

**Klasifikace: Veřejný dokument**



Technická specifikace

Příloha č. 4 Výzvy k podání nabídek pro výběrové řízení „Výstavba interní certifikační autority a implementace systému pro bezpečnou správu privátních klíčů“

Obsah

[1 Verze dokumentu 2](#_Toc106277756)

[2 Seznam zkratek 3](#_Toc106277757)

[3 Úvod 7](#_Toc106277758)

[3.1 Předmět plnění veřejné zakázky 7](#_Toc106277759)

[3.2 Oblasti, které nejsou předmětem plnění veřejné zakázky 8](#_Toc106277760)

[4 Současný stav a popis prostředí 8](#_Toc106277761)

[5 Požadavky na plnění 8](#_Toc106277762)

[5.1 Zpracování metodik a dokumentace k obnově interní kořenové CA a vytvoření nové struktury CA 9](#_Toc106277763)

[5.1.1 Analýza současného stavu 9](#_Toc106277764)

[5.1.2 Návrh budoucího stavu 9](#_Toc106277765)

[5.1.3 Plán přechodu 21](#_Toc106277766)

[5.2 Dodávka technologií, licencí a školení 23](#_Toc106277767)

[5.2.1 Prvek pro HW podporu kryptografie a bezpečné uložení klíčů pro kořenovou CA 23](#_Toc106277768)

[5.2.2 Síťové HSM 24](#_Toc106277769)

[5.2.3 Záruka a záruční servis 26](#_Toc106277770)

[5.2.4 Licence 26](#_Toc106277771)

[5.2.5 Školení 27](#_Toc106277772)

[5.3 Supervize implementačních prací a navržených testů, včetně řešení nestandardních stavů 27](#_Toc106277773)

[5.3.1 Supervize a technická podpora zadavatele při implementaci řešení. 27](#_Toc106277774)

[5.3.2 Supervize a technická podpora při testování 28](#_Toc106277775)

[5.4 Post-implementační a technická podpora 28](#_Toc106277776)

[5.4.1 Post-implementační podpora 28](#_Toc106277777)

[5.4.2 Odborná technické podpora 29](#_Toc106277778)

[5.5 Služby na vyžádání 30](#_Toc106277779)

[6 Fáze dodávky a akceptační milníky 30](#_Toc106277780)

# Verze dokumentu

|  |  |  |
| --- | --- | --- |
| **Verze** | **Datum** | **Změny** |
| 1.0 | 15.6.2022 | Úvodní verze |

# Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

|  |  |
| --- | --- |
| Zkratka | Popis |
| AD, MS AD | Microsoft Active Directory |
| ACS | Administrator Card Set. Sada karet pro aktivaci bezpečnosti HSM |
| AS-IS | Současný stav |
| AKB | Architekt kybernetické bezpečnosti |
| API | Rozhraní pro programování aplikací (Application Programming Interface) |
| CA | Certifikační autorita |
| CLRDP | CRL Distribution Point. Distribuční místo pro získání CRL. |
| CP | Certifikační politika |
| CLR | Seznam zneplatněných certifikátů |
| Certifikát (pro PKI) | Je datová zpráva, která je vydána CA, spojuje veřejný klíč (=data pro ověřování elektronických podpisů) s podepisující osobou a umožňuje ověřit její identitu. |
| CISO | Manažer informační bezpečnosti (Chief Information Security Officer) |
| ČSN | Česká státní norma |
| DC | Domain controller. Řadič domény s Active Directory |
| eIDAS | Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES |
| GPA | Garant primárního aktiva |
| GPdA | Garant podpůrného aktiva |
| HA | Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance |
| Hardening | Hardening je proces zabezpečení konfigurace systému takovým způsobem, který omezí výskyt zranitelností využitelných útočníkem |
| Harmonogram | Harmonogram stanovený ve Smlouvě o dílo, konkrétně v její příloze „Harmonogram“ |
| HLD | Přehledový vysokoúrovňový design (High Level Design) |
| HSM | Hardware Security Module; hardwarový kryptografický prostředek pro ochranu provádění operací s kryptografickými klíči, včetně bezpečného ukládání klíčů |
| HW | Hardware |
| ICT | Informační a komunikační technologie (Information and Communication TechnoLogies) |
| IDM | Správa uživatelských účtů (Identity Management) |
| IS | Informační systém |
| ISVS | Informační systémy veřejné správy |
| ITSM | IT Service Management |
| KII | Kritická informační infrastruktura |
| LDAP | Lightweight Directory Access Protocol |
| LLD | Nízko úrovňový design (Low Level Design) |
| MB | Mega Byte |
| MCAS | Microsoft Cloud App Security |
| MD | Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day) |
| MDM | Správa mobilních zařízení (Mobile Device Management) |
| MFA | Vícefázové ověření (Multifactor Authentication) |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| On-premise | On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá |
| OS | Operační Systém |
| OTP | Jednorázové heslo (One Time Password) |
| PAM | Správa privilegovaných přístupů (Privileged Access Management) |
| párové klíče | Vzájemně svázaná dvojice klíčů pro vytváření digitálních podpisů (soukromý klíč) a pro ověřování digitálních podpisů (veřejný klíč). Veřejné klíče jsou vesměs publikovány v certifikátech spolu s dalšími údaji zejména o identitě podepisujícího subjektu. |
| PD | Pracovní Den |
| PKI | Infrastruktura správy a distribuce veřejných klíčů (Public Key Infrastructure); informační systém, produkující a využívající digitální certifikáty |
| Privilegovaný účet | Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění |
| RDP | Protokol na přenos vzdálené plochy (Remote Desktop Protocol) |
| RPO | Recovery Point Objective – cílový bod zotavení |
| RTO | Recovery Time Objective – cílová doba zotavení |
| s2s VPN | Site to site VPN |
| SaRS | Save and Recovery System. Systém online zálohování CA |
| SLA | Dohoda o úrovni poskytovaných služeb (Service Level Agreement) |
| Smlouva o dílo | Smlouva o dílo – Výstavba interní certifikační autority a implementace systému pro bezpečnou správu privátních klíčů  Závazný vzor Smlouvy o dílo je přílohou výzvy k podání nabídky |
| SSH | Zabezpečený protokol pro připojení k serverům |
| SSO | Systém jednotného přihlášení (Single Sign-On) |
| SW | Software |
| SŽ | Správa železnic, státní organizace |
| Token | Dedikované HW úložiště soukromého klíče uživatele – zpravidla čipová karta. |
| tps | Transakcí / sekundu |
| UAS | Uživatelsko-aplikační síť |
| VPN | Virtuální privátní síť (Virtual Private Network) |
| Uchazeč | Subjekt, který se v rámci tohoto výběrového řízení uchází o realizace veřejné zakázky s názvem „Výstavba interní certifikační autority a implementace systému pro bezpečnou správu privátních klíčů“. Uchazeč, který bude vybrán SŽ, se stane dodavatelem. |

