SMLOUVA

o dodávce bezpečného úložiště klíčů, souvisejícího software včetně poskytování podpory

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

SEFIRA spol. s r.o.
Antala Staška 2027/77
140 00 Praha
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572
zastoupenou: Ing. Marián Juríkem, jednatelem
IČO: 62907760
DIČ: CZ62907760
(dále jen „zhotovitel")

a

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

Článek I.
Předmět plnění

1. Předmětem této smlouvy je povinnost zhotovitele dodat, nainstalovat a zprovoznit technické a programové prostředky pro ukládání a využití kryptografických klíčů v informačních systémech objednatele (dále jen HSM), vypracovat projektovou dokumentaci a zaškolit zaměstnance objednatele (dále též „dílo") a poskytovat záruční a pozáruční podporu dle této smlouvy. Technické a programové prostředky musí splňovat funkční požadavky uvedené v příloze č. 5 smlouvy. Předmět plnění musí být realizován v souladu s návrhem technického řešení obsaženým v příloze č. 7.
2. Plnění podle odst. 1 této smlouvy, vyjma poskytování záruční a pozáruční podpory, bude realizováno ve čtyřech etapách takto:
   a) **První etapa** zahrnuje vypracování realizační studie, která bude obsahovat veškeré informace nezbytné pro implementaci technických a programových prostředků do prostředí objednatele včetně mapování funkčních požadavků a vlastností uvedených v příloze č. 5 tak, aby byla prokázána jejich realizovatelnost.

      Součástí studie bude zejména (v závislosti na konkrétním návrhu řešení):

      - způsob zapojení do struktur objednatele;
      - konfigurace prostředků a zabezpečení;
      - popis zajištění dohledu/správy;

- postup migrace dat s důrazem na zachování kontinuity provozu;
- nároky na součinnost objednatele;
- testovací scénáře;
- harmonogram.

b) **Druhá etapa** zahrnuje dodávku technických a programových prostředků podle specifikace uvedené v příloze č. 1, instalaci technických prostředků a jejich implementaci do prostředí objednatele, zprovoznění zrcadlení, připojení nejméně 5 serverů objednatele a instalaci programových prostředků na tyto servery, instalaci SW pro management dodaných technických prostředků. Dále zahrnuje konfiguraci minimálně 3 slotů, přiřazení k serverům, testovací provoz v délce 1 týdne zahrnující posouzení souladu navrhovaného řešení se zadáním podle testovacích scénářů, ukázky základních operací s HSM a zaškolení obsluhy (2 odborných zaměstnanců objednatele) v délce, kterou určí zhotovitel tak, aby zaměstnanci byli zaškoleni v rozsahu dle přílohy č. 2. Součástí plnění je i dodání dokumentace výrobce technických prostředků a programových prostředků.

c) **Třetí etapa** zahrnuje asistenci při konfiguraci dodaných technických prostředků dle specifických požadavků objednatele (asistence při vytváření dalších cca 7 slotů pro konkrétní systémy), provedení instalace programového vybavení na ostatní servery dle přílohy č. 4 a migraci dat dle přílohy č. 2 pro stávající aplikace objednatele. Dále zahrnuje školení programátorů (2 odborných zaměstnanců objednatele) v délce, kterou určí zhotovitel tak, aby zaměstnanci byli proškoleni v rozsahu dle přílohy č. 2, ještě před provedením migrace. Po kompletní konfiguraci a migraci bude proveden zkušební provoz v délce 2 týdnů, během kterého bude ověřeno, zda dodané řešení splňuje veškeré požadavky objednatele uvedené v příloze č. 5, a provedeno měření významných provozních stavů dodaného řešení a případně návrh optimalizace;

d) **Čtvrtá etapa** zahrnuje vypracování projektové dokumentace, v níž bude zachycen popis konečného stavu a provozních postupů a jejíž součástí bude i havarijní plán. Seznam požadované dokumentace je uveden v příloze č. 2. Zhotovitel je povinen předat objednateli projektovou dokumentaci v elektronické podobě ve formátu MS Word 2003-2007/2010, včetně dokumentace všech verzí software, resp. firmware.

3. Zhotovitel bude zajišťovat buď průběžně, nebo v rámci určité etapy činnosti uvedené v příloze č. 2.
4. Zhotovitel se zavazuje poskytovat pro dodané technické a programové prostředky záruční a pozáruční podporu dle čl. V této smlouvy.
5. Zhotovitel podpisem této smlouvy prohlašuje a stvrzuje, že řešení splňuje veškeré požadavky vyplývající pro něj z přílohy č. 5.
6. Objednatel se zavazuje za poskytnutá plnění uhradit ceny dle čl. III této smlouvy.

Článek II.
Lhůty, místo a 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) 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 6 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 10 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 1 týdne bude realizován jako poslední činnost druhé etapy;
   c) třetí etapa bude zhotovitelem dokončena nejpozději do 15 týdnů od podpisu smlouvy. Termíny školení odborných zaměstnanců objednatele dohodnou smluvní strany podle realizační studie, školení musí proběhnout před migrací dat. Zkušební provoz v délce 2 týdnů bude probíhat po kompletní konfiguraci a migraci. V posledním týdnu zkušebního provozu bude provedeno měření, na jehož základě zhotovitel vypracuje návrh optimalizace;
   d) čtvrtá etapa zahrnující dokumentaci specifikovanou v příloze č. 2 bude končena do 17 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. Lhůty uvedené v odst. 2 tohoto článku mohou být změněny na základě dodatku ke smlouvě.
4. 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.
5. Akceptaci s výhradami nelze provést, pokud existuje alespoň 1 podstatná vada. Podstatné vady jsou vady, které způsobují tak závažné problémy, že objednatel nemůže produkt 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.
6. 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.
7. Místem plnění budou prostory výpočetního střediska v objektech objednatele na adrese Praha 1, Senovážná ul. 3 a Praha 5, Strojírenská 175.

8. 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.

9. 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 7 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 2 423 698,- Kč, z toho cena zaškolení dle čl. I odst. 2 písm. b) 14 400,- Kč a cena školení dle čl. I. odst. 2) písm. c) této smlouvy činí 14 400,- Kč. Podrobnější rozpis ceny je obsažen v příloze č. 1 smlouvy.

3. Cena za provozní údržbu podle čl. V odst. 3 této smlouvy bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby, která činí 1 800 Kč bez DPH. K ceně prací je zhotovitel oprávněn účtovat kilometrovné ve výši 8 Kč/km.

4. Paušální cena za pozáruční podporu technických prostředků a programových prostředků, které jsou nedílnou součástí technických prostředků podle čl. V odst. 2 této smlouvy, činí měsíčně 28 064,- Kč.

5. 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 zálohy ve výši ceny za 1. etapu stanovené podle přílohy č. 1 této smlouvy nejdříve v den podpisu dílčího akceptačního protokolu za 1. etapu;

   ii. Zhotovitel je oprávněn vystavit doklad na úhradu zálohy ve výši ceny za 2. etapu stanovené podle přílohy č. 1 této smlouvy nejdříve v den podpisu dílčího akceptačního protokolu za 2. etapu;

   iii. Daňový doklad na cenu díla je zhotovitel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu o předání a převzetí díla;

   iv. V daňovém dokladu na cenu díla bude vyúčtována poskytnutá záloha.

7. Cena za provozní údržbu podle odst. 3 tohoto článku bude hrazena na základě daňového dokladu vystaveného nejdříve po poskytnutí služby.

8. Paušální cena podle odst. 4 tohoto článku bude hrazena měsíčně na základě jednoho 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. Každý doklad k úhradě vystavený v souvislosti s touto smlouvou bude vedle náležitostí stanovených v § 435 občanského zákoníku a podle zákona o DPH obsahovat i evidenční číslo smlouvy ČNB. V případě, že daňový doklad 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. 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 dodavatel 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.

