Smlouva
o poskytnutí, instalaci a podpoře API pro komunikaci s TPP

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „o.z."), mezi:

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

(dále jen „objednatel" nebo „ČNB")

a

Wultra s.r.o.

Bělehradská 858/23
120 00 Praha 2 – Vinohrady
zastoupenou: Mgr. Petrem Dvořákem, CEO a jednatelem
IČO: 03643174
DIČ: CZ03643174
č. účtu: 3643174999/5500

(dále jen „poskytovatel")

Článek I
Předmět smlouvy

1. Předmětem této smlouvy je závazek poskytovatele dodat a implementovat API (Application Programming Interface) dle Českého standardu pro Open Banking vydaný Českou bankovní asociací (dále též „programové vybavení" nebo „dílo") a poskytnout objednateli oprávnění k jeho užívání (licenci) v rozsahu dle čl. VI. Programové vybavení musí splňovat požadavky dle přílohy č. 1 a přílohy č. 3 této smlouvy a musí být plně funkční v systémovém prostředí objednatele, které je specifikováno v příloze č. 2 této smlouvy.
2. Součástí programového vybavení je dokumentace, kterou poskytovatel poskytne v elektronické podobě ve formátu PDF, MS Office 2010 a vyšším nebo HTML. Dokumentace bude obsahovat:
    a) administrátorskou příručku,
    b) příručku technického správce,
    c) uživatelskou příručku,

(dohromady dále též „dokumentace"). Dokumentaci je poskytovatel povinen poskytnout v českém nebo anglickém jazyce nebo v cizojazyčném originálu s překladem do češtiny.

3. Součástí plnění podle čl. I odst. 1 je zaškolení 2 administrátorů ohledně věcné a technické správy programového vybavení v rozsahu 1 pracovního dne, a to v sídle objednatele, nedohodnou-li se smluvní strany jinak.
4. Předmětem této smlouvy je rovněž závazek poskytovatele poskytovat podporu programovému vybavení v rozsahu a za podmínek uvedených v čl. IV a dodání datového média s čitelným, nešifrovaným a kompletním zdrojovým kódem programového vybavení.
5. Poskytovatel se dále zavazuje poskytovat budoucí rozvoj programového vybavení v rozsahu a za podmínek stanovených v článku V.
6. Objednatel se zavazuje zaplatit za uvedená plnění dohodnuté ceny podle čl. V této smlouvy.

Článek II
Lhůty a místo plnění

1. Dílo bude prováděno postupně v následujících lhůtách:
   a) Poskytovatel předá programové vybavení spolu s dokumentací k instalaci do testovacího prostředí objednatele nejpozději do 8 týdnů od podpisu této smlouvy.
   b) Objednatel provede testování dodaného programového vybavení v testovacím prostředí. Testování bude prováděno po dobu 2 týdnů.
   c) Zaškolení administrátorů bude poskytovatelem provedeno nejpozději 3 pracovní dny před předáním programového vybavení k akceptačnímu testování. O plánovaném datu zaškolení informuje poskytovatel objednatele nejméně 5 pracovních dnů předem. O provedení školení sepíše poskytovatel protokol obsahující den, čas a místo školení, jména školených osob a stručný popis obsahu školení, který bude podepsán pověřenými osobami obou smluvních stran.
   d) Poskytovatel předá kompletní programové vybavení k instalaci do provozního prostředí objednatele, a to bez vad zjištěných v rámci testování v testovacím prostředí, včetně datového média se zdrojovým kódem k akceptačnímu testování do 12 týdnů od podpisu smlouvy.
   e) Objednatel provede akceptační testování dodaného programového vybavení v provozním prostředí objednatele. Akceptační testování bude prováděno po dobu 2 týdnů.
   f) Poskytovatel předá programové vybavení, dokumentaci dle čl. I odst. 2 a datové médium se zdrojovým kódem dle čl. I odst. 4 objednateli nejpozději do 16 týdnů od podpisu této smlouvy. Nejpozději při předáním provede poskytovatel také základní uživatelské nastavení programového vybavení.
2. Objednatel je oprávněn k užití programového vybavení ode dne úspěšného ukončení akceptačního testování v provozním prostředí objednatele. Poskytování podpory podle čl. I odst. 4 zahájí poskytovatel v den převzetí programového vybavení.
3. Místem plnění je sídlo objednatele na adrese Česká národní banka, Na Příkopě 28, 115 03 Praha 1, nestanoví-li dále tato smlouva nebo nedohodnou-li se pověřené osoby smluvních stran jinak.

Článek III
Testování, předání a převzetí díla

1. Při testování v testovacím a v provozním prostředí objednatele bude objednatelem ověřeno, zda programové vybavení je funkční, splňuje veškeré stanovené požadavky a nevykazuje přítomnost zranitelností (viz finální část přílohy č. 3 smlouvy – „Bezpečnost IT").
2. Během testování je přítomen pracovník poskytovatele.
3. Vyskytne-li se během testování vada, která si vynutí přerušení testování, zejména že programové vybavení je nefunkční, ohrožuje bezpečnost objednatele, odstraní tuto vadu poskytovatel ve lhůtě určené objednatelem. Vyskytne-li se taková vada více než dvakrát nebo nebude-li v určené lhůtě odstraněna, je objednatel oprávněn od této smlouvy odstoupit. Testování se na dobu opravy vady přerušuje.
4. Vady zjištěné během testování v testovacím prostředí objednatele odstraní poskytovatel na místě, jinak bez zbytečného odkladu, nejpozději však do 1 týdne od jejich zjištění. Poté se testování opakuje a nejsou-li vady odstraněny, je objednatel oprávněn od smlouvy odstoupit; tím nejsou dotčeny lhůty podle čl. II smlouvy.
5. Vadám zjištěným během akceptačního testování bude přidělena některá z níže uvedených kategorií:

