Příloha č. 4 Zadávací dokumentace – Technická dokumentace zadavatele

Příloha č. 1 Kupní smlouvy – Technická dokumentace kupujícího

Technická dokumentace

Dodávka IT infrastruktury a licencí pro zvýšení kybernetické bezpečnosti

Verze 015 ze dne 30.07.2025

Obsah dokumentu

1. Technická specifikace zadavatele (kupujícího)

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

Propojení zařízení – SFP moduly a kabely

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Plnění jednotlivých komponent dle specifikace níže je požadováno v následujícím rozsahu, a to včetně příslušenství:

Položka plnění	Počet kusů
Next Generation Firewall s příslušenstvím	2
Páteřní přepínače 48p s příslušenstvím	2
Přístupové přepínače 48p PoE s příslušenstvím	28
Přístupové přepínače 24p s příslušenstvím	2
Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x	1
Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI	1
Autentizační prostředky	300
Klávesnice s integrovanou čtečkou karet, včetně ovladačů	150
Samostatné USB čtečky čipových karet, včetně ovladačů	150
Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM	1

1.1. Next Generation Firewall s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Pro montáž do 19“ datového rozvaděče, včetně montážního materiálu
NGFW	Min. základní funkce Next-generation firewall – viz https://en.wikipedia.org/wiki/Next-generation_firewall – firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
Porty	Min 2× 2.5GbE, 8x 1GbE a 2× 1OGbE
Počet současných spojení	Min. 6 000 000.
Propustnost VPN	Min. 10 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 100 klientů.
Propustnost firewallu	Min. 18 Gbps pro pakety 1518 bytů a větší, provoz UDP.
Propustnost NGFW	Min. 15 Gbps při aktivní IPS.
Propustnost IPS	min. 15 Gbps pro provoz typu Enterprise mix.
Propustnost detekce škodlivého kódu	Min. 5 Gbps při zapnuté IPS.
Virtualizace	Podpora min 5 izolovaných virtuálních kontextů (virtuálních firewallů). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů.
Vysoká dostupnost	Režimy Active/Active se společnou konfigurací, včetně případných nezbytných licencí.
Dualstack	Podpora současného běhu IPv4 a IPv6.
VPN	Podpora IPSec, SSL VPN
Bezpečné DNS	Automatická blokace přístupu k škodlivým doménám a IP adresám, definice součástí bezpečnostních aktualizací. Ochrana proti DNS tunelování.
Aplikační kontrola	Detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.
Antivir	Integrovaný antivirus, podpora protokolu ICAP pro externí antivir
ZeroDay	Ochrana před ZeroDay útoky formou emulace neznámého kódu v bezpečném prostředí – Sandboxu
Kategorizace a blokace provozu	Založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu
Antispam	Antispamová a antivirová a antiphishingová inspekce elektronické pošty. Transparentní (průchozí) kontrola i MTA režim.
Aktualizace	Automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení.
Ověřování uživatelů	LDAP, Active Directory, Radius, Ověřování na základě certifikátu.
Management a monitoring	HTTP/S, SSH, SNMP, syslog.

Centrální správa	Jednotná centrální správa samostatných boxů i clusteru, monitorování a aktualizace firmware z centrální grafické konzole. Lokální i cloudová správa s podporu spolupráce více správců (např. při řešení bezpečnostních událostí/incidentů) při zachování konzistence konfigurační nastavení.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent).
Geolokace	Možnost nastavovat firewall politiky na základě geografických údajů IP adres
Standardní funkce	NAT, statické a dynamické routování (OSPFv3, BGP, RIP), publikace interních serverů, routování založené na politikách (policy based routing).
API	Integrované API rozhraní pro automatizaci a orchestraci
Napájení	Redundantní napájecí zdroje.
Záruční doba, podpora a záruční servis, technická podpora výrobce	Záruční doba, podpora a záruční servis min. 60 měsíců v režimu 8x5 poskytovaný výrobcem zařízení, odeslání náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a všech bezpečnostních funkcí – URL filtrace, DNS, IPS, antimalvare, antispam, aplikační kontrola, sandbox, ZeroDay).

