KUPNÍ SMLOUVA č. 165310317

I.
Smluvní strany

Česká republika – Ministerstvo obrany

Se sídlem: Tychonova 1, 160 01 Praha 6
IČO: 60162694
DIČ: CZ60162694
Bankovní spojení: Česká národní banka, pobočka Praha, Na Příkopě 28, Praha 1
Číslo účtu: 404881/0710
Zaměstnanec pověřený jednáním:
ředitel odboru komunikačních a informačních systémů
Sekce vyzbrojování a akvizic MO
Ing. Jiří NYKODÝM
Se sídlem na adrese: Sekce vyzbrojování a akvizic MO
odbor komunikačních a informačních systémů
nám. Svobody 471/4
160 01 Praha 6
Kontaktní osoba: Ing. Josef Novotný
Telefonické a faxové spojení:
telefon: + 420 973 213 994
fax: + 420 973 215 232
Adresa pro doručování korespondence:
Sekce vyzbrojování a akvizic MO
odbor komunikačních a informačních systémů
nám. Svobody 471/4
160 01 Praha 6

(dále jen „kupující“)

a

SEFIRA spol. s r.o.

Zapsaná (ý) v OR vedeném městským soudem v Praze, oddíl C, vložka 34572
Se sídlem: Antala Staška 2027/77, 140 00 Praha
IČO: 62907760
DIČ: CZ62907760
Bankovní spojení: Komerční banka, a.s.
Číslo účtu: 107-8809470257/0100
Osoba oprávněná k jednání: Marián Jurík, ředitel
Kontaktní osoba: Daniel Šrámek, projektový manažer
Telefonické a faxové spojení: telefon: 222 558 111
Adresa pro doručování korespondence: shodná se sídlem firmy

(dále jen „prodávající“)

Smluvní strany uzavírají dle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „OZ") a příslušných ustanovení zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „AZ") na veřejnou zakázku, zadanou v otevřeném řízení dle § 27 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů tuto **kupní smlouvu (dále jen „smlouva").**

II.
Účel smlouvy

Účelem této smlouvy je vytvoření funkční implementace PKI infrastruktury jako základu pro správu osobních a systémových certifikátů, nasazení využití služeb elektronického podpisu, šifrování a časových razítek pro práci s dokumenty, pro potřebu datových komunikací, dvoufaktorové autentizace a autorizace uživatelů.

III.
Předmět smlouvy

1. Předmětem smlouvy je:
   a) závazek prodávajícího dodat kupujícímu HW, SW a související služby k vybudování PKI infrastruktury MO ČR, její přizpůsobení a implementaci v souladu s potřebami resortu obrany podle dokumentace výrobce v jakosti podle ČSN a souvisejících obecně platných právních předpisů a podle specifikace zboží, která je uvedena v příloze č. 1 této smlouvy (dále jen „zboží") a převést na něho vlastnické právo k tomuto zboží;
   b) závazek kupujícího dodávané zboží převzít a za řádně dodané zboží zaplatit dohodnutou kupní cenu.
2. Prodávající prohlašuje, že má k dispozici dokumentaci výrobce a že zboží dodá přesně podle této dokumentace a specifikace.

IV.
Kupní cena

1. Smluvní strany se ve smyslu zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, dohodly na celkové kupní ceně zboží, specifikovaného v čl. III. této smlouvy, a to ve výši: **8 056 180,- Kč včetně DPH**
   (slovy: osmmiliónůpadesátšesttisícstoosmdesát korun českých).

2. Celková kupní cena zboží bez DPH činí 6 658 000,- Kč, sazba DPH 21 % činí 1 397 180,- Kč. **Celková kupní cena zboží v Kč bez DPH je stanovena jako cena nejvýše přípustná.**
   Ceny za jednotlivé položky zboží jsou uvedeny v příloze č. 2 smlouvy.

   V těchto cenách jsou již zahrnuty veškeré náklady spojené s dodáním zboží.

V.
Místo plnění

Místem plnění je VÚ 3255, Generála Píky 1, Praha 6 – Dejvice.

VI.
Doba plnění

1. Prodávající zahájí plnění po podpisu smlouvy a plnění ukončí do 30. listopadu 2016.

VII.
Dodací podmínky

1. Smluvní strany se dohodly, že následující zboží - **Pracoviště vydávající CA, Pracoviště TSA, Pracoviště RA** - bude předmětem katalogizace ve smyslu zákona č. 309/2000 Sb., o obranné standardizaci, katalogizaci a státním ověřování jakosti výrobků a služeb určených k zajištění obrany státu a o změně živnostenského zákona, ve znění pozdějších předpisů (dále jen „zákon č. 309/2000 Sb."). K tomu se prodávající zavazuje řádně provést katalogizaci, což znamená, že na dosud v ČR nekatalogizované zboží a v ČR již katalogizované zboží, které však ve svém datovém záznamu nemá identifikační referenční data (RN a NCAGE) výrobce, dodá Oddělení katalogizace majetku Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, náměstí Svobody 471, 160 01 Praha 6 (dále jen „Úřad") **soubor povinných údajů pro katalogizaci** (dále jen „SPÚK") podle pokynů uvedených v příloze č. 3 „Katalogizační doložka" smlouvy. Předání SPÚK a návrhu katalogizačních dat o zboží je součástí plnění povinností prodávajícího podle této smlouvy a prodávající nemá nárok na úhradu nákladů spojených s vypracováním katalogizačních dat. Úřad po ověření předloženého SPÚK a návrhu katalogizačních dat o zboží vystaví souhlasné „Stanovisko Úř OSK SOJ k naplnění katalogizační doložky", které bude nedílnou součástí dodávky zboží a fakturace. Prodávající se zavazuje zpřístupnit či zabezpečit zpřístupnění dokumentace zboží k ověření a doplnění katalogizačních dat agentuře a k případnému ověření nebo doplnění katalogizačních dat Oddělení katalogizace majetku Úřadu.

2. Kupující pověřil jako svého zástupce k převzetí zboží ředitele VÚ 3255 Praha, nebo jím písemně pověřenou osobou (dále jen „pověřená osoba").