   Vady kategorie A:

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

   Vady kategorie B:

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

Vady kategorie C:

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

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

Článek IV
Podpora

1. Poskytování podpory programového vybavení dle čl. I odst. 4 v sobě zahrnuje provozní podporu a budoucí rozvoj.

2. Součástí provozní podpory je:

a) Informování objednatele o všech poskytovatelem připravovaných a realizovaných změnách programového vybavení, zasláním informace na e-mailové adresy pověřených osob objednatele podle čl. VII této smlouvy, a to nejméně 3 pracovní dny před realizací změny programového vybavení.

b) Podpora při řešení provozních problémů přímo souvisejících s programovým vybavením ve formě konzultací objednateli sloužících jako návody a rady jak použít programové vybavení v určité situaci a jak by mělo být nastaveno prostředí programové vybavení k jeho optimálnímu fungování. Konzultace budou poskytovány telefonicky na tel. +420 728 727 71 nebo e-mailem na *support@wultra.com*, a to v pracovní dny v mezi 8:00 a 16:00. V případě, že objednatel v rámci konzultací zašle poskytovateli dotaz na výše uvedenou emailovou adresu, je poskytovatel povinen poskytnout informace nejpozději následující pracovní den od doručení emailové zprávy objednatele.

c) Odstraňování vad programového vybavení v následujících lhůtách:

   i. do 24 hod; jde-li o vadu závažnosti 1, tedy:

- programové vybavení je kompletně nefunkční a svou činností ohrožuje chod systému, na kterém je provozováno;
- objednatel nepovažuje provoz programového vybavení za bezpečný, činnost programového vybavení generuje významné bezpečnostní riziko (typicky jde o nálezy kategorie 4-5 softwarového nástroje QualysGuard);
- významné funkce programového vybavení nelze použít;

ii. do 48 hod; jde-li o vadu závažnosti 2, tedy:

- významné funkce programového vybavení nelze spolehlivě použít, chování systému je nestandardní (vykazuje chyby);
- objednatel nepovažuje provoz programového vybavení za bezpečný, činnost programového vybavení generuje bezpečnostní riziko (typicky jde o nálezy kategorie 1- 3 softwarového nástroje QualysGuard);

iii. do 5 pracovních dnů o vadu závažnosti 3, tedy:

- ostatní vady zabraňující řádnému užívání nebo správě programového vybavení, popř. narušující běh dalších součástí systémového prostředí objednatele, výše nepopsané.

Závažnost vady určuje objednatel. Lhůta pro odstranění vady počíná běžet od oznámení vady objednatelem na e-mail support@wultra.com nebo telefonicky na tel. +420 728 727 714, nedohodnou-li se smluvní strany jinak. Zajistí-li poskytovatel ve lhůtách podle tohoto písmene workaround (dočasné řešení), prodlužuje se lhůta pro řešení příslušné vady o 15 pracovních dnů.

d) Aktualizace programového vybavení v případě změny právních předpisů ČR nebo EU či změny Českého standardu pro Open Banking vydaného Českou bankovní asociací (dále jen „standard ČOBS"), a to nejpozději v den nabytí účinnosti příslušného právního předpisu ČR nebo EU nebo vydání nového standardu ČOBS.

e) Aktualizace programového vybavení uvolňované na trh výrobcem programového vybavení (upgrade / patch), a to nejpozději v den jejich uvolnění na trh.

f) Aktualizace dokumentace související s aktualizacemi podle písm. d) a e) tohoto odstavce vč. překladu do češtiny (je-li originál dokumentace v jiném, než českém), a to nejpozději v den poskytnutí související aktualizace.

g) Udržování metodické a technologické jednotnosti a konzistentnosti všech prvků programového vybavení.

h) Na žádost objednatele provést instalaci a otestování objednatelem určených aktualizací programového vybavení. Podporu podle tohoto písmene poskytuje poskytovatel ve lhůtách dle dohody pověřených osob smluvních stran; nedohodnou-li se, určí lhůtu k poskytnutí služeb objednatel doručením na e-mail pověřených osob poskytovatele s tím, že tato lhůta nebude kratší než 15 pracovních dnů ode dne doručení e-mailu.

i) Konzultace, popř. jiná odborná pomoc, poskytovaná na žádost objednatele a přímo související s programovým vybavením, určená k jeho optimálnímu fungování, a to v rozsahu 10 člověkodnů (8 člověkohodin na člověkoden) vždy za každý rok poskytování podpory. Podporu podle tohoto písmene poskytuje poskytovatel ve lhůtách dle dohody pověřených osob smluvních stran; nedohodnou-li se, určí lhůtu k poskytnutí služeb

objednatel doručením na e-mail pověřených osob poskytovatele s tím, že tato lhůta nebude kratší než 15 pracovních dnů ode dne doručení e-mailu.

Článek V
Budoucí rozvoj programového vybavení

1. Rozvoj zahrnuje:

a) Konzultace nových uživatelských požadavků objednatele na úpravy programového vybavení.

b) Vypracování písemných analýz a návrhů řešení nových uživatelských požadavků objednatele na úpravy programového vybavení.

c) Upgrade programového vybavení, jehož potřeba vznikla na základě organizačních a technických změn u objednatele a změn vnitřních předpisů objednatele, a rovněž upgrade programového vybavení spojený se změnou systémového prostředí objednatele nad rámce nasazování aktualizací (update / upgrade / patch) komponent systémového prostředí objednatele.

d) Programátorské práce požadované objednatelem v souvislosti s požadovanými úpravami programového vybavení.

