrální řízení řešení ▪ nefunkční prvky modulárního řešení (celý cluster) ▪ nefunkční gateway na perimetru (celý cluster) ▪ kompletně nefunkční bezpečnostní řešení
Střední	Závada se týká prvků sítě nebo bezpečnostního prvku, jejichž výpadek způsobuje, že jen část uživatelů má znemožněn	▪ výpadek jednoho prvku ve skupině řešení ▪ výpadek gateway na perimetru

	přístup z/do sítě LAN/WAN/DMZ/Internetu a existuje postup pro náhradní řešení problému.	▪ nefunkční část bezpečnostního řešení ▪ nefunkční jednotlivé bezpečnostní funkce
Nízká	Provozní problémy, které omezují pouze jednotlivé uživatele.	▪ bezpečnostní prvek je v provozuschopném stavu, přesto se v logu OS vyskytují chyby

Zhotovitel může po prozkoumání problému navržený stupeň důležitosti požadavku ve spolupráci – po schválení objednatelem překlasifikovat. V případě, že objednatel nesouhlasí se stanovením klasifikace, je problém eskalován podle Eskalačního procesu.

Eskalační proces

V případě, že nestandardní situaci při řešení problému není možné vyřešit v rámci dané úrovně, pracovníci této úrovně řeší tuto situaci s pracovníkem nejbližší vyšší úrovně.

1. úroveň: oprávněné osoby/Service Desk objednatele a Help Desk zhotovitele
2. úroveň: ředitel odboru objednatele a jmenovaný Service Manager zhotovitele
3. úroveň: ředitel sekce informatiky objednatele a ředitel společnosti zhotovitele

Definice pojmů

Response time – jedná se o reakční dobu, kdy je objednateli sděleno, že jeho požadavek byl zaevidován a je zpracován.

Fix time – jedná se o dobu od doby nahlášení do doby, kdy je nahlášený incident vyřešen a to ať dočasným řešením (work-around) nebo je vyřešen. V případě, že je požadavek znovu otevřen, je doba potřebná k jeho opětovnému vyřešení přičtena k době, po kterou byl požadavek již řešen.

Priorita vysoká – fix time 4 hod;
znamená, že nahlášený incident bude vyřešen nejpozději do 4 hodin od nahlášení, v garantované době poskytování služby. V případě, že bude nutnost dodávky nového HW, bude závada odstraněna nejpozději do 4 hodin od dodání nového HW. V případě nutnosti dodání nové verze SW, hotfixu, servis patce, upgrade atd. bude oprava provedena do 4 hodin od obdržení nové verze SW, hotfixu, servis patce, upgrade atd. od výrobce.

Priorita střední – fix time 16 hod;
znamená, že nahlášený incident bude vyřešen nejpozději do 16 hodin od nahlášení, v garantované době poskytování služeb. V případě nutnosti dodání nové verze SW, hotfixu, servis patce, upgrade atd. bude oprava provedena do 16 hodin od obdržení nové verze SW, hotfixu, servis patce, upgrade atd. od výrobce.

Priorita nízká – fix time 30 hod;
znamená, že každý nahlášený incident bude vyřešen nejpozději do 30 hodin od nahlášení v garantované době poskytování služby.

3. Patchování

1. Součástí podpory řešení proxy serveru je i zajištění pravidelného cyklu patch

managementu.

2. Zhotovitel v rámci zajištění podpory zajistí náhradní díly, nové a opravné verze mikrokódu/firmware dodaných technických prostředků řešení proxy serveru a nové a opravné verze dodaných programových prostředků řešení proxy serveru včetně jejich implementace v cyklech a rozsahu dle doporučení jejich výrobce. Součástí podpory je také informování objednatele o vydání nových nebo opravných verzích a konzultace k těmto verzím.

4. Konzultace

Konzultace jsou prováděny na základě výzvy objednatele, přičemž předem je stanovena problematika a časový rozsah konzultace – je oboustranně odsouhlaseno před zahájením konzultací.

Příloha č. 6

Standardní systémové prostředí objednatele

Níže je uveden stručný výtah z popisu standardního systémového prostředí objednatele. Nejedná se o úplný popis, ale o výtah informací relevantních k danému zadávacímu řízení na dodávku a implementaci řešení proxy serveru.

1. OBECNÉ INFORMACE

V ČNB jsou v provozu dvě výpočetní střediska. Obě tato střediska jsou provozována systémem aktiv-aktiv, tj. v obou střediscích jsou zpracovávány různé informační systémy. Obě střediska mají konektivitu do Internetu a tato konektivita je provozována v režimu active-passive; mezi středisky je zřízeno několik síťových příček v různých úrovních.

Běžný uživatel není schopen rozlišit, ve kterém středisku je jeho požadavek zpracován.