1.2. Páteřní přepínače 48p příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní parametry	L2/L3 přepínač v rackovém provedení, 1U včetně montážního materiálu
Porty	min. 48x 10 Gb SFP+, 4x 100 Gb QSFP28 s podporou QSFP+
Propustnost	Neblokovaná architektura, přepínací kapacita je min. součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Agregace portů	Podpora LACP, min. 50 skupin, min. 8 portů ve fyzické agregační skupině, min. 16 portů ve virtuální agregační skupině při zapojení přepínačů do logického páru.
Směrování	Statické směrování (routování) včetně VLAN, dynamické směrování (min. RIP, OSPF, BGP), směrování založené na politikách, min. routovacích záznamů pro IPv4 24 000 a IPv6 12 000
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Minimální přepínací výkon: 1,7 Tbps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření, podpora IEEE 802.1ad (Q-in-Q), podpora statických a dynamických VXLAN, min. 1024 VLAN. Podpora privátních VLAN (PVLAN) pro izolaci klientů ve stejné VLAN (mikrosegmentace, dynamická segmentace)
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora min. 140 000 MAC adres.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent. sFlow není ekvivalent.
Zrcadlení portů	Zrcadlení provozu (odchozího i příchozího) do lokálního i vzdáleného portu

Parametr	Popis minimální úrovně parametru
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST API a integrovaná podpora skriptů pro automatizaci. Interní detailní monitorování funkcí/služeb přepínače s možností konfigurovatelných automatických reakcí.
Nezávislý management	Vyhrazený LAN port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Napájení, chlazení	Integrované redundantní interní napájecí zdroje, zdroje i ventilátory vyměnitelné za provozu (hot-swap)
Centrální správa	Podpora stávajícím systém centrální správy
Stohování	Pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG/MCLAG (Multi-Chassis Link Aggregation) nebo obdobná. Synchronizace konfigurací přepínačů ve stohu. Min. 32 portů v agregační skupině stohu. Kapacita stohovacího propojení: 400 Gbps
Záruční doba a záruční servis	Záruční doba a záruční servis min. 60 měsíců v režimu 24×7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace SW a aktualizace firmware.

Příslušenství pro páteřní přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství centrálních přepínačů	Pro celý komplet dodávaných centrálních přepínačů požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: • 92x SFP+ 10 Gbps modul, SM, 10 km, LC, DMI diagnostika pro nabízené přepínače • 4x SFP+ 10GbE modul, RJ-45, DMI diagnostika pro nabízené přepínače • 8x QSFP28 100GBASE-SR4, MM, 100 m • 2x patch kabel MM OM3/4 MPOf-MPOf, překřížený, 1 m – pro propojení nabízených přepínačů • 4x patch kabel MM OM4, MPOf – 8x LC (4 páry), 3 m • 60x patch kabel SM LC-SC, 3 m • 36x patch kabel SM LC-LC, 3 m Cena příslušenství musí být zohledněna v ceně samotných přepínačů. Záruční doba na příslušenství min. 36 měsíců
Licence pro centrální správu	Je požadováno dodání licencí pro začlenění dodávaných přepínačů do systému centrální správy kupujícího.

1.3. Přístupové přepínače 48p PoE příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	L2+ přepínač v rackovém provedení max. 1U; maximální hloubka přepínače 35 cm (z důvodu omezených rozměrů pobočkových rozvaděčů)
Porty	Min. 48× 1 GbE, 4× 10 Gb SFP+.
Propustnost	Neblokovaná architektura, přepínací kapacita je min. součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Power on Ethernet	Podpora PoE/PoE+ 802.3af/at na všech metalických portech, celkový PoE výkon min. 700 W.

Parametr	Popis minimální úrovně parametru
Agregace portů	Podpora LACP, min. 16 portů v agregační skupině, min. 20 skupin.
Směrování	Statické směrování (routování), min. 500 směrovacích cest pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Minimální přepínací výkon 175 Gbps Minimální paketový výkon 120 Mpps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN na základě 802.1X ověření.
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora min. 16 000 MAC adres.
Zrcadlení provozu	Zrcadlení příchozího i odchozího síťového provozu
Napájení	Interní napájecí zdroj.
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API a integrovaná podpora skriptů pro automatizaci
Nezávislý management	Vyhrazený LAN port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent. sFlow není ekvivalent
Centrální správa	Podpora stávajícím systém centrální správy
Stohování	Pokročilé stohování po SFP+ portech s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG/MCLAG (Multi-Chassis Link Aggregation) nebo obdobná. Synchronizace konfigurací přepínačů ve stohu. Podpora min. 4 členů ve stohu.
Záruční doba a záruční servis	Záruční doba a záruční servis min. 60 měsíců v režimu 24×7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace a aktualizace firmware.