10. Splatnost dokladů k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch zhotovitele.
11. Výše paušální ceny za období kratší, než je sjednané období, se vypočte jako alikvotní část sjednané ceny.
12. 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.
13. 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 paušální ceny podpory programových prostředků dle odst. 4 toto článku může zhotovitel navrhnout po uplynutí dvou let od zahájení poskytování podpory.
14. Smluvní strany se ve smyslu § 1991 občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za zhotovitelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce zhotovitele za objednatelem, ať splatné či nesplatné.

Článek IV.
Součinnost, 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. 5, 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 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

- za zhotovitele: Petr Dolejší, tel.: 222 558 111, email: dolejsi@sefira.cz

3. Zhotovitel prohlašuje, že technické i programové prostředky, které jsou předmětem plnění podle této smlouvy, pochází od certifikovaného/autorizovaného distributora a poskytovatele technické podpory pro Českou republiku 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 7.4.1 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 subdodavatele platí všechna relevantní ustanovení tohoto článku také pro subdodavatele 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 subdodavatele, je povinen v případě změny tohoto subdodavatele na požádání objednatele prokázat, že nový subdodavatel tento požadavek splňuje, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.
6. Objednatel si vyhrazuje právo ověřit si skutečnosti dle odst. 3 až 5 tohoto článku. Nesplnění kteréhokoliv požadavku objednatele uvedeného odst. 3 až 5 je považováno za podstatné porušení smlouvy.

Článek V.
Záruční podmínky a podpora

1. Zhotovitel poskytuje objednateli na technické prostředky a na programové prostředky, které jsou nedílnou součástí technických prostředků (např. firmware/mikrokód, licence atd.), specifikované v příloze č. 1, záruku v délce 36 měsíců. Záruční doba běží ode dne podpisu protokolu o předání a převzetí plnění jako celku dle čl. II této smlouvy.
2. Podmínky pro záruční a pozáruční podporu technických a programových prostředků, které jsou nedílnou součástí technických prostředků:

   a) pro uskutečnění **servisního zásahu** techniků zhotovitele platí nepřetržitý režim, tj. technici zhotovitele budou k dispozici po dobu 24 hodin a 7 dnů v týdnu. Tento režim platí pro technické i programové prostředky;

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

   Za kritickou závadu se považuje taková závada, kdy kryptografické klíče nejsou dostupné nebo s nimi není možné realizovat digitální podpis a dešifrování (ověření podpisu) na úrovni operačního systému serveru alespoň v jedné z lokalit. Mezi kritické závady dále patří také:

   - nemožnost generovat klíčový pár v HSM a žádost o certifikát v obou lokalitách;
   - nefunkční zrcadlení mezi lokalitami, které není způsobené na komunikační trase zajišťované objednatelem;

- zásadní výkonnostní problémy.

Odstranění kritických závad musí být ukončeno do 6 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 první z redundantních komponent HSM.

Odstranění nekritické závady musí být ukončeno do 24 hodin od nahlášení.

d) při vzniku **nekritické závady programových prostředků** bude zahájeno řešení závady nejpozději do 2 hodin 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.

Podporu programových prostředků, které nejsou nedílnou součástí technických prostředků, nebude zhotovitel poskytovat, neboť dle jeho nabídky jsou veškeré nabízené programové prostředky nedílnou součástí technických prostředků dle odst. 2 tohoto článku.

3. Součástí podpory technických a programových prostředků je i jejich provozní údržba. Provozní údržba technických a programových prostředků zahrnuje 1x za čtvrtletí kontrolu funkce všech HSM modulů včetně kontroly logů na zařízeních samotných a na klientech. Na základě provedené analýzy a připomínek objednatele pak naplánování a realizace případného zásahu nebo úprav. Dále zahrnuje činnosti realizované na výzvu objednatele, zejména se jedná o asistenci při generování párů klíčů, provedení jejich zrcadlení a zálohování nových sad klíčů.
4. Zhotovitel v rámci zajištění záruční a pozáruční podpory poskytne nové a opravné verze všech dodaných programových prostředků včetně jejich implementace. Součástí podpory je také:
   - informování objednatele o nových nebo opravných verzích;
   - konzultace k plánovaným změnám;
   - aktualizaci konfigurace a dokumentace, pokud na ni bude mít implementace vliv
5. Pokud závadu zjistí zhotovitel, oznámí ji neprodleně objednateli a další postup se řídí ustanoveními tohoto článku.
6. Zhotovitel je srozuměn s tím, že veškerá komunikace při hlášení a řešení závad bude mezi objednatelem a pracovníky zhotovitele probíhat v českém jazyce.
7. Služby poskytované zhotovitelem musí vyhovovat technickým specifikacím a požadavkům výrobce příslušného technického prostředku.
8. Požadavky na odstranění závad a na ostatní služby podle této smlouvy budou předávány způsobem uvedeným v příloze č. 3 této smlouvy. Kritické závady objednatel současně oznámí telefonicky. Přijetí požadavku na servisní zásah je zhotovitel povinen potvrdit e-mailem na adresu osob uvedených v příloze č. 3 nejpozději do 2 hodin od přijetí požadavku.

9. O každém provedeném servisním zásahu nebo údržby vyhotoví pracovník zhotovitele zápis o provedení práce, který stvrdí svým podpisem přejímající pracovník objednatele.
10. Záruka se nevztahuje na vady, které byly prokazatelně způsobeny objednatelem, vyšší mocí anebo byly způsobeny užíváním nebo obsluhou v rozporu s technickými podmínkami uvedenými v dodané uživatelské dokumentaci.
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 nedostupnosti ani jednoho z kontaktů zhotovitele uvedených v příloze č. 3 této smlouvy v době dle čl. V odst. 2 písm. a) této smlouvy;
   b) ve výši 20 000 Kč za každou hodinu prodlení ve lhůtě dle čl. V odst. 2 písm. b) této smlouvy;
   c) ve výši 1 000 Kč za každou hodinu prodlení ve lhůtě dle čl. V odst. 2 písm. c) této smlouvy;
   d) ve výši 1 000 Kč za každou hodinu prodlení ve lhůtě dle čl. V odst. 2 písm. d) této smlouvy.
3. V případě, že se po dobu účinnosti této smlouvy prokáže, že nebyly splněny některé z požadavků uvedených v příloze č. 5 („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 počítána jako jedno zařízení) více závad než 10 za rok, 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 předložení prohlášení nebo potvrzení výrobce podle článku IV odst. 3 až 5 nebo článku XI odst. 6 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 5 % z celkové ceny podle článku III odst. 2 této smlouvy za každý započatý měsíc prodlení.
6. Ujednáními o smluvní pokutě není dotčeno právo smluvních stran na náhradu škody.
7. V případě prodlení s uhrazením daňového dokladu zaplatí objednatel zhotoviteli úrok z prodlení podle předpisů občanského práva.
8. Smluvní strany se ve smyslu § 1991 občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za zhotovitelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce zhotovitele za objednatelem, ať splatné či nesplatné.

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 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 (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. 6 této smlouvy.
3. Dle § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOU"), strany sjednaly:
   a) zpracování veškerých osobních údajů objednatelem, který je ve smyslu ZOOU zpracovatelem, probíhá podle ZOOU, zejména je zpracovatel povinen ve smyslu § 7 ZOOU splnit obdobně všechny povinnosti stanovené v § 5 ZOOU pro správce osobních údajů,

b) toto ujednání o zpracování osobních údajů se uzavírá za účelem zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB způsobem, v rozsahu a postupem dle smlouvy, jejímž je toto ujednání dle § 6 ZOOU součástí. Rozsah zpracování osobních údajů odpovídá účelu zpracování, tedy obsahuje identifikační osobní údaje (jméno, příjmení a číslo průkazu totožnosti zaměstnanců zhotovitele). Zpracování osobních údajů podle tohoto ujednání se sjednává na dobu existence závazkového vztahu vzniklého ze smlouvy, jejíž součástí je toto ujednání, nejpozději do likvidace posledního osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle ZOOU,

c) objednatel poskytuje zhotoviteli následující záruky technického a organizačního zabezpečení ochrany osobních údajů:
   - veškeré materiály s osobními údaji jsou zajištěny v uzamykatelném nábytku v uzamčených prostorách v sídle objednatele,
   - všechny osobní údaje jsou následně zpracovávány na PC, která jsou zabezpečena heslem, a jsou přístupná pouze vybraným zaměstnancům objednatele,
   - organizace a povinnosti zaměstnanců objednatele ohledně ochrany osobních údajů, jsou stanoveny ve vnitřním předpisu objednatele.

