INTEGROVANÝ OPERAČNÍ PROGRAM
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ
MINISTERSTVO VNITRA
CESKE REPUBLIKY

Příloha č. 1e zadávací dokumentace

PRINCIPY CMS KIVS

Centrální místo Služeb – Komunikační infrastruktura Informačních systémů veřejné správy (CMS KIVS)

část
INFRASTRUKTURA

Verze 1.0

Obsah

1 Úvod

KIVS je navržena jako centralizovaná komunikační infrastruktura s Centrálním místem služeb (dále jen „CMS“), které je jediným místem výměny dat mezi jednotlivými informačními systémy veřejné správy (dále jen „ISVS“) a zároveň jediným místem propojení k veřejné síti internet a specifických neveřejných sítí např. sítí Evropské unie (dále jen „EU“).

CMS dále zajistí propojení jednotlivých technologických center ORP a Krajů (dále jen „eGoncentra“), propojení regionálních a metropolitních infrastruktur, dále zajistí realizaci generických a centrálních služeb pro eGoncentra. Bude realizovat služby centrální podpory uživatelů (Služby Servicedesk). Součástí CMS vzniknou i datové sály CMS pro hostování infrastruktury CMS a centrálních systémů eGovernment, včetně infrastruktury pro systémy Základních registrů, Czechpoint, PVS, ePusa, Smartadministration a další. CMS zajistí i propojení a konsolidaci služeb hlasové telefonie pro subjekty KIVS. CMS bude poskytovat infrastrukturu pro připojení, dohled, monitoring a řízení služeb poskytovaných nebo provozovaných v rámci CMS.

Komunikační infrastruktura Informačních systémů veřejné správy (dále jen „KIVS“) je založena na Koncepci KIVS, která byla schválena usneseními vlády č. 1156, č. 1270, č. 1453. Koncepce KIVS byla připravená na přelomu let 2006 a 2007 a uvedená do života v roce 2007. Nová koncepce je přijata na čtyřleté období do roku 2011, v jehož průběhu lze očekávat další výrazné úspory a to zejména v důsledku zavedené konkurence poskytovatelů služeb, koordinace rozvoje a odstraňování komunikačních bariér mezi složkami veřejné správy a postupnou migrací na perspektivní a nákladově efektivnější koncepčně technologická řešení.

Nová koncepce KIVS významně posiluje koordinovanost jednotlivých složek veřejné správy v procesech využívání a rozvoje komunikační infrastruktury, což ve výsledku vede k efektivnějšímu vynakládání veřejných (státních) finančních prostředků v této oblasti.

1.1 Přínos Centrálního místa služeb

Budování a zavádění řešení pro efektivní veřejnou správu (Smart administration) a eGovernment je jednou z hlavních priorit vlády, sledujících zefektivnění fungování státní správy a místní samosprávy a zjednodušení služeb státu pro občany i fyzické a právnické osoby. Ministerstvo vnitra se rozhodlo výrazně zkvalitnit přípravu i vlastní realizaci všech projektů ISVS (informačních systémů veřejné správy) spojených se zaváděním eGovernment řešení, aby se neúspěšným projektům zabránilo a zvýšila se efektivita vynaložených finančních prostředků.

CMS tvoří geograficky redundantní informační a komunikační infrastruktura, která slouží k řízenému bezpečnému propojování subjektů veřejné a státní správy mezi sebou a ke komunikaci těchto subjektů s jinými subjekty ve vnějších veřejných či neveřejných sítích, jako jsou Internet nebo komunikační infrastruktura EU (TESTA-II, s-TESTA, dále jen „TESTA“, Extranet EU). CMS vytvoří jednotné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS.

Cíle CMS:

- CMS vytvoří jako geograficky redundantní informační a komunikační infrastrukturu, která zajistí řízené a bezpečné propojování subjektů veřejné a státní správy mezi sebou a bude sloužit ke komunikaci těchto subjektů s jinými subjekty ve vnějších veřejných či neveřejných sítích, jako jsou Internet nebo komunikační infrastruktura EU (TESTA-II, s-TESTA, nebo Extranet EU).
- CMS je v rámci KIVS jediným místem, kde dochází k výměně dat mezi centrálními informačními systémy. Zároveň je jediným centrálním místem, kde je KIVS připojen k veřejné síti Internet a k dalším sítím, jako např. neveřejné datové sítě provozované v rámci EU.
- Vznik datových sálu CMS pro technologie CMS a eGovernment
- Vznik centrální dohledového systému
- Vznik centrální podpory uživatelů (Service desk CMS)

- Poskytovat infrastrukturní služby, ze kterých bude subjektu KIVS nebo systémům ISVS sestaveno řešení na míru:
  služba č. 1 „Základní služba CMS – centrální firewall“
  služba č. 2 „Přímé připojení k Internetu“
  služba č. 3 „Bezpečné připojení k Internetu“
  služba č. 4 „Přístup subjektů KIVS do zákaznické VPN přes Internet“
  služba č. 5 „Přístup koncových uživatelů subjektů KIVS do zákaznické VPN přes Internet“
  služba č. 6 „Služby S-TESTA“
  služba č. 7 „Propojení s jiným subjektem KIVS“
  služba č. 8 „Služby DNS Internet“
  služba č. 9 „Služby MTA“
  služba č. 10 „Služba Mail Storage“
  služba č. 11 „Služba DMZ1“
  služba č. 12 „Služba DMZ2“
  služba č. 13 „Provozní a servisní služby CMS“