1.1. Komunikační infrastruktura

Jedno výpočetní středisko je umístěno v budově ústředí v Praze 1 (instalační lokalita č. 1) a druhé v Praze 5 – Zličín (instalační lokalita č. 2). Každé středisko má zřízen svůj perimetr s DMZ.

Obě výpočetní střediska jsou propojena optickými vlákny (single mode) dvěma nezávislými trasami. Jedna z tras je dlouhá 22,0 km, druhá trasa je dlouhá 24,4 km. Obě trasy jsou rovnocenné z hlediska přenášených protokolů (TCP/IP, FC) a přibližně i objemu přenášených dat. Na obou koncích jsou umístěny multiplexory DWDM. Na těchto spojích jsou právě realizované síťové příčky mezi oběma výpočetními středisky.

Pro správnou funkci clusterů („stěhování" IP adres clusterových skupin) jsou lokality propojeny protokolem TCP/IP na úrovni L2 z hlediska rozhraní Ethernet.

1.2. Standardní komunikační vybavení

- LAN - strukturovaná kabeláž pro připojení uživatelů umožňující připojení rychlostí minimálně 100 Mbit/s. Standardní provedení je metalické (RJ-45), optická vlákna jsou typem doplňkovým;
- Páteřní LAN – Gigabit Ethernet až 10 Gbps;
- Připojení každé lokality do Internetu – 1 Gbps (provider T-mobile) v režimu active-passive;
- aktivní síťové prvky – platforma CISCO, plně přepínaná síť;
- LAN, MAN, WAN – multiplexory typu DWDM;
- Ethernet dle ISO 802.3 pro připojení uživatelských stanic;
- Protokol TCP/IP;
- Jmenné služby - DNS;
- Přesný čas – NTP.

  Jako zdroj přesného času je použit SNTP (Simple Network Time Protocol) server MTS (Moba Time Server). Server je synchronizován externím časovým signálem s GPS (Global Positioning System). Protokolem NTP (Network Time Protocol) se pak synchronizují další síťová zařízení. Struktura synchronizace je hierarchická.

1.3. Aplikace a systémové služby

- Backup – HP Data Protector v9.07,

- SIEM – HP ArcSight v6.9.1,
    1. konektor pro sběr logů z RHEL (Syslog+audit): 7.3.0
    2. konektor pro sběr logů z Oracle DB: do verze 11: 7.2.3
    3. konektor pro sběr logů z Oracle DB 12c: 7.1.7 (flex)
- HSM Thales (aktuálně 64bitová verze SW SecurityWorld 11.72.00 pro Linux a HSM Thales nShield Connect 6000 (firmware 2.51.12).
- MS Active Directory – provozováno na MS Windows 2008 R2 serveru

Pozn.: Verze aplikací a služeb jsou platné ke dni vyhlášení zadávacího řízení. Později může být aplikován minoritní update či patch, který může uvedenou verzi povýšit.

1.4. Předpokládaná zařízení komunikující do Internetu

1.4.1. Klientská zařízení

Uživatelé objednatele používají pro přístup do Internetu následující klientská zařízení s WWW prohlížeči:

1. Pracovní stanice PC (x86 IBM kompatibilní) s instalovaným operačním systémem MS Windows 7 Pro (32 bit) nebo Windows 10 Enterprise (64 bit) – MS IE11 a Edge, GoogleChrome, FireFox,
2. Virtuální klientská stanice vPC (publikovaný desktop založený na operačním systému MS Windows Server 2008 R2 + Citrix XenApp 6.5; v blízké budoucnosti upgrade na MS Windows Server 2016 + Citrix XenApp 7.1x),
3. Dále pak mobilní zařízení typicky mimo MS doménu objednatele připojované typicky přes Wi-Fi HotSpot (např. notebooky s operačním systémem Windows, tablety/mobilní telefony s operačním systémem Android, iOS a BlackBerry.).

V případě uživatelů využívajících vPC se jedná o konfiguraci, kdy na každém serveru hostujícím vPC pracuje současně cca 15 uživatelů. Každý takový server má z hlediska sítě LAN jednu IP adresu a všichni uživatelé vPC na tomto serveru pod ní také společně vystupují do sítě.

1.4.2. Ostatní zařízení (servery)

Ostatní zařízení, typicky: servery platformy x86 (Windows, RedHad Linux), pro které musí být z Internetu (krom jiného) umožněno stahování SW balíků, aktualizací, apod.

