SMLOUVA
o realizaci rozšíření bezpečného úložiště klíčů pro QSCD mód a úprav souvisejícího HW a SW včetně poskytování provozní podpory

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

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milan Zimsák, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450
(dále jen „objednatel")

a

SEFIRA spol. s r.o.
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572
se sídlem: Antala Staška 2027/77, 140 00 Praha 4
IČO: 62907760
DIČ: CZ62907760
zastoupenou: Ing. Petrem Dolejším, jednatelem
a
Ing. Danielem Marešem, jednatelem
č. účtu: 107-8809470257/0100 *(účet je zveřejněn podle § 98 zákona o DPH)*
(dále jen „zhotovitel")

Preambule

Objednatel provozuje ve svém standardním systémovém prostředí moduly pro bezpečné uchovávání klíčů (tzv. „HSM moduly" /Hardware Security Module"/). V souvislosti s Nařízením Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru na vnitřním trhu známém pod jménem eIDAS, a v souvislosti se zákonem č. 297 ze dne 24. srpna 2016, o službách vytvářejících důvěru pro elektronické transakce objednatel hodlá předmětné HSM moduly a související software upravit tak, aby tyto HSM moduly vyhovovaly definici pro tzv. „QSCD" zařízení, tj. „Qualified Seal Creation Device" a bylo je tak možno použít pro poskytování služby „kvalifikované pečeti".

HSM moduly a související software podporují kritické činnosti objednatele.

Článek I.
Předmět smlouvy

1. Předmětem této smlouvy je povinnost zhotovitele:

   a) upravit v současné době objednatelem provozované technické a programové prostředky HSM modulů, případně dodat, nainstalovat a zprovoznit další technické a programové prostředky nezbytné pro jejich správné fungování tak, aby nyní objednatelem provozované HSM moduly splňovaly po implementaci požadavky na QSCD zařízení tak, aby na ně pak bylo možno kvalifikovaným poskytovatelem služeb vytvářejících

[redacted]

důvěru vydat certifikát, který bude použit pro vnitřní službu kvalifikované pečeti ve standardním systémovém prostředí objednatele;

b) pro účely a po dobu testování před vlastní implementací řešení vytvořit ověřovací testovací prostředí na bázi HSM modulu(ů) shodné konfigurace, jako nyní provozuje objednatel (Thales nShield Connect 1500+); (viz též odstavec 3 písm. b)),

c) vypracovat projektovou dokumentaci skutečného stavu implementace a úprav HSM modulů a navazujícího software,

d) zaškolit zaměstnance objednatele,

(dále také jako „dílo")

2. Dílo musí splňovat funkční požadavky uvedené v příloze č. 4 smlouvy. Dílo musí být realizováno v souladu s návrhem technického řešení obsaženým v příloze č. 6.

3. Dílo bude realizováno v následujících etapách:

a) **První etapa** zahrnuje vypracování realizační studie zhotovitelem, dle vzoru realizační studie uvedeném příloze č. 8, která bude obsahovat veškeré informace nezbytné pro implementaci nově dodaných technických a programových prostředků do prostředí objednatele, postup úprav a migrace současných HSM modulů objednatele do režimu QSCD včetně mapování funkčních požadavků a vlastností uvedených v příloze č. 4 tak, aby byla prokázána jejich realizovatelnost, a dále pak popis režimu provozní podpory.

b) **Druhá etapa** zahrnuje:

- dodávku technických a programových prostředků podle specifikace uvedené v příloze č. 1 a v souladu s akceptovanou realizační studií (viz 1. etapa),
  1. instalaci těchto nových prostředků a jejich implementaci do prostředí objednatele zhotovitelem,
  2. revize konfigurace a úpravy u stávajících HSM modulů objednatele,
  3. zprovoznění režimu vysoké dostupnosti všech HSM modulů podle návodu a dokumentace poskytnuté zhotovitelem,
  4. konfiguraci HSM modulů pro připojení definovaných serverů objednatele, které nyní využívají HSM moduly pro služby pečetění – realizují pracovníci zhotovitele za asistence pracovníků objednatele,
  5. instalaci a úpravy programových prostředků na těchto serverech – realizují pracovníci objednatele podle návodu či dokumentace poskytnuté zhotovitelem a za jeho asistence v místě plnění,
  6. instalaci a úpravu SW pro management dodaných technických prostředků – realizují pracovníci objednatele podle návodu či dokumentace poskytnuté zhotovitelem a za jeho asistence v místě plnění.
- vytvoření dedikovaného testovacího prostředí na zhotovitelem zajištěném/zapůjčeném HSM modulu v QSCD režimu pro testovací provoz v délce nejméně 2 týdnů zahrnující posouzení souladu navrhovaného řešení se zadáním podle testovacích scénářů, ukázky základních operací s HSM v QSCD režimu a zaškolení obsluhy (2 odborných zaměstnanců objednatele) v délce, kterou určí zhotovitel tak, aby zaměstnanci byli zaškoleni v rozsahu dle přílohy č. 2. Na toto testovací prostředí HSM modulů budou napojeny vybrané informační systémy

objednatele, resp. taktéž jejich testovací verze (testovat se budou vždy zástupci technologie používané na serverech, tj. CA, Java a PKCS11).

Součástí plnění v této etapě je i dodání či zpřístupnění dokumentace výrobce technických prostředků a programových prostředků.

c) **Třetí etapa** zahrnuje:

- migraci provozního prostředí stávajících a případně nově dodaných technických a programových prostředků (viz předchozí etapa) tak, aby došlo k vytvoření provozního prostředí HSM modulů v QSCD režimu a v konfiguraci pro jejich vysokou dostupnost, asistence při provedení instalace a úpravách programového vybavení na ostatní aplikační servery dle přílohy č. 3 a migraci dat dle přílohy č. 2 pro stávající aplikace objednatele. Příslušné činnosti zajišťuje zhotovitel za asistence a součinnosti pracovníků objednatele;
- etapa dále zahrnuje zajištění nových certifikátů pro kvalifikovanou pečeť – budou realizovat pracovníci objednatele za asistence zhotovitele v místě plnění.

Po kompletní konfiguraci napojení stávajících informačních systémů objednatele na upravené HSM moduly bude proveden zkušební provoz v délce 2 týdnů, během kterého bude ověřeno, zda dodané řešení splňuje veškeré požadavky objednatele uvedené v příloze č. 4, a bude provedeno měření významných provozních stavů dodaného řešení a případně návrh optimalizace.

d) **Čtvrtá etapa** zahrnuje vypracování projektové dokumentace, v níž bude zachycen popis skutečného stavu implementace HSM modulů do QSCD režimu a provozních postupů a jejíž součástí bude i aktualizace současného havarijního plánu. Seznam požadované dokumentace je uveden v příloze č. 2. Zhotovitel je povinen předat objednateli projektovou dokumentaci v elektronické podobě ve formátu MS Word 2010 a vyšší (případně PDF), včetně dokumentace všech verzí software, resp. firmware.

4. Činnosti uvedené výše u jednotlivých etap jsou podrobněji také popsány v příloze č. 4.
5. Zhotovitel se zavazuje poskytovat pro stávající i nově dodané technické a programové prostředky provozní podporu dle čl. V této smlouvy.
6. Zhotovitel prohlašuje, že dodané technické prostředky budou nové a nepoužité (maximálně z továrny zahořelé z výroby), popř. zapnuté pro ověření funkčnosti v rámci případné kompletace prostředků zhotovitelem před dodáním.
7. Dílo bude prováděno v pracovní dny v době od 8.00 hod. do 17.00 hod., nedohodnou-li se smluvní strany jinak.
8. Místem plnění budou prostory výpočetního střediska v objektech objednatele na adrese:
    - Praha 1, Senovážná ul. 3,
    - Praha 5, Strojírenská 175.
9. K technickým ani programovým prostředkům nebude poskytován vzdálený přístup.
10. Objednatel se zavazuje za poskytnutá plnění uhradit ceny dle čl. III této smlouvy.

Článek II.
Lhůty, způsob předání díla

1. Objednatel převezme dílo jako celek pouze tehdy, pokud:
   - byly odsouhlaseny všechny dílčí etapy na základě akceptačních protokolů, jak je stanoveno dále v tomto článku, a případné vady byly odstraněny,
   - zhotovitel dodal kompletní řešení prosté vad a včetně požadované dokumentace,
   - zhotovitel poskytl veškeré potřebné licence pro provoz řešení,
   - zhotovitel předal v elektronické podobě na sjednaném datovém médiu (např. CD, DVD, USB Flash disk) veškeré podklady a dokumenty potřebné ke správě a údržbě díla.

   Převzetí díla jako celku bude uskutečněno podpisem závěrečného akceptačního protokolu. Tím bude plnění předáno objednateli k běžnému provoznímu využití. Ukončení každé etapy stvrdí pověřené osoby smluvních stran podpisem dílčího akceptačního protokolu.
2. Smluvní strany vzájemně dohodly pro jednotlivé etapy dle čl. I odst. 2 této smlouvy následující lhůty:
   a) zhotovitel předá objednateli realizační studii do 10 týdnů od podpisu smlouvy. Tato doba zahrnuje i připomínková kola objednatele v délce nejvýše 1 týden pro každé připomínkové kolo (očekávají se nejméně 2 připomínková kola);
   b) druhá etapa bude ukončena nejpozději do 15 týdnů od podpisu smlouvy. Termíny zaškolení odborných zaměstnanců objednatele dohodnou smluvní strany podle realizační studie, zaškolení musí proběhnout po instalaci a konfiguraci. Testovací provoz v délce 2 týdnů bude realizován jako poslední činnost druhé etapy;
   c) třetí etapa bude zhotovitelem dokončena nejpozději do 22 týdnů od podpisu smlouvy. Zkušební provoz v délce 2 týdnů bude probíhat po kompletní konfiguraci a migraci. V posledním týdnu zkušebního provozu bude provedeno vyhodnocení, na jehož základě zhotovitel vypracuje návrh případné optimalizace;
   d) čtvrtá etapa zahrnující dokumentaci specifikovanou v příloze č. 2 bude končena do 25 týdnů od podpisu smlouvy. Tato doba zahrnuje i připomínková kola objednatele v délce nejvýše 2 týdnů pro každé připomínkové kolo (očekávají se nejméně 2 připomínková kola).
3. Každá etapa bude považována za ukončenou pouze tehdy, pokud bude plnění prosté vad, nerozhodne-li se objednatel přijmout předmět akceptace s výhradami. V takovém případě budou jednotlivé výhrady zaznamenány v akceptačním protokolu a zhotovitel je oprávněn pokračovat v navazující etapě. Pokud objednatel přijme předmět akceptace s výhradami, musí být vady odstraněny do termínu uvedeného v akceptačním protokolu.
4. Akceptaci s výhradami nelze provést, pokud existuje alespoň 1 podstatná vada implementovaného díla. Podstatné vady implementovaného díla jsou vady, které způsobují tak závažné problémy, že objednatel nemůže dílo nebo jeho klíčovou část používat, ovládat nebo konfigurovat. Zhotovitel není oprávněn pokračovat v navazující etapě, dokud nebudou vady odstraněny a objednatel předmět prací neodsouhlasí bez výhrad.
5. K akceptačnímu protokolu vyhotovenému objednatelem vyjádří zhotovitel své stanovisko vždy nejpozději do 5 pracovních dnů od jeho obdržení. Pokud tak neučiní, má se za to, že s uvedeným závěrem souhlasí.

6. Objednatel se zavazuje umožnit zhotoviteli vykládku a úschovu technických prostředků v prostorách objednatele určených k instalaci v termínu, o kterém bude zhotovitelem zpraven nejméně tři pracovní dny předem.
7. Objednatel převezme technické prostředky do úschovy a zajistí jejich bezpečné uskladnění do zahájení instalace.

Článek III.
Cena plnění a platební podmínky

1. Ceny plnění uvedené v odst. 2 až 4 tohoto článku byly stanoveny dohodou smluvních stran v úrovni bez DPH a zahrnují veškeré náklady zhotovitele spojené s plněním podle této smlouvy.
2. Cena díla činí celkem 504 500 Kč, z toho cena zaškolení dle čl. I odst. 1 písm. d) činí 16 000 Kč. Podrobnější rozpis ceny je obsažen v příloze č. 7 smlouvy.
3. Cena za plnění na výzvu podle čl. V odst. 4 této smlouvy bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby, která činí 2 000 Kč bez DPH. K této ceně bude připočtena cena za výjezd (cena zahrnuje náklady na cestu tam a zpět a ztrátu času na cestě), která činí bez DPH 2 000 Kč.
4. Paušální cena za podporu technických a programových prostředků podle čl. V této smlouvy činí měsíčně 44 100 Kč.
5. Ceny zahrnují veškeré náklady zhotovitele na realizaci předmětu plnění. K cenám bude účtována DPH v sazbě platné v den uskutečnění příslušného zdanitelného plnění.
6. Cena díla bude hrazena takto:
   i. Zhotovitel je oprávněn vystavit doklad na úhradu 1. zálohy ve výši 10 % z ceny díla dle čl. III odst. 2 této smlouvy nejdříve v den podpisu dílčího akceptačního protokolu za 1. etapu;
   ii. Zhotovitel je oprávněn vystavit doklad na úhradu 2. zálohy ve výši 25 % z ceny díla dle čl. III odst. 2 této smlouvy nejdříve v den podpisu dílčího akceptačního protokolu za 2. etapu;
   iii. Daňový doklad na cenu celého díla je zhotovitel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu o předání a převzetí díla;
   iv. V daňovém dokladu na cenu celého díla budou vyúčtovány poskytnuté zálohy.
7. Cena za plnění na výzvu podle odst. 3 tohoto článku bude hrazena na základě daňového dokladu vystaveného nejdříve po poskytnutí služby. Přílohou daňového dokladu bude i objednatelem odsouhlasený výkaz práce.
8. Paušální cena podle odst. 4 tohoto článku bude hrazena měsíčně na základě daňového dokladu vystaveného nejdříve ke dni uskutečnění zdanitelného plnění, kterým je poslední den měsíce, ve kterém bylo příslušné plnění poskytováno. Paušální cena podpory zahrnuje veškeré náklady (včetně náhradních dílů, práce, dopravného apod.) zhotovitele spojené s jejím poskytováním.
9. Doklady k úhradě (faktury) budou obsahovat údaje podle § 435 občanského zákoníku, evidenční číslo smlouvy ČNB a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován zhotovitelem (dále jen „určený účet"). Daňový doklad bude nadto obsahovat náležitostí stanovené v zákoně o dani z přidané hodnoty. V případě, že doklad k úhradě bude postrádat některou ze stanovených

náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit zhotoviteli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu k úhradě.