Seznam zkratek pro specifické aplikace SŽ:

|  |  |
| --- | --- |
| Zkratka | Popis |
| ASVC | Automatické stavění vlakových cest |
| DŘT | Dispečerská řídicí technika |
| DDTS | Dálková diagnostika technologických systémů |
| CDP | Centrální dispečerské pracoviště |
| CDS | Centrální dispečerský systém |
| DŽDC | Dispečer železniční dopravní cesty |
| DŽIN | Dispečer železniční infrastruktury |
| ED | Elektro dispečer |
| GVD | Grafikon vlakové dopravy |
| SSZT | Správa sdělovací a zabezpečovací techniky |
| ST | Správa tratí |
| SŽE | Správa železniční energetiky |
| TechDS | Technologický a dohledový systém |
| TDS | Technologická datová síť |
| TDCDP | Traťový dispečer dálkového ovládání zabezpečovacího zařízení na CDP |
| VS | Vlakové soupravy |

# Úvod

Tento dokument je přílohou a nedílnou součástí výběrového řízení pro výběr dodavatele veřejné zakázky „Výstavba interní certifikační autority a implementace systému pro bezpečnou správu privátních klíčů“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

## Předmět plnění veřejné zakázky

Předmětem plnění veřejné zakázky je dodávka metodik a dokumentace, dodávka technologií, supervize implementace systémů certifikačních autorit (CA) v ICT prostředí SŽ. Nedílnou součástí plnění je také technická podpora dodaných technologií a post-implementační podpora zadavatele.

Tato zakázka bude obsahovat následující poptávané oblasti:

* Zpracování metodik a dokumentace k obnově interní kořenové CA a vytvoření nové struktury CA (vč. business, technologické a legacy zóny)
  + Analýza současného stavu
  + Návrh budoucího stavu
  + Plán přechodu
* Dodávka technologií, licencí a školení (pouze pro kořenovou CA a business zónu)
* Supervize implementačních prací a navržených testů, včetně řešení nestandardních stavů (pouze pro kořenovou CA a business zónu)
* Post-implementační a technická podpora
* Služby na vyžádání

## Oblasti, které nejsou předmětem plnění veřejné zakázky

Pro vyloučení pochybností Zadavatel uvádí, že následující oblasti **nejsou** předmětem plnění veřejné zakázky:

* **Dodávky licencí produktů Microsoft, výpočetní prostředky na platformě VMware, a zařízení typu notebook/PC:**
  + Součástí plnění dodavatele nejsou žádné licence produktů Microsoft. V případě, že dodavatel v návrhu budoucího stavu (TO-BE) využije licencí produktů Microsoft, tyto licence pro fázi implementace zajistí zadavatel v rámci své smlouvy se společností Microsoft centrálním nákupem potřebných licencí.
  + V případě, že návrh řešení nové PKI (TO-BE) vyžaduje výpočetní prostředky pro implementaci nových CA na platformě VMware, zadavatel vyčlení potřebné prostředky podle specifikace dodavatele.
  + Pro offline kořenovou CA provozovanou na zařízení typu notebook/PC, bude takové zařízení dodáno zadavatelem podle specifikací dodavatele.
* Dodávka technologií, licencí a školení pro technologickou a legacy zónu.
* Implementace navrženého řešení nové soustavy CA sestávající se z kořenové CA a soustavy podřízených CA.

Samotnou implementaci navrženého řešení provede zadavatel pod supervizí dodavatele.

# Současný stav a popis prostředí

Současný stav ICT prostředí zadavatele v oblastech certifikačních autorit, ActiveDirectory, komunikační infrastruktury a rozmístění datových center je přílohou č. 5 výzvy k podání nabídek.

# Požadavky na plnění

Plnění Veřejné zakázky se musí skládat alespoň z níže uvedených částí:

1. Zpracování metodik a dokumentace k obnově interní kořenové certifikační autority a vytvoření nové struktury certifikačních autorit
2. Dodávka technologií, licencí a školení
3. Supervize implementačních prací a navržených testů včetně řešení nestandardních stavů
4. Post-implementační a technická podpora
5. Služby na vyžádání

## Zpracování metodik a dokumentace k obnově interní kořenové CA a vytvoření nové struktury CA

V oblasti zpracování metodik a dokumentace k obnově interní kořenové certifikační autority a vytvoření nové struktury certifikačních autorit požaduje Zadavatel dodat následující části:

* Analýzu současného stavu
* Návrh budoucího stavu
* Plán přechodu

### Analýza současného stavu

**Zpracování analýzy současného stavu** prostředí interních certifikačních autorit v infrastruktuře SŽ a souvisejících technologií (především soustavy MS Active Directory a dalších systémů podílejících se na PKI nebo využívající PKI)

Provedení analýzy současného stavu interních CA a souvisejících systémů (AS-IS analýza) nutnou k tvorbě technického návrhu implementace a k zajištění všech potřeb této veřejné zakázky.

Výstupem analýzy bude zejména obecný popis současného stavu interních certifikačních autorit a PKI, komponent, jejich vztahů, souvislosti s doménovým modelem organizace a systémy Active Directory, použité hashovací a šifrovací algoritmy, současné nastavení obslužných procesů apod.

Součástí tohoto kroku musí být i analýza současných a budoucí potřeb zadavatele v oblasti interních CA a PKI, zejména ve vztahu k souvisejícím projektům.

Výstupem analýzy je samostatný dokument, který musí být oboustranně schválen (SŽ i budoucím dodavatelem) před zahájením dalších kroků (viz další kapitoly).

### Návrh budoucího stavu

Návrh budoucího stavu musí vycházet ze schváleného znění výstupu Analýzy současného stavu a být s ním plně v souladu a respektovat identifikované potřeby zadavatele a specifické vlastnosti jeho ICT prostředí.