2. ZDROJE SYSTÉMOVÉHO PROSTŘEDÍ NABÍZENÉ PRO ZHOTOVITELE

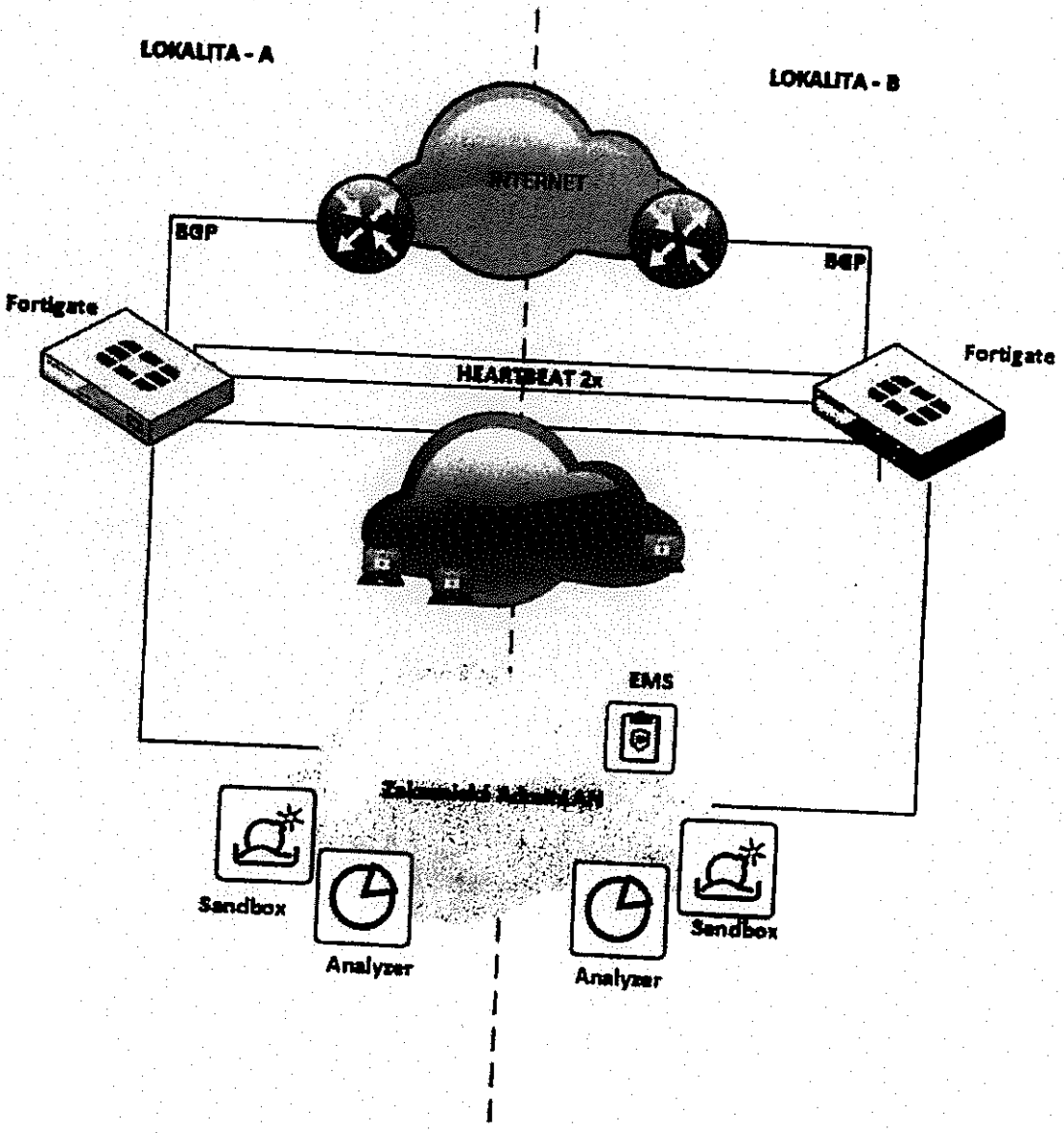
Zhotovitel může v rámci realizace této smlouvy využít následující prvky a komponenty standardního systémového prostředí ČNB.

- V každé instalační lokalitě objednatele je k dispozici 21U volného prostoru ve standardním 19'' racku (60cm šířka, 80cm hloubka),
- chlazení,
- Nosnost podlah – 200 kg / m2
- Nezávislé napájení 240V/50Hz (2 nezávislé okruhy).
- Potřebný rozsah IPv4 adres (vnitřních i veřejných) a výchozí brána (jinde, než v tomto řešení).

Technický návrh řešení proxy serveru

Řešení proxy serveru a firewallu se skládá z dvou Firewallů, které tvoří geocluster na dvou lokalitách zadavatele. Dále je součástí řešení implementace Sandboxingu, včetně licencí Windows 7, Windows 8/10 - Win8 / Win10 na obě lokality. Celé prostředí je centrálně logováno a dále je nad logy prováděna analýza a jejich archivace, což umožňuje zařízení Analyzéru, které je taktéž umístěno v obou lokalitách.