2. Součástí prací podle odstavce 1 písm. c) a d) je

a) Testování s tím, že čl. III se použije obdobně; délku testování určí objednatel nejméně v délce 3 dnů.

b) Předání čitelného a kompletního zdrojového kódu programového vybavení a dalších podkladů potřebných ke správě, údržbě a úpravám programového vybavení, včetně aktualizované dokumentace (např. datový model, programové knihovny), to vše v elektronické podobě na CD/DVD.

3. Činnosti podle odstavce 1 písm. b) až d) poskytuje poskytovatel ve lhůtách dle dohody pověřených osob smluvních stran. Nedohodnou-li se, určí lhůtu objednatel e-mailem s tím, že bude činit nejméně 60 pracovních dnů ode dne doručení e-mailu.

4. Konzultace podle odstavce 1 písm. a) poskytuje poskytovatel ve lhůtě dohodnuté pověřenými osobami. Nedohodnou-li se, určí lhůtu objednatel s tím, že bude činit nejméně 7 pracovních dnů od doručení e-mailu objednatele, Pokud v rámci konzultace bude objednatel požadovat zpracování rámcového návrhu řešení nového požadavku a nedojde-li k dohodě ohledně lhůty, určí ji objednatel s tím, že nebude kratší než 5 pracovních dnů ode dne doručení e-mailu.

Článek VI
Cena a platební podmínky

1. Cena za dodávku a implementaci programového vybavení podle čl. I odst. 1 činí 800 000 Kč bez DPH, cena za zaškolení administrátorů činí 10 000 Kč bez DPH. K ceně bude připočtena DPH v sazbě platné v den uskutečnění zdanitelného plnění. Sjednaná cena zahrnuje veškeré náklady poskytovatele spojené s plněním uvedeným v tomto odstavci.

2. Cena dle odst. 1 tohoto článku bude uhrazena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den předání a převzetí programového vybavení podle čl. III odst. 8 této smlouvy.

3. Cena za služby podpory dle čl. IV je stanovena paušálně a činí ročně 320 000 Kč bez DPH. Cena bude hrazena měsíčně. Daňový doklad je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce. V případě, že podpora nebude poskytována celý kalendářní měsíc, bude poskytovatel účtovat alikvótní část měsíční úhrady.

4. Cena za služby podle článku V bude stanovena na základě hodinové sazby ve výši 250 Kč bez DPH.

5. Ceny za služby dle čl. V odst. 1 písm. b) až d) budou sjednány vždy dohodou smluvních stran na základě odhadovaného počtu odpracovaných hodin a hodinové sazby podle odstavce 4 tohoto článku.

6. Ceny za konzultace dle čl. V odst. 1 písm. a) budou stanoveny jako součin hodinové sazby podle odstavce 4 a počtu skutečně odpracovaných hodin.

7. Daňový doklad na ceny plnění podle odst. 5 a 6 je poskytovatel oprávněn vystavit po poskytnutí příslušného plnění. Přílohou daňového dokladu na ceny podle odstavce 5 bude vždy příslušný protokol o předání plnění. Přílohou daňového dokladu na ceny za konzultace podle odstavce 6 bude vždy objednatelem schválený výkaz práce.

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

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

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

10. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřený pracovník poskytovatele povinen na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že

lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle předchozí věty.

11. Splatnost dokladů k úhradě je 14 dnů ode dne jejich doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

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

Článek VII
Rozsah práva k užití programového vybavení (licence)

1. Poskytovatel poskytuje objednateli na dobu trvání majetkových práv k dílu nevýhradní a místně neomezené licence k užívání programového vybavení a všech aktualizací programového vybavení nebo úprav v rámci budoucího rozvoje programového vybavení včetně aktualizací nebo úprav dokumentace, které vzniknou na základě plnění podle této smlouvy a ponesou znaky autorského díla (dále jen „Modifikace"). Objednatel je oprávněn:

   a) spojit Modifikace nebo kteroukoliv jejich část s jiným autorským dílem, zařadit do jiného díla, zařadit do díla souborného, a takto je užít způsoby dle této smlouvy,

   b) zasahovat do kterékoliv části Modifikací včetně zdrojových kódů, provádět úpravy a změny ve kterékoliv části Modifikací včetně zdrojových kódů, a to jak sám, tak i prostřednictvím třetí osoby, a užívat takto změněné nebo upravené Modifikace jako součásti programového vybavení nebo i samostatně,

   c) rozmnožovat Modifikace, jejich části nebo části programového vybavení nebo dokumentace obsahující Modifikace a užívat tyto rozmnoženiny jako součásti programového vybavení nebo i samostatně,

   d) instalovat Modifikace, jejich části nebo části programového vybavení obsahující Modifikace na více serverů.

2. Objednatel se stane vlastníkem jakéhokoliv hmotného substrátu obsahujícího Modifikace jeho předáním (poskytnutím) poskytovatelem objednateli. Objednatel si vyhrazuje právo zapůjčit Modifikace nebo dokumentaci obsahující Modifikace třetí straně za účelem zajištění údržby, provozu nebo rozvoje programového vybavení nebo za účelem aktualizace dokumentace. Objednatel se dnem předání (poskytnutí) stává vlastníkem zdrojových kódů Modifikací (jsou-li zdrojové kódy předávány).

3. Licence umožňuje užívání Modifikací nebo jejich částí neomezeným počtem pracovníků objednatele a bez omezení počtu současně pracujících uživatelů nebo kategorií uživatelského přístupu.

4. Za den poskytnutí příslušné licence se považuje vždy den, kdy je příslušné plnění poskytnuto objednateli k prvnímu užití.