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

11. Daňové doklady bude zhotovitel zasílat elektronicky na adresu faktury@cnb.cz, přičemž doklad 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 daňový doklad zaslat elektronicky, zašle zhotovitel daňový doklad v analogové formě na adresu objednatele:

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

12. Splatnost dokladů k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch zhotovitele.

13. Výše paušální ceny za období kratší, než je sjednané období, se vypočte jako alikvotní část sjednané ceny.

14. Ke konci kalendářního roku, nejdéle však do 31. 12., je zhotovitel povinen sdělit objednateli písemně, jakou část z uhrazené roční ceny za podporu programových prostředků tvoří cena nových verzí představující jejich technické zhodnocení.

15. Zhotovitel je oprávněn navrhnout změnu hodinové sazby dle odst. 3 a paušální ceny dle odst. 4 tohoto článku v návaznosti na vývoj indexu cen tržních služeb, stejné období předchozího roku = 100, konkrétně index „Tržní služby celkem" sloupec „Průměr od počátku roku", a to průměr za předchozí kalendářní rok, který vyhlašuje Český statistický úřad. Ceny mohou být zvýšeny maximálně o částku odpovídající předmětné roční inflaci. Úprava ceny bude provedena formou dodatku ke smlouvě a nabývá účinnosti dnem účinnosti dodatku. První úpravu cen může zhotovitel navrhnout po uplynutí dvou let od zahájení poskytování podpory.

16. Smluvní strany se 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.

Článek IV.
Další povinnosti smluvních stran, pověření zaměstnanci

1. Objednatel se zavazuje vytvořit zhotoviteli k instalaci potřebné podmínky, zejména:
    a) zajistit provozní odstávky aplikací dotčených migrací dat s tím, že v rámci geografického clusteru je v pracovní době možná odstávka vždy jen jednoho serveru clusteru. Odstávky celého clusteru je možné provádět jen během víkendu. Takovou odstávku je nutné avizovat nejméně 10 pracovních dnů předem. Maximální přípustné doby provozních odstávek jsou uvedeny v příloze č. 4, část Provozní odstávky;

b) zajistit potřebné rekonfigurace technických a programových systémů dotčených přechodem na dodávané prostředky za podmínky, že neohrozí stávající provoz;

c) přidělit IP adresy pro dodávané prostředky;

d) zajistit přístup odborných zaměstnanců zhotovitele na příslušná pracoviště objednatele.

2. Pověřenými zaměstnanci pro:

a. technická jednání a k předání a převzetí plnění jsou:

- za objednatele:

Ing. Martin Podstata, tel.: 224 412 628, e-mail: martin.podstata@cnb.cz,

Ing. Luboš Minár, tel.: 224 412 606, e-mail: lubos.minar@cnb.cz,

Ing. Pavel Štádler, tel.: 224 413 433, email: pavel.stadler@cnb.cz,

- za zhotovitele:

Daniel Šrámek, tel.: 222 558 111, email: sramek@sefira.cz,

b. jednání o obchodních otázkách a změnách smlouvy:

- za objednatele:

Ing. Martin Podstata, tel.: 224 412 628, e-mail: martin.podstata@cnb.cz,

Ing. Luboš Minár, tel.: 224 412 606,e-mail: lubos.minar@cnb.cz,

- za zhotovitele:

Ing. Robert Kuzma, tel.: 222 558 111, email: kuzma@sefira.cz,

c. řešení problémů v rámci provozní podpory (právo zadávat požadavky):

- za objednatele:

Ing. Martin Podstata, tel.: 224 412 628, e-mail: martin.podstata@cnb.cz,

Ing. Luboš Minár, tel.: 224 412 606,e-mail: lubos.minar@cnb.cz,

Lenka Černá, tel.: 224 413 874, email: lenka.cerna@cnb.cz,

Dana Blovská, tel.: 224 412 109, email: dana.blovska@cnb.cz,

- za zhotovitele:

Daniel Šrámek, tel.: 222 558 111, email: sramek@sefira.cz.

3. Zhotovitel prohlašuje, že jim dodané technické i programové prostředky, které jsou předmětem plnění podle této smlouvy, pochází od certifikovaného/autorizovaného distributora a poskytovatele technické podpory pro Českou republiku („ČR") a jsou určeny pro prodej v ČR. Zhotovitel je po dobu účinnosti této smlouvy povinen na požádání objednateli tuto skutečnost doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.

4. Zhotovitel je povinen zajistit, aby jeho pracovníci, kteří se budou podílet na plnění této smlouvy, splňovali kvalifikační kritéria, která objednatel požadoval v kvalifikačních požadavcích zadávacího řízení na předmět této smlouvy (bod 8.3.1 zadávací dokumentace). Zhotovitel je po dobu účinnosti této smlouvy povinen na požádání kvalifikaci jednotlivých osob objednateli doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.

5. V případě poskytování služeb prostřednictvím poddodavatele platí všechna relevantní ustanovení tohoto článku také pro poddodavatele a jeho pracovníky, kteří se budou na

plnění smlouvy podílet. V případě, že zhotovitel splnil některý z požadavků stanovených objednatelem v zadávací dokumentaci zadávacího řízení na předmět této smlouvy prostřednictvím poddodavatele, je povinen v případě změny tohoto poddodavatele na požádání objednatele prokázat, že nový poddodavatel tento požadavek splňuje, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.

6. Zhotovitel je povinen prokázat, že má oprávnění zajišťovat provoz HSM zařízení objednatele v režimu QSCD, která jsou současně uvedena na seznamu kvalifikovaných prostředků - https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds a je schopen zajistit dodání certifikátů pro kvalifikovanou pečeť pro tato zařízení. Tuto povinnost musí zhotovitel splňovat po celou dobu účinnosti smlouvy a je povinen ji na požádání objednateli prokázat, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.
7. Objednatel si vyhrazuje právo ověřit si skutečnosti dle odst. 3 až 6 tohoto článku. Objednatel si dále vyhrazuje právo prověřovat schopnost zhotovitele dostát lhůtám definovaným v článku V odst. 2 (např. existence záložních HSM modulů, schopnost dopravit potřebná zařízení v daných časových lhůtách do ČNB apod.).

Článek V.
Podpora a údržba

1. Zhotovitel poskytuje objednateli pro stávající i nově dodané technické a programové prostředky provozní podporu, a to ode dne následujícího po podpisu akceptačního protokolu 1. etapy.
2. Podmínky pro provozní podporu stávajících i nově dodaných technických a programových prostředků, klasifikace vad (kritické/nekritické) a navazující požadavky a lhůty jsou následující:

   a) Pokud uskutečnění servisního zásahu bude vyžadovat provozní odstávku, musí zhotovitel dodržet maximálně stanovené časy odstávek dle přílohy č. 4 požadavek „Provozní odstávky".

   b) **Odstraňování kritických závad technických a programových prostředků**:

   Za kritickou závadu se považuje taková závada, kdy na úrovni operačního systému serveru běžícího v libovolné lokalitě:

   - nejsou dostupné kryptografické klíče nebo s nimi není možné realizovat digitální podpis a dešifrování (ověření podpisu);
   - není možné generovat klíčový pár a žádost o certifikát;
   - není dostupné ani jedno HSM a není to způsobeno závadou na komunikační trase zajišťované objednatelem.

   Mezi kritické závady dále patří také zásadní výkonnostní problémy.

   Řešení kritické závady musí být zahájeno nejpozději do 2 hodin a závada musí být odstraněna do 24 hodin od nahlášení závady.

   c) **Odstraňování nekritických závad technických prostředků**:

   Za nekritickou závadu se považuje taková závada dodaných technických prostředků, která neohrožuje vlastní provoz těchto prostředků, zejména:

   - závady na managementu HSM;
   - výpadek jedné z redundantních komponent HSM.

Řešení nekritické závady musí být zahájeno nejpozději do 4 hodin a závada musí být odstraněna nejpozději do 5 pracovních dní od nahlášení závady.

d) Při vzniku **nekritické závady programových prostředků** bude zahájeno řešení závady nejpozději do 2pracovních dnů po jejím ohlášení zhotoviteli. Na jejím odstranění musí zhotovitel pracovat bez zbytečného odkladu a přerušení a musí využít všech prostředků k dosažení nápravy.

Odstranění nekritické závady musí být dokončeno nejpozději do 10 pracovních dnů od jejího nahlášení. Dohodou smluvních stran může být tato lhůta prodloužena v případě, kdy zhotovitel prokáže objektivní důvody, které mu brání v odstranění vady.

3. Součástí podpory předmětných technických a programových prostředků je i jejich provozní údržba. Provozní údržba technických a programových prostředků zahrnuje 1x za čtvrtletí provedení kontroly funkce všech HSM modulů včetně kontroly logů na zařízeních samotných a na klientech, provedení analýzy a naplánování případného zásahu.
4. Zhotovitel bude na výzvu objednatele poskytovat další činnosti, zejména se jedná o asistenci při generování párů klíčů, konzultace k provozním a vývojovým činnostem, konzultace k plánovaným změnám a jejich realizace, implementace opravných a nových verzí v prostředí objednatele a aktualizaci konfigurace a dokumentace, pokud na ni bude mít implementace vliv.
5. Zhotovitel v rámci zajištění provozní podpory poskytne nové a opravné verze všech programových prostředků. Součástí podpory je také informování objednatele o nových nebo opravných verzích
6. Pokud závadu zjistí zhotovitel, oznámí ji neprodleně objednateli a další postup při jejím odstraňování se řídí ustanoveními tohoto článku s tím, že stanovené lhůty běží od oznámení závady objednateli.
7. Zhotovitel je srozuměn s tím, že veškerá komunikace při hlášení a řešení závad bude mezi objednatelem a pracovníky zhotovitele probíhat v českém jazyce. Při eskalaci řešení problémů k výrobci technických a programových prostředků je akceptována i komunikace v anglickém jazyce.
8. Služby poskytované zhotovitelem musí vyhovovat technickým specifikacím a požadavkům výrobce příslušného technického prostředku.
9. Požadavky na odstranění závad a na ostatní služby podle této smlouvy budou hlášeny na tel: 222 558 810, a s následným písemným potvrzením e-mailem na e-mailovou adresu cnbhsmsla@sefira.cz nebo vadu nahlásí e-mailem na mailovou adresu zhotovitele: cnbhsmsla@sefira.cz. Přijetí požadavku na servisní zásah je zhotovitel povinen potvrdit e mailem na adresu osob uvedených v čl. IV odst. 2 písm. c), a to nejpozději do 2 hodin od přijetí požadavku.
10. O každém provedeném servisním zásahu nebo údržbě vyhotoví pracovník zhotovitele zápis o provedení práce, který stvrdí svým podpisem přejímající pracovník objednatele.
11. Zhotovitel souhlasí s tím, že pokud nebude možné na vadné komponentě prokazatelně bezpečně smazat data objednatele, nemůže být tato komponenta předána zhotoviteli k provedení opravy. Oprava v tomto případě musí proběhnout v prostorech objednatele.
12. Zhotovitel souhlasí s tím, že při výměně vadného média, nebo komponenty, na které jsou/byla data objednatele a nelze prokazatelně tato data bezpečně vymazat (typicky paměťová média, čipové karty apod.), nebudou tato média nebo komponenty po výměně

vráceny zhotoviteli a objednatel zajistí jejich odpovídající mechanickou likvidaci (viz též požadavek „Opravy HW“).

13. Odstranění závady zahrnuje jak výměnu nebo opravu vadného technického nebo programového prostředku, tak zprovoznění nového nebo opraveného prostředku včetně jeho úplné konfigurace.

Článek VI
Smluvní pokuty, úrok z prodlení

1. V případě prodlení zhotovitele má objednatel právo požadovat smluvní pokutu:
   a) ve výši 2 000 Kč za každý den prodlení ve lhůtě dle čl. II odst. 2 písm. a) této smlouvy;
   b) ve výši 2 000 Kč za každý den prodlení ve lhůtě dle čl. II odst. 2 písm. b) této smlouvy;
   c) ve výši 10 000 Kč za každý den prodlení ve lhůtě dle čl. II odst. 2 písm. c) této smlouvy;
   d) ve výši 2 000 Kč za každý den prodlení ve lhůtě dle čl. II odst. 2 písm. d) této smlouvy.
2. V případě prodlení zhotovitele má objednatel právo požadovat smluvní pokutu:
   a) ve výši 20 000 Kč za každou hodinu prodlení ve lhůtě pro zahájení řešení kritické závady dle čl. V odst. 2 písm. b) této smlouvy;
   b) ve výši 20 000 Kč za každou hodinu prodlení ve lhůtě pro odstranění kritické závady dle čl. V odst. 2 písm. b) této smlouvy;
   c) ve výši 1 000 Kč za každou hodinu prodlení ve lhůtě pro zahájení řešení nekritické vady technických prostředků dle čl. V odst. 2 písm. c) této smlouvy;
   d) ve výši 1 000 Kč za každý pracovní den prodlení ve lhůtě pro odstranění nekritické vady technických prostředků dle čl. V odst. 2 písm. c) této smlouvy;
   e) ve výši 1 000 Kč za každý pracovní den prodlení ve lhůtě pro zahájení řešení nekritické závady programových prostředků dle čl. V odst. 2 písm. d) této smlouvy;
   f) ve výši 1 000 Kč za každý pracovní den prodlení ve lhůtě pro odstranění nekritické závady programových prostředků dle čl. V odst. 2 písm. d) této smlouvy;
   g) ve výši 2 000Kč za každou hodinu prodlení ve lhůtě pro potvrzení přijetí požadavku na servisní zásah dle čl. V odst. 9 této smlouvy.
3. V případě, že se po dobu 12 měsíců ode dne předání díla prokáže, že nebyly splněny některé z požadavků uvedených v příloze č. 4 („Striktně vyžadované funkce a vlastnosti“), jejichž splnění požadoval objednatel jako povinné (tzn. vlastnosti označené „musí“ „bude“), má objednatel právo požadovat smluvní pokutu ve výši 100 000 Kč za každý případ nedodržení takového požadavku. Tím není dotčeno právo na odstoupení od smlouvy ani na náhradu vzniklé škody.
4. V případě, že bude na zařízení v jedné lokalitě (počítáno pro každou lokalitu zvláště; všechny komponenty dodané do jedné lokality jsou počítány jako jedno zařízení) více závad než 10 za 12 měsíců, má objednatel právo požadovat smluvní pokutu ve výši 5 000 Kč za každý případ závady nad počet 10.
5. V případě prodlení zhotovitele ve lhůtě pro prokázání skutečností požadovaných objednatelem podle článku IV odst. 3 až 5 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý den prodlení.
6. V případě prodlení zhotovitele ve lhůtě pro prokázání skutečností požadovaných objednatelem podle článku IV odst. 6 této smlouvy je objednatel oprávněn požadovat

smluvní pokutu ve výši 3 % z celkové ceny podle článku III odst. 2 této smlouvy za každý započatý měsíc prodlení.

