



Příloha č. 3: Technická specifikace

V této příloze jsou uvedeny výchozí podmínky a požadavky na dodávku v rámci této veřejné zakázky.

OBSAH

Obsah	1
Využití zdroje.....	2
Seznam tabulek	2
Seznam zkratk a pojmů	2
1 Předmět plnění	5
2 Rozsah dodávky a souvisejících služeb	5
2.1 Vymezení předmětu a rozsahu dodávky	5
2.1.1 Související služby a náležitosti dodávky	5
2.1.2 Dodávkou nedotčené oblasti stávajícího řešení.....	6
2.1.3 Vyloučení z dodávky.....	6
2.2 Požadavky na dodávky.....	6
2.2.1 Obecné a společné požadavky	6
2.2.2 Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet 7	
2.2.3 Vybudování PKI infrastruktury ZZS KHK	9
2.2.4 Čipové karty.....	10
2.2.5 Tiskárna na potisk čipových karet	11
2.2.6 Bezpečnostní požadavky	12
2.2.7 Implementační a provozní požadavky.....	12
2.3 Požadavky na služby	13
2.3.1 Realizace předmětu plnění.....	13
2.3.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií	15
2.4 Záruky	15
3 Harmonogram.....	16
4 Místa plnění	17
5 Výchozí stav	18
5.1 Stav informačních a komunikačních technologií	18
5.1.1 Datové centrum, HW infrastruktura, systémový SW a technologie	18



5.1.2	Datové sítě	20
5.1.3	Síťová infrastruktura	20
Konec dokumentu		20

VYUŽITÉ ZDROJE

Nejsou

SEZNAM TABULEK

Tabulka 1: Seznam zkratk a pojmů	4
Tabulka 2: Předmět a rozsah dodávky	5
Tabulka 3: Obecné požadavky	7
Tabulka 4: Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet...	9
Tabulka 5: Vybudování PKI infrastruktury ZZS KHK	9
Tabulka 6: Čipové karty	11
Tabulka 7: Tiskárna na potisk čipových karet	11
Tabulka 8: Bezpečnostní požadavky	12
Tabulka 9: Provozní požadavky	13
Tabulka 10: Dokumentace – požadavky na zpracování	14
Tabulka 11: Harmonogram	16
Tabulka 12: Místa plnění	17
Tabulka 13: Datové centrum, HW infrastruktura, systémový SW	19
Tabulka 14: Datové sítě	20
Tabulka 15: Síťová infrastruktura	20

SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
AD	Active Directory - řízení přístupů do informačních systémů
AES	Advanced Encryption Standard (standard pokročilého šifrování) je standardizovaný algoritmus používaný k šifrování dat v informatice
CD / CD-ROM / DVD / USB	Datový nosič
CA	Certifikační autorita



Zkratka/pojem	Význam
ČR	Česká republika
DB	Databáze
DC	Datové centrum
eIDAS	Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu
EU	Evropská unie
FW	Firewall
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob
HW	Hardware
HZS	Hasičský záchranný sbor
ICT	Informační a komunikační technologie
IP	Internet Protocol
IROP	Integrovaný regionální operační program
IS	Informační systém
IT	Informační technologie
IZS	Integrovaný záchranný systém
KII	Kritická informační infrastruktura
KHK	Královéhradecký kraj
ks	Počet kusů
LAN	Lokální počítačová síť
MS	Microsoft
OS	Operační systém
PNK	Prováděcí nařízení Komise (EU)
QSCD	Qualified Signature Creation Device (kvalifikovaný prostředek pro vytváření elektronických podpisů)
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SNMP	Simple Network Monitoring Protocol
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích
SW	Software
TS	Technická specifikace



**Spolufinancováno
Evropskou unií**



**MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR**

Zkratka/pojem	Význam
UPS	Uninterruptible Power Supply/Source (zdroj nepřerušovaného napájení)
VPN	Virtuální privátní síť
VŘ	Výběrové řízení
WAN	Rozsáhlá počítačová síť
ZOS	Zdravotnické operační středisko
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS KHK	Zdravotnická záchranná služba Královéhradeckého kraje

Tabulka 1: Seznam zkratek a pojmů



1 PŘEDMĚT PLNĚNÍ

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace technologií, dodávky SW, HW a infrastruktury pro autentizaci uživatelů pomocí čipové karty.