Příslušenství pro přístupové přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství přístupových přepínačů	Pro celý komplet dodávaných přístupových přepínačů 48p PoE požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: • 112 ks 10 Gb SFP+ modul SM, min. 10 km, diagnostika, LC konektor • 56 ks 2 m propojovacích SM kabelů LC-LC • 56 ks 2 m propojovacích SM kabelů LC-SC Cena příslušenství musí být zohledněna v ceně samotných přepínačů. Záruční doba na příslušenství min. 36 měsíců
Licence pro centrální správu	Je požadováno dodání licencí pro začlenění dodávaných přepínačů do systému centrální správy kupujícího.

1.4. Přístupové přepínače 24p PoE příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	L2+ přepínač v rackovém provedení max. 1U
Porty	Min. 24× 1 GbE, 4× 10 Gb SFP+.
Propustnost	Neblokovaná architektura, přepínací kapacita je min. součtem plných rychlostí duplexního provozu všech portů s výjimkou nezávislého portu pro správu
Agregace portů	Podpora LACP, min. 8 portů v agregační skupině, min. 8 skupin.
Směrování	Statické směrování (routování), min. 500 směrovacích cest pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p.
Výkon	Minimální přepínací výkon 125 Gbps Minimální paketový výkon 90 Mpps
VLAN	VLAN 802.1Q, MAC i založená na protokolu, podpora zařazování do VLAN na základě 802.1X ověření.
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X.
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS.
MAC	Podpora min. 8000 MAC adres.
Zrcadlení provozu	Zrcadlení příchozího i odchozího síťového provozu
Napájení	Interní napájecí zdroj.
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST API pro automatizaci.
Síťové toky	Plný přímý export síťových toků – Netflow, IPFIX nebo ekvivalent. sFlow není ekvivalent
Centrální správa	Podpora stávajícím systém centrální správy
Záruční doba a záruční servis	Záruční doba a záruční servis min. 60 měsíců v režimu 24×7 poskytovaný výrobcem zařízení, odeslání náhradního zařízení do 2 pracovních dnů po nahlášení závady, nárok na aktualizace a aktualizace firmware.

Příslušenství pro přístupové přepínače jako celek

Parametr	Popis minimální úrovně parametru
Příslušenství přístupových přepínačů	Pro celý komplet dodávaných přístupových přepínačů 24p požadujeme následující celkový počet příslušenství v podobě SFP modulů a kabelů: • 8 ks 10 Gb SFP+ modul SM, min. 10 km, diagnostika, LC konektor • 4 ks 2 m propojovacích SM kabelů LC-LC • 4 ks 2 m propojovacích SM kabelů LC-SC Cena příslušenství musí být zohledněna v ceně samotných přepínačů. Záruční doba na příslušenství min. 36 měsíců
Licence pro centrální správu	Je požadováno dodání licencí pro začlenění dodávaných přepínačů do systému centrální správy kupujícího.

1.5. Licence SW pro řízení přístupu do sítě založeného na protokolu 802.1x

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Software nebo softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází – Active Directory, LDAP, ODBC
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, autorizace proti externí SQL databázi
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth)
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory
Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google
Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období
Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení
Profilování	Zjišťování doplňujících informací pro koncová zařízení (min. typ, výrobce, OS a pod.)
TACACS+	Podpora autentifikace a autorizace na síťové prvky protokolem TACACS+
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační) stránky
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-bit.
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, UPS, technologické prvky, IoT.

Parametr	Popis minimální úrovně parametru
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance není součástí dodávky.
Licence	Trvalá licence pro min. 1000 současných (konkurenčních) koncových zařízení ověřených pomocí 802.1X bez omezení počtu uživatelů
Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA.
Kompatibilita	Software nebo appliance bude výrobcem podporována pro provoz v prostředí stávající serverové virtualizace
Podpora	Podpora výrobce 60 měsíců včetně nároku na nové verze a aktualizace software