7. Ujednáními o smluvní pokutě není dotčeno právo smluvních stran na náhradu škody.
8. V případě prodlení s uhrazením daňového dokladu zaplatí objednatel zhotoviteli úrok z prodlení podle předpisů občanského práva.

Článek VII
Vlastnictví, nebezpečí škody na věci a licenční ujednání

1. Vlastnictví k technickým prostředkům dle této smlouvy přechází na objednatele dnem převzetí díla. Právo užívání programových prostředků nabývá objednatel ode dne jejich instalace.
2. Dnem převzetí nových technických prostředků objednatelem do úschovy přechází nebezpečí škody na těchto prostředcích na objednatele.
3. Zhotovitel poskytuje objednateli nevýhradní, nepřevoditelnou a časově i množstevně neomezenou licenci umožňující užívat předmětný SW pouze pro vnitřní potřebu objednatele. Odměna za poskytnutí licence je zahrnuta v ceně díla.
4. Objednatel není povinen dodané licence 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 předmětného software (tj. update/upgrade/patch/hotfix atd.).

Článek VIII
Mlčenlivost, bezpečnostní požadavky objednatele

1. 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 seznámí a které nejsou veřejně známy. Povinnost mlčenlivosti není časově omezena.
2. Zhotovitel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 5 této smlouvy.

Článek IX
Odstoupení od smlouvy, výpověď

1. V případě, že některá ze smluvních stran podstatně poruší smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit. Objednatel je oprávněn odstoupit i od části smlouvy.
2. Zhotovitel bere na vědomí, že pro objednatele je nezbytné, aby veškeré dodané technické a programové prostředky splňovaly všechny požadavky/požadované funkce uvedené v příloze č. 4.
3. Za podstatné porušení smluvní povinnosti se považuje zejména, ale nejen:

   - ze strany zhotovitele:

     - nesplnění kteréhokoli požadavku/požadované funkce uvedených v příloze č. 4,

- prodlení zhotovitele s předáním kterékoliv dílčí etapy dle čl. I odst. 3 písm. a) až d) této smlouvy po dobu delší než 30 kalendářních dnů,
- případ, kdy se v rámci zkušebního provozu dle čl. I odst. 3 písm. c) této smlouvy vyskytnou takové vady implementovaného díla, které objednatel vyhodnotí jako podstatné a tyto nebudou odstraněny ani v určené dodatečné přiměřené lhůtě,
- prodlení zhotovitele se zahájením prací na odstraňování kritické závady v rámci provozní podpory do 2 hodin od nahlášení podle čl. V této smlouvy,
- prodlení zhotovitele se zahájením prací na odstraňování nekritické závady v rámci provozní podpory programových prostředků delším než 2 pracovní dny od nahlášení podle čl. V této smlouvy,
- případ, kdy zhotovitel nebude schopen v rámci implementace dodržet maximálně stanovené časy odstávek dle přílohy č. 4 požadavek „Provozní odstávky",
- porušení kterékoliv povinnosti zhotovitele dle čl. IV odst. 3 až 7,
- rozpor mezi licencemi uvedenými v příloze č. 1 a licencemi skutečně dodanými. Jedná se zejména o rozpory ve způsobu licencování nebo v jejich množství;

- ze strany objednatele:

- prodlení s úhradou dokladů k úhradě delší než 30 dnů.

4. Smluvní strany si sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 50 000 Kč na účet zhotovitele, a to kdykoli do akceptace realizační studie (článek I odst. 3 písm. a)). Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet zhotovitele. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti zhotovitele.
5. V případě odstoupení od smlouvy objednatelem před ukončením zkušebního provozu se zhotovitel zavazuje na své náklady uvést dotčené IS/aplikace do původního stavu a zajistit odvoz technických a programových prostředků, a to nejpozději do 30 dnů ode dne doručení oznámení o odstoupení od smlouvy.
6. Odstoupení od smlouvy je účinné dnem doručení oznámení o odstoupení od smlouvy druhé smluvní straně.
7. Smlouva se v části týkající se podpory uzavírá na dobu neurčitou a lze ji vypovědět v 12 měsíční výpovědní lhůtě, která počíná běžet prvním dnem kalendářního měsíce následujícího po doručení písemné výpovědi druhé smluvní straně.
8. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek zhotovitele odstoupit od této smlouvy. Odstoupení je účinné doručením.

Článek X
Uveřejnění smlouvy a skutečně uhrazené ceny za plnění smlouvy

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. 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://czak.cnb.cz/.

2. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
3. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XI
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. Za písemnou formu nebude pro účel uvedený v tomto odstavci považována výměna e-mailových či jiných elektronických zpráv. To neplatí v případě změny pověřených osob nebo jejich kontaktních údajů dle článku IV odst. 2 písm. b) a c), kdy bude změna provedena jejím písemným oznámením druhé smluvní straně.
3. Práva a povinnosti vzniklé z této smlouvy mohou být postoupeny pouze po předchozím písemném souhlasu druhé smluvní strany. Za písemnou formu se nepovažuje e-mail či jiné elektronické zprávy.
4. Zhotovitel prohlašuje, že po dobu účinnosti této smlouvy bude mít sjednáno pojištění pro případ vzniku odpovědnosti za škodu způsobenou třetí osobě v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 5 000 000 Kč (slovy: pět milionů korun českých) s tím, že jeho spoluúčast nepřevyšuje 5 %. 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.
5. Použije-li zhotovitel při své činnosti podzhotovitele, nahradí škodu jím způsobenou, jakoby ji způsobil sám.
6. Smlouva je sepsána v českém jazyce. 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.
7. Závazkové vztahy touto smlouvou založené se řídí českým právním řádem, zejména zákonem č.89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
8. 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.
9. Smlouva je vyhotovena ve třech stejnopisech, z nichž objednatel obdrží dvě a zhotovitel jedno vyhotovení.
10. Odpověď strany této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
11. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.

Přílohy:

č. 1	Specifikace dodávaných technických a programových prostředků
č. 2	Specifikace činností.
č. 3	Seznam zařízení objednatele

č. 4	Technická a funkční specifikace předmětu plnění
č. 5	Bezpečnostní požadavky objednatele
č. 6	Návrh technického řešení
č. 7	Podrobný rozpis ceny plnění
č. 8	Vzor realizační studie

V PRAZE dne: 27.5.2019

Za zhotovitele:

[redacted]

Ing. Petr Dolejší
jednatel SEFIRA spol. s r.o.

[redacted]

Ing. Daniel Mareš
jednatel SEFIRA spol. s r.o.

sefira spol. s r.o.
Antala Staška 2027/77
140 00 Praha 4 - Krč
DIČ: CZ62907760
www.sefira.cz

V Praze dne: 30 -05- 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

Příloha č. 1

Specifikace technických prostředků a programových prostředků

V rámci smlouvy nebudou dodány žádné technické prostředky a žádné programové prostředky.

Příloha č. 2

Specifikace činností

Detailní specifikace požadovaných činností zhotovitele

Činnost	**Poznámka**
Zapojení nově dodaných technických prostředků do datových struktur ČNB a instalace/úpravy HW/SW	Zapojení nových technických prostředků v režimu vysoké dostupnosti a připojení všech stávajících serverů. Instalace a úpravy HSM a základní konfigurace, instalace a úpravy SW pro management a SW/skriptu pro dohled na dedikovaném serveru (pokud to bude nutné). Po instalaci a konfiguraci zajistí zhotovitel zaškolení pro 2 zaměstnance technické správy ČNB v rozsahu nezbytném pro zajištění provozu všech provozovaných prostředků v ČNB (konfigurace, administrace, běžná správa).
Instalace a úpravy SW na serverech	Asistence při instalaci a případných úpravách veškerého dodaného SW na všech serverech z platforem Linux i Windows. Maximální přípustné doby provozních odstávek jsou uvedeny v příloze č. 4, část Provozní odstávky:
Testovací provoz s HSM v QSCD režimu	definice jednotlivých kroků a součinnosti, detailní harmonogram a specifikace testů, volba ochrany klíčů • nový SecWorld včetně nového RFS na záložním HSM v eIDAS konfiguraci (testovací provedení ACS) • vytvoření konfigurace pro klienty • ověření v testovacích aplikacích • test migrace klíčů testovací CA • dokumentace postupu a plán ostrého přechodu
Konfigurace a provoz HSM v QSCD režimu	•Vytvoření základní konfigurace HSM modulů v režimu QCSD (včetně vytvoření ACS setu); •Vytvoření pomocného OCS setu pro autorizaci požadavků na vytváření OCS setů a softkaret a operace s nimi pro jiné účely než kvalifikovanou pečeť z důvodů provozu ve striktním FIPS módu; •Reset HSM a jeho nová inicializace do HSM infrastruktury v QSCD režimu; •Doplnění nového HSM do HSM infrastruktury (nový modul nebo výměna za jiný v rámci technické podpory) v QSCD režimu; •Aktualizace firmware; •Vytvoření nového OCS setu pro potřeby kvalifikované pečeti; •Vygenerování klíčů pro kvalifikovanou pečeť, žádosti o příslušný kvalifikovaný certifikát a jeho import; •Obnova OCS setu pro kvalifikovanou pečeť na nové čipové karty; •Zničení/smazání klíčů a OCS setů pro kvalifikovanou pečeť, které již nejsou nadále potřebné; •Protokolární dokumentace provedených operací."

Migrace do QSCD režimu	Vypracování migračního postupu a asistence při migraci dat aplikací dle požadavků uvedených v příloze č. 4. v části Migrace dat. Maximální přípustné doby provozních odstávek jsou uvedeny v příloze č. 4 v části Provozní odstávky: Účast zástupce zhotovitele je nezbytná při migraci dat pro MS PKI 2008R2 a pro jednu z aplikací, tj. zástupce zhotovitele bude v ČNB dohlížet a řídit zaměstnance ČNB při importu dat v obou případech. Migraci dat z ostatních aplikací zajišťuje dle dodaného postupu ČNB za účasti zhotovitele.
Skripty	Úprava skriptů pro dohled, pokud to bude nutné.
Optimalizace	Zkušební provoz po ukončení importu dat, provedení měření významných provozních stavů dodaného řešení a návrh optimalizace konfigurace.
Zaškolení	Zaškolení proběhne v prostorech objednatele v rozsahu max. 1 den pro max. 6 odborných pracovníků objednatele. Předmětem zaškolení bude seznámit technické správce komponent systémového prostředí ČNB (typicky operační systém Windows Server a Oracle Linux a RedHat Enterprise Linux; dále pak správce certifikační autority provozované na Windows serveru) s: • instalací, konfigurace, upgrade programového vybavení pro komunikaci s HSM modulem, • Procesem řešení poruch technických či programových prostředků provozovaných v rámci díla dle této smlouvy – postupy a součinnost se zhotovitelem. Při školení může být využita aktualizovaná dokumentace viz níže či potřebné materiály připraví a dodá zhotovitel.
Dokumentace	- vedení deníku o instalaci, tj. průběžné zaznamenávání provedených změn v celém průběhu implementace *); - zajišťování zápisů z jednání a protokolů o předání funkčních celků; - zpracování realizační dokumentace (skutečný stav zapojení, nastavení systému, postupů při provozu, nastavení omezení přístupu,…); - Aktualizace havarijního plánu **); - zpracování protokolů o školení.

*) instalační deník by měl být veden formou el. souboru, kde se **průběžně** (pokud možno okamžitě) zaznamenávají provedené akce a nastavení.

**) Havarijní plán by měl obsahovat všechny nezbytné informace pro zaměstnance objednatele, jak mají postupovat v případě závady a jakou součinnost musí poskytovat případně zhotoviteli. Měl by obsahovat zejména následující informace:

- o umístění nezbytných záznamů (logů) vedoucí k bližší identifikaci závady a základní informace o tom, jak logy analyzovat (případně informaci, že konkrétní log je určen pro analýzu ve vyšších stupních podpory a jak se tento log dá uložit do souboru, aby mohl být odeslán např. e-mailem)
- o postupech při typických závadách a chybových hlášeních a popis postupu/ů jak blíže identifikovat závadu. V této části by měl být uveden popis typických závad, které mohou nastat a mohou být odstraněny zaměstnanci objednatele (např. při výpadku jednoho HSM -> je potřeba uvést HSM do stavu on-line příkazem „abcd"; nefunguje komunikace mezi serverem a HSM-> je potřeba ověřit zda je příslušný port HSM funkční a následně provést akci „xyz"; atd.). Rozsah těchto typických závad bude záviset na složitosti navrženého řešení. Mezi typické „závady" považujeme i postupy při vypínání a zapínání systému, jak po předchozím korektním vypnutí, tak i po neočekávaném vypnutí.
- o postupech při atypických závadách (např. informaci o tom, že se má kontaktovat servisní podpora).
- o postupu při havárii lokality, tj. zejména postup jak zprovoznit systémy v druhé lokalitě.