5. Poskytovatel prohlašuje, že je právo k užívání programového vybavení (licenci) dle tohoto článku objednateli oprávněn poskytnout a že na žádném z plnění dle této smlouvy neváznou žádná práva třetích osob, která by poskytnutí bránila. V případě porušení práv třetích osob chráněných autorským zákonem poskytovatel zajistí na své náklady náhradu

škod uplatněných třetími osobami a nápravu vzniklého stavu tak, aby objednatel mohl programové vybavení oprávněně užívat.

6. Objednatel není licence získané podle této smlouvy povinen užít.
7. Odměna za poskytnutí licencí podle této smlouvy je součástí cen podle čl. VI této smlouvy.

Článek VIII
Pověřené osoby

1. Pověřenými osobami smluvních stran jsou:

   za objednatele:

   [redacted]

   za poskytovatele:

   [redacted]

2. V případě změny v osobě nebo údajích uvedených v odst. 1 tohoto článku je změna účinná dnem doručení e-mailu pověřeným osobám druhé smluvní strany.

Článek IX
Mlčenlivost, bezpečnost a ochrana informací a další povinnosti poskytovatele

1. Poskytovatel se zavazuje zajistit, že jeho pracovníci, jakož i jiné osoby, které se budou podílet na plnění dle této smlouvy, zachovají mlčenlivost o všech skutečnostech, se kterými se po dobu plnění smlouvy seznámí a které nejsou veřejně dostupné. Uvádění dodávky programového vybavení dle této smlouvy poskytovatelem jako referenční zakázky po převzetí programového vybavení objednatelem tímto není dotčeno, vyjma případu, že by objednatel od této smlouvy odstoupil.
2. Závazek mlčenlivosti trvá i po skončení plnění podle této smlouvy.
3. Poskytovatel je v souvislosti s plněním této smlouvy povinen postupovat v souladu s obecnými pravidly v oblasti bezpečnosti IT, které tvoří přílohu č. 4 této smlouvy.
4. Poskytovatel se zavazuje, že plnění dle čl. I bude realizováno osobami, z nichž vždy minimálně jedna bude disponovat alespoň jedním z těchto certifikátů: IMPA (Certified Project Management Association), PMI (Project Management Institute), PMP (Project Management Professional), nebo Prince2 (Projects in Controlled Environments). Požadovaný certifikát musí být platný po celou dobu účinnosti této smlouvy. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na výzvu objednatele tuto skutečnost doložit, a to do 5 pracovních dnů od doručení výzvy.

Článek X
Smluvní pokuty, úrok z prodlení

1. V případě prodlení poskytovatele v kterékoliv lhůtě podle čl. II odst. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 5.000 Kč za každý pracovní den prodlení.
2. V případě, že poskytovatel neposkytne informace ve lhůtě podle čl. IV odst. 2 písm. a) této smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 1.000 Kč za každý takovýto případ porušení smlouvy.
3. V případě, že poskytovatel neposkytne objednateli podporu v souladu s čl. IV odst. 2 písm. b) této smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý takovýto případ, a to i opakovaně až do poskytnutí požadované podpory.
4. V případě prodlení poskytovatele ve lhůtě pro odstranění vady závažnosti 1 nebo 2 podle čl. IV odst. 2 písm. c) je objednatel oprávněn požadovat smluvní pokutu ve výši 100 Kč za každou hodinu prodlení a každou neodstraněnou vadu. V případě prodlení poskytovatele ve lhůtě pro odstranění vady závažnosti 3 podle čl. IV odst. 2 písm. c) je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý pracovní den prodlení a každou neodstraněnou vadu.
5. Odmítá-li poskytovatel poskytovat objednateli podporu podle čl. IV odst. 2 písm. h) nebo i) této smlouvy i přesto, že uplynula objednatelem pro poskytnutí podpory stanovená lhůta, je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý pracovní den prodlení.
6. V případě porušení jakékoliv povinnosti poskytovatele dle čl. IX je objednatel oprávněn požadovat smluvní pokutu ve výši 10 000 Kč za každé jednotlivé porušení.
7. V případě prodlení objednatele s uhrazením daňového dokladu je poskytovatel oprávněn požadovat úrok z prodlení podle předpisů občanského práva.
8. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů od doručení dokladu k úhradě povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
9. Strany se dohodly, že jejich vzájemná odpovědnost za škodu není smluvní pokutou vyloučena.

Článek XI
Trvání smlouvy, ukončení smlouvy, odstoupení od smlouvy

1. Tato smlouva se uzavírá na dobu neurčitou s výpovědní dobou 6 měsíců, která počíná běžet v první den měsíce následujícího po měsíci, v němž byla výpověď doručena druhé smluvní straně.
2. V případě, že některá ze smluvních stran podstatným způsobem poruší smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit.
3. Odstoupení od smlouvy je účinné doručením písemného oznámení o odstoupení druhé smluvní straně.
4. Za podstatné porušení smluvní povinnosti se považuje:

   a) ze strany poskytovatele:

   - prodlení v kterékoliv ze lhůt podle čl. II odst. 1 delší než 20 pracovní dnů;
   - prodlení ve lhůtě pro poskytnutí aktualizace delší než 30 dnů;

- prodlení ve lhůtě pro odstranění vady závažnosti 1 nebo 2 podle čl. IV písm. c) delší než 10 pracovní dnů;
- nesplnění povinností stanovených v čl. IX odst. 4;

b) ze strany objednatele:

- prodlení s úhradou daňového dokladu delší než 30 dnů.