1.6. Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Systém pro autentizaci uživatele identifikačním prostředkem vůči adresářové službě včetně nástrojů pro správu
Autentizace	Autentizace uživatele ve stávajících operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft) pomocí nabízených autentizačních médií
Obnova certifikátů	Automatické hlídání expirace osobních certifikátů a vyvolání uživatelského průvodce pro jeho jednoduchou uživatelskou obnovu podle nastavených politik. Včetně automatického odstranění neplatných certifikátů na základě politik.
Uživatelská správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK)
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu v operačním systému, testování integrity a použitelnosti
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů vystavených veřejnými certifikačními autoritami (min. Postsignum) a vyvolání průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik
Správa prostředků	Evidence a správa životního cyklu identifikačních prostředků
Prostředky	Podpora kontaktních i hybridních identifikačních prostředků
Správa systému	Webové rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory
Evidence	Systém umožní evidovat minimálně - typ prostředku (kontaktní, bezkontaktní, hybridní) - druh prostředku (uživatelský, administrační, operátorský) - stav prostředku (používaný, k recyklaci, skartovaný) - historii prostředku (datum zavedení do evidence, vydání uživateli, recyklace) - držitele prostředku (aktuálního držitele i všechny předchozí držitele) - data uložená v prostředku (certifikáty a další data, včetně historie dat)

Parametr	Popis minimální úrovně parametru
Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných): - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance
Obnova prostředků	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (I vzdálené), tisk protokolů
Personifikace	Integrované prostředí pro generování podkladů pro potisk identifikačních karet externím dodavatelem i na vlastní tiskárně
Ukládání dat	Centrální databázové úložiště údajů, podpora Microsoft SQL server (stávající hlavní databázové úložiště zadavatele)
Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování informací napojených systémům
Notifikace	E-mailové notifikace uživatelů i správců o blížící se expiraci certifikátů doménových i veřejných certifikačních autority
PKI	Součástí dodávky bude vybudování kompletní kompatibilní infrastruktury PKI (public key infrastructure) pro zajištění celého životního cyklu osobních přihlašovacích certifikátů a jejich šablon, včetně dodávky potřebných licencí
Licence	Licence pro 300 uživatelů
Podpora	Podpora výrobce po dobu 60 měsíců včetně nároku na nové verze a aktualizace software

1.7. Autentizační prostředek

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Hybridní identifikační karta s kontaktní částí SmartCard a bezkontaktní částí čipem EM4102
Podporované certifikáty	Karta musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit (I. CA, Postsignum, eidentity)
Identity	Karta musí umožnit ukládání více identit
Kvalifikovaný podpis	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku), viz https://www.dia.gov.cz/cs/legislativa/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/informace-pro-uzivatele/seznam-vydavanych-kvalifikovanych-prostredku-pro-vytvareni-elektronickych-podpisu-v-ceske-republice
SW podpora	Součástí dodávky bude software a ovladače pro zpřístupnění jejich rozhraní v operačních systémech Windows, Linux, macOS a systému terminálových služeb Microsoft RDS včetně rozšířených funkcionalit, tzv. middleware.
Záruční doba	Záruční doba 2 roky včetně nároku na aktualizace middleware

1.8. Klávesnice s integrovanou čtečkou karet, včetně ovladačů

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Standardní PC klávesnice se samostatným numerickým blokem a integrovanou čtečkou čipových karet
Rozhraní	USB rozhraní
Čtečka	Kompatibilita s čipovou částí nabízených identifikačních prostředků a nabízeným SW pro vícefaktorové ověřování
Lokalizace	České (QWERTZ) rozložení kláves, české popisky
SW podpora	Součástí dodávky bude software a ovladače pro operační systémy Windows, Linux, macOS – nejsou-li ovladače standardní součástí operačních systémů.
Záruční doba	Záruční doba min. 2 roky

1.9. Samostatné USB čtečky čipových karet, včetně ovladačů

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Provedení	Samostatná čtečka čipových karet
Rozhraní	USB rozhraní
Čtečka	Kompatibilita s čipovou částí nabízených identifikačních prostředků a nabízeným SW pro vícefaktorové ověřování
SW podpora	Součástí dodávky bude software a ovladače pro operační systémy Windows, Linux, macOS – nejsou-li ovladače standardní součástí operačních systémů.
Záruční doba	Záruční doba min. 2 roky

1.10. Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní funkce	Privilegovaný přístup na cílový systém bude zprostředkován prostřednictvím tzv. terminal/jump serveru zvoleným komunikačním protokolem tak, aby privilegovaný uživatel neměl přístup k přihlašovacím údajům cílového systému. Izolace přístupu bude možná až na úroveň aplikace (typu webový prohlížeč s konkrétním URL, MMC konzole s vybraným snap-in, konkrétní aplikace - např. MS SQL Management Studio, WinSCP atp.) a uživatel nebude mít možnost přistupovat k jiným službám či aplikacím v rámci dané relace. Ukončením aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI systému nebo pomocí standardních protokolů RDP a SSH a standardních klientů.
Bezpečná autentizace	Podpora vynucení silné autentizace pro připojení ke vzdálené relaci
SSH připojení	Privilegovaný přístup prostřednictvím SSH protokolu bude v rámci vzdálené relace prováděn přes ssh proxy, na které bude uživatel ověřen svými přihlašovacími údaji (s možností spárování s Active Directory). K cílovému systému bude uživatel připojen a přihlášen podle bezpečností politiky vybraným privilegovaným účtem bez zadávání hesla. Pro připojení