Příloha č. 3

Seznam zařízení objednatele

Platforma (účel)	verze OS	Aplikační Cluster	Počet licencí celkem	poznámka
Virtualizace – OracleVM 3.4.5				
Základní registry	RHEL 6.10 (Santiago)	Ano	4	
Geocluster Windows				
2 servery provozní CA	Win 2008R2, SP1	Ano	4	
Exadata - Oracle Linux Server release 6.9				
Databáze	Oracle Linux Server release 6.9	Ano	12	
Virtualizace – Vmware vSphere 6				
Spisovna	Win 2008R2, SP1	Ne	4	
RFS	Win 2008R2, SP1	Ne	2	Server pro Management / dohled
Ostatní				
Kořenová CA	Win 2008R2, SP1	Ne	2	
Vývojáři	Win 7, SP1	Ne	4	

Příloha č. 4

Technická a funkční specifikace předmětu plnění

Terminologie

Cluster - skupina zařízení (zpravidla serverů nebo HSM), která umožňuje zajistit obnovu zpracování v řádu jednotek minut po výpadku některé z komponent. Vzájemná vzdálenost zařízení od sebe může být do desítek metrů.

Cluster geografický/geocluster - obdoba lokálního clusteru s tím rozdílem, že i data jsou zdvojená a tato technologie umožňuje kompletní obnovu zpracování ve fyzicky jiné lokalitě (vzdálenost desítky kilometrů). V různých lokalitách jsou nejen servery, ale i HSM.

High Availability – řešení, které zajišťuje dohodnutou spolehlivost zpracování nebo systémů. V tomto řešení je typicky zajištěno, že při výpadku jedné (nebo i více komponent) není zpracování narušeno.

IS (Informační systém/aplikace) - je funkční celek, který slouží k získávání, uchovávání, přenášení, zpracovávání a poskytování informací pomocí informačních technologií. Zahrnuje informační technologie, data, správu informačního systému a zaměstnance, kteří ji zajišťují, uživatele a vzájemné vazby mezi nimi.

Slot (Softcard, ACS) – samostatně přístupný, bezpečnostně oddělený prostor se samostatnou autentizací, sloužící jako úložiště pro klíče a certifikáty. Je vytvořen konfiguračními prostředky HSM.

Data – jedná se o páry kryptografických klíčů a souvisejících certifikátů, pokud není uvedeno jinak

MSCS (Microsoft Cluster Service) – SW dodávaný firmou Microsoft zajišťující funkci clusteru. Tento SW je součástí MS Windows Enterprise Edition.

RHEL (Red Hat Enterprise Linux) – zkratka pro operační systém typu Linux vyvinutý firmou RedHat.

Synchronní/Asynchronní přenos - pojmem synchronní přenos je označován typ přenosu, kdy data z jednoho HSM do druhého jsou automatizovaně přenesena na základě jejich změny v jednom z HSM. Naproti tomu při asynchronním přenosu jsou data po změně přenesena až na základě pokynu obsluhy.

ZP – záložní pracoviště ČNB Praha-Zličín.

HSM (Hardware Security Module) – bezpečnostní modul pro uchování certifikátů a klíčů aplikací a PKI. Modul zajišťuje prostřednictvím uložených klíčů elektronický podpis nebo dešifrování.

PKI (Public Key Infrastructure) – infrastruktura veřejných klíčů

CAPI (CryptoAPI) – je aplikační programové rozhraní, které umožňuje šifrování a digitální podpis pro aplikace v systému Windows

CNG (Cryptography API Next Generation) – je náhrada za CryptoAPI

FIPS 140-2 (Federal Information Processing Standards) – standardy, které ve verzi 140-2 specifikují požadavky na kryptografické moduly

EAL (Evaluation Assurance Level) – udává, na jaké úrovni testování daný produkt vyhověl bezpečnostním kritériím (Common Criteria)

USB (Universal Serial Bus) – je univerzální sériová sběrnice pro připojení periferií k počítači

CSP (Cryptographic Service Provider) – zprostředkovatel kryptografických služeb v systému Windows

KSP (Key Storage Provider) – je náhrada za CSP v systému Windows

PKCS (Public Key Cryptographic Standards) – je skupina standardů pro kryptografii s veřejným klíčem navržená a publikovaná společností RSA Security

SIEM (Security Information Event Management) – je nástroj pro správu bezpečnostních informací a událostí

RSA, SHA-2 – kryptografické algoritmy

Popis současného stavu a infrastruktury HSM v ČNB

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. Běžný uživatel není schopen rozlišit, ve kterém středisku je jeho požadavek zpracován. V případě potřeby (havárie, údržba,....) je zpracování konkrétního informačního systému přesunuto na jiný uzel.

Do prostředí (geografických) clusterů jsou umísťovány IS přímo podporující jednu nebo více kritických činností ČNB. Jiné IS se do tohoto prostředí umisťují jen výjimečně (např. z licenčních důvodů, striktního požadavku na shodnost akceptačního a provozního prostředí apod.).

V případě havárie je výpadek ve zpracování (doba mezi zastavením IS a jeho nastartováním na jiném serveru) v délce do 5 minut pro ČNB akceptovatelný. V případě plánované údržby je nutné konkrétní dobu přesunu zpracování individuálně dohodnout se správcem příslušného IS (liší se dle IS, zpravidla na počátku nebo konci pracovní doby).

Komunikační infrastruktura

Jedno výpočetní středisko je umístěno v budově ústředí v Praze 1 a druhé v Praze 5 - Zličín. Obě střediska jsou plnohodnotně vybavena jak po stránce komunikační (LAN), tak i po stránce zpracování a uložení dat (servery, disková pole, magnetopáskové knihovny). Z kapacitního hlediska převažuje (počty serverů, objemy dat) objekt ústředí, ve kterém jsou také umístěny systémy nevyžadující zdvojení (méně významné IS, systémy pro testování a vývoj apod.).

Obě výpočetní střediska jsou propojena optickými vlákny (single mode) dvěma nezávislými trasami.

Prostředí HighAvailability (HA)

V ČNB je nasazeno několik typů prostředí HA. V zásadě je lze rozdělit na prostředí, kde je HA podporováno na úrovni celých virtuálních strojů a na prostředí na úrovni jednotlivých aplikací uvnitř serveru (virtuálního nebo fyzického). Obě tyto úrovně mají různý stupeň automatizace.

V současné době jsou v ČNB provozovány dvě virtualizační platformy – VMware a Oracle VM. Zde jsou využívány funkcionality typu FailOver (přesun celého virtuálního stroje (VM) při havárii hypervizoru) a SRM (VMware Site Recovery Manager).

V oblasti aplikační je na operačním systému Linux RHEL využíván software HP MC/ServiceGuard (MC/SG), k němuž byly v ČNB vyvinuty scripty zajišťující manipulaci s příslušnými disky v návaznosti na operace vyžadované clusterem.

V prostředí operačního systému Windows je provozován Microsoft Cluster Server (MSCS) s arbitrem - File share witness.

.

Úložiště klíču

V ČNB je využíváno několik typů úložišť. V zásadě je lze rozdělit na prostředí softwarová, kde jsou klíče uloženy v operačním systému nebo databázi a na prostředí hardwarová, kdy jsou klíče uloženy na čipových kartách nebo HSM modulech. Pokud je využito standardních úložišť MS Windows (MS PKI 2008R2), nejsou pro aplikace realizovány žádné specifické programové nadstavby. V ostatních případech jsou pro aplikace vytvořeny programové moduly, které umožňují spolupráci s příslušným úložištěm.

Popis stávajícího prostředí HSM

1.1. Security World

Security world (SecW) je kompletní infrastruktura, která slouží k zabezpečení kompletního životního cyklu šifrovacích a podepisovacích klíčů.
Vlastní security world se skládá z těchto komponent:

- jeden nebo více Thales HSM modulů;
- set administrátorských čipových karet (ACS) pro správu a obnovu security world;
- volitelně jeden nebo více setů operátorských čipových karet nebo softkaret pro ochranu vybraných aplikačních klíčů
- vybrané klíče a certifikáty zašifrované hlavním klíčem security worldu (Security World key) uložené na klientských počítačích mimo vlastní HSM moduly.

Jeden security world sdílí společný hlavní klíč (Security World key) pro všechny použité HSM moduly pro zabezpečení klíčů a souvisejících dat mimo vlastní HSM moduly.
SecWorld je provozován v režimu FIPS Level 2 a starší necertifikované verzi FW 11.70.00.
Podrobnosti k ostatním komponentám jsou popsány níže.

1.2. Administrátorský set čipových karet (ACS)

Sada administrátorských čipových karet, na kterých jsou uloženy fragmenty master klíče celého security world tak, aby byl nutný přístup k **n** různým čipovým kartám z celkového počtu **N** administrátorských karet.

1.3. Operátorský set čipových karet (OCS)

Set čipových karet, které mají k dispozici správci PKI, využity jsou OCS sety velikosti k/N u obou CA.

1.4. Softcards

V případě vybraných aplikací nebo rozhraní je použita alternativa k fyzickým čipovým kartám v podobě tzv. softcards, což jsou virtuální SW varianty čipové karty.
Jedná se o soubor se zašifrovaným klíčem, který je uložen na příslušném klientovi a chráněn heslem.
Tato varianta je používána pro aplikace využívající PKCS#11 rozhraní.

1.5. Remote File System (RFS)

Uplatněná architektura zabezpečení security world umožňuje uchovávat klíčové konfigurace a data mimo vlastní HSM moduly v šifrované podobě. Za tímto účelem každý HSM modul používá vzdálený souborový systém na definovaném klientovi.
Na tomto souborovém systému jsou uloženy zálohy konfigurací jednotlivých modulů, které je možné použít např. při obnově poškozeného HSM modulu. Dále jsou sem ukládány všechny klíče a certifikáty, které jsou k dispozici v rámci celého security world.

Synchronizace mezi jednotlivými klienty se neprovádí.

1.6. Klient

Klientem je počítač s IP adresou, který fyzicky komunikuje s konkrétním HSM modulem. Pro každého takového klienta je třeba mít na příslušném HSM modulu klientskou licenci, která je pevně spjata s konkrétním HSM modulem.
Pro případ požadavku řešení v režimu vysoké dostupnosti jsou k dispozici 2 HSM moduly a každý klient je registrován na 2 HSM modulech.
Na klientu je nainstalováno aplikační SW vybavení Thales zajišťující krom jiného režim vysoké dostupnosti a soubory s klíči v zašifrovaném formátu pro konkrétní IS.

1.7. Aplikace

Aplikací se v rámci terminologie myslí především použité aplikační rozhraní. Přehled využívaných aplikačních rozhraní uvádí následující seznam:
PKCS #11 aplikace – aplikace a technologie používající PKCS#11 rozhraní –

- RHEL (2+2záložní) servery, celkem 2 IS (využívají IAIK PKCS#11)
- Exadata (2+2záložní) - celkem 2 IS (využívají IAIK PKCS#11);
- MS Win LTD server (1+1test) – celkem 4 IS (využívají PKCS#11).

Microsoft CNG CSP - PKI infrastruktura MS Windows – 1x kořenová CA a 1+1 provozní CA (MS Cluster)

1.8. HSM moduly

V prostředí jsou zapojeny dva HSM moduly Thales nShield Connect 1500+ v HA režimu. Každý z modulů má 16 licencí.

Moduly jsou nastaveny následujícím způsobem:

- jsou součástí jednoho security world, používají stejné RFS;
- záznamy událostí se zaznamenávají jak v modulu, tak i na RFS.

1.9. Konfigurace náhradního HSM modulu

V rámci celkové infrastruktury HSM modulů je v produkčním SecW rovněž konfigurován náhradní modul, který je možné v rámci stávající podpory dočasně zapůjčit po dobu nezbytně nutnou na opětovné zprovoznění standardního produkčního HSM modulu.

Standardní systémové prostředí ČNB (výňatek pro účely této smlouvy)

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 *(v běhu upgrade na platformu Windows 2016 Server)*
- Platforma Red Hat Linux v. 6.10 jako alternativní prostředí
- Platforma Oracle Linux (systém Oracle Exadata)
- Platforma VMware vSphere 6
- Platforma Oracle VM 3.4.5

Monitoring systémů

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

1. **Striktně vyžadované funkce a vlastnosti**:

V následující tabulce jsou uvedeny požadavky, které musí být zhotovitelem ve finálním řešení splněny. U jednoho „požadavku" (=řádku tabulky) může být současně i několik požadovaných vlastností (viz např. požadavek „spolehlivost"), které musí být splněny všechny.

Použité výrazy jsou poplatné obecné terminologii a nejrozšířenějším technologiím. V některých místech se však mohou lišit od technologie nabízené zhotovitelem (vše není možné popsat zcela obecně). V tom případě musí zhotovitel jasně vysvětlit vzájemný vztah nabídnutého řešení a požadavku objednatele a zdůvodnit způsob splnění požadavku. Rozhodující je splnění příslušné funkce nebo vlastnosti po její funkční/výkonové stránce nikoliv způsob jakým je výsledku dosaženo.

