Technická specifikace předmětu plnění

Informační systém řízení přístupu

(dále jen „Technická specifikace“)

Technické požadavky plnění VZ

Obsah

Seznam tabulek

1 Projekt Informační systém řízení přístupu (ISŘP)

1.1 Cíl projektu a jeho základní charakteristika

Vybudováním informačního systému Ministerstvo vnitra (dále jen „MV ČR“ nebo „Objednatel“) sleduje primárně zajištění požadavků kybernetické bezpečnosti na ochranu přístupu do sítě a na řízení síťové bezpečnosti v souladu s legislativními požadavky. Cílem projektu je dodávka a zprovoznění informačního systému řízení přístupu do síťové infrastruktury MV ČR na základě principu řízení síťové bezpečnosti pomocí centrálně spravovaných bezpečnostních politik včetně systému jejich vynucení v infrastruktuře.

ISŘP je centralizovaným nástrojem pro ochranu integrity komunikačních sítí; obsahuje funkční komponenty pro autentizaci koncových zařízení a uživatelů a autorizaci přístupu do sítě, pro řízení přístupových oprávnění a zajišťuje auditní stopu procedur AAA v úrovni síťové infrastruktury. Jedná se o centralizovaný systém s dopadem na celou síť. Požaduje se proto architektura systému v provedení s vysokou dostupností.

Součástí projektu je obnova aktivních prvků včetně obnovy prvků hlasové sítě, segmentace síťového provozu, zavedení dynamického řízení sítě v modernizované části sítě, zavedení procesu a nástrojů pro hodnocení kvality sítě a ověření funkční architektury prvků AAA (Autentizace, Autorizace, Accounting) v testovacím rozsahu.

Součástí projektu je dále rozšíření nástroje pro centrální správu identit (IDM, AD) a vyčlenění některých služeb SIP (Sjednocené informační prostředí) pro vybrané uživatele MV ČR do samostatného prostředí. Služby Active Directory, Poštovní server (on-prem) a Prostředí pro sdílení (on-prem) pro uživatele MV ČR budou přeneseny do nového prostředí.

1.2 Projektové výstupy

1.2.1 Analýza výchozího stavu sítě

- Hodnocení kvality sítě a úrovně kybernetické bezpečnosti.

1.2.2 Modernizovaná síť

- Validace/optimalizace adresního plánu, návrh segmentace sítě MV ČR na základě vstupního hodnocení kvality sítě
- Demontáž původní technologie, dodávka, montáž a zprovoznění aktivních prvků L2, L3, WLAN, zdrojů napájení a stojanů
- Dodávka a připojení IP telefonů do sítě
- Dodávka a zprovoznění Systému pro zpracování a přístup k datům (IS)
- Dodávka a zprovoznění Serveru pro nezávislou zálohu konfigurací
- Konfigurace modernizované části sítě bude provedena v souladu s návrhem segmentace sítě a s ohledem na minimalizaci celkového provozního výpadku v lokalitě.

1.2.3 Implementované a zprovozněné komponenty ISŘP

- Dodávka, montáž a zprovoznění komponent ISŘP (centrální prvky, testovací pracoviště, lokalitní prvky, komunikační vazby na související informační infrastrukturu MV ČR)

- Zprovoznění základních síťových služeb a dynamické řízení sítě (DHCP, přidělení VLAN) v koncových lokalitách
- Řízení přístupu do sítě na základě identity zařízení a pro vynucení komunikace na úrovni aktivních prvků podle přiřazeného autorizačního profilu
- Zprovoznění funkcionalit ISŘP proběhne s ohledem na minimalizaci provozních omezení koncových zařízení, resp. pracovišť MV ČR v lokalitách.
- Poskytování technické a konzultační podpory po dobu záruky.

1.2.4 Rozšířený a integrovaný nástroj pro centrální správu identit a bezpečnostních politik

- Architektura, návrh procesů
- Konfigurace a zprovoznění konektorů (včetně testování, migrace dat, aktualizace dokumentace)
- Vytvoření organizačních rolí na základě funkce uživatele v organizaci, odboru, oddělení a systemizované pozici automaticky na základě dat z EKIS
- Poskytování technické a konzultační podpory po dobu záruky.

1.2.5 Ověření prvků AAA

- Řídicí server ISŘP a implementace vybraných funkcionalit AAA na testovacím pracovišti (řešení na bázi RADIUS serveru, připravenost systému pro další průběžné rozšiřování provozními kapacitami Objednatele (beneficienta) s využitím mechanismů dle standardu 802.1x)
- Zpracování Technické zprávy *Ověření prvků AAA s využitím metod dle 802.1x*

1.2.6 Vyčlenění části služeb SIP

- Služby Active Directory domén *mvcr.cz, resortmv.cz, exresortmv.cz* budou replikovány do prostředí UPAAS
- Dodávka, instalace a zprovoznění Poštovního serveru (on-prem) v prostředí UPAAS
- Dodávka, instalace a zprovoznění Prostředí pro sdílení (on-prem) pro vybrané uživatele MV ČR v prostředí UPAAS
- Součástí vyčlenění části služeb SIP je migrace dat z původního do nového prostředí

1.2.7 Technické návrhy, zprávy, dokumentace

- Prováděcí projekty č.1 a č.2 (viz dále v kap. 8.1.1 Technické specifikace)
- Návrh segmentace sítě a optimalizace adresního plánu MV ČR (*Adresní plán a segmentace sítě)* (viz dále v kap. 3.1 Technické specifikace)
- Hodnocení rizik ISŘP (viz dále v kap. 2.1 Technické specifikace)
- Vstupní hodnocení kvality sítě (viz dále v kap. 2.2 Technické specifikace)
- Technická zpráva *Ověření prvků AAA s využitím metod dle 802.1x* (viz dále v kap. 6 Technické specifikace)
- Dokumentace skutečného provedení (viz dále v kap. 8.1.2 Technické specifikace)

- Technická dokumentace k aplikacím pořizovaným dle kapitol 7.1, 7.2, 7.3 Technické specifikace, a to včetně
    - Dokumentace postupů pro nasazení a konfiguraci
    - Dokumentace postupů pro přidání nodů a konfiguraci replikace
- Dokumentace migračních postupů a plánů obnovy Poštovního systému (viz dále v kap. 7.2 Technické specifikace)
- Dokumentace postupů pro nasazení a konfiguraci prostřední pro sdílení (viz dále v kap. 7.3 Technické specifikace)

1.3 Architekturní informace

Přehled architektury ISŘP je obsahem Přílohy č.1 Technické specifikace ve standardizovaném formátu a po částech je uveden v dalších podkapitolách.

1.3.1 Architekturní rámec

Projekt ISŘP vychází z existujícího stavu technologií zavedených v prostředí MV ČR a architekturního rámce dosaženého v projektech Modernizace komunikační infrastruktury (MKI), Informační systém interní komunikace (ISIK) a Sjednocené informační prostředí (SIP):

- MKI, ISIK:
    - zaveden technologický standard pro LAN a WLAN (viz *Záměr standardizace a rozvoje datových uzlů komunikační infrastruktury Ministerstva vnitra a Policie České republiky* z 31. května 2024, viz Příloha č. 2 této Technické specifikace),
    - zaveden a provozován systém pro poskytování základních síťových služeb (platforma ADDNET),
    - rozšířen systém IP telefonie Cisco Systems včetně integrace s administračním systémem SAS-PBX fy OpSoft a systémem pro tarifikaci Calom.
- SIP:
    - zavedeny technologie a systémy Microsoft Active Directory, poštovní server MV ČR, prostředí pro sdílení dat mezi organizacemi rezortu MV ČR, dbase SQL pro ukládání dat rezortu MV ČR, SCOM pro dohled nad provozovanými řešeními, Identity management složený z portálu EasyIDM a synchronizační služby Microsoft Identity Manager Synchronization Service a dalších.

Projekt ISŘP dále posouvá a rozvíjí dosažený architekturní rámec o:

- Zavedení prostředků pro správu adresního prostoru (IPAM) a segmentace sítě
- Dynamické řízení sítě: přidělování VLAN pomocí mechanismů NAC podle centrálně spravovaných pravidel a dynamické přidělování IP adres
- Propojení informačních zdrojů (EKIS-IDM-AD-ISŘP-LAN) za účelem dosažení centralizace a vyšší míry automatizace při správě sítě na základě identity uživatele, jeho umístění a role v organizaci
- Návrh/ověření procedur AAA (zavedení doménových certifikátů, využití principů AAA na bázi standardu 802.1x jádrovou komponentou (serverem) ISŘP)

- Replikace služeb AD (pro domény *mvcr.cz, resortmv.cz, exresortmv.cz*), Poštovního serveru a Prostředí pro sdílení do nového prostředí se současnou migrací těchto služeb a dat na výrobcem aktuálně poskytované verze těchto produktů.

V rámci projektu ISŘP je nutno splňovat technické a provozní podmínky a kompatibilitu se stávajícím technologickým prostředím:

- Zachování datového připojení objektů prostředky ITS MV ČR a využití stávajících komunikačních spojů, které odpovídají doporučeným parametrům uvedeným v dokumentu *Záměr standardizace a rozvoje datových uzlů komunikační infrastruktury Ministerstva vnitra a Policie České republiky* z 31. května 2024, viz Příloha č. 2 této Technické specifikace)
- Připravenost na zavádění IPv6 v souladu s Usnesením vlády ČR č.727 ze dne 8.6.2009 ke Zprávě o přechodu na internetový protokol verze 6
- Začlenění nového informačního systému do stávající rezortní sítě, jak bude specifikováno v dalších kapitolách Technické specifikace
- Zachování a využití strukturované datové rozvodné sítě v objektu o potřebném počtu portů (dle aktuálního provozního stavu)
- Využití stávajících technologických místností pro umístění stojanových skříní pro montáž technologií
- Využití stávajících aktivních prvků v modernizovaných lokalitách, které jsou Objednatelem řádně provozovány a splňují technické podmínky modernizované sítě, takže nevyžadují náhradu novým prvkem. V rámci implementace budou začleněny do celkového řešení ISŘP, konkrétně přístup připojených koncových zařízení bude řízen prostředky ISŘP.

  Zapojení stávajících aktivních prvků v modernizovaných lokalitách bude provedeno mimo rámec projektu ISŘP, tj. nebude požadováno po Dodavateli.

  Seznam předmětných aktivních prvků je uveden v následující tabulce:

Tabulka 1: Seznam aktivních prvků v provozním režimu

Výrobce	Typové označení	Počet
Cisco Systems	C8300-2N2S-4T2X	1
Cisco Systems	C8300-1N1S-6T	1
Cisco Systems	C8200-1N-4T	7
Cisco Systems	C9200-48P	6
Cisco Systems	C9200-24P-A	20

- Požaduje se začlenění pořizovaných přístupových bodů sítě WLAN do stávající sítě WLAN Objednatele, tj. připojení pořizovaných přístupových bodů ke stávajícím kontrolérům, které jsou Objednatelem řádně provozovány a splňují technické podmínky modernizované sítě. Jedná se o kontroléry výrobce Cisco Systems, typové označení C9120AXI-E.

  Veškeré práce a činnosti na WLAN kontrolérech, které jsou v provozním režimu, budou prováděny pracovníky Objednatele (nebo pracovníky jím pověřené organizace) v rámci nezbytné součinnosti a nebudou požadovány po Dodavateli.

- Pracoviště centrálního dohledu zajišťuje nepřetržitý dohled nad funkčností a fyzickým přístupem k ICT technologiím MV ČR umístěným ve stojanech vybavených zabezpečovacím systémem RAMOS připojeným k nadřazené dohledové aplikaci Zabbix (protokol SNMPv3) a CONTEG Pro Server (CPS, softwarová aplikace pro centrální správu, dohled monitorovaného prostředí a přístupu s využitím hardwaru RAMOS, viz https://www.conteg.cz/conteg-pro-server-management-software-cz).

  Způsob zajištění kompatibility se stávajícím prostředím je specifikován v kap. 3.4.2 Technické specifikace (STd) a 3.6 Technické specifikace (DUPS).

  Veškeré práce a činnosti na stávajícím systému DUPS, který je v provozním režimu, budou prováděny pracovníky Objednatele (nebo pracovníky jím pověřené organizace) v rámci nezbytné součinnosti a nebudou požadovány po Dodavateli.

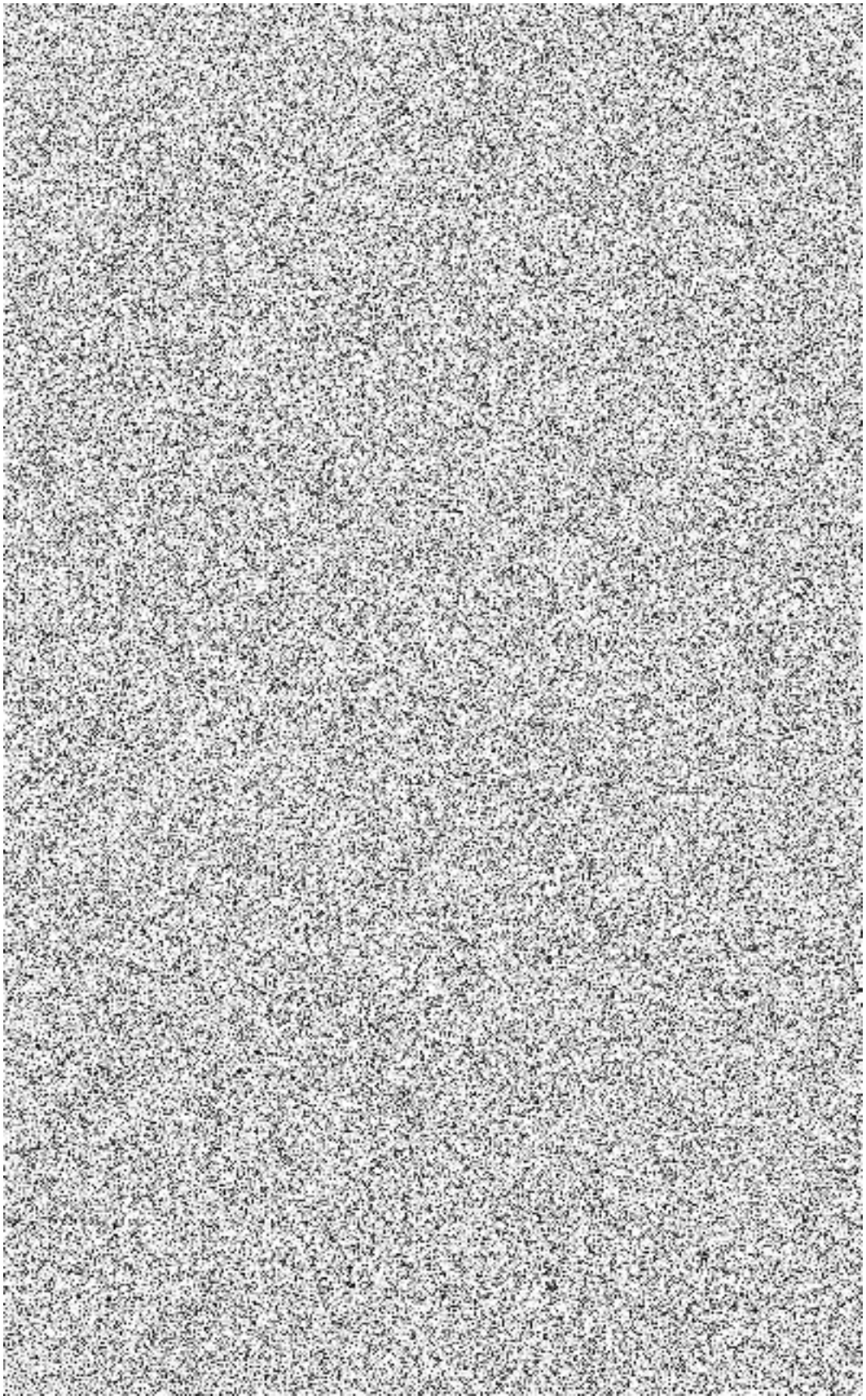
1.3.2 Aplikační architektura

Aplikační architektura sestává z 4 funkčních celků:

1. aplikační komponenta Poštovní server (on-prem) a jeho součásti,
2. aplikační komponenta Prostředí pro sdílení (on-prem) a jeho součástí,
3. IDM s vazbou na IS EKIS a Active Directory. EKIS je zdrojem dat pro IDM, IDM je zdrojem dat pro Active Directory,
4. aplikační komponenta Systém pro zpracování a přístup k datům (zpracování dat provozovaného tarifikačního systému CALOM a další funkcionality specifikované v 3.3.4).

Externí aplikační komponenty připojené k ISŘP (LogManager, systém dohledu sítě, prostředí DCeGOV), jejichž implementace není předmětem projektu, jsou uvedeny v diagramu technické architektury kvůli přehlednosti.

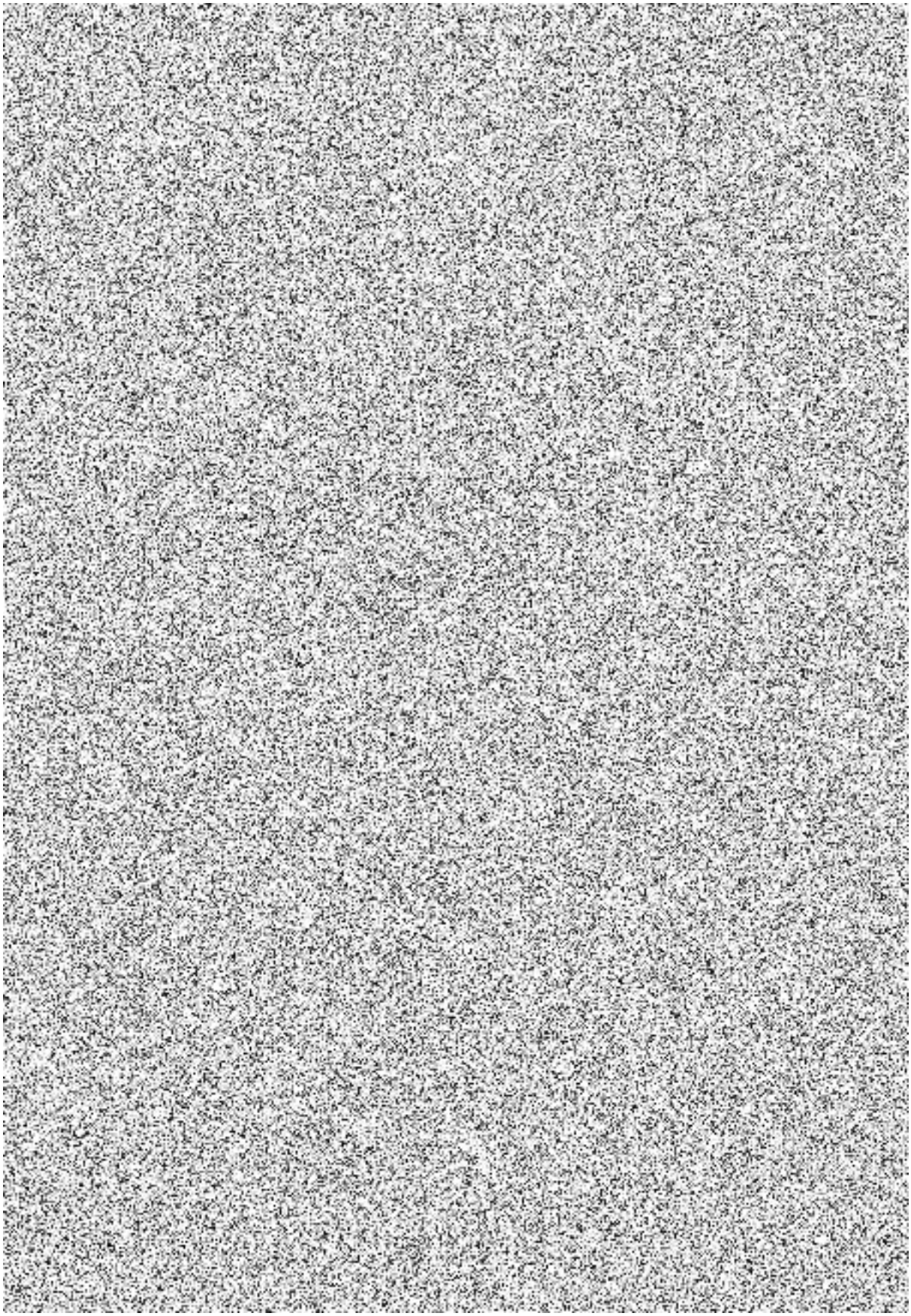
Diagram 1: Aplikační architektura



1.3.3 Technologická architektura

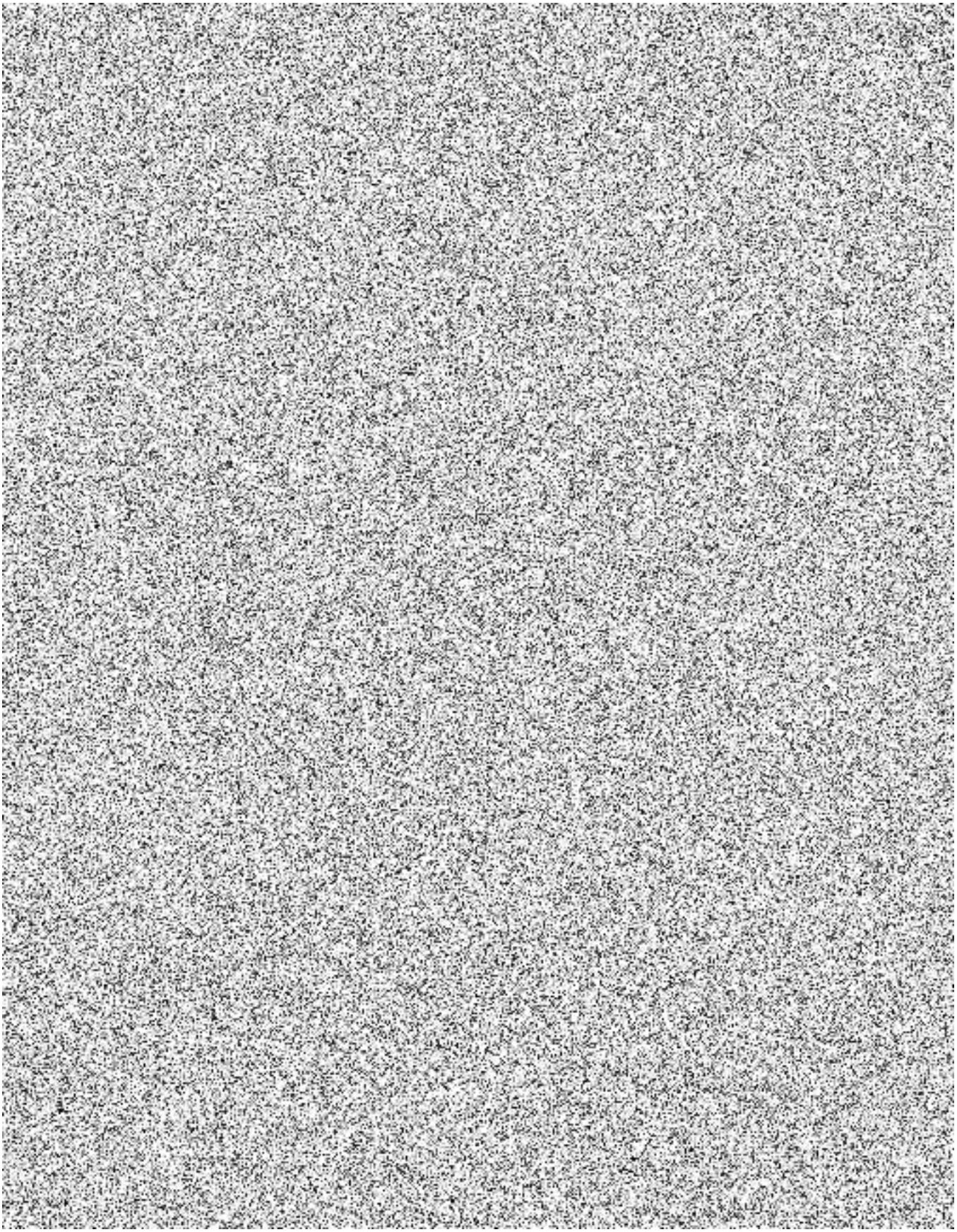
1. Aplikační komponenty Poštovní server, Prostředí pro sdílení a systémy IDM, AD budou provozovány v prostředí UPAAS, tedy ve stávajících datových centrech.
2. Centrální systémy ISŘP budou provozovány v prostředí UPAAS.
3. Lokální komponenty ISŘP (workservery) budou provozovány v lokalitách.
4. V rámci ISŘP identifikujeme funkcionality, resp. odpovídající infrastrukturní služby:
    - DHCP server, resp. DHCP,
    - Autentizační server připojený protokolem Radius k Autentizátoru (funkcionalita přepínače) realizují NAC (Network Access Control),
    - IPAM (IP Address Management: správa IP adresního prostoru),
    - Alarm/Log management, resp. služba Alert Centrum.
5. Analyzátor IP sítě zajišťuje vstupy pro službu Hodnocení kvality sítě.
6. V diagramu technické architektury nejsou uvedena specifická řešení komunikační sítě v lokalitách

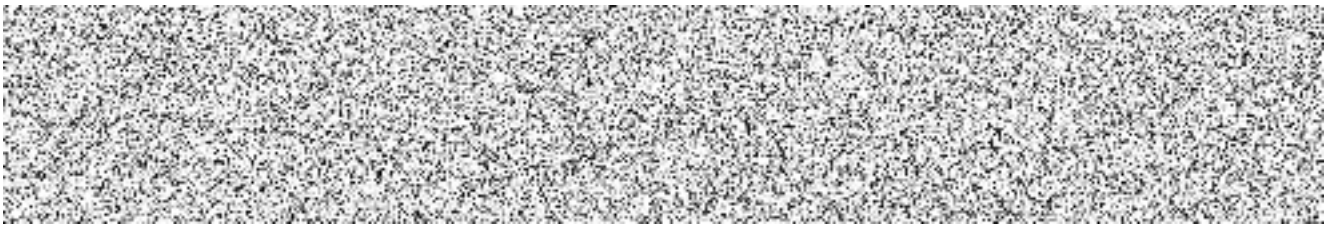
Diagram 2: Technická architektura



1.3.4 Místa plnění

Místy plnění jsou objekty Objednatele („Lokality“) dle tabulky níže.





