



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Možnosti napojení regionálních sítí k ITS MV – aktuální stav

ISSS Hradec Králové
14.5.2024



Integrovaná telekomunikační síť (ITS)

ITS je provozována Ministerstvem vnitra na základě zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, pro Policii ČR, složky IZS a územní orgány státní správy.

Ministerstvo vnitra je ústředním orgánem státní správy se svěřenou kompetencí pro koordinaci organizace a výkonu veřejné správy, komunikačních technologií a **zajišťuje komunikační sítě pro Policii ČR, složky integrovaného záchranného systému a územní orgány státní správy** a provozuje informační systém pro nakládání s utajovanými informacemi mezi orgány veřejné moci.

Geograficky ITS propojuje krajská ředitelství Policie ČR a Hasičského záchranného sboru v kruhu, s propustností až 100Gbps a většinu územních odborů Policie ČR na úrovni okresních měst z celkového počtu 77 nově s propustností 10Gbps.



Co je ITS

Po technické stránce je páteřní komunikační infrastruktura (ITS) založena na **využití optických tras ve směru centrum, kraj, okres.**

Nad optickou infrastrukturou je provozována **DWDM** síť umožňující vícenásobné využití s rychlostmi **až 100Gbps.**

Síť je určena pro přístup k centrálním informačním systémům složek IZS a současně je z úrovně kraj využívána pro přístup subjektů ke službám CMS.

CMS je základním stavebním prvkem pro digitální úřadování státu a **zprostředkovává oprávněným subjektům bezpečný a auditovatelný přístup k potřebným informačním systémům** a současně vzájemnou výměnu informací realizovanou pomocí služby „Publikace“.



Co je ITS

Jako přístupová místa k CMS slouží v **Národních datových centrech NDC bloky** (bloky Národních datových center), na úrovni kraje jsou to krajské konektory.

Přípojnými body k ITS pro lokální operátory a obce s rozšířenou působností jsou **krajské konektory v datových centrech jednotlivých krajských úřadů**.

Tyto krajské konektory jsou základním přípojným místem ke službám CMS a disponují kapacitou rovněž 10Gbps.



Co je ITS

Hranice ITS

Komunikační uzel (nejčastěji v lokalitě Krajského ředitelství Policie ČR (KŘP) nebo Krajského ředitelství Hasičského záchranného sboru (HZS); v lokalitě Územního odboru Policie ČR (ÚO PČR – dříve Okresní ředitelství Policie ČR), mezinárodních Letišť a v dalších, exaktně vyjmenovaných lokalitách v rámci ČR), který splňuje následující podmínky:

- lokalita je připojena pomocí optických vláken z minimálně dvou různých směrů (geografická redundance), které jsou součástí neveřejných komunikačních tras nekomerčních poskytovatelů ve vlastnictví nebo v přímém pronájmu MV na úrovni síťového rozhraní protokolu TCP/IP – vrstvě L1 dle síťového modelu ISO OSI – tj. na úrovni připojení pomocí „nenasvíceného vlákna (dark fiber)“
- v lokalitě je osazen síťový prvek MV ve správě NAKIT – ITS Transportní router, který zajišťuje komunikaci mezi Hraničním routerem lokální sítě Objednatele (resp. Beneficienta) ve správě Objednatele (resp. Beneficienta) a páteřní sítí ITS MV. Předávací rozhraní služeb na lokalitě je dáno mezi ITS Transportním routerem ve správě NAKIT a Hraničním routerem Objednatele (resp. Beneficienta) ve správě Objednatele (resp. Beneficienta). Na tomto rozhraní je monitorováno a vykazováno poskytování Generálních a Zákaznických služeb.
- v lokalitě je osazen síťový prvek DWDM (Dense Wavelength Division Multiplexing), zajišťující komunikaci mezi optickou vrstvou sítě ITS a ITS Transportním routerem. DWDM šifruje datový provoz na síti ITS na úrovni světelných kvant, tj. na vrstvě síťového rozhraní L1 dle síťového modelu ISO OSI.