Součástí dodávky budou aplikace a opatření potřebná k zajištění autentizace všech uživatelů pomocí dvou faktorů, přičemž druhým bude hybridní čipová karta, kterou bude možno využít i k dalším účelům, zejména jako bezkontaktní čip pro přístupový systém (Mifare DesFire), průkaz zaměstnance s potiskem po obou stranách a úložiště kvalifikovaných certifikátů pro podepisování zdravotnické dokumentace.

Předmět plnění (dílo) je detailně popsán v kap. 2 – Rozsah dodávky a souvisejících služeb.

2 ROZSAH DODÁVKY A SOUVISEJÍCÍCH SLUŽEB

2.1 VYMEZENÍ PŘEDMĚTU A ROZSAHU DODÁVKY

Rozsah dodávky je následující:

#	Položka rozpočtu	Počet	Stručný popis položky
1	Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet	1 soubor	Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet. Součástí je vybudování systému, dodávka systému, instalace, zapojení a konfigurace prvků přístupového systému a zajištění všech nezbytných integrací (přístupový systém, napojení na RADIUS server, MS AD atd.).
2	Vybudování PKI infrastruktury ZZS KHK	1 soubor	Dodávka technologií pro bezpečnostní vrstvu vybudovanou na bázi PKI MS Windows, která je primárně určena pro vydávání klientských karetních a infrastrukturních certifikátů pro zavedení 2FA autentizace.
3	Čipové karty	500 ks	Hybridní čipové karty ve velikosti ID-1 (bankovní karta) s bezkontaktním čipem (Mifare DesFire) pro přístupový systém a funkcí bezpečného zařízení (kvalifikovaný prostředek QSCD) pro ukládání kvalifikovaných i komerčních certifikátů a vytváření elektronického podpisu (QESCD) v souladu s legislativou.
4	Tiskárna na potisk čipových karet	1 ks	Tiskárna na oboustranný potisk dodávaných čipových karet.

Tabulka 2: Předmět a rozsah dodávky

2.1.1 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení.
2. Zpracování návrhu dodávky a konfigurace dodávaných technologií, související konzultace.
3. Dodávka, implementace, instalace, zapojení a konfigurace dodávaných technologií.
4. Ověření funkčnosti dodaných technologií a jejich (sou)částí.



5. Dodávka dokumentace dodaného vybavení a jeho částí (min. administrátorská dokumentace, dokumentace skutečného provedení/stavu po implementaci, systémová dokumentace). Dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace.
6. Seznámení s obsluhou dodávaného systému a jeho budoucím provozem (správci).
7. Zařazení do provozního prostředí objednatele (dohled, zálohování apod.).
8. Provedení zkušebního provozu.
9. Poskytnutí záruky minimálně 3 roky na dodané vybavení.

2.1.2 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou negativně dotčeny současné systémy, technologie.

2.1.3 Vyloučení z dodávky

Předmětem dodávky není:

1. Čtečky karet do notebooků, PC a tabletů.
2. Čtečky karet pro přístupový systém a dveřní systémy napojené na přístupový systém.
3. Zámky dveří kompatibilní s dodávaným systémem zajistí Objednatel v součinnosti.
4. Zajištění v rámci požadavků neuvedené komunikační infrastruktury (sítě apod.) mezi jednotlivými prvky systému.
5. Infrastruktura, HW a systémový SW poskytovaný Objednatelem (ZZS KHK) uvedený ve výchozím stavu a neuvedený v požadavcích.
6. Spotřební materiál využívaný v následném provozu informačních systémů neuvedený v rámci požadavků.