1.4 Popis a požadované osazení komponent infrastruktury

Seznam a množství požadovaných komponent ***Díla*** je uvedeno v tabulce č. 3. Detailní rozmístění komponent v lokalitách je potom uvedeno v Příloze č.3 Závazného návrhu smlouvy *Rozpad ceny plnění* (soubor: *ISŘP_Př. 3 Smlouvy_Rozpad ceny plnění.xlsx* ve formátu MS Excel, list *Dílo-osazení*).

Tabulka 3: Seznam a množství požadovaných komponent Díla

Položka / Lokalita	Popis položky	Kapitola Technické specifikace	Technické návrhy, zprávy, dokumentace	Školení	Podpora po dobu záruky	UPAAS primární - fáze A	UPAAS primární - fáze B	UPAAS sekundární - fáze A	UPAAS sekundární - fáze B	Koncové lokality celkem
Projektový výstup: Analýza výchozího stavu sítě										
DHS	TZ, Příloha DPP1 Vstupní hodnocení kvality sítě	2.1	1	-	-	-	-	-	-	**0**
DHR	TZ, Příloha DPP1 Hodnocení rizik ISŘP	2.2	1	-	-	-	-	-	-	**0**
Projektový výstup: Modernizovaná síť										
DAPSS	TZ, Příloha DPP1 Adresní plán a segmentace sítě	3.1	1	-	-	-	-	-	-	**0**
S2C	Přístupový přepínač 12 portů po koncové objekty typu 1,2 kompaktní	3.2.1	-	-	-	-	-	-	-	**3**
S2	Přístupový přepínač 24 portů po koncové objekty typu 1, 2	3.2.2	-	-	-	-	-	-	-	**43**
S2sfp1	Příslušenství S2: 1000BASE-T SFP transceiver modul Cat 5 Cu	3.2.2	-	-	-	-	-	-	-	**81**
S2sfp2	Příslušenství S2: 1000BASE-LX/LH SFP transceiver modul, MMF/SMF, 1310nm, DOM	3.2.2	-	-	-	-	-	-	-	**36**

S2sfp3	Příslušenství S2: 1000BASDE-SX SFP transceiver MMF, 850nm, DOM	3.2.2	-	-	-	-	-	-	-	**18**
S3	Přístupový přepínač 48 portů pro uzlové objekty 1, 2	3.2.3	-	-	-	-	-	-	-	**34**
S3sfp	Příslušenství přepínače S3: 8x10GE síťový modul	3.2.3	-	-	-	-	-	-	-	**16**
S3D	Přístupový přepínač 48 portů pro síť dohledu	3.2.4	-	-	-	-	-	-	-	**2**
S3AP	Přístupový přepínač 48 portů pro připojení AP	3.2.5	-	-	-	-	-	-	-	**8**
S5	Agregační přepínač pro uzlový objekt typu 1	3.2.6	-	-	-	-	-	-	-	**4**
S5sfp	Příslušenství přepínače S5: 10GBASE-LRM SFP modul	3.2.6	-	-	-	-	-	-	-	**44**
S8D	Přístupový přepínač 8 portů pro síť dohledu	3.2.7	-	-	-	-	-	-	-	**33**
R0	Páteřní směrovač R0	3.2.8	-	-	-	-	-	-	-	**2**
R4	Směrovač R4	3.2.9	-	-	-	-	-	-	-	**22**
R4nim	Příslušenství R4: NIM (GbE přepínač 4 porty)	3.2.9	-	-	-	-	-	-	-	**22**
R4sfp1	Příslušenství R4: 1000BASE-T SFP transceiver modul Cat 5 Cu	3.2.9	-	-	-	-	-	-	-	**34**
R4sfp2	Příslušenství R4: 1000BASE-LX/LH SFP transceiver modul, MMF/SMF, 1310nm, DOM	3.2.9	-	-	-	-	-	-	-	**16**
R4sfp3	Příslušenství R4: 1000BASDE-SX SFP transceiver MMF, 850nm, DOM	3.2.9	-	-	-	-	-	-	-	**12**
WAP	Přístupový bod bezdrátové sítě WA	3.2.10	-	-	-	-	-	-	-	**65**
DATAd	Dohled aktivních prvků	3.2.11	-	-	-	1	-	1	-	**114**
IMlclc3	Instalační materiál: optický patchcord MM (LC-LC, 3m)	3.2.13	-	-	-	-	-	-	-	**21**
IMcat5e1	Instalační materiál: patchcord 1m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**83**
IMcat5e2	Instalační materiál: patchcord 2m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**100**

IMcat5e5	Instalační materiál: patchcord 5m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**15**
IMcat5e7	Instalační materiál: patchcord 7m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**10**
IMe2apc3	Instalační materiál: optický patch cord SM, 3m (optický patchcord SM, E2/APC - LC/PC,duplex, 3m)	3.2.13	-	-	-	-	-	-	-	**55**
IMkb	Instalační materiál: Kabel C13-C14 (prodlužovací kabel, 3m)	3.2.13	-	-	-	-	-	-	-	**47**
IMpdu	Instalační materiál: Napájecí jednotka 8x230V (19" montáž, IEC320 C14)	3.2.13	-	-	-	-	-	-	-	**46**
IMlcsc3	Instalační materiál: optický patch cord MM (LC-SC PC min. OM2 – délka 3 m)	3.2.13	-	-	-	-	-	-	-	**2**
SZ	Server pro nezávislou zálohu konfigurací	3.3	-	-	-	1	-	0	-	**0**
A3	Telefon typu A3 – přístroj pro standardní uživatele	3.4.1	-	-	-	-	-	-	-	**466**
B	Telefon typu B – přístroj pro střední management včetně SW licencí	3.4.1	-	-	-	-	-	-	-	**0**
C	Telefon typu C – přístroj pro sekretariát	3.4.1	-	-	-	-	-	-	-	**23**
D	Telefon typu D – přístroj pro management	3.4.1	-	-	-	-	-	-	-	**36**
AB24	Analogová brána s min. 24 porty typu FXS včetně SW licencí včetně SW licencí	3.4.1	-	-	-	-	-	-	-	**1**
IS	Systém pro zpracování a přístup k datům	3.4.1	-	-	-	1	-	0	-	**0**
ST 600-600-19U	Technologický stojan 19“ 600-600-19U	3.5.1	-	-	-	-	-	-	-	**1**
STd	Monitoring stojanu (teplota, vlhkost, otevření dveří)	3.5.2	-	-	-	-	-	-	-	**86**
UPS180	Záložní zdroj napájení 180kW - objektová UPS	3.6.1	-	-	-	-	-	-	-	**1**
UPS1,5r	Záložní zdroj napájení 1,5 kW – stojanová UPS	3.6.2	-	-	-	-	-	-	-	**8**
UPS1,5t	Záložní zdroj napájení 1,5 kW – samostatně stojící UPS	3.6.2	-	-	-	-	-	-	-	**2**
UPS3r	Záložní zdroj napájení 3 kW – stojanová UPS	3.6.2	-	-	-	-	-	-	-	**12**

UPS3t	Záložní zdroj napájení 3 kW – samostatně stojící UPS	3.6.2	-	-	-	-	-	-	-	**6**
DUPS	Dohled UPS a monitoringu stojanů	3.7	-	-	-	1	-	0	-	**0**
Projektový výstup: Implementované a zprovozněné komponenty ISŘP										
CIPAM	Systém pro správu a řízení základních síťových služeb	4.1	-	-	-	1	-	1	-	**34**
CS	Centrální server/servery systému pro správu a řízení základních síťových služeb a pro řízení přístupu	4.1	-	-	-	1	-	1	-	**0**
WS	Lokalitní server systému pro správu a řízení základních síťových služeb a pro řízení přístupu	4.1	-	-	-	-	-	-	-	**35**
WSv	Virtualizované záložní instance WS v DC	4.1	-	-	-	1	-	1	-	**0**
NAC	Systém pro řízení přístupu	4.2	-	-	-	-	1	-	1	**34**
ISŘPd	Dohled ISŘP	4.3	-	-	-	-	1	-	1	**0**
ISŘPsupp	ISŘP: Součinnost po dobu záruky [člověkodny]	4.4	-	-	100	-	-	-	-	**0**
Projektový výstup: Rozšířený a integrovaný nástroj pro centrální správu identit a bezpečnostních politik										
DIAM	Příloha PP2 Analýza a návrh rozšíření a integrace nástroje pro centrální správu identit a bezpečnostních politik	5.1	1	-	-	-	-	-	-	**0**
CON	Konfigurace a zprovoznění konektorů	5.2	-	-	-	-	1	-	-	**0**
MO	Licence pro automatickou tvorbu matice oprávnění modulu EasyIDM	5.3	-	-	-	-	1	-	-	**0**
IAMsupp	IAM: Součinnost po dobu záruky [člověkodny]	5.4	-	-	120	-	-	-	-	**0**
Projektový výstup: Ověření prvků AAA										
DAAA	TZ Ověření prvků AAA s využitím metod dle 802.1x	6	1	-	-	-	-	-	-	**0**
Projektový výstup: Vyčlenění části služeb SIP										
AD	Active Directory	7.1	-	-	-	-	1	-	1	**0**
MAIL	Poštovní server	7.2	-	-	-	-	1	-	1	**0**
MAILsupp	MAIL: Součinnost po dobu záruky [člověkodny]	7.2.5	-	-	180	-	-	-	-	**0**
PS	Prostředí pro sdílení	7.3	-	-	-	-	1	-	1	**0**
Projektový výstup: Technické návrhy, zprávy, dokumentace										

DAD	Technická dokumentace k novému prostředí AD	7.1.4	1	-	-	-	-	-	-	**0**
DADP	Dokumentace postupů pro přidání nodů a konfiguraci replikace	7.1.4	1	-	-	-	-	-	-	**0**
DMAIL	Technická dokumentace k novému prostředí Poštovního serveru	7.2.4	1	-	-	-	-	-	-	**0**
DMAILP	Dokumentace migračních postupů a plánů obnovy Poštovního serveru	7.2.4	1	-	-	-	-	-	-	**0**
DPS	Technická dokumentace k novému Prostředí pro sdílení	7.3.4	1	-	-	-	-	-	-	**0**
DPSP	Dokumentace postupů pro nasazení a konfiguraci Prostředí pro sdílení	7.3.4	1	-	-	-	-	-	-	**0**
DPP1	Prováděcí projekt č.1	8.1.1	1	-	-	-	-	-	-	**0**
DPP2	Prováděcí projekt č.2	8.1.1	1	-	-	-	-	-	-	**0**
DSP	Dokumentace skutečného provedení	8.1.2	1	-	-	-	-	-	-	**0**
Školení										
ŠLAN	Školení pro specialisty provozu LAN	9	-	1	-	-	-	-	-	**0**
ŠIPT	Školení pro koncové uživatele telefonních systémů	9	-	1	-	-	-	-	-	**0**
ŠISŘP	Školení pro specialisty platformy ISŘP	9	-	1	-	-	-	-	-	**0**
ŠKZ	Školení pro specialisty správy koncových zařízení	9	-	1	-	-	-	-	-	**0**
ŠIAM	Školení administrátorů systému IAM MVČR	5.3 9	-	1	-	-	-	-	-	**0**
ŠAD	Školení administrátorů systému AD MVČR	7.1.4 9	-	1	-	-	-	-	-	**0**
ŠMAIL	Školení administrátorů Poštovního serveru	7.2.4 9	-	1	-	-	-	-	-	**0**
ŠPS	Školení administrátorů Prostředí pro sdílení	7.3.4 9	-	1	-	-	-	-	-	**0**

Seznam a množství požadovaných komponent ***Pozáručního plnění*** je uvedeno v tabulce č. 4. Detailní rozmístění komponent v lokalitách je potom uvedeno v Příloze č.3 Závazného návrhu smlouvy *Rozpad ceny plnění* (soubor: *ISŘP_Př. 3 Smlouvy_Rozpad ceny plnění.xlsx*, list *Pozáruční-osazení*).

Tabulka 4: Seznam a množství požadovaných komponent Pozáručního plnění

Položka / Lokalita	Popis položky	Kapitola Technické specifikace	Technické návrhy, zprávy, dokumentace	Školení	Podpora po dobu záruky	UPAAS primární - fáze A	UPAAS primární - fáze B	UPAAS sekundární - fáze A	UPAAS sekundární - fáze B	Koncové lokality celkem
Projektový výstup: Analýza výchozího stavu sítě										
DHS	TZ, Příloha DPP1 Vstupní hodnocení kvality sítě	2.1	-	-	-	-	-	-	-	**0**
DHR	TZ, Příloha DPP1 Hodnocení rizik ISŘP	2.2	-	-	-	-	-	-	-	**0**
Projektový výstup: Modernizovaná síť										
DAPSS	TZ, Příloha DPP1 Adresní plán a segmentace sítě	3.1	-	-	-	-	-	-	-	**0**
S2C	Přístupový přepínač 12 portů po koncové objekty typu 1,2 kompaktní	3.2.1	-	-	-	-	-	-	-	**3**
S2	Přístupový přepínač 24 portů po koncové objekty typu 1, 2	3.2.2	-	-	-	-	-	-	-	**43**
S2sfp1	Příslušenství S2: 1000BASE-T SFP transceiver modul Cat 5 Cu	3.2.2	-	-	-	-	-	-	-	**0**
S2sfp2	Příslušenství S2: 1000BASE-LX/LH SFP transceiver modul, MMF/SMF, 1310nm, DOM	3.2.2	-	-	-	-	-	-	-	**0**
S2sfp3	Příslušenství S2: 1000BASDE-SX SFP transceiver MMF, 850nm, DOM	3.2.2	-	-	-	-	-	-	-	**0**
S3	Přístupový přepínač 48 portů pro uzlové objekty 1, 2	3.2.3	-	-	-	-	-	-	-	**34**
S3sfp	Příslušenství přepínače S3: 8x10GE síťový modul	3.2.3	-	-	-	-	-	-	-	**0**
S3D	Přístupový přepínač 48 portů pro síť dohledu	3.2.4	-	-	-	-	-	-	-	**2**
S3AP	Přístupový přepínač 48 portů pro připojení AP	3.2.5	-	-	-	-	-	-	-	**8**

S5	Agregační přepínač pro uzlový objekt typu 1	3.2.6	-	-	-	-	-	-	-	**4**
S5sfp	Příslušenství přepínače S5: 10GBASE-LRM SFP modul	3.2.6	-	-	-	-	-	-	-	**0**
S8D	Přístupový přepínač 8 portů pro síť dohledu	3.2.7	-	-	-	-	-	-	-	**33**
R0	Páteřní směrovač R0	3.2.8	-	-	-	-	-	-	-	**2**
R4	Směrovač R4	3.2.9	-	-	-	-	-	-	-	**22**
R4nim	Příslušenství R4: NIM (GbE přepínač 4 porty)	3.2.9	-	-	-	-	-	-	-	**0**
R4sfp1	Příslušenství R4: 1000BASE-T SFP transceiver modul Cat 5 Cu	3.2.9	-	-	-	-	-	-	-	**0**
R4sfp2	Příslušenství R4: 1000BASE-LX/LH SFP transceiver modul, MMF/SMF, 1310nm, DOM	3.2.9	-	-	-	-	-	-	-	**0**
R4sfp3	Příslušenství R4: 1000BASDE-SX SFP transceiver MMF, 850nm, DOM	3.2.9	-	-	-	-	-	-	-	**0**
WAP	Přístupový bod bezdrátové sítě WA	3.2.10	-	-	-	-	-	-	-	**65**
DATAd	Dohled aktivních prvků	3.2.11	-	-	-	1	-	1	-	**114**
IMlclc3	Instalační materiál: optický patchcord MM (LC-LC, 3m)	3.2.13	-	-	-	-	-	-	-	**0**
IMcat5e1	Instalační materiál: patchcord 1m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**0**
IMcat5e2	Instalační materiál: patchcord 2m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**0**
IMcat5e5	Instalační materiál: patchcord 5m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**0**
IMcat5e7	Instalační materiál: patchcord 7m (síťový kabel Cat-5e, zakončení 2x RJ-45 konektor, přímé propojení)	3.2.13	-	-	-	-	-	-	-	**0**

IMe2apc3	Instalační materiál: optický patch cord SM, 3m (optický patchcord SM, E2/APC - LC/PC,duplex, 3m)	3.2.13	-	-	-	-	-	-	-	**0**
IMkb	Instalační materiál: Kabel C13-C14 (prodlužovací kabel, 3m)	3.2.13	-	-	-	-	-	-	-	**0**
IMpdu	Instalační materiál: Napájecí jednotka 8x230V (19" montáž, IEC320 C14)	3.2.13	-	-	-	-	-	-	-	**0**
IMlcsc3	Instalační materiál: optický patch cord MM (LC-SC PC min. OM2 – délka 3 m)	3.2.13	-	-	-	-	-	-	-	**0**
SZ	Server pro nezávislou zálohu konfigurací	3.3	-	-	-	1	-	0	-	**0**
A3	Telefon typu A3 – přístroj pro standardní uživatele	3.4.1	-	-	-	-	-	-	-	**466**
B	Telefon typu B – přístroj pro střední management včetně SW licencí	3.4.1	-	-	-	-	-	-	-	**0**
C	Telefon typu C – přístroj pro sekretariát	3.4.1	-	-	-	-	-	-	-	**23**
D	Telefon typu D – přístroj pro management	3.4.1	-	-	-	-	-	-	-	**36**
AB24	Analogová brána s min. 24 porty typu FXS včetně SW licencí včetně SW licencí	3.4.1	-	-	-	-	-	-	-	**1**
IS	Systém pro zpracování a přístup k datům	3.4.1	-	-	-	1	-	0	-	**0**
ST 600-600-19U	Technologický stojan 19“ 600-600-19U	3.5.1	-	-	-	-	-	-	-	**0**
STd	Monitoring stojanu (teplota, vlhkost, otevření dveří)	3.5.2	-	-	-	-	-	-	-	**0**
UPS180	Záložní zdroj napájení 180kW - objektová UPS	3.6.1	-	-	-	-	-	-	-	**0**
UPS1,5r	Záložní zdroj napájení 1,5 kW – stojanová UPS	3.6.2	-	-	-	-	-	-	-	**0**
UPS1,5t	Záložní zdroj napájení 1,5 kW – samostatně stojící UPS	3.6.2	-	-	-	-	-	-	-	**0**
UPS3r	Záložní zdroj napájení 3 kW – stojanová UPS	3.6.2	-	-	-	-	-	-	-	**0**
UPS3t	Záložní zdroj napájení 3 kW – samostatně stojící UPS	3.6.2	-	-	-	-	-	-	-	**0**

DUPS	Dohled UPS a monitoringu stojanů	3.7	-	-	-	-	-	-	-	**0**
Projektový výstup: Implementované a zprovozněné komponenty ISŘP										
CIPAM	Systém pro správu a řízení základních síťových služeb	4.1	-	-	-	1	-	1	-	**0**
CS	Centrální server/servery systému pro správu a řízení základních síťových služeb a pro řízení přístupu	4.1	-	-	-	1	-	1	-	**0**
WS	Lokalitní server systému pro správu a řízení základních síťových služeb a pro řízení přístupu	4.1	-	-	-	-	-	-	-	**35**
WSv	Virtualizované záložní instance WS v DC	4.1	-	-	-	1	-	1	-	**0**
NAC	Systém pro řízení přístupu	4.2	-	-	-	-	1	-	1	**0**
ISŘPd	Dohled ISŘP	4.3	-	-	-	-	1	-	1	**0**
ISŘPsupp	ISŘP: Součinnost po dobu záruky [člověkodny]	4.4	-	-	-	-	-	-	-	**0**
Projektový výstup: Rozšířený a integrovaný nástroj pro centrální správu identit a bezpečnostních politik										
DIAM	Příloha PP2 Analýza a návrh rozšíření a integrace nástroje pro centrální správu identit a bezpečnostních politik	5.1	-	-	-	-	-	-	-	**0**
CON	Konfigurace a zprovoznění konektorů	5.2	-	-	-	-	-	-	-	**0**
MO	Licence pro automatickou tvorbu matice oprávnění modulu EasyIDM	5.3	-	-	-	-	-	-	-	**0**
IAMsupp	IAM: Součinnost po dobu záruky [člověkodny]	5.4	-	-	-	-	-	-	-	**0**
Projektový výstup: Ověření prvků AAA										
DAAA	TZ Ověření prvků AAA s využitím metod dle 802.1x	6	-	-	-	-	-	-	-	**0**
Projektový výstup: Vyčlenění části služeb SIP										
AD	Active Directory	7.1	-	-	-	-	1	-	1	**0**
MAIL	Poštovní server	7.2	-	-	-	-	1	-	1	**0**
MAILsupp	MAIL: Součinnost po dobu záruky [člověkodny]	7.2.5	-	-	-	-	-	-	-	**0**

PS	Prostředí pro sdílení	7.3	-	-	-	-	-	-	-	**0**
Projektový výstup: Technické návrhy, zprávy, dokumentace										
DAD	Technická dokumentace k novému prostředí AD	7.1.4	-	-	-	-	-	-	-	**0**
DADP	Dokumentace postupů pro přidání nodů a konfiguraci replikace	7.1.4	-	-	-	-	-	-	-	**0**
DMAIL	Technická dokumentace k novému prostředí Poštovního serveru	7.2.4	-	-	-	-	-	-	-	**0**
DMAILP	Dokumentace migračních postupů a plánů obnovy Poštovního serveru	7.2.4	-	-	-	-	-	-	-	**0**
DPS	Technická dokumentace k novému Prostředí pro sdílení	7.3.4	-	-	-	-	-	-	-	**0**
DPSP	Dokumentace postupů pro nasazení a konfiguraci Prostředí pro sdílení	7.3.4	-	-	-	-	-	-	-	**0**
DPP1	Prováděcí projekt č.1	8.1.1	-	-	-	-	-	-	-	**0**
DPP2	Prováděcí projekt č.2	8.1.1	-	-	-	-	-	-	-	**0**
DSP	Dokumentace skutečného provedení	8.1.2	-	-	-	-	-	-	-	**0**
Školení										
ŠLAN	Školení pro specialisty provozu LAN	9	-	-	-	-	-	-	-	**0**
ŠIPT	Školení pro koncové uživatele telefonních systémů	9	-	-	-	-	-	-	-	**0**
ŠISŘP	Školení pro specialisty platformy ISŘP	9	-	-	-	-	-	-	-	**0**
ŠKZ	Školení pro specialisty správy koncových zařízení	9	-	-	-	-	-	-	-	**0**
ŠIAM	Školení administrátorů systému IAM MVČR	5.3 9	-	-	-	-	-	-	-	**0**
ŠAD	Školení administrátorů systému AD MVČR	7.1.4 9	-	-	-	-	-	-	-	**0**
ŠMAIL	Školení administrátorů Poštovního serveru	7.2.4 9	-	-	-	-	-	-	-	**0**

ŠPS	Školení administrátorů Prostředí pro sdílení	7.3.4 9	-	-	-	-	-	-	-	**0**

2 Analýza výchozího stavu sítě

2.1 Hodnocení kvality sítě

Primárním cílem vstupního hodnocení kvality sítě je zdokumentovat počáteční stav a posoudit nastavení sítě (síťové prvky, konfigurace, topologie, bezpečnostní politiky) a získat současně technická data pro hodnocení rizik a realizaci následných technických návrhů, tj. pro optimalizaci adresního prostoru a návrh segmentace sítě MVČR. Zhotovení dokumentace a posouzení nastavení sítě bude provedeno minimálně v rozsahu dle specifikace v tabulce níže a bude zpracováno formou Technické zprávy *Vstupní hodnocení kvality sítě*, která bude tvořit nedílnou součást (přílohu) Prováděcího projektu č.1.