Požadavek	**Popis**	**Poznámka/zdůvodnění**
Dostupnost	Řešení musí být odolné proti výpadku. Jednotlivé komponenty musí být zdvojené, nesmí existovat tzv. „Single Point of Failure".	Pro potřeby ČNB je důležitá spolehlivost a bezvýpadkovost systému jako celku.
Spolehlivost	Je vyžadováno: - zajištění provozu 24x7 včetně garance dostupnosti dat na úrovni operačního systému serveru alespoň v jedné lokalitě do 6 hodin. V tomto případě není rozhodující, zda se jedná o chybu HW nebo SW; - výměna libovolné jedné vadné komponenty za provozu (bez přerušení přístupu k datům, výkonnost může být částečně snížena); - HSM cluster nesmí mít SPOF (Single Point of Failure); - konfigurační změny online (viz dále); - zajištění podpory výrobce zařízení tak, aby v případě vážné chyby byl výrobcem vytvořen fix pro tuto vážnou chybu, která se vyskytla v ČNB; - zařízení nesmí být příliš poruchové (podrobnosti viz čl. VI, odst. 4) této smlouvy) - přetížení jedné komponenty nesmí způsobit zastavení celku. Jmenovitě nesmí dojít k situaci, kdy přetížením jednoho komponenty dojde k podstatnému ovlivnění dostupnosti a výkonnosti poskytované druhou komponentou.	Pokud bude požadavek na zajištění dostupnosti dat do 6 hod řešen studenou zálohou ve formě dalšího zařízení, musí být toto zařízení v nabídce uvedeno. Vysoká spolehlivost provozu je součástí zajištění dostupnosti dat. V noci probíhá dávkové zpracování v délce několika hodin. Případné odstávky při výměně vadných komponent, upgrade FW/mikrokódu nebo konfigurační změny mající dopad na provoz systému jsou v ČNB organizačně náročné. Zajištění bezchybného uložení dat je pro ČNB jedním z prioritních požadavků. Zhotovitel musí na základě svých kontraktů s výrobce/distributorem zajistit takovou úroveň podpory, aby bylo možné problém eskalovat k výrobci (případně pověřené organizaci), kde

	- dodávané technické prostředky musí být vyráběny sériově, nesmí být vyvíjeny pro potřeby této konkrétní zakázky. Dodaná verze FW/mikrokódu v době instalace musí být stabilní provozní verze instalovaná ve světě nejméně u 50 zákazníků v jejich produkčním prostředí. Splnění požadavku je nutné doložit prohlášením výrobce.	se tímto problémem budou seriózně zabývat. Výsledné stanovisko samozřejmě může být závislé na konkrétní situaci (bude/nebude vytvořen fix, bude implementováno do nové verze FW apod.). Každá závada znamená čas zaměstnanců ČNB strávený její řešením. A to přináší na straně objednatele určité náklady. S ohledem na význam HSM není naprosto přípustné, aby zhotovitel prováděl jakékoliv ladění FW/mikrokódu nebo jiného dodaného SW v prostředí ČNB.
Režim vysoké dostupnosti	V rámci řešení musí být zajištěn režim vysoké dostupnosti. Mezi dvěma různými instalačními lokalitami. Technologie musí být transparentní a může vyžadovat pouze konfigurační zásah do IS.	ČNB má v provozu tzv. nouzové záložní pracoviště, které je provozováno systémem aktiv-aktiv, tj. v obou lokalitách jsou provozovány různé IS. V případě výpadku/odstávky je zpracování převedeno do druhé lokality. Toto nouzové pracoviště je také koncipováno jako „disaster recovery" centrum ČNB.
Zabezpečení dat	Data musí být zabezpečena proti selhání nebo přetížení prostřednictvím clusterového řešení (zdvojení komponent) a zálohováním dat do bezpečného úložiště a jejich rozdělení na více částí. Pokud je vyžadován pro tuto funkci speciální hardware, musí být dodán v takovém množství, aby odpovídal minimální poptávané kapacitě a dvěma nezávislým zálohám.	Pro případ selhání obou nodů clusteru musí být k dispozici odpovídajícím způsobem zabezpečená záloha.
Zabezpečení proti úniku dat	HSM a servery jsou umístěny v prostorech s omezeným přístupem v dedikovaném uzamčeném racku. V případě pokusu o fyzické narušení	HW, kde bude umístěn klíčový materiál včetně záloh, bude umístěn v prostorech s omezeným

	HSM musí dojít k automatickému vymazání dat a to i v případě že bude HSM ve vypnutém stavu.	přístupem v dedikovaném uzamčeném racku nebo v trezoru podle typu média.
Ochrana investic	Požadované funkce řešení musí být aplikačně nezávislé (změna verze IS/aplikace nesmí mít vliv na funkce poskytované řešením).	Všechny poskytované funkce musí být nezávislé na IS. Pro všechny informační systémy musí být poskytované služby transparentní, tj. nesmí existovat vazba mezi informačními systémy a řešením ve smyslu nutnosti certifikace výrobcem dodaného HW nebo SW.
Připojení	Připojení je vyžadováno prostřednictvím minimálně 2 nezávislých přípojek LAN.	V ČNB je vybudovaná infrastruktura LAN, která umožňuje připojení zařízení do dvou nezávislých síťových prvků.
Množství připojených serverů	Navržená technologie musí umožňovat připojení minimálně 14 serverů ke každému nodu.	V budoucnu se předpokládá navýšení počtu připojených serverů.
Kapacita a prostor pro data	Celková kapacita pro data (v každé lokalitě) musí být minimálně 20 klíčových párů a certifikátů o velikosti každého klíče/certifikátu max. 4096 bitů. Tyto klíčové páry musí být možné umístit do minimálně 10 slotů.	Požadavek na celkovou kapacitu vychází, ze současného stavu a z očekávaného nárůstu pro další období. Vysvětlení pojmu „celková kapacita pro data (v každé lokalitě)“: je to prostor, který může být přidělen nějakému serveru/ům (aplikacím).
Kapacitní rozšiřitelnost	Z hlediska rozšiřitelnosti kapacity musí navržené řešení umožňovat zvětšení kapacity minimálně o dalších 20 klíčových párů a certifikátů o velikosti každého klíče/certifikátu max. 4096 bitů. Tyto klíčové páry musí být možné umístit do dalších minimálně 10 slotů. To vše bez koncepčního zásahu do navrženého řešení. Kapacitní rozšiřování nesmí mít dopad na provoz již instalovaných komponent. Rozšíření musí být v rámci navrženého řešení, tj. veškeré dodané i rozšířené kapacity musí být spravovány a provozovány jako jeden celek. Zejména z hlediska provozu se musí jednat o celek, který mj.	V závislosti na skutečných potřebách v následujících 3-4 letech se očekává možnost požadavků na kapacitní rozšíření. Nabízené zařízení musí umožnit rozšíření, ale toto rozšíření není v tuto chvíli předmětem dodávky.

	umožní připojení nových kapacit k serverům bez potřeby složitých rekonfigurací.	
Výkonnost	Každé HSM v nabízené konfiguraci musí být schopno realizovat minimálně 600 podpisových operací za sekundu algoritmem RSA s klíčem o velikosti 1024bitů. Splnění požadavku je nutné doložit prohlášením výrobce.	Výkonnost musí být jednoznačně doložena výrobcem.
Výkonnostní rozšiřitelnost	Navržené řešení musí umožňovat rozšíření nejméně o dalších 600 podpisových operací za sekundu algoritmem RSA s klíčem o velikosti 1024bitů v každé lokalitě. Rozšíření musí být v rámci navrženého řešení, tj. veškeré dodané i rozšířené kapacity musí být spravovány a provozovány jako jeden celek. Zejména z hlediska provozu se musí jednat o celek, který mj. umožní připojení nových kapacit k serverům bez potřeby složitých rekonfigurací.	Z hlediska výkonnosti se očekává v následujících 3-4 letech možný nárůst počtu požadovaných podpisových operací a proto musí být zajištěna možnost výkonnostního rozšíření. Rozšíření není v tuto chvíli předmětem dodávky.
Operace s HSM	Zařízení musí umožnit zvětšení počtů slotů bez ztráty uložených dat. Změny na HSM (přidání/odebrání serveru nebo přidání/odebrání slotu u jednoho HSM) v žádném případě nesmí ovlivnit provoz ostatních serverů (aplikací) připojených k HSM ani ostatních HSM jako celku.	Funkce nutná z důvodu zabezpečení nezávislého přístupu serverů jen k přiděleným slotům.
Homogenita	Navržené řešení musí být homogenní, tzn. že ke všem komponentám musí být přistupováno rovnocenně. Tím je míněno, že veškeré komponenty stejného významu nebo funkce musí mít také stejná privilegia, omezení, stejné funkce a odpovídající výkonnost. Není proto přípustné, aby ke slotům některého z HSM nebylo možné přistupovat z některého ze serverů. Je vyžadováno jednotné řešení z hlediska zajištění správy navrženého řešení. Navržené řešení musí být symetrické (shodné) pro obě lokality.	Z důvodu flexibility (možnost bezproblémové změny umístění aplikací) a z důvodu zjednodušení správy musí být navržené řešení stejné pro obě lokality (ústředí/ZP).

Ladění výkonnosti/přesun zpracování na jiný HSM	Je požadována funkcionalita SW umožňující přesun zpracování na druhý HSM s menším zatížením. Přesun musí proběhnout on-line vzhledem k aktivitě serveru a bez narušení jeho provozu. Tato funkcionalita nemusí zajišťovat automatický návrh přesunů ani jej automaticky provádět. Pokud bude SW umět automatické přesuny, musí být možné je zablokovat nebo alespoň konfigurovat na uživatelské úrovni.	Jedná se o „poloautomatickou" optimalizaci zátěže HSM bez nutnosti odstávek provozu v případě kdy je jeden HSM např. v určitou denní dobu přetížen.
Kompatibilita s prostředím ČNB	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. Navržené řešení musí dodržovat standardy uvedené v části „Popis současného stavu a infrastruktury ČNB".	
Kompatibilita aplikací	Musí být zajištěn provoz MS PKI 2008R2 a ostatních aplikací na platformě RHEL, pracujících v režimu vysoké dostupnosti. Přesun aplikací mezi lokalitami nesmí mít vliv na funkčnost clusteru těchto aplikací, ani dodaného řešení jako celku.	Režim vysoké dostupnosti je v prostředí MS Windows 2008R2 realizován jako geografický cluster MSCS. Na platformě RHEL je cluster realizován jako lokální prostřednictvím SW HP MC/ServiceGuard s geografickou nadstavbou ČNB.
Kompatibilita serverů	Navržené řešení musí umožnit připojení serverů na platformách uvedených v tabulce **„Seznam zařízení objednatele"**. Kompletní seznam serverů včetně je uveden v příloze č. 3. Možnost připojení těchto serverů v kombinaci s operačním systémem musí být výrobcem HSM podporována. Jedná se zejména o serverové operační systémy/platformy: MS Windows Server 2008 R2 a RedHat Linux 6.10 nebo Oracle Linux Server release 6.9, které mohou být provozovány buď na fyzickém HW, nebo na virtualizační platformě	Navržené řešení musí zajistit možnost připojení stávajícího technického vybavení (serverů) a umožňovat i rozvoj do budoucna (přechod na vyšší verze provozovaného programového vybavení-operačních systémů). Vynucená změna operačních systémů nebo jejich verzí je v rámci nasazení řešení zcela vyloučena.

	VMware 6 nebo OracleVM 3.4.5 Dále musí být podporováno připojení serverů s operačními systémy Windows 2012 a Windows 2016, RedHat 7. Dále pak Oracle Linux provozovaný na systému Oracle Exadata 6.9.	
Rozhraní pro programátory a aplikace	Na serverech viz „kompatibilita serverů" musí být k dispozici rozhraní PKCS#11 a rozhraní pro programovací jazyk Java. Zároveň musí být k dispozici rozhraní MS CNG pro servery s operačním systémem Windows Server 2008R2 a vyšším. Funkce a možnosti rozhranní musí být dokumentovány a musí být dodán příslušný SDK včetně příkladů použití.	Je nutné vybavit minimálně dvě pracoviště dvou programátorů.
Základní funkce	Musí být možné generovat klíčový pár v HSM a žádost o certifikát. Tato žádost musí být vygenerována ve formátu PKCS#10 včetně diakritiky. Certifikát musí být následně možné naimportovat do HSM ve formátu X.509v3 a to v kódování DER nebo base 64. Musí být možné provést import certifikátů a klíčů ze souboru ve formátu PKCS#12, pokud HSM nepracuje v režimu FIPS 140-2 Level 3. Přepnutí do režimu FIPS 140-2 Level 3 nesmí způsobit ztrátu takto uložených dat. S takto uloženými nebo vygenerovanými klíči musí být možné realizovat digitální podpis a dešifrování (ověření podpisu) Pokud je pro některou z funkcí nutný alternativní postup, musí být zhotovitelem podrobně popsán. Všechny nezbytné skripty i případné utility (např. OpenSSL) musí být součástí dodávky a zhotovitelem	Jedná se o minimální a povinný výčet funkcí.

	podporovány! Zhotovitel musí mít oprávnění zajišťovat provoz HSM zařízení objednatele v režimu QSCD, která jsou současně uvedena na seznamu kvalifikovaných prostředků - https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds a musí být schopen zajistit dodání certifikátů pro kvalifikovanou pečeť pro tato zařízení. Tuto povinnost musí zhotovitel splňovat po celou dobu účinnosti smlouvy.	
Množina podporovaných kryptografických algoritmů	Minimálně musí být podporován asymetrický algoritmus RSA o délce klíče až 4096 bitů, hešovací algoritmus SHA-256 a symetrický algoritmus AES o velikosti klíče 256 bitů.	Volitelně mohou být podporovány další algoritmy, které vyhovují FIPS 140-2, např. TDES.
Autentizační mechanismus	Pro přístup je vyžadována minimálně autentizace prostřednictvím hesla, přístup ke klíčům omezen pouze na vymezené servery. Musí být možné v případě aplikací vynutit použití pouze jednoho autentizační údaje, pokud řešení disponuje autentizačním mechanismem, který pro přístup vyžaduje více částí.	V případě aplikací není přípustné, aby byl vyžadován více než jeden autentizační údaj pro přístup ke klíčům. Nesplnění tohoto požadavku by vyžadovalo značné úpravy na straně aplikací. Případné náklady spojené s úpravou komponent zhotovitel musí zahrnout do celkových nákladů na realizaci.
Zabezpečení proti infiltraci a odposlechu komunikace	Proti zneužití odposlechem na sběrnici nebo na síti musí řešení umožnit vytvoření důvěryhodného kanálu mezi sebou a participující aplikací. Řešení i aplikace musí být nastavené tak, aby vyžadovaly vytvoření důvěryhodného kanálu před tím, než si mezi sebou začnou vyměňovat jakékoliv kryptograficky citlivé informace tak, jak to vyžaduje FIPS 140-2 Level 3.	Objednatel bude realizovat pravidelné testy HSM monitorovacím nástrojem Qualys.
Bezpečnostní certifikace	Řešení musí zajistit minimálně certifikaci odpovídající úrovni EAL 4+ nebo kompatibilní, případně FIPS 140-2 Level 3 nebo vyšší a musí v tomto módu také pracovat.	Certifikace musí být doložena příslušným certifikátem.
Systém provozu	V obou lokalitách budou IS provozovány systémem active-active, tj. v každé lokalitě mohou s kteroukoliv částí řešení v režimu HA	Tento systém umožňuje využití pořízených kapacit v běžném provozu k rozložení zátěže