5. Odstoupením od smlouvy nezaniká nárok smluvních stran na smluvní pokuty dle čl. X ani nárok na náhradu škody.

Článek XII
Uveřejnění smlouvy a dalších souvisejících skutečností

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

Článek XIII
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední ze smluvních stran.
2. Smlouvu lze měnit nebo doplňovat pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak.
3. Závazkový vztah založený touto smlouvou se řídí českým právním řádem, zejména o. z. a dále rovněž příslušnými ustanoveními zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
4. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
5. Stane-li se některé ustanovení této smlouvy neplatné či neúčinné, nedotýká se to ostatních ustanovení této smlouvy, která zůstávají platná a účinná. Smluvní strany se v tomto případě zavazují dohodou nahradit ustanovení neplatné/neúčinné novým ustanovením platným/účinným, které nejlépe odpovídá původně zamýšlenému účelu ustanovení neplatného/neúčinného. Do té doby platí odpovídající úprava obecně závazných právních předpisů České republiky.
6. Smlouva je vyhotovena ve třech vyhotoveních s platností originálu, z nichž objednatel obdrží dvě a poskytovatel jedno vyhotovení.

Přílohy:

č. 1 – Požadavky na programové vybavení
č. 2 – Systémové prostředí ČNB
č. 3 – Metodický list stanovující požadavky na kryptografické prostředky využívané v IS a systémovém prostředí ČNB
č. 4 - Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

V Praze dne: 25. 9. 2019

Za objednatele:

[redacted]

Ing. Milan Zirnsák
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní

[redacted]

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

V PRAZE dne: 25. 9. 2019

Za poskytovatele:

[redacted]

Mgr. Petr Dvořák
CEO a jednatel

Příloha č. 1

Požadavky na programové vybavení

1. Obecné funkční požadavky na API

a) Vystavení API dle standardu ČOBS

Veškerá API, které budou konzumovat TPP, budou založeny na standardu ČOBS min. verze 3.0 platné od 1.1.2019.

b) Autentizace a autorizace

Dodání autentizační a autorizační služby, která bude zajišťovat komunikaci mezi TPP a systémy ČNB v rámci procesu autentizace uživatele přistupujícího přes aplikaci TPP

c) Registr souhlasů udělených třetím stranám

Dodávaný systém musí zajistit funkčnost, pokrývající ukládání a správu consentů, které udělí uživatelé aplikacím TPP. Dále také musí zajistit vystavení rozhraní pro získání seznamu consentů pro potřeby zobrazení v rámci ČNB IBS.

d) Registr třetích stran

Poptávaný systém musí zajistit funkčnost, pokrývající ukládání a správu ověřených TPP, přes jejichž aplikace mohou uživatelé ČNB IBS přistupovat ke svým datům, která mají dostupná v ČNB IBS.

e) On-line dokumentaci

Poptávaný systém pro PSD2 musí zajistit funkčnost, pokrývající vystavení dokumentace potřebné pro TPP k implementaci integrace na PSD2 API ČNB. Součástí developers portálu musí být i vystavená testovacích API, přes která si budou moci vývojáři ze strany TPP vyzkoušet provolání těchto API za účelem ověření funkčnosti jejich implementace integrace na PSD2 API.

f) Test GUI application

V rámci dodávky systému je nutné zajistit dodání testovací aplikace (simulace TPP) pro potřeby provedení testů v ČNB test prostředí. Tato aplikace musí obsahovat GUI část, aby bylo možné jednoduše testovat a sledovat výsledky testů.

g) Návrh PL/SQL API pro integraci se systémy ČNB

2. Povinné funkční požadavky na API

ID	Název	Popis požadavku
W-1	Webová služba	Webová služba vystavená pro přístup třetích stran.
A-1	Autentizace TPP uživatele	Procedura zajišťující autentizaci TPP uživatele který přichází z aplikace TPP
A-2	Registrace TPP	Procedura zajišťující registraci TPP
A-3	Informace o registračních údajích TPP	Procedura vrací registrační údaje TPP
A-4	Změna registračních údajů TPP	Procedura mění registrační údaje TPP
A-5	Výmaz registračních údajů TPP	Procedura maže registrační údaje TPP
A-6	Žádost o nový CLIENT_SECRET	Procedura generuje nový client_secret (registrační token)
A-7	Získání refresh a access tokenu	Procedura pro získání refresh a acces token TPP
A-8	Obnova ACC tokenu	Procedura pro obnovu acces tokenu
A-9	Zneplatnění tokenu	Procedura pro zneplatnění exitujícího acces nebo refresh tokenu
A-11	Autentizační logon stránka disponenta ABO-K pro TPP	Autentizační logon stránka kam bude přesměrována uživatel z aplikace TPP pro potřeby provedení autentizace klienta ABO-K. Stránka umožní autentizaci buď pomocí certifikátu, nebo pomocí jména, hesla a autentizační SMS

A-13	Seznam_Uctu	Procedura pro získání seznamu účtů klienta
A-14	Zustatek_Uctu	Procedura pro získání zůstatku účtu
A-15	Prehled_Transakci	Procedura pro získání historii transakcí od konkrétního účtu
A-16	Dostatek_prostredku	Procedura pro ověření dostatku prostředků na účtu klienta
A-17	Nova_platba	Procedura pro vložení nové platby
A-18	Info_zal_platba	Procedura – informace o založené platbě
A-19	Stav_platby	Procedura – informace o stavu platby
A-20	smaz_platbu	Procedura pro smazání neautorizované platby
A-21	Gen_aut_id	Procedura pro generování autorizačního ID a scénářů
A-22	Detail_aut_platby	Procedura pro zjištění stavu autorizace platby
A-23	Aut_platby	Procedura pro ověření podpisu a SMS
A-24	Autorizační stránka	Autorizační stránka pro autorizaci plateb: pomocí hesla a autorizačního SMS kódu, nebo pomocí elektronického podpisu a autorizačního SMS kódu
A-27	Testovací aplikace TPP	Testovací aplikace TPP, ze které bude možné provést otestování API