Tabulka 5: Hodnocení kvality sítě

Požadavek	Způsob splnění požadavku	Doplní Dodavatel dle nabízeného zařízení
Scan sítě. Automatizovaný neinvazivní scan sítě provedený prostředky Dodavatele. Objednatel: • zajistí přístup k aktivním prvkům za podmínky, že nebude omezena nebo ohrožena provozuschopnost infrastruktury a nebude narušena bezpečnost informací, služeb a integrita komunikačních sítí; • poskytne v případě požadavku na instalaci analytických přístrojů Dodavatele virtualizovanou výpočetní infrastrukturu v rámci DC MV ČR podle specifikace Dodavatele. Výstupem scanu jsou výchozí data pro další analýzy, technické zprávy a dokumentační výstupy.	ANO	Ano, produktem IP Fabric, využitím virtualizovnaé výpočetní infrastruktury DC MV ČS
Seznam síťových zařízení. Detekce síťových zařízení a jejich základních parametrů.	ANO	ANO
Konfigurace sítě. Přehled síťové topologie a konfigurace, analytický popis, vizualizace.	ANO	ANO
Výjimky. Detekce a posouzení výjimek a anomálií v konfiguraci síťových prvků.	ANO	ANO
Výkonnostní omezení. Detekce a posouzení konfiguračních nastavení s významným dopadem na výkonnost.	ANO	ANO
Bezpečnost – slabá místa. Detekce a posouzení bezpečnostních nedostatků vyplývajících z konfiguračních nastavení.	ANO	ANO
Segmentace. Analytické vyhodnocení stavu segmentace (VLAN) a aktualizace zásad podle provozních a bezpečnostních požadavků.	ANO	ANO
Připravenost k zavedení NAC. Analýza připravenosti síťového prostředí, infrastruktury správy identit a bezpečnostních politik a domén pro zavedení NAC (Řízený přístup do sítě, 802.1x).	ANO	ANO

2.2 Hodnocení rizik

Objednatel požaduje provést vstupní hodnocení rizik síťového prostředí podle metodiky a standardu MV ČR, jak je uvedeno v Přílohách č. 7–11 této Technické specifikace. Hodnocení rizik se bude vztahovat k výchozímu stavu sítě před modernizací a bude obsahovat návrh opatření

vedoucích ke snížení míry rizika. Dodavatel označí ty návrhy opatření, která budou implementována v rámci dodávky Díla.

Hodnocení rizik bude zpracováno formou Technické zprávy *Hodnocení rizik ISŘP* a bude tvořit nedílnou součást (přílohu) Prováděcího projektu č.1.

3 Modernizace sítě

Kapitola 3 Technické specifikace specifikuje požadavky Objednatele na dodávanou síťovou infrastrukturu a komponenty IP telefonie včetně služeb, které jsou nedílnou součástí dodávky, zahrnující:

- Demontáž původní technologie, montáž a zprovoznění aktivních prvků L3, L2 a IP telefonů, analogových bran, zdrojů napájení a stojanu.
- Provedení konfigurace modernizované části sítě v souladu s návrhem segmentace sítě akceptovaným v Prováděcím projektu č.1 a s ohledem na minimalizaci celkového provozního výpadku v lokalitě. Dodavatel zpracuje návrh segmentace sítě podle požadavků kapitoly 3.1 Technické specifikace.

3.1 Validace/optimalizace adresního plánu a návrh segmentace sítě MV ČR

Objednatel požaduje odborné zhodnocení aktuálního adresního plánu a zpracování doporučení na event. *optimalizaci adresního plánu*. Objednatel dále požaduje zpracovat návrh segmentace sítě na základě struktury datového provozu v lokalitách Objednatele a s ohledem na realizovatelnost řízeného přístupu do sítě.

Objednatel požaduje vytvoření bezpečnostních domén, které budou vyjadřovat příslušnou bezpečnostní úroveň, např. doména uživatelských PC, doména administrace síťových prvků, doména tiskáren atd. Oddělení domén bude provedeno na druhé vrstvě OSI modelu (VLAN). Každá doména bude mít přiděleno svoje nativní VLAN ID, které bude globální a stejné napříč lokalitami.

Validace/optimalizace adresního plánu a návrh segmentace sítě MV ČR bude zpracován formou Technické zprávy *Adresní plán a segmentace sítě* a bude tvořit nedílnou součást (přílohu) Prováděcího projektu č.1.

3.2 Specifikace aktivních síťových prvků

S ohledem na požadavek uvedený v kap. 1.3.1 Technické specifikace budou pořizované komponenty LAN sítě plně kompatibilní s technologiemi uvedenými formou obecné technické specifikace v Příloze č.2 této Technické specifikace *Záměr standardizace a rozvoje datových uzlů komunikační infrastruktury Ministerstva vnitra a Policie České republiky*.

Pokud nejsou pro řešení v konkrétní lokalitě, nebo jako parametr specifikovaný u konkrétního typu aktivního prvku (v kap. 3.2 Technické specifikace) uvedeny rozměry prvků, uplatní se průřezový požadavek Objednatele na rozměry aktivních prvků: šířka 19“, výška 1U (v případě stohovatelných prvků platí pro jednotlivá zařízení stohu), maximální hloubka 40 cm.

3.2.1 Přístupový přepínač (S2C)

Přístupový LAN přepínač s pasivním chlazením bez ventilátoru a musí disponovat min. dvěma porty typu 1GE a dvěma porty 10G SFP+.

Přístupový LAN přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Přístupový LAN přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Přístupový LAN přepínač musí být schopen automaticky aplikovat specifickou konfiguraci pro daný typ koncového zařízení (např. IP telefon, IP kamera) po detekci jeho připojení na portu.

Přístupový LAN přepínač musí podporovat standardy pro napájení po Ethernetu (PoE) dle norem 802.3af a 802.3at a disponovat PoE výkonem min. 180 W. Rovněž musí podporovat zabezpečení portů dle standardu 802.1x s podporou pro koncové IP telefony.

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, mapování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 guard, IPv6 source guard).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Přístupový LAN přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S2C je uvedena v následující tabulce.

Tabulka 6: Specifikace přístupového přepínače S2C

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9200CX-12P-2X2G-A

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Kompaktní	ANO
Maximální hloubka=28 cm	ANO	ANO
Chlazení pasivní, bez ventilátoru	ANO	ANO
Minimální počet portů 10/100/1000Base-T s PoE napájením	12	ANO
Uplink porty min. 2x1GE	ANO	ANO
Uplink porty min. 2x10G SFP+	ANO	ANO
Velikost MAC address tabulky	15000	ANO
Min. počet IPv4 routes	2000	ANO
Min. počet konfigurovatelných security ACL	1000	ANO
Min. velikost sdíleného systémového bufferu	3 MB	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	24	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	500	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi- domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9000 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	1	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS – Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
IEEE 802.1ae (AES-GCM-128) na uplink portech	ANO	ANO
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu, a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	180W	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Application Visibility – Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Application Visibility – Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (RSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.2 Přístupový přepínač (S2)

Přístupový LAN přepínač musí být stohovatelný a musí disponovat min. jedním slotem pro uplink modul s dvěma porty typu 1GE, případně 10GE. Přístupový LAN přepínač musí umožnit propojení do stohu s podporou agregace portů do virtuálních trunků napříč jednotlivými členy stohu.

Přístupový LAN přepínač musí v případě potřeby umožnit instalaci interního redundantního napájecího zdroje.

Přístupový LAN přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Přístupový LAN přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Přístupový LAN přepínač musí být schopen automaticky aplikovat specifickou konfiguraci pro daný typ koncového zařízení (např. IP telefon, IP kamera) po detekci jeho připojení na portu.

Přístupový LAN přepínač musí podporovat standardy pro napájení po Ethernetu (PoE) dle norem 802.3af a 802.3at a disponovat PoE výkonem min. 370 W. Rovněž musí podporovat zabezpečení portů dle standardu 802.1x s podporou pro koncové IP telefony.

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, mapování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 guard, IPv6 source guard).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Přístupový LAN přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S2 je uvedena v následující tabulce.

Tabulka 7: Specifikace přístupového přepínače S2

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9200-24P-A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Možnost instalovat modul s dedikovanými stohovacími porty	ANO, min. 2 porty	ANO
Možnost instalovat modul s minimální kapacitou sběrnice stohu 160Gb/s	ANO	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Za provozu vyměnitelné ventilační moduly	ANO	ANO
Minimální počet portů 10/100/1000Base-T s PoE napájením	24	ANO
Možnost instalovat uplink modul s min. 4x1GE porty	ANO	ANO
Možnost instalovat uplink modul s min. 4x10GE porty	ANO	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	4000	ANO
Min. počet konfigurovatelných security ACL	1500	ANO
Min. velikost sdíleného systémového bufferu	6 MB	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	500	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9000 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	4	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS – Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
IEEE 802.1ae (AES-GCM-128) na uplink portech	ANO	ANO
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu, a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	370W	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Application Visibility – Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Application Visibility – Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (RSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.3 Přístupový přepínač (S3)

Přístupový LAN přepínač musí být stohovatelný a musí disponovat min. jedním slotem pro uplink modul s dvěma porty typu 10/25GE. Přístupový LAN přepínač musí umožnit propojení do stohu s podporou agregace portů do virtuálních trunků napříč jednotlivými členy stohu.

Přístupový LAN přepínač musí v případě potřeby umožnit instalaci interního redundantního napájecího zdroje a musí podporovat sdílení napájecích zdrojů napříč stohem přepínačů.

Přístupový LAN přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Přístupový LAN přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Přístupový LAN přepínač musí být schopen automaticky aplikovat specifickou konfiguraci pro daný typ koncového zařízení (např. IP telefon, IP kamera) po detekci jeho připojení na portu.

Přístupový LAN přepínač musí podporovat standardy pro napájení po Ethernetu (PoE) dle norem 802.3af a 802.3at a disponovat PoE výkonem min. 820 W. Rovněž musí podporovat zabezpečení portů dle standardu 802.1x s podporou pro koncové IP telefony

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, mapování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 guard, IPv6 source guard).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Přístupový LAN přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S3 je uvedena v následující tabulce.

Tabulka 8: Specifikace přístupového přepínače S3

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9300-48P-A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Počet portů 10/100/1000 Base-T s PoE napájením	48	ANO
Minimální počet uplink portů 1/10/25 GE s volitelným fyzickým rozhraním typu SFP28	2	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Podpora dual-rate 10/25GE SFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
Podpora dual-rate 10/25GE SFP rozhraní umožňujících přenos signálu přes duplexní singlemodová vlákna	ANO	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9100 bytes)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
BGPv4, MP-BGP	ANO	ANO
Bezvýpadkové uvedení přepínače do režimu maintenance mode (Graceful Insertion and Removal nebo ekvivalentní)	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	64	ANO
VXLAN s MP-BGP EVPN control plane	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMP a MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS – Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
PACL, VACL pro IPv4 i IPv6	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO	ANO
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	ANO	ANO
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	820W	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Software patching	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Application hosting	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.4 Přístupový přepínač (S3D)

Přístupový přepínač 48 portů pro síť dohledu. V konfiguraci jednotlivých lokalit (viz 1.4, lokalita MV ČR pracoviště Olšanská 4) je požadován přepínač S3D za účelem připojení prvků do dohledového systému, konkrétně STd, WS (IPMI).

Přístupový LAN přepínač musí být stohovatelný a musí disponovat min. jedním slotem pro uplink modul s dvěma porty typu 1GE, nebo 10GE. Přístupový LAN přepínač musí umožnit propojení do stohu s podporou agregace portů do virtuálních trunků napříč jednotlivými členy stohu.

Přístupový LAN přepínač musí v případě potřeby umožnit instalaci interního redundantního napájecího zdroje a musí podporovat sdílení napájecích zdrojů napříč stohem přepínačů.

Přístupový LAN přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Přístupový LAN přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Přístupový LAN přepínač musí být schopen automaticky aplikovat specifickou konfiguraci pro daný typ koncového zařízení (např. IP telefon, IP kamera) po detekci jeho připojení na portu.

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, mapování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 guard, IPv6 source guard).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Přístupový LAN přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S3D je uvedena v následující tabulce.

Tabulka 9: Specifikace přístupového přepínače S3D

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9300-48T-A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Počet portů 10/100/1000 Base-T	48	ANO
Minimální počet uplink portů 1 GE nebo 10GE s volitelným fyzickým rozhraním typu SFP nebo SFP+	4	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9100 bytes)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
BGPv4, MP-BGP	ANO	ANO
Bezvýpadkové uvedení přepínače do režimu maintenance mode (Graceful Insertion and Removal nebo ekvivalentní)	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Min. počet oddělených (nezávislých) směrovacích tabulek	64	ANO
VXLAN s MP-BGP EVPN control plane	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMP a MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS – Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
PACL, VACL pro IPv4 i IPv6	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO	ANO
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	ANO	ANO
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Software patching	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Application hosting	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.5 Přístupový přepínač (S3AP)

Přístupový LAN přepínač musí být stohovatelný a musí disponovat min. jedním slotem pro uplink modul s dvěma porty typu 10/25GE. Přístupový LAN přepínač musí umožnit propojení do stohu s podporou agregace portů do virtuálních trunků napříč jednotlivými členy stohu.

Přístupový LAN přepínač musí v případě potřeby umožnit instalaci interního redundantního napájecího zdroje a musí podporovat sdílení napájecích zdrojů napříč stohem přepínačů.

Přístupový LAN přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Přístupový LAN přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Přístupový LAN přepínač musí být schopen automaticky aplikovat specifickou konfiguraci pro daný typ koncového zařízení (např. IP telefon, IP kamera) po detekci jeho připojení na portu.

Přístupový LAN přepínač musí podporovat standardy pro napájení po Ethernetu (PoE) dle norem 802.3af a 802.3at a disponovat PoE výkonem min. 820 W. Rovněž musí podporovat zabezpečení portů dle standardu 802.1x.

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, mapování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 guard, IPv6 source guard).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Přístupový LAN přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S9 je uvedena v následující tabulce.

Tabulka 10: Specifikace přístupového přepínače S3AP

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9300-48UXM-A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Počet portů 0.1/1/2.5/5 GE s PoE napájením	12	ANO
Počet portů 2.5 GE s UPoE napájením	36	ANO
Minimální počet uplink portů 1/10/25 GE s volitelným fyzickým rozhraním typu SFP28	2	ANO
Podpora dual-rate 10/25GE SFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
Podpora dual-rate 10/25GE SFP rozhraní umožňujících přenos signálu přes duplexní singlemodová vlákna	ANO	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Stateful Switch Over v rámci stohu	ANO	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9100 bytes)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
BGPv4, MP-BGP	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Bezvýpadkové uvedení přepínače do režimu maintenance mode (Graceful Insertion and Removal nebo ekvivalentní)	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	64	ANO
VXLAN s MP-BGP EVPN control plane	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMP a MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS – Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
PACL, VACL pro IPv4 i IPv6	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO	ANO
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	ANO	ANO
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	820W	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Software patching	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Application hosting	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.6 Agregační přepínač (S5)

Agregační přepínač musí zajistit plnou podporu IP adresace a směrovacích protokolů pro IPv4 i IPv6 s minimálními požadavky na směrovací protokoly IS-IS, OSPFv2/v3, BGPv4 a Multiprotocol BGP.

Agregační přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Agregační přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Agregační přepínač musí podporovat směrování IP multicast provozu s minimálními požadavky na podporu protokolů PIM SM a PIM SSM, a to jak pro protokol IPv4, tak i IPv6. Agregační přepínač musí dále podporovat širokou škálu bezpečnostních mechanismů jako je ochrana proti podvržení zdrojové IP a MAC adresy, ochrana proti neautorizovaným službám DHCP a šifrování provozu s využitím technologie IEEE 802.1ae.

Agregační přepínač musí podporovat funkcionalitu, která umožňuje sloučit dva fyzické přepínače do jednoho virtuálního, který se vůči okolním systémům (LAN přepínače, servery atd.) chová jako jeden logický přepínač. L3 páteřní přepínač musí rovněž podporovat agregaci portů do virtuálních trunků napříč fyzickými šasi.

Agregační přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, markování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty pro provoz IP telefonie.

Agregační přepínač musí podporovat technologii DualStack (IPv4 a IPv6) a musí mít plnou podporu IPv6 služeb jako jsou DNS, Telnet/SSH, DHCP, Multicast a QoS.

Agregační přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Agregační přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S5 je uvedena v následující tabulce.

Tabulka 11: Specifikace přístupového přepínače S5

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9500-48Y4C-A
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Interní redundantní AC napájecí zdroj	ANO	ANO
Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28	48	ANO
Minimální počet neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	4	ANO
Podpora dual-rate 10/25GE SFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
Podpora dual-rate 10/25GE SFP rozhraní umožňujících přenos signálu přes duplexní singlemodová vlákna	ANO	ANO
Podpora dual-rate 40/100GE QSFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
Podpora virtualizace – možnost sloučit dvě fyzická šasi do jednoho logického	ANO	ANO
Min. velikost sdíleného systémového bufferu	36MB	ANO
Velikost MAC address tabulky	80000	ANO
Min. počet IPv4 routes	100000	ANO
Min. počet IPv6 routes	100000	ANO
Min. počet konfigurovatelných security ACL	15000	ANO
Flexibilní alokace SRAM a TCAM zdrojů (MAC/IP/ACL záznamy)	ANO	ANO
IEEE 802.3ad (Link Aggregation – LAG)	ANO	ANO
IEEE 802.3ad přes více šasi (Multichassis LAG)	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
Podpora jumbo rámců (min. 9000 bytes)	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
BGPv4, MP-BGP	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Bezvýpadkové uvedení přepínače do režimu maintenance mode (Graceful Insertion and Removal)	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
IGMPv2/v3 a MLD snooping	ANO	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	64	ANO
VXLAN s MP-BGP EVPN control plane	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS – Strict Priority Queue	ANO	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard)	ANO	ANO
Port ACL, VLAN ACL pro IPv4 i IPv6	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na všech portech	ANO	ANO
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	ANO	ANO
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
Application Visibility – Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Application Visibility – Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Software patching	ANO	ANO
Python scripting	ANO	ANO
Linux shell	ANO	ANO
Model-driven telemetrie pro real-time streaming stavových a statistických informací	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (ERSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.7 Přístupový přepínač (S8D)

Přístupový přepínač 8 portů pro síť dohledu. V konfiguraci jednotlivých lokalit (viz dle kap. 1.4 Technické specifikace je požadován přepínač S8D za účelem připojení prvků do dohledového systému, konkrétně STd, WS (IPMI). V této aplikaci je postačující konfigurace přepínače s 1 uplinkem a 8 uživatelskými porty. V této aplikaci je dále přípustná varianta přepínače s PoE za předpokladu, že technické řešení navrhované Dodavatelem v jeho nabídce využije PoE pro napájení dohledu stojanů (STd).

Přístupový LAN přepínač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Přístupový LAN přepínač musí umožňovat mikrosegmentaci síťové infrastruktury využívající tzv. group-based bezpečnostní politiky.

Přístupový LAN přepínač musí být schopen automaticky aplikovat specifickou konfiguraci pro daný typ koncového zařízení (např. IP telefon, IP kamera) po detekci jeho připojení na portu.

Přístupový LAN přepínač musí podporovat optimalizaci IP multicast provozu (IGMP a MLD snooping).

Přístupový LAN přepínač musí umožnit zabezpečení na portech proti podvržení zdrojové MAC a IP adresy a ochranu proti neautorizovaným službám DHCP.

Přístupový LAN přepínač musí plně podporovat řízení kvality služeb (QoS) s možností definice frontování, klasifikace provozu, mapování provozu (DSCP, COS) s možností omezení a vyčlenění šířky pásma provozu v jednotlivých kategoriích a definici prioritní fronty.

Přístupový LAN přepínač musí plně podporovat IPv6 protokoly a služby jako jsou DNS, Telnet/SSH, DHCP, ACL a QoS. Přepínač musí podporovat funkcionalitu IPv6 First Hop Security (Port ACL, RA guard, DHCPv6 guard, IPv6 source guard).

Přístupový LAN přepínač musí plně podporovat monitorování aplikačních toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Přístupový LAN přepínač rovněž musí umožňovat implementaci síťových služeb a síťových politik s využitím principů softwarově definovaných sítí (SDN).

Přesná požadovaná funkční specifikace přepínače S8D je uvedena v následující tabulce.

Tabulka 12 Specifikace přístupového přepínače S8D

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9200CX-12P-2X2G-E
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Kompaktní	ANO
Minimální počet portů 10/100/1000Base-T	12	ANO
Minimální počet uplink portů 10/100/1000Base-T	2	ANO
Minimální počet uplink portů 1/10 GE s volitelným fyzickým rozhraním typu SFP+	2	ANO
Pasivní chlazení (Fanless provedení)	ANO	ANO
Interní AC napájecí zdroj	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	4000	ANO
Min. počet konfigurovatelných security ACL	1000	ANO
Min. velikost sdíleného systémového bufferu	6 MB	ANO
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	500	ANO
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9000 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2, OSPFv3	ANO	ANO
ISIS	ANO	ANO
VXLAN Group Policy Option nebo ekvivalentní	ANO	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	4	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS – Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Podpora mikrosegmentace s využitím security-based group tags nebo ekvivalentní technologie	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchore	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Minimální PoE budget	240W	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Application Visibility – Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Application Visibility – Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
Vzdálený port mirroring (RSPAN)	ANO	ANO
NTPv3 server	ANO	ANO

3.2.8 Páteřní směrovač (R0)

Páteřní směrovač zajišťuje připojení pracoviště v lokalitě MV ČR pracoviště Olšanská 4 do páteřní sítě ITS. Na základě přijatých a řádně odůvodněných opatření Objednatel požaduje konkrétní typ aktivního prvku ASR9902 výrobce Cisco Systems v sestavě specifikované v následující tabulce. V samostatných sloupcích Dílo, resp. Pozáruční plnění jsou specifikovány komponenty v množství pro 1 ks směrovače.