Článek IX
Odstoupení od smlouvy, výpověď

1. V případě, že některá ze smluvních stran poruší smluvní povinnost vyplývající pro ni z této smlouvy, je druhá smluvní strana oprávněna od smlouvy odstoupit.
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. 5.
3. Za podstatné porušení smluvní povinnosti se považuje zejména, ale nejen:

   - ze strany zhotovitele:

   - nesplnění kteréhokoli požadavku/požadované funkce uvedených v příloze č. 5.
   - prodlení zhotovitele s předáním kterékoliv dílčí etapy dle čl. I odst. 2. písm. a) až d) této smlouvy po dobu delší než 30 kalendářních dnů.
   - případ, kdy se v rámci zkušebního provozu dle čl. I odst. 2. písm. c) této smlouvy vyskytnou takové vady, které objednatel vyhodnotí jako podstatné a tyto nebudou odstraněny ani v určené dodatečné přiměřené lhůtě.
   - prodlení zhotovitele se zahájením prací na odstraňování kritické závady do 24 hodin od nahlášení podle čl. V této smlouvy.
   - prodlení zhotovitele se zahájením prací na odstraňování nekritické závady programových prostředků do 2 pracovních dní od nahlášení podle čl. V této smlouvy.
   - případ, kdy zhotovitel nebude schopen v rámci implementace dodržet maximálně stanovené časy odstávek dle přílohy č. 5 požadavek „Provozní odstávky".
   - 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 daňových dokladů 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. 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 objednatele od smlouvy je účinné dnem doručení oznámení o odstoupení od smlouvy zhotoviteli.
7. Smlouvu lze v části týkající se podpory (vyjma záruční podpory) vypovědět v 6 měsíční výpovědní lhůtě, která počíná běžet prvním dnem kalendářního měsíce následujícího po doručení písemné výpovědí druhé smluvní straně. Zhotovitel je oprávněn smlouvu vypovědět nejdříve 2 roky po skončení záruky poskytnuté na technické prostředky.
8. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek zhotovitele vypovědět tuto smlouvu v části týkající se podpory, a to ve 14 denní výpovědní lhůtě, která počíná běžet dnem následujícím po doručení písemné výpovědi zhotoviteli.

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

1. Zhotovitel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků, výši skutečně uhrazené ceny za plnění této smlouvy a seznam subdodavatelů, kterým zhotovitel za plnění subdodávky uhradil více než 10 % z ceny za plnění dle této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ") uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.
3. Zhotovitel je povinen dle § 147a odst. 4 ZVZ předložit objednateli nejpozději vždy do 28. února následujícího kalendářního roku seznam subdodavatelů, jímž za plnění subdodávky uhradil více než 10 % z části ceny uhrazené objednatelem zhotoviteli za plnění dle této smlouvy v předchozím kalendářním roce či prohlášení, že nemá subdodavatele, jimž by za plnění subdodávky uhradil více než 10 % z části ceny uhrazené objednatelem zhotoviteli za plnění dle této smlouvy v předchozím kalendářním roce. Má-li subdodavatel formu akciové společnosti, tvoří přílohu seznamu i seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu. Seznam vlastníků akcií musí být vyhotoven ve lhůtě 90 dnů před dnem předložení seznamu subdodavatelů. Zhotovitel zašle seznam objednateli na adresu:

   Česká národní banka
   sekce správní
   odbor obchodní
   Na Příkopě 28

115 03 Praha 1

4. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 147a ZVZ a uveřejňování bude prováděno dle ZVZ a příslušného prováděcího předpisu ZVZ.

Článek XI
Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran. Smlouva se v části týkající se pozáruční podpory technických a programových prostředků, které jsou nedílnou součástí technických prostředků uzavírá na dobu neurčitou.
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 přílohy č. 3, 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 subdodavatele, nahradí škodu jím způsobenou, jakoby ji způsobil sám.
6. Smluvní strany se dohodly, že tato smlouva a právní vztahy jí založené se řídí podle zákona č. 89/2012 Sb., občanský zákoník.
7. 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.
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 čtyřech stejnopisech, z nichž objednatel obdrží tři 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 technických a programových prostředků
č. 2	Specifikace činností.
č. 3	Kontakty pro poskytování záruční a pozáruční podpory
č. 4	Seznam zařízení objednatele
č. 5	Technická specifikace předmětu plnění
č. 6	Bezpečnostní požadavky objednatele
č. 7	Návrh technického řešení

V Praze dne: 10. 9. 2014

Za zhotovitele: [redacted]

.....

Ing. Marián Jurík
jednatel

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

V Praze dne: 10. 9. 2014

Za objednatele: [redacted]

.....

Ing. Vladimír Mojžíšek
ředitel sekce informatiky

[redacted]

.....

Ing. Zdeněk Virius
ředitel sekce správní

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

Příloha č. 1

Specifikace technických prostředků a programových prostředků

název (popis)	rozlišení HW/SW	Množství (u HW počet ks, u SW počet licenčních jednotek a jejich typ)	Cena za jednotku v Kč bez DPH
nShield Connect 1500+ F3	HW	2,00	685 053,50
Additional Client Activation	SW	15,00	162,67
Slide rails for nShield Connect	HW	2,00	8 132,50
Additional 'soft' client	SW	9,00	56 840,89
Security World Software for Windows	SW	1,00	465,00
Security World Software for Linux 64bit	SW	1,00	465,00
10 pack standard nCipher smartcards	HW	2,00	3 098,00

Součástí dodávky nejsou žádné programové prostředky, které nejsou nedílnou součástí technických prostředků.

Podrobný rozpis ceny plnění (v Kč bez DPH)

1. etapa				121 866,00
2. etapa				2 084 607,00
z toho	dodávka HW			1 392 568, 00
	dodávka SW			514 938,00
	instalace technických prostředků a jejich implementace, zprovoznění zrcadlení, připojení nejméně 5 serverů objednatele a instalace programových prostředků na tyto servery, instalace SW pro management dodaných technických prostředků, konfigurace minimálně 3 slotů, přiřazení k serverům, dodání dokumentace výrobce technických prostředků a programových prostředků (čl. I odst. 2 písm. b) návrhu smlouvy)			162 701,00
		Počet dní (1 den = 8 hod.)	Cena v Kč bez DPH za 1 den	Celková cena v Kč bez DPH
	zaškolení obsluhy	1	14 400,-	14 400,-
3. etapa				131 333,00
z toho	dodávka SW			0,00
	asistence při konfiguraci dodaných technických prostředků dle specifických požadavků objednatele (asistence při vytváření dalších cca 7 slotů pro konkrétní systémy), provedení instalace programového vybavení na ostatní servery dle přílohy č. 4 smlouvy a migrace dat dle přílohy č. 2 smlouvy pro stávající aplikace objednatele (čl. I odst. 2 písm. c) návrhu smlouvy)			116 933,00
		Počet dní (1 den = 8 hod.)	Cena v Kč bez DPH za 1 den	Celková cena v Kč bez DPH
	školení programátorů	1	14 400,-	14 400,-
4. etapa				85 892,00