Parametr	Popis minimální úrovně parametru
	pomocí ssh proxy bude systém podporovat vynucení silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí ssh klíče).
Webové připojení	Systém umožní zprostředkovat privilegovanému uživateli bezpečné připojení v rámci vzdálené relace na vybrané webové aplikace, přístup do cloudu apod. pomocí webové proxy, na které bude uživatel ověřen neprivilegovaným účtem (s možností ověření vůči Active Directory). K cílovému systému bude uživatel připojen a přihlášen podle bezpečností politiky vybraným privilegovaným účtem bez zadávání hesla. Systém bude podporovat transparentní SSO (single-sign-on).
Nahrávání relace	Monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu a ve formátu screenshotů. Záznam relace musí být vytvářen kontinuálně. V nahrávkách bude možné zpětně vyhledávat podle metadat. Přehrávání musí být dostupné přímo z GUI systému běžným internetovým prohlížečem a nesmí vyžadovat instalaci komponent třetích stran (flash, java, codec apod.).
Metadata	Zaznamenávání rozšířených informací (metadat) o relacích, minimálně stisky kláves a odpovědí monitorovaných zařízení
Nahrávky	Ukládání nahrávek relací v optimalizované kvalitě s možností volby cílového uložiště.
Politiky	Logické zařazení napojených systémů do skupin či profilů, nad kterými bude možno nastavit a aplikovat společné politiky a nastavení.
Ukončení relací	Možnost okamžitého ukončení potenciálně nebezpečných relací administrátorem či operátorem systému.
Auditování	Integrovaný audit jednotlivých akcí uživatelů s privilegovanými účty – min. zobrazení hesla, změny uložených údajů, vytvoření relace. Export auditních záznamů.
Bezpečnost auditních záznamů	Nezpochybnitelná auditovatelnost jednotlivých operací, reportování a textových logů. Auditní záznamy musí být bezpečně uloženy tak, aby k nim měli přístup pouze oprávnění uživatelé.
Reportování	Integrovaný generátor reportu veškerých aktivit správce systému. Přístupu k reportům musí být možno nastavit pouze vybraným uživatelům.
Autentizace	Podpora minimálně LDAP/S, SAML2, RADIUS pro autentizaci, autorizaci a vícefaktorové ověřování
Workflow	Integrované workflow pro zadávání a schvalování žádostí o přístup. Funkční požadavky na workflow: - Zadávání požadavků uživatelů - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů
Změna privilegií	Podpora delegace a eskalace privilegií na bázi schvalovacího workflow.
Vícedoménová autentizace	Podpora současného napojení více Active Directory/LDAP domén současně.
API rozhraní	Integrované API s podporu REST, aktivované v rámci dodávky. Výrobce, resp. dodavatel musí poskytovat volně dostupný aktualizovaný popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací.
Integrace servicedesk	Podpora napojení a integrace na servicedeskové/tiketovací systémy.
Odolnost	Veškeré komponenty systémy musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště účtů, přihlašovacích údajů, nahrávek relací a auditních záznamů musí být zabezpečeno a odděleno od ostatních komponent řešení.