Co není ITS

Hranice ITS

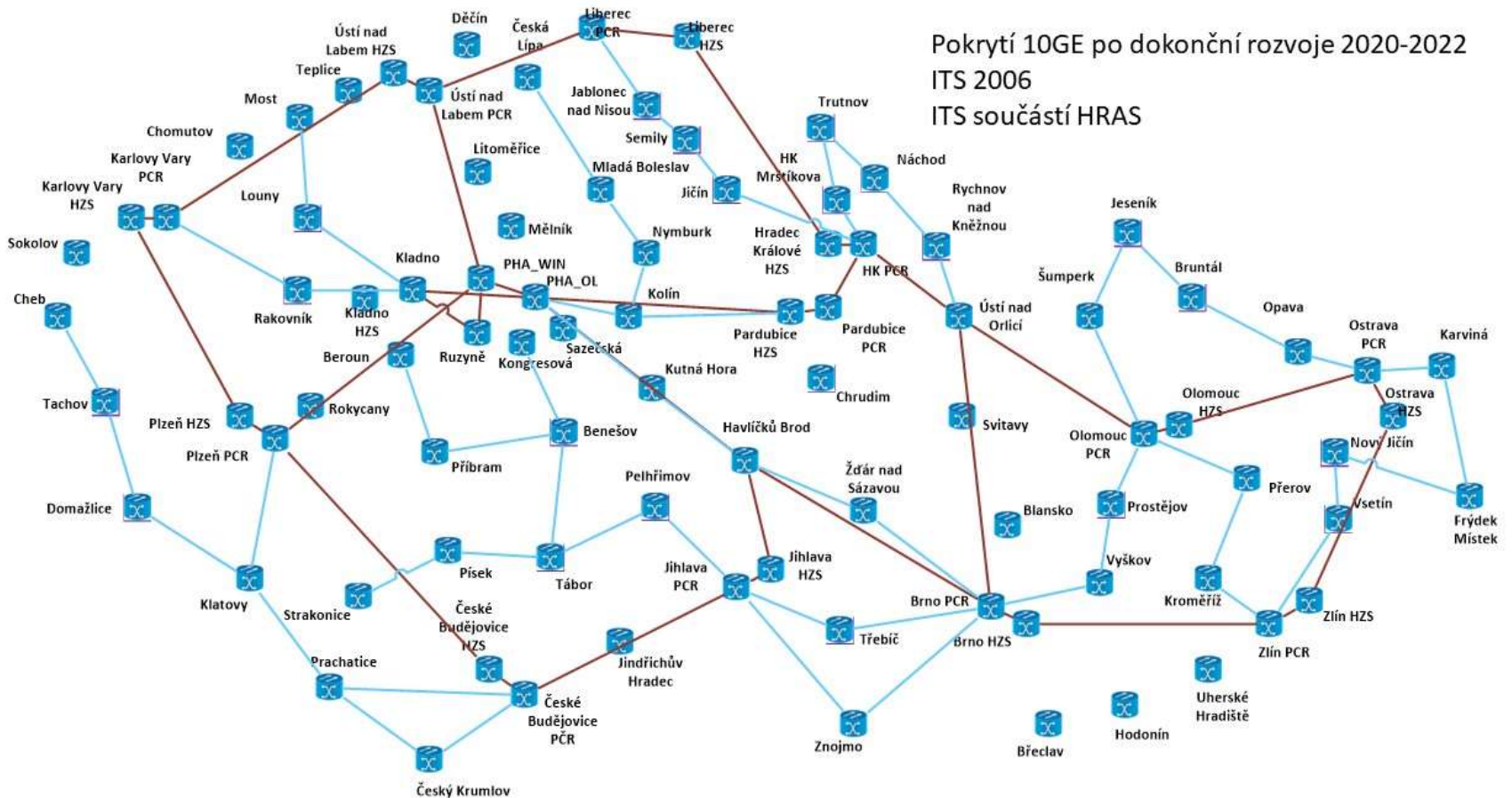
Komunikační uzel, nejčastěji na tzv. poslední míli (LM – Last Mile), který prostřednictvím KIVS přistupuje do sítě ITS a splňuje následující podmínky:

- lokalita je připojena alespoň jednou komunikační trasou (optickou, metalickou, bezdrátovou apod.), která je nejčastěji součástí veřejných komunikačních tras komerčních poskytovatelů na úrovni L2/L3 dle síťového modelu ISO OSI – tj. na úrovni připojení pomocí sdílené konektivity na bázi TCP/IP – internetové L2 a transportní L3 vrstvy.
- v lokalitě je osazen síťový prvek MV ve správě NAKIT – Transportní router, který zajišťuje komunikaci mezi Hraničním routerem lokální sítě Objednatele (resp. Beneficienta) ve správě Objednatele (resp. Beneficienta) a komunikační trasou KIVS. Předávací rozhraní služeb na lokalitě je dáno mezi Transportním routerem ve správě NAKIT a Hraničním routerem Objednatele (resp. Beneficienta) ve správě Objednatele (resp. Beneficienta). Na tomto rozhraní je monitorováno a vykazováno poskytování Zákaznických služeb.
- Hraniční router Objednatele (resp. Beneficienta) šifruje datový provoz na výstupu z routeru na úrovni TCP/IP vrstev – internetové L2 a transportní L3 vrstvy., tj. na úrovni L2/L3 dle síťového modelu ISO OSI.



Topologie ITS

Pokrytí 10GE po dokonční rozvoje 2020-2022
ITS 2006
ITS součástí HRAS





Stěžejní principy bezpečnosti ITS

Komunikační infrastruktura MV obecně musí

- být **odolná proti útokům** cíleným na její jednotlivé uzly, přenosové trasy, kritické služby i útokům vedeným na síť jako celek, ale současně musí **zajistit ochranu důvěrnosti a integrity všech přenášených dat**,
- disponovat technologiemi a nástroji, které budou **zaznamenávat a vyhodnocovat informace o aktivitách jednotlivých uživatelů a koncových zařízení** a které umožní **monitorování** předem definovaných **informací o jednotlivých datových tocích** za účelem detekce anomálií a potenciálních bezpečnostních hrozeb,
- disponovat možností **monitorovat v reálném čase datové toky** a poskytovat podrobná data o stěžejních charakteristikách jednotlivých datových toků (zdroj/cíl datového toku, typ datového toku, počet paketů, deformované pakety atd.), což je kritickou vlastností nutnou pro rychlou detekci a eliminaci případných bezpečnostních incidentů.

V rámci implementace standardu je předpokládána realizace ucelených či dílčích řešení, která musí být vždy připravena s ohledem na stav cílový, resp. realizace projektů vytvářených dle standardu nesmí vytvářet bariéry k dosažení cílového stavu.



Projekt MPLS

Projekt je rozdělen na pět dílčích podprojektů

1. Přístup do páteřní transportní sítě na úrovni „kraj“ rychlostí 100Gbps ve stupni HA,
2. Obměna MPLS infrastruktury na úrovni kraj/okres za perspektivní, dostatečně výkonnou technologii s životností 10 let; doplnění route reflektorů, vybudování centra řízení MPLS infrastruktury v souladu s požadavky na provozní a kybernetickou bezpečnost,
3. Náhrada obsoletních technologií ATM v páteřní komunikační infrastruktuře,
4. Obnova OoB management sítě,
5. Obnova napájecích zdrojů komunikačních uzlů.



Projekt MPLS

Vlastní projekt obměny technologií ITS - aktivity

Realizace projektu naplní cíle následujících parametrů budoucího stavu:

- Přístup do páteřní datové sítě (MPLS) na úrovni „okres“ rychlostí 10Gbps,
- Přístup do páteřní datové sítě (MPLS) na úrovni „kraj“ rychlostí 100Gbps,
- Možnost šifrování komunikace na úrovni L1(DWDM) a L2/L3 (MPLS),
- HW boxy v HA provedení a konfiguraci,
- Rezervní kapacita pro další doplnění/posílení konektivity a možnost připojit nové lokace.



Projekt MPLS

Vlastní projekt obměny technologií ITS – klíčová očekávání

Předmětem projektu je obměna MPLS infrastruktury na úrovni kraj/okres a na vybraných lokalitách (kde technologie je již bez možnosti podpory) za **perspektivní, dostatečně výkonnou technologii s životností 10 let**, dále obměna route reflektorů a vybudování centra řízení MPLS infrastruktury **v souladu s požadavky na provozní a kybernetickou bezpečnost**, vše s garancí 5letého supportu výrobce.