3. Prodávající je povinen předat zboží kupujícímu pouze v pracovní dny v době od 7.00 do 15.30 hod. po předchozím projednání, odsouhlasení termínu a doby dodání zboží s pověřenou osobou.

4. O předání a převzetí zboží je prodávající povinen vyhotovit ve třech výtiscích dodací list. Dodací list za kupujícího podepíše pověřená osoba, která současně na něm doplní číslo IDED (identifikátor dodávky). Prodávající je povinen dodací list označit číslem této smlouvy uvedeným kupujícím v jejím záhlaví. Jeden výtisk dodacího listu obdrží pověřená osoba a dva výtisky obdrží prodávající s tím, že jeden z těchto výtisků je prodávající povinen přiložit k faktuře - daňovému dokladu.

5. Prodávající je povinen při dodání zboží předat pověřené osobě v tištěné a elektronické podobě (formát Word, Excel) na hmotném nosiči (CD/DVD) dokumentaci a doklady nezbytné k převzetí a užívání zboží v českém jazyce:
   a) záruční list;
   b) návod k obsluze;
   c) prohlášení o shodě;

6. Prodávající se zavazuje, že při předání zboží pověřené osobě bude přítomna osoba pověřená statutárním orgánem prodávajícího se znalostí českého jazyka, která bude schopna řešit případné nedostatky zjištěné při přejímce zboží.

7. Prodávající je povinen při předání zboží provést seznámení s obsluhou zboží v nezbytně nutném rozsahu.

8. Prodávající je povinen dodat kupujícímu zboží nové, tj. nepoužité, nepoškozené, nerepasované a zkompletované z dílů, které nebudou staršího data výroby než roku 2015, odpovídající platným technickým, bezpečnostním a hygienickým normám a předpisům. Prodávající je povinen doložit doklady prokazující tuto skutečnost nebo předložit o této skutečnosti prohlášení při předání zboží. Pro případ pochybnosti o pravdivosti skutečností uvedených v prohlášení je prodávající povinen tyto skutečnosti prokázat.

9. Pověřená osoba nepřevezme zboží, které při přejímce vykazuje vady na balení nebo jiné zjevné vady. O této skutečnosti zástupci smluvních stran ihned vyhotoví zápis, který potvrdí podpisem. Prodávající je v tomto případě povinen dodat nové zboží náhradním plněním.

10. Vstup pracovníků prodávajícího do objektů v místě plnění musí být schválen pověřenou osobou. Prodávající je povinen písemně nahlásit jména těchto pracovníků pověřené osobě do 5 kalendářních dnů od podpisu této smlouvy. Změny těchto osob je prodávající povinen hlásit neprodleně, nejpozději 5 pracovních dnů před jejich vstupem do objektů v místě plnění. Při každém vstupu budou tito pracovníci po celou dobu doprovázeni pověřenou osobou kupujícího.

11. Informace v jakékoliv podobě či jejich části, se kterými se pracovníci prodávajícího při plnění této smlouvy seznámí, nesmí být poskytnuty v jakékoliv podobě třetí straně. To se vztahuje i na informace, nesouvisející s předmětem plnění smlouvy, se kterými se však pracovníci prodávajícího seznámí na pracovištích a v objektech kupujícího.

VIII.

Fakturační a platební podmínky

1. Prodávající po vzniku práva fakturovat, tj. okamžikem podpisu dodacího listu po předání dodávky zboží, do tří kalendářních dnů doručí kupujícímu daňový doklad (dále jen „faktura“) v českém jazyce ve dvojím vyhotovení. Faktura podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a podle požadavků kupujícího, musí obsahovat tyto údaje:
   - označení dokladu jako „**Daňový doklad – faktura**“ s uvedením evidenčního čísla;
   - obchodní firmu nebo jméno a příjmení, popřípadě název, dodatek ke jménu a příjmení nebo názvu, sídlo a místo podnikání prodávajícího s uvedením IČO a DIČ;
   - název a sídlo kupujícího s uvedením IČO a DIČ;
   - číslo smlouvy, podle které se uskutečňuje plnění;
   - rozsah a předmět plnění;
   - datum uskutečnění plnění, datum vystavení faktury;
   - název přejímajícího podle smlouvy;
   - jednotkovou cenu v Kč bez DPH a včetně DPH (tj. cenu za ks);
   - základ daně v korunách a haléřích za dodávku;
   - základní nebo sníženou sazbu daně v % nebo sdělení, že se jedná o plnění osvobozené od daně a odkaz na příslušné ustanovení zákona č. 235/2004 Sb.;
   - výši daně uvedenou v korunách a haléřích, popřípadě zaokrouhlenou na desítky haléřů nahoru;
   - kupní cenu celkem za dodávku v Kč včetně DPH;
   - označení peněžního ústavu a čísla účtu prodávajícího, na který má být poukázána platba;

- počet příloh a razítko s podpisem odpovědné osoby prodávajícího za vystavení faktury;
- údaj o zápisu prodávajícího v obchodním rejstříku včetně spisové značky, není-li v něm zapsán údaj o zápisu z jiné evidence.