A-29	Stránka pro udělení souhlasu uživatele ABO-K	Stránka pro udělení souhlasu uživatele ABO-K pro aplikaci TPP

3. Specifické požadavky na API

ID	Název	Popis požadavku
B-1	Ověřování certifikátů	Musí být zajištěna možnost ověření certifikátů TPP napříč EU.
B-2	Integrita	Data v API budou zabezpečena elektronickým podpisem klientů ČNB.
B-3	Generování tokenů	Musí být zajištěn bezpečný způsob generování access a refresh tokenů.
B-4	Dostupnost	API musí být dostupné 7/24, stejně jako webové služby ABO-K.
B-5	Výkonnost	Předpokládaný objem transakcí je 1000 denně. Předpokládaný počet dotazů na data klientů ABO-K je 2000 denně.
B-6	Časová odezva	Časová odezva musí být max 1 vteřina

4. Bezpečnostní požadavky

ID	Název	Popis
BEZ001	Záložní lokalita	Systém je provozován ve dvou lokalitách v takovém režimu, že při zničení provozní lokality je možné obnovit provoz v záložní lokalitě do 8 hodin se ztrátou dat maximálně za posledních 24 hodin.
BEZ002	Oddělená prostředí	Řešení zahrnuje testovací a provozní prostředí. Přenos změn (kódu) mezi prostředími je řízen.
BEZ003	Odolnost proti známým hrozbám	IS musí být odolný proti známým hrozbám (SQL Injection, cross site scripting apod.). Systém neobsahuje zejména zranitelnosti dle seznamů OWASP Top 10 a CWE/SANS top 25.
BEZ004	Žádná hesla v kódu	Citlivé údaje (sdílená tajemství apod.) nejsou součástí kódu aplikace.
BEZ005	Žádný trvalý přístup	K žádné části systému není možné získat přístup s využitím autentizačních informací (hesel, kryptografických klíčů apod.), které není možné změnit. Tj. systém neobsahuje „hardcoded" hesla, „maintenance backdoor" apod.
BEZ006	Servisní přístup jen z ČNB	K funkcím pro správu, změny, diagnostiku apod. systému je přístup pouze ze sítě ČNB (příp. prostřednictvím běžného vzdáleného přístupu

		pracovníků ČNB do této sítě.) Dodavatelé nemají ze svých sítí přístup k systému. Systém může stahovat aktualizace z určených serverů.
BEZ007	Zabezpečení komunikace	Přenosy dat mezi stanicemi uživatelů a správců a dalšími částmi systému (servery) v síti objednatele i mimo ni jsou chráněny kryptografickými technikami proti odposlechu (důvěrnost) a modifikaci (integrita), například pomocí TLS. Přenosy dat mimo vnitřní síť objednatele jsou chráněny kryptografickými technikami proti odposlechu (důvěrnost) a modifikaci (integrita).
BEZ008	Audit bezpečnosti	Systém zaznamenává do logů významné administrátorské zásahy a všechny bezpečnostně významné události v rozsahu dle metodického listu Logování, například: - změnu přiřazených přístupových práv (rolí a kompetencí), - vytvoření nebo smazání (zablokování) uživatele/aplikačního účtu mimo AD, Změna rozsahu zaznamenávaných údajů je vždy zaznamenána.
BEZ009	Zajištění logů	Záznamy a auditní logy jsou chráněny proti jakékoliv neautorizované modifikaci a smazání na aplikační a infrastrukturní úrovni.
BEZ010	Připojení k monitoringu	Systém je zařazen do provozního a bezpečnostního dohledu IS ČNB a poskytuje příslušným systémům včetně SIEM potřebná data.
BEZ011	Synchronizace času	Čas na všech komponentách systému mimo stanic uživatelů je synchronizován se zdrojem přesného času v síti ČNB (pro zajištění správného vyhodnocení auditních záznamů).
BEZ012	Pouze bezpečná kryptografie	Jsou používány pouze kryptografické protokoly považované aktuálně za bezpečné, především nejsou používány protokoly SSL a TLS 1.0. Dále jsou splněny požadavky metodického listu kryptografie (Metodický list stanovující požadavky na kryptografické prostředky využívané v IS a systémovém prostředí ČNB, viz příloha č. 3 smlouvy).
BEZ013	Anonymizace předávaných dat	Pokud budou data k testu předávána mimo systémové prostředí ČNB, musí být anonymizovaná tak, že z nich není možné identifikovat klienta nebo disponenta (ani identifikátorem aplikace ABO) ani získat čísla účtů či jiné citlivé informace.
BEZ014	Archivace dat	Systém umožňuje archivovat data (přesunout a smazat z provozní databáze) bez odstávky systému, a to po dobu 10 ti let.
BEZ015	Postupy obnovy	Součástí dodané dokumentace jsou postupy obnovy systému po havárii.