Koncept řešení, principy a požadavky na dodávky a služby jsou uvedeny dále v tomto dokumentu.

2.2 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

2.2.1 Obecné a společné požadavky

V této kapitole jsou uvedeny obecné požadavky na požadované řešení:

#	Požadavek
P.1	Dodávané technologie musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy a technologiemi ZZS KHK.
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz dodávaných technologií min. po dobu účinnosti servisní smlouvy.
Legislativa a další normy	
P.4	Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General data protection regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.



#	Požadavek
P.5	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti v aktuálním znění.
P.6	Soulad s prováděcím nařízením Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný (dále jen „PNK“- Prováděcí nařízení Komise).
Ostatní obecné požadavky	
P.7	Zajištění jednotného času na všech technologiích a zařízeních (synchronizace s time serverem).

Tabulka 3: Obecné požadavky

Pro konkrétní oblasti jsou uvedeny specifické požadavky samostatně v dílčích podkapitolách.

2.2.2 Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.8	Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet Součástí je vybudování systému, dodávka systému, instalace, zapojení a konfigurace prvků přístupového systému a zajištění všech nezbytných integrací (napojení na RADIUS server, MS AD atd.).
Obecné funkcionality	
P.9	Zjednodušení životního cyklu karet a certifikátů, automatizace procesů životního cyklu karet formou průvodců pro správce životního cyklu i pro držitele certifikátů. Odstínění koncových uživatelů od technologie.
P.10	Podpora činností spojených se správou životního cyklu čipových karet a certifikátů, zastřešení registračního místa doménové CA.
P.11	Webová aplikace, určená správcům certifikátů. Možnost vyhledávat a prohlížet informace o certifikátech, odvolávat certifikáty, generovat a prohlížet reporty.
P.12	Automatizovaná obnova kvalifikovaných i komerčních certifikátů alespoň od dvou externích poskytovatelů v ČR. Podpora minimálně eIdentity a PostSignum.
P.13	Napojení na dodávanou doménovou CA (viz dále), automatizovaná obnova interních uživatelských certifikátů z doménové CA na čipových kartách.
P.14	Aplikace pro nahrávání certifikátů na dodávané karty, a to jak pro správce, tak pro uživatele v rámci jejich obnovy pro minimálně 2 pracoviště.
P.15	Aplikace pro kvalifikované elektronické pečetění dokumentů prostřednictvím kvalifikovaného certifikátu uloženého na eIDAS ready bezpečnostním prostředku.



#	Požadavek
P.16	Prostřednictvím e-mailové notifikace upozorňování uživatelů na blížící se konec platnosti certifikátu, nebo na další stavy při změně životního cyklu certifikátu. Např. vystavení, konec platnosti apod.
P.17	Anonymizace údajů o uživatelích, kteří ukončí pracovní poměr.
P.18	Možnost do dokumentu PDF, Word nebo Excel připojit kvalifikovaný elektronický podpis + pečeti + vodoznak v rámci jednoho kroku
Dvoufaktorová autentizace	
P.19	Integrace do domény MS Windows 2016 a vyšší pro dvoufaktorovou autentizaci uživatelů na základě certifikátu a kryptografických operací, kde jako druhý faktor bude sloužit bezpečnostní předmět (karta) nebo mobilní telefon (mobilní aplikace nebo autentikátor, min pro platformy iOS a Android).
Integrace	
P.20	Exporty pro Přístupový systém – export karet a jim příslušejících uživatelů a platnosti karet ve formátu MS Excel. <i>Přesná struktura bude poskytnuta v rámci implementační analýzy.</i>
P.21	Exporty pro Docházkový systém – export karet a jim příslušejících uživatelů a platnosti karet ve formátu MS Excel. <i>Přesná struktura bude poskytnuta v rámci implementační analýzy.</i>
P.22	Integrace na MS Active Directory: 1. Přebírání seznamu uživatelů a relevantních uživatelských dat. 2. Dvoufaktorová autentizace – viz výše. 3. Přebírání začátku a konce platnosti uživatelských účtů a zneplatnění účtů, karet a certifikátů po ukončení platnosti účtu uživatele.
P.23	Poskytnutí API pro získání seznamu karet, jejich příslušnosti k uživatelům (dle MS AD) a veřejných částí komerčních certifikátů.
P.24	Integrace dvoufaktorové autentizace na RADIUS server pro zajištění vzdálených VPN přístupů v rámci domény MS Windows. Implementace pro VPN / Access přístup pomocí RADIUS serveru (Microsoft NPS) s využíváním atributů protokolu RADIUS (závislé podle dodavatele – AV-Pair apod.) pro jednotlivé skupiny uživatelů AD.
Dodávka / instalace	
P.25	Instalace, zapojení a konfigurace systému. <i>Provozní infrastrukturu poskytne objednatel.</i>
P.26	Veškerá nastavení a oprávnění musí být v souladu se zákonnými požadavky na ochranu osobních údajů.