2. K faktuře musí být připojen originál dodacího listu potvrzený pověřenou osobou, která je uvedena v bodu 2. čl. VII. smlouvy a „Stanovisko Úř OSK SOJ k naplnění katalogizační doložky". Dodací list musí obsahovat tyto údaje:
   - označení názvu dokladu s uvedením jeho evidenčního čísla;
   - obchodní firmu nebo jméno a příjmení, popřípadě název, dodatek ke jménu a příjmení nebo názvu, sídlo a místo podnikání prodávajícího s uvedením IČO a DIČ;
   - název a sídlo kupujícího s uvedením IČO a DIČ;
   - číslo smlouvy, podle které se uskutečňuje plnění;
   - předmět plnění označený v souladu se smlouvou a množství dodaných měrných jednotek včetně výrobních čísel jednotlivých ks zboží;
   - jméno odpovědné osoby prodávajícího, razítko a podpis této odpovědné osoby;
   - jméno pověřené osoby přejímajícího, razítko, datum převzetí a podpis této pověřené osoby;
   - kupní cenu za měrnou jednotku položky zboží v Kč bez DPH;
   - kupní cenu celkem za dodávku zboží v Kč bez DPH.
3. Kupující uhradí fakturovanou částku prodávajícímu do 30 dnů ode dne doručení faktury. Faktura se považuje za uhrazenou okamžikem odepsání platby z účtu kupujícího a směrováním na účet prodávajícího. V případě, že faktura bude kupujícímu doručena v období od 15. prosince příslušného kalendářního roku do 15. ledna roku následujícího, prodlužuje se splatnost takové faktury o 30 dnů.
4. Kupující neposkytuje zálohové platby.
5. Faktura bude prodávajícím doručena kupujícímu na adresu:
   Sekce vyzbrojování a akvizic MO
   odbor komunikačních a informačních systémů
   nám. Svobody 471/4
   160 01 Praha 6
6. Jednu kopii faktury včetně příloh zašle prodávající osobě pověřené k převzetí zboží.
7. Kupující je oprávněn fakturu vrátit před uplynutím její splatnosti, neobsahuje-li některý údaj nebo doklad uvedený ve smlouvě nebo má jiné závady v obsahu nebo nedostatečný počet výtisků. Při vrácení faktury kupující uvede důvod jejího vrácení a v případě oprávněného vrácení prodávající vystaví fakturu novou. Oprávněným vrácením faktury přestává běžet původní lhůta splatnosti a běží znovu ode dne doručení nové faktury kupujícímu. Prodávající je povinen novou fakturu doručit kupujícímu do 10 dnů ode dne doručení oprávněně vrácené faktury prodávajícímu.
8. Pokud budou u prodávajícího shledány důvody k naplnění institutu ručení za daň podle § 109 zákona č. 235/2004 Sb., bude kupující při zasílání úplaty vždy postupovat zvláštním způsobem zajištění daně podle § 109a tohoto zákona.

IX.
Přechod vlastnického práva a odpovědnost za škody na zboží

1. Vlastnické právo ke zboží přechází na kupujícího okamžikem podpisu dodacího listu zástupci obou smluvních stran po předání zboží.
2. Nebezpečí škody na zboží přechází z prodávajícího na kupujícího okamžikem podpisu dodacího listu zástupci obou smluvních stran po předání zboží.

X.
Záruka za jakost a vady zboží

1. Ve smyslu ustanovení § 2113 a násl. OZ prodávající přejímá záruku za jakost dodaného zboží od data převzetí zboží pověřenou osobou po dobu 24 měsíců.
2. Práva z vadného plnění se řídí ustanoveními § 2099 a násl. OZ.
3. Vady zboží v záruce je oprávněn uplatnit supervizor KIS VÚ 3255, ředitel VÚ 3255 nebo jím pověřené osoby u prodávajícího bezodkladně po jejich zjištění mailem, a to na e-mail: mopki@sefira.cz.
4. Prodávající je povinen zahájit odstraňování vady v nejkratším možném termínu, nejpozději však následující pracovní den od nahlášení vady (Response Time). Nahlášenou vadu je prodávající povinen odstranit nejpozději do 3 pracovních dnů (Repair Time) od zahájení opravy v místě plnění s tím, že objednatel zajistí technikům prodávajícího po uvedenou dobu přístup k opravovaným technologickým komponentům. V případě e-mailového nahlášení se tato doba počítá od odeslání těchto nahlášení kupujícím. V případě, že v požadované lhůtě nebude prodávající schopen tuto vadu odstranit, je povinen do dalších 24 hodin zabezpečit bezplatné poskytnutí náhradního zboží minimálně stejných či vyšších technických parametrů jako je vadné zboží. Vyměněné vadné díly s výjimkou paměťových médií (pevných disků – HDD, SSD, SD atd.) se stanou majetkem prodávajícího. Místo plnění z hlediska záručních reklamací je stejné jako místo plnění podle čl. V. smlouvy.
5. O odstranění vady bude sepsán a podepsán zástupci prodávajícího a kupujícího „Protokol o odstranění vady a předání zboží".

XI.
Smluvní pokuty a úroky z prodlení

1. Prodávající zaplatí kupujícímu v případě prodlení s dodáním zboží v termínu uvedeném v bodu 1. čl. VI. smlouvy smluvní pokutu ve výši 5 000,- za každý započatý den prodlení a to až do úplného splnění závazku nebo do zániku smluvního vztahu. Tím nejsou dotčena ustanovení čl. XIII. smlouvy. Okamžik práva fakturace vzniká prvním dnem prodlení.
2. Prodávající zaplatí kupujícímu v případě nedodržení sjednaného termínu odstranění vady zjištěné v záruční době podle podmínek uvedených v čl. X. smlouvy smluvní pokutu ve výši 2 500,- Kč za každý započatý den prodlení, a to až do podpisu „Protokolu o odstranění vady a předání zboží". Tím nejsou dotčena ustanovení čl. XIII. smlouvy. Okamžik práva fakturace vzniká prvním dnem prodlení.
3. Smluvní pokuty a úroky z prodlení jsou splatné do 30 dnů ode dne doručení vyúčtování.
4. Kupující zaplatí prodávajícímu za prodlení s úhradou faktury za každý započatý den prodlení úrok z prodlení v zákonné výši.

5. Smluvní pokuty a úrok z prodlení hradí povinná smluvní strana bez ohledu na to, zda a v jaké výši vznikla druhé smluvní straně v této souvislosti škoda. Náhrada škody je vymahatelná samostatně vedle smluvních pokut a úroku z prodlení v plné výši.