High level design:



Dodávka řešení serveru proxy

	Realizační studie - 1. etapa projektu	
1	Realizační studie	
a	Realizační studie včetně procesu její oponentury a akceptace	Cena v Kč bez DPH

	Řešení proxy serverů - dodávka a instalace - 2. + 3. etapa projektu	
2	Dodávka, instalace a aktivace řešení proxy serverů	Cena v Kč bez DPH
a	Cena za dodané technické prostředky proxy serveru (výpočetní + úložné + komunikační prvky) včetně jejich instalace v racích, napojení na napájení a datové sítě objednatele a včetně jejich podpory do finální akceptace	3 677 405,00
b	SW licence řešení proxy serveru (operační systém, aplikační software, HA řešení apod.) včetně jejich podpory do finální akceptace- serverová část	62 497,00
c	SW licence řešení proxy serveru (aplikační software apod.) včetně jejich podpory do finální akceptace - klientská část	529 271,00
d	Bezpečnostní služby řešení proxy serveru - aktivace a jejich podpora do finální akceptace	16 956,00
e	Implementace a konfigurace řešení proxy serveru	71 217,00
f	Zaškolení odborných pracovníků objednatele	54 261,00
	Řešení proxy serverů - dodávka, instalace a aktivace (2a+2b+2c+2d+2e+2f)	4 411 607,00

Příloha č. 9

Doklady prokazující odbornou způsobilost odborníků zhotovitele

Čestné prohlášení

uskutečněné v souvislosti s podáním nabídky na veřejnou zakázku „Dodávka řešení proxy serveru" pro veřejného zadavatele Česká národní banka

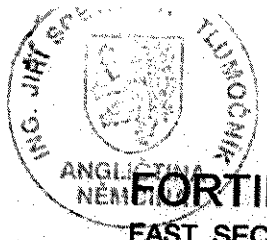
Já, níže podepsaný oprávněný zástupce T-Mobile Czech Republic a.s., IČ 64949681, se sídlem Tomíčkova 2144/1, 148 00 Praha 4, na základě pověření uděleného statutárním orgánem společnosti, vyzvaný k podání nabídky na plnění výše uvedené veřejné zakázky (dále jen „uchazeč") uvádím níže seznam techniků, jež se budou podílet na plnění veřejné zakázky.

Jméno	email, telefonní číslo	Funkce	Odborná kvalifikace (certifikáty a osvědčení)
Jan Bártl Hlavní technik	jan.bartl@t-mobile.cz 603 605 303	Vedoucí týmu řízených služeb	Fortinet - NSE 4 Security Professional - je odborně způsobilý pro administrátorskou správu a provozní podporu nabízeného proxy serveru
Ing. Attila Tóth Zástupce hlavního technika	attila.toth@t-mobile.cz 603 607 002	Senior specialista řízených služeb	Fortinet NSE 8 Fortinet Network Security Expert 8 NSE 7 Security Troubleshooter NSE 6 Security Specialist NSE 5 Security Analyst Fortinet Certified Network Security Professional NSE 4 Security Professional - je odborně způsobilý pro administrátorskou správu a provozní podporu nabízeného proxy serveru

V Praze dne 31.1.2018

Digitálně podepsal Radek Podzemský

Radek Podzemský
Na základě pověření



FORTINET®
FAST. SECURE. GLOBAL.

OVĚŘENÝ PŘEKLAD

Certifikováno NSE

Tímto se osvědčuje, že

Jan Bartl

byl úspěšně certifikován jako

NSE 4 Security Professional

29. května 2014

nečitelný podpis
KEN XIE
VÝKONNÝ ŘEDITEL
FORTINET

nečitelný podpis
MICHAEL XIE
TECHNICKÝ ŘEDITEL
FORTINET

FORTINET
Network Security Expert Program
(Program pro specialisty na zabezpečení sítí)

FORTINET
FAST. SECURE. GLOBAL.

NSE Certified

This certifies that

Jan Bartl

has successfully certified for

NSE 4 Security Professional

5/29/2014

[redacted]

KEN XIE
CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]

MICHAEL XIE
CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
Network Security Expert Program

Jako tlumočník jazyka anglického a německého, jmenovaný rozhodnutím předsedy Městského soudu v Praze ze dne 27.9.1992, č.j. Spr 203/92 stvrzuji, že překlad souhlasí s textem připojené listiny.

V překladu jsem provedl tyto opravy: žádné

Tlumočnický úkon je zapsán pod poř. číslem 03/2016 deníku.

Praha 4. 1. 2016

Ing. Jiří Spěváček
Na Santince 2
160 00 Praha 6

ING. JIŘÍ SPĚVÁČEK
ANGLIČTINA
NĚMČINA

[redacted]

ING. JIŘÍ ... ÚŘEDNÍ PŘEKLADATEL ... ANGLIČTINA ... NĚMČINA ... SOUDNÍ TLUMOČNÍK

OVĚŘENÝ PŘEKLAD

FORTINET®
FAST. SECURE. GLOBAL.