#	Požadavek
Potisk / tiskárna	
P.27	Služby pro personalizovaný oboustranný potisk čipových karet z evidence karet/uživatelů na dodávané tiskárně pro potisk čipových karet (viz kap. 2.2.5).

Tabulka 4: Dodávka centrálního systému pro řízení přístupů pracovníků ZZS KHK pomocí čipových karet

2.2.3 Vybudování PKI infrastruktury ZZS KHK

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.28	Dodávka technologií pro bezpečnostní vrstvu vybudovanou na bázi PKI MS Windows, která je primárně určena pro vydávání klientských karetních a infrastrukturních certifikátů pro zavedení 2FA autentizace. Z doménového PKI se budou vydávat uživatelské certifikáty na čipové karty za účelem zavedení primárně dvoufaktorové autentizace (náhrada autentizace jménem/heslem). Mimo přihlášení do PC budou z interní CA vydávány případně certifikáty pro přihlášení do VPN a interní elektronický podpis. Interní PKI bude také poskytovat infrastrukturní certifikáty pro interní použití, např. certifikáty pro web servery a DC.
P.29	Zpracovat návrh implementace PKI v rámci ZZS. Bude využita dvouvrstvá hierarchie CA na OS MS Windows. Privátní klíče všech CA budou hostovány v úložišti OS.
P.30	Implementace zvolené architektury hierarchie PKI, zprovoznění PKI v prostředí objednatele.
P.31	Předat podklady na implementaci šablon pro vydání certifikátů pro autentizaci uživatelů do domény, případně další uživatelské akce.
P.32	Předat podklady na implementaci šablon pro vydání technologických certifikátů pro Web server a DC.
P.33	Implementace šablon uživatelských a technologických certifikátů.
P.34	Definici distribučních bodů CRL.
P.35	Ochrana a uložení klíče CA.
P.36	Dodání havarijní a provozní dokumentace k vybudované vrstvě PKI.
P.37	Zálohování dodané doménové CA, aby v případě havárie bylo možno CA obnovit, znovu zprovoznit a provést kompletní obnovu dat
P.38	Instalace, zapojení a konfigurace systému.
P.39	Veškerá nastavení a oprávnění musí být v souladu se zákonnými požadavky na ochranu osobních údajů.