XII.
Zvláštní ujednání

1. Vztahy mezi smluvními stranami se řídí právním řádem České republiky.
2. Ve smluvně výslovně neupravených otázkách se tento závazkový vztah řídí ustanoveními OZ.
3. Prodávající prohlašuje, že dodané zboží není zatíženo žádnými právy třetích osob. Prodávající odpovídá za případné porušení práv z průmyslového nebo jiného duševního vlastnictví třetích osob.
4. Smluvní strany si bezodkladně sdělí skutečnosti, které se týkají změn některého z jejich základních identifikačních údajů, včetně právního nástupnictví.
5. Jednacím jazykem při jakémkoliv ústním jednání či písemném styku, souvisejícím s plněním této smlouvy, je český jazyk.
6. Prodávající souhlasí se zveřejněním obsahu smlouvy s výjimkou informací týkajících se obchodního tajemství.
7. Prodávající není oprávněn v průběhu plnění svého závazku podle této smlouvy a ani po jeho splnění bez písemného souhlasu kupujícího poskytovat jakékoli informace, se kterými se seznámil v souvislosti s plněním svého závazku a podkladovými materiály v listinné či elektronické podobě, které mu byly poskytnuty v souvislosti s plněním závazku podle této smlouvy, třetím osobám (mimo subdodavatele). Poskytnuté informace jsou ve smyslu § 1730 OZ důvěrné.
8. Prodávající s podpisem smlouvy uděluje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, souhlas kupujícímu, jako správci údajů, se zpracováním jeho osobních a dalších údajů ve smlouvě uvedených pro účely naplnění práv a povinností vyplývajících z této smlouvy, a to po dobu její platnosti a dobu stanovenou pro archivaci.
9. Prodávající není oprávněn zcela ani zčásti postoupit na třetí osobu žádné ze svých práv, ani žádný ze svých závazků plynoucích z této smlouvy a ani tuto smlouvu jako celek.

XIII.
Zánik závazků ze smluvního vztahu

1. Smluvní strany se dohodly, že závazek ze smluvního vztahu zaniká v těchto případech:
   a) splněním všech závazků řádně a včas;
   b) dohodou smluvních stran při vzájemném vyrovnání účelně vynaložených a prokazatelně doložených nákladů ke dni zániku smlouvy;
   c) jednostranným odstoupením od smlouvy kupujícím pro její podstatné porušení prodávajícím;
   d) jednostranným odstoupením od smlouvy v případě, že bude vůči majetku prodávajícího vyhlášeno insolvenční řízení, v němž bude vydáno rozhodnutí o úpadku nebo byl-li vůči prodávajícímu insolvenční návrh zamítnut, z důvodů, že majetek společnosti nepostačuje k úhradě nákladů insolvenčního řízení;

e) v případě, že prodávající uvedl v nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek zadávacího řízení.

2. Smluvní strany se dohodly, že podstatným porušením smlouvy ze strany prodávajícího ve smyslu § 2002 odst. 1 OZ je:
   a) nedodržení doby plnění delší než 10 dnů;
   b) nedodržení sjednaného množství, jakosti nebo druhu zboží;
   c) nedodržení ujednání o záruce za jakost zboží;
   d) neodstranění vad zboží ve sjednané době delší než 3 dny.

XIV.
Závěrečná ujednání

1. Smlouva je vyhotovena ve dvou výtiscích o 8 listech a třech přílohách o 6 listech, z nichž každý má platnost originálu. Každá ze smluvních stran obdrží po jednom výtisku.
2. Smlouva může být měněna či doplňována vzájemně odsouhlasenými a podepsanými písemnými a vzestupně očíslovanými dodatky, které se stávají její nedílnou součástí.
3. Smluvní strany prohlašují, že jim nejsou známy žádné skutečnosti, které by uzavření smlouvy vylučovaly a berou na vědomí, že v plném rozsahu nesou veškeré právní důsledky plynoucí z vědomě jimi udaných nepravdivých údajů. Na důkaz svého souhlasu s obsahem smlouvy připojují pod ní své podpisy.
4. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední smluvní stranou.
5. Nedílnou součástí smlouvy jsou přílohy:
   - příloha č. 1 – „Specifikace zboží" – 7 listů
   - příloha č. 2 – „Cenový rozklad" – 1 list
   - příloha č. 3 – „Katalogizační doložka" – 1 list

V Praze dne 19.10.2016

Ing. Jiří NYKODÝM
ředitel odboru

V Praze dne 18.10.2016

Ing. Marián JURÍK
ředitel

MO - Sekce vyzbrojování a akvizic

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

Podrobná technická specifikace dodávaného hardware, software a služeb

Hardware

Datový rozvaděč

- 2x datový rozvaděč 19", výška 27U, hloubka 1000mm včetně systému pro monitoring teploty, vlhkosti a kódového zámku racku
- 2x záložní zdroj APC Smart-UPS 2200VA
- 2x přepínač vstupního napájení APC AP7721
- 2x KVM přepínač včetně LCD pro správu serverů
- 2x gigabitový L2 přepínač Cisco 2960X, 24 portů

HSM

- 2x HSM Thales nShield Connect 500+ F3; SEE Ready (no nTokens) včetně podpory na 2 roky
- 1x Thales Security World Software for Windows
- 6x Thales Additional 'soft' Client Licence - [does not include nToken]
- 10x Thales standard nCipher smartcards

Server

- 8x server HP DL1200 Gen9 včetně podpory NBD na 3 roky
- konfigurace serveru
  - CPU - Xeon E5-2603v4
  - RAM - 16GB, DDR4 ECC
  - HDD - 2x SAS 300GB, zapojený v RAID-1
    - 1x SATA 1000GB
  - 2x síťová karta 10/100/1000Mbit/s
  - 2x napájecí zdroj

Notebook

- 2x notebook DELL Latitude E5570
- konfigurace notebooku
  - CPU - i5-6300U
  - 8GB RAM
  - 500GB HDD
  - integrovaná čtečka čipových karet včetně podpory NBD na 3 roky
- 2x externí čtečka čipových karet s numerickou klávesnicí (PIN pad)

Software

- 8x licence OS Windows Server 2012R2 Standard
- 2x licence MS SQL Server 2014 Standard
- 2x certifikační autorita Safelayer KeyOne CA s licencí pro 10.000 uživatelů, 200 serverů a zařízení.
  Licence zahrnuje služby validační autority pomocí OCSP, službu KeyRecovery a konektor na HSM moduly Thales.
- 2x registrační autorita Safelayer KeyOne XRA
- 2x lokální pracovitě registrační autority Safelayer KeyOne LXRA
- 2x autorita časových razítek Safelayer KeyOne TSA včetně konektoru na HSM Thales.