	komunikovat za běžného provozu různé IS.	mezi jednotlivé servery.
Duální připojení serverů	Požadován je nejen FailOver, ale i load balancing (všechny cesty mezi serverem a HSM musí být v normálním režimu aktivní a musí nad nimi být zajištěn load balancing). Tato povinnost platí pro servery dle přílohy č. 3. Ztráta některé z cest k HSM nesmí mít dopad na činnost serveru s výjimkou snížení propustnosti, tj. nesmí dojít k činnosti serveru, která povede k jeho nefunkčnosti (např. přesun zpracování aplikací na jiný uzel geoclusteru).	Pro některé náročné IS je nebo v budoucnu může být nezbytné současné využití více komunikačních kanálů k HSM tak, aby došlo k rozložení zátěže mezi jednotlivými HSM. Ztrátou dostupnosti některé z cest k HSM nesmí být ovlivněna řádná činnost operačního systému nebo aplikací.
Dopad na provoz serverů	Dodávaný SW nesmí mít zásadní dopad na výkonnost serveru. Vyžadováno je tedy řešení, které má minimální dopad na celkovou zátěž serveru (tj. jeho CPU, RAM, NIC,....). Pokud bude navřeno řešení s dopadem na výkonnost serveru, nesmí mít větší dopad, než 10% výkonu CPU, nejvýše 10% kapacity RAM a nejvýše 10% LAN.	Zatížení serveru dodávanými komponentami nesmí zásadním způsobem omezovat výkonnost provozovaných aplikací.
Zátěž komponent síťového prostředí ČNB	Navržené řešení nesmí neúměrně zvyšovat zátěž prvků stávajícího systémového prostředí ČNB. Navýšení zátěže každé z komponent systémového prostředí je povoleno nejvýše o 10%.	Navržené řešení nesmí zcela svévolně, resp. pouze pro zajištění své vlastní režie navyšovat zátěž síťových komponent současného prostředí ČNB. Tím by mohla vzniknout nutnost některé z komponent posílit.
Rozměry a chlazení	Případně nově dodávané technické prostředky musí být umístitelné v těchto prostorech ČNB: Praha 1, Senovážná ul. 3 (místnosti VP304) Praha 5, Strojírenská 175 (místnost PP117) Zařízení bude v **objektu ústředí** umístěno do standardního 19" stojanu ČNB (výrobce Triton, 42U 600x900mm, bez podstavce, s krytím IP20). Zařízení musí být dodáno včetně komponent, které umožní montáž do tohoto typu stojanu.	Požadavek vychází ze specifikace prostor očekávaného umístění. Jiný stojan by přinesl problémy se zastřešením teplé uličky a s chlazením prostoru.

	V objektu ústředí je vytvořen systém tzv. teplé uličky. Zařízení jsou tedy ve stojanech s přívodem chladného vzduchu před stojan a výdech ohřátého vzduchu je zadem do zastřešené uličky a odtud je odváděn pryč. V objektu ZP bude k dispozici stojan obdobných parametrů jako v ústředí. V ZP Zličín je v současné době chlazení zajištěno foukáním chladného vzduchu do zdvojené podlahy. V budoucnu se předpokládá stejný systém jako v Senovážné, tedy systém teplé a studené uličky. Dodávaná zařízení musí splňovat podmínku sání na přední straně a výdech na zadní straně v kombinaci s umístěním do stojanu ČNB.	
Napájení	Požadováno je připojení na rozvod s napětím 230V (=jednofázové) s jištěním nejvýše 25A. Je požadováno zajištění uložených dat tak, aby i při výpadku napájení trvajícím nejvýše 24 hodin nebyla tato ztracena (např., baterie pro zálohování).	Ve výpočetních střediscích ČNB jsou rozvaděče připraveny pro připojení systémů s 1 fázovým napájením.
Diagnostika	HSM musí mít zajištěnu trvalou diagnostiku poruch. V případě poruchy musí HSM problém hlásit objednateli, který rozhodne o urgentnosti odstranění závady. Pokud budou mít úpravy vliv na funkčnost stávajících skriptů, musí být v rámci dodávky upraveny.	Pro zajištění maximální spolehlivosti a včasného zajištění nápravy je vyžadována trvalá diagnostika poruch řešení.
Dohledový nástroj/skript	Diagnostika musí být realizována buď prostřednictvím dohledového nástroje, nebo skriptu, který musí zajistit: - aktivní zasílání informací o chybách e-mailem nebo alespoň zápisem do textového souboru se stanovenou strukturou a významem obsahu nebo syslogu, případně SNMP minimálně verze 2. Pro všechny uvedené možnosti odesílání informací musí být možnost uživatelského nastavení, které informace budou zasílány a které nikoliv nejlépe až na úroveň konkrétní události	Z důvodu zajištění správy a minimalizace nároků na správu je požadováno zajištění odpovídajícího nástroje/skriptu a jeho funkčnosti i po rozšíření. Pro dohledový nástroj/skript může je ze strany ČNB poskytnut 1x Virtuální server (max.

	s členěním významnosti minimálně na 2 úrovně. Dohledový nástroj/skript musí splňovat minimálně tato bezpečnostní kritéria: - klientský přístup protokolem https nebo ssh případně jiným. ale z hlediska bezpečnosti zabezpečeným protokolem: - zajištění autentizaci/autorizaci uživatelů;	1xCPU, 2GB RAM, 30 GB HDD) s připojením do LAN. Více viz příloha č. 4.
Konfigurační změny	Řešení musí umožňovat minimálně tyto uživatelsky (=zaměstnanci ČNB) prováděné operace: - definice serverů s garantovaným přístupem. - konfigurace módu provozu v režimu vysoké dostupnosti - definování slotů a jejich konfigurace Řešení musí umožňovat minimálně tyto zhotovitelem prováděné operace: - konfigurace lokálního zabezpečení: - rozšiřování kapacity a výkonnosti (případné přidávání HSM a ostatních souvisejících komponent); Provádění všech operací musí být on-line, tj. bez přerušení přístupu k datům, výkonnost může být částečně snížena (týká se uživatelsky i zhotovitelem prováděných operací). Konfiguraci lokálního zabezpečení je možné přenést na uživatele. Tyto konfigurační změny musí být možné provádět prostřednictvím CLI, případně GUI (týká se uživatelsky prováděných operací). Konfigurační změny je možné provádět pouze za následujících „bezpečnostních kritérií": - klientský přístup protokolem https nebo ssh případně jiným. ale z hlediska bezpečnosti zabezpečeným protokolem; - zajištění autentizace/autorizace uživatelů.	Pro pružné a efektivní využití HSM je nezbytné zajistit možnost konfiguračních změn HSM na úrovni zaměstnanců objednatele. Další požadované operace musí zajistit technická podpora zhotovitele.
Manipulace v clusteru-funkčnost	Pro zajištění funkce geografického clusteru musí být zajištěny minimálně tyto funkce:	

clusteru	- provedení FailOver/FailBack; Provádění všech operací musí být on-line, tj. bez přerušení přístupu k datům, výkonnost může být částečně snížena. Přechod na druhý node clusteru musí proběhnout automatizovaně na platformách dle přílohy č. 4. Provedení operace musí být zajištěno do 4 minut (čas od okamžiku výpadku některé komponenty do okamžiku kdy jsou přístupné operačnímu systému v druhé lokalitě.	
Řídící komunikace a ovládání	Komunikace pro řízení a ovládání řešení (např. konfigurační změny, FailOver při havárii atd.) může být realizována různými způsoby. Zhotovitel musí specifikovat používané porty pro tuto komunikaci (nastavení lokálních firewallů na serverech, např. IP tables). Řídící komunikace s HSM musí být možná z příkazové řádky (CLI) nebo prostřednictvím grafického rozhraní (GUI)	Pro konfigurační a řídící potřeby není nutné zajistit bezvýpadkový provoz (případný server zajišťuje ČNB).
Zálohování konfigurace	Musí být zajištěna možnost zálohování konfigurace řešení na serveru (pokud systém sám o sobě neprovádí tuto zálohu i do jiného vzdáleného prostoru). Musí být také zajištěna možnost zálohování konfigurace jednotlivých HSM.	Jedná se minimálně o požadavek na možnost automatického vytvoření textového (čitelného) reportu o konfiguraci dané komponenty (konfigurace HSM, serverů,...) pro potřeby případné nutné obnovy (ruční vložení).
Auditing	Logy řešení musí být externě ukládány ve formátu se stanovenou strukturou a významem dat – dokumentace formátu a možnost jeho strojového zpracování je veřejně dostupná.	Textový výstup je nezbytný pro budovaný systém SIEM.
Migrace dat	Po provedení rozšíření bude důležitým a náročným okamžikem migrace dat. Na tuto operaci bude kladen zřetel a ČNB neumožní dlouhodobé odstávky. Podmínky pro provedení migrace dat jsou následující: 1) Migrační postup pro MS PKI 2008R2:	Prioritními požadavky jsou ochrana dat, minimalizace odstávek a minimalizace rizik plynoucích z přechodu (např. performance problémy). V nabídce musí být uvedeny navržené principy migrace a jejich dopady na nedostupnost dat.

	Musí být zajištěna možnost migrace/import klíčů stávající PKI bez nutnosti generace nových klíčů a certifikátů a reinstalace PKI. Zhotovitel zajišťuje migraci/import. Pokud bude nutné realizovat reinstalaci PKI pro testování, pak musí být také provedena zhotovitelem. Podmínkou realizace je zachování vrstvy MSCS v prostředí Windows a zachování stávajících dat. 2) Migrační postup pro ostatní aplikace (i v clusteru): Musí být zajištěna migrace/import stávajících dat aplikací bez nutnosti generace nových dat a bez změny konfigurace aplikací. Zhotovitel zajišťuje kompletní migraci. Podmínkou realizace je zachování stávajících dat.	
Provozní odstávky	Při instalaci SW vybavení a migraci dat musí být dodrženy následující podmínky: - odstávka pouze jednoho node clusteru (aplikačního) na nejvýše 8 hodin v běžné pracovní době - odstávka celého clusteru serveru (aplikačního) na maximálně 4 hodiny a to jen v době o víkendu - odstávka non-cluster serveru na nejvýše 4 hodiny dle významu serveru buď po pracovní době, nebo jen během víkendu Odstávky jsou možné jen po předchozí domluvě se zadavatelem!	
Opravy HW	Pro případ poruchy musí být HSM vybaveno funkcí, která v případě poruchy (tj. i ve vypnutém stavu) zajistí prokazatelné vymazání dat. V případě výměny samotných nosičů s daty ČNB bude postupováno následovně: - u nosičů s magnetickou vrstvou bude demontována elektronika a budou znehodnoceny v tzv. magnetické peci (degausser) a zhotovitel	Ochrana dat patří mezi klíčové požadavky ČNB. Pokud nebude možné prokazatelně zajistit vymazání dat, není možné HSM jako celek předat zhotoviteli k opravě mimo ČNB. Tento způsob oprav se týká všech nosičů, **které obsahují data ČNB** a současně na nich

	si je na své náklady vyzvedne následující pracovní den po výměně (snahou bude provést znehodnocení okamžitě po výměně, ale zejména pro lokalitu Zličín toto nelze zajistit); - magnetické nosiče, kde nebude možné elektronickou část demontovat, ČNB nevrací a zajistí jejich mechanické zničení. - ostatní nosiče ČNB nevrací a zajistí jejich mechanické zničení.	nedochází k jejich ztrátě dat při odpojení napájení (tedy veškeré technologie pevných disků, flash disků, čipových karet apod.) Znehodnocení nebo zničení zajišťují zaměstnanci objednatele.
Licencování	Není rozhodující forma licencování programového vybavení – SW (tj. zda jsou licence na server nebo na kapacitu). Zhotovitel však ve své nabídce musí uvést **veškerý** dodávaný SW včetně způsobu jeho licencování a včetně počtu dodávaných kusů. Součástí dodávky budou i veškeré licenční podmínky a případné licenční klíče.	Licence musí pokrýt minimální požadované množství serverů viz příloha č. 4 a minimální počet slotů (viz „Kapacita a prostor pro data") a pracoviště 2 programátorů (SDK).

Omezení

A) *Technická omezení*

V rámci implementace (realizace) musí zhotovitel dodržet standardy ČNB a současně musí respektovat současnou infrastrukturu tak, aby nedošlo ke změnám, které by mohly ovlivnit funkčnost systémů ČNB.

Jedná se zejména o specifikace uvedené v popisu současného stavu, standardech ČNB, kompatibilitu řešení se stávajícími technologiemi (příloha č. 4), dodržení požadovaných funkcí a vlastností a zajištění dostatečné bezpečnosti.

B) *Dopad na IS a servery*

Navržené řešení nesmí mít negativní dopad na vlastní IS a servery na kterých běží, tj. zvýšení jejich zátěže z pohledu CPU, RAM, síťových interface apod. Vzhledem k tomu, musí být striktně dodrženy definované parametry viz „Striktně vyžadované funkce a vlastnosti".

Z hlediska výkonnosti musí nové řešení zajistit minimálně stejné odezvy (při realizaci podpisu nebo dešifrování) jako jsou v současné době, aby nedošlo ke zpomalení provozovaných IS.

C) *Zachování stávajícího stavu aplikací/IS*

Stávající aplikace/IS nebudou přeprogramovány a budou i nadále používat současná volání služeb HSM modulu (PKCS11) a maximálně budou upravena konfiguračně, že mohou volat jiný HSM modul (jiný hostname apod.).