Tabulka 13: Specifikace směrovače R0

P/N	Popis	Doba podpory P/N [*měsíc*]	Dílo Množství [*ks*]	Pozáruční plnění Množství [ks]
ASR-9902-FC	ASR 9902 Flexible Consumption Compact Chassis, 2 RU	---	1	0
SD-ARC-ASR9902M	SIA AR NCD NO SW ASR 9902, 2RU, Flexible Consumption Chas	12	3	2
ADN-ED-400G-RTU1	Edge Advantage w/ Essentials Software RTU License per 400G	---	1	0
SD-SWK-ADNED400	SW SUPPORT NO UPG Advantage Software RTU License per 400G	12	3	2
A99-RP-F-FC	ASR 9900 Fixed Chassis Route Processor FCM	---	1	0
SD-ARC-A99RPFFC	SIA AR NCD NO SWASR 9900 Fixed Chassis Route Processor	12	3	2
QSFP-40/100-SRBD	100G and 40GBASE SR-BiDi QSFP Transceiver, LC, 100m OM4 MMF	---	3	0
SFP-10G-SR	10GBASE-SR SFP Module	---	3	0
SFP-10G-LR	10GBASE-LR SFP Module	---	6	0
SFP-1G-SX	1000BASE-SX SFP transceiver module for SFP+ ports	---	6	0
SFP-1G-LH	1000BASE-LX/LH SFP transceiver module for SFP+ ports	---	4	0
ASR-9902-FAN	ASR 9902 Fan Module	---	3	0
ASR-9902-4P-KIT	ASR 9902 4-Post Mounting Kit for 19 & 23 inch Rack	---	1	0
ASR-9902-CAB-MGMT	ASR 9902 Cable Management Brackets	---	1	0
ASR-9902-FILTER	ASR 9902 Air Filter	---	1	0
A9K-OTHER	ASR9000; Other Network Applications; For Tracking Only	---	1	0
A99-RP-F-FLR	ASR 9900 Fixed Chassis Route Processor Slot Filler	---	1	0
A9K-FCM	ASR 9000 Flexible Consumption Business Model -Tracking onl	---	1	0
ASR-9902-TRK	ASR 9902 FCM Chassis Hardware Tracking PID	---	1	0
XR-7.9-A9K-K9-TRK	Cisco ASR 9000 IOS XR 64-bit 3DES Software for 7.9 Rls - FCM	---	1	0
PWR-1.6KW-AC	ASR 9900 Fixed Chassis AC Power Supply	---	2	0

CAB-TA-EU	Europe AC Type A Power Cable	---	2	0
SD-SVS-FC-IOSXR	Flexible Consumption IOSXR	---	1	0
ADN-ED-400G-SIA5	Edge Advantage w/ Essentials SIA per 400G for 60-120 months	---	1	0
R-CISCO-S-EPNMC-K9	Cisco EPN Manager Smart - Electronic	---	1	0
SD-SNK-RSCISCO S	SW SUPT NO UPG NET Cisco EPN Manager Smart - Electronic	12	3	2
EPNM-E-LG-SRTM	EPNM Smart Large Device Essentials RTM	---	1	0
SD-SNK-EPNMMDSR	SW SUPT NO UPG NET EPNM Smart Large Dev	12	3	2
EPNM-E-LG2-SRTMSIA	EPNM Smart Large Ess RTM SIA 60 momths SIA	---	1	0
SD-SVS-EPNM-S	Cisco Evolved Programmable Network Manager Smart - SIA	---	1	0
QSFP-40G-SR4-S=	40GBASE-SR4 QSFP Trnscvr Module, MPO Conn, Enterprise-Class	---	3	0
SFP-10G-SR	10GBASE-SR SFP Module	---	1	0
DWDM-SFP10G-C=	DWDM Tunable SFP+ 10 Gigabit Ethernet Transceiver Module	---	1	0
CON-SNC-DWDMS0GC	SNTC-NCD DWDM Tunable SFP+ 10 Gigabit Ethernet	12	3	2

3.2.9 Směrovač (R4)

Směrovač musí mít modulární architekturu s možností přidávat moduly rozhraní dle budoucí potřeby a musí umožnit připojení objektu prostřednictvím komunikačních linek s přenosovou kapacitou až 100Mbps.

Směrovač musí zajistit plnou podporu IP adresace a směrovacích protokolů pro IPv4 i IPv6 s minimálními požadavky na směrovací protokoly OSPFv2/v3, BGPv4 a Multiprotocol BGP.

Směrovač musí podporovat šifrování datového provozu s využitím technologie IPSec a s podporou Suite-B šifrovacích algoritmů definovaných v RFC 6379. Směrovač musí umožnit případné nasazení Quantum-Safe šifrování dle RFC 8784 na základě budoucích požadavků prostřednictvím upgrade jeho SW vybavení.

Směrovač musí podporovat možnost makrosegmentace datového provozu s využitím standardizované technologie Virtual Routing and Forwarding (VRF).

Směrovač musí plně podporovat pokročilé mechanismy pro řízení kvality služeb (QoS) včetně Hierarchical QoS, klasifikace provozu, markování provozu (DSCP, COS) a vyčlenění šířky pásma provozu v jednotlivých aplikačních kategoriích.

Směrovač musí plně podporovat monitorování datových toků prostřednictvím technologie NetFlow za účelem detekce anomálních datových toků a bezpečnostních hrozeb.

Směrovač musí být možné provozovat v autonomním režimu nebo v režimu SD-WAN (Softwarově definovaná WAN síť).

Přesná požadovaná funkční specifikace směrovače R4 je uvedena v následující tabulce.

Tabulka 14: Specifikace směrovače R4

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C8200-1N-4T
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8200-series-edge-platforms/nb-06-cat8200-series-edge-plat-ds-cte-en.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ zařízení	Směrovač	ANO
Formát zařízení	Modulární	ANO
Počet WAN portů typu 10/100/1000Base-T	2	ANO
Počet WAN portů typu 1000Base-X	2	ANO
Min. 1 volný slot pro rozšiřující modul	ANO	ANO
Interní AC napájecí zdroj	ANO	ANO
Možnost rozšířit směrovač o Wireless WAN modul s rozhraním 5G LTE s následujícími parametry: - Podpora dual SIM Podpora připojení min. ke dvěma APN	 ANO	ANO
Propustnost systému	3,5 Gb/s	ANO
OSPFv2, OSPFv3	ANO	ANO
BGPv4, MP-BGP	ANO	ANO
Podpora 4 byte AS numbers in BGP	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6	ANO	ANO
GRE (Generic Routing Encapsulation)	ANO	ANO
Policy-based routing podle ACL	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
uRPF pro IPv4 i IPv6	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
DHCP relay pro IPv4 i IPv6	ANO	ANO
IPv6 Multicast (MLDv1 & v2)	ANO	ANO
IPv6 Multicast (PIM SM, PIM SSM)	ANO	ANO
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS Shaping and Policing	ANO	ANO
Class Based and Priority queuing	ANO	ANO
Rate Limiting	ANO	ANO
Hierarchical QoS	min. 3 úrovně	ANO
Virtualizace směrovacích tabulek – Virtual Routing and Forwarding (VRF)	ANO	ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	64	ANO
Podpora protokolů a služeb per VRF (OSPF, TACACS+, VRRP nebo HSRP, SNMP, Syslog)	ANO	ANO
Zone-based statefull firewall	ANO	ANO
IPSec AES-GCM-256	ANO	ANO
Hardwarová akcelerace šifrování pro IPSec AES-GCM-256	ANO	ANO
Minimální šifrovací výkon pro IPSec AES-GCM-256	400 Mb/s	ANO
IPSec IKEv2	ANO	ANO
SHA-2 (SHA-256, SHA-512)	ANO	ANO
QoS pre-classification for IPSec	ANO	ANO
VRF aware IPSec	ANO	ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami	ANO	ANO
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů	ANO	ANO
Podpora Suite-B šifrovacích algoritmů (RFC 6379)	ANO	ANO
VRF aware GDOI group member (selektivní šifrování provozu per IP VPN)	ANO	ANO
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) včetně možnosti definovat signatury pro vlastní aplikace	ANO	ANO
Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX	ANO	ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků – tzv. hardware anchore	ANO	ANO
Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility	ANO	ANO
Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému	ANO	ANO
Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Programovatelnost prostřednictvím NETCONF/YANG	ANO	ANO
Python scripting	ANO	ANO
Application hosting	ANO	ANO
Model-driven telemetrie pro real-time streaming informací o stavu zařízení	ANO	ANO
SNMPv2/v3	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO
Možnost provozovat směrovač v autonomním módu nebo v módu, kdy je řízen SD-WAN kontrolerem	ANO	ANO

3.2.10 Přístupový bod bezdrátové sítě (WAP)

WLAN přístupová jednotka (access point) musí být vybavena radiem pro 2,4, 5 i 6 GHz pásmo a musí podporovat standardy 802.11a/b/g/n/ac/ax a Wi-Fi6E.

WLAN přístupová jednotka musí dále podporovat mechanismy pro přepojení klientů z 2.4GHz a 5GHz do 6GHz pásma a disponovat hardwarovou podporou spektrální analýzy pro detekci zdroje rušivého signálu. Musí rovněž podporovat výpočet závažnosti dopadu interference na kvalitu radiového signálu bezdrátové sítě.

WLAN přístupová jednotka musí umožňovat 802.3af/802.3.at PoE napájení z LAN přepínače nebo prostřednictvím power injectoru a musí podporovat mechanismy pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11ac/ax klientům.

Přesná požadovaná funkční specifikace WLAN přístupové jednotky je uvedena v následující tabulce.

Tabulka 15: Specifikace přístupového bodu sítě WLAN

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	CW9164I-E
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9164-series-access-points/catalyst-9164-series-access-points-ds.html
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu (Pozáruční plnění) po ukončení záruky.	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Typ zařízení	Přístupový bod WLAN	ANO
Přístupový bod (AP) určený pro instalaci na strop/podhled	ANO	ANO
Typ antén	Integrované pro obě pásma	ANO
Tři rádia pracující v režimu 2.4 + 5 + 6 GHz pro standardní prostředí	ANO	ANO
Samostatné rádio pro monitorování 2.4, 5 a 6 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou síť, lokalizace klientů	ANO	ANO
Podpora standardů 802.11a/b/g/n/ac/ax a Wi-Fi6E	ANO	ANO
Podpora minimálně 2x2 pro 2.4 GHz	ANO	ANO
Podpora minimálně 4x4 pro 5 a 6 GHz	ANO	ANO
Podpora MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	ANO	ANO
Minimální počet inzerovaných SSID (BSSID) per radio	8	ANO
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming)	ANO	ANO
Podpora mechanismu pro přepojení klientů z 2.4GHz do 5GHz pásma	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Podpora mechanismu pro přepojení klientů z 2.4GHz a 5GHz do 6GHz pásma	ANO	ANO
Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI	ANO	ANO
Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant	ANO	ANO
Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ANO	ANO
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH	ANO	ANO
Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference) pro 2.4, 5 a 6 GHz	ANO	ANO
Podpora rozpoznání zdroje rušivého signálu podle signatur 2.4, 5 a 6 GHz	ANO	ANO
Access Point obsahuje radio podporující BLE 5.1 a USB 2.0 port s podporou napájení minimálně 4.5W	ANO	ANO
Access Point ANO kontejnerové prostředí pro běh aplikací	ANO	ANO
1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz	ANO	ANO
Možnost 802.3af/at/bt PoE napájení AP z přepínače nebo injectoru. Plná funkce obou rádií AP i při použití 802.3at, tj. 2x2 + 4x4 + 4x4 MIMO bez sníženého vysílacího výkonu	ANO	ANO
Možnost napájení z DC zdroje	ANO	ANO
AP uzavřené konstrukce bez větracích otvorů a ventilátoru	ANO	ANO
Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu	ANO	ANO
AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem.	ANO	ANO
Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům	ANO	ANO

Objednatel požaduje na dodavateli provedení průzkumu lokality **MV ČR pracoviště Olšanská 4** (*Site survey*) s detailním proměřením signálu. Na jeho základě potom dodavatel zpracuje návrh optimálního rozmístění přístupových bodů, který bude součástí Prováděcího projektu č.1.

Kabelové připojení přístupových bodů bude uloženo ve stropních podhledech zhotovitelem stavby a po dodavateli se dodávka kabeláže nepožaduje.

Konfigurace přístupových jednotek a registrace ke kontrolérům WLAN, které jsou v provozním režimu, budou prováděny pracovníky Objednatele (nebo pracovníky jím pověřené organizace) v rámci nezbytné součinnosti a nebudou požadovány po dodavateli.

3.2.11 Dohled aktivních prvků (DATAd)

Systém dohledu a managementu aktivních prvků musí poskytovat funkcionality pro dohled a správu rozsáhlého síťového prostředí:

- **Monitoring a analýza:** monitoring sítě v reálném čase, včetně zobrazení stavu zařízení, výkonu sítě a identifikace problémů.
- **Management konfigurací:** konfigurace a nastavení síťových prvků.
- **Správa životního cyklu zařízení:** sledování/správa zařízení od jejich nasazení až po jejich vyřazení, včetně aktualizací firmwaru.
- **Automatizace a orchestrace:** automatizace při nasazení a konfiguraci sítě (zjednodušení správy rozsáhlé sítě a snížení rizika lidské chyby).
- **Optimalizace výkonu sítě:** analýza výkonu sítě s návrhem doporučení pro jeho optimalizaci (optimalizace toků dat, přizpůsobení konfigurací apod.).
- **Zprávy a reporty:** podrobné reporty o stavu a výkonu sítě pro účely plánování a ostatní rozhodovací procesy.

Požaduje se kompatibilita s dodávanými síťovými prvky S2C, S2, S3, S3AP, S5, R4 a současně s prvky v provozním režimu uvedenými v tabulce č.1 Technické specifikace. Směrovač R0 není dohledován systémem DATAd, nýbrž provozovanou dohledovou aplikací EPNM. Odpovídající licence je součástí výčtu požadovaných komponent (specifikace) R0.

Požaduje se dodávka licencí tak, aby byly k systému dohledu a managementu připojeny aktivní prvky S2C, S2, S3, S3AP, S5, R4 ve všech lokalitách. Tomu odpovídá požadované množství licencí DATAd v lokalitách (součet počtu zařízení S2C, S2, S3, S3AP, S5, R4 v lokalitě.)

Systém dohledu a managementu aktivních prvků bude provozován ve virtualizovaném prostředí DC UPAAS.

Dále se požaduje:

- přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky,
- přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění),
- licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).

3.2.12 Požadavky na zabezpečení komunikace

Instalovaná komunikační infrastruktura musí zajistit zabezpečení WAN linek mezi jednotlivými objekty. Minimální požadavky na technologii pro vytváření šifrovaných spojení jsou:

- Podpora technologií AES 256, IKEv2 a SHA-2,
- Podpora selektivního šifrování provozu per IP VPN,
- Podpora vytváření šifrovaných VPN dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů,
- Podpora autentizace směrovačů pomocí certifikátů X.509 a infrastruktury PKI (s certifikační autoritou),

Propoje v lokalitách mimo režimová pracoviště realizované pomocí L2/L3 přepínačů je požadováno zabezpečit prostřednictvím šifrovací technologie MACSec (IEEE 802.1ae).

Minimální požadavky na technologii pro vytváření šifrovaných spojení jsou:

- Podpora technologie AES 256
- Hardwarová podpora šifrování na L3 přepínači

3.2.13 Příslušenství a instalační materiál

Nedílnou součástí dodávky Díla je veškeré příslušenství aktivních prvků (jako jsou volitelné síťové moduly, SFP, panely PDU pro připojení zařízení ve stojanech apod.) a montážní příslušenství (např. spojovací materiál, kabely, konektory, patch panely apod.) potřebné k dosažení bezvadné funkcionality dodávaného Díla.

Příslušenství a instalační materiál požadovaný pro jednotlivé lokality (viz kap. 1.4 Technické specifikace) jsou Objednatelem specifikovány *v nezbytně požadovaném množství* s tím, že Dodavatel je vždy povinen dodat veškeré příslušenství a instalační materiál v množství potřebném k dosažení bezvadné funkcionality dodávaného Díla. Kompletní sestavu příslušenství a instalačního materiálu Dodavatel předloží ve své nabídce v souladu se svým návrhem technického řešení.

Ve specifikaci *nezbytně požadovaného množství* není zohledněno příslušenství a instalační materiál potřebný k připojení lokalitních serverů Systému pro správu a řízení základních síťových služeb (WS) a k propojení prvků dohledového systému, které je Dodavatel rovněž povinen do své nabídky v odpovídajícím množství zahrnout.

Objednatel požaduje instalaci nové kabeláže v úseku *port přepínače – rozvodný panel zakončení strukturované kabeláže budovy* (tzn. patchcordy). Pro účely přípravy nabídky (nacenění instalace nové kabeláže) Objednatel uvádí, že:

- délka patchcordu v lokalitě MV ČR pracoviště Olšanská 4 nepřesáhne 20 m,
- délka patchcordu v ostatních lokalitách nepřesáhne 10 m.

3.3 Server pro nezávislou zálohu konfigurací (SZ)

Je požadován integrovaný sběr a automatické ukládání konfiguračních dat jednotlivých zařízení a aplikačních serverů na dedikovaném FTP a SFTP serveru ve virtuálním prostředí. Způsob ukládání konfigurací bude v textových souborech.

Tabulka 16: Specifikace serveru pro nezávislou zálohu konfigurací

Požadovaná funkcionalita / vlastnost	Způsob splnění požadované funkcionality / vlastnosti	Doplní Dodavatel dle nabízeného zařízení
Výrobce zařízení	Uvedení výrobce	Novicom s.r.o.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	AN-SYS-CONFIG
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.novicom.cz/addnet-tech-docs
Požadovaný formát zařízení	Virtuální server	ANO Virtuální server
Podpora FTP	ANO	ANO
Podpora SFTP	ANO	ANO
Textový formát zálohovaných dat	ANO	ANO

Dále se požaduje:

- přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky,
- přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění),
- licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).

3.4 Specifikace komponent IP telefonního systému

S ohledem na požadavek uvedený v kap. 1.3.1 Technické specifikace budou pořizované komponenty zapojeny do IP telefonního systému provozovaného Objednatelem. Jedná se o koncová zařízení specifikovaná dále.

3.4.1 Požadavky na koncová zařízení a jejich zprovoznění

Součástí telefonního systému je dodávka IP telefonních přístrojů v různých kategoriích, a to včetně veškerých potřebných licencí:

- **telefon typu A3** – základní telefon pro uživatele
- **telefon typu C** – asistentský telefon s velkým displejem a velkým počtem tlačítek linek s indikací jejich stavu
- **telefon typu D** – telefon pro vyšší management telefon s integrovanou HD kamerou pro video hovory a velkým barevným displejem
- **analogová brána** – převodník pro integraci analogových zařízení do IP telefonní infrastruktury

Konfigurace koncových zařízení a registrace k centrálnímu serveru IP telefonního systému, který je v provozním režimu, budou provádět pracovníci Objednatele (nebo pracovníci jím pověřené organizace) v rámci nezbytné součinnosti a nebudou požadovány po dodavateli. Po dodavateli se požaduje konfigurace a zprovoznění připojení koncového zařízení do sítě, tj. zajištění autentizace a autorizace přístupu do sítě, přidělení VLAN a IP adresy.

Specifikace jednotlivých typů telefonních přístrojů je uvedena v následujících tabulkách.

Tabulka 17: Specifikace IP telefonu typu A3

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	**Cisco**
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	**DP-9851-K9=**
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	**https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/desk-phone-9800-series-ds.html**

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	**ANO**
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	**ANO**
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	**ANO**
Napájení po Ethernetu IEEE 802.3af PoE, nebo přes ext. Zdroj	ANO	**ANO**
VLAN 802.1q, možnost tagování rámců dle 802.1p	ANO	**ANO**
Signalizační protokol	SIP	**ANO**
Audio kodeky	G.711, G.722, G.729	**ANO**
Podpora DHCP, možnost manuální konfigurace sítě včetně konfigurace VLAN a možnost automatického přiřazení do hlasové VLAN dle konfigurace přepínače	ANO	**ANO**
Integrovaný Ethernet switch pro připojení do LAN a připojení PC s minimální rychlostí	10/100/1000 Mbps	**ANO**
Displej telefonu s minimálními parametry	Grafický podsvětlený, monochromatický, min. 800x400 pixelů	**ANO**
Řízení hlasitosti vyzvánění, reproduktoru a sluchátka	ANO	**ANO**
Min. počet programovatelných funkčních tlačítek	9	**ANO**
Min. počet tlačítek nezávislých linek či předvolby s indikací stavu linky/předvolby	5	**ANO**
Handsfree hlasitý odposlech včetně vestavěného reproduktoru i mikrofonu s odstraněním echa	ANO	**ANO**
Připojení náhlavní soupravy	ANO	**ANO**
Adresářové služby s možností vyhledávání v tlf. Seznamech	ANO	**ANO**
Plná lokalizace přístroje pro český jazyk	ANO	**ANO**
Šifrování tel. hovorů včetně signalizačního protokolu	ANO	**ANO**

Tabulka 18: Specifikace IP telefonu typu C

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	**Cisco**
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	**DP-9861-K9=** **+** **DP-9800-KEM=**
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	**https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/ip-phones/desk-phone-9800-series-ds.html**
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	**ANO**
Napájení po Ethernetu IEEE 802.3af PoE, nebo přes ext. Zdroj	ANO	**ANO**
VLAN 802.1q, možnost tagování rámců dle 802.1p	ANO	**ANO**
Signalizační protokol	SIP	**ANO**
Audio kodeky	G.711, G.722, G.729	**ANO**
Podpora DHCP, možnost manuální konfigurace sítě včetně konfigurace VLAN a možnost automatického přiřazení do hlasové VLAN dle konfigurace přepínače	ANO	**ANO**
Integrovaný Ethernet switch pro připojení do LAN a připojení PC s minimální rychlostí	10/100/1000 Mbps	**ANO**
Displej telefonu s minimálními parametry	Víceřádkový grafický podsvětlený barevný displej, min 800x400 pixelů	**ANO**
Řízení hlasitosti vyzvánění, reproduktoru a sluchátka	ANO	**ANO**
Min. počet programovatelných funkčních tlačítek	9	**ANO**
Tlačítka nezávislých linek či předvolby s indikací stavu linky/předvolby	Min. 30, možno s externím modulem	**ANO**
Funkce Bluetooth pro připojení bezdrátové náhlavní soupravy	ANO	**ANO**
Handsfree hlasitý odposlech včetně vestavěného reproduktoru i mikrofonu s odstraněním echa	ANO	**ANO**
Adresářové služby s možností vyhledávání v tlf. seznamech	ANO	**ANO**
Podpora XML aplikací v telefonu	ANO	**ANO**
Plná lokalizace přístroje pro český jazyk	ANO	**ANO**
Šifrování tlf. hovorů včetně signalizačního protokolu	ANO	**ANO**

Tabulka 19: Specifikace IP telefonu typu D

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	**Cisco**
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	**CP-8875-K9=**
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	**https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/video-phone-8875-ds.html?dtid=osscdc000283&linkclickid=srch**
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	**ANO**
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	**ANO**
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	**ANO**
Napájení po Ethernetu IEEE 802.3af PoE, nebo přes ext. Zdroj	ANO	**ANO**
VLAN 802.1q, možnost tagování rámců dle 802.1p	ANO	**ANO**
Signalizační protokol	SIP	**ANO**
Audio kodeky	G.711, , G.722, G.729	**ANO**
Podpora DHCP, možnost manuální konfigurace sítě včetně konfigurace VLAN a možnost automatického přiřazení do hlasové VLAN dle konfigurace přepínače	ANO	**ANO**
Integrovaný Ethernet switch pro připojení do LAN a připojení PC s minimální rychlostí	10/100/1000 Mbps	**ANO**
Displej telefonu s minimálními parametry	Víceřádkový barevný podsvětlený grafický displej	**ANO**
Řízení hlasitosti vyzvánění, reproduktoru a sluchátka	ANO	**ANO**
Min. počet programovatelných funkčních tlačítek	9	**ANO**
Tlačítka nezávislých linek či předvolby	5	**ANO**
Rozšiřující modul tlačítek nezávislých linek, či předvolby s min. 10 tlačítky. Modul je možno připojit i k telefonu typu B	ANO	**ANO**

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Handsfree hlasitý odposlech včetně vestavěného reproduktoru i mikrofonu s odstraněním echa	ANO	**ANO**
Funkce Bluetooth pro připojení bezdrátové náhlavní soupravy	ANO	**ANO**
Podpora video hovorů – HD kvalita	ANO	**ANO**
Adresářové služby s možností vyhledávání v tlf. seznamech	ANO	**ANO**
Podpora XML aplikací v telefonu	ANO	**ANO**
Plná lokalizace přístroje pro český jazyk	ANO	**ANO**
Podpora videohovorů, vestavěná kamera	ANO	**ANO**
Šifrování tlf. hovorů včetně signalizačního protokolu	ANO	**ANO**

Analogová brána (AB24) bude primárně sloužit pro integraci starších analogových přístrojů typu fax nebo dveřník. Analogová brána musí disponovat min. 24 porty typu FXS.