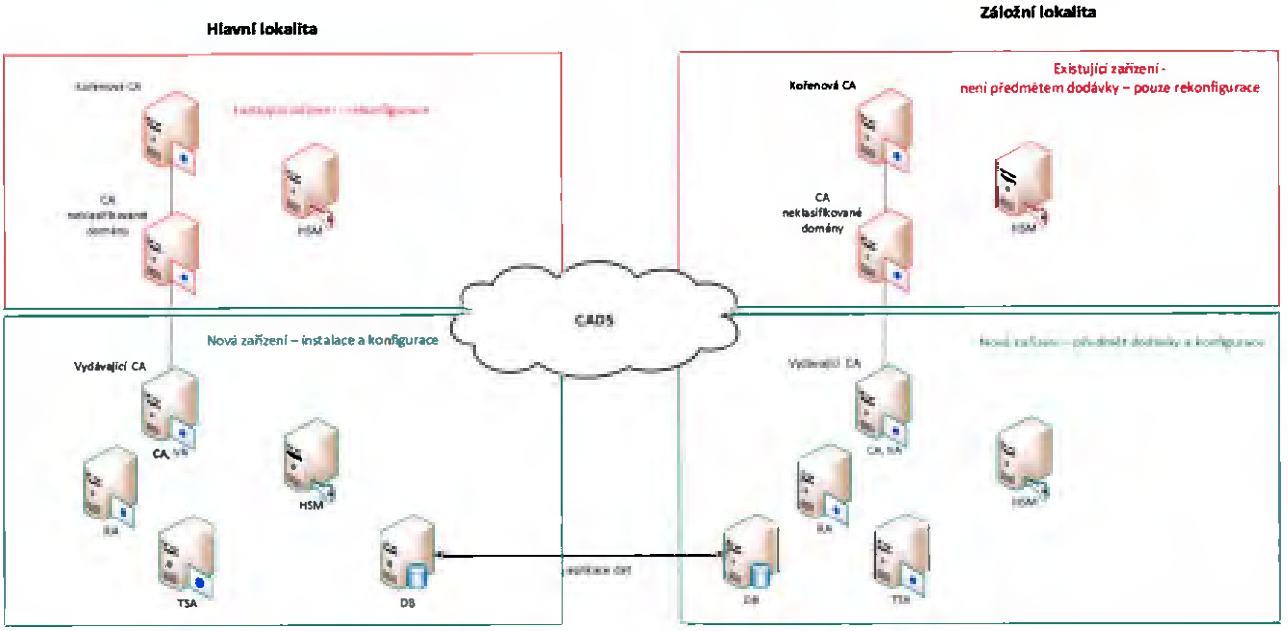
Certifikační autorita

Pracoviště vydávající CA bude realizováno jako samostatný fyzický server s operačním systémem MS Windows Server 2012 R2. Služby CA budou realizovány produktem Safelayer KeyOne CA, který bude instalován na server CA. Klíče vydávající CA budou uloženy v HSM. Server bude umístěn v racku, který bude součástí pracoviště vydávající CA. Součástí racku bude dále veškerá další nezbytná technologie zahrnující:

- systémy pro monitoring teploty a vlhkosti, kódový zámek racku;
- nepřerušitelný zdroj napájení (UPS);
- automatický přepínač vstupního napájení (ATS);
- KVM přepínač pro správu serverů;
- přepínač Cisco 2960X;
- kryptografický modul HSM Thales pro ukládání kryptografických klíčů;
- databázový server s MS SQL Server 2014 pro ukládání provozních dat CA, VA a TSA.

Produkt KeyOne společnosti Safelayer patří mezi robustní PKI řešení určené pro enterprise prostředí. Je využíván například pro vydávání španělských eID průkazů (FNMT - Fábrica Nacional de Moneda y Timbre) s více než 2 milióny certifikátů vydávaných každý rok nebo pro Generální španělské ředitelství policie a civilní stráže s více než 30 milióny vydaných certifikátů. Dále je KeyOne CA používán ve vojenských strukturách členských zemích NATO a je certifikován na úroveň NATO Secret a Common Criteria EAL4 + (profil ALC_FLR.2).

Vydávající CA bude se všemi podpůrnými technologiemi vybudována ve dvou zcela identických vyhotoveních (hlavní a záložní). Záložní pracoviště není určeno k rutinnímu provozu, pouze jako záloha pro případ výpadku hlavního pracoviště. Celková architektura navrženého řešení je znázorněna na Obr. 1.



Obrázek 1 - Architektura řešení

Autorita časových razítek
Pracoviště autority časových razítek (TSA) bude realizováno jako samostatný fyzický server s operačním systémem MS Windows Server 2012 R2. Služby TSA budou realizovány produktem Safelayer KeyOne TSA, který bude instalován na server. Klíče TSA budou uloženy v HSM. Server bude umístěn v racku, který bude součástí pracoviště vydávající CA. Primárním zdrojem přesného času pro TSA bude časový server Zadavatele dostupný pomocí protokolu NTP. Součástí realizace pracoviště výdeje časových razítek bude i vytvoření provozní a bezpečnostní dokumentace autority časových razítek této úrovně a vyškolení obsluhy.

Registrační autorita
Pracoviště registrace uživatelů (RA) bude realizováno jako samostatný fyzický server s operačním systémem MS Windows Server 2012 R2. Služby RA budou realizovány produktem Safelayer KeyOne XRA, který bude instalován na server. Klíče RA budou uloženy v HSM. Server bude umístěn v racku, který bude součástí pracoviště vydávající CA.
Pracoviště RA bude dále obsahovat dva notebooky se software Safelayer KeyOne LXRA, které budou realizovat lokální registrační místa.
Součástí realizace pracoviště registrace uživatelů bude i vytvoření provozní a bezpečnostní dokumentace certifikačních autorit této úrovně a vyškolení obsluhy.