Příloha č. 2

Specifikace činností

Detailní specifikace požadovaných činností zhotovitele

Činnost	Poznámka
Instalace HW/SW	Instalace HSM a základní konfigurace, instalace SW pro management a SW/skriptu pro dohled na dedikovaném serveru. Po instalaci a konfiguraci zajistí zhotovitel zaškolení pro 2 zaměstnance technické správy ČNB v rozsahu nezbytném pro zajištění provozu dodaných prostředků v ČNB (konfigurace, administrace, běžná správa).
Zapojení do datových struktur ČNB a testovací provoz	Zapojení do clusteru, zprovoznění zrcadlení, připojení nejméně 5 serverů a vytvoření minimálně 3 slotů.
Konfigurace HSM	Asistence při konfiguraci jednotlivých slotů pro servery v rozsahu do 10.
Instalace SW	Zajištění instalace veškerého dodaného SW na všech serverech z platforem Linux i Windows. Maximální přípustné doby provozních odstávek jsou uvedeny v příloze č. 5, část Provozní odstávky;
Zajištění školení	Před migrací dat zajistí zhotovitel školení pro 2 programátory ČNB v rozsahu nezbytném pro zvládnutí programového napojení aplikací na bezpečné úložiště přes rozhraní PKCS#11 a v rámci programovacího jazyka Java. Předpokládaná minimální délka školení je 1 den. Školení je požadováno v ČR, zhotovitel zajistí lektora a příslušné školící materiály. V případě, že školení bude mimo Prahu, musí zhotovitel na své náklady zajistit dopravu do místa školení a zpět, ubytování a celodenní stravování pro zaměstnance objednatele po dobu školení. Školícím jazykem může být čeština nebo angličtina. Preferován je český jazyk.
Migrace dat	Vypracování migračního postupu a asistence při migraci dat aplikací dle požadavků uvedených v příloze č. 5. v části Migrace dat. Maximální přípustné doby provozních odstávek jsou uvedeny v příloze č. 5 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 s tím, že v případě problémů souvisejících s dodanými komponentami bude k dispozici zástupce zhotovitele pro telefonické konzultace a tyto problémy pomůže operativně řešit.
Skripty	Příprava skriptů pro dohled, pokud již nebudou součástí dohledového SW.
Asistence při testování	Spolupráce při testovacím a zkušebním provozu.
Optimalizace	Zkušební provoz po ukončení importu dat, provedení měření významných provozních stavů dodaného řešení a návrh optimalizace konfigurace.

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,...); - zpracování havarijního plánu **); - zpracování protokolů o školení.

*) instalační deník by měl být veden formou notesu/knihy, 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. Měl by obsahovat 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 na druhém zrcadleném systému.

Příloha č. 3

Kontakty pro poskytování záruční a pozáruční podpory

Kontaktní osoby 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

Kontaktní osoby/centrum zhotovitele:
Předávání požadavků objednatelem bude probíhat standardními kanály dodavatele, formou systémů pro správu požadavků.

Pověřenými zaměstnanci pro technická jednání a k předání a převzetí plnění jsou:

Petr Dolejší, tel.: 222 558 111, email: dolejsi@sefira.cz

Příloha č. 4

Seznam zařízení objednatele

Platforma (Hostname)	verze OS	Aplikační Cluster	HW	poznámka
Geocluster fyzický				
(sip0/sip1)	RHEL 5	Ano	DELL R710	
Geocluster Windows				
(aslhcs31r/azlhcs31r)	Win 2008R2, SP1	Ano	DELL PE510	
Virtualizace – OracleVM 3.2				
(orel1/orel2)	RHEL 5	Ano	HP ML 350G6, HP DL380G7, DELL PER720	
(ue0/ue1)	RHEL 5	Ano		
(uv0/uv1)	RHEL 5	Ano		
Virtualizace – Vmware vSphere 5.1				
(aalhms240)	Win 2008R2, SP1	Ne	DELL PER510, DELL PER710, DELL PER720,HP DL180G6, HP DL180G6	
(aalhms226)	Win 2008R2, SP1	Ne		
(aalhms243)	Win 2008R2, SP1	Ne		Server pro Management / dohled
Ostatní				
(RootCA)	Win 2008R2, SP1	Ne	DELL PE510	

Příloha č. 5

Technická 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 – 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.

Zrcadlení – je technologie zajišťující zápis dat z jednoho HSM do jiného HSM, které je umístěno v jiném objektu. Rozlišujeme synchronní a asynchronní zrcadlení.

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 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. Druhé z výpočetních středisek je též koncipováno jako tzv. nouzové záložní pracoviště ČNB pro případ, kdy bude budova ústředí ČNB mimo provoz (dále jen ZP). 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 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) a nadstavbou Hitachi Storage Cluster (HSC) pro manipulaci s disky (viz také „Seznam zařízení objednatele“).

Úložiště klíčů

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 USB tokenech. 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. Mezi využívané tokeny patří čipové karty Safenet typu 330u, 400 a 4100 a USB tokeny eTokenNG-FLASH 72k (Java). Obslužný software je Safenet Authentication Client 8.x v OS Windows i Linux.

Standardní systémové prostředí ČNB

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

Standardní komunikační vybavení:

- LAN - strukturovaná kabeláž pro připojení uživatelů umožňující připojení rychlostí minimálně 100 Mbit/s. Standardní provedení je metalické, optická vlákna jsou typem doplňkovým;
- Páteřní LAN – Gigabit Ethernet;
- aktivní síťové prvky – platforma CISCO, plně přepínaná síť;
- LAN, MAN, WAN – multiplexory typu DWDM;
- Ethernet dle ISO 802.3 pro připojení uživatelských stanic;
- Protokol TCP/IP;
- WAN – (připojení poboček) zálohovaná trasa s propustností min 2 Mbit/s.

Páteřní síťové služby:

- DNS
  - primární DNS pro domény cnb.cz, dealing.cnb.cz – provozováno v prostředí HP-UX nebo GNU Linux,;
  - primární DNS pro doménu ms.cnb.cz - provozováno v prostředí MS Windows;
- DHCP (v doméně ms.cnb.cz)
  - provozováno na platformě MS Windows 2008R2 Serveru (ústředí i pobočky);
  - zajišťuje obsluhu klientských stanic a tiskových zařízení;
- BOOTP/DHCP
  - provozováno v prostředí HP-UX;
  - zajišťuje obsluhu síťových zařízení, která nejsou v doméně ms.cnb.cz;
- TFTP
  - provozováno v prostředí HP-UX, verze 1.4, i pro MX doménu;
- MTA
  - provozováno na HP-UX, sendmail;
- Přesný čas – NTP

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

Platforma architektury PA-RISC:

- servery s 1-16 procesory;
- operační systém HP-UX 11.00 a vyšší; ISO 8859.2;
- redundantní HW komponenty a síťová připojení;
- dohledový SW – systémové nástroje HP-UX.

Pozn: tato platforma je postupně opouštěna

Platforma architektury x86:

- servery s 1-8 procesory
- operační systém:
    - MS Windows Server 2008R2 Standard či v clusteru Enterprise Edition Eng.; cp 1250; pro kritické aplikace či služby použit MS Cluster Service;
    - Red Hat Enterprise Linux 5 a vyšší, pro kritické aplikace či služby použit MC/ServiceGuard.
    - Platforma VMware vSphere 5.1
    - Platforma Oracle VM 3.0.3
- redundantní HW komponenty a síťová připojení;
- dohledový SW – dodávaný výrobcem serverů.