#### Architektura a technické řešení nové kořenové certifikační autority a soustavy podřízených autorit

Zadavatel požaduje kompletní návrh budoucí architektury interních CA a technického návrhu jejich implementace v prostředí zadavatele s ohledem na současné i identifikované budoucí potřeby a využití PKI (TO-BE návrh). Zadavatel požaduje zpracování nejen pro obnovu současných služeb svých CA se zvýšeným důrazem na bezpečnost a škálovatelnost, ale návrh architektury a technického řešení bez ohledu na skutečnost, že v rámci této veřejné zakázky bude technicky implementována pouze část týkající se kořenové CA a „business zóny“.

Zadavatel požaduje zpracovat celkový HLD a LLD nové struktury interních CA v následujícím členění:

1. **kořenová certifikační autorita**
2. **podřízené vydávající certifikační autority pro „business zónu“**

Pro „business zónu“ navrhne dodavatel strukturu podřízených CA, které budou vydávat certifikáty uživatelům, aplikacím, službám a části infrastruktury.

1. **podřízené vydávající certifikační autority pro „technologickou zónu“**

Pro „technologickou zónu“ navrhne dodavatel strukturu podřízených CA, které budou vydávat certifikáty uživatelům, aplikacím, službám a infrastrukturním zařízením pro technologickou část (IoT, OT).

1. **podřízené vydávající certifikační autority pro „legacy zónu“**

V případě, že z analýzy současného stavu prostředí zadavatele a jeho potřeb v oblasti interní CA a PKI vyplyne potřeba vytvořit zvláštní podřízenou CA pro „legacy“ zařízení, dodavatele navrhne strukturu a technické řešení těchto podřízených CA.

Tato „legacy zóna“ může z důvodu zajištění zpětné kompatibility umožňovat práci s méně bezpečnými kryptografickými funkcemi a kratší délkou klíčů, pokud tato skutečnost vyplyne z úvodní analýzy.

U kořenové CA požaduje zadavatel využití prvků pro hardwarovou podporu kryptografie a bezpečného uložení certifikátů/klíčů (HSM) přímo připojitelných k hostitelskému systému[[1]](#footnote-2)

U všech podřízených CA požaduje zadavatel využití síťových prvků pro hardwarovou podporu kryptografie a bezpečného uložení certifikátů/klíčů (síťové HSM)[[2]](#footnote-3).

Dodavatel navrhne architekturu i technické řešení jako vysoce dostupné s ohledem na topologii ICT prostředí zadavatele.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| K.1 | návrh architektury | Dodavatel zpracuje:   * + - 1. Celkový HLD a LLD návrhu architektury budoucího stavu interních CA a PKI pro prostředí zadavatele       2. Popis architektury řešení a její rozkreslení v jazyce ArchiMate 3 nebo v jiném adekvátním nástroji       3. Architektura musí obsahovat minimálně všechny komponenty, popis vazeb, popř. datových toků, definici a popis všech integračních rozhraní poskytovaných jednotlivými komponentami, služby a popis zajištění vysoké dostupnosti s ohledem na celkovou architekturu.   Zejména musí být obsažen popis struktury soustavy CA, který ukazuje subsystémy a jejich vzájemný vztah, definice hlavních vazeb mezi jednotlivými prvky a vazby mezi soustavou CA a strukturou AD. |
| K.2 | platforma interních CA | Návrh platformy pro budování systému nových interních CA a související PKI.  Zadavatel požaduje využití platformy MS Windows, dodavatel navrhne přesnou specifikaci platformy. |
| K.3 | kořenová certifikační autorita | Specifikace vytvoření nové kořenové certifikační autority a návrh technického řešení kořenové certifikační autority (zóna kořenové CA).  Dodavatel navrhne i technické řešení pro zajištění vysoké bezpečnosti kořenové autority a její odolnosti proti kybernetickým útokům.  Zadavatel požaduje vytvoření samostatné kořenové certifikační autority v offline režimu s bezpečným uložením privátního klíče kořenové autority za využití budoucím dodavatelem dodaného prvku hardwarové podpory kryptografie a bezpečného uložení klíčů (HSM přímo připojitelné k hostitelskému systému)[[3]](#footnote-4). Zadavatel současně požaduje návrh kořenové certifikační autority s využitím virtualizace.  Související rizika dodavatel promítne do analýzy rizik. |
| K.4 | podřízené CA pro „business zónu“ | Zadavatel požaduje návrh architektury a technického řešení pro „business zónu“ v následující struktuře:   * + - 1. Enterprise SubCA pro UAS user (e-mail, timestamp, code-sign)       2. Enterprise SubCA pro UAS device (web, LDAP, server)       3. Enterprise SubCA pro UAS network (802.1x a další)       4. Privátní klíče uvedených CA budou uloženy v budoucím dodavatelem dodaných síťových prvcích hardwarové podpory kryptografie a bezpečného uložení klíčů, dostupných online[[4]](#footnote-5) |
| K.5 | podřízené CA pro „technologickou zónu“ | Zadavatel předpokládá návrh architektury a technického řešení pro „technologickou zónu“ v následující struktuře:   * + - 1. Enterprise SubCA pro TechDS user (e-mail, timestamp, code-sign)       2. Enterprise SubCA pro TechDS device (web, ldap, server)       3. Enterprise SubCA pro TechDS network (802.1x a další)       4. Enterprise SubCA pro TechDS KMC (key management centre pro TechDS)       5. Privátní klíče uvedených CA budou uloženy v bezpečném síťovém HW kryptografickém prostředku dostupném online[[5]](#footnote-6) |
| K.6 | vydávající certifikační autority „legacy zóna“ | Zadavatel předpokládá návrh architektury a technického řešení pro „legacy zónu“, pokud tento požadavek vyplyne z analýzy současného stavu prostředí zadavatele a jeho požadavků na budoucí stav CA a PKI.  Požadavky na uložení privátních klíčů všech CA pro legacy zóny (kořenové CA i podřízených CA) odpovídají požadavkům ostatních CA (kořenové CA a podřízených CA business a technologické zóny). |
| K.7 | HW podpora kryptografie a bezpečného uložení klíčů | Pro HW podporu kryptografie a bezpečného uložení klíčů je požadováno využití   * přímo napojeného HSM pro kořenovou CA * síťových HSM pro podřízené CA   (viz též T.2 / T.3) |
| K.8 | vysoká dostupnost systému interních CA | * + - 1. Produkční prostředí interních CA musí být instalováno v režimu HA. Musí být zajištěno, aby při výpadku jedné části systému nebyla dotčena funkčnost celého řešení.       2. Každá z komponent interních CA, která je nezbytná pro provoz CA/PKI, musí obsahovat minimálně dvě samostatné instance provozované v HA režimu s maximální dobou výpadku dostupnosti v řádu nízkých desítek sekund[[6]](#footnote-7).       3. Řešení vysoké dostupnosti musí být automatické. Řešení, která vyžadují jakoukoliv manuální intervenci pro zajištění dostupnosti služeb CA/PKI v případě vzniku chybového stavu, nejsou přípustná.       4. Dodavatel navrhne metodiku testů měření dostupnosti jako součást návrhu funkčních, výkonnostních a bezpečnostních testů řešení. |
| K.9 | HW a SW prostředí | Dodavatel zpracuje v rámci návrhu architektury řešení:   * + - 1. Detailní popis potřebného HW a SW včetně rozpisu všech modulů, aktiv, virtuálních instancí do úrovně virtuálních kontejnerů (pokud budou použity);       2. Všechny hardwarové komponenty (HSM, servery, počítače) a software používaný v systému. Popis obecné konfigurace hardwaru a vysvětlení, jak se funkce definované ve funkční specifikaci mapují na hardware;       3. Popis všech částí komponent a uvede podrobnější informace o hardwarovém a softwarovém prostředí:          * primární konfigurace hardwaru          * seznam dalších hardwarových konfigurací (např. záložní systémy)          * vztah mezi hardwarem a externími rozhraními          * seznam veškerého SW potřebného k implementaci obsahující minimálně: přesnou specifikaci SW, verzi, platformu a přiřazení ke konkrétnímu HW          * Detailní přehled všech licencí |
| K.10 | škálovatelnost řešení | Dodavatel uvede, jakým způsobem bude realizována škálovatelnost celé soustavy CA řešení, včetně příkladů. |