Parametr	Popis minimální úrovně parametru
Správa účtů	Integrované vyhledávání (discovery) a správa účtů v systémech Windows Server, Microsoft SQL Server, Active Directory.
Správa zařízení	Podpora automatického vyhledávání (discovery) zařízení a jimi používaných uživatelských účtů.
Správa privilegovaných účtů	Podpora vyhledávání (discovery) privilegovaných (administrátorských) účtů v Active Directory.
Automatický onboarding	Podpora automatického přidávání nalezených účtů a zařízení do vlastního bezpečného úložišt (onboarding účtů a zařízení)
Rotace hesel	Podpora automatické správu účtů a rotace hesel minimálně pro systémy Windows Server a Linux, síťová zařízení (např. aktivní prvky) a webové aplikace. Rotaci hesel musí být možné provádět na základě nastavitelných intervalů.
Komplexita hesel	Podpora stanovení požadavků na délku, složitost (komplexnost) a maximální stáří hesel.
Rotace ssh klíčů	Automatická správa a rotace ssh klíčů.
Kontrola shody	Automatická identifikace hesel, která neodpovídají nastaveným politikám a odepření jejich uložení.
Vytváření hesel	Generování náhodných hesel podle nastavených pravidel.
Role	Podpora model RBAC (Role-based User Access Control). Možnost nastavení a přidělování oprávnění na skupiny/role.
Politiky zařízení	Možnost nastavení přístupových politik na zařízení.
Logování	Zasílání bezpečnostních logů do nadřazených logovacích systémů centrálního logování – min. syslog
Automatické odhlášení	Automatické odhlášení z centrální konzole při nečinnosti
Sdílené účty	Podpora rozlišení jedinečných uživatelů pro sdílené účty
Nouzový přístup	Integrovaný mechanismus zobrazení přihlašovacích údajů v čitelné podobě v případě nedostupnosti síťového propojení na cílový systém.
Dočasný přístup	Podpora dočasného povolení k užívání přístupových údajů na základě žádosti (pro procesní opatření „čtyř očí“).
Notifikace	Integrovaný systém emailových upozornění/notifikací, s možnosti přímého prokliku k řešení notifikované události
Reporting	Integrovaný reportovací systém. Předdefinované reporty min.: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup • Seznam aktivit nad účty (check out/in, přidělení účtů atp.) • Seznam automaticky vyhledaných nových uživatelských účtů a zařízení
Zálohování	Integrované nastavení a provádění pravidelných záloh.
Bezagentový systém	Podpora implementace bez potřeby instalace agentů na cílové systémy
Dokumentace	Dokumentace v českém jazyce poskytovaná a aktualizovaná výrobcem min. v rozsahu administrátorského a uživatelského manuálu včetně popisu konfigurace
Licence	Poskytnutá licence umožní nasazení a provoz pro 30 uživatelů a 300 napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace (počet a délka záznamů, velikost databází, počet reportů atd.).

Parametr	Popis minimální úrovně parametru
Podpora	Podpora výrobce po dobu 60 měsíců včetně nároku na nové verze a aktualizace software

2. Požadavky na instalační a implementační práce

Dodané řešení bude sloužit jako vysoce dostupná hyperkonvergovaná infrastruktura pro chod agendových IS kupujícího a jeho zálohování. Dodávka musí obsahovat kompletní instalaci a implementaci řešení, nad kterým pak bude v režii kupujícího se třetí stranou provedena implementace agendových systémů (virtuální databázové, aplikační a komunikační servery) a konfigurace úloh pro zálohování nově vytvořených virtuálních serverů s agendovými IS.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Dodavatel je povinen zahrnout (zohlednit do ceny) do nabídky i veškeré další činnosti a prostředky, které jsou nezbytné pro řádnou dodávku plnění v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Popis stávajícího prostředí kupujícího vstupujícího do plnění podle této specifikace:

Firewall – Za účelem úvodní konfigurace nově nasazovaných firewallů zajistí prodávajícímu kupující přístup ke stávajícím firewallům typu CheckPoint QUANTUM 3800 SECURITY GATEWAY, ze kterých prodávající převezme aktuální bezpečnostní politiky a konfigurace a navrhne jejich přenesení a úpravu pro nově nasazované firewally.

Aplikační firewall F5 BIG-IP.

Sekundární firewall Microsoft TMG (Microsoft Forefront Threat Management Gateway).

Serverové prostředí – Kupující provozuje serverové prostředí, které je virtualizované s využitím hypervisoru typu VMware ESX a v tomto prostředí provozuje jako majoritní serverový operační systém Windows server 2019 a v něm provozované doménové služby s MS Active Directory na OS MS Windows server 2012 (pro realizaci plnění podle této specifikace provede prodávající povýšení na verzi 2019 s využitím stávajících licencí kupujícího). Za účelem nasazení technologií v rámci plnění podle této specifikace umožní v rámci stávajícího hypervisoru užití přiděleného virtuálního stroje a dále užití licencí výše uvedeného serverového operačního systému. Pro implementaci služeb PKI a 802.1x bude prodávajícímu umožněn přístup do doménového prostředí kupujícího.

SIEM Qradar 7.5.