Tabulka 5: Vybudování PKI infrastruktury ZZS KHK



2.2.4 Čipové karty

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.40	Hybridní čipové karty ve velikosti ID-1 (bankovní karta) s bezkontaktním čipem (Mifare DesFire) pro přístupový systém a funkcí bezpečného zařízení (kvalifikovaný prostředek QSCD) pro ukládání kvalifikovaných i komerčních certifikátů a vytváření elektronického podpisu (QESCD) v souladu s legislativou.
P.41	Karty musí být v souladu (certifikované): 1. s normou ČSN EN ISO 7816, část 1-4 a 2. standardem EN 419 211 a profily: a. BSI-CC-PP-0059 b. BSI-CC-PP-0075 c. BSI-CC-PP-0071 d. BSI-CC-PP-0072 e. BSI-CC-PP-0076
P.42	Kompatibilní s centrálním systémem (viz kap. 2.2.2).
Kontaktní čip a PKI	
P.43	Možnost uložení elektronických certifikátů X.509 (a generování / uložení příslušných kryptografických klíčů), kontaktní čip na bázi GlobalPlatform/JavaCard s personalizovanou PKI aplikací.
P.44	Všechny operace s privátním klíčem probíhají uvnitř čipu. Privátní klíč uložený na kartě nelze z karty vyexportovat.
P.45	Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS. Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu.
P.46	Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány
P.47	Vytváření elektronického podpisu na bázi certifikátů ve formě: 1. kvalifikovaného elektronického podpisu, 2. zaručeného elektronického podpisu, 3. uznávaného elektronického podpisu a 4. jiné formy elektronického podpisu.
P.48	Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12. Generování a práce s RSA a ECC klíči v čipu.
P.49	Archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů.
P.50	Podpora minimálních kryptografických algoritmů: 1. Symetrické: 3DES, AES 2. Eliptické křivky: P-224, P-256, P-384, P-521 3. RSA: 1024, 2048 bitů



#	Požadavek
	4. Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
P.51	Zablokování bezpečnostního kódu PIN, QPIN resp. PUK po opakovaném chybném zadání PIN, QPIN resp. PUK. Podpora odblokování bezpečnostního kódu PIN pomocí PIN nebo PUK, podpora odblokování bezpečnostního kódu QPIN pomocí QPIN nebo PUK.
P.52	Zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů)
P.53	Dvoufaktorovou autentizaci na bázi certifikátů X.509 (do PC v prostředí Microsoft AD, webových služeb, VPN, aplikací atd.). Hybridní čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů.
Ovladače do OS a související SW	
P.54	Čipové karty budou dodány s ovládacím software, pro integraci kontaktního čipu karty do operačního systému. Vlastnosti ovládacího software: 1. Podléhá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V5.07 nebo vyšší 2. Podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11 3. Použití na MS Windows 10 nebo vyšších verzích; 4. Použití na Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11) OS X (PKCS#11) 5. Instalace z MSI balíčků (podpora obslužné a bezobslužné instalace), RPM, DEB
Stav dodané karty	
P.55	Inicializovaná PKI aplikace s PIN, QPIN a PUK.
P.56	Předání seznamu personalizovaných karet, pro import do evidence CMS (viz kap. 2.2.2). U každé karty uvedeno číslo kontaktního, případně i bezkontaktního čipu.
P.57	Inicializovaná PKI aplikace výchozími hodnotami PIN, QPIN a PUK. Technickými prostředky bude vynuceno, aby si uživatel po přijetí karty změnil hodnotu bezpečnostních kódů.

Tabulka 6: Čipové karty

2.2.5 Tiskárna na potisk čipových karet

V této kapitole jsou uvedeny základní požadavky tuto část předmětu plnění.

#	Požadavek
P.58	Dodávka tiskárny na oboustranný potisk dodávaných čipových karet.
P.59	Tisk oboustranného potisku z nástrojů centrálního systému pro řízení přístupů uživatelů (viz kap. 2.2.2).
P.60	Instalace, zapojení a konfigurace tiskárny včetně napojení na centrální systém a ověření oboustranného tisku na dodávání karty. <i>Potisk všech dodávaných karet není předmětem dodávky, předmětem je jen seznámení personálu s použitím.</i>

Tabulka 7: Tiskárna na potisk čipových karet



2.2.6 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.61	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup.
P.62	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.63	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.64	Evidence přístupů všech uživatelů do systémů a technologií (logování) včetně časových údajů.
P.65	Veškeré přístupy k datům a aktivitě uživatelů v rámci dodávaných systémů a technologií budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů.
P.66	Veškeré logy budou dostupné pro externí systém sběru a analýzy logů.