#### Obslužné procesy

Zpracování návrhu obslužných procesů souvisejících se soustavou interních CA.

Po dodavateli je požadováno zpracování návrhu obslužných procesů instalace a konfigurace všech komponent soustavy interních CA a PKI, podpory životního cyklu vydávaných certifikátů, správy SW a HW komponent včetně správy prvků vysoké dostupnosti, procesů zálohování a obnovy apod.

V rámci implementace nového PKI zadavatel požaduje návrh procesů minimálně pro: instalaci a konfiguraci jednotlivých CA, HW kryptografických prostředků pro ochranu privátních klíčů, zprovoznění PKI systému, instalaci a konfiguraci SW komponent pro správu a řízení životního cyklu certifikátů.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| K.11 | návrh obslužných procesů | Požadován je návrh obslužných procesů soustavy CA, zejména procesů   * + - 1. instalace a konfigurace všech komponent soustavy certifikačních autorit;       2. provozní obsluhy offline CA;       3. správy certifikačních autorit (včetně definice rolí a oprávnění pro správu);       4. aktualizace systémů;       5. vydávání certifikátů (včetně návrhu segregace rolí), přidělení rolí jednotlivým uživatelům;       6. správy životního cyklu certifikátů (viz také K.14);       7. využívání uživatelských certifikátů (popř. certifikátů služeb) k podepisování interních operací a dokumentů;       8. správy prvků vysoké dostupnosti / redundance;       9. zálohování a obnovy;       10. business kontinuity;       11. vyšetřování a řešení provozních a bezpečnostních incidentů včetně způsobů zaručeného zajištění stop.   Zadavatel požaduje popis rozhraní online služeb správy životního cyklu certifikátů a rozhraní k vybudování online služeb podepisování a ověřování elektronických popisů, včetně odkazu na dokumentace příslušných API[[7]](#footnote-8).  Dále zadavatel požaduje návrh rozhraní/procesu pro získávání logů[[8]](#footnote-9) z navrhovaného řešení včetně procesu ukládání logů z offline kořenové CA.  Součástí návrhu musí být také odhad požadavku na kapacity zadavatele pro řádné a pravidelné vykonávání navržených procesů. |
| K.12 | požadavky na správu životního cyklu certifikátů | Návrh pro procesy/systém správy životního cyklu certifikátů musí splňovat minimálně tyto požadavky na funkcionalitu:   * + - 1. vydání certifikátu v zastoupení, který umožní privilegovanému správci certifikátů požádat o certifikát v zastoupení jiného uživatele, který nemá znalosti nebo oprávnění k vytvoření vlastní žádosti o certifikát       2. ukládání informací o certifikátech z nového PKI v relační databázi v reálném čase       3. vkládání žádosti o certifikát, validaci, zaslání žádosti do CA a stažení vydaného certifikátu       4. automatizovaná notifikace o expiraci vydaných certifikátů z CA       5. automatizované odvolávání certifikátů (neprivilegovaný uživatel může zneplatňovat certifikáty pouze na základě integrované autentizace)       6. vyhledávání informací o certifikátech, odvolávání certifikátů bez nutnosti oprávnění uživatele proti CA, generování reportů a statistik       7. online dostupnost informací o stavu certifikátů včetně informací o případném zneplatnění certifikátu (systém tedy musí umožňovat poskytnutí dat o platných/odvolaných certifikátech v čase blízkém reálnému bez časové prodlevy spojené s umístěním odvolaného certifikátu na CLR list a publikací nového CLR listu) |

#### Použití šifrovacích/hashovacích algoritmů

Zpracování návrhu použití šifrovacích/hashovacích algoritmů, typů a délky klíčů pro všechny uvažované kategorie infrastruktury, služeb a uživatelů.