Základní aplikace:

- WWW server
    - externí WWW server - WWW server Apache, J2EE server Tomcat, DB MySQL, kódování stránek UTF-8;
    - interní WWW servery
        - Oracle Portal Server – nadstavba pro WWW server Apache;
        - Microsoft Internet Information Server 6.0 a vyšší; kódování stránek Windows 1250.
- databáze
    - Oracle RDBMS verze 8 a vyšší;
    - Oracle aplikační servery verze 9i, 10g a vyšší.
- klientský systém elektronické pošty – MS Exchange Server 2010
- antivirová kontrola el. pošty – Microsoft ForeFront for Exchange server
- programové vybavení pro management
    - produkty platformy HP Open View – verze 6.0;
    - Microsoft System Management server 2003 + SP1
    - Microsoft System Center Operation Manager
- certifikační autorita:
    - Microsoft PKI na serveru 2003 a MS PKI na serveru 2008R2 v clusteru
- Java IAIK – signer pro ostatní aplikace vyjma používajících Signer.dll – podrobnosti na http://jce.iaik.tugraz.at/;
- zálohovací systém – HP DataProtector 6.0;
- archivační systém – IBM OnDemand;
- systém pro centrální sběr a správu logů – Microsoft System Centre Operation Manager Server 2007 R2;

- Monitoring zranitelností - QUALYS

Prostředí klientské stanice

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

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

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

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

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

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

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

V následující tabulce jsou uvedeny požadavky, které musí být zhotovitelem 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. HSM musí být zdvojené, nesmí existovat „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. 5) této smlouvy) - přetížení jedné komponenty nesmí způsobit zastavení clusteru HSM jako celku. Jmenovitě nesmí dojít k situaci, kdy přetížením jednoho HSM dojde k podstatnému ovlivnění dostupnosti a výkonnosti poskytované druhým HSM	Pokud bude požadavek na zajištění dostupnosti dat do 6 hod řešen studenou zálohou ve formě dalšího HSM modulu, musí být tento modul uveden v cenové nabídce a fyzicky dodán objednateli. 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

	- 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.	k výrobci (případně pověřené organizaci), kde 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.
Zrcadlení	V rámci clusteru HSM musí být zajištěno alespoň asynchronní zrcadlení dat mezi dvěma různými lokalitami. Technologie zrcadlení musí být transparentní a může vyžadovat pouze konfigurační zásah do IS. Je vyžadována možnost uživatelské volby směru zrcadlení (určení primárního a sekundárního zrcadla, pokud v tomto smyslu existují). Volba směru zrcadlení musí být dynamická bez potřeby plné synchronizace dat a bez nutnosti zrušení a znovu vytvoření zrcadleného páru. Zrcadlení musí být realizovatelné vzájemně mezi oběma lokalitami – obě lokality jsou v režimu active/active. Po případném přerušení zrcadlení (ať již havárií nebo operátorsky přerušením zrcadlení HSM) musí být nezbytné pouze „rozdílově" dorovnání stavu na úrovni obsahu slotu.	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. Veškeré provozované informační systémy předpokládají konzistenci svých dat v druhé lokalitě (tj. nejsou schopny se automaticky zotavit ze stavu, kdy jsou v lokalitách různá data). Z těchto důvodů je požadováno zrcadlení alespoň v asynchronním režimu.
Zabezpečení dat	Data musí být zabezpečena proti selhání nebo přetížení prostřednictvím clusterového řešení (zdvojení komponent) a	Pro případ selhání obou nodů clusteru musí být k dispozici odpovídajícím způsobem

	zálohováním dat do bezpečného úložiště a jejich rozdělení na více částí. Z důvodu bezpečnosti musí být možné provést zálohu klíčového materiálu rozděleného mezi více správců tak, aby klíče bylo možné zrekonstruovat za přispění minimálně 2 částí/správců. Pokud je vyžadován pro tuto funkci speciální hardware, musí být dodán v takovém množství, aby odpovídal minimální poptávané kapacitě a dvěma nezávislým zálohám.	zabezpečená záloha.
Zabezpečení proti úniku dat	HSM bude umístěn v prostorech s omezeným přístupem v dedikovaném uzamčeném racku. V případě pokusu o fyzické narušení úložiště dat musí dojít k automatickému vymazání dat a to i v případě že bude HSM ve vypnutém stavu.	HW, kde bude umístěn klíčový materiál včetně záloh bude umístěn v prostorech s omezeným přístupem v dedikovaném uzamčeném racku nebo v trezoru podle typu média.
Ochrana investic	Požadované funkce HSM musí být aplikačně nezávislé (změna verze IS/aplikace nesmí mít vliv na funkce poskytované HSM).	Všechny funkce poskytované HSM musí být nezávislé na IS. Pro všechny informační systémy musí být poskytované služby transparentní, tj. nesmí existovat vazba mezi informačními systémy a HSM ve smyslu nutnosti certifikace výrobcem dodaného HW nebo SW (netýká se HW a OS serverů a clusterových komponent).
Připojení HSM	Připojení HSM 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 <u>každému</u> z HSM.	V budoucnu se předpokládá navýšení počtu připojených serverů.
Kapacita a prostor pro data	Celková kapacita HSM pro data (v <u>každé</u> lokalitě) musí být minimálně 20 klíčových párů a certifikátů o velikosti každého klíče/certifikátu max. 4096 bitů. Tyto klíčové páry musí být možné	Požadavek na celkovou kapacitu vychází, ze současného stavu a z očekávaných nárůstu pro další období.

	umístit do minimálně 10 slotů.	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 HSM 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. umožní připojení nových kapacit k serverům bez potřeby složitých rekonfigurací.	V závislosti na skutečných potřebách v následujících 3-4 letech se očekává možnost požadavků na kapacitní rozšíření HSM. Nabízené zařízení musí umožnit rozšíření, ale toto rozšíření není v tuto chvíli předmětem dodávky.
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	Funkce nutná z důvodu zabezpečení nezávislého přístupu serverů jen k přiděleným slotům.

	u jednoho HSM) v žádném případě nesmí ovlivnit provoz ostatních serverů (aplikací) připojených k HSM ani ostatních HSM jako celku.	
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.	Režim vysoké dostupnosti je v prostředí MS Windows 2008R2 realizován jako geografický

	Přesun aplikací mezi lokalitami nesmí mít vliv na funkčnost clusteru těchto aplikací, ani dodaného řešení jako celku.	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. 4. 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 5, které mohou být provozovány buď na fyzickém HW, nebo na virtualizační platformě VMware 5.1 nebo OracleVM 3.2. Dále musí být výrobcem podporováno připojení serverů s operačními systémy Windows 2012 a RedHat 6.	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 HSM zcela vyloučena.
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. 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 HSM a souvisejícího SW	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	Jedná se o minimální a povinný výčet funkcí.

	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 podporovány!	
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 k HSM je logován a omezen pouze na vymezené servery. Musí být možné v případě aplikací vynutit použití pouze jednoho autentizační údaje, pokud HSM disponuje autentizačním mechanismem, který pro přístup vyžaduje více částí.	V případě aplikací není přípustné aby byl vyžadován více než jeden autentizační údaj pro přístup k HSM. 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 HSM umožnit vytvoření důvěryhodného kanálu mezi sebou a participující aplikací. HSM 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.
Zabezpečení provozu	Musí být zajištěn provoz v režimu vysoké dostupnosti a zrcadlení za	

v režimu vysoké dostupnosti - geografický cluster	využití algoritmů dle FIPS 140-2 při transportu obsahu mezi moduly v oddělených geografických lokalitách.	
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 (tj. na obou HSM) budou IS provozovány systémem active-active, tj. v každé lokalitě mohou s kterýmkoliv HSM v režimu HA komunikovat za běžného provozu různé IS.	Tento systém umožňuje využití pořízených kapacit v běžném provozu k rozložení zátěže 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. 4. 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	Dodávané technické prostředky musí být umístitelné v těchto prostorech ČNB: Praha 1, Senovážná ul. 3 (místnosti VP304)	Požadavek vychází ze specifikace prostor očekávaného umístění. Jiný stojan by přinesl problémy se zastřešením teplé uličky a s chlazením prostoru.

	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. 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.	Pro zajištění maximální spolehlivosti a včasného zajištění nápravy je vyžadována trvalá diagnostika poruch HSM

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 s členěním významnosti minimálně na 3 úrovně (např. information, warning, critical/fatal); - možnost generování přehledů o konfiguraci a přiřazení slotů na HSM. 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;	Z důvodu zajištění správy a minimalizace nároků na správu je požadováno zajištění odpovídajícího nástroje/skriptu. Pro dohledový nástroj/skript může být ze strany ČNB poskytnut 1x Virtuální server (max. 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: - konfigurace jednotlivých HSM - 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);	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.

	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. Operace požadované pro provádění uživatelem však není možné přenést na zhotovitele. 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.	
Manipulace v clusteru-funkčnost clusteru	Pro zajištění funkce geografického clusteru musí být zajištěny minimálně tyto funkce: - provedení FailOver/FailBack; - volba směru zrcadlení. Provádění všech operací musí být on-line, tj. bez přerušení přístupu k datům, výkonnost může být částečně snížena. Přechod na druhý node clusteru HSM 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 HSM	Komunikace pro řízení a ovládání HSM (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 rozhranní (GUI)	Pro konfigurační a řídící potřeby není nutné zajistit bezvýpadkový provoz (případný server zajišťuje ČNB).