Přepínače – Ze stávajících páteřních přepínačů typu HP/HPE řad 2530, 5130, 5800, 6300, AP HP 425 řízené clusterem kontrolerů WLC MSM 760 a Centrální správy LAN a WiFi multi-vendor nástrojem IMC (Intelligent Management Center) požaduje kupující převzít a navrhnout rozšíření segmentace a konfigurace pravidel prodávajícím s návrhem lepší optimalizace a bezpečnosti provozu sítě. Za účelem plnění podle této specifikace umožní kupující prodávajícímu přístup ke konfiguraci těchto přepínačů a dále v rámci plnění bude požadovat jejich novou konfiguraci k plnění jim nově přidělených rolí v souvislosti s úpravou prostředí na základě plnění podle této specifikace.

Umístění dílčích nových přepínačů do stávajícího prostředí je dále omezeno velikostí pobočkových racků, která je pouze omezená a umožňuje osazení přepínačů pouze některých velikostí (nižší hloubka, která je promítnuta do požadavků na typová zařízení v rámci jejich specifikaci v tomto dokumentu).

Pro propojení páteřních přepínačů jsou připraveny a instalovány stávající optická vlákna typu SM a dále pro napojení přístupových přepínačů budou užita stávající optická vlákna typu SM. Stávající optická vlákna jsou vždy zakončena konektory a není vyžadováno jejich navařování.

Kupující dále provozuje monitorování síťových toků Flowmon IDP-1000-CU.

2.1. Specifikace konkrétních instalačních a implementačních požadavků

V rámci předmětu plnění kupující požaduje provedení min. následujících služeb pro následující oblasti plnění:

Obecné požadavky

• dodávka požadovaného hardware a software,
• doprava hardware do místa instalace,
• montáž dodaných zařízení do stávajících datových rozvaděčů,
• konfigurace portů pro správu a karet pro vzdálenou správu jednotlivých zařízení a jejich připojení do vyhrazené sítě pro správu,
• aktualizace firmware v jednotlivých zařízeních a jejich komponentách na nejnovější doporučené verze,
• zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zasílání e-mailové notifikace o stavu zařízení,
• kompletní ověření funkčnosti celého řešení
  ○ simulovaný výpadek jednoho z páteřních přepínačů,
  ○ odpojení jednoho z propojů mezi páteřními přepínači,
  ○ otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů,
• propojení celého řešení do stávající síťové infrastruktury a vybudování služeb pro síťovou a serverovou infrastrukturu v rámci dodávaných technologií
• ověření registrací zařízení a licencí u výrobců, aktivace licencí a služeb

Implementační služby

Next Generation Firewall s příslušenstvím
• analýza současného prostředí • návrh nové architektury, musí zahrnovat integraci se stávajícími firewally s možností jednotné správy a flexibilního využití (perimetrový/segmentační firewall, VPN koncentrátor apod.), převod role TMG do nového prostředí (a následné zrušení TMG), zachování a optimalizace role aplikačního firewallu. • migrace na nové firewally (export pravidel ze stávajících firewallů pro potřebu analýzy zajistí kupující) • optimalizace pravidel/politik včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) s využitím nových či vylepšených funkcionalit a začlenění firewallu do LAN prostředí. • související rekonfigurace stávajících zařízení

Páteřní přepínače a přístupové přepínače
• analýza stávajícího prostředí • návrh nové architektury včetně přeskupení a náhrady stávajících zařízení, bude zahrnovat i návrh segmentace LAN – tj. VLAN včetně adresace a řízení/filtrování provozu mezi nimi – předpokládaný počet VLAN jsou nižší desítky • sestavení stohů přepínačů a jejich propojení pro zajištění vysoké dostupnosti v co nejvyšším rozsahu • začlenění prvků do systému centrální správy a jeho rekonfigurace • konfigurace agregačních skupin (LACP) na přepínačích pro propojení přepínačů, připojení serverů • konfigurace VLAN, trunk portů a přístupových portů na jednotlivých přepínačích • vytvoření oddělených LAN a SAN komunikačních domén • nastavení exportu a zpracování NETFLOW/IPFIX • související rekonfigurace stávajících zařízení

Licence SW pro řízení přístupu do sítě 802.1X
• analýza současného prostředí • návrh nové architektury, způsob autentizace jednotlivých typů klientů (počítače, mobilní zařízení, periferie, OT/IOT atd.) a identitní databáze (primárně Active Directory) • implementace systému 802.1X • začlenění přepínačů a WiFi přístupových bodů do systému 802.1X • vytvoření a aplikování Connection Request Policy a Network Policy pro 802.1X • vytvoření návodů pro zařazení běžných koncových zařízení do systému 802.1X (PC, notebook, chytrý telefon/tablet) • související rekonfigurace stávajících zařízení