BEZ016	Bezpečný vývoj	Systém je vyvíjen dle principů bezpečného vývoje stanoveným patřičným metodickým listem. Při externím vývoji jsou tyto požadavky přeneseny do zadávací dokumentace.
BEZ017	Řízení přístupu ke zdrojovým kódům programů	Ke zdrojovému kódu přistupují pouze schválení uživatelé.
BEZ018	Správa klíčů	Kryptografické klíče jsou generované, vydávané, spravované a ničené podle metodického listu kryptografie.
BEZ019	Ochrana transakcí aplikačních služeb	Transakce jsou chráněny před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
BEZ020	Kontrola integrity	Integrita softwarových balíčků dodaných dodavatelem musí být před instalací ověřena.
BEZ021	Ochrana dat pro testování	Testování je běžně prováděno s daty, která neobsahují údaje skutečných osob a organizací, tj. byla náhodně vygenerována nebo vytvořena anonymizací z reálných dat. Testování, u kterého je nezbytné použít data s údaji o skutečných osobách nebo transakcích, je prováděno v prostředí zabezpečeném shodně s provozním prostředím, včetně rozsahu přístupových práv, a pouze po předem stanovenou dobu, po které jsou data bezpečně vymazána.
BEZ022	Bezpečnostní požadavky v dohodách s dodavateli	Bezpečnostní požadavky jsou určeny na základě analýzy rizik dodávky a jsou součástí smlouvy o úrovni služeb.
BEZ023	Autentizace/Autorizace	Systém umožňuje uživateli provádět operace a přistupovat k datům až po autentizaci a autorizaci na základě přidělené role. Autentizace musí zůstat dvoufaktorová.
BEZ024	Tokeny	Všechny autorizační kódy/tokeny musí být generovány vhodnými a ověřenými algoritmy.

Příloha č. 2

SYSTÉMOVÉ PROSTŘEDÍ ČNB

Standardní systémové prostředí je soubor konkrétních produktů technického a programového vybavení včetně pravidel pro jejich provoz a dále seznam definovaných služeb, které souhrnně tvoří základní platformu pro provoz informačních systémů a informačních technologií (IS/IT) v prostředí České národní banky (ČNB).

Prostředí datové sítě

- Klientské stanice připojeny rychlostí typicky 100 $Mbsec^{-1}$ 100Base-T
- Servery připojeny typicky rychlostí 1 Gb 1000Base-T
- Mezi servery a klientskými stanicemi pouze L3 konektivita, mezi servery možná L2 nebo L3 konektivita
- Adresace dle RFC 1918 (10.x.y.z)
- Plně přepínaná síť s redundantním jádrem

Serverové prostředí

- Platforma architektury x86 - MS Windows Server 2008R2 Server, cp 1250
- Platforma Red Hat Linux v. 6.5 jako alternativní prostředí
- Platforma VMware vSphere 5.1
- Platforma Oracle VM 3.0.3

Centrální diskové kapacity

Slouží pro ukládání dat spravovaných databázovými systémy, pro sdílení programového vybavení a dat organizačních útvarů ČNB, poskytují prostor pro uložení dat jednotlivých uživatelů.

Jsou využita fault tolerantní disková pole, zálohování dat centrálních diskových kapacit je zajištěno.

Zálohování dat

Zálohování informačních systémů a dalších dat je v ČNB řešeno centrálně. Zálohována jsou pouze data uložená na centrálních kapacitách ve správě sekce informatiky. Pro zálohování je určen zálohovací systém HP Data Protektor 7.0 nebo vyšší.

Elektronická pošta

- Server elektronické pošty - MS Exchange 2010
- Klient elektronické pošty – MS Outlook 2010 nebo OWA

Tisková zařízení

- Síťová tisková zařízení,

- Komunikační protokol – TCP/IP,
- Podporované síťové služby – SNMP, DHCP, DNS.

Databázové servery

Data standardních IS jsou uložena v databázích Oracle:

- Oracle RDBMS 11g
- Protokol Oracle Net

Zálohování dat provozních databází je zajištěno stanovenými prostředky a postupy.

Aplikační a WWW servery

- Oracle Web Logic Server 11,
- JBoss,
- Microsoft IIS 6.0 a vyšší.

Monitoring systémů

- System Center Operations Manager 2007, 2012 R2 – centrální sběr logů
- QUALYS – monitoring zranitelností

Prostředí klientské stanice

Klientská stanice uživatele je osobní počítač IBM-PC kompatibilní koncipovaný jako nástroj zajišťující přístup uživatele k centrálně provozovaným IS nebo virtualizovaný desktop (dále jen vDesktop) pomocí technologie Citrix. Minimální parametry klientské stanice provozované ve standardním systémovém prostředí ČNB:

- MS Windows 7 Professional , cp 1250, Service Pack 1 (operační systém) + aktuální aktualizace
- Citrix XenApp 6.5 na MS Windows 2008 Serveru R2 (virtuální desktop využívající MS terminálové služby)
- TCP/IP síťové služby (DHCP klient, SNMP klient)
- MS Office 2010 Professional Plus CZ + Service Pack 2MS Internet Explorer 9.0 CZ (aktuální SP)
- Adobe Acrobat Reader 10 CZ – prohlížeč souborů ve formátu PDF
- Symantec EndPoint Protection v.12.1 - antivirový program

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

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

Dávkové zpracování centrálně uložených dat je přípustné spouštět a provádět pouze na databázovém serveru nebo případně na aplikačním serveru.

Uživatel nebo aplikace mohou ukládat na klientskou stanici dočasná data a programové komponenty, které jsou odvozeny z centrálně uložených dat, mohou také provádět lokální zpracování dat. Pro případné vytváření dočasných souborů a ukládání dat při činnosti komponent je třeba využívat předdefinované adresáře dostupné přes proměnné prostředí (USERPROFILE, TEMP, TMP, APPDATA). V případě vDesktop jsou data na lokálním disku po restartu serveru smazána.

Přístupová práva na klientských stanicích a vDesktop odpovídají defaultnímu nastavení od firmy Microsoft po instalaci MS Windows 7 Professional (v případě vDesktop se jedná o Win 2008R2). Výjimky pro potřeby aplikací je v nezbytných případech možné povolit po přesném definování potřebných změn v adresářích a v registrech a po náležitém zdůvodnění požadovaných změn. Výjimky jsou centrálně řízeny a aplikovány na klientské stanice a vDesktop prostřednictvím GPO (politiky v Active Directory). Obdobné požadavky platí i pro registrování knihoven a vytváření nebo změny hodnot klíčů v registrech.