Hlasová brána musí podporovat technologii DualStack (IPv4 a IPv6) a rovněž je vyžadována podpora šifrování pro hlas (SRTP) včetně signalizace SIP/TLS.

Přesná požadovaná funkční specifikace analogové brány je uvedena v následující tabulce.

Tabulka 20: Specifikace analogové brány typu 24xFXS (AB24)

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/unified-communications/vg-series-gateways/vg410-analog-voice-gateway-ds.html?dtid=osscdc000283&linkclickid=srch
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	**ANO**
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky. (Pozáruční plnění)	ANO	**ANO**

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	**ANO**
Napájení přes externí zdroj	ANO	**ANO**
VLAN 802.1q, možnost tagování rámců dle 802.1p	ANO	**ANO**
Dva porty Ethernet 10/100 Mbps pro možnost redundantního připojení k síti LAN	ANO	**ANO**
Signalizační protokol	SIP, H.323	**ANO**
Audio kodeky	G.711, G.729	**ANO**
Přenos faxu přes protokol IP	Standard T.38	**ANO**
Plnohodnotný port FXS včetně podpory signalizace Loop-Start a Ground-Start	ANO	**ANO**
Minimální počet analogových portů FXS	24	**ANO**
In-Band DTMF	ANO	**ANO**
Konferenční hovory	ANO	**ANO**
Funkce přidržení/pokračování hovoru	ANO	**ANO**
Funkce přímého nebo konzultačního přepojení hovoru	ANO	**ANO**
Funkce přesměrování hovoru	ANO	**ANO**
Identifikace volajícího	ANO	**ANO**
Music-on-Hold pro analogové telefony	ANO	**ANO**
Podpora protokolů SRTP a SIP/TLS pro šifrovaný přenos hlasu	ANO	**ANO**

3.4.2 Požadavky na integraci IP telefonní infrastruktury s LAN sítí

Z důvodu minimalizace nákladů na provoz a správu datové a hlasové infrastruktury MV ČR a podřízených rezortních organizací musí navržené řešení komunikačního systému umožňovat:

- automatickou detekci IP telefonu připojeného k portu LAN přepínače a jeho automatické přiřazení do dedikované hlasové VLAN,
- automatickou detekci IP telefonu připojeného k portu LAN přepínače a automatické nastavení vhodných QoS parametrů daného portu,
- automatickou detekci IP telefonu připojeného k portu LAN přepínače a inteligentní PoE management – zajištění napájení IP telefonu podle konkrétních požadavků daného typu IP telefonu,
- možnost připojení pracovní stanice uživatele ke komunikační infrastruktuře prostřednictvím IP telefonu,
- provoz dvou různých VLAN (hlasové a datové) na druhé vrstvě komunikačního modelu ISO/OSI v rámci jednoho portu.

3.4.3 Požadavky na bezpečnost IP telefonního systému

Nabízené řešení umožní snadnou implementaci šifrovaného přenosu telefonních hovorů v prostředí transportní IP sítě:

- šifrovaný přenos signalizace mezi „řídící server – IP telefon“ i „řídící server – hlasová brána“

- šifrovaný přenos telefonního hovoru (RTP stream) mezi „IP telefon – IP telefon“ i „IP telefon – hlasová brána“

Řídící servery IP telefonie, hlasové brány a koncové telefonní přístroje nebo video konferenční jednotky musí být připojeny do stávající dedikované IP VPN sítě „Voice“. SW IP telefony a aplikace provozované na pracovních stanicích, tabletech nebo smartphonech jsou připojeny do stávající datové IP VPN „Hermes“. IP telefonní systém musí zajistit bezpečnou a rychlou komunikaci mezi klienty v datové IP VPN síti „Hermes“ a klienty v hlasové IP VPN síti „Voice“ bez nutnosti směrování real-time telefonního provozu (UDP/RTP) přes centrální firewall propojující obě oddělené IP VPN sítě.

3.4.4 Systém pro zpracování a přístup k datům (IS)

Účelem systému je zajistit jeho uživatelům přístup k datům komunikačního systému a umožnit správu uživatelů, uživatelských služeb a koncových zařízení z webového prohlížeče v rozsahu podle přidělené úrovně oprávnění. Zároveň je cílem umožnit integraci a synchronizaci dat komunikačního systému s dalšími informačními zdroji dat v prostředí Objednatele.

Je požadován centrální systém přístupu k datům IP spojovacího systému, uživatelů, uživatelských služeb a koncových zařízení v počtu 2000, který zajišťuje:

- přístup k datovým strukturám IP spojovacího systému přes API
- službu webového telefonního seznamu
- správu koncových zařízení

Systém musí být navržen jako centralizovaný. Systém je požadováno instalovat na virtualizační platformě.

Systém musí být navržen jako multi-tenantní, aby umožňoval oddělení samostatně spravovaných oblastí.

Je požadován:

- přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky,
- přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění),
- licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění),.

Systém musí dále splňovat minimální požadavky uvedené v následující tabulce.

Tabulka 21: Specifikace systému pro zpracování a přístup k datům

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	OPSOFT s.r.o
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	www.opsoft.cz
Správa uživatelské databáze		
Správa hierarchie v uživatelské struktuře	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Možnost synchronizace s externími zdroji dat (AD, personalistické systémy, pasportizace majetku apod.)	ANO	ANO
Aktivní nástroje pro kontrolu konzistence a platnosti dat (záznamy na ústředně vs. podklady externích operátorů vs. personální systém)	ANO	ANO
Autorizovaný přístup k záznamům uživatele (historie hovorů, nastavení přesměrování, konfigurace osobního telefonního seznamu)	ANO	ANO
Telefonní seznam		
Webová aplikace telefonního seznamu	ANO	ANO
Možnost definice více telefonních seznamů	ANO	ANO
Vyhledávání v telefonním seznamu	ANO	ANO
Vyhledávání uživatelů na sdílených telefonních číslech	ANO	ANO
Vyhledávání uživatelů dle topologických parametrů (lokalita – budova – patro – kancelář)	ANO	ANO
Správa ústředen		
Automatický import parametrů ústředen	ANO	ANO
Multitenantní přístup na ústředny, možnost definice omezení přístupu až na úroveň parametrů koncových zařízení	ANO	ANO
Automatická kontrola a registrace změn všech parametrů, které byly provedeny mimo administrační systém, např. přímým přístupem na ústřednu	ANO	ANO
Správa koncových zařízení		
Konfigurace parametrů koncových zařízení (z web prohlížeče)	ANO	ANO
Konfigurace tlačítek IP telefonních přístrojů (z web prohlížeče)	ANO	ANO
Možnost vzdáleného zobrazení grafického displeje IP telefonních přístrojů	ANO	ANO
Odeslání notifikačních zpráv na displej telefonního přístroje	ANO	ANO
Správa koncových zařízení a čísel s možností automatické konfigurace dat na ústředně za účelem zobrazení v telefonním seznamu	ANO	ANO
Automatický import parametrů z koncových zařízení (verze FW, sériové číslo, kvalita hovorů, atd …)	ANO	ANO
Administrace topologického umístění koncových zařízení (lokalita-budova-patro-místnost) s možností automatického importu konfiguračních parametrů	ANO	ANO
Možnost definice uživatelsky definovatelných číselníkových informací (min 20)	ANO	ANO
Možnost definice uživatelsky definovatelných textových informací (min 20)	ANO	ANO
Možnost definicí obecných sekvencí příkazů na koncových zařízeních	ANO	ANO
Možnost provedení factory reset na koncovém zařízení	ANO	ANO
Vedení historie uživatelů koncových zařízení	ANO	ANO
Vedení historie registrace zařízení a topologického umístění	ANO	ano

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Zobrazení koncových zařízení v mapových podkladech	ANO	ANO
Kontrola koncových zařízení		
Detekce zařízení s neplatnými certifikáty	ANO	ANO
Možnost výběru platných podpisů certifikátů koncových zařízení za účelem validace	ANO	ANO
Možnost vynuceného nahrání platného certifikátu na koncovém zařízení	ANO	ANO
Kontrola aktuálnosti firmware koncových zařízení	ANO	ANO
Správa a monitoring síťových prvků		
Podpora síťových prvků VoIP gateway, routers, switch, Cisco IOS	ANO	ANO
Automatický import parametrů podle důležitosti prvku	ANO	ANO
Prezentace konfigurace ve stromové struktuře	ANO	ANO
Identifikace koncových bodů podle IP, CDP, sys description	ANO	ANO
Operace nad síťovými prvky, restart, vyp/zap E1/BRI, aktuální vytížení BOXu	ANO	ANO
Možnost umístění prvků do mapových podkladů	ANO	ANO
Analytické zpracování CDR záznamů		
Automatický import CDR záznamů z CCM a VoIP gateways	ANO	ANO
Analýza CDR a CMR záznamů až na úroveň koncového zařízení	ANO	ANO
Perioda automatického importu a zpracování dat minimálně 5 min	ANO	ANO
Statistické zpracování dat o hovorech	ANO	ANO
Detekce podezřelých volání na základě analýzy dat z ústředen a VoIP bran	ANO	ANO
Možnost označení dat pro účely dalších analýz	ANO	ANO
Možnost analytického zpracování dat o hovorech na úroveň vytížení trunku, vytížení E1/při rozhraní na VoIP branách	ANO	ANO
Analytické zpracování tarifikačních záznamů		
Automatický import tarifikačních záznamů z externích tarifikačních systémů	ANO	ANO
Automatický import tarifikačních záznamů z externího tarifikačního systému CALOM	ANO	ANO
Analýza podezřelého chování koncového účastníka na základě parametrického zadání	ANO	ANO
Analýza podezřelého chování koncového účastníka na základě neparametrického zadání (s využitím strojového učení na základě latentních souvislostí obsažených v datech o chování účastníků)	ANO	ANO
Přístup ke službám IS		
Možnost autorizace a integrace se systémem IDM	ANO	ANO
Možnost LDAP autorizace	ANO	ANO
Multitenantní architektura	ANO	ANO
Konfigurace uživatelských rolí	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Možnost definice detailních oprávnění: do částí systému, do úrovní uživatelské hierarchie, do úrovní topologie	ANO	ANO
Přístup k vybraným údajům pouze po autorizaci uživatele	ANO	ANO
Obecné funkční požadavky		
Autonomní mapové podklady, podpora veřejných mapových podkladů (OpenStreetMap, GoogleMap, …)	ANO	ANO
Podpora moderních prohlížečů Chrome, Firefox, Microsoft Edge	ANO	ANO
Přístup ke službám přes webové rozhraní	ANO	ANO
Logování veškerých operací se změnami parametrů systému	ANO	ANO
Podpora českého a anglického jazyka v uživatelském rozhraní	ANO	ANO

3.5 Stojanové rozvaděče

3.5.1 Stojan (ST)

Stojan (datový rozvaděč) pro instalaci komunikačních zařízení s montáží do 19“ lišt musí splňovat parametry uvedené v následující tabulce.

Tabulka 22: Specifikace stojanu:

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Conteg
Produktové číslo (typ) nabízeného zařízení (pokud je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	RM7
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení www odkazu	https://www.conteg.com/userfiles/iseven-flex-rm7-datasheet-conteg-en-f9474fb1.pdf
Rozměry (š x h x v) (variantně): 800 mm – 1000 mm – 42U (sálový stojan) 800 mm – 800 mm – 42U (sálový stojan) 800 mm – 1000 mm – 18 až 42U (podružný stojan) 800 mm – 800 mm – 18 až 42U (podružný stojan) 600 mm – 800 mm – 18 až 42U (podružný stojan) 600 mm – 600 mm – 18 až 42U (podružný stojan)	ANO	ANO
Montážní rám 19“ vpředu i vzadu	ANO	ANO
Rozebíratelná konstrukce rámu stojanu při rozměrech š=800 mm a současně h=800 mm, snadné sestavení stojanu v místě instalace	ANO	ANO

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Přední dveře perforované (míra perforace min 70 %), uzamykatelné, výklopná klika s bezpečnostní vyměnitelnou vložkou, univerzální klíč, min. jednobodové zamykání	ANO	ANO
Zadní dveře perforované (míra perforace min 70 %), uzamykatelné, výklopná klika s bezpečnostní vyměnitelnou vložkou, univerzální klíč, min. jednobodové zamykání	ANO	ANO
2 bočnice se zámky, celoplechové, univerzální klíč; bez horního krytu	ANO	ANO
Statická zatížitelnost pro výšku 42U	min. 1 000 kg	ANO
Statická zatížitelnost pro výšku 21U	min. 400 kg	ANO
Horní kryt s vylamovacími otvory s kabelovými vstupy pro vedení kabeláže a pro montáž ventilátorů	ANO	ANO
Kabelové vstupy opatřené dělenými kabelovými průchodkami s kartáči	ANO	ANO
Výškově stavitelné, vyrovnávací a odnímatelné nožky	ANO	ANO
Napájecí panel (PDU), zásuvky min. 12x UTE, 6x C13	2	ANO
Konzole (set) pro instalaci napájecího panelu	2	ANO
Boční třmen pro vedení kabelů se vstupy v úrovni každého U pro vedení kabelů v prostoru mezi 19“ lištami a bočnicí	2	ANO
Horizontální kabelové instalační lišty 1U, oboustranné, zakryté, s víkem	4	ANO
Monitoring stojanu (teplota, vlhkost, otevření dveří) napojení na dálkový dohled	ANO	ANO
Ventilační jednotka řízená termostatem, min. 2x ventilátor, jedna varianta montáže a) pod horní kryt, b) shora na horní kryt, c) do 19“ rámu pod horní kryt	1	ANO
Rám pro instalaci ventilační jednotky do horního rámu stojanu nebo do 19“ montážních lišt	1	ANO
Přívod kabelů a napájecích přívodů podle lokální dispozice (vrchem, resp. spodem stojanu)	ANO	ANO
Vodorovná police s montáží do 19“ rámu, min. hl. 350 mm	4	ANO
Souprava pro uzemnění stojanu	1	ANO
Zemnící lišta	1	ANO
Montážní příslušenství v ks (šroub M6, podložka, plovoucí matka)	50	ANO
Vyvazovací oko vertikální 40x50 mm	8	ANO
Průchozí panel 1U s kartáčem a vyvazováním	3	ANO
Záslepka 1U, 2U,3U (á 2ks), 4U, 6U (á 2ks)	ANO	ANO

3.5.2 Monitoring stojanu (STd)

Monitoring stojanu je požadováno osadit ve stojanech v modernizovaných lokalitách v množství uvedeném v kapitole 1.4 Technické specifikace. Je požadováno monitorovat teplotu, vlhkost, otevření dveří a dle nastavených parametrů zasílat poplachová hlášení. (U nově dodávaných stojanů je monitoring stojanu součástí specifikace stojanu).

Požadavky na monitoring stojanu jsou uvedeny v tabulce č. 22 Technické specifikace. Dále se požaduje kompatibilita se systémem DUPS (viz. kapitola 3.6 Technické specifikace), resp. plnohodnotná funkčnost STd k připojenému nadřazenému systému DUPS. Dále se požaduje nastavení posílání poplachových událostí do stávajícího serveru nadřazeného dohledového nástroje Zabbix pomocí protokolu SNMPv3.

Tabulka 23: Specifikace monitoringu stojanu

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Conteg
Produktové číslo (typ) nabízeného zařízení (pokud je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	RAMOS PLUS EXP
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení www odkazu	https://www.conteg.cz/userfiles/ramos-plus-technicky-list-conteg-cz-7d1b0489.pdf
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Velikost zařízení maximálně 1U	ANO	ANO
Sledování teploty, možnost nastavení min. a max. hranice	ANO	ANO
Sledování vlhkosti, možnost nastavení min. a max. hranice	ANO	ANO
Sledování otevření/zavření dveří	ANO	ANO
Kontrola vstupu (identifikace vstupu pomocí čipu, nebo kodem z klávesnice apod..)	ANO	ANO
SNMP v3	ANO	ANO

3.6 Záložní zdroj napájení (UPS180, UPS1,5r, UPS1,5t, UPS3r UPS3t)

UPS musí v objektu při přerušení dodávky napájení např. při výpadku rozvodu SN energie zabezpečit napájení všech napájených zařízení po definovanou dobu. Počet, typ a provedení zásuvek musí být dostatečný pro připojení požadovaných zařízení. U stojanových UPS (označení v názvu písmenem „r“) musí hloubka UPS vyhovovat rozměrům příslušného stojanu, tj. UPS včetně připojených kabelů musí umožnit zavření dveří stojanu. Samostatně stojící UPS je označena v názvu písmenem „t“.

Specifikace zařízení v jednotlivých lokalitách je zpracována s ohledem na rozměrová omezení takto:

- UPS1,5 *Záložní zdroj napájení 1,5 kW – stojanová UPS*: šířka 19“, max. hloubka 31 cm,
- UPS3 *Záložní zdroj napájení 3 kW – stojanová UPS*: šířka 19“, max. hloubka 67 cm,
- V případě nevyhovujícího prostoru ve stojanu je potom zvolena varianta *samostatně stojící UPS*.

Dodavatel navrhuje a zajišťuje (dodávkou potřebného materiálu a montážními pracemi včetně revizní zprávy) celou napájecí trasu od výstupů UPS až k zásuvkám napájecích zdrojů připojených technologií. Požadovanou délku zálohy garantuje Dodavatel po celou dobu záruky.

3.6.1 UPS objektová (UPS180)

Tabulka 24: Specifikace UPS objektové

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Schrack Technik
Produktové číslo (typ) nabízeného zařízení (pokud je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	USMPWPW300
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení www odkazu	UPS GENIO Dual Midi 3000VA/2700 W 5 min, 1/1f, VFI online - Online Shop: Schrack Technik spol. s r.o. Certifikáty https://www.schrack.cz/eshop/nouzove-osvetleni-ups-co/ups/rada-avara-10kva-az-1000kva/avara-multi-power-online-vfi-15-25-42-kva-kw-az-1-mw-3-3-faze/ups-avara-multi-power-skrin-s-max-7x-pm-25kw-nebo-7x-42kw-usmpwpw300.html?q=USMPWPW300
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Třífázový zdroj UPS- online s dvojí konverzí	ANO	ANO
Celkový výkon záložního zdroje UPS až 225 kVA	ANO	ANO
Doba zálohy při plné zátěži (180kW) minimálně po dobu 5 min	ANO	ANO
Jmenovité 3-fázové vstupní napětí 400 V	ANO	ANO
Rozsah vstupního napětí pro napájení z rozvodné sítě 340–477 V	ANO	ANO

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Vstupní účiník při plném zatížení - 0,99	ANO	ANO
Celkové vstupní harmonické zkreslení méně než 5 % pro plnou zátěž	ANO	ANO
Jmenovité výstupní napětí 230V, 400V 3fázové	ANO	ANO
Třífázové jmenovité výstupní napětí nastavitelné na 380, 400 nebo 415 V	ANO	ANO
Celkové zkreslení (THD) výstupního napětí <2 % pro lineání zátěž od 0 do 100 % a < 6 % pro plnou nelineární zátěž	ANO	ANO
Výstupní účiník výkonových modulů PF=1 (kVA = kW)	ANO	ANO
Centralizovaná architektura se společným statickým bypassem pro všechny výkonové moduly	ANO	ANO
Redundance výkonových modulů N+1	ANO	ANO
Výkonové moduly o výkonu 25kW nebo 30 kW, za provozu vyměnitelné	ANO	ANO
Maximální hmotnost výkonových modulů o výkonu 25 kW PF=1 do 30 kg na modul, maximální hmotnost výkonových modulů o výkonu 30 kW PF=1 do 35 kg na modul.	ANO	ANO
Modulární baterie vyměnitelné uživatelsky v online režimu	ANO	ANO
Maximální hmotnost modulárních baterií 30 kg	ANO	ANO
Modulární baterie plně monitorovatelné prostřednictvím záložního zdroje	ANO	ANO
Hlavní skříň UPS (bez baterií) o max. rozměrech: 42U(v) x 1200 mm (š) x 1100 mm(h) , barva černá	ANO	ANO
Bateriová skříň (samostatná) ve stejném provedení jako Hlavní skříň (rozměry, barva), perforované přední dveře.	ANO	ANO
V hlavní skříni musí být integrovány: -výkonové moduly -modulární výstupní distribuce – vyměnitelné ochranné prvky -statický bypass - řídící moduly s redundancí -síťová karta	ANO	ANO
Vyměnitelné jističové okruhy 1f/3f 16A/32A/63A s pevně připojenými napájecími kabely s koncovkou IEC 309 musí umožnovat měření odběru na výstupu, monitoring proudu na individuálním okruhu, musí umožňovat auto-detekci instalace jističového modulu nadřazeným systémem centrálního monitoringu (celkem 32ks 32A 1f jističů).	ANO	ANO
Redundantní vyměnitelné řídící moduly	ANO	ANO
Síťová karta musí být v UPS předinstalována a musí plnit min. následující funkce: -vzdálená správa pomocí Telnet a SSH protokolů, -možnost provozu v síti využívající protokol IPv6, -kompatibilní se všemi systémy UPS SmartSlot, -podpora Modbus TCP, -vzdálené aktualizace firmwaru zařízení UPS, -zasílání SNMP zpráv, splňuje specifikaci RFC 1628 MIB, -podpora produktů Radius, -podpora až čtyř přístupových úrovní oprávnění, -ochrana uživatelským heslem	ANO	ANO

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
UPS musí obsahovat další volnou pozici pro druhou síťovou kartu nebo kartu modbus/jbus, nebo kartu s beznapěťovými kontakty	ANO	ANO

3.6.2 UPS pro koncové lokality (UPS1,5r, UPS1,5t, UPS3r, UPS3t)

Tabulka 25: Specifikace UPS pro koncovou lokalitu

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Schrack Technik
Produktové číslo (typ) nabízeného zařízení (pokud je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	USPRD300--(3kVA) resp. USPRD150--(1,5kVA)

Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace v českém nebo anglickém jazyce	Uvedení www odkazu	https://www.schrack.cz/eshop/nouzove-osvetleni-ups-co/ups/rada-genio-online-0-7kva-az-10kva/genio-dual-midi-online-vfi-1000-az-3000-va-1-1-faze/ups-genio-dual-midi-3000va-2700w-5-min-1-1f-vfi-online-usprd300.html?q=USPRD300- https://image.schrackcdn.com/katalogseiten/k_usv_21_049-053_genio%20dual%20midi_usprd_en.pdf resp. https://www.schrack.cz/eshop/nouzove-osvetleni-ups-co/ups/rada-genio-online-0-7kva-az-10kva/genio-dual-midi-online-vfi-1000-az-3000-va-1-1-faze/ups-genio-dual-midi-1500va-1350w-5-min-1-1f-vfi-online-usprd150.html?q=USPRD150 https://image.schrackcdn.com/katalogseiten/k_usv_21_049-053_genio%20dual%20midi_usprd_en.pdf

Požadovaná vlastnost	**Způsob splnění požadované vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Provedení pro montáž do stojanu 19“ (neplatí pro vyjmenované případy umístění samostatně mimo stojan)	ANO	ANO
Hloubka zařízení umožní jeho vodorovnou montáž do stojanu hloubky 60 cm, a to včetně připojených kabelů tak, aby bylo možné dveře stojanu zavřít. (U zařízení 5kW platí obdobně pro hloubku stojanu 80 cm).	ANO	ANO
Výstupní výkon (UPS1,5r, UPS1,5t)	1500 VA (1200 W)	ANO
Výstupní výkon (UPS3r, UPS3t)	3000 VA (2500 W)	ANO
Výstupní výkon dostatečný pro 10 minut provozu napájené technologie	ANO	ANO
Vstupní jmenovité napětí	1x 230 V AC	ANO
Stabilita vstupního napětí	±20 %	ANO
Vstupní kmitočet	40÷70 Hz	ANO
Korekce vstupního účiníku	ANO	ANO
Výstupní napětí	1x 230 V AC	ANO
Stabilita výstupního napětí	statická <± 1 % dynamická <± 4 %	ANO
Zkreslení výstupního napětí při zatížení	lineárním <± 3 % nelineárním <± 5 %	ANO
Regulace výstupního napětí	ANO	ANO
Výstupní kmitočet (Hz)	50	ANO
Tolerance výstupního kmitočtu	<± 4 % (±2 Hz)	ANO
Max. výška zařízení	6 RU	ANO
Typ baterií bezúdržbový	ANO	ANO
Test baterií automatický a periodický (nastavitelný) a manuální z ovládacího panelu	ANO	ANO
Nouzové vypínání, ochrana proti přetížení	ANO	ANO
Komunikační modul pro dálkovou správu a dohled	ANO	ANO
SNMP v3	ANO	ANO
HTTPs management	ANO	ANO
Plná kompatibilita s dodávaným dohledovým systémem	ANO	ANO
Automatický bypass	ANO	ANO
Počet zásuvek dostatečný pro napájenou technologii, možno řešit přídavným napájecím kabelem PDU	ANO	ANO

3.7 Dohled UPS a jednotek monitoringu stojanů (DUPS)

S ohledem na požadavek provozní a technické kompatibility uvedený v kapitole 1.3.1 Technické specifikace (aktuálně provozovaný systém CPS) Objednatel připouští 2 varianty způsobu plnění:

1. Dodavatel zajistí rozšíření licence provozované instance CPS formou poskytnutí odpovídajícího počtu licence dle specifikace:

P/N	**Popis**

RMS-CPS-VS-25	Rozšiřující licence CONTEG Pro Server – pro 25 virtuálních senzorů

2. Dodavatel ve své nabídce uvede alternativní řešení, které splňuje dále uvedené požadavky.

Pro dohled UPS a jednotek monitoringu provozních podmínek ve stojanu je požadováno dodat v souladu s kap. 3.4.2 Technické specifikace dohledový systém, který bude centralizovaný a instalovaný na virtualizační platformě. Je požadována plná kompatibilita s dodávanými typy UPS a jednotek monitoringu stojanů a podpora všech jejich funkcionalit. Je požadováno zavedení všech dodaných komponent UPS a jednotek monitoringu stojanů do tohoto dohledu. Současně je požadováno nastavení posílání událostí do stávajícího serveru nadřazeného dohledového nástroje Zabbix pomocí SNMPv3.