Zálohování konfigurace	Musí být zajištěna možnost zálohování konfigurace systému 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/zabezpečení přístupu	Přístupy musí být logovány buď na HSM, nebo na serverech ze kterých je realizován k HSM přístup. Logy musí být externě ukládány v textovém formátu se stanovenou strukturou a významem dat.	Textový výstup je nezbytný pro budovaný systém SIEM.
Migrace dat	V rámci náhrady stávajících softwarových úložišť, případně HW tokenů 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: Musí být zajištěna možnost migrace/import klíčů stávající PKI bez nutnosti generace nových klíčů a certifikátů. To zahrnuje export dat ze stávajícího úložiště do dodaných HSM spojenou buď se změnou konfigurace PKI, nebo s reinstalací stávající PKI. Zhotovitel zajišťuje jak export tak import dat. Pokud bude nutné realizovat reinstalaci PKI, 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 zajištěn import stávajících dat aplikací ze souboru bez nutnosti generace nových dat, pouze se změnou konfigurace aplikací. Zhotovitel zajišťuje pouze import dat do dodaných HSM ze souborů pfx dodaných objednatelem. Podmínkou realizace je zachování stávajících dat.	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.

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 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.	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 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) *Programové moduly realizované zaměstnanci ČNB*

Za dobu provozu byly zaměstnanci ČNB vytvořeny programové moduly pro spolupráci se stávajícími úložišti v programovém jazyce Java. Tyto moduly bude nutné v souvislosti s změnou technologie přepracovat. Zároveň bude nutné v těchto modulech dopracovat podporu pro spolupráci HSM se systémem pro správu hesel od společnosti CyberArk.

Příloha č. 6

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 získání souhlasu subjektů osobních údajů se zpracováním osobních údajů v ČNB ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů". Zhotovitel v něm prohlásí a nese odpovědnost za to, že jeho pracovníci uvedení v seznamu vydali souhlas se zpracováním osobních údajů Českou národní bankou v rozsahu: jméno, příjmení a číslo průkazu totožnosti. Důvodem předání těchto osobních údajů je zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB.
3. 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.
4. 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.
5. 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. Pracovníci zhotovitele se budou v rámci objektů ČNB pohybovat pouze v pracovním oděvu s viditelným a nesnímatelným označením („logem") zhotovitele.
6. V případě mimořádné události se pracovníci zhotovitele musí řídit pokyny bankovních policistů nebo dozorujícím zaměstnancem ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem.
7. 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.
8. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka zhotovitele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
9. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
10. 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.
11. 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

Návrh technického řešení

6. Návrh řešení předmětu veřejné zakázky

Předmětem této nabídky je poskytnutí služeb spočívajících v dodávce, instalaci a zprovoznění technických a programových prostředků pro ukládání a využití kryptografických klíčů v informačních systémech objednatele, vypracování projektové dokumentace a zaškolení zaměstnanců zadavatele.

Návrh řešení předmětu veřejné zakázky spočívá v dodávce

- bezpečnostních HSM modulů společnosti Thales,
- odpovídajících klientských licencí a klientského SW,
- záruky a technické podpory k výše uvedenému na tři roky,
- rozšířené pozáruční podpora k výše uvedenému na jeden rok,
- odpovídajících implementačních služeb a
- podpory řešení.

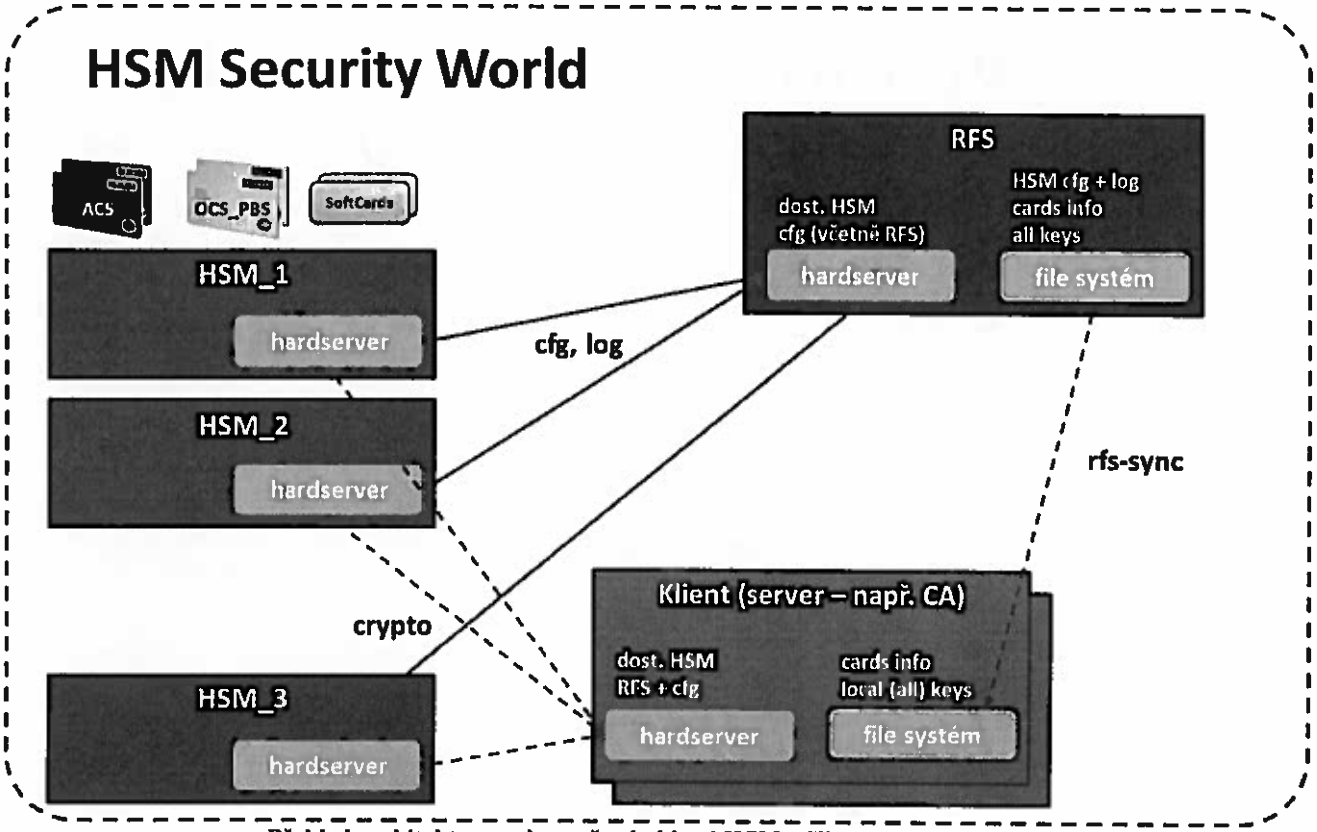
Jednotlivé dodávané služby jsou podrobněji popsány níže.

6.1. Popis řešení

Pro splnění požadavků zadávací dokumentace budou dodány 2 ks síťových HSM modulů **Thales nShield Connect 1500+**, kde v každé z lokalit bude umístěn jen HSM modul. Pro podporu správy a konfigurace všech používaných síťových modulů musí být v jedné z lokalit k dispozici server s instalovaným klientským SW, který bude plnit speciální roli Remote File System (RFS).

Tento RFS server bude obsahovat informace o konfiguraci pro jednotlivé HSM moduly, bude sbírat logy z jednotlivých modulů, bude umožňovat přístup k SNMP zprávám z hlediska dohledu a dále bude obsahovat potřebné administrační nástroje a utility. Tento RFS server může být provozován na libovolné platformě podporované klientským SW. Přehled podporovaných OS a virtualizačních platforem je uveden na přiloženém produktovém listu v příloze.