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

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

Funkce Single Sign-On

U IS ČNB je požadována realizace funkce Single Sign-On s využitím služby MS AD (autentizační protokol Kerberos).

Vazby na další IS

Napojení úlohy na informace z primárních zdrojů dat je standardně zajištěno prostřednictvím databázových pohledů na příslušné tabulky přes synonyma dostupná v databázi Oracle.

Bezpečnost IT

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

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

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

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

Příloha č. 3

Metodický list stanovující požadavky na kryptografické prostředky využívané v IS a systémovém prostředí ČNB

Článek 1

Certifikáty a související klíče musí být uloženy na hardwarovém prostředku s odpovídající certifikací minimálně na úrovni FIPS 140-2 Level 2. V případech, kdy není možné certifikát a související klíče uložit na hardwarový prostředek, musí být jejich ochrana realizována prostřednictvím dostatečně silného hesla.

Článek 2
Symetrické algoritmy

1) Blokové a proudové šifry pro ochranu důvěrnosti a integrity:

a) Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů,

b) Triple Data Encryption Standard (3DES) s využitím délky klíčů 168 bitů, omezené použití jen se zatížením klíče menším než 10 GB, postupně přecházet na AES,

c) Triple Data Encryption Standard (3DES) s využitím délky klíčů 112, bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu,

d) Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB,

e) Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB,

f) Twofish s využitím délky klíčů 128 až 256 bitů,

g) Serpent s využitím délky klíčů 128, 192, 256 bitů,

h) Camellia s využitím délky klíčů 128, 192 a 256 bitů,

i) SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů.

2) Módy šifrování s ochranou integrity:

a) CCM,

b) EAX,

c) OCB,

d) Složená schémata typu "Encrypt-then-MAC". Tato schémata musí používat k šifrování pouze uvedené šifrovací módy a k výpočtu MAC pouze uvedené módy pro ochranu integrity.

3) Módy šifrování:

a) CTR,

b) OFB,

c) CBC,

d) CFB,

4) Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným inicializačním vektorem, při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru, při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače, v případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

5) Módy pro ochranu integrity:

a) HMAC,

b) CBC-MAC-X9.19, omezené použití jen se zatížením menším než 109 MAC,

c) CBC-MAC-EMAC,

d) CMAC.

Článek 3
Asymetrické algoritmy

1) Pro technologii digitálního podpisu:

a) Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů a více, délky parametru cyklické podgrupy 224 bitů a více.

b) Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů a více.

c) Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů a více.

2) Pro procesy dohod na klíči a šifrování klíčů:

a) Diffie-Hellman (DH) s využitím délky klíčů 2048 bitů a více, délky parametru cyklické podgrupy 224 bitů a více.

b) Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů a více.

c) Elliptic Curve Integrated Encryption System - Key Encapsulation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více.

d) Provably Secure Elliptic Curve - Key Encapsulation Mechanism (PSECKEM) s využitím délky klíčů 256 bitů více.

e) Asymetric Ciphers and Key Encapsulation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více.

f) Rivest Shamir Adleman - Optimal Asymetric Encryption Padding (RSAOAEP) s využitím délky klíčů 2048 a více.

g) Rivest Shamir Adleman - Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 2048 a více.

Článek 4
Algoritmy hash funkcí

1) SHA-2

a) SHA-224,

b) SHA-256,

c) SHA-384,

d) SHA-512,

e) SHA-512/224,

f) SHA-512/256.

2) SHA-3

a) SHA3-224,

b) SHA3-256,

c) SHA3-384,

d) SHA3-512,

e) SHAKE-128,

f) SHAKE-256.

3) Ostatní hašovací funkce:

a) Whirpool,

b) RIPEMD-160,

c) SHA 1 s omezeným použitím:

i. SHA-1 se nesmí používat pro generování nových digitálních podpisů, časových razítek, jakékoliv jiné aplikace vyžadující nekolizní SHA-1.

ii. SHA-1 lze používat pouze pro ověřování již existujících digitálních podpisů a časových razítek, generování a ověřování HMAC-SHA1, funkce pro odvozování klíčů a pseudonáhodné generátory.

Článek 5
Nastavení algoritmů

1) Nastavení algoritmů daného konkrétního protokolu musí být v souladu s minimálními požadavky na kryptografické algoritmy:

2) Pro zabezpečení webových spojení se použije protokol TLS 1.1 nebo vyšší, přičemž preferován je protokol TLS 1.2.

3) V případě bezdrátové komunikace je minimálním vyhovujícím protokolem WPA2 s enterprise autentizací 802.1X. V případech povolených jako výjimka nebo akceptovaných jako riziko lze použít PSK.

Příloha č. 4

Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu smlouvy nebo zadávací dokumentace nebo její jiná příloha.
2) Dodavatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
3) Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
4) Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
6) Dodavatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Dodavatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro dodavatele, jejichž předmět smlouvy obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit, a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku.

8) Pracovníci dodavatele nesmí:

   a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);

   b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).

9) Pracovníci dodavatele nejsou oprávněni:

   a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;

   b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;

   c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).

10) Dodavatel a jeho pracovníci nejsou oprávněni:

   a) nepovoleně používat, kopírovat a šířit software, jako např.:

      i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);

      ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy obsahuje tuto činnost;

      iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí

         (1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a

         (2) v případech, kdy předmět smlouvy obsahuje tuto činnost;

   b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;

   c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

11) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.

12) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

3) Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).