Tabulka 26: Specifikace dohledu UPS a jednotek monitoringu stojanů

Požadovaná funkcionalita / vlastnost	Způsob splnění požadované funkcionality / vlastnosti	Doplní Dodavatel dle nabízeného zařízení
Výrobce zařízení	Uvedení výrobce	Conteg
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	RMS-DCIM-CPS-VS-25/5
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.conteg.com/userfiles/conteg-pro-server-extended-description-conteg-en-d3ba2e06.pdf
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Požadovaný formát zařízení	Virtuální server	ANO
Minimální počet spravovaných zařízení	1000	ANO
Možnost navýšení počtu spravovaných zařízení	ANO	ANO
Kompletní správa životního cyklu infrastruktury (nasazení, administrace, monitoring, odstraňování problémů)	ANO	ANO
Grafické web rozhraní pro správu	ANO	ANO
Podpora SNMPv1, SNMPv2, SNMPv3	ANO	ANO
Podpora autorizace a autentizace vůči RADIUS	ANO	ANO
Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení v souhrnném pohledu	ANO	ANO
Inventarizace nasazeného HW v síti	ANO	ANO

4 Implementace a zprovoznění ISŘP

Systém musí zajistit centrální správu základních sítových služeb, jako je DHCP, DNS, RADIUS a IPAM a dynamické řízení sítě. Modul pro správu IP adresního prostoru (IPAM) musí umožnit spolupráci se stávajícími systémy správy IP prostoru. Systém musí být plně kompatibilní s nástrojem AddNet, který je v síti MV ČR již provozován. Musí obsahovat integrované nástroje základních síťových služeb DNS, DHCP, RADIUS a L2 monitoring sítě (CIPAM, *Centrální IPAM*) specifikované v kap. 4.1 Technické specifikace a funkcionality NAC (*Network Access Control*) specifikované v kap. 4.2 Technické specifikace.

Požaduje se řešení, které integruje jednotlivé funkční nástroje a poskytuje unifikované a jednotné uživatelské rozhraní (GUI).

Systémové prostředky pro běh komponent ISPŘ jsou obecně označeny jako instance (1) řídicího serveru/serverů v centrální lokalitě (CS, jedná se o virtualizované instance) a (2) pracovního serveru/serverů v lokalitě WS (jedná se o fyzický HW v lokalitě), každý s virtualizovanou záložní instancí (WSv) v centrální lokalitě. Návrh systémových prostředků bude splňovat minimální požadavky uvedené v Tabulka 26 a bude výkonnostně dimenzován tak, aby zajistil funkčnost v prostředí Objednatele pro až 20000 koncových síťových zařízení (požadovaná licenční kapacita je uvedena v tabulce č. 26). Nabízené technické řešení navržené v souladu s vlastnostmi nabízené technologie popíše Uchazeč v nabídce.

Implementace a zprovoznění ISŘP se požaduje ve 2 etapách:

1. V rozsahu modernizované sítě (viz Místa plnění v tabulce č.1 této Technické specifikace) a jako součást implementace a zprovoznění nově pořizovaných aktivních prvků a lokalitních serverů a s přihlédnutím na požadavky v kap. 1.3.1 Technické specifikace ohledně začlenění provozovaných aktivních prvků bude zprovozněno dynamické řízení sítě, aniž to bude (v této etapě) vyžadovat integraci a funkční vazbu s MS AD a implementaci certifikátů (nebo analogických prostředků) v KZ. Dynamické řízení sítě je pro tento účel definováno jako funkcionalita *dynamického přiřazení IP adresy a VLAN autentizovanému koncovému* zařízení. Pravidla pro autorizaci a autentizaci přístupu do sítě jsou spravována v rámci komponent ISŘP a vynucována v kooperaci s aktivními prvky LAN.

   V této fázi se nepožaduje autentizace pomocí pokročilých metod 802.1x, dostačující je použití metody MAB (MAC Authentication Bypass) jakožto metody univerzální a základní. KZ, pro která budou vyžadovat výjimku z požadavku na dynamické přiřazení IP adresy a VLAN (jelikož např. nepodporují DHCP nebo vyžadují statickou konfiguraci portu přepínače), budou zdokumentována v Dokumentaci skutečného provedení (DSP).

   Koncová zařízení připojená do bezdrátové sítě WLAN v lokalitě jakožto i síťové prvky bezdrátové sítě WLAN (přístupové body, kontroléry) nebudou do ISŘP v této etapě integrovány.

   Z uvedeného je zřejmé, že součástí implementovaných komponent ISŘP musí být server s funkcionalitou AAA a že při implementaci a správě provozu je nutno udržovat evidenci MAC KZ autorizovaných pro připojení do sítě. Evidence MAC KZ bude zajištěna prostředky ISŘP, a to jak evidence aktuální (v reálném čase), tak historická (historie připojení KZ do sítě).

2. Následná etapa je specifikována v kap. Ověření prvků AAA. Bude navržena a pilotně ověřena optimální architektura a konfigurace pro prostředí MV ČR s využitím pokročilých metod AAA dle standardu 802.1x na bázi komponent, které jsou součástí dodávky ISŘP, viz podrobně kap. 6 této Technické specifikace.

Celková strategie Objednatele mající za cíl plošné rozšíření pokročilého řešení pro řízení přístupu do celé sítě MV ČR předpokládá povýšení, resp. rozšíření architekturního vzoru navrženého a pilotně ověřeného v rámci dodávky ISŘP do celé sítě v rámci následných projektů Objednatele.

4.1 Systém pro správu a řízení základních síťových služeb (CIPAM, CS, WS, WSv)

Tabulka 27: Specifikace systému pro správu a řízení základních síťových služeb

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Novicom s.r.o.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	AN-ES-10K
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.novicom.cz/addnet-tech-docs
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Systém musí obsahovat samostatný subsystém pro centrální správu a nastavení appliancí	ANO	ANO
Systém musí být schopen integrace se systémy pokročilé síťové analýzy (NBA) nebo SIEM	ANO	ANO
Systém musí obsahovat dostatečný počet všech licencí pro správu celkového počtu 10000 koncových zařízení	ANO	ANO
Systém musí umožňovat odesílání autentizačních informací uživatelům přes SMS bránu	ANO	ANO
GUI systému musí být k dispozici v českém a anglickém jazyce	ANO	ANO
Zabezpečení appliancí		
Zabezpečení appliancí umožňuje udržet konzistenci systémového prostředí po rebootu zařízení	ANO	ANO
flexibilní instalace systémového nastavení appliancí s využitím nástroje centrální správy	ANO	ANO
appliance musí mít dostatečné systémové zdroje pro zajištění provozu výše uvedeného funkčního rozsahu	ANO	ANO
Adresní plánování		
Nástroj pro návrh a definici IP adresního plánu s možností definice sítí, výběr konkrétní sítě a práce s ní	ANO	ANO
Systém musí podporovat v sítích možnost definice bloků adres, výběry dle bloků adres	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Systém musí podporovat import MAC/IP adres z online monitoringu sítě, automatický výběr správné sítě pro importované adresy	ANO	ANO
Systém musí podporovat import/export záznamů do/z adresního plánování v XML nebo CSV formátu	ANO	ANO
Systém musí podporovat automatické generování pravidel pro DHCP servery z adresního plánování	ANO	ANO
Systém musí podporovat automatické vytváření DNS záznamů z adresního plánování	ANO	ANO
Systém musí podporovat vytváření profilů dle sítí, po výběru profilu zobrazení a možnost práce pouze s IP adresami sítí daných profilem	ANO	ANO
Systém musí podporovat nástroj pro hromadné práce s definovanými skupinami zařízení a podporu krizového řízení	ANO	ANO
Systém musí podporovat možnost hierarchického rozdělení IP adresního prostoru mezi podřízené řídící servery a propagaci výseku adresního prostoru a vybraných politik na podřízené řídící servery. Z těchto serverů pak být schopen přebírat vybrané informace z monitoringu a prezentovat je v celkovém přehledu sítě	ANO	ANO
Plná kompatibilita systému s nástrojem AddNet	ANO	ANO
Monitoring sítě		
Systém musí podporovat monitoring na L2 vrstvě – MAC a IP adres v reálném čase, včetně toho, na kterém fyzickém portu přepínače se daná MAC adresa nachází, pokud přepínač tuto možnost poskytuje (na kterém portu kterého přepínače je připojené zařízení s danou MAC adresou), včetně podpory historie	ANO	ANO
Systém musí podporovat dostupnost monitoringu i v lokalitách, kde je přístup přes třetí vrstvu (routované lokality), data musí být online k dispozici přes uživatelské rozhraní na centrální lokalitě	ANO	ANO
Systém musí podporovat online sledování a vyhodnocení monitoringu ve formě: povolená dvojice MAC-IP, zakázaná dvojice MAC-IP, nekorektní DHCP MAC-IP, neznámá MAC-IP	ANO	ANO
Systém musí podporovat vypsání „mrtvých“ MAC nebo IP adres (adresy, které se v síti nevyskytly např. půl roku), s možností přes uživatelské rozhraní provést vymazání z DHCP, DNS a Radius záznamů a vrácení příslušných IP adres do adresního plánování	ANO	ANO
Systém musí podporovat export monitorovaných záznamů do XML nebo CSV	ANO	ANO
Integrovaný DHCP server		
Musí se jednat o distribuovaný DHCP systém s možností existence více DHCP serverů na stejné síti (redundance)	ANO	ANO
Systém musí podporovat centrální řízení a zakládání pravidel	ANO	ANO
Systém musí podporovat redundanci řídícího serveru, nezávislé na lokalitě	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Systém musí podporovat uživatelsky definované DHCP volby	ANO	ANO
Systém musí podporovat definice adresních skupin, k nim vázané DHCP volby	ANO	ANO
Systém musí podporovat vytvoření DHCP pravidla s vazbou více MAC na více IP adres	ANO	ANO
Systém musí podporovat možnost definice i statického záznamu (pro danou MAC není přidělovaná adresa DHCP serverem, pouze existuje záznam pro Radius server a monitoring, že daná MAC a IP adresa je na síti platná)	ANO	ANO
Systém musí podporovat možnost existence DHCP záznamů jedné MAC adresy ve více různých sítích – v každé síti obdrží daná MAC adresa přesně svou IP adresu z rozsahu dané sítě – cestující uživatelé	ANO	ANO
Systém musí podporovat automatické vytvoření/změna/smazání DHCP záznamu při operacích v adresním plánování	ANO	ANO
Systém musí podporovat automatickou propagaci MAC adres z DHCP záznamů v uživatelsky definovaném formátu do Radius serverů pro realizaci dalších bezpečnostních mechanizmů prostřednictvím aktivních prvků sítě (podpora heterogenních aktivních prvků pro 802.1x autentizaci)	ANO	ANO
Integrovaný DNS server		
Systém musí podporovat centrální řízení a zakládání pravidel	ANO	ANO
Systém musí podporovat automatické vytváření „A“ a PTR záznamů z adresního plánování	ANO	ANO
Centrální řídící server musí mít redundanci nezávislou na lokalitě	ANO	ANO
Systém musí podporovat možnost rozdělení zón na vnitřní a vnější pro stejnou zónu, definice vazby na vnitřní nebo vnější zónu dle IP adres (sítí) DNS klientů (klienti ve vnější sítí dostávají odpovědi pouze pro DNS záznamy z vnější zóny, klienti z vnitřní zóny dostávají DNS odpovědi pro vnitřní i vnější zónu)	ANO	ANO
Systém musí podporovat replikaci zvolených zónových souborů na podřízený DNS server	ANO	ANO
Systém musí podporovat automatického vytváření PTR reverzních záznamů při zakládání “A” záznamů	ANO	ANO
Systém musí nastavování oprávnění k zónovým souborům a SOA záznamům	ANO	ANO
Systém musí podporovat porovnání DNS z Adresního plánování s DNS záznamy na DNS serveru, včetně automatizovaného nástroje pro řešení rozdílů	ANO	ANO
Systém musí podporovat automatická kontrola existence reverzního záznamu k primárnímu A záznamu a naopak	ANO	ANO
Spolupráce s aktivními prvky		
Systém musí podporovat automatické zálohování konfigurací aktivních prvků	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Systém musí podporovat sledování výskytu MAC adres na portech s historií pro účely určení, kde se v daném čase vyskytuje nebo vyskytovala MAC adresa	ANO	ANO
Systém musí podporovat automatické repository – informace o verzi firmware, typu zařízení, S/N apod.	ANO	ANO
Systém musí podporovat sledování využití portů síťových prvků v čase – detekce nepoužívaných	ANO	ANO
Podpora BYOD a WiFi		
Podporovaná veškerá funkcionalita rovněž pro mobilní zařízení s přístupem přes WiFi	ANO	ANO
Podpora samoobslužného rozhraní pro automatizovanou IP správu nových zařízení v síti	ANO	ANO
Možnost vytváření recepčních zón pro zajištění přístupů návštěv (Guest zóna)	ANO	ANO
Rozsah implementace		
Zprovoznění systému adresní správy a přístupové politiky	ANO	ANO
Možnost integrace s AD	ANO	ANO
Centrální IPAM (CIPAM)		
Provoz centrálních systémových komponent na virtuální platformě	ANO	ANO
Možnost rozšíření licence pro IP koncová zařízení	ANO	ANO
Řídicí server/servery v centrální lokalitě (CS)		
Provoz na virtuální platformě	ANO	ANO
Pracovní server/servery v lokalitě (WS, WSv)		
Požaduje se konfigurace distribuovaného řízení síťových služeb, kdy dle konfigurace v lokalitě (Tabulka č. 3 Technické specifikace) bude provozována (a) samostatná hardwarová appliance s 1 aplikační instancí WS, nebo (b) dvě hardwarové appliance (každá se svojí aplikační instancí WS) pracující v zálohovacím režimu 1:1	ANO	ANO
WS musí využívat zabezpečený operační systém, musí být schopen poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti)	ANO	ANO
Minimální konfigurace HW appliance pro WS ve vzdálené lokalitě: 8c Atom, 16GB, 4x 1Gb Eth, 2x 960GB SSD, redundantní napájecí modul, dále veškeré nutné příslušenství a instalační materiál (síťové moduly, SFP, kabely a konektory potřebné k zapojení appliance do infrastruktury)	ANO	ANO
Provozované aplikační instance WS budou mít svojí provozní zálohu v architektuře 1:N v centrální lokalitě v rámci virtualizace (WSv). (Parametr N uvede Uchazeč v nabídce v souladu s technickými vlastnostmi nabízeného řešení).	ANO	ANO

4.2 Systém pro řízení přístupu (NAC)

Tabulka 28: Požadavky na systém pro řízení přístupu

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Novicom s.r.o.
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízení popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	AN-ES-10K
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.novicom.cz/addnet-tech-docs
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Systém pro řízení přístupu (NAC)		
Provoz centrálních systémových komponent na virtuální platformě	ANO	ANO
Možnost rozšíření licence pro IP koncová zařízení	ANO	ANO
Globální bezpečnostní politiky. Komunikace mezi bezpečnostními doménami má vždy procházet přes FW. Bezpečnostní domény (VLAN) mají být ukončeny na FW, kde lze per sub-interface definovat a vynucovat bezpečnostní politiku. FW pravidla pro řízení přístupů mezi doménami mají být definována globálně. Globální politika určuje prostupy mezi jednotlivými doménami, a to nezávisle na lokalitě.	ANO	ANO
Bezpečnost v rámci stejné domény. Zajištění bezpečnosti ve stejné doméně musí být možno realizovat mikrosegmentačními technikami aplikovanými dynamicky na přístupových aktivních prvcích v rámci řízení přístupů do sítě. Tyto mikrosegmentační politiky budou typicky určovat, jaká komunikace je povolena mezi zařízeními ve stejné bezpečnostní doméně. Bude tak možno např. blokovat komunikaci, po které se běžně šíří škodlivý kód, např. ransomware, a zabránit tak “nakažení“ zařízení mezi sebou, byť jsou ve stejné síti a připojené např. do stejného přístupového síťového prvku (přepínače).	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Centrální řízení. Správa globálních a mikrosegmentačních politik bude prováděna centrálně. Pro požadavky auditu musí být prováděné operace při řízení globálních a mikrosegmentačních politik auditovány takovým způsobem, aby auditní informace nemohly být obsluhou centrálního řízení modifikovány či vymazány a aby byla zajištěna možnost nezávislého auditu.	ANO	ANO
Požadavek na spolehlivost. Jednotlivé prvky realizující globální a mikrosegmentační politiky musí být schopny fungovat v režimu vysoké dostupnosti s vyloučením SPOF. Návrh řešení musí zohledňovat možnost vypracování jednotného plánu obnovy, který bude stejný pro všechny lokality.	ANO	ANO
Integrace s jinými systémy. Systémy realizující globální a mikrosegmentační bezpečnostní politiky musí být schopné integrace s návaznými systémy (SOC a SIEM) v takové míře, aby co nejvíce automatizovaly činnosti obsluhy a minimalizovaly nároky na odbornost obsluhy. Jedná se minimálně o možnost generování automatizovaných odkazů do ostatních systémů, např. možnost zobrazení detailu o zařízení, které bylo v důsledku konkrétní politiky omezeno, o zasílání informací na ostatní návazné systémy v uživatelsky definovaném tvaru, např. zaslání informace o tom, že nějaké zařízení bylo v rámci politiky zablokováno ve formátu vhodném pro SIEM.	ANO	ANO
Napojení na Microsoft Active Directory. Systémy realizující bezpečnostní politiky musí být schopné provádět autentizaci zařízení, případně autorizaci vstupu do sítě vůči MS AD. Zároveň musí poskytovat možnost efektivně spravovat politiky pro zařízení, které nemohou být v MS AD (jedná se typicky o zařízení, která nemohou v rámci NAC použít plné 802.1x, nemají suplikant pro využití plné 802.1x autentizace). Tato zařízení musí mít přístup do sítě (NAC) založen na základě jejich MAC adresy, a proto je třeba, aby celkové řešení bylo schopno detekovat pokusy o zneužití MAC adresy a zároveň poskytovalo informace pro obsluhu nutné k jednoznačné identifikaci takovýchto zařízení v síti.	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Řízení přístupu do sítě a model segmentace jako součást systému kybernetické bezpečnosti. Systém řízení přístupu do sítě musí být budován jako otevřený systém, který umožní využít standardní technologie běžných výrobců síťové správy na přístupové vrstvě. Rovněž musí být v maximální možné míře integrovatelný se systémem kybernetické ochrany. Musí umožnit nastavení speciální uživatelské role pro operátory bezpečnostního dohledu, kteří tak získají možnost okamžité reakce na incident. Tzn. mít možnost reagovat a provádět změny v nastavené přístupové politice bez nutné součinnosti se síťovými správci (například odpojení nebo izolace infikovaného zařízení). Pro maximální efektivitu mechanismu reakce na incident se požaduje, aby systém přístupu do sítě byl integrován s dalšími součástmi řízení sítě jako jsou IPAM, síťové služby DHCP/DNS a realtime L2 a DHCP monitoring. Tím bude umožněno sdílení kompletního nastavení IP politiky a řízení přístupu do sítě včetně nezbytného auditu činností síťových správců a možných externích bezpečnostních specialistů.	ANO	ANO
Integrovaná správa sítě a efektivita zajištění provozu. Pro zajištění co nejefektivnější provozní správy je přínosem využívání nástrojů síťové správy, které dokáží integrovat nástroje řízení IP politiky, základních síťových služeb a řízení přístupů do sítě, a to s maximální možnou funkční vazbou na další nástroje jako je správa uživatelů v prostředí MS AD, nástroje pro řízení privilegovaných přístupů, nástroje vizualizace assetů, monitoringu datových toků, log managementu a SIEMu. Integrovaná správa sítě zvyšuje efektivitu síťové správy a umožňuje její sdílení s bezpečnostními správci tak, aby byli schopni, bez ohrožení provozu, reagovat na incident samostatně (nezávisle). Současně se tímto snižují nároky na kvalifikaci obsluhy. Všechny činnosti běžné správy jsou nastaveny pro plnohodnotné zvládnutí síťovými operátory, tj. bez nutného zapojení vysoce kvalifikovaných síťových administrátorů. Integrovaná správa sítě musí být řešena jako plně heterogenní v tom smyslu, aby podporovala všechny běžné síťové technologie (minimálně na úrovni přístupové vrstvy), běžné klientské prostředí (MS, MAC, Linux a další) a rovněž si efektivně poradila s prostředky, které běžně nemají podporu síťového suplikanta pro 802.1x.	ANO	ANO
Dále jsou uvedeny požadované funkce integrovaného nástroje pro řízení sítě.		
Kabelová kniha. Umožňuje zobrazení vazby mezi portem přepínače a datovou zásuvkou na zdi tak, aby bylo možné kdykoli určit fyzickou lokalitu výskytu zařízení formou výpisu i grafické vizualizace.	ANO	ANO

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
L2 monitoring. Poskytuje v reálném čase informace o výskytu zařízení v síti a jejich fyzickém umístění. Tento monitoring je prováděn na úrovni L2 (IP/MAC/lokalita) a DHCP (DHCP události a otisky paketů). Vedle vyhodnocování v reálném čase musí být zajištěno rovněž ukládání těchto dat pro forenzní účely po dobu minimálně 12 měsíců.	ANO	ANO
Funkce IPAM. Součástí řešení musí být nástroj IP adresního plánování pro rozdělení sítě a nastavování základních parametrů základních síťových služeb (DHCP/DNS/NAC). Musí být integrován se síťovým monitoringem tak, aby bylo možné v reálném čase ověřování nastavení IP a přístupových pravidel.	ANO	ANO
Funkce DHCP. Požaduje se distribuovaný model DHCP služby, která v podpoří možnost přidělování IP adres z rezervací pro známá zařízení a podporuje automatizovanou správu a přihlašování důvěryhodných zařízení ve vzdálených lokalitách organizace.	ANO	ANO
Funkce DNS. Řešení musí umožnit distribuované DNS služby pro bezpečný interní i externí síťový provoz. Alternativně umožnit řízení externích DNS služeb (včetně MSAD) tak, aby integrovaný nástroj řízení sítě bylo možné využít jako primární místo informací pro nastavení síťového provozu.	ANO	ANO
Funkce NAC. Řešení musí poskytnout funkcionalitu pro řízení přístupu síťových zařízení do sítě s podporou autentizace a autorizace. Vedle běžných módů řízení sítě (802.1x a MAC autentizace) se požaduje i podpora pokročilejších technik mikrosegmentace za účelem řízení/omezení komunikace mezi zařízeními v rámci bezpečnostní domény (např. jako prevence šíření ransomware nákazy), integrace s DHCP a funkcionalita pro prevenci podvržení MAC adres. Systém musí podporovat omezení přístupu do domény nebo sítě mimo povolený časový rámec.	ANO	ANO
Distribuovaný model řídicích funkcí, redundance funkčních bloků, zachování provozních funkcí v lokalitě při přerušení komunikace s centrální lokalitou. Architektura systému pro řízení přístupů musí být v síťovém prostředí distribuována a navržena s redundancí z hlediska rozmístění.	ANO	ANO

4.3 Dohled ISŘP (ISŘPd)

Dohled komponent ISŘP a stavu služeb jím poskytovaných bude zajištěn ve vazbě na dohledové aplikace a provozní postupy zavedené v prostředí MV ČR.