Licence SW aplikace pro vícefaktorové ověřování uživatelů a správu autentizačních prostředků a certifikátů, licence SW systému PKI
• analýza prostředí se zaměřením na zavedení vícefaktorové autentizace • vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority integrované s Active Directory • vybudování systému vícefaktorové autentizace s využitím kontaktních identifikačních prostředků (karet, tokenů) pro systémy Windows a terminálové služby Microsoft RDS. • Instalace klávesnic/čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění • návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (karet a doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti certifikátů • návrh a realizace zálohování • související rekonfigurace stávajících zařízení

Licence k nástroji pro správu privilegovaných účtů serverů – PIM/PAM
• analýza ICT prostředí se zaměřením na vyhledání a inventarizaci privilegovaných účtů a systémů, u nichž bude činnost privilegovaných účtů monitorována • návrh a vybudování systému pro správu a řízení privilegovaných účtů, včetně rotace hesel • související rekonfigurace stávajících technologií • Návrh a provedení akceptačních testů, musí prokázat minimálně funkčnost v obvyklých scénářích použití (přístup správce pomocí vzdálené plochy a příkazové řádky (ssh)), ukládání relací a rotaci hesel.

2.2. Požadavky na předimplementační analýzu

Dodavatel před implementací řešení zpracuje předimplementační analýzu, minimálně pro následující oblasti:

- způsob začlenění nabízeného řešení do stávajícího ICT prostředí,
- analýza požadavků na síťovou infrastrukturu,
- analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat,
- požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití,
- dopady implementace na dostupnost a funkčnost stávajících služeb,
- další podklady relevantní pro návrh řešení,
- požadovaná součinnost kupujícího,
- návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

2.3. Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

Prováděcí dokumentace musí být před zahájením implementačních prací písemně schválena kupujícím.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

- detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému,
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
- detailní návrh a popis postupu implementace předmětu plnění,
- detailní popis zajištění bezpečnosti informací,
- detailní harmonogram projektu včetně uvedení kritických milníků,
- návrh designu úložišť a virtuálních serverů a jeho konfigurace,
- návrh designu zálohování a jeho konfigurace,
- návrh designu síťového řešení a jeho konfigurace,
- návrh monitorování řešení monitorovacími nástroji,
- vazby na stávající systémy a jejich konfigurace,
- návrh akceptačních kritérií a akceptačních testů,
- detailní popis navrhovaných zaškolení administrátorů.

2.4. Požadavky na provozní dokumentaci

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy.

2.5. Požadavky na zaškolení

Dodavatel zajistí zaškolení zaměstnanců Zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to minimálně v rozsahu předávané provozní dokumentace.

- zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin,
- minimální rozsah zaškolení je 8 hodin,
- zaškolení bude probíhat v sídle kupujícího,
- předpokládá se účast 2 administrátorů,
- náklady na zaškolení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

2.6. Požadavky na provedení zkušebního provozu a akceptačních testů

Nabídne-li Dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje nižší záruční dobu, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruční doby, popř. podpory na jím požadovanou úroveň.

Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po záruční dobu, záručního servisu a podpory.

Veškeré opravy v rámci záruční doby budou provedeny bez dalších nákladů pro kupujícího.

Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení opravy do deseti pracovních dnů.

2.7. Další požadavky na záruční dobu, záruční servis a další podmínky v rámci záruky

Nabídne-li Dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje nižší záruční dobu, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruční doby, popř. podpory na jím požadovanou úroveň.

Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po záruční dobu, záručního servisu a podpory.

Veškeré opravy v rámci záruční doby budou provedeny bez dalších nákladů pro kupujícího.

Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení záruční opravy do deseti pracovních dnů.

3. Harmonogram plnění

Kupující požaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti kupní smlouvy. Čísla značí počet kalendářních dnů.

Aktivita	Termín splnění
Nabytí účinnosti smlouvy (uveřejnění v registru smluv)	D
Předimplementační analýza – zpracování	D+21
Předimplementační analýza – připomínkové řízení, schválení	D+28
Prováděcí dokumentace – zpracování	D+42
Prováděcí dokumentace – připomínkové řízení, schválení	D+49
Realizace předmětu plnění	D+100
Školení administrátorů	D+110
Zkušební provoz	D+110
Akceptace předmětu plnění	D+120 dnů