Tabulka 8: Bezpečnostní požadavky

2.2.7 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.67	Všechny komponenty musí být připraven na provoz 24x7x365 (non-stop).
P.68	Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce. Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.
P.69	Instalace do prostředí objednatele uvedeného v kap. 5.1 – Stav informačních a komunikačních technologií.
P.70	V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů a technologií. To vše s minimálním omezením provozu. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.
P.71	Zajištění administrátorských aplikací, konzolí pro všechny součásti systému pro zajištění konfiguračního managementu systému anebo jeho součástí.



#	Požadavek
P.72	Dohled – dodávané systémy a technologie musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.73	Synchronizace času všech zařízení s time serverem nebo zprostředkovaně přes centrální systém.

Tabulka 9: Provozní požadavky

2.3 POŽADAVKY NA SLUŽBY

2.3.1 Realizace předmětu plnění

Součástí předmětu plnění je zajištění služeb souvisejících s realizací předmětu plnění minimálně v následujícím rozsahu:

- 1) Objednatel požaduje před zahájením implementačních prací zpracování **Implementační analýzy včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace a montáže předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení musí zohlednit podmínky stávajícího stavu a požadavky cílového stavu.
- 2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.
- 3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele:

Provedením těchto činností bude zajištěna připravenost pro ověření ze strany objednatele.

- 4) **Dodávka předmětu plnění.** Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:
 - a) Instalace, upgrade a zahoření HW na místě
 - b) Instalace a nastavení HW a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení
 - c) Nastavení HW a SW aplikací
- 5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.
- 6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.
- 7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším objemu dat, s menším počtem uživatelů a na menším počtu zařízení.
- 8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.
- 9) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:



Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a systémová/provozní dokumentace	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační)

Tabulka 10: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2016 (MS Word 2016, MS Excel 2016, MS PowerPoint 2016)
- MS Project 2016
- WinZip (formát .zip)
- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky, a to na elektronických nosičích (CD, DVD, flash disk atp.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2 kopiích v elektronické formě ve standardních formátech (MS Office a PDF) používaných objednatelem na datovém nosiči, listinná forma se nepožaduje.

- 10) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
- 11) **Uvedení systému do produkčního provozu,** zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.
- 12) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.



- 13) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

2.3.2 Seznámení s funkcionalitami, obsluhou dodávaných technologií

V této kapitole jsou uvedeny požadavky na seznámení s funkcionalitami, obsluhou dodávaných technologií a jejich budoucím provozem:

- 1) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
 - a) Základní produktové seznámení s jednotlivými dílčími technologickými celky.
 - b) Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
 - c) Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
 - d) Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
 - e) Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.
- 2) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- 3) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
- 4) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
- 5) Seznámení s funkcionalitami, obsluhou dodávaných technologií se týká správců.

Veškeré náklady na zajištění těchto činností musí být zahrnuty v ceně odpovídající části předmětu dodávky.

2.4 ZÁRUKY

V této kapitole jsou uvedeny požadavky na záruky dodávky jako celku, případně specificky dílčích částí dodávky.

Objednatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně 36 měsíců.

Záruka začíná běžet od okamžiku předání do ostrého (produkčního) provozu. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky. Zhotovitel ve své nabídce výslovně uvede všechny podmínky záruk.

- a) Po dobu záruky na části dodávky musí zhotovitel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.
- b) Součástí záruky je i shoda dodávaných systémů s platnou legislativou.
- c) Max. doba na odstranění vady díla je 30 dnů od prokazatelného oznámení dodavateli.
- d) Zhotovitel uvede provozní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému.