Tabulka 29: Požadavky na dohled ISŘP

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.novicom.cz/addnet-tech-docs
Výrobce zařízení garantuje minimální dobu podpory produktové řady 5 let od doby ukončení prodeje produktu, ukončení prodeje produktu nebylo ohlášeno k termínu podání nabídky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.	ANO	ANO
Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).	ANO	ANO
Dohled zařízení (vrstva HW) pomocí protokolu SNMPv3 přes rozhraní IPMI zařízení, napojení na nadřazený dohledový systém.	ANO	ANO
Dohled komponent aplikační vrstvy umožňující ověřit provozní stav (funkčnost) poskytovaných základních síťových služeb ISŘP a stavu aplikační infrastruktury ISŘP.	ANO	ANO
Podpora protokolu syslog, odesílání zpráv do serveru syslog.	ANO	ANO
Dohled mezních provozních a bezpečnostních stavů, odesílání zpráv provozní obsluze mailovou službou.	ANO	ANO
Dohledované mezní stavy		
Zaplnění přiděleného DHCP rozsahu	ANO	ANO
Indikace žádosti o přístup neautorizovaným zařízením	ANO	ANO
Hlášení detekce události DHCP Reject (např. v důsledku konfliktu IP adres)	ANO	ANO
Porušení pravidel IP adresního plánu	ANO	ANO
Hlášení události NAC Reject (odmítnutí přístupu do sítě)	ANO	ANO

4.4 Podpora po dobu záruky

Součástí plnění bude zajištění technické a konzultační podpory po dobu záruky:

- při realizaci konfiguračních úprav a bezpečnostních nastavení,
- při instalacích nových verzí SW a bezpečnostních záplat,
- při změnách a rekonfiguracích v lokalitách,
- při řešení a analýze poruch a bezpečnostních incidentů,
- při plánování a návrhu rozvoje ISŘP.

Objem poskytované technické a konzultační podpory je omezen na 100 člověkodnů.

5 Rozšíření a integrace nástroje pro centrální správu identit a bezpečnostních politik

V rámci projektu ISŘP je nutné provést úpravy stávajícího nástroje pro správu uživatelských účtů a jejich oprávnění Identity & Access Management resortu MV ČR (IAM MVČR). Stávající systém IAM MVČR je postaven na technologii Microsoft Identity Manager Synchronization Service 2016 SP2 a portálu EasyIDM verze 4.3.

V rámci realizace ISŘP musí dojít k úpravě a rozvoji tohoto řešení tak, aby byly splněny požadavky kladené projektem ISŘP na systém IAM MVČR.

Součástí úprav bude:

- Architektura, návrh procesů
- Konfigurace a zprovoznění konektorů (včetně testování, migrace dat, aktualizace dokumentace)
- Vytvoření organizačních rolí na základě funkce uživatele v organizaci, odboru, oddělení a systemizované pozici automaticky na základě dat z EKIS

5.1 Architektura, návrh procesů

V rámci architektury a návrhu procesů budou realizovány tyto činnosti:

- Analýza požadavků projektu ISŘP na systém IAM MVČR
- Detailní návrh správy procesů realizovaných systémem IAM pro ISŘP obsahující minimálně:
    - Revize procesů správy životního cyklu uživatelských a administrátorských účtů u identit zaměstnanců MVČR z pohledu požadavků ISŘP
    - Rozšíření správy aplikací a zdrojů o aplikace a zdroje projektu ISŘP
    - Rozšíření správy aplikačních rolí o aplikační role aplikací a zdrojů ISŘP
    - Rozšíření správy organizačních a činnostních business rolí pro potřeby ISŘP s využitím modulu *Modul EasyIDM – automatická tvorba matice oprávnění* (MO)
    - Vytvoření matice oprávnění v souladu s politikou *ISMS 03.01.05.P02 Proces vytvoření matice oprávnění MV* na základě vstupních dat ISŘP s pomocí Modulu Easy IDM
    - Požadavky na doplnění reportů o reporty členství uživatelů v aplikačních rolích systémů používaných v rámci ISŘP a o reporty vazeb business rolí a aplikačních rolí systémů používaných v rámci ISŘP
- Návrh architektury upraveného systému IAM MVČR pro potřeby projektu ISŘP
- HW a SW požadavky na servery požadované pro realizaci druhé instance IAM MVČR v DC UPAAS a zajištění provozu systému v režimu vysoké dostupnosti ve dvou datových centrech MVČR

- Požadavky na prostupy mezi zdrojovými systémy, systémem IAM MVČR a řízenými systémy včetně uvedení portů
- Revize atribut flow mezi zdrojovými systémy, systémem IAM MVČR a řízenými systémy MVČR po úpravě systému IAM MVČR pro potřeby projektu ISŘP
- Detailní návrh harmonogramu realizace
- Návrh požadavků na součinnost ze strany MVČR v rámci realizace navržených úprav systému IAM MVČR.

Návrh bude zpracován v dokumentu *Analýza a návrh rozšíření a integrace nástroje pro centrální správu identit a bezpečnostních politik projektu ISŘP* schvalovaném vedením projektu ISŘP za stranu MVČR jako příloha Prováděcího projektu č.2 (viz kap. 8.1 Technické specifikace).

5.2 Konfigurace a zprovoznění konektorů (včetně testování, migrace dat, aktualizace dokumentace)

V rámci konfigurace a zprovoznění konektorů budou dodavatelem provedeny minimálně následující realizace:

- Konektor na Microsoft Active Directory *resortmv.cz*

a to dle schváleného dokumentu *Analýza a návrh rozšíření a integrace nástroje pro centrální správu identit a bezpečnostních politik projektu ISŘP.*

Dodavatel realizuje výstupy:

- Aktualizace nastavení portálu EasyIDM dle schváleného návrhu
- Aktualizace dokumentace systému IAM MVČR o procesy a popis nově instalovaných konektorů
- Testovací scénáře pro otestování konektorů a jejich potvrzení zástupcem MVČR potvrzující úspěšné otestování funkčnosti konektoru
- Školení administrátorů systému IAM MVČR na správu konektorů.
- Akceptační protokol potvrzující úspěšné nasazení a zprovoznění konektorů v produkčním systému IAM MVČR, aktualizaci dokumentace a školení administrátorů.

5.3 Vytvoření organizačních rolí na základě funkce uživatele v organizaci, odboru, oddělení a systemizované pozici automaticky na základě dat z EKIS

V rámci této části realizace Objednatel požaduje:

- Automatizované vytvoření vazby mezi BRO a aplikačními rolemi potřebnými pro výkon organizační činnosti pomocí modulu EasyIDM – automatická tvorba matice oprávnění, který vyčte aktuální přiřazení aplikačních rolí uživatelům v integrovaných systémech, provede návrh přiřazení aplikačních rolí do BRO a po schválení nastaví vazbu mezi aplikací, aplikační rolí a BRO.
- Aplikační role přiřazené mimo BRO bude možné sloučit do BRC. I pro BRC bude možné definovat pravidlo autoobsazení nebo konfigurovat schvalovací workflow pro přiřazení uživatele do BRC. Stejně tak bude u BRC možné automatizovaně přiřazovat aplikační role členů BRC do BRC s využitím modulu EasyIDM – automatická tvorba matice oprávnění,

který provede návrh aplikačních rolí na přiřazení do BRC a po jeho schválení přiřazení provede.

Dodavatel realizuje výstupy:

- Dodávka licence pro automatickou tvorbu matice oprávnění modulu EasyIDM ve verzi *No limit Licence*.
- Implementace automatické tvorby matice oprávnění; konfigurace pravidel pro automatické přiřazování aplikačních rolí systému zahrnutých do projektu ISŘP do BRO a BRC.
- Instalace do testovacího prostředí
- Vytvoření testovacích scénářů dle schváleného návrhu
- Realizace testu funkčnosti v testovacím prostředí IAM MVČR
- Instalace do produkčního prostředí
- Vytvoření matice oprávnění s využitím instalovaných konfigurací a komponent
- Aktualizace dokumentace systému IAM MVČR
- Školení administrátorů systému IAM MVČR na správu matice oprávnění
- Akceptační protokol potvrzují implementaci, úspěšné otestování a instalaci do produkčního prostředí, vytvoření matice oprávnění, aktualizovanou dokumentaci a školení administrátorů

5.4 Podpora po dobu záruky

Součástí plnění bude zajištění technické a konzultační podpory po dobu záruky:

- při realizaci konfiguračních úprav a bezpečnostních nastavení,
- při instalacích nových verzí SW a bezpečnostních záplat,
- při změnách v nastavení procesů,
- při řešení a analýze poruch a bezpečnostních incidentů,
- při plánování a návrhu rozvoje nástroje pro centrální správu identit.

Objem poskytované technické a konzultační podpory je omezen na 120 člověkodnů.

6 Ověření prvků AAA

Cílem ověření prvků AAA je navrhnout a pilotně ověřit optimální architekturu pro prostředí MV ČR s využitím pokročilých metod AAA dle standardu 802.1x na bázi komponent, které jsou součástí dodávky ISŘP.

Tyto módy budou zároveň porovnány s výchozím stavem podporujícím dynamickou správu sítě – MAC autentizací se zapnutou ochranou proti MAC promiskuitě.

Specifikace výsledného řešení včetně návrhu a doporučení postupu při implementaci bude zpracována formou Technické zprávy *Ověření prvků AAA s využitím metod dle 802.1x*.

Tabulka 30: Požadavky na ověření prvků AAA

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní Dodavatel dle nabízeného zařízení**
PEAP – uživatelská autentizace (jméno, heslo)	ANO	ANO
PEAP – autentizace zařízení (ID, dynamicky generované klíče)	ANO	ANO
TLS – autentizace uživatelským certifikátem	ANO	ANO
TLS – autentizace certifikátem zařízení	ANO	ANO

7 Vyčlenění části služeb SIP

Sjednocené informační prostředí (SIP) MV ČR je komplexní informační systém navržený k integraci a správě různých datových a komunikačních systémů používaných v rámci resortu. Cílem SIP je zajistit efektivní a bezpečný tok informací mezi jednotlivými složkami a odděleními MV ČR. SIP zajišťuje centralizaci různých datových a aplikačních zdrojů, což vede k lepší správě a dostupnosti informací pro všechny relevantní uživatele. Poskytuje jednotnou platformu pro ukládání, sdílení a správu dokumentů, záznamů a dalších důležitých dat. SIP zahrnuje pokročilé bezpečnostní mechanismy pro ochranu dat a komunikací, včetně autentizace uživatelů, šifrování dat a monitorování přístupu k citlivým informacím. Je navržen tak, aby mohl být integrován s dalšími externími informačními systémy a aplikacemi, což zajišťuje interoperabilitu a umožňuje snadnou výměnu informací mezi různými platformami. SIP také poskytuje nástroje pro analýzu a vizualizaci dat, což podporuje rozhodovací procesy na všech úrovních řízení v rámci MV ČR a zjednodušuje různé administrativní a operativní procesy tím, že automatizuje rutinní úkoly a zlepšuje komunikaci mezi odděleními MV ČR.

Objednatel požaduje realizaci následujících činností ve vztahu k posílání kybernetické ochrany níže uvedených části SIP.

7.1 Přenesení služeb AD do prostředí UPAAS

Objednatel požaduje rozšíření infrastruktury Active Directory (AD) pro domény *mvcr.cz*, *resortmv.cz*, *exresortmv.cz*. Cílem je přidání dvou nových řadičů AD do lokality UPAAS, čímž vzniknou celkem čtyři řadiče, které budou navzájem replikovány. Tato změna je nezbytná pro zvýšení dostupnosti a redundance AD infrastruktury.

7.1.1 Současný stav

Architektura Active Directory

- Aktuální infrastruktura zahrnuje vždy dva řadiče AD pro domény *mvcr.cz*, *resortmv.cz*, *exresortmv.cz* umístěné v různých geografických lokalitách.
- Active Directory foresty a domény jsou následující:
    - Forest, tree a doména *mvcr.cz* – obsahuje objekty subjektu MV ČR.
    - Forest, tree a doména *resortmv.cz* – sdílená doména, která byla vytvořena během realizace projektu SIP. Obsahuje objekty provozovaných serverů a linkovaných účtů z domény mvcr.cz, na které jsou vázány emailové schránky.
    - Forest a doména *exresortmv.cz* – sdílená doména, která byla vytvořena během realizace projektu CMS (Centrální místo služeb). Obsahuje objekty třetích stran

(externí subjekty, dodavatelé apod.), kterým je nutno poskytnout přístup k prostředkům v doméně resortvm.cz.

Replikace

- Replikace mezi současnými nody probíhá pomocí standardních AD replikací.

Bezpečnostní aspekty

- Přístup k AD je chráněn pomocí základních bezpečnostních opatření.

Monitoring a správa

- Monitoring a správa AD probíhá pomocí interních nástrojů a služeb.

7.1.2 Požadavky na nový systém

Rozšíření infrastruktury AD

- Přidání dvou nových nodů AD pro jednotlivé domény *mvcr.cz*, *resortmv.cz*, *exresortmv.cz* do lokality UPAAS.

Replikace

- Zajištění replikace mezi všemi čtyřmi nody každé domény, aby byla zajištěna vysoká dostupnost a redundance.

Bezpečnostní opatření

- Implementace pokročilých bezpečnostních opatření pro ochranu přístupu k AD.

Monitoring a správa

- Zajištění monitoringu a správy všech nodů AD pomocí moderních nástrojů a služeb.

Podpora výrobce

- Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.
- Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).

SW licence po ukončení záruky

- licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).

Tabulka 31: Specifikace požadavků na přenesení služeb AD do prostředí UPAAS

Technický parametr / aspekt	Současný stav	Požadovaný přechodný stav	Cílový stav	Jak toho Dodavatel dosáhne
Architektura AD	2 nody AD v různých geografických lokalitách	Přidání 2 nových nodů do lokality UPAAS pro každou doménu (*mvcr.cz*, *resortmv.cz*, *exresortmv.cz*)	4 nody AD, vzájemně replikované pro každou doménu (*mvcr.cz*, *resortmv.cz*, *exresortmv.cz*)	Konfigurace a nasazení nových nodů AD do lokality UPAAS. Využití virtuálních strojů s přidělenými parametry.
Replikace	Standardní AD replikace	Zajištění replikace mezi všemi nody jednotlivých domén	Vysoce dostupná a redundantní replikace	Zajištění standardní AD replikace mezi všemi nody každé domény. Ověření funkčnosti v

				rámci testovacího plánu.
Bezpečnostní opatření	Základní bezpečnostní opatření	Implementace přechodných opatření	Pokročilá bezpečnostní opatření	Implementace pokročilých bezpečnostních opatření dle požadavků zadavatele. Zajištění řízení přístupu, aktualizací a odolnosti vůči hrozbám. Nastavení zálohování a plánu pro obnovu pomocí moderních nástrojů.
Monitoring a správa	Interní nástroje a služby	Modernizace monitoringu a správy	Moderní nástroje pro monitoring a správu	Nasazení moderních nástrojů pro monitoring a správu AD infrastruktury.

Objednatel vyčlení pro realizaci rozšíření AD šest virtuálních strojů v prostředí UPAAS. Každý z těchto strojů bude mít 4 jádra, 32 GB RAM a 500 GB SSD diskového prostoru. Objednatel vyčlení aktuální verzi Windows Server Datacenter pro výše uvedené virtuální prostředí.

7.1.3 Migrační strategie

Plán rozšíření

- Dodavatel předloží v rámci Prováděcího projektu č.1 (viz kap. 8.1 Technické specifikace) detailní časový harmonogram rozšíření infrastruktury zahrnující přípravné kroky, přidání nových nodů a konfiguraci replikace.

Postup bude zahrnovat minimálně:

Postupy pro přidání nových nodů

- Konfigurace a nasazení nových nodů AD do lokality UPAAS.
- Zajištění replikace mezi všemi čtyřmi nody.

Testování a ověřování

- Plán testování funkčnosti a výkonu nové infrastruktury po přidání nových nodů.

Plán obnovy a zotavení

- Postupy pro obnovu dat a provozu v případě výpadků. Plán zálohování a archivace konfigurací AD.

7.1.4 Požadavky na dokumentaci a školení

Specifikace potřebné dokumentace

- Detailní technická dokumentace k novému prostředí. Dokumentace postupů pro přidání nodů a konfiguraci replikace.

Požadavky na školení

- Školení administrátorů (L2 a L3) pro správu nové infrastruktury. Školení L1 podpory pro uživatele.

7.2 Dodávka, instalace a zprovoznění Poštovního serveru (on-prem) v prostředí UPAAS (MAIL)

Objednatel požaduje migraci infrastruktury Exchange z prostředí Policie ČR do nového, samostatného prostředí. Tato migrace je nezbytná pro zlepšení provozní efektivity, zvýšení bezpečnosti a škálovatelnosti IT infrastruktury. Předmětem níže uvedeného zadání je popis požadavků na vlastnosti nového řešení.

7.2.1 Současný stav

Architektura Exchange Serverů

- Aktuální infrastruktura je postavena na Exchange 2019 v režimu vysoké dostupnosti a je provozována na VMware platformě.
- Active Directory zahrnuje mimo jiné foresty *mvcr.cz*, *resortmv.cz* a *exresortmv.cz*.

Licencování

- Používané licence zahrnují Exchange server Enterprise, licencované pomocí EA Windows Server Datacenter.

Vysoká dostupnost a redundance

- Vysoká dostupnost je zajištěna pomocí VMware HA, geograficky oddělených datových center a DNS balancování.

Struktura uživatelských účtů a mailboxů

- Konfigurace linked mailboxů, synchronizace účtů mezi foresty mvcr.cz a resortmv.cz přes Azure AD connect.

Bezpečnostní aspekty

- Přístup přes Outlook a OWA z veřejného internetu není zabezpečený MFA. Monitoring a správa je prováděna pomocí DCeGOV SIEM.

Zálohování a archivace

- Denní zálohování pomocí Veeam Backup & Replication. Archivace pomocí Retain for Exchange.

Analýza současného stavu

- Administrátoři nemají přístup k fyzické a virtualizační platformě. Nedostatečná kapacita mailboxů.

7.2.2 Požadavky na nový systém

Architektura Exchange Serverů

- Přechod na nové Exchange servery s konfigurací DAG, VMware prostředím a optimalizovanou topologií Active Directory.

Licencování

- Zajištění nových licencí pro Exchange servery a všechny uživatele.

Vysoká dostupnost a redundance

- Implementace moderních mechanismů pro vysokou dostupnost a redundanci. Objednatel disponuje pro dané účely řešením WAF F5, které požaduje, aby bylo použito pro funkci Load balanceru, Failover, Reverzní proxy .

- Využití funkce Managed Availability pro monitorování klíčových komponent a služeb poštovního systému.

Struktura uživatelských účtů a mailboxů

- Migrace všech uživatelských účtů a mailboxů na nové prostředí. Každý uživatel bude mít mailbox o velikosti 10 GB.

Bezpečnostní aspekty

- Použití protokolu minimálně TLS 1.2 (s podporou pro TLS 1.3) pro komunikaci mezi Exchange servery a klienty.

Objednatel požaduje nejnovější postupy pro zabezpečení serverů Exchange, včetně konfigurace firewallu, řízení přístupu a monitorování bezpečnostních událostí. Důraz bude kladen na implementaci aktualizací, správu oprávnění a nasazení kryptografických standardů pro šifrování komunikace.

Dodavatel musí věnovat pozornost zodolnění prostředí Exchange, s důrazem na minimalizaci útoků a snížení rizik spojených s potenciálními hrozbami a analyzovat a doporučit nastavení pro zvýšení odolnosti proti neoprávněným přístupům a útokům.

Souhrn požadavků Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) na Exchange prostředí vztahující se k provozu dat a přístupů MV ČR, které je Dodavatel povinen zohlednit:

- Akt o kybernetické odolnosti – Tento akt stanovuje společný postoj k bezpečnostním požadavkům na digitální produkty, včetně těch, které jsou připojeny k internetu. Cílem je zajistit, že tyto produkty jsou před vstupem na trh bezpečné a chrání podniky a spotřebitele před kybernetickými hrozbami.
- Vyhláška č. 315/2021 Sb. – Tato vyhláška se týká bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci.

Zálohování a archivace

- Modernizace zálohovacích a archivačních postupů. Zajištění vyšší dostupnosti a bezpečnosti archivačního systému. Dodání licencí pro zálohování a archivaci.
- Sestavení plánů pro archivaci, zálohování. Nastavení těchto plánů.
- Implementace funkce Litigation Hold poštovního systému.
- Software pro zálohování Exchange musí umožňovat obnovení položek do původního umístění (do mailboxu/složky uživatele) a na úrovni jednotlivých položek. Software musí umožňovat vytvoření samoobslužného portálu pro obnovu položek vybraným uživatelům nebo správcům organizace.

Koexistence se stávajícím Exchange prostředím – foresty

- Sdílení availability informací, autodiscovery redirect a mailflow včetně SMTP relay pro neomezenou komunikaci.
- Nové prostředí musí mít své unikátní uspořádání. Cname musí být přeložitelné a dostupné ze všech forestů.
- Směřování pošty, která je zasílána z PČR na MV ČR interní zabezpečenou cestou přímo mezi partnerskými Edge servery.

Podpora výrobce

- Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu záruky.
- Přístup k asistenčnímu centru výrobce a k aktuálním či opravným verzím Software po dobu 2 let po ukončení záruky (Pozáruční plnění).

SW licence po ukončení záruky

- licenční zajištění SW min. po dobu 2 let po ukončení záruky (Pozáruční plnění).