Příloha č. 5

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 subjektu 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. 7

Podrobný rozpis ceny plnění (v Kč bez DPH)

				Cena v Kč bez DPH
1. etapa				165 800,00
2. etapa				118 900,00
z toho	dodávka HW			0,00
	dodávka SW			0,00
	implementace			102 900,00
		Počet dní (1 den = 8 hod.)	Cena v Kč bez DPH za 1 den	
	školení zaměstnanců	1	16 000,00	16 000,00
3. etapa				154 900,00
4. etapa				64 900,00
		Cena za 1 hodinu v Kč bez DPH		
Plnění na výzvu podle čl. V odst. 4 návrhu smlouvy		2 000,00		
		Cena za 1 měsíc v Kč bez DPH		
Paušální cena za podporu technických a programových prostředků		44 100,00		
		Cena za jeden výjezd v Kč bez DPH		
Cena za výjezd při plnění na výzvu		2 000,00		

Příloha č. 8

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

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

1. ÚVOD

1.1. Účel dokumentu

[Dokument realizační studie popisuje způsob realizace, aktivace a následného provozu služby včetně analýzy funkčních požadavků, softwarové architektury a systémových požadavků tak, aby byla prokázána realizovatelnost všech objednatelem zadaných požadavků. ***Text kurzívou v hranatých závorkách je návodem, neměl by zůstat součástí výsledného dokumentu.]***

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. REALIZACE VĚCNÉHO ZADÁNÍ

2.1. Analýza procesů

[Kapitola obsahuje analýzu procesů spojených s používáním nyní implementovaného řešení HSM modulů v prostředí Objednatele a jejich převod/změnu pro nově implementované HSM moduly provozované v QSCD režimu. Pro jejich grafické znázornění lze použít například UML Activity diagram, nebo BPMN (Business Process Model and Notation), dále diagramy typu MS Visio apod.].

2.2. Analýza funkčních a procesních požadavků

[Kapitola obsahuje mapování požadavků na cílové řešení – viz příloha č. 4 návrhu smlouvy („Technická a funkční specifikace předmětu plnění"). Popis tak ve stručné formě představuje způsob realizace jednotlivých požadavků.]

ID[1)]	Popis požadavku	Název funkcionality	Poznámka / jak bude realizováno

3. TECHNICKÁ REALIZACE ŘEŠENÍ

3.1. Integrace s IS ČNB

[Kapitola obsahuje:

- *popis možností integrace řešení HSM modulů provozovaných v QSCD režimu s jednotlivými stávajícími a budoucími (projektovanými) IS ČNB,*
- *detailní popis rozhraní pro komunikaci s IS ČNB.]*

3.2. Migrace dat

[Kapitola obsahuje analýzu přechodu z původního zapojení a provozu HSM modulů a nově projektované zapojení 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 poskytovatel.]

3.3. Bezpečnost

[Kapitola obsahuje popis řešení z hlediska bezpečnosti, integrity a důvěrnosti dat, relevantní normy, politiky a standardy, vnitřní předpisy Objednatele.]

3.3.1. Analýza bezpečnostních požadavků

[Podkapitola obsahuje analýzu bezpečnostních požadavků.]

3.3.2. Autentizace a autorizace, řízení přístupu

[V podkapitole je popsán princip řízení přístupů k informacím resp. informačním aktivům nové řešení HSM modulů v QSCD režimu: 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.]

[1)] ID požadavku objednatele ze zadávací dokumentace případě identifikace části smlouvy, kde se požadavek nachází.

3.3.3. Logování

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

3.3.4. Zabezpečení síťové komunikace a uložených dat

[V podkapitole je popsán způsob, jak je zabezpečena síťová komunikace mezi HSM moduly a klientskými informačními systémy a zabezpečení uložených dat – FileSystem/DataBase/jiné.]

3.3.5. Soulad s legislativou (Compliance)

[V podkapitole je popsán způsob, jak je zabezpečen soulad s legislativou – např. ZoKB, ISO20022, eIDAS apod. V případě, že navrhované řešení nebude splňovat nějaké legislativní požadavky, uvede se to v této kapitole včetně zdůvodnění proč.]

3.4. Návrh architektury technického řešení

[Kapitola popisuje globální architekturu řešení HSM modulů v QSCD režimu a fyzickou architekturu nasazení řešení v infrastruktuře ČNB s ohledem na provoz, high-availability, monitoring, zálohování a archivaci.]

3.4.1. Požadavky na systémové prostředí

[Podkapitola obsahuje SW a HW specifikaci pro nasazení v prostředí ČNB. Součástí je i sizing HW prostředků pro účely implementace. Různá prostředí provoz/test/vývoj/školení/atd. jsou popsána zvlášť.]

Tabulka 1: HW specifikace

Prvek	Typ	Výkon	RAM	Disková kapacita	Síťové rozhraní	Poznámka
APP1	*Virtuální server*	*2 – 4 virtuální CPU, 2 – 3 GHz*	*4 – 8 GB*	*15 GB*	*100 Mbps*	

Tabulka 2: SW specifikace

Prvek	OS	Databázové služby	Aplikační služby	Poznámka
APP1	*Windows Server 2008 R2 ENG x64*	*Oracle client 10g*	*MS IIS 7.5 ASP.NET 3.5 SP1*	

3.5. Způsob implementace do systémového prostředí ČNB

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

4. Návrh projektové realizace

4.1. 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 díla nebo jeho části k akceptačnímu řízení.]*

4.2. Požadavky na součinnost (*pro externí dodávku)*

[V kapitole je uveden rozsah kapacit požadovaných poskytovatelem 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

4.3. Akceptační testy

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

ID testu	Testovaná oblast	Testovací scénář	ID požadavku[2)]	Testovací scénář vypracovává

Legenda:
ID scénáře: jedinečný identifikátor testovacího scénáře
Testovaná oblast: oblast testování např.: Komunikace s IS na Oracle Linux, ...
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

4.4. Školení

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

4.5. Dokumentace

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

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

5. Popis režimu provozní podpory

[Kapitola detailněji popisuje způsob zajištění provozní podpory. Jedná se například o konkretizaci kontaktních bodů podpory a kontaktního místa pro dodávku náhradního HSM modulu. Dále o případnou doplňkovou diagnostiku a mechanizmu uzavření řešení závady.]

6. 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. 6

5. NÁVRH TECHNICKÉHO ŘEŠENÍ

Tato kapitola obsahuje návrh realizace nabízeného řešení včetně zajištění služeb dostupnosti, ověřovacího provozu i provozu v režimu kvalifikovaného prostředku dle nařízení eIDAS.

Vlastní řešení lze rozdělit na následující části:

- **Zpracování úvodní realizační studie (1. etapa)**
- **Vytvoření ověřovací konfigurace na jednom HSM modulu včetně ověření migrace případných klíčů v režimu QSCD**
- **Vytvoření ostré konfigurace a migrace na QSCD pro všechna HSM**
- **Zajištění podpory a údržby pro všechna zařízení včetně provozu jako kvalifikovaného prostředku pod správou QTSP Postsignum**

Vybrané body jsou níže podrobněji popsány.

5.1. Zpracování realizační studie – 1. etapa

Realizační studie, která bude vypracována v rámci 1. etapy projektu, bude sloužit především ke správnému plánování jednotlivých implementačních a migračních kroků, které jsou nezbytné pro plynulý přechod produkčního provozu na novou více striktní konfiguraci HSM modulů.

Mezi klíčové body studie bude patřit především:

- **Finální konfigurace všech HSM modulů**
- **Napojení jednotlivých klientů na HSM moduly v cílovém stavu**
- **Způsob provedení ověřovací konfigurace včetně ověřovacího provozu a ověřovací migrace (pokud bude nutná)**
- **Podrobný harmonogram jednotlivých kroků a požadavky na součinnost**
- **Popis testů pro ověření správného chování**
- **Popis omezení provozu HSM modulů jako QSCD oproti současnému stavu**
- **Postup získávání a obnovy certifikátů v novém režimu kvalifikovaného prostředku**

Na základě akceptované realizační studie budou podrobně rozplánovány jednotlivé implementační kroky a odpovědnosti včetně součinnosti systémů, které budou vybrány pro ověřovací provoz.

5.2. Vysoká dostupnost

Vzhledem k tomu, že musí být v cílovém stavu HSM moduly provozovány v režimu QSCD, což znamená pod správou kvalifikovaného poskytovatele, je nutné, aby veškeré změny konfigurace a uvedení do provozu prováděli pouze k tomu pověření pracovníci. Vybraní pracovníci SEFIRA jsou k tomu ze strany QTSP Postsignum oprávněni na základě smlouvy jako správně vyškolení a vybavení pracovníci externí registrační autority.

Z těchto důvodů pro zajištění požadované dostupnosti bude umožněno nastavit klíčové aplikace tak, aby mohly používat všechny dostupné HSM moduly. V případě výpadku jednoho z HSM bude pro tyto kritické aplikace vždy k dispozici další HSM modul bez nutnosti změny konfigurace.

V případě, kdy nebudou všichni klienti napojeni na všechny HSM moduly, bude možné zbývající přístupové licence použít pro nové aplikace. Upřesnění konfigurace klientů bude popsáno v realizační studii.

5.3. Příprava přechodu a ověřovací provoz

Vlastní ověřovací konfigurace bude vytvořena na HSM modulu, který je využíván jako náhradní. Tato konfigurace (nový SecurityWorld) nebude nijak ovlivňovat stávající produkční provoz ve vysoké dostupnosti.

Nad touto novou ověřovací konfigurací bude realizováno především:

- Proces vlastní konfigurace HSM jako QSCD v prostředí ČNB
- Migrace klientského SW na požadovaných platformách
- Proces generování klíčů a certifikátů v režimu QSCD
- Migrace vybraných klíčů (např. CA)
- Změny v administraci z důvodů provozu v režimu FIPS 140-2 Level 3 a provozu pod správou QTSP
- Školení pracovníků správy v nové konfiguraci včetně upravených plánů obnovy

V rámci realizační studie budou upřesněny další technické parametry související s tímto ověřovacím provozem jako jsou IP adresy, zapojené systémy, požadavky na testovací certifikáty apod.

Po ukončení ověřovacího provozu může být tato ověřovací konfigurace smazána a znovu vytvořena, nebo může být zachována, neboť bude již od počátku prováděna pod správou QTSP. Rozhodnutí bude provedeno v rámci přípravy realizační studie.

5.4. Provoz HSM modulů v režimu kvalifikovaného prostředku

Vzhledem ke specifickým podmínkám certifikace nabízených HSM modulů od společnosti Thales je pro jejich využití jako kvalifikovaného prostředku nutné zajistit, aby správa a provoz zařízení byly zajištěny prostřednictvím kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Pro účely dodávky nabízeného řešení zajišťuje správu a provoz HSM modulů společnost SEFIRA na základě smlouvy o zajištění služeb externí registrační autority s Českou poštou, s. p. jako kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Předmětem nabízených služeb zajištění správy a provozu QSCD je

- smluvní zajištění správy s kvalifikovaným poskytovatelem důvěryhodných služeb (QTSP);
- registrace QSCD a administrativní zajištění správy zařízení;
- servisní služby spojené se zajištěním správy HSM modulů jako QSCD v rozsahu max. 4 MD za rok;
- garance poskytnutí služeb v dohodnuté kvalitě;
- dopravné v rámci Hlavního města Prahy.

Reakční doba pro poskytování služeb je 2 pracovní dny od nahlášení požadavku na servisní podporu.

5.5. Provedení migrace, dokumentace a požadované odstávky

Po úspěšném ověřovacím provozu bude 1 HSM modul přepojen do nové konfigurace kvalifikovaného prostředku a jednotlivé aplikace budou postupně přepínány/migrovány na novou konfiguraci.

Paralelně s tímto stavem bude k dispozici stávající produkční konfigurace HSM v HA variantě (1 stávající a 1 zapůjčený) a nebude tedy ohrožen provoz kritických systémů.

Po překlopení všech klientů bude provedena rekonfigurace druhéhoHSM modulu a budou vytvořeny finální konfigurační soubory pro jednotlivé klienty dle návrhu cílové konfigurace popsané v realizační studii.

Výsledný stav bude zanesen do aktualizované dokumentace, kde změny budou zohledňovat především změnu v rozdělení odpovědnosti za správu HSM modulů a klientů, striktní provoz v režimu QSCD a nový model zajištění vysoké dostupnosti (podpora 2 současně dostupných HSM modulů).

Odstávky budou naplánovány v realizační studii. Instalace příslušného klientského SW a jeho konfigurace vyžaduje odstávku zhruba 1 hodinu, pokud jsou provedeny potřebné přípravné práce. U více uzlových clusterů je možné provádět tyto kroky nezávisle na po jednotlivých uzlech. Prvotní instalace vyžaduje restart dotčeného serveru.

5.6. Funkce a vlastnosti řešení

Požadavek	Popis splnění požadavků
Dostupnost	HSM moduly jsou rutinně používány v mnoha bankách a certifikačních autoritách. Budou implementovány celkem 2 HSM moduly a každý modul má redundantní zdroje napájení, ventilátory i síťové rozhraní.
Spolehlivost	Síťové HSM moduly Thales jsou navrženy pro provoz 24x7. Zároveň princip tzv. Security Worldu a příslušných sad čipových karet pro správce (ACS) resp. vlastníky klíčů (OCS) umožňují nahradit existující HSM modul novým zařízením, jednoduše do něj dohrát příslušnou konfiguraci a zpřístupnit mu potřebné klíče. Na straně klientských serverů se následně jedná o drobnou změnu v konfiguračním souboru.