Dodavatel zpracuje návrh pro využití šifrovacích/hashovacích algoritmů a souvisejících typů a délky klíčů pro využití ve všech kategoriích a službách PKI a v souvislosti s uvažovanými souvisejícími projekty.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| K.13 | návrh použití šifrovacích/hashovacích algoritmů, typů a délky klíčů | Požadován je návrh pro použití šifrovacích a hashovacích algoritmů, generování klíčů a jiného kryptografického materiálu apod. a s tím souvisejících typů a délky klíčů pro využití ve všech kategoriích a službách PKI[[9]](#footnote-10). Dodavatel návrh zpracuje zejména   * + - 1. s přihlédnutím k best practice;       2. v souladu s doporučením NÚKIB[[10]](#footnote-11): „Doporučení v oblasti kryptografických prostředků verze 2.0“;       3. s ohledem na zajištěním kompatibility[[11]](#footnote-12) a technologických předpokladů pro budoucí využití uživatelských certifikátů k identifikaci a vícefaktorové autentizaci uživatele (MFA), zejména s využitím SmartCard[[12]](#footnote-13). |

#### Zásady a politiky pro jednotlivé CA

Zpracování zásad a politik pro jednotlivé certifikační autority

Dodavatel zpracuje pro všechny navržené CA (budoucí stav) zásady jejich konfigurace a využití a související politiky.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| K.14 | zásady a politiky pro jednotlivé certifikační autority | Dodavatel zpracuje pro všechny navržené CA (budoucí stav) zásady jejich konfigurace a využití a související politiky. |

#### Specifikace struktury šablon pro jednotlivé CA

Zpracování specifikace struktury šablon pro jednotlivé certifikační autority

Dodavatel zpracuje pro všechny navržené CA (budoucí stav) strukturu šablon, popř. i vlastní šablony.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| K.15 | struktura šablon pro jednotlivé certifikační autority | Dodavatel zpracuje pro všechny navržené CA (budoucí stav) strukturu šablon a v případě využití i jiných než standardních vestavěných (built-in) šablon zpracuje dodavatel i návrh těchto šablon.  Dodavatel zpracuje tento požadavek formou dokumentů pro jednotlivé CA s definicí jednotlivých šablon a oprávnění vůči nim. |

#### Instalační a konfigurační dokumentace

Zpracování kompletní instalační a konfigurační dokumentace

Dodavatel zpracuje kompletní a podrobnou dokumentaci všech instalacích a konfiguračních procesů, včetně konkrétního nastavení SW a HW komponent pro prostředí zadavatele.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| K.23 | kompletní instalační a konfigurační dokumentace | Zpracování kompletní a podrobné dokumentace všech instalačních a konfiguračních procesů, včetně konkrétního nastavení SW a HW komponent pro prostředí zadavatele (až do úrovně snímků obrazovek jednotlivých komponent). Instalační a konfigurační dokumentace musí být natolik podrobná, aby na základě dokumentace pracovníci zadavatele byli schopni instalační a konfigurační práce provést.  Součástí dokumentace musí být i podrobný popis procesů týkajících se koncových uživatelů (zejména procesů a návodů využívání uživatelských certifikátů k podepisování interních operací a dokumentů).  Jako součást dokumentace požaduje zadavatel také zpracování odhadu pracnosti implementace a konfigurace (např. v MD), které bude muset zadavatel vynaložit k dokončení implementace podle návrhu.  Části dokumentace popisující prostředí systémů (dokumentace výrobce a snímky obrazovek) mohou být v anglickém jazyce.  Dokumenty pro koncové uživatele (návody, popis procesů) musí být v českém jazyce. |
| K.24 | minimální požadovaná struktura dokumentace | Zadavatel požaduje zpracování dokumentace odpovídající požadavkům ISMS a ITSM. Požadavky na dokumentaci jsou uvedeny v interním předpisu č.j. 56805/2018-SŽDC-GŘ-O30 (viz příloha Závazného vzoru smlouvy č. 8). |

#### Analýza rizik cílového řešení

Zpracování analýzy rizik informační a kybernetické bezpečnosti cílového řešení, včetně návrhu opatření k řízení rizik.

Dodavatel zpracuje analýzu rizik informační a kybernetické bezpečnosti cílového řešení. Zpracuje model bezpečnosti provozu soustavy CA včetně vzájemných vztahů/souvislostí a vazeb na analýzu rizik. K identifikovaným rizikům navrhne opatření k jejich řízení.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| K.25 | analýza rizik projektu a provozu nové PKI | Zpracování analýzy rizik informační a kybernetické bezpečnosti cílového řešení v souladu s požadavky Vyhlášky 82/2018, o kybernetické bezpečnosti. Kromě standardních rizik požaduje do analýzy zadavatel zahrnout také:   * + - 1. vliv „legacy zóny“ na kořenovou CA       2. rizika využití virtualizace pro provoz jednotlivých podřízených CA       3. rizika návrhu kořenové CA a souvisejících technologií       4. rizika topologie síťového prostředí soustavy interních CA       5. rizika využití technologií označených příslušnými autoritami[[13]](#footnote-14) za nedůvěryhodné nebo k nim tyto autority vydaly varování (např. technologie HUAWEI, ZTE, technologie s původem v Ruské federaci apod.)       6. soulad s doporučením NÚKIB pro oblast kryptografických prostředků |
| K.26 | návrh opatření k řízení rizik | Na základě výstupů předchozího kroku navrhne dodavatel model bezpečnosti provozu soustavy CA včetně vzájemných vztahů/souvislostí a vazeb na analýzu rizik a návrh opatření k řízení rizik.  Součástí opatření musí být i návrh scénáře bezpečnostního dohledu nové PKI. |

#### Návrh testů implementovaného řešení

Zpracování návrhu funkčních, výkonových a bezpečnostních testů implementovaného řešení.

Dodavatel navrhne metodiku funkčních, výkonnostních a bezpečnostních testů implementovaného řešení, včetně návrhu testů obnovy a zotavení pro vybrané typy událostí/závad.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| K.27 | návrh funkčních, výkonových a bezpečnostních testů | Dodavatel navrhne metodiku a plán provedení funkčních, výkonových a bezpečnostních testů implementovaného řešení, včetně návrhu testů obnovy a zotavení pro vybrané typy událostí/závad, včetně výkonnostních parametrů obnovy a zotavení (RPO, RTO apod.).  Testy ověří, že implementované řešení nové PKI poskytuje bezchybně všechny požadované funkcionality, včetně integrace s AD zadavatele.  Součástí návrhu budou i testovací scénáře provozního monitoringu[[14]](#footnote-15).  Součástí návrhu testů bude také odhad pracnosti testů (např. v MD) a požadavky na součinnost zadavatele v průběhu testů. |

### Plán přechodu

#### Technologické, organizační a procesní předpoklady

Definování technologických, organizačních a procesních předpokladů úspěšné implementace nového PKI.