Výše uvedený hardware, software a služby budou dodány v souladu se specifikací zadavatele:

1. Služba implementace PKI do doménového prostředí, v rámci které:
- zaktualizuje obsah stávajícího elektronického dokumentu „Analýza implementace projektu Integrace funkčních služeb do neutajované domény" na bázi HW a SW s certifikací FIPS 140-2 úrovně dle ACP185 v dotčených bezpečnostních doménách komunikačních a informačních systémů (KIS) rezortu MO; do dokumentu zapracuje i způsob řešení archivace certifikátů a Certificate Revocation List (dále jen „CRL"), zálohování všech dat PKI MO, řešení zpětného ověřování platnosti certifikátů a způsob publikace certifikátů; HSM se požaduje dodat a použít pro CA i pro TSA; tyto HSM musí umožňovat i práci v režimu FIPS 140.2 Level 3, ale požaduje se ji nyní konfigurovat pro Level 2;
- rekonfiguruje stávající hlavní a záložní offline certifikační autoritu (dále jen „CA") první a druhé úrovně do souladu s ACP185;
- instaluje a konfiguruje všechny technologie PKI, dodané v rámci této zakázky, v souladu s ACP185 včetně integrace se zaváděnou správou jednotné identity (IdM) na platformě MS Identity Manager 2016 (v době plnění zakázky bude nainstalován a bude probíhat jeho konfigurace; v případě zdržení jeho konfigurace se požaduje čerpat informace pro PKI z Active Directory; v systému nebudou v době plnění zakázky reální uživatelé, ale pouze testeři);
- vyškolí správu dodaných registračních autorit (dále jen „RA"), vydávajících CA a autorit pro časová razítka (dále jen „TSA") i novou správu dříve dodaných KCA a CA;
- implementuje řešení archivace certifikátů a CRL, a zálohování všech dat PKI MO, potřebných pro zotavení z případné havárie; u certifikátů pro zařízení aktualizuje návrh optimální doby krátkodobé archivace s ohledem na jejich velký počet a možnosti dostupného úložného prostoru; technologie a licence, spojené s tímto řešením, zahrne do souprav CA; při výběru licencí je nutné počítat s tím, že na pracovních stanicích je instalován MS Windows 7 (výhledově MS Windows 10) a na serverech MS Windows Server 2012R2 (výhledově MS Windows Server 2016);
- dodá licence pro správu certifikátů pro 10.000 uživatelů, 200 serverů a aplikací; technologicky musí být řešení dimenzováno pro 25.000 uživatelů;

- implementuje řešení zpětného ověřování platnosti certifikátů až 50 let zpětně; technologie a licence, spojené s tímto řešením, zahrne do souprav CA; toto řešení bude nahrazovat jednu z funkcionalit zatím neexistujícího systému správy dokumentů (DMS) a elektronického archivu;
- realizuje bezpečný a provozně spolehlivý způsob publikace certifikátů, proces vydávání CRL pro publikaci odvolaných certifikátů a implementuje Online Certificate Status Protocol (dále jen „OCSP"), (technologie a licence, spojené s tímto řešením, zahrne do souprav CA) pomocí Online Responderů s vysokou dostupností pro online ověřování certifikátů certifikačních autorit:
  - pomocí publikace do Active Directory provozovaných systémů, do metabáze MS Identity Manager a pomocí HTTP protokolu na webové servery v síti resortu MO a v DMZ Internetu;
  - pro mobilní zařízení a aktivní síťové prvky pomocí protokolu Simple Certificate Enrollment Protocol (dále jen „SCEP") do interní sítě;
- navrhne a do provozní dokumentace CA, RA a TSA zahrne Plán obnovy po havárii (Recovery plan) a proces jeho testování; v rámci testování ověří i přebírání rolí záložními technologiemi PKI MO a jejich správou;
- vytvoří provozní a bezpečnostní dokumentaci CA, RA a TSA, která bude svou strukturou a rozsahem vycházet z legislativy pro APCS a bude adaptovaná na prostředí rezortu MO;
- navrhne právně korektní znění smluvního ujednání mezi provozovatelem (který je zároveň zaměstnavatelem) a uživatelem (který je zároveň zaměstnancem) o právech a povinnostech při využívání služeb PKI MO.

2. Hlavní a záložní pracoviště vydávající - CA (certifikační autorita) pro uživatele, aplikace a technologie jedné subdomény neklasifikované domény, související technologie, dokumentaci a zaškolení provozního a bezpečnostního managementu (vydávající CA bude při žádosti o vydání certifikátu ověřovat identitu žadatele vůči IdM);

3. Hlavní a záložní pracoviště výdeje časových razítek - TSA (autorita pro časová razítka) v takovém rozsahu, aby bylo možné v celé budované části PKI MO využívat funkcionalitu časových razítek (synchronizaci času zajistit se stávajícím NTP serverem);

4. Hlavní a záložní pracoviště registrace uživatelů a zařízení - RA (registrační autorita) v budované části PKI MO.

S ohledem na výhledovou možnost křížové certifikace s NATO PKI a s PKI dalších orgánů státní správy ČR požaduje kupující při realizaci veřejné zakázky zohlednit tyto podmínky a požadavky:

- PKI MO založit na tříúrovňové architektuře zdvojených teritoriálně vzdálených certifikačních autorit. Hlavní a záložní certifikační autority 1. a 2. úrovně již byly dodány a uvedeny do testovacího provozu. Prodávající na základě informací, vyžádaných od managementu jednotlivých IS, upraví stávající návrh optimálního počtu vydávajících CA v bezpečnostních subdoménách jednotlivých IS a možné využívání společných CA pro více IS konkrétní bezpečnostní domény. Prodávající rovněž zaktualizuje návrh vhodného řešení geografického clusteru CA v jednotlivých úrovních (failover, load balancing, jejich kombinace, jiné vhodné řešení). Přitom se požaduje akceptovat následující názvosloví:
  - Certifikační autority, cílově umístěné v hlavním datovém centru (Main Datacenter):
    a) CA první úrovně v režimu offline:
       - Hlavní kořenová CA (Main root CA)

b) CA druhé úrovně v režimu offline:
- Hlavní CA neklasifikované domény (Main CA- unclassified domain)
- Hlavní CA důvěrné domény (Main CA - confidential domain)
- Hlavní CA tajné domény (Main CA - secret domain)

c) CA třetí úrovně v režimu online:
- Hlavní vydávající CA subdomény IS1 (Main issuing CA - subdomain IS1)
- Hlavní vydávající CA subdomény IS2 (Main issuing CA - subdomain IS2)
- Hlavní vydávající CA subdomény ISn (Main issuing CA - subdomain ISn)

o Certifikační autority, cílově umístěné v záložním datovém centru (Backup Datacenter):

a) CA první úrovně v režimu offline:
- Záložní kořenová CA (Backup root CA)

b) CA druhé úrovně v režimu offline:
- Záložní CA neklasifikované domény (Backup CA - unclassified domain)
- Záložní CA důvěrné domény (Backup CA - confidential domain)
- Záložní CA tajné domény (Backup CA - secret domain)

c) CA třetí úrovně v režimu online:
- Záložní vydávající CA subdomény IS1 (Backup issuing CA - subdomain IS1)
- Záložní vydávající CA subdomény IS2 (Backup issuing CA - subdomain IS2)
- Záložní vydávající CA subdomény ISn (Backup issuing CA - subdomain ISn)