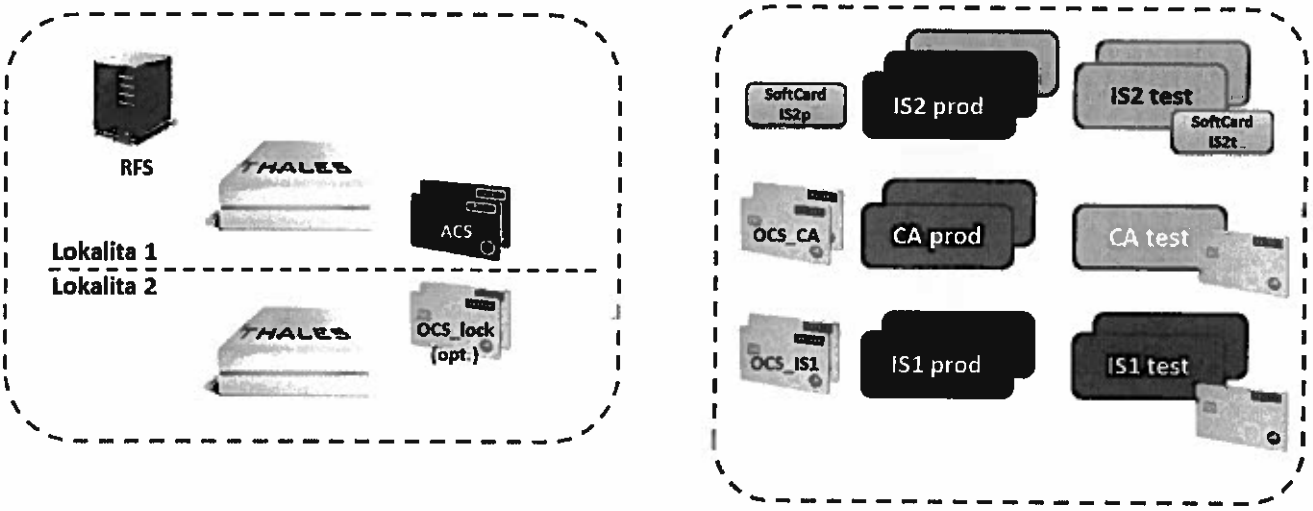
SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.



Přehled architektury zabezpečené oblasti HSM – Thales Security World

Nabízené síťové HSM moduly umožňují zapojení do dvou nezávislých síťových větví pomocí dvou síťových karet.

Na všechny servery, na kterých budou provozovány aplikace využívající služeb HSM modulů, musí být instalován klientský SW společnosti Thales pro příslušnou platformu. Předmětem dodávky budou instalační média pro prostředí MS Windows a Linux. Tyto servery musí být registrovány jako povolené v rámci konfigurace jednotlivých HSM modulů.

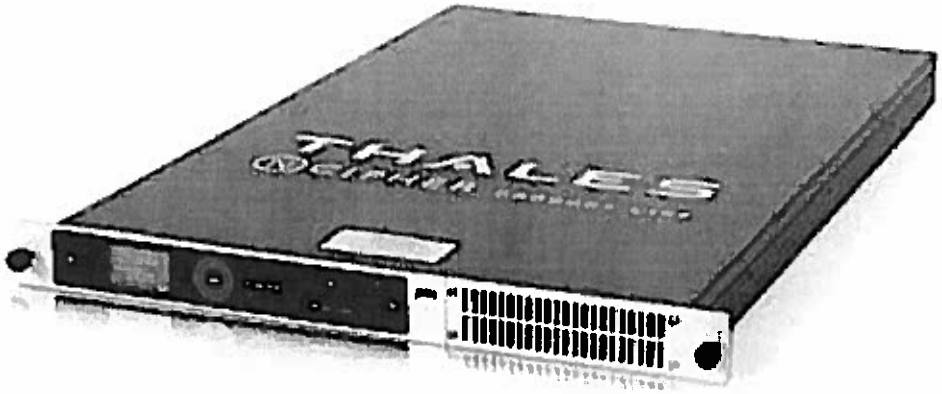


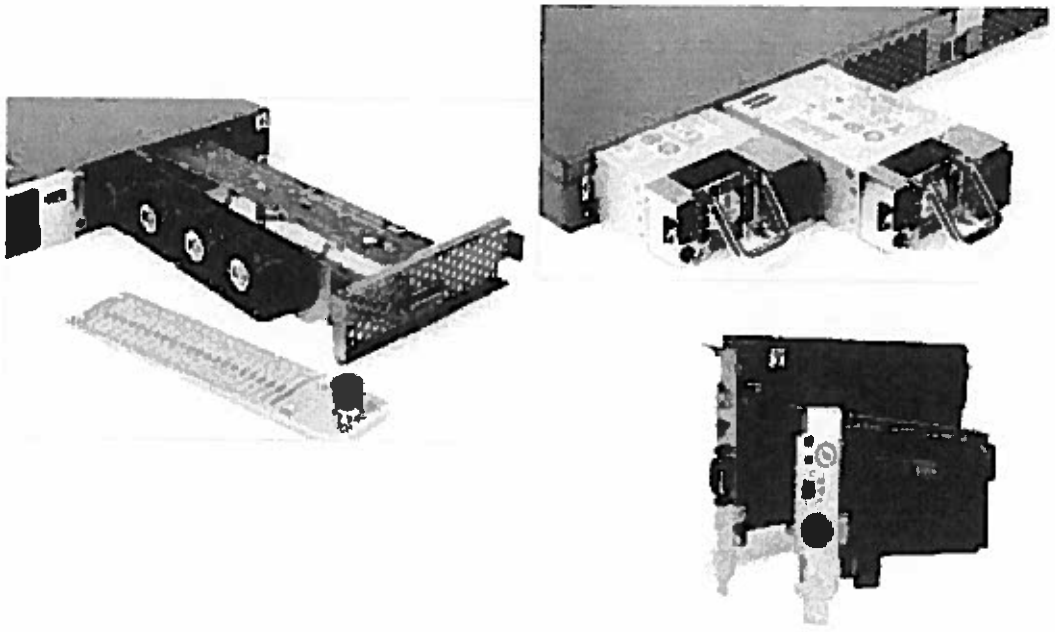
Příklad uplatnění konfigurace pro různé typy slotů

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.

Pro komunikaci mezi jednotlivými prvky infrastruktury je používán bezpečný firemní protokol Impath, který zajišťuje šifrování veškeré komunikace a autentizaci jednotlivých prvků. Výchozí komunikace probíhá na TCP portech 9000 a 9001.

Plnění projektu předpokládáme v požadovaných etapách a termínech jak je uvedeno v návrhu smlouvy.





6.2. Splnění výkonnostních požadavků

Nabízené HSM moduly Thales nShield Connect 1500+ umožňují připojení až 20 klientů současně s tím, že maximální výkon jednoho HSM modulu je 1500 operací za sekundu pro RSA algoritmus s délkou klíče 1024 bitů. Výkonnost jednoho HSM pro další délky klíčů a pro další algoritmy je uvedena v přiloženém produktovém listu v příloze.

Pro potřeby této nabídky budou dodány potřebné přístupové licence pro požadovaný počet klientů (serverů). Klientem je v terminologii společnosti Thales míněn fyzický nebo virtuální server, v rámci kterého je provozována příslušná koncová aplikace nebo technologie využívající HSM modul. V rámci jednoho klienta je možné provozovat více aplikací využívajících různá aplikační rozhraní pro HSM moduly. Klientský přístup se licencuje adresně pro každý konkrétní HSM modul.

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.

6.3. Návrh postupu migrace dat

Vlastní migrace potřebných dat odpovídá spíše migraci jednotlivých aplikací/systémů na nový typ úložiště klíčů pro kryptografické operace. Jako hlavní typy systémů jsou identifikovány tyto:

- certifikační autorita na platformě Microsoft
- aplikace používající souborové úložiště klíčů
- aplikace využívající PKCS#11 rozhraní k HW úložišti klíčů (např. čipová karta nebo USB token)

Pro tyto typy aplikací budou vždy rozdílné migrační scénáře. Jednotlivé předběžné návrhy těchto migračních scénářů jsou uvedeny níže. Podrobné migrační postupy budou definovány a popsány v rámci implementační studie vytvořené v rámci Etapy 1 projektu.