Dodavatel zpracuje detailní přehled předpokladů (prerekvizit) pro úspěšnou implementaci nové soustavy CA/PKI.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| K.16 | Definice předpokladů implementace nové PKI | Dodavatel zpracuje detailní přehled prerekvizit pro úspěšnou implementaci nové soustavy CA/PKI minimálně pro oblasti:   * + - 1. technologická oblast       2. organizační oblast       3. procesní oblast |

#### Proces přechodu

Návrh procesu přechodu ze současného stavu na provoz nové PKI

Dodavatel zpracuje detailní návrh přechodu ze stávajícího systému certifikačních autorit na nově vybudovanou PKI, včetně návrhu integrace s AD.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| K.17 | návrh přechodu na nové PKI | Dodavatel zpracuje detailní návrh procesu přechodu ze současné soustavy CA na nově vybudovanou soustavu CA a PKI včetně detailního časového plánu.  Součásti návrhu bude i provedení decommissioningu původního PKI řešení po dokončení přechodu na nové řešení PKI.  Dodavatel současně uvede popis veškerých požadavků na součinnost na straně útvarů a rolí na straně zadavatele, včetně časové posloupnosti požadavků. |
| K.18 | návrh integrace s AD | Detailní návrh integrace se současnou strukturou AD zadavatele. |

#### Technologický GAP

Revize připravenosti ICT prostředí zadavatele k implementaci v oblasti technologií a kapacit (technologického gapu), návrh opatření k odstranění gapu.

Dodavatel na základě AS-IS analýzy a TO-BE návrhu identifikuje chybějící technologie, popř. kapacity stávajících technologií pro doplnění do stavu vyhovujícího požadovaným prerekvizitám včetně odpovídajícího kapacitního plánování (sizing). Součástí identifikace budou i požadavky na technické prostředky zadavatele nutné pro implementaci soustavy nových interních CA.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| K.19 | revize připravenosti prostředí zadavatele k implementaci (technologický gap) | Dodavatel na základě AS-IS analýzy a TO-BE návrhu upřesní/potvrdí finální konfigurace jím dodávaných technologií (HSM a související klientském, popř. SW licence), identifikuje chybějící technologie, popř. kapacity stávajících technologií pro doplnění do stavu vyhovujícího požadovaným prerekvizitám včetně odpovídajícího kapacitního plánování (sizing), zejména pro oblasti   * + - 1. dedikovaný HW pro provoz kořenové CA       2. požadavků na technické prostředí zadavatele (virtualizace, výpočetní prostředky, diskové kapacity, licence Microsoft, změny síťového prostředí apod.) |
| K.20 | návrh technologií k odstranění gapu | Na základě předchozího kroku navrhne dodavatel seznam technologií (HW, SW) k odstranění technologického gapu.  Návrh zpracuje minimálně pro vybudování kořenové CA a „business zónu“. Návrh zpracuje s ohledem na budoucí potřeby zadavatele (škálování řešení) a požadavky v oblasti bezpečnosti řešení. |

#### Organizační a procesní GAP

Identifikace organizačního a procesního gapu

Dodavatel na základě AS-IS analýzy a TO-BE návrhu identifikuje procesní a organizační nedostatky, které bude nezbytné pro implementaci soustavy nových interních CA změnit nebo doplnit. Navrhne také změny procesů a organizačního zajištění implementace a provozu nové PKI.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| K.21 | identifikace organizačního a procesního gapu | Dodavatel provede analýzu organizační a procesní připravenosti prostředí zadavatele pro implementaci a provoz nového PKI, zejména   * + - 1. ve vztahu ke správě CA       2. ve vztahu k užívání certifikátů pro interní účely       3. ve vztahu k externím subjektům (např. pro řízení s2s VPN, …) |
| K.22 | návrh organizačních a procesních opatření | Na základě předchozího kroku navrhne dodavatel příslušná organizační a procesní opatření k odstranění identifikovaného gapu |

## Dodávka technologií, licencí a školení

Dodavatel na základě své nabídky zajistí dodávku požadovaných technologií pro implementaci a bezpečný provoz kořenové CA a „business zóny“ nového PKI a zajistí školení pracovníků zadavatele v oblasti administrace a provozu dodaných technologií.

### Prvek pro HW podporu kryptografie a bezpečné uložení klíčů pro kořenovou CA

Dodávka prvku pro hardwarovou podporu kryptografie a bezpečné uložení klíčů pro kořenovou CA.

Dodavatel dodá prostředky pro bezpečný provoz kořenové certifikační autority.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| T.1 | dodávka technických prostředků pro kořenovou autoritu | Pro bezpečný provoz kořenové CA dodá dodavatel přímo připojitelný HSM (HW pro podporu kryptografických operací a bezpečného uložení klíčů), splňující minimálně následující požadavky:   * + - 1. podpora kryptografických algoritmů, délky klíčů a protokolů v souladu s doporučením NÚKIB       2. certifikace FIPS 140-2 Level 3       3. nesmí obsahovat technologie označené NÚKIB jako nedůvěryhodné nebo k nim NÚKIB vydal varování       4. součástí dodávky musí být i SW licence (pokud budou třeba) spjaté s HSM a nezbytné k provozu HSM v rámci kořenové CA   Pro vybudování a provoz kořenové CA navrhne dodavatel specifikaci hostitelského systému (HW typu notebook/PC, hostitelský systém, virtualizační platformu atd.) kompatibilní s dodaným HSM.  Dodávku hostitelského systému podle specifikací dodavatele zajistí zadavatel. |

### Síťové HSM

Dodávka 3ks prvků pro hardwarovou podporu kryptografie a bezpečné uložení klíčů pro podřízené CA „business zóny“ (síťové HSM)

Dodavatel zajistí dodávku prostředků pro hardwarovou podporu kryptografie a bezpečné uložení klíčů[[15]](#footnote-16).