Tabulka 32: Specifikace poštovního serveru

Technický parametr / aspekt	Současný stav	Požadovaný přechodný stav	Cílový stav	Jak toho Dodavatel dosáhne
Architektura Exchange Serverů	Exchange 2019, DAG, VMware	Optimalizovaná konfigurace DAG	Nové Exchange servery, DAG, optimalizovaná AD topologie	Implementace nové topologie s DAG, optimalizací pro dvě lokality, využití čtyř vyhrazených VM.
Licencování	Enterprise a Standard, EA Windows Server Datacenter	Zajištění přechodných licencí	Nové licence pro Exchange servery (vysoká dostupnost) a uživatele (3600 uživatelů)	Zajištění potřebných licencí pro Exchange servery i 3600 uživatelů včetně pozáručního krytí.
Vysoká dostupnost a redundance	VMware HA, geografická redundance, DNS balancování	Zajištění přechodných mechanismů	Moderní mechanismy pro vysokou dostupnost a redundanci. Využití Site resilience clusteru v módu Active/Active. Provoz ve dvou lokalitách.	Nasazení Site Resilience Clusteru v režimu Active/Active, využití WAF F5 pro LB, Failover, Reverzní proxy.
Struktura uživatelských účtů	Linked mailboxy, synchronizace přes Azure AD connect	Migrace uživatelských účtů	3600 uživatelů, mailboxy o velikosti 10 GB	Migrace účtů pomocí New-MoveRequest, zajištění koexistence přes autodiscover, SMTP relay, přenos dat mezi foresty.
Bezpečnostní aspekty	Bez MFA, monitoring přes DCeGOV SIEM	Implementace přechodných bezpečnostních opatření	Pokročilá bezpečnostní opatření. Primární komunikační protokoly MAPI/https a OWA/https.	Zavedení TLS 1.2+/1.3, konfigurace firewallu, řízení přístupu, aktualizace, nasazení šifrování a protokolů MAPI/HTTPS, OWA/HTTPS.
Zálohování a archivace	Denní zálohování pomocí Veeam	Modernizace zálohovacích postupů	Moderní zálohovací a archivační systém – licence, implementace.	Použití softwaru s možností granulární obnovy dat a

	Backup & Replication			objektů, zavedení Litigation Hold, portál pro obnovu dat, archivační systém s licencemi.

Objednatel vyčlení pro realizaci migrace Exchange čtyři virtuální stroje v prostředí UPAAS. Dva z těchto strojů budou mít 16 jader, 64 GB RAM a 20 000 GB SSD diskového prostoru. Další dva z těchto strojů budou mít 8 jader, 32 G RAM a 1 000 GB SSD diskového prostoru. Objednatel vyčlení aktuální verzi Windows Server Datacenter pro výše uvedené virtuální prostředí.

7.2.3 Migrační strategie

Plán migrace

Dodavatel předloží v rámci Prováděcího projektu č.1 (viz kap. 8.1 Technické specifikace) detailní časový harmonogram migrace zahrnující přípravné kroky, samotnou migraci a testování.

Postup bude zahrnovat minimálně:

Postupy pro migraci dat

- Použití nativního přenosu New-MoveRequest pro migraci mailboxů mezi organizacemi. Zajištění koexistence mezi foresty během migrace, včetně konfigurace mailflow a autodiscover.

Testování a ověřování

- Plán testování funkčnosti a výkonu nové infrastruktury před a po migraci. Ověření správné funkčnosti nových Exchange serverů a migračních postupů.

Plán obnovy a zotavení

- Postupy pro obnovu dat a provozu v případě výpadků. Plán zálohování a archivace schránek.

7.2.4 Požadavky na dokumentaci a školení

Specifikace potřebné dokumentace

- Detailní technická dokumentace k novému prostředí. Dokumentace migračních postupů a plánů obnovy.

Požadavky na školení

- Školení administrátorů (L2 a L3) pro správu nového prostředí. Školení L1 podpory pro uživatele.

7.2.5 Podpora po dobu záruky

Součástí plnění bude zajištění technické a konzultační podpory po dobu záruky:

- při realizaci konfiguračních úprav a bezpečnostních nastavení,
- při instalacích nových verzí SW a bezpečnostních záplat,
- při změnách a rekonfiguracích v lokalitách,
- při řešení a analýze poruch a bezpečnostních incidentů,

- při plánování a návrhu rozvoje.

Objem poskytované technické a konzultační podpory je omezen na 180 člověkodnů.

7.3 Dodávka, instalace a zprovoznění Prostředí pro sdílení (on-prem) pro vybrané uživatele MV ČR v prostředí UPAAS (PS)

Objednatel požaduje dodávku a implementaci nového on-premise řešení, které bude sloužit jako sdílený pracovní prostor pro 50 uživatelů. Toto řešení bude primárně využito pro ověření integrace s EasyIDM v rámci projektu. Předmětem níže uvedeného zadání je popis požadavků na vlastnosti nového řešení.

7.3.1 Současný stav

Aktuálně neexistuje žádné sdílené pracovní prostředí, které by splňovalo požadavky na integraci s EasyIDM a poskytovalo funkce potřebné pro týmovou spolupráci a správu dokumentů.

7.3.2 Požadavky na nové řešení

Kolekce webů pro týmy

- Možnost vytváření a správy týmových webů, které umožní jednotlivým týmům spolupracovat na projektech, sdílet dokumenty a komunikovat.

Sdílený pracovní prostor

- Poskytnutí sdíleného pracovního prostoru, kde budou moci uživatelé sdílet a spravovat dokumenty, úkoly a kalendáře.

Integrace s EasyIDM

- Plná integrace s EasyIDM pro správu uživatelských účtů a oprávnění.

Správa dokumentů

- Funkcionalita pro verze dokumentů, kontrolu přístupu a auditování aktivit s dokumenty.

Uživatelsky přívětivé rozhraní

- Intuitivní a uživatelsky přívětivé rozhraní, které umožní snadné používání a správu obsahu bez potřeby pokročilých technických znalostí.

Bezpečnostní opatření

- Implementace pokročilých bezpečnostních opatření pro ochranu dat a uživatelských informací.
- Přístup bude umožněn ze sítě internetu, DMZ. Mohou být použity důvěryhodné externí identity pro autentizaci uživatelů.

Škálovatelnost

- Možnost rozšíření řešení pro případné zvýšení počtu uživatelů nebo rozšíření funkcionalit. Předpokládaný počet uživatelů po rozšíření je 5000.

7.3.3 Plán implementace

Dodavatel předloží v rámci Prováděcího projektu č.1 detailní časový harmonogram implementace nového řešení zahrnující přípravné kroky, nasazení a testování. Postup bude zahrnovat minimálně:

Postupy pro nasazení

- Postupy pro konfiguraci a nasazení nového řešení, včetně nastavení integrace s EasyIDM.

Testování a ověřování

- Plán testování funkčnosti a výkonu nového řešení po jeho nasazení. Ověření správné funkčnosti a integrace s EasyIDM.

Plán obnovy a zotavení

- Postupy pro obnovu dat a provozu v případě výpadků. Plán zálohování a archivace dat.

7.3.4 Požadavky na dokumentaci a školení

Specifikace potřebné dokumentace

- Detailní technická dokumentace k novému prostředí. Dokumentace postupů pro nasazení a konfiguraci.

Požadavky na školení

- Školení administrátorů (L2 a L3) pro správu nového prostředí. Školení L1 podpory pro uživatele.

Tabulka 33: Specifikace prostředí pro sdílení

Technický parametr / aspekt	Cílový stav	Jak toho Dodavatel dosáhne (software, cesta)
Kolekce webů pro týmy	Možnost vytváření a správy týmových webů	Nasazení SharePoint Server (on-premise) s aktivovanou funkcí Team Sites; jednotlivé týmy budou moci spravovat vlastní kolekce webů.
Sdílený pracovní prostor	Poskytnutí sdíleného pracovního prostoru	Využití SharePoint Team Sites pro sdílení souborů, seznamů, kalendářů a úkolů v rámci projektového týmu.
Integrace s EasyIDM	Plná integrace s EasyIDM	Propojení SharePointu s EasyIDM přes AD synchronizaci a přidělování oprávnění dle rolí.
Správa dokumentů	Verze dokumentů, kontrola přístupu, auditování	SharePoint umožňuje nativní správu verzí dokumentů, řízení přístupu (ACL), práci s metadata, retention policies a auditní logy pro sledování akcí.
Uživatelsky přívětivé rozhraní	Intuitivní a uživatelsky přívětivé rozhraní	Webové rozhraní SharePointu s podporou pro moderní UI (v nové verzi), integrace s Office aplikacemi a možností přizpůsobení vzhledu podle potřeb uživatelů.
Bezpečnostní opatření	Pokročilá bezpečnostní opatření	Využití role-based access control, možnost autentizace externích identit, šifrování přenosu (HTTPS), propojení s WAF/DMZ, auditní logy.
Škálovatelnost	Možnost rozšíření počtu uživatelů a funkcionalit	SharePoint Server podporuje horizontální škálování (více frontend a backend serverů), rozšíření pro další uživatele (až 5000 a více) pomocí webových aplikací a service aplikací.

Objednatel vyčlení pro realizaci Prostředí pro sdílení dva virtuální stroje v prostředí UPAAS. Každý z těchto strojů bude mít 4 jádra, 32 GB RAM a 500 GB SSD diskového prostoru. Objednatel vyčlení aktuální verzi Windows Server Datacenter pro výše uvedené virtuální prostředí.

8 Technické návrhy, zprávy a dokumentace

8.1 Projektová dokumentace

Je požadováno zpracování projektové dokumentace na úrovni prováděcího projektu a dokumentace skutečného provedení. Projektová dokumentace musí být zpracována v českém jazyce. Technická dokumentace, odkazy na technickou a doporučenou dokumentaci výrobce mohou být v českém nebo anglickém jazyce. Dokumentaci je požadováno dodat v editovatelné elektronické podobě.

Dokumentace požadovaná v rámci této veřejné zakázky se dělí na dvě projektové fáze Výstavba a Předání:

8.1.1 Výstavba

V rámci této fáze požaduje Objednatel zpracování Prováděcího projektu č.1 v rozsahu:

- architektura, specifikace zařízení pro jednotlivé lokality včetně příslušenství a instalačního materiálu,
- vytvoření detailních konfigurací aktivních prvků,
- průzkum lokality s proměřením signálu (site survey) a návrh rozmístění přístupových bodů (viz kap. 3.2.9),
- specifikace požadavků na součinnost a připravenost jednotlivých lokalit k realizaci,
- plán postupného přechodu a časový harmonogram ze stávajícího do cílového stavu,
- sady testovacích scénářů, kterými Dodavatel prokáže, že předmět plnění je proveden v souladu s dokumentací a odpovídá požadovaným funkcionalitám v zadávací dokumentaci,
- časový harmonogram rozšíření infrastruktury AD (viz kap. 7.1.3 Technické specifikace),
- časový harmonogram migrace Poštovního serveru (viz kap. 7.2.3 Technické specifikace),
- časový harmonogram implementace nového řešení Prostředí pro sdílení (viz kap. 7.3.3 Technické specifikace).

V rámci této fáze požaduje Objednatel dále zpracování Prováděcího projektu č.2 v rozsahu:

- analýza a návrh rozšíření a integrace nástroje pro centrální správu identit a bezpečnostních politik projektu ISŘP (viz kap. 5 Technické specifikace),

8.1.2 Předání

V rámci této fáze požaduje Objednatel zpracování Dokumentace skutečného provedení (DSP) a provozní dokumentace v rozsahu:

- vytvoření typizovaných šablon konfiguračních postupů s ohledem na konfigurované funkcionality,
- dokumentaci fyzické instalace a zapojení zařízení v jednotlivých lokalitách včetně kabeláže,

- vytvoření podkladů pro inventarizaci zařízení v jednotlivých lokalitách (detailní informace o zařízení – fyzická instance/virtuální zařízení, výrobní číslo, produktový tzv. part number, číslo chassis a instalovaných modulů v zařízení),
- v případě virtualizovaných strojů dokumentace přidělených HW prostředků,
- dokumentace SW verzí aktivních prvků,
- předání technické dokumentace výrobce sloužící ke konfiguraci a diagnostice chybových stavů,
- dokumentace nastavené IP adresace.

Objednatel požaduje předání projektové dokumentace vždy k ukončení příslušné projektové fáze, tzn. předání Prováděcího projektu č.1 nebo č.2 ve fázi Výstavba a předání Dokumentace skutečného provedení včetně podkladů pro tvorbu provozní a bezpečnostní dokumentace ve fázi Předání. Přechod z jedné fáze do druhé bude možný vždy po akceptaci předané projektové dokumentace dané fáze.

Součástí předávky Objednateli jsou dále technické návrhy a zprávy k jednotlivým projektovým výstupům uvedené v kap. 1.2.7., 7.1.4, 7.2.4 a 7.3.4 Technické specifikace.

9 Školení

Jako součást předmětu plnění je požadováno zajistit do Konečného termínu plnění ve smyslu čl. 4 odst. 3 písm. e) Smlouvy školení pro pracovníky Objednatele a dalších Objednatelem určených osob v následujícím rozsahu:

- **Školení pro specialisty Provozu LAN** - 6 pracovníků
  - Náplní školení bude zejména zajištění chodu LAN/WAN infrastruktury, rekonfigurace zařízení, lokalizace a odstraňování závad, pravidelné aktualizace SW prostředků.
  - Časový rozsah školení min 16 hodin.
- **Školení pro specialisty platformy ISŘP** – 3 pracovníci
  - Náplní školení bude zejména správa a administrace platformy ISŘP.
  - Časový rozsah školení min 32 hodin.
- **Školení pro specialisty správy koncových zařízení** – 6 pracovníků
  - Náplní školení bude zejména ovládání dodávaných aplikací a metodické postupy připojování KZ do sítě
  - Celkový časový rozsah školení min 32 hodin.
- **Školení pro koncové uživatele Telefonních systémů**
  - Základní uživatelské školení formou prezentace nebo videa nebo webcastu pro uživatele telefonních přístrojů.
- **Školení administrátorů systému IAM MVČR** – 2 pracovníci
  - Školení v oblasti správy matice oprávnění systému IDM
  - Celkový časový rozsah školení min 8 hodin.

- **Školení administrátorů systému AD MVČR** – 2 pracovníci
  - Školení v oblasti L2, L3 podpory
  - Školení L1 podpory pro uživatele
  - Celkový časový rozsah školení min 8 hodin.
- **Školení administrátorů Poštovního serveru** – 2 pracovníci
  - Školení v oblasti L2, L3 podpory
  - Školení L1 podpory pro uživatele
  - Celkový časový rozsah školení min 8 hodin.
- **Školení administrátorů Prostředí pro sdílení** – 2 pracovníci
  - Školení v oblasti L2, L3 podpory
  - Školení L1 podpory pro uživatele
  - Celkový časový rozsah školení min 8 hodin.

10 Další podmínky plnění

- Nedílnou součástí plnění je instalace, zprovoznění a kompletní konfigurace všech dodávaných komponent.
- Instalace PoE switchů do stávajících stojanů představuje jejich osazení do pozic stávajících zařízení v provozu. Instalaci / obměnu je požadováno realizovat v úzké spolupráci s místním technikem v předmětné lokalitě za součinnosti Objednatele s minimálním dopadem na provoz zařízení, a to v předem dohodnutém čase v souladu s Prováděcím projektem č.1.
- Instalace nových stojanů představuje v případech uvedených v kapitole 1.4 Technické specifikace obměnu stávajícího stojanu. Je požadována demontáž stávajícího stojanu a přemístění stávajících zařízení do nově dodávaného stojanu. Instalaci / obměnu je požadováno realizovat v úzké spolupráci s místním technikem v předmětné lokalitě za součinnosti Objednatele s minimálním dopadem na provoz, a to v předem dohodnutém čase v souladu s Prováděcím projektem č.1.
- Pro primární napájení zařízení z UPS je požadováno dodání dostatečného počtu zásuvek v rámci UPS.
- Je požadováno dodání veškeré kabeláže potřebné pro zprovoznění předmětu plnění. Zejména kabely pro propojení dodávaných zařízení, kabely pro připojení dodávaných zařízení ke stávající přenosové síti, datové síti, napájecí síti, hlasovým rozvodům, patch panelům a propojení na stávající panely strukturované kabeláže.
- Je požadováno dodání veškerých konektorů a rozhraní potřebných pro zprovoznění předmětu plnění. Pokud je pro zprovoznění předmětu plnění potřebný konektor nebo rozhraní, které nejsou jmenovitě uvedeny v tabulce specifikace u zařízení, je požadováno jejich dodání.
- Stojany, ve kterých jsou umístěny komponenty dodávané v rámci projektu, včetně zařízení, je požadováno uzemnit.
- Je požadováno plné začlenění dodaného systému do stávající sítě.

- Je požadována kompletní konfigurace všech dodávaných komponent (včetně odesílání logů, konfigurací, SNMP trapů).
- Je požadována plná integrace dodávaných komponent do management nástrojů, zavedení komponent do těchto nástrojů (u stávajících dohledů v úzké spolupráci se správci systémů).
- Je požadována konfigurace šifrování přenosu dat.
- Veškeré dodávané komponenty musí být nové a výrobcem určené pro český trh.
- Softwarové produkty potřebné pro provozování díla je požadováno instalovat v rámci rezortní sítě MV ČR. Řádnou činnost dodaných komponent je požadováno zajistit bez nutnosti jejich konektivity do sítě Internet.
- V rámci dílčího akceptačního řízení je požadováno předat uživatelská jména a hesla pro přístup k veškerým instalovaným zařízením/aplikacím ve 3 kompletech, které budou obsahovat data v papírové formě a na datovém médiu (USB flash disku).

11 Seznam zkratek

Tabulka 34: Seznam zkratek

Zkratka	Význam
AAA	Authentication, Authorization and Accounting
AC/DC	Alternating Current/Direct Current
ACL	Access Control List
ACS	Access Control Server
AD	Active Directory
AD LDS	Active Directory Lightweight Directory Services
AES	Advanced Encryption Standard
AP	Access Point
BFCP	Binary Floor Control Protocol
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
BSSID	Basic SSID
CAC	Call Admission Control
CAEAP	Center for the Advancement of Enterprise Architecture
CFP	Standard Performance Evaluation floating operation
CINT	Standard Performance Evaluation integer operation
CIPAM	Centralized IPAM
CLI	Command Line Interface
CLIP	Calling Line Identification
CNID	Calling Party Name Identification
CoS	Class of Service
CPU	Central Processor Unit
ČR	Česká republika

Zkratka	Význam
CSTA	Computer Supported Telecommunications Applications
CSV	Comma Separated Values
CTI	Computer Telephony Integration
DCM	Dispersion Compensation Module
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
DTMF	Dual-Tone Multi-Frequency
DWDM	Dense wavelength division multiplexing
E1	E-carrier
ECDSA	Edwards-Curve Digital Signature Algorithm
ECMA	European Computer Manufacturers Association
EMC	Electromagnetic Compatibility
EPNM	Evolved Programmable Network Manager
ERSPAN	Encapsulated Remote Switched Port Analyzer
ETSI	European Telecommunications Standards Institute
EVPN	Ethernet VPN
FEC	Forward Error Correction
FOV	Field of View
FTP	File Transfer Protocol
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber
GDOI	Group Domain of Interpretation
GM	Group Member
GNSS	Global Navigation Satellite System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HD	High Definition
HDMI	High-Definition Multimedia Interface
HSRP	Hot Standby Router Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IAM	Identity & Access Management
ICMP	Internet Control Message Protocol
IDM	Identity Management
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IN/OUT	Input/Output

Zkratka	Význam
IOS	Integrovaná operační střediska
IP	Internet Protocol
IPAM	IP Address Management
IPFIX	Internet Protocol Flow Information Export
IPMI	Intelligent Platform Management Interface
IPSec	Internet Protocol Security
IPT	IP Telephony
IPv4	IP version 4
IPv6	IP version 6
IS	Systém pro zpracování a přístup k datům
ISDN	Integrated Services Digital Network
ISIK	Informační systém interních komunikací
ISIS	Intermediate System to Intermediate System
ITS	Integrovaná telekomunikační síť
ITU	International Telecommunication Union
KO	koncový objekt
L2	Layer 2
L3	Layer 3
LAG	Link Aggregation Group
LAN	Local Access Network
LCR	Low-Cost Routing
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAB	MAC Authentication Bypass
MAC	Media Access Control
MACSec	MAC Security
MIMO	Multiple-Input Multiple-Output
MM	Multi-Mode
MoH	Music on Hold
MP BGP	Multiprotocol BGP
MP3	Moving Picture
MPLS	Multiprotocol Label Switching
MS	Microsoft
MS AD	Microsoft Active Directory
MV	Ministerstvo vnitra
NAD	Network Access Device
NETCONF/YANG	Network Configuration/Yet Another Next Generation
NTP	Network Time Protocol
NVMe	Non-volatile Memory express
OSI	Open Systems Interconnection model
OSPF	Open Shortest Path First

Zkratka	Význam
OTN	Optical Transport Network
OTU	Optical channel Transport Unit
PČR	Policie Čerské republiky
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PIM SSM	Protocol Independent Multicast Source-Specific Multicast
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PTP	Precision Time |Protocol
PTR	Pointer
PTZ HD	pan–tilt–zoom
Q.SIG	Q signaling
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
RADIUS	Remote Access Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RESTCONF	Representational State Transfer Configuration Protocol
RFC	Request for Comments
RSVP	Resource Reservation Protocol
SAS	Serial Attached Small Computer System Interface
SATA	Serial Advanced Technology Attachment
SDN	Software Defined Network
SFF	Small Form Factor
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SIP	Session Initiated Protocol
SLA	Service Level Agreement
SM	Single Mode
SN	silové napájení
SNMP	Simple Network Management Protocol
SNMPv2	Simple Network Management Protocol version 2
SNMPv3	Simple Network Management Protocol version 3
SOA	Start of Authority
SPOF	Single Point of Failure
SRAM	Static Random Access Memory
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell

Zkratka	Význam
SSID	Service Set Identifier
STM	Synchronous Transport Module
SW	Software
SyncE	Synchronous Ethernet
SZ	Server pro nezávislou zálohu konfigurací
TACACS	Terminal Access Controller Access Control System
TAR	Tarifikační systém
TCAM	Ternary Content Addressable Memory
TCP	Transmission Control Protocol
TELNET	Teletype Network
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TRP	Trusted Relay Point
TTL	Time-to-Live
TWAMP	Two-Way Active Measurement Protocol
UO	uzlový objekt
UPAAS	Univerzální prostředí aplikací a služeb
UPS	Uninterruptible Power Supply/Source
URI	Uniform Resource Identifier
uRPF	Unicast Reverse Path Forwarding
USB	Universal Serial Bus
UTE	Union Technique de l'Electricité
VESA	Video Electronics Standards Association
vHBA	Virtual Host Bus Adapter
VLAN	Virtual LAN
vNIC	Virtual Network Interface Card
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
VTS	Veřejná telefonní síť
VXLAN	Virtual Extensible LAN
VZ	Veřejná zakázka
WAN	Wide Area Network
WAV	Waveform Audio File Format
WDM	Wavelength division multiplexing
WEB	World Wide Web
WLAN	Wireless LAN
XML	Extended Markup Language
XMPP	Extensible Messaging and Presence Protocol

12 Přílohy

Tabulka 35: Přílohy

Příloha č.1	Přehled architektury ISŘP (soubor: *P1_Architektura_ISŘP.archimate*)
Příloha č.2	Záměr standardizace a rozvoje datových uzlů komunikační infrastruktury Ministerstva vnitra a Policie České republiky (soubor: *P3_2024-Standardy_datovych_uzlu_MV-FINAL-Sig.pdf*)
Příloha č.3	ISMS 03.01.05 Politika řízení přístupu
Příloha č.4	ISMS 03.01.05.P02 Proces vytvoření matice oprávnění MV
Příloha č.5	ISMS 03.01.05.P03 Správa e-mailových schránek zaměstnanců na DPP a DPČ MV
Příloha č.6	ISMS 03.01.05.P04 Správa viditelnosti atributů zaměstnanců MV
Příloha č.7	Metodika identifikace a hodnocení aktiv a rizik (soubor: *ISMS 03.01.02.P01 Metodika identifikace a hodnocení aktiv a rizik.docx*)
Příloha č.8	Identifikace a hodnocení primárních aktiv systému XXX (soubor: *ISMS 02.10.03.P06 Šablona identifikace a hodnocení primárních aktiv.pdf*)
Příloha č.9	Plán zvládání rizik systému XXX pro rok 202X (soubor: *ISMS 02.10.03.P08 Šablona plánu zvládání rizik.pdf*)
Příloha č.10	Zpráva o hodnocení aktiv a rizik systému XXX (soubor: *ISMS 02.10.03.P07 Šablona zprávy o hodnocení aktiv a rizik.pdf*)
Příloha č.11	Manažerské shrnutí k hodnocení aktiv a rizik systému XXX (soubor: *ISMS 02.10.03.P07 Šablona zprávy o hodnocení aktiv a rizik.pdf*)