6.3.1. Certifikační autorita MS

V případě přechodu od stávající konfigurace s klíči uloženými v rámci OS pro MS certifikační autoritu je nutné provést zálohu autority a vyexportovat klíče. Dále bude vytvořen speciální operátorský set čipových karet (OCS) pro zabezpečení klíčů (odpovídá termínu slot) používaných CA (typicky v režimu alespoň 2 z N), provedení instalace certifikačních služeb na server s instalovaným a konfigurovaným HSM klientem a obnovení autority pomocí nového krypto providera a vytvořeného OCS.

Většinu výše uvedených operací bude podle požadavků Objednatele zajišťovat Zhotovitel.

V závislosti na sledu a přípravě jednotlivých kroků předpokládáme odstávku v rozsahu maximálně 8 hodin, což by nemělo být pro systém tohoto typu na překážku.

6.3.2. Aplikace se souborovým úložištěm klíčů

V případě toho typu aplikací budou do připraveného slotu se zvolenou autentizací naimportovány klíče a certifikáty ve formě PKCS#12.

Následně zajistí Objednatel úpravu dotčených aplikací tak, aby využívaly přes zvolené API HSM moduly jako úložiště klíčů. Po nasazení a úpravě konfigurace aplikace bude provedeno ověření chování pomocí HSM modulů.

V tomto scénáři bude Zhotovitel zajišťovat pouze asistenci při vytváření a konfiguraci příslušného slotu, import klíčů do daného slotu za účasti správců daného slotu a dále může Zhotovitel zajistit technickou konzultační podporu při konfiguraci a testování finální aplikace.

Typická příprava prostředí a migrace příslušných klíčů vyžaduje odstávku v rozsahu 2 až 4 hodin.

6.3.3. Aplikace s PKCS#11 úložištěm klíčů

Proces migrace pro tento typ aplikací předpokládáme obdobný jako v předchozím případu. Vzhledem k povaze aplikace se může v tomto případě jednat pouze konfigurační záležitost na straně aplikace (jiný PKCS#11 vendor), ale toto nelze dopředu zajistit.

Dále musí Objednatel zajistit přístup k potřebným klíčům a certifikátům využívaným současnými technologiemi zpřístupněnými přes PKCS#11 ve formátu souboru PKCS#12, který bude možné importovat do HSM modulu. Alternativně je možné pro vybrané aplikace iniciovat obnovu klíčů tak, že nové klíče budou vygenerovány přímo v HSM modulech.

Typická příprava prostředí a migrace příslušných klíčů vyžaduje odstávku v rozsahu 2 až 4 hodin.

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.

6.4. Fnkce a vlastnosti řešení

Požadavek	Popis splnění požadavků
Dostupnost	Nabízené HSM moduly jsou rutinně používány v mnoha bankách a certifikačních autoritách. Budou implementovány 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 k oběma aktivním HSM modulům, které využívá paralelně. V případě poruchy HSM modulu bude v požadovaných lhůtách zajištěno zapůjčení náhradního HSM modulu odpovídajících kvalit a výkonu.
Zrcadlení	Každý klient bude mít standardně nastaven přístup k oběma 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 zajištěno jejich zrcadlení na jednotlivé uzly aplikačních clusterů.
Zabezpečení dat	Každý klient bude mít standardně nastaven přístup k oběma 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	Nabízené síťové HSM moduly Thales nabízí podporu pro širokou paletu operačních systémů včetně nejnovějších verzí a zároveň nabízí širokou škálu rozhraní využitelných v jednotlivých prostředích. Úplný přehled podporovaných systémů je uveden v přiloženém produktovém listu v příloze.
Připojení HSM	Nabízené HSM moduly disponují 2 síťovými rozhraními pro duální zapojení do dvou fyzických sítí.
Množství připojených serverů	Nabízené modely Thales nShield Connect 1500+ podporují připojení až 20 různých serverů současně.

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.

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. Těchto objektů je možné vytvářet minimálně 256 – tedy minimálně 256 nezávislých slotů.
Kapacitní rozšiřitelnost	Nabízené 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 nabízené 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 a případné náhradní zařízení bude mít minimálně stejné nebo lepší parametry než produkčně provozované HSM moduly. 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 HSM modul). 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 modul. Pro vybraná rozhraní je možné definovat preference využívaného HSM modulu.
Kompatibilita s prostředím ČNB	Nabízené 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 podporuje všechny požadované operační systémy a virtualizační platformy. Blíže viz přiložený produktový list v příloze.
Rozhraní pro programátory a aplikace	Nabízené řešení podporuje všechna požadovaná aplikační rozhraní včetně příslušné dokumentace. Blíže viz přiložený produktový list v příloze.
Základní funkce HSM a souvisejícího SW	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.

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.

Množina podporovaných kryptografických algoritmů	Výčet podporovaných algoritmů je uveden v přiloženém produktovém listu v příloze.
Autentizační mechanismus	Aby mohl server (klient) využívat služeb nabízených 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.
Zabezpečení provozu v režimu vysoké dostupnosti - geografický cluster	Vzhledem k tomu, že je k dispozici bezpečná výměna/sdílení klíčového materiálu mimo vlastní HSM moduly není nutná přímá synchronizace mezi HSM moduly. Ačkoliv i tato je možná pro speciální klíče chráněné pouze uvnitř HSM modulů. Tyto ale z důvodů jejich dalších omezení nepředpokládáme využívat v prostředí ČNB.
Bezpečnostní certifikace	Nabízené 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	Nabízené 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 nabízených HSM modulů je pouze 0,6A při napájení 230V. Blíže viz přiložený produktový list v příloze.

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.

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.
Manipulace v clusteru-funkčnost clusteru	Při standardní konfiguraci jsou oba HSM využívány rovnoměrně a při detekci nedostupnosti jednoho z modulů, je zpracování směrováno na zbývající uzly. Role obou HSM jsou ekvivalentní – není definován primární a sekundární modul. 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 HSM	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/zabezpečení přístupu	Logování činnosti a operací je primárně logováno v HSM modulu a následně v pravidelných (nastavitelných) intervalech ukládány na centrální RFS server. Pokud bude RFS na platformě Linux/UNIX jsou tyto logy ukládány v souborovém systémy, pokud bude na platformě MS Windows budou 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 je třeba počítat s reinstalací stávající autority a jejím obnovením pomocí HSM úložiště (data zůstanou nedotřena), ale bude vyžadovat odstávku této technologie. Migrace ostatních klíčů pomocí importu dat z připravených PKCS#12 souborů bude probíhat za provozu a zahájení používání těchto klíčů bude záležet na nasazení upravené aplikace s podporou HSM nebo po změně její konfigurace, pokud HSM standardně podporuje. Pro všechny tyto operace bude nutná přítomnost potřebného počtu správců pro daný slot. Minimální počet správců záleží na konfiguraci konkrétního slotu.
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 víceuzlových clusterů je možné provádět tyto kroky nezávisle na po jednotlivých uzlech. Prvotní instalace vyžaduje restart dotřeného serveru.
Opravy HW	Vybrané opravy HSM modulu je možné provést na místě (výměna zdroje, výměna ventilátorů) a není třeba odvážet zažízení. V případě požadavku na opravu HSM modulu je navržena konfigurace, která neukládá žádné klíčové informace permanentně

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572

	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. Případné náhradní zařízení, které bude zapůjčeno v případě problémů s dodanými HSM moduly, bude obsahovat licence pro potřebný počet klientů.

SEFIRA spol. s r.o. | Antala Staška 2027/77, 140 00 Praha | IČ: 62 90 77 60 | telefon: +420 222 558 111 | www.sefira.cz
Společnost SEFIRA spol. s r.o. je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 34572.