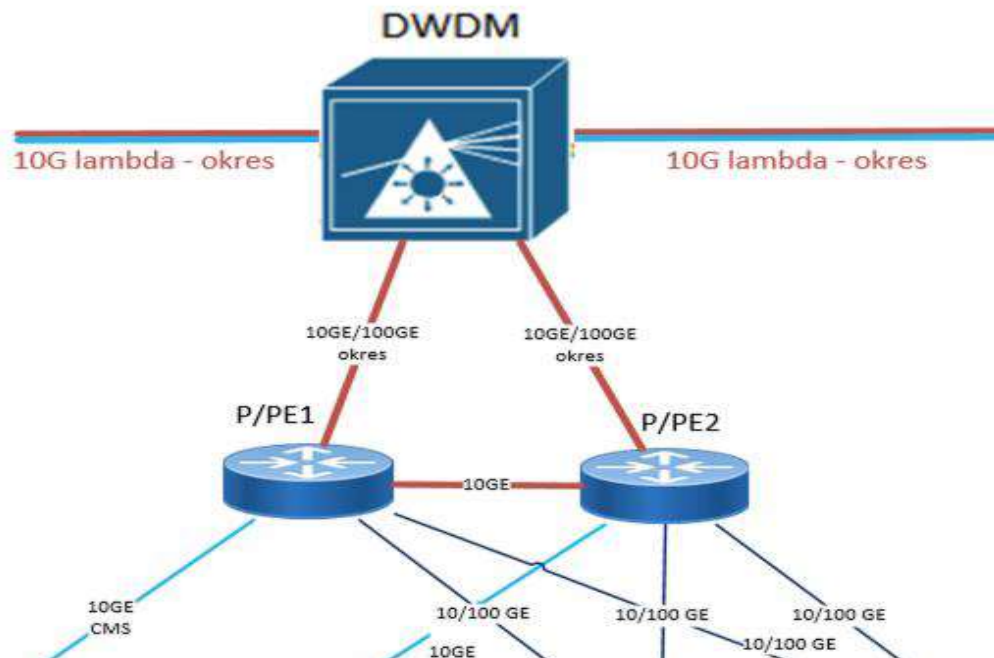
Rozšíření a obnova MPLS sítě ITS navazuje na realizaci nových přenosových technologií a **obsahuje rozšíření 10GE na stávajících směrovačích MPLS sítě** v krajských lokalitách a obnovu stávajících agregačních směrovačů MPLS sítě v okresních uzlech, které jsou již bez podpory **výrobce** a jejich další provozování není dlouhodobě udržitelné.

Projekt je realizován jako projekt **komplementární k projektu obnovy / posílení CMS (CMS DSŘ)**



Projekt MPLS

Obnova páteřní infrastruktury ITS představuje instalovat jeden pár PE routerů s možností připojení lokality PČR napřímo do PE routerů, případně možnost připojení i další subjektů (obce s rozšířenou působností) do oddělené MPLS VPN sítě vytvořené nad sdílenou ITS MPLS sítí.





Projekt MPLS

KRAJ – 2 x PE router

Obnova ve 23 lokalitách.

Stávající MPLS infrastruktura na úrovni kraj již nepostačuje svou výkonností a potřebnými typy rozhraní. Pro zachování parametrů v horizontu 5 let budou implementovány výkonné, modulární routery umožňující upgrade podle rostoucích provozních požadavků. Základním požadavkem je redundance na úrovni řídicí karty, napájení i chlazení.

Typem, který je již v komunikační infrastruktuře MV zaveden a splňuje parametry je Cisco řada ASR9900.



Projekt MPLS

OKRES – 2 x PE router

Obnova ve 59 lokalitách.

Jako dva PE routery budou implementovány routery s dostatečnou propustností a odpovídajícím počtem portů s parametry dle typové specifikace.

Typem, který je již v komunikační infrastruktuře MV zaveden a splňuje parametry je Cisco NCS540.



Projekt MPLS

Vlastní projekt obměny technologií ITS MV - shrnutí přínosů

- Posílení odolnosti sítě proti výpadkům – zajištěním vyšší redundance klíčových komponent a aktivních prvků
- Posílení spolehlivosti sítě – dosažení požadované úrovně SLA
 - obnova nového HW
 - pořízení podpory Výrobce
 - vyřazení obsoletního HW z provozu
- Rozšíření možností konektivity
 - pro připojení nových koncových lokalit a technologií
 - pro doplnění/posílení připojení do stávajících lokalit
- Navýšení výkonu, rychlosti komunikace a portových kapacit sítě ITS – nutný předpoklad pro realizaci dalších projektů a zavádění nových služeb
- Posílení bezpečnosti
 - doplnění kryptografických funkcionalit pro zabezpečenou komunikaci
 - up-to-date OS/FW/SW
- Eliminace obsoletní technologie
- Posílení zabezpečení provozu sítě pro vzdálenou správu a dohled
- Úspora nákladů při zajišťování správy a servisu