3 HARMONOGRAM

Následující tabulka obsahuje požadovaný časový harmonogram realizace dodávky (T ~ datum účinnosti smlouvy o dílo):

#	Fáze	Doba trvání od zahájení	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	30	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace.
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.	90	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace úprav SW, dodávka dokumentace k SW.	90	Vlastní vývoj a implementace úprav IS dle analýzy a návrhu řešení.
5	Ověření funkčnosti dodaných technologií a systémů.	100	Otestování funkčnosti technologií a systémů a ověření jejich plné funkčnosti.
6	Seznámení s funkcionalitami, obsluhou dodávaných technologií	100	Seznámení s funkcionalitami, obsluhou dodávaných technologií
7	Dodávka dokumentace dodaného systému a jeho částí.	100	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
8	Převedení do zkušebního provozu.	100	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
9	Ukončení realizace dodávky.	110	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Tabulka 11: Harmonogram

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.
- Zhotovitel má možnost definovat kratší termíny plnění (v rámci dodávky), v nabídce nelze zkrátit dobu zkušebního provozu, která musí být minimálně 10 dnů.
- Zkrácení zkušební doby je možné pouze na základě písemné dohody se Zadavatelem.



4 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Sídlo a centrální datové centrum	Hradecká 1690/2a, Hradec Králové PSČ: 500 12	<u>Centrální datové centrum ZZS KHK</u> – dodávka částí technologie. <u>Sídlo ZZS KHK</u> – místo předání výstupů projektu. <i>Pozn.: toto DC je také označováno jako „primární“.</i>
Datové centrum IS ZOS ZZS KHK	Pražská 230/153z, Hradec Králové PSČ: 500 04	<u>Datové centrum IS ZOS ZZS KHK</u> – dodávky v návaznosti na technologie umístěné v tomto DC a dodávka částí technologie. Lokalita, kde je provozován IS ZOS a kde je DC ZOS a kde je umístěn ZOS (dispečink). <i>Pozn.: lokalita označovaná také jako „Bláhovka“</i>

Tabulka 12: Místa plnění



5 VÝCHOZÍ STAV

V této kapitole je uveden výchozí stav a výchozí podmínky pro dodávku předmětu plnění.

5.1 STAV INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

V této kapitole je uveden základní popis výchozího stavu jednotlivých prvků ostatních informačních a komunikačních technologií.

5.1.1 Datové centrum, HW infrastruktura, systémový SW a technologie

V následující tabulce je uveden popis datového centra, HW infrastruktury a systémového SW:

Parametr	Údaj(e), parametry a informace
Datové centrum <u>IS ZOS (Lokalita Bláhovka)</u>	
Záložní zdroj el. energie	Záložní napájení je využíváno v rámci napájení serverovny HZS, zajištěné jak UPS, tak motorgenerátorem.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v několika RACK skříních.
Servery	Jako virtualizační servery je využíváno celkem pět serverů DELL PowerEdge. Pro další potřeby jsou provozovány ještě další tři samostatné servery DELL PowerEdge a jeden HP ProLiant. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.
Disková úložiště	Úložiště je realizováno diskovým polem DELL SCv3020 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou vyhrazeny 10Gbps switche DELL, které tak tvoří infrastrukturu pro iSCSI.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware, případně prostou kopií dat na záložní NAS.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány licence Windows Server 2012 Datacenter. Pro některé servery je využit OS Linux v různých distribucích.
Virtualizační SW	Pro virtualizační servery je využito licence VMware Essentials Plus kit, který je určen pro 3 dvouprocesorové servery. Pro další dva servery je využito Oracle virtualizace.
DB	Pro provoz jsou využity databázové licence, a to jak ORACLE, tak Microsoft SQL server.
Dohled	Je realizován jako služba v rámci maintenance smlouvy s dodavatelem a za pomoci jeho prostředků.