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| T.2 | dodávka prvků pro hardwarovou podporu kryptografie a bezpečné uložení klíčů | Dodavatel zajistí prvky pro hardwarovou podporu kryptografie a bezpečné uložení klíčů:   * + - 1. zadavatel požaduje dodávku 3 ks síťových HSM splňujícími minimálně parametry definované v T.3 a konfigurovaných pro zajištění vysoké dostupnosti služeb HSM a pokrytí potřeb vybudování „business zóny“       2. virtuální stroje pro vybudování a provoz podřízených CA zajistí zadavatel podle specifikací dodavatele       3. síťové prostředí pro provoz podřízených CA zajistí zadavatel podle specifikace dodavatele   V rámci dodávky požadovaných síťových HSM dodavatel zajistí v souladu s návrhem budoucího stavu (TO-BE) a prostředím zadavatele:   * konfiguraci síťových rozhraní HSM v souladu s požadavky prostředí zadavatele * instalaci dodaných HW prvků v prostředí datových center zadavatele * připojení dodaných HW prvků do prostředí zadavatele * základní testování funkčnosti dodaných HW prvků |
| T.3 | požadavky na prvky pro hardwarovou podporu kryptografie a bezpečné uložení klíčů | Síťové prvky pro hardwarovou podporu kryptografie a bezpečné uložení klíčů (HSM) musí splňovat minimálně tyto parametry:   * + - 1. dostatečná škálovatelnost, jak z hlediska výkonu, tak kapacity, pro pokrytí budoucích potřeb zadavatele vyplývajících z návrhu řešení nové PKI (TO-BE), zadavatel požaduje řešení rozšiřitelné z uvedených hledisek: kapacita, výkon, virtuální kontext[[16]](#footnote-17)       2. podpora kryptografických algoritmů, délky klíčů a protokolů v souladu s doporučením NÚKIB       3. podpora přístupu klientských systémů: rozšiřitelná minimálně na 150 v rámci jednoho sítového HSM       4. možnost zajištění vysoké dostupnosti, podpora Load Balancing       5. podpora bezpečných virtuálních kontextů/partitions HSM (požadováno minimálně 8 s možností budoucího rozšíření na minimálně 20)       6. certifikace FIPS 140-2 Level 3       7. certifikace Common Criteria EAL4+       8. soulad s požadavky GDPR, PCI-DSS, HIPAA, eIDAS       9. podpora OS: Windows, Linux       10. podpora virtualizačních platforem minimálně VMware a Hyper-V       11. výkon: asymetrická kryptografie:           * ECC-256: min. 4000 tps           * RSA-4096: min. 600 tps           * RSA-2048: min. 3000 tps       12. nesmí obsahovat technologie označené NÚKIB jako nedůvěryhodné nebo k nim NÚKIB vydal varování |

### Záruka a záruční servis

Zajištění záruky za jakost a záruční servis: Dodavatel zajistí pokrytí záruk všech dodaných technologií v délce 5 let.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| T.5 | záruka a servis dodaných technologií | Dodavatel zajistí záruku za jakost a záruční servis všech dodaných technologií:   * + - 1. v délce minimálně 5 let       2. v souladu s ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT – Příloha č. 6 Závazného vzoru smlouvy. |

### Licence

Dodávka licencí souvisejících s dodávanými technologiemi nezbytných k využití HSM.

Dodavatel zajistí všechny potřebné licence a subskripce nezbytné k využití dodávaných technologií pro budování a provoz nové kořenové CA a soustavy podřízených CA pro „business zónu“.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| T.6 | zajištění licencí | Dodavatel zajistí potřebné licence v rámci dodávaných technologií:   * + - 1. nezbytné SW licence       2. nezbytné výkonnostní nebo kapacitní licence (podle licenčních modelů dodávaných technologií)       3. nezbytné subskripce a/nebo službu licenční a technologické údržby (maintenance) na dobu min. 5 let (pokud budou třeba, podle licenčních modelů dodaných technologií) |

### Školení

Dodavatel zajistí školení pověřených pracovníků zadavatele v oblasti administrace a provozu dodaných technologií.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| T.7 | zajištění školení | K dodaným technologiím, zejména prvkům pro hardwarovou podporu kryptografie a bezpečné uložení klíčů, zajistí dodavatel školení pověřených pracovníků v oblasti administrace a provozu dodaných technologií. |

## Supervize implementačních prací a navržených testů, včetně řešení nestandardních stavů

Dodavatel zajistí supervizi při implementaci navrženého řešení nové soustavy CA sestávající se z kořenové CA a soustavy podřízených CA „business zóny“ nového PKI, supervizi funkčních, výkonnostních a bezpečnostních testů implementovaného řešení, řešení nestandardních stavů a technickou podporu při implementaci řešení.

Supervize a technická podpora bude poskytována po dobu implementace řešení zadavatelem podle Dodavatelem zpracované dokumentace, včetně doby provádění navržených testů, maximálně však po dobu stanovenou v Harmonogramu (Harmonogram je přílohou Smlouvy o dílo).

### Supervize a technická podpora zadavatele při implementaci řešení.

Dodavatel zajistí supervizi implementačních činností, konfigurace technologií a technickou podporu při implementaci, včetně řešení nestandardních stavů.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| S.1 | supervize a technická podpora zadavatele při implementaci řešení | Dodavatel poskytne zadavateli službu supervize a technické podpory, včetně řešení nestandardních stavů při:   * + - 1. instalaci komponent nové PKI       2. integraci se stávajícím prostředí       3. úpravách stávajícího prostředí pro potřeby nové PKI       4. implementaci procesů správy PKI a procesů vydávání a správy životního cyklu certifikátů |

### Supervize a technická podpora při testování

Supervize a podpora zadavatele při provedení funkčních, výkonových a bezpečnostních testů implementovaného řešení.

Dodavatel zajistí supervizi a technickou podporu zadavatele implementace při realizaci funkčních, výkonových a bezpečnostních testů, včetně řešení nestandardních stavů.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| S.2 | supervize a technická podpora zadavatele provedení funkčních testů řešení | Dodavatel poskytne zadavateli službu supervize a technické podpory při provedení funkčních, výkonových a bezpečnostních testů řešení, včetně řešení nestandardních stavů. |
| S.3 | provedení testů obnovy a zotavení | Dodavatel provede navržené testy obnovy a zotavení pro vybrané typy událostí/závad jako součást akceptace Fáze 3. |

## Post-implementační a technická podpora

### Post-implementační podpora

Dodavatel zajistí post-implementační podporu implementovaného řešení po dobu 6 měsíců.

Detailní požadavky obsahuje následující tabulka:

|  |  |  |
| --- | --- | --- |
| ID | Oblast | Popis |
| P.1 | součinnost při penetračních testech a auditu řešení | Dodavatel poskytne zadavateli v období do 6 měsíců od akceptace řešení:   * + - 1. nezbytnou součinnost při provedení penetračních testů a auditu řešení nové PKI       2. zpracuje návrh opatření k odstranění zjištěných nedostatků a neshod       3. supervizi implementace navržených opatření |
| P.2 | post-implementační podpora | Dodavatel poskytne zadavateli službu post-implementační podpory v délce 6 měsíců od dokončení implementace řešení a provedení funkčních, výkonnostních a bezpečnostních testů implementovaného řešení:  Službu post-implementační podpory poskytne dodavatel pro oblasti   * + - 1. instalovaných komponent a jejich konfigurací       2. integrace s prostředím zadavatele       3. procesů správy PKI a procesů vydávání a správy životního cyklu certifikátů       4. řešení nestandardních stavů   Post-implementační podpora bude poskytována v souladu ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 6 Závazného vzoru smlouvy) podle servisního modelu C2. |

### Odborná technické podpora

Dodavatel zajistí technickou podporu pro dodané technologie pro období 5 let.