- Všechny technologie dodat do lokality Praha – přesun záložních technologií mimo lokalitu Praha zabezpečí kupující.
- Technologie všech CA i TSA použít ve verzi pro datové rozvaděče (rackmount), které se rovněž požaduje dodat. Datové rozvaděče opatřit technologií (např. CMC-TC) pro monitoring teploty, vlhkosti a otevírání rozvaděče včetně zabezpečení elektronickým kódovým zámkem.
- Každá CS, TSA i RA musí tvořit samostatný technologický celek (tzn. celkem 6 celků, každý s vlastním kusovníkem). Požaduje se jeden rack v každém DC (tj. celkem 2 ks), který bude obsahovat CA i TSA. V případě sdílení některých technologií mezi CA a TSA musí být sdílené technologie účetně přiděleny pouze k jedné z těchto autorit.
- S ohledem na průměrnou dobu trvání servisní podpory hardware a software ze strany výrobců je cyklus jeho obměny stanoven na 10 let. Při přechodu na nový hardware a software může být ten původní vyřazen z provozu až po zahájení a ověření funkčnosti nového. V datových rozvaděčích je tedy nutné prostorově počítat s překryvnou dobou chodu obměňované i nové technologie a musí k tomu být dimenzováno i napájení a kapacita datových rozvodů.
- Z důvodu nižších pořizovacích, provozních a servisních nákladů upřednostnit (ale pouze v případě, že budou splňovat všechna kritéria tohoto zadání) již používanou platformu Microsoft a HP pro serverové technologie a licence SW, Cisco pro síťové technologie, Thales pro kryptografické technologie a APC pro technologie UPS. V současné době jsou pořízeny hlavní a záložní offline Root CA a hlavní a záložní offline Policy CA na platformě serverů HP ProLiant DL360 Gen9 s licencemi MS Windows Server 2012R2, nainstalovanými ve virtuálním prostředí VMware ESXi, a s moduly HSM Thales nShield Connect 500+. Propojení technologií v rozvaděčích s hlavními a záložními CA je řešeno pomocí Cisco Catalyst 2960-CG. Technologie jsou pouze v testovacím provozu.
- Zabezpečení životního cyklu čipových karet (PKI smartcard) je a zůstane v režii Hlavního velitelství Vojenské policie (HVVP), které zároveň provozuje registrační autoritu (RA) smluvního akreditovaného poskytovatele certifikačních služeb (APCS). Uchazeči budou na požádání poskytnuty technické údaje používaných karet a jejich čteček a případně i popis

jejich životního cyklu. Uživatelské certifikáty se požaduje vydávat na aktuálně používané karty s embeddingem čipu Gemalto TOP GX4 72kB, splňující parametry ISO 7816, s middleware CryptoPlus ProID. Tyto karty jsou opatřovány samolepkou s personalizačními údaji a jsou aktivovány a vydávány (příp. vraceny a deaktivovány) na registračním místě.

- Pracoviště RA se požaduje vybavit i technologiemi a licencemi SW včetně možnosti správy přes webové rozhraní pro evidenci certifikátů a žádostí o ně. Technologie RA pro výdej certifikátů se požaduje fyzicky oddělit od stávajících technologií pro výdej a správu čipových karet z důvodu možného umístění v odlišně zabezpečených objektech, ale se zachováním konektivity do společné datové sítě.
- Distribuce certifikátů, CRL a dalších potřebných dat bude mezi CA jednotlivých úrovní řešena offline na vhodných datových nosičích cestou jejich provozně-bezpečnostních správ. Veškerý transfer těchto dat bude auditován a kontrolován.
- V aktualizovaném návrhu a při následné realizaci PKI MO zohlednit vydávání certifikátů pro:
  - prokazování identity koncových i síťových zařízení;
  - ochranu software po jeho zveřejnění před změnami;
  - ochranu (podpis a šifrování) zpráv, zasílaných elektronickou poštou;
  - podepisování dat digitálním podpisem, obsahujícím aktuální čas;
  - zabezpečení komunikace přes méně zabezpečené sítě včetně mezinárodní sítě Internet;
  - šifrování dat na datových nosičích;
  - přihlašování (autentizaci) pomocí karty SmartCard.
- U všech komponent, které to umožňují a u kterých to má opodstatnění, realizovat osazení dvěma napájecími zdroji, jejich napájení zabezpečit ze dvou nezávislých napájecích větví (pokud to v místě instalace bude možné) a jejich zálohování řešit pomocí UPS.
- Vydání certifikátu umožnit vždy až po ověření identity uživatele, serveru, aplikace nebo síťového prvku. Zároveň vždy ověřit oprávněnost k jeho vlastnictví a v případě uživatelského certifikátu navíc akceptovat podmínky k jeho korektnímu používání a ochraně. V případech, kdy tyto kroky mohou být zautomatizovány, se požaduje využít autoenrollmentu a přístupu přes zabezpečené webové rozhraní.
- Dobu platnosti certifikátů stanovit takto:
  - Platnost certifikátů CA 1. úrovně: 20 let;
  - Platnost certifikátů CA 2. úrovně: 10 let;
  - Platnost certifikátů CA 3. úrovně: 5 let;
  - Platnost certifikátů pro uživatele: 2 roky;
  - Platnost certifikátů pro zařízení: navrhnout optimální dobu platnosti podle účelu použití.
- Dobu archivace certifikátů a CRL u certifikátů pro uživatele a certifikátů CA stanovit minimálně na 50 let od ukončení jejich platnosti. Archivaci provádět na dvě geograficky vzdálená úložiště (datová centra).
- V provozní dokumentaci popsat proces migrace platných i archivovaných certifikátů a CRL na nový HW a SW v návaznosti na jeho relativně krátký životní cyklus.
- Minimální délka klíčů, použitelné hashovací a šifrovací algoritmy:
  a) CA 1. úrovně:
  - SHA-2, size 512b;
  - RSA, size 4096b;
  - ECDSA, P-521;
  - AES, size 256b;
  - MQV, size 256b;
  - ECDH, size 256b;

b) CA 2. úrovně:

- SHA-2, size 384b;
- RSA, size 2048b;
- ECDSA, P-384;
- AES, size 256b;
- MQV, size 256b;
- ECDH, size 256b;

c) CA 3. úrovně:

- SHA-2, size 384b;
- RSA, size 2048b;
- ECDSA, P-384;
- AES, size 256b;
- MQV, size 256b;
- ECDH, size 256b;

d) Pro podepisování:

- SHA-2, size 256b;
- RSA, size 2048b;
- ECDSA, P-256;
- AES, size 128b;
- MQV, size 256b;
- ECDH, size 256b;
- Diffie-Hellman, size 256b.

Příloha č. 2 smlouvy č. 165310317

CENOVÝ ROZKLAD

Název zboží	MJ	Počet MJ	Cena bez DPH za MJ v Kč	DPH 21% za MJ v Kč	Cena včetně DPH za MJ v Kč	Celková cena bez DPH v Kč	Celková cena včetně DPH v Kč
Pracoviště - CA, včetně dokumentace a implementace	kus	2	2 375 000,-	498 750,-	2 873 750,-	4 750 000,-	5 747 500,-
Pracoviště - TSA, včetně dokumentace a implementace	kus	2	535 000,-	112 350,	647 350,-	1 070 000,-	1 294 700,-
Pracoviště - RA, včetně dokumentace a implementace	kus	2	419 000,-	87 990,-	506,990,-	838 000,-	1 013 980,-
CELKEM ZA PŘEDMĚT SMLOUVY						**6 658 000,-**	**8 056 180,-**

Příloha č. 3 smlouvy č. 165310317

KATALOGIZAČNÍ DOLOŽKA[1]

K zabezpečení procesu katalogizace položek majetku (výrobků), které jsou předmětem tohoto obchodně-závazkového vztahu (dále jen „**smlouva**") a které podléhají katalogizaci podle zásad Kodifikačního systému NATO (dále jen „**NCS**") a Jednotného systému katalogizace majetku v ČR (dále jen „**JSK**") se **prodávající** zavazuje:

1. Na vlastní náklady zpracovat nebo zabezpečit zpracování Souboru povinných údajů pro katalogizaci (dále jen „**SPÚK**") všech nekatalogizovaných položek majetku definovaných smlouvou (platí i pro položky pro provoz a údržbu, jejichž katalogizace je vyžadována) seřazené podle rozpadu vždy prostřednictvím aplikace umístěné na www.cz-katalog.cz nebo na www.aura.cz/mcrlnew/.

2. Povinnou součástí zpracování SPÚK každé dosud nekatalogizované položky majetku je:
   a) fotografie reálně zobrazující dodávanou položku majetku ve formě elektronického souboru ve formátu JPG, rozlišení do 1024x768 bodů[2];
   b) hypertextový odkaz na webovou stránku nebo elektronický soubor, které obsahují technické údaje o výrobku. Elektronický soubor musí být ve formátu JPG, rozlišení do 1024x768 bodů, nebo ve formátu PDF, v rozměrech strany A4. V případě, že nelze poskytnout hypertextový odkaz nebo elektronický soubor, doložit na vyžádání oddělení katalogizace majetku Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti (dále jen „**OdKM**") správnost údajů nezbytných k provedení popisné identifikace jiným způsobem.

3. Doručit OdKM SPÚK v termínu *5 dnů* před fyzickým dodáním předmětu smlouvy prostřednictvím aplikace umístěné na www.cz-katalog.cz nebo na www.aura.cz/mcrlnew/.

4. Na vlastní náklady zabezpečit zpracování návrhu katalogizačních dat o výrobku popisnou metodou identifikace položek v podobě elektronických transakcí LNC (Žádost o přidělení identifikačního čísla NATO s popisnými charakteristikami) vybranou katalogizační agenturou[3] každé smlouvou definované položky zásobování vyrobené v ČR nebo zemích mimo NATO či Tier 2[4] a podléhající katalogizaci podle zásad NCS a JSK.

5. Zabezpečit doručení návrhu katalogizačních dat o výrobku (transakce LNC) nejpozději 10 dnů před fyzickým dodáním předmětu smlouvy.

6. Dodat bez prodlení v průběhu realizace smlouvy informace o všech změnách, týkajících se předmětu smlouvy, které mají vliv na identifikaci katalogizovaných položek majetku, včetně změn u položek majetku nakupovaných prodávajícím od subdodavatelů.

Katalogizační doložka je naplněna dodáním úplných a bezchybných dat, které je potvrzeno vydáním kladného „Stanoviska Úř OSK SOJ k naplnění katalogizační doložky".

Přidělené identifikátory (KČM, NSN) a zpracovaná katalogizační data jsou dostupná na www.cz-katalog.cz nebo na www.aura.cz/mcrlnew/ po ukončení procesu katalogizace majetku.

Kontaktní adresa:

Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti
ODDĚLENÍ KATALOGIZACE MAJETKU
nám. Svobody 471
160 01 PRAHA 6

TEL.: 973 213 913 INTERNET: www.okm.army.cz WAP: http://wap.okm.army.cz
FAX: 973 213 930 E-MAIL: katalogizace@army.cz

[1] Platná pro kupní smlouvy uzavírané po 1. červenci 2013.

[2] Prodávající tímto souhlasí s použitím dodané fotografie pro účely JSK a NCS.

[3] Fyzická nebo právnická osoba, držitel osvědčení podle §11 zákona č. 309/2000 Sb., o obranné standardizaci, katalogizaci a státním ověřování jakosti výrobků a služeb určených k zajištění obrany státu a o změně živnostenského zákona. Aktuální seznam katalogizačních agentur umístěn na www.okm.army.cz.

[4] Aktuální seznam zemí NATO, Tier 2 a Tier 1 viz odkaz na www.okm.army.cz, odkaz na www.int/structur/AC/135/welcome.htm.