Certifikováno NSE

Tímto se osvědčuje, že

Attila Toth

byl úspěšně certifikován jako

NSE 6 Security Specialist

24. července 2015

nečitelný podpis
KEN XIE
VÝKONNÝ ŘEDITEL
FORTINET

nečitelný podpis
MICHAEL XIE
TECHNICKÝ ŘEDITEL
FORTINET

FORTINET
Network Security Expert Program
(Program pro specialisty na zabezpečení sítí)

FORTINET
FAST. SECURE. GLOBAL.

NSE Certified

This certifies that

Attila Toth

has successfully certified for

NSE 6 Security Specialist

7/24/2015

[redacted]

KEN XIE
CHIEF EXECUTIVE OFFICER
FORTINET

[redacted]

MICHAEL XIE
CHIEF TECHNOLOGY OFFICER
FORTINET

FORTINET
Network Security Expert Program

Jako tlumočník jazyka anglického a německého, jmenovaný rozhodnutím předsedy Městského soudu v Praze ze dne 27.9.1992, č.j. Spr 203/92 stvrzuji, že překlad souhlasí s textem připojené listiny.

V překladu jsem provedl tyto opravy: žádné

Tlumočnický úkon je zapsán pod poř. číslem 05/2016 deníku.

Praha 4. 1. 2016

Ing. Jiří Spěváček
Na Santince 2
160 00 Praha 6

ING. JIŘÍ SPĚVÁČEK TLUMOČNÍK
ANGLIČTINA
NĚMČINA

[redacted]

Příloha č. 10

Šablona realizační studie

ČESKÁ ČNB NÁRODNÍ BANKA

Projekt *ID projektu*

„*Název projektu*“

Realizační studie

Verze	
Datum verze	
Autor	
Vedoucí projektu *poskytovatele*	
Vedoucí projektu objednatele	

Historie změn

Verze	Datum	Autor	Popis změny

Obsah

Pozn.: Hlavní kapitoly realizační studie jsou povinné, struktura podkapitol je doporučená a je možno ji rozšiřovat či upravovat dle potřeb projektu a nabízeného řešení.

1 ÚVOD

1.1 Účel dokumentu

[Dokument realizační studie popisuje způsob realizace řešení včetně analýzy funkčních požadavků, softwarové architektury a systémových požadavků tak, aby byla prokázána realizovatelnost všech zadaných požadavků.]

1.2 Seznam pojmů a zkratek

[Výčet klíčových zkratek a pojmů s jejich vysvětlením]

Termín/Zkratka	Popis/Význam

1.3 Přehled použitých symbolů

[Popis použitých grafických symbolů v dokumentu]

Grafický symbol	Význam

1.4 Legislativa, technické normy a standardy

[Seznam legislativy, standardů a norem používaných při realizaci řešení.]

Č. zákona/ ČSN..... ISO.....	Název/Popis

2 NÁVRH A POPIS REALIZACE ŘEŠENÍ

2.1 Popis současného a cílového stavu

[Kapitola popisuje popis současného stavu (pokud existuje) a popis cílového stavu.]

2.2 Analýza funkčních požadavků

[Kapitola obsahuje mapování funkčních požadavků na cílové řešení. Popis tak ve stručné formě představuje způsob realizace jednotlivých funkčních požadavků.]

ID[1]	Název požadavku	Popis realizace	Poznámka

2.3 Analýza specifických požadavků

[Kapitola obsahuje mapování specifických požadavků na cílové řešení. Popis tak ve stručné formě představuje způsob realizace jednotlivých požadavků.]

ID[2]	Popis požadavku	Popis realizace	Poznámka

2.4 Analýza procesů a datových toků

[Kapitola obsahuje analýzu procesů a toků dat spojených s provozem a využíváním cílového řešení, pro jejich grafické znázornění lze použít například UML Activity diagram, nebo BPMN (Business Process Model and Notation).]

2.5 Migrace nastavení a dat

[Kapitola obsahuje analýzu a namapování datových struktur původního a nově projektovaného řešení z hlediska jejich převoditelnosti a datové migrace (tj. jednoznačné srovnání datových objektů, které budou využívány při migraci dat mezi oběma systémy) a popis vlastní migrace. Na analýze se podílejí jak zadavatel, tak poskytovatelé obou systémů.]

2.6 Bezpečnost a osobní údaje

[Kapitola obsahuje popis řešení z hlediska bezpečnosti, integrity a důvěrnosti dat, použitých standardů atd. Zároveň zde budou zohledněny požadavky objednatele na bezpečnostní politiku nastavení proxy serveru vyplývajících z vnitřních předpisů objednatele.]

2.6.1 Analýza bezpečnostních požadavků

[Podkapitola obsahuje analýzu bezpečnostních požadavků, pokud není uvedeno v kapitolách 2.2 a 2.3.]