Hmgm modernizace ITS

Manažerský přehled stavu projektu Modernizace a optimalizace MPLS komunikační a informační infrastruktury

aktivita	DS	Status realizace	Status fakturace	IV.24	V.24	VI.24	VII.24	VIII.24	IX.24	X.24	XI.24	XII.24	I.25	II.25	III.25	
Technicko realizační projekt	11	dokončeno	ukončeno													
Přístup do páteřní transportní sítě na úrovni „kraj“ rychlostí 100Gbps ve stupni HA	15	dokončeno	ukončeno													
Obměna MPLS infrastruktury na úrovni kraj/okres, doplnění route reflektorů, vybudování centra řízení MPLS infrastruktury	28	probíhá	0	přejímky HW a SW, rozvoz po teritoriu	testy na platformě, instalace v Praze	realizace v místech plnění					administrativa, faktura					
Vymístění služeb ATM pro hlasové TDM technologie	16	probíhá	0	realizace v místech plnění	administrativa, faktura											
Obnova OoB management sítě	14	dokončeno	I.FM; II.FM po podpisu dodatku	administrativa, fakturace												
Obnova napájecích zdrojů	23	probíhá	0	místní šetření v místech plnění	technologická příprava	přejímky HW, I.FM	realizace v místech plnění					administrativa, faktura				



Zkušenosti z debat o napojení Jihočeských nemocnic

- Vedení Jihočeského kraje (JČK) a Krajského úřadu Jihočeského kraje (KÚ JČK) deklarovalo potřebu **zajistit oblast kybernetické a informační bezpečnosti u subjektů založených krajem** – nemocnice (právní forma akciová společnost), subjektů zřizovaných krajem – zdravotnická záchranná služba (právní forma příspěvková organizace) a KÚ JČK.
- JČK by za účelem vytvoření bezpečné a robustní komunikační infrastruktury rád **využil část páteřní sítě MV** – tato část páteřní sítě MV však nemůže být přímou součástí komunikační infrastruktury JČK, ale jen její tzv. virtuální částí
- Vedení holdingu Jihočeské nemocnice tuto aktivitu podpořilo a schválila ji i představenstva jednotlivých nemocnic, potřebuje připojení i pro aktivity ministerstva zdravotnictví.



Definice subjektů a etapy

Subjekty:

- Krajský úřad JČK (KÚ JČK)
- Zdravotnická záchranná služba Jihočeského kraje (ZZS JČK)
- Nemocnice České Budějovice (Nem CB)
- Nemocnice Český Krumlov (Nem CK)
- Nemocnice Dačice (Nem DA)
- Nemocnice Jindřichův Hradec (Nem JH)
- Nemocnice Písek (Nem PI)
- Nemocnice Prachatice (Nem PT)
- Nemocnice Strakonice (Nem ST)
- Nemocnice Tábor (Nem TA)
- Centrum kybernetické bezpečnosti Jihočeského kraje (JCK CKB)

Etapy:

1. Připojení jihočeských nemocnic a ZZS k ITS/KIVS/CMS2
2. Vytvoření virtuální privátní sítě a provoz JCK CKB

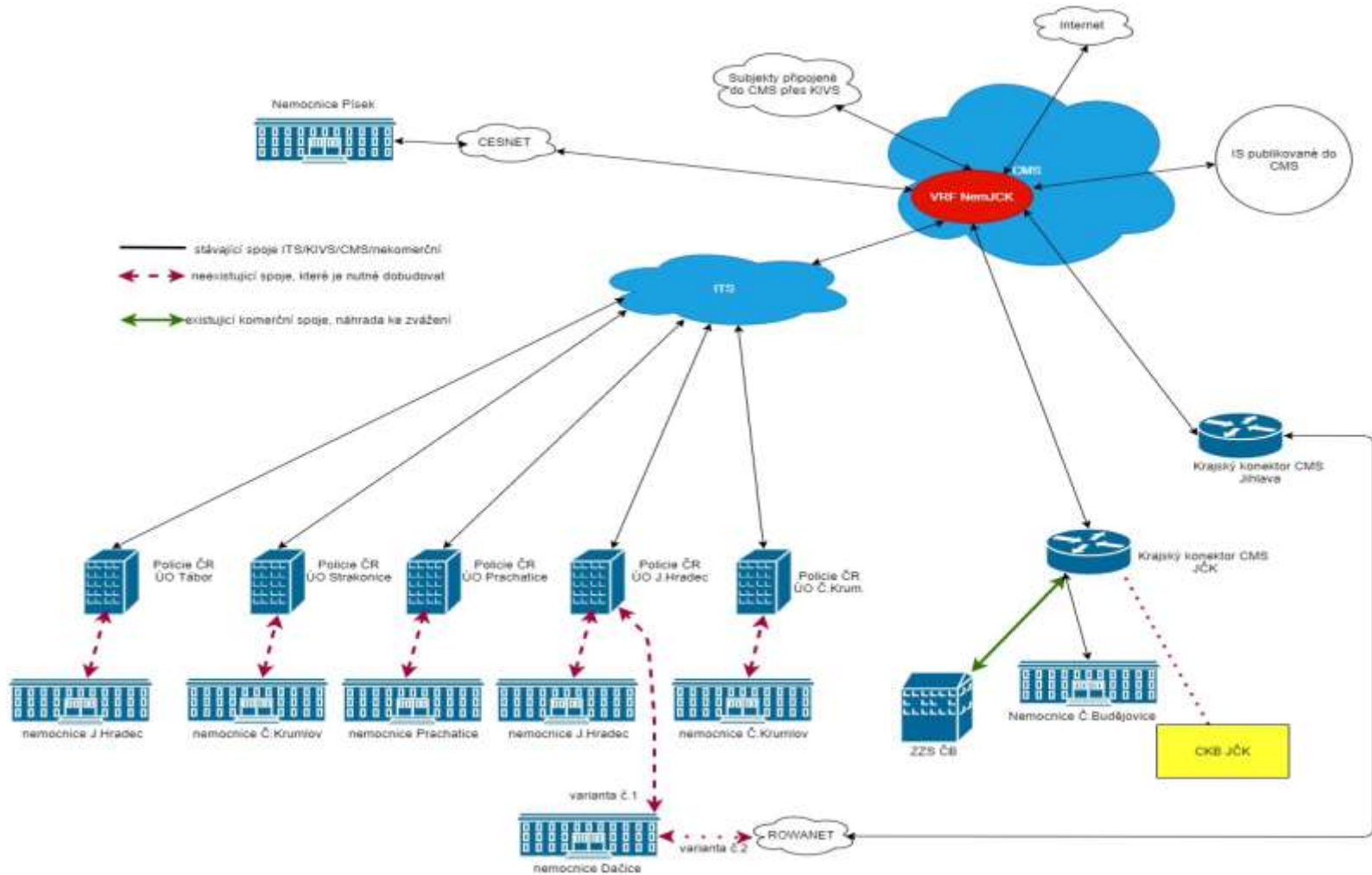


Předpoklady pro realizaci

- Subjekty (nemocnice se sídlem v bývalých okresních městech) **si zřídí dostatečnou konektivitu v parametrech pro připojení ke ITS/KIVS/CMS2 mezi sídlem subjektu (nemocnice) a sídlem příslušného Územního pracoviště Policie ČR (okres)**, jedná se o optický propoj min. 1Gbps s možností upgrade na 10Gbps
- Nem CB, ZZS JČK se připojí na „krajský konektor“, a jeho prostřednictvím k páteřní síti MV ČR (ITS/KIVS/CMS2)
- Nem DA bude připojena jiným navrženým způsobem (v.1 na ÚO PČR Jindřichův Hradec nebo v.2 do sítě ROWANET)
- V případě, že bude vytvořeno JCK CKB, bude připojeno k páteřní síti MV ČR (ITS/KIVS/CMS2) buď prostřednictvím „krajského konektoru“ nebo jiným navrženým způsobem
- Subjekty, které mají možnost se připojit přes síť **CESNET** (nekomerční operátor KIVS) se mohou připojit přes tohoto operátora
- **V rámci páteřní sítě MV (ITS/KIVS/CMS2) bude vytvořena virtuální privátní síť umožňující propojení všech subjektů rychlostí min. 1Gbit/s**



Schéma zamýšleného připojení





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DĚKUJEME ZA POZORNOST!

Q&A?

Odbor provozu informačních technologií a komunikací MV

Mgr. Bohdan Urban, CMICT

Ing. Petr Vobejda

s díky za podporu technického garanta - Ing. Roman Martiniak, CMICT