Parametr	Údaj(e), parametry a informace
<u>Primární (centrální) datové centrum (Lokalita Hradecká)</u>	
Záložní zdroj el. energie	Záložní napájení je zajištěno jak UPS, tak motorgenerátorem.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříní.
Servery	Jako virtualizační servery jsou využívány 2 servery DELL PowerEdge. Pro další potřeby je provozován ještě jeden samostatný server DELL PowerEdge pro zálohu klíčového SW IS ZOS. Servery jsou osazeny síťovým rozhraním jak na technologii Gigabit ethernet, tak také TenGigabitethernet.
Disková úložiště	Úložiště je realizováno diskovým polem DELL SCv3020 10Gbps iSCSI a doplněno polem pro odkládání záloh QNAP NAS, který je také osazený 10Gbit rozhraním. Pro komunikaci diskových polí jsou využity přímo core switche HP datového centra (10Gbit) a fyzická rozhraní SAS serverů a diskového pole.
Zálohování	Zálohování virtualizovaného prostředí je realizováno v rámci nastavených zálohovacích scénářů pomocí SW Veeam Backup pro VMware.
Systémový SW	
Operační systémy	V rámci dodávky virtualizačních serverů byly dodány licence Windows Server 2016 Datacenter. Pro některé servery je využit OS Linux v různých distribucích.
Virtualizační SW	Pro virtualizační servery je využito licence VMware Essentials Plus kit, který je určen pro 3 dvouprocesorové servery.
DB	Pro záložní server je využita databázová licence ORACLE.
Dohled	V rámci infrastruktury je využíván produkt HP IMC pro dohled a monitoring.
<u>Záložní/zálohovací datové centrum (Lokalita LZS)</u>	
Záložní zdroj el. energie	Záložní napájení je zajištěno jen UPS.
HW infrastruktura	
Rackové skříně	Veškerá technologie v rámci serverovny je umístěna v RACK skříní.
Dohled	V rámci infrastruktury je využíván produkt HP IMC pro dohled a monitoring (společný s primárním DC).

Tabulka 13: Datové centrum, HW infrastruktura, systémový SW



5.1.2 Datové sítě

V rámci projektu budou využity následující sítě:

Datová síť	Popis
WAN ZZS	Bude využita pro komunikaci mezi lokalitami z důvodu nutné výměny dat souvisejících s realizací a provozem projektu.

Tabulka 14: Datové sítě

5.1.3 Síťová infrastruktura

V následující tabulce je uveden popis síťové infrastruktury:

Parametr	Údaj(e), parametry a informace
Směrovače	Lokality ZZS jsou propojeny do jedné WAN sítě prostřednictvím VPN WAN. Pro tyto účely jsou všechny lokality vybaveny routery Cisco, na kterých jsou nakonfigurovány IPSec tunely do obou centrálních lokalit. Správa těchto routerů jsou zajištěna servisní maintenance smlouvou s dodavatelem.
Firewally	V rámci centrálních lokalit jsou umístěny centrální FireWally FortiGate, které zajišťují zabezpečení WAN ZZS do sítě Internet a v rámci konfigurace centrálního FW jsou ukončovány i VPN přístupy pracovníků ZZS a externích firem do sítě ZZS. FireWall odděluje interní síť ZZS nejenom od sítě Internet, ale i od ostatních externích sítí jako je NIS IZS a AKČR apod.
LAN	Lokalita Bláhovka: V rámci DC IS ZOS jsou využity LAN prvky na bázi switchů. Přičemž centrální stack switchů Cisco 3850 realizuje i routování VLAN segmentů LAN sítě. Lokalita Hradecká: V rámci Primárního DC jsou využity LAN prvky na bázi switchů. Přičemž centrální stack switchů HP 5800 realizuje i routování VLAN segmentů LAN sítě.
Připojení k internetu	V obou centrálních lokalitách je i centrální napojení do sítě Internet. Toto připojení je zabezpečeno FireWallem (viz výše). Poskytovatelem připojení do sítě Internet je CESNET. Záložní připojení je zajištěno nezávislým lokálním operátorem HK Free.

Tabulka 15: Síťová infrastruktura

KONEC DOKUMENTU