2.6.2 Autentizace a autorizace, řízení přístupu

[V podkapitole je popsán princip řízení přístupů k informacím resp. informačním aktivům: jakým prostřednictvím přistupují interní a externí uživatelé, popis technických (aplikačních) účtů – bez časového omezení; způsob automatického blokování účtů uživatelů při ukončení zaměstnaneckého poměru v ČNB, povolené protokoly apod.]

2.6.3 Logování

[V podkapitole je popsán způsob logování a monitorování logů, napojení na SIEM.]

---

[1] ID požadavku objednatele
[2] ID požadavku objednatele

2.6.4 Zabezpečení síťové komunikace a uložených dat

[V podkapitole je popsán způsob, jak je zabezpečena síťová komunikace mezi servery a klientem a zabezpečení uložených dat – File-System / Database.]

2.6.5 Ochrana osobních dat, soulad s legislativou (Compliance)

[V podkapitole je popsán způsob, jak je zabezpečen soulad s legislativou – např. ZoKB, ISO20022 – případně podporuje procesy a požadavky spojené s GDPR apod. V případě, že navrhované řešení nebude splňovat nějaké legislativní požadavky, uvede se tato skutečnost v této kapitole včetně zdůvodnění proč.]

2.7 Návrh architektury technického řešení

[Kapitola popisuje globální architekturu navrhovaného řešení a fyzickou architekturu nasazení řešení v infrastruktuře ČNB s ohledem na jeho provoz, monitoring, zabezpečení, zálohování a archivaci atd.]

2.8 Popis administrátorského a uživatelského rozhraní (GUI)

[Kapitola obsahuje popis a použití grafického rozhraní pro administraci a použití cílového řešení.]

2.9 Integrace se systémovým prostředím objednatele

[Kapitola a následující kapitoly popisují integraci navrhovaného řešení do systémového prostředí objednatele, případně požadavky na jeho změny či doplnění. Níže uvedené podkapitoly jsou pouze návodné a neposkytují plný výčet – bude doplněno dle potřeb cílového řešení.]

2.9.1 Požadavky na systémové prostředí

[Podkapitola obsahuje SW a HW specifikaci pro dodávané řešení, případně požadavky na další HW či SW v systémovém prostředí ČNB. Součástí specifikace je i sizing HW prostředků pro účely implementace řešení. Různá prostředí provoz/test/vývoj/školení/atd. jsou popsána zvlášť.]

Tabulka 1: HW specifikace

Prvek	Typ	Výkon	RAM	Disková kapacita	Síťové rozhraní	Poznámka
PrvekHW001	*Virtuální server*	*2 – 4 virtuální CPU, 2 – 3 GHz*	*4 – 8 GB*	*15 GB*	*100 Mbps*	*Dodává zhotovitel / Poskytuje objednatel*
PrvekHW002	*Fyzický server (logy)*					

Tabulka 2: SW specifikace

Prvek	OS	Databázové služby	Aplikační služby	Způsob instalace	Poznámka
PrvekSW001	*Windows Server 2008 R2 ENG x64*	*Oracle client 10g*	*MS IIS 7.5 ASP.NET 3.5 SP1*		
PrvekSW002	*MS Windows 7 Pro MS Windows 10 Ent.*	*n/a*	*Agent pro autentizaci uživatele (Kerberos) k řešení*	*Automatická, MSI balíček distribuovaný prostřednictvím GPO*	

2.9.2 Autentizace a autorizace, řízení přístupu

[V podkapitole je popsáno technické řešení, požadavky na napojení na adresářové služby systémového prostředí, použité postupy a protokoly, vytváření účtů a práv s nimi spojených apod.]

2.9.3 Administrace a řízení řešení

[V podkapitole je popsán způsob centrální správy řešení.]

2.9.4 Systémové logování

[V podkapitole je popsán způsob provozního logování a monitorování logů řešení, jejich napojení na SIEM.]

2.9.5 Logování přístupu do Internetu

[V podkapitole je popsán způsob logování uživatelských a jiných přístupů do Internetu, jejich kategorizace, uložení a objemy přenesených dat, životní cyklus dat v lozích (retence logů) apod.]

2.9.6 Zabezpečení síťové komunikace a uložených dat

[V podkapitole je popsán způsob zabezpečení protokolů a dat – šifrování, řízení přístupu apod.]

2.9.7 Zálohování

[V podkapitole je popsán způsob zálohování dat, konfigurací, backup/restore postupy (scénáře) apod.]

2.10 Integrace řešení s IS ČNB

[Kapitola obsahuje:

- *popis možností integrace řešení s jednotlivými stávajícími a budoucími (projektovanými) IS ČNB*
- *detailní popis rozhraní pro pravidelné, automatizované předávání a přebírání dat z/do IS ČNB.]*

2.11 Způsob implementace do systémového prostředí ČNB, součinnost

[Kapitola obsahuje postup nasazení řešení do cílového prostředí s ohledem na stanovení příslušné součinnosti ze strany ČNB.]