Detailní požadavky obsahuje následující tabulka:

| ID | Oblast | Popis |
| --- | --- | --- |
| P.3 | zajištění technické podpory dodaných technologií | Dodavatel zajistí technickou podporu dodaných technologií:   * + - 1. poskytování expertních služeb, které budou využívány zejména pro podporu činností zadavatele v případě řešení nestandardních stavů       2. technická podpora bude poskytována po dobu 5 let od akceptace dodávky technologií       3. odborná technická podpora bude poskytována v souladu ustanoveními Zvláštních obchodních podmínek pro Zakázky v oblasti ICT (Příloha č. 6 Závazného vzoru smlouvy) podle servisního modelu A3       4. Měření SLA bude realizováno na straně zadavatele prostřednictvím jeho servisdeskového systému |

## Služby na vyžádání

Dodavatel poskytne zadavateli služby konzultace na vyžádání. Maximální souhrn těchto služeb bude činit 40 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb zadavatele.

Zadavatel požaduje uvést cenu za následující položky ve formě ceny za 1MD a celkové ceny za položku podle předpokládaného objemu čerpání:

|  |  |
| --- | --- |
| Položka | Předpokládané čerpání v MD |
| Služba konzultační technické podpory dodaného řešení (technické a metodické otázky související s provozem a rozvojem dodaného řešení) | 25 |
| Změnová řízení, dovývoj, doplnění řešení | 15 |

Celková cena za výše uvedené položky musí být součástí cenové nabídky Budoucího Dodavatele.

Zadavatel není povinen nadstandardní služby čerpat.

# Fáze dodávky a akceptační milníky

Dodávka má být dodána v níže uvedených následujících fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být Zadavatelem separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané Fáze, jestliže je Dodavatel provedl v šíři a kvalitě požadované ve výzvě k podání nabídek této veřejné zakázky. V opačném případě je Dodavatel povinen napravit nedostatky dodávky.

| **Fáze** | **Popis** | **Kapitola obsahující požadavky** |
| --- | --- | --- |
| F1.a | Analýza současného stavu | 5.1.1 |
| F1.b | Návrh budoucího stavu a plán přechodu pro oblasti:   * kořenová CA * business zóna | 5.1.2 a 5.1.3, pro části týkající se kořenové CA a business zóny |
| F1.c | Návrh budoucího stavu a plán přechodu pro oblasti:   * technologická zóna * legacy zóna | 5.1.2 a 5.1.3, pro části týkající se technologické a legacy zóny |
| F2 | Dodávka technologií, licencí a školení | 5.2 |
| F3 | Supervize implementačních prací a navržených testů | 5.3 |
| F4.a | Post-implementační podpora | 5.4.1 |
| F4.b | Technická podpora dodaných technologií | 5.4.2 |
| F5 | Služby na vyžádání | 5.5 |

1. Uvedené HSM je požadovanou součástí dodávky technologií [↑](#footnote-ref-2)
2. Pro „business zónu“ budou využita síťová HSM, která jsou součástí požadované dodávky technologií [↑](#footnote-ref-3)
3. Viz Dodávka technologií a licencí – HSM přímo napojitelný na hostitelský systém [↑](#footnote-ref-4)
4. Viz Dodávka technologií a licencí – síťové HSM [↑](#footnote-ref-5)
5. Zadavatel připouští využití dodaných síťových HSM (požadovaná součást dodávky technologií), popř. využití požadované škálovatelnosti dodaných technologií. [↑](#footnote-ref-6)
6. Dodavatel navrhne řešení jako vysoce dostupné z hlediska využitých a dodaných technologií CA a HSM. Dále popíše vazby na ICT prostředí zadavatele, kde jím navržená vysoká dostupnost spoléhá na funkčnost dalších aktiv zadavatele (HW, VM, sítě apod.), které nemůže dodavatel ovlivnit. [↑](#footnote-ref-7)
7. Případně odkazů na dokumentaci příslušných API. [↑](#footnote-ref-8)
8. V systémech kybernetické bezpečnosti typu SIEM nebo LogManager alespoň v rozsahu odpovídajícím požadavkům ZoKB a VoKB. [↑](#footnote-ref-9)
9. Zadavatel předpokládá definování úzké součinnosti dodavatele se zadavatelem v oblasti identifikace provozovaných systému konzumujících certifikáty z budovaného PKI řešení a zohlednění kompatibility systému s novým PKI. [↑](#footnote-ref-10)
10. https://nukib.cz/cs/infoservis/doporuceni/1843-doporuceni-v-oblasti-kryptografickych-prostredku-verze-2-0/ [↑](#footnote-ref-11)
11. Zadavatel plánuje využití vytvořené PKI v souvisejících projektech, zejména „Nasazení vícefaktorové autentizace s pořízení nosičů certifikátů“ a „PAM“ [↑](#footnote-ref-12)
12. Včetně možné varianty budoucího využití kvalifikovaného prostředku dle eIDAS (SmartCard) pro možné ukládání interních certifikátů a jejich případném využití využití pro vícefaktorovou autentizaci. [↑](#footnote-ref-13)
13. Zejména NÚKIB. Současně zadavatel doporučuje vzít v úvahu i doporučení dalších autorit, např. Bundesamt für Sicherheit in der Informationstechnikn (BSI). [↑](#footnote-ref-14)
14. Např. testovací scénář založený na transakce prováděných ze ZABBIX systému zadavatele vůči CA a dodaným HSM. Obdoba tohoto scénáře může být využita i pro testování parametrů vysoké dostupnosti služeb dodaného řešení (zejména HSM). [↑](#footnote-ref-15)
15. Zadavatel požaduje využití přímo napojeného HSM pro offline kořenovou CA a využití síťových HSM pro všechny podřízené CA [↑](#footnote-ref-16)
16. Zadavatel připouští škálovatelnost řešení formou rozšiřování kapacity úložišť, instalací dalších zařízení pro zvýšení výkonu, dokoupení llicencí apod. [↑](#footnote-ref-17)