	Každý klient bude mít standardně nastaven přístup ke všem aktivním HSM modulům, které využívá paralelně. V případě poruchy jednoho HSM modulu bude tedy pro klienty vždy přístupný zbývající 1 HSM modul.
Režim vysoké dostupnosti	Každý klient může mít standardně nastaven přístup až ke 2 aktivním HSM modulům, které využívá paralelně. Zpřístupňování klíčů pro HSM je iniciováno ze strany klientů (vlastních serverů) a pomocí centrální komponenty Remote File Systém (RFS) je možné zajistit jejich sdílení na jednotlivé uzly aplikačních clusterů. V případě umístění HSM modulů v různých lokalitách bude zajištěna i nezávislá geografická dostupnost.
Zabezpečení dat	Každý klient bude mít standardně nastaven přístup minimálně ke dvěma aktivním HSM modulům, které využívá paralelně. Klíčový materiál bude vždy zabezpečen pomocí HSM modulu a příslušných operátorských oprávnění, realizovaných buď formou sady fyzických čipových karet, nebo pomocí virtuální SW karty a vždy chráněných heslem. Jednotlivé objekty jsou v šifrované podobě dostupné v rámci komponenty RFS nebo jednotlivých serverů a je možné provádět běžné zálohování. Pokud bude nastaveno používání operátorských setů s fyzickými čipovými kartami v režimu 2 nebo více z N, bude třeba vždy 2 nebo více správců pro zpřístupnění klíčů a to pouze v rámci dané skupiny HSM modulů. V jiných HSM modulech není možné tyto klíče obnovit.
Zabezpečení proti úniku dat	Klíčový materiál bude vždy zabezpečen pomocí HSM modulu a příslušných operátorských oprávnění, realizovaných buď formou sady fyzických čipových karet, nebo pomocí virtuální SW karty a vždy chráněných heslem. Bez těchto prvků není možné získat přístup k vlastním klíčům. Pokud je HSM vypnuto, neobsahuje žádné klíče, které by mohly být aktivně využity. Vždy je při jejich zpřístupnění vyžadováno poskytnutí příslušných operátorských oprávnění.
Ochrana investic	Síťové HSM moduly Thales nabízí podporu pro širokou paletu operačních systémů a zároveň nabízí širokou škálu rozhraní využitelných v jednotlivých prostředích. Úplný přehled podporovaných systémů je uveden v přiloženém produktovém listu v příloze. Vzhledem k nutnosti používat striktní certifikovanou verzi software a firmware nemusí být okamžitě k dispozici podpora nejnovějších verzí operačních systémů.
Připojení	HSM moduly disponují 2 síťovými rozhraními pro duální zapojení do dvou fyzických sítí.
Množství připojených serverů	Modely Thales nShield Connect 1500+ podporují připojení až 20 různých serverů současně. Provozovaná infrastruktura (stávající i nové HSM) obsahují licenci pro přístup 16 serverů ke každému HSM modulu.
Kapacita a prostor pro data	Vzhledem k používané architektuře a principům Security Worldu je možné pro HSM zpřístupnit téměř neomezené množství klíčů. Vytváření jednotlivých operátorských setů nebo virtuálních SW karet s heslem representuje v požadované terminologii slot. Počet těchto objektů (OCS a softkarty) není omezen. V případě klíčů v režimu QSCD je možné jeden ochranný prvek (OCS, softkartu) použít pouze pro jeden klíčový pár.

Kapacitní rozšiřitelnost	HSM moduly umožňují licenční rozšíření až na maximální počet 20 současně připojených serverů (klientů) ke každému HSM moduly. Rozšiřitelnost na počet klíčů je dána automaticky z architektury HSM modulů.
Výkonnost	Výkonnost garantovaná výrobcem je pro HSM moduly Thales nShield Connect 1500+ uvedena v přiloženém produktovém listu v příloze. Aktuální výkonnost pro RSA klíče o délce 2014 bitů je 1500 operací za sekundu.
Výkonnostní rozšiřitelnost	Aktuální výkonnost pro RSA klíče o délce 2014 bitů je 1500 operací za sekundu, a tudíž vyhovuje potenciálnímu požadavku na výkon 1200 operací za sekundu.
Operace s HSM	Vytváření nových slotů (operátorský set nebo virtuální SW karta) neovlivňuje provoz ostatních aplikací. Každá aplikace může využívat jeden nebo více slotů v závislosti na architektuře a požadavcích dané aplikace. Různé aplikace provozované na jednom serveru mohou používat různé sloty. Jeden slot může být sdílen více aplikacemi na různých serverech. Vše je záležitost návrhu struktury slotů a bezpečnostních politik organizace.
Homogenita	Pro každou lokalitu se předpokládá použití stejného HSM modulu včetně nového náhradní zařízení. Každý server může využívat všechny sloty bez omezení a také všechny moduly (v závislosti na konfiguraci klienta – na straně klienta je možné zpřístupnit pouze jeden, dva nebo všechny HSM moduly). Je možné privilegovat vybraného klienta pro provádění vzdálených administračních zásahů, pokud bude vyžadováno. Typicky se může jednat o nutný pomocný server RFS.
Ladění výkonnosti/přesun zpracování na jiný HSM	Klientský SW ve spolupráci s příslušným aplikačním rozhraním automaticky rozkládá zátěž na všechny klientovi přístupné HSM moduly a v případě výpadku jednoho z modulů automaticky směruje zátěž na zbývající nakonfigurované moduly. Pro vybraná rozhraní je možné definovat preference využívaného HSM modulu.
Kompatibilita s prostředím ČNB	HSM moduly Thales nShield Connect 1500+ podporují všechny platformy provozované v rámci infrastruktury ČNB.
Kompatibilita aplikací	MS PKI 2008 R2 bude využívat poskytnutého MS CNG security providera. Aplikace v prostředí Linux/MS Windows mohou využívat rozhraní PKCS#11, Java JCE providera nebo MS CAPI/CNG providera. Dále je k dispozici nativní API pro maximální využití vlastností nabízených HSM modulů.
Kompatibilita serverů	Nabízené řešení obecně podporuje všechny požadované operační systémy a virtualizační platformy v závislosti na použité verzi klientského SW (verze 11.x a 12.x). V případě požadavku na využívání HSM modulu jako kvalifikovaného prostředku je pro klienta certifikováno použití pouze verze klientského SW 11.72.02, která je kompatibilní s následujícími verzemi OS: • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 x64 • Microsoft Windows 7 IA-32/x64 • Red Hat Enterprise Linux AS/ES 6 x86/x64

	• Red Hat Enterprise Linux AS/ES 5 x86/x64 Prakticky máme ověřeno, že tuto verzi je možné instalovat i do prostředí Windows Server 2016, ale vzhledem k požadavku na certifikaci toto nedoporučujeme. Instalaci s nejnovějšími verzemi OS Linux nemáme vyzkoušenu.
Rozhraní pro programátory a aplikace	Nabízené řešení podporuje všechna požadovaná aplikační rozhraní včetně příslušné dokumentace. Blíže viz přiložený produktový list v příloze.
Základní funkce	Tato funkcionalita podporována jak pomocí standardně dodaných nástrojů, tak i pomocí obvyklých utilit využívajících příslušné aplikační rozhraní. Rovněž je podporován import klíčového páru včetně certifikátu, pokud nejsou HSM moduly v restriktivním FIPS 140-2 Level 3 režimu. Provozované HSM moduly jsou uvedeny na seznamu kvalifikovaných prostředků jako položka *„nShield Connect 500, nShield Connect 500+, nShield Connect 1500, nShield Connect 1500+, nShield Connect 6000, nShield Connect 6000+"* v sekci pro Itálii. Provoz v režimu QSCD zajišťujeme jménem QTSP Postsignum na základě smlouvy a dle podmínek QTSP.
Množina podporovaných kryptografických algoritmů	Výčet podporovaných algoritmů je uveden v přiloženém produktovém listu v příloze.
Autentizační mechanismus	Aby mohl server (klient) využívat služeb HSM modulů musí být tento klient registrován na každém požadovaném HSM modulu a zároveň musí v rámci klientského SW obsahovat konfiguraci s informací o všech jemu dostupných HSM modulech. Na základě těchto údajů je vytvořeno důvěryhodné spojení mezi serverem a vlastním modulem. Následně je pro přístup ke klíčům vyžadováno zpřístupnění požadovaného počtu čipových karet (OCS – každá může být chráněna různým alfanumerickým PINem) nebo pomocí virtuální SW karty vždy chráněné heslem. Pro splnění požadavku na jeden autentizační údaje je pro případ využívání OCS požadováno nastavení stejného PINu pro všechny čipové karty z daného OCS. Obdobně je pro vybrané administrátorské operace požadováno zpřístupnění příslušných administrátorských čipových karet (ACS – opět každá karty s různým alfanumerickým PINem).
Zabezpečení proti infiltraci a odposlechu komunikace	Mezi klientským SW na straně serveru (klienta) a jednotlivými HSM moduly je vždy navázáno nezávislé šifrované spojení, pro které dochází automaticky v nastavených intervalech (čas, přenesený objem dat) ke změně použitých šifrovacích klíčů. Pro tuto komunikaci se používá proprietární protokol výrobce a není možné přistupovat k funkcím HSM jinak než prostřednictvím tohoto kanálu.
Bezpečnostní certifikace	HSM moduly Thales nShield Connect 1500+ disponují požadovanými certifikacemi a vždy bude nasazena certifikovaná verze FW. Informace o certifikaci jsou uvedeny v přiloženém produktovém listu v příloze a lze je ověřit přímo u jednotlivých certifikačních organizací.

Systém provozu	Nabízené řešení standardně funguje v režimu active-active a klienti využívají rovnoměrně všechny jim dostupné HSM moduly.
Duální připojení serverů	Nabízené řešení standardně funguje v režimu active-active a klienti využívají rovnoměrně všechny jim dostupné HSM moduly.
Dopad na provoz serverů	Klientský SW na straně aplikačních serverů vyžaduje pouze minimální zdroje na provoz a údržbu spojení s HSM moduly a nepřesahuje požadované limity.
Zátěž komponent síťového prostředí ČNB	Vzhledem k tomu, že jsou typicky vůči HSM komunikovány pouze velmi malé objemy dat (hashe dokumentů k podpisu, podpisy k ověření), negeneruje toto použití významné zatížení sítě. Výjimkou by mohlo být, pokud by byly HSM moduly používány pro šifrování/dešifrování dat; v tomto případě může docházet ke zvýšení zatížení sítě v závislosti na objemu šifrovaných/dešifrovaných dat.
Rozměry a chlazení	HSM moduly respektují montáž do standardních racků. HSM moduly jsou standardní 1U zařízení s hloubkou 705 mm. Maximální tepelné vyzařování při plné zátěži dosahuje hodnot 327 až 362 BTU/h. Blíže viz přiložený produktový list v příloze.
Napájení	Maximální požadovaný příkon HSM modulů je pouze 0,6A při napájení 230V. Blíže viz přiložený produktový list v příloze.
Diagnostika	HSM moduly automaticky monitorují svůj stav a prostřednictví logů ukládaných na server RFS a prostřednictví SNMP umožňují automatizaci dohledu nad provozem HSM modulů. Další informace o stavu zařízení je možné získat prostřednictvím dodaných administračních nástrojů nebo přímo na předním panelu jednotlivých HSM modulů.
Dohledový nástroj/skript	Pro účely dohledu bude využíváno management serveru RFS, který kromě role ukládání konfigurace a logů z HSM modulů umožňuje propagaci SNMP informací a zároveň obsahuje potřebné administrační nástroje a utility pro správu a monitoring HSM modulů. Alternativně je možné nastavit logování pomocí syslogd démona na vzdálený server.
Konfigurační změny	Vybrané konfigurační změny na straně HSM modulů je možné realizovat pomocí displeje a ovládacích prvků na předním panelu, pomocí změn konfigurace v konfiguračních souborech na RFS a uploadu změněné konfigurace do HSM nebo pomocí dílčích administračních nástrojů rovněž dostupných na management uzlu RFS. V případě provozu HSM modulů v režimu kvalifikovaných prostředků (QSCD) je změny konfigurace HSM modulů oprávněn provádět pouze zástupce QTSP. V případě konfigurace klientů probíhá konfigurace na straně provozovatele.
Manipulace v clusteru-funkčnost clusteru	Při standardní konfiguraci jsou všechny HSM využívány rovnoměrně a při detekci nedostupnosti jednoho z modulů, je zpracování směrováno na zbývající uzly. Role všech HSM jsou ekvivalentní. Alternativně lze přístup k jednotlivým modulům řešit změnou konfigurace na klientech (serverech), zde je ale vyžadován manuální zásah správce, pokud by aplikace standardně komunikovala pouze s jedním HSM (pokud by nebyla v režimu vysoké dostupnosti).

Řídící komunikace a ovládání	Pro komunikaci mezi HSM moduly a jednotlivými klienty včetně management serveru RFS využívají vlastní zabezpečený protokol využívající standardní porty 9000 resp. 9001. K dispozici jsou jak řádkové utility, tak i grafická Java administrační konzole.
Zálohování konfigurace	Zálohování konfigurace se řeší pomocí souborové zálohy vybraných souborů na centrálním management RFS serveru. Podrobnosti budou uvedeny v dokumentaci.
Auditing	Logování činnosti a operací je primárně logováno v HSM modulu a následně v pravidelných (nastavitelných) intervalech ukládány na centrální RFS server. Tyto logy jsou v textovém formátu bez ohledu na platformu RFS (Windows/Linux). Logy jednotlivých klientů HSM včetně RFS jsou na platformě Linux/UNIX ukládány v souborovém systémy, a na platformě MS Windows jsou záznamy uloženy v Event Logu.
Migrace dat	Migrační postupy budou detailně popsány v implementační dokumentaci vytvořené v rámci první etapy projektu. Pro migraci MS certifikační autority není třeba počítat s reinstalací stávající autority a jejím obnovením pomocí HSM úložiště (data zůstanou nedotřena), a realizaci bude. Migrace klíčů ostatních aplikací se bude lišit podle toho, zda se bude jednat o klíče pro kvalifikované pečeti (ty se musí vždy vygenerovat nové v nové konfiguraci podle specifických pravidel QTSP) nebo pro ostatní účely – v rámci studie bude rozhodnuto o migraci nebo novém vytvoření.
Provozní odstávky	Pro potřeby napojení klienta (serveru) vyžaduje instalace příslušného klientského SW a jeho konfigurace zhruba 1 hodinu, pokud jsou provedeny potřebné přípravné práce. U více uzlových clusterů je možné provádět tyto kroky nezávisle na po jednotlivých uzlech. Prvotní instalace vyžaduje restart dotčeného serveru.
Opravy HW	Vybrané opravy HSM modulu je možné provést na místě (výměna zdroje, výměna ventilátorů) a není třeba odvážet zařízení. V případě požadavku na opravu HSM modulu je navržena konfigurace, která neukládá žádné klíčové informace permanentně v HSM modulu. Bude-li to případná závada umožňovat, bude vždy před odpojením zařízení provedena jeho inicializace do výrobního nastavení z předního panelu, které znemožňuje práci a přístup s jakýmikoliv klíčovými informacemi.
Licencování	Licenční model společnosti Thales vyžaduje přístupové licence pro přístup určitého počtu klientů (serverů) ke konkrétnímu HSM modulu. Rovněž umožňuje pomocí aktivačních čipových karet aktivaci doplňkové funkčnosti HSM bez nutnosti jeho reinstalace, pokud by byla takováto funkčnost v budoucnu požadována.