3 Návrh projektové realizace

3.1 Detailní harmonogram realizace

[Harmonogram realizace uvádí rozpad realizace projektu do jednotlivých přírůstků (dílčích plnění), etap, fází a činností s ohledem na dodržení stanovených termínů/lhůt. Harmonogram *musí obsahovat milníky pro předání řešení nebo jeho částí k akceptačnímu řízení.]*

3.2 Požadavky na součinnost (*pro externí dodávku)*

[V kapitole je uveden rozsah kapacit požadovaných zhotovitelem po objednateli]

ID	Popis součinnosti	Rozsah	Čerpání

Legenda:
ID: jedinečný identifikátor požadované součinnosti
Popis součinnosti: popis aktivit, požadovaných poskytovatelem po objednateli
Rozsah: odhadovaný rozsah požadovaných kapacit v čld
Čerpání: četnost, způsob čerpání kapacit např. 1x týdně; 2hod v Pá

3.3 Akceptační testy

[V kapitole je uveden seznam všech připravovaných akceptačních testů, které kompletně ověří požadovanou funkcionalitu řešení a zodpovědnost za vypracování testovacích scénářů]

ID testu	Testovaná oblast	Testovací scénář	ID požadavku[3)]	Testovací scénář vypracovává

Legenda:
ID scénáře: jedinečný identifikátor testovacího scénáře
Testovaná oblast: oblast testování např.: Personalistika, ...
Testovací scénář: popis testovacího scénáře
ID požadavku: jedinečné identifikátory požadavků objednatele, které jsou daným testovacím scénářem ověřovány.
Testovací scénář vypracovává: jméno/firma autora testovacího scénáře

3.4 Školení

[Kapitola detailněji popisuje způsob zajištění školení a proškolení příslušných pracovníků, okruh školených uživatelů a správců, kdo zodpovídá za zpracování školící dokumentace a pokud není uvedeno v harmonogramu, tak i předpokládané termíny školení]

3.5 Dokumentace

[V kapitole je uveden seznam technické, provozní a uživatelské dokumentace a zodpovědnost za její zpracování/aktualizaci.]

[3)] Požadavky z předběžné studie (funkční a specifické)

4 Registr změn

[V kapitole je uveden seznam změn oproti předběžné studii/zadávací dokumentaci, jejich akceptace a jejich dopady do projektu -- časové, zdrojové a finanční.]

ID změny	Popis změny	Akceptována Ano/Ne	Realizace (termín, zdroje a finance)

PŘÍLOHA č. 12

POVĚŘENÍ

Společnost T-Mobile Czech Republic a.s., se sídlem v Praze 4, Tomíčkova 2144/1, PSČ 149 00, IČ 64949681, (dále jen „Společnost") jednající prostřednictvím představenstva Společnosti tímto **p o v ě ř u j e** níže uvedeného zaměstnance

Ing. Petra MALIMÁNKA

nar. 21. 4. 1970

aby za Společnost jednal a vykonával:

- veškeré úkony, které souvisí se smlouvami o poskytování služeb elektronických komunikací služeb a o prodeji komunikačních zařízení a jejich příslušenství firemním zákazníkům a se smlouvami o zprostředkování anebo spolupráci při uzavírání uvedených smluv; zejména se jedná o uzavírání, změny a ukončování takových smluv
- veškeré úkony, které souvisí se smlouvami, které upravují komplexní řešení ProfiNet, prodej jakýchkoli nehlasových služeb a služeb s přidanou hodnotou anebo souvisí se smlouvami o spolupráci na Partnerském programu T-Mobile, které upravují podmínky pro vzájemnou spolupráci mezi Společností a jejími obchodními partnery při využití sítě T-Mobile pro poskytování služeb třetím osobám; zejména se jedná o uzavírání, změny a ukončování takových smluv
- veškeré úkony podle zákona o veřejných zakázkách, to znamená, aby podával nabídky a prováděl veškeré právní úkony ve veřejných zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění veřejné zakázky
- veškeré úkony, které souvisejí se smlouvami o propagaci Společnosti, s darovacími smlouvami a sponzoringovými smlouvami, u nichž výše plnění Společnosti nepřesahuje částku 300.000 Kč;zejména se jedná o uzavírání, změny a ukončování takových smluv
- veškeré úkony, které souvisí se smlouvami o propagaci třetích stran, zejména smluv o užívání reklamního prostoru Společnosti či rozesílání SMS či MMS s reklamou třetí strany. Jedná se především o uzavírání, změny a ukončování takových smluv, nepřevyšuje-li výše plnění z těchto smluv 3.000.000,- Kč.

Zmocněnec není oprávněn zmocnit ani jinak pověřit jinou osobu, aby místo něho jednala za Společnost, s výjimkou oprávnění ke zmocnění zaměstnanců Společnosti, aby místo pověřeného zaměstnance zastupovali Společnost při otevírání obálek, prohlídce místa plnění, nebo při ústním vysvětlení nabídky v termínech stanovených zadavateli veřejných zakázek v jednotlivých výběrových řízeních.

Podepisování pověřeného zaměstnance se děje tak, že k napsané nebo vytištěné obchodní firmě Společnosti či otisku razítka Společnosti připojí pověřený zaměstnanec svůj podpis.

V Praze dne 17. března 2016

[redacted]

Mark Klein
předseda představenstva

[redacted]

Martin Schlieker
člen představenstva

Toto pověření přijímám:

[redacted]

Ing. Petr Malimánek

[redacted]

Ověření – legalizace
Běžné číslo ověřovací knihy O I 366 - 395/2016
Ověřuji, že Mark Klein, nar. 30.9.1971, s bydlištěm Flemingweg 29, Düsseldorf, SRN, a Martin Schlieker, nar. 14.9.1961, s bydlištěm Im Michelsfeld 7a, Bonn, SRN, jejichž totožnosti byly prokázány, tuto listinu přede mnou vlastnoručně podepsali.
V Praze dne 17.3.2016

[redacted]

Ověřovací doložka pro vidimaci Poř.č: 14800-0057-0380
Podle ověřovací knihy pošty: Praha 414

Tato úplná kopie, obsahující 2 stran souhlasí doslovně s předloženou listinou, z níž byla pořízena a tato listina je prvopis, obsahující 2 stran.

Listina, z níž je vidimovaná listina pořízena, neobsahuje viditelný zajišťovací prvek, jenž je součástí obsahu právního významu této listiny.

Praha 414 dne 05.04.2016
Orgoníková Michaela

[redacted]
Podpis, úřední razítko

POVĚŘENÍ

Společnost T-Mobile Czech Republic a.s., se sídlem v Praze 4, Tomíčkova 2144/1, PSČ 148 00, IČ 64949681, (dále jen „Společnost") jednající prostřednictvím představenstva Společnosti tímto **pověřuje** níže uvedeného zaměstnance:

Ing. Petra ŽÁČKA

nar. 23. 6. 1972

aby za Společnost jednal a vykonával:

- veškeré úkony, které souvisí s nabídkami a se smlouvami (zejména podávání nabídek a uzavírání, změny či ukončování smluv), které se týkají plnění Společnosti vůči svým zákazníkům, a to v oblasti:
  - poskytování služeb elektronických komunikací;
  - prodeje či pronájmu komunikačních zařízení a jejich příslušenství,
  - poskytování komplexního řešení ProfiNet nebo Firemní řešení;
  - prodeje jakýchkoli nehlasových služeb a služeb s přidanou hodnotou;
  - poskytování dalších ICT služeb a řešení, včetně služeb podpory takových řešení;
  - poskytování práv k užití software;
  - zachování důvěrnosti informací při poskytování plnění dle výše uvedených nabídek nebo smluv;
  - spolupráce s dodavateli při plnění dle výše uvedených nabídek nebo smluv.
- veškeré úkony podle zákona o veřejných zakázkách, to znamená, aby podával nabídky a prováděl veškeré právní úkony ve veřejných zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění veřejné zakázky,
- veškeré úkony v případě, kdy zadavatel dobrovolně zvolí aplikaci zákona o veřejných zakázkách, to znamená, aby podával nabídky a prováděl veškeré právní úkony v takových zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění zakázky

V Praze dne 12 -10- 2016

[redacted]

[redacted]

Toto pověření přijímám:

[redacted]

Ing. Petr Žáček

Ověření - legalizace

Běžné číslo ověřovací knihy O Ľ 4-21/2016

Ověřuji, že Hochar Schleker, nar. 14.9.1961, SRN, Bonn, Jan Hubels-feld 2 A

jehož (jejíž) totožnost byla prokázána, tuto listinu přede mnou vlastnoručně podepsal (a).

V Praze dne 12. 10. 2016

[redacted]

JUDr. Jitka Sladk[redacted]
pověřená notářem
JUDr. Romanem Hochmanem
Praha 1, Hybernská 1032/9
tel.: 224 221 058, 224 247 137

JUDr. ROMAN HOCHMAN 2 Notář v Praze

Ověření - legalizace

Běžné číslo ověřovací knihy O Ľ 4-21/2016

Ověřuji, že Dr. Ralph Roland Rentschler, nar. 4.11.1960, SRN, Stuttgart, Liederlückweg 3

jehož (jejíž) totožnost byla prokázána, tuto listinu přede mnou vlastnoručně podepsal (a).

V Praze dne 12. 10. 2016

[redacted]

JUDr. Jitka Sladká
pověřená notářem
JUDr. Romanem Hochmanem
Praha 1, Hybernská 1032/9
tel.: 224 221 058, 224 247 137

JUDr. ROMAN HOCHMAN 2 Notář v Praze