- CMS plní v konceptu eGON center úlohu centrálního technologického centra (TC C). Hlavní funkcí je směrem k eGON centrům, zabezpečit provoz:

  G*enerických služeb (CMS I + CMS II)*

  - Adresářové služby
  - Identity management
  - Jmenné služby DNS – zajišťují překlad IP adres na jména v prostředí eGON center
  - Služba přesného času NTP – zajišťuje synchronizaci přesného času jednotlivých eGON center s CMS.

  Dalších centralizovaných služeb:

  - Poštovní server – poskytuje služby pro uživatele, kteří nemají vlastní poštovní server, služby poštovní relaye včetně antispamové a antivirové ochrany poštovního provozu
  - Antivir – odvirovávání dat, která přicházejí do eGON centra prostřednictvím CMS na úrovni protokolu HTTP, FTP, SMTP a provádí detekci virů v jazycích Java a ActiveX.
  - Centrální dohledový systém – zajišťuje kontrolu dostupnosti eGON center a umožňuje jejich správu.
  - Centrální podporu uživatelů (Service desk CMS)

  eGON centra ORP a Krajů budou s CMS propojena virtuální privátní sítí sloužící k přenosu dat a samostatnou virtuální privátní sítí, sloužící ke správě a dohledu eGON center.

1.2 Návaznost projektu na cíle a priority celostátní a evropské politiky

Intervence v oblasti Smart Administration vycházejí ze strategických materiálů vlády ČR pro reformu veřejné správy.

Prvním z nich je soubor základních tezí pro strategii modernizace veřejné správy ČR, který obsahuje materiál „Základní cíle Strategie efektivní veřejná správa a přátelské veřejné služby (Smart Administration) v období 2007 – 2015“, který vláda ČR projednala spolu s IOP dne 28. února 2007 (usnesení vlády č.197/2007).

Druhým materiálem je „Strategie Efektivní veřejná správa a přátelské veřejné služby (Smart Administration) v období 2007 – 2015“, která dále rozpracovává materiál „Základní cíle Strategie Efektivní veřejná správa a přátelské veřejné služby (Smart Administration) v období 2007 – 2015“ (usnesení vlády č.757/2007). Cílem strategie je vytvořit a zajistit koordinovaný a efektivní způsob zlepšování veřejné správy a veřejných služeb s využitím prostředků ze strukturálních fondů v programovém období 2007 – 2013.

Strategie realizace Smart Administration představuje komplexní, reformně orientovanou „cestovní mapu“ jejíž realizace přinese významnou kvalitativní změnu v systému veřejné správy a veřejných služeb ČR.

Mezi hlavní priority strategie realizace Smart Administration patří především:

- zkvalitnění tvorby a implementace politik;
- zlepšení a zjednodušení regulatorního prostředí a vytvoření atraktivního prostředí pro
- podnikatele, domácí i zahraniční investory;
- zefektivnění činnosti úřadů veřejné správy, snížení finančních nároků na chod administrativy a
- zajištění transparentního výkonu veřejné správy;
- zkvalitnění činnosti justice využitím informačních a telekomunikačních technologií;
- přiblížení a zkvalitnění veřejných služeb občanovi, zajištění jejich maximální dostupnosti a kvality.

Projekt CMS/KIVS je také plně v souladu s IOP Prioritní osou 1 – Modernizace veřejné správy.

Tato prioritní osa se zaměřuje na zavádění informačních a komunikačních technologií do státní správy, vytváření komunikačních sítí a elektronických databází. Cílem je zavést služby elektronické veřejné správy, vytvořit systém bezpečného sdílení dat a zajistit oprávněný přístup orgánům veřejné správy i občanům k těmto datům. Prioritní osa je programově navázána po stránce „tvrdých“ projektů na komplexní strategii zefektivňování veřejné správy Efektivní veřejná správa a přátelské veřejné služby - strategie realizace Smart Administration v letech 2007 - 2015.

Implementace IOP je realizována v souladu s legislativou EU a ČR. Základní právní rámec programu je obsažen v:

- Nařízení Rady (ES) č. 1083/2006 (dále jen “obecné nařízení”),
- Nařízení Komise (ES) č. 1828/2006 (dále jen “prováděcí nařízení”),
- Nařízení Evropského parlamentu a Rady (ES) č. 1080/2006,
- Národním strategickém referenčním rámci pro čerpání finančních prostředků ze strukturálních fondů EU v letech 2007 – 2013 (NSRR) – usnesení vlády ČR č. 1466/2006,
- Programovém dokumentu IOP.

Implementací se rozumí řízení, monitorování a kontrola ve smyslu hlavy VI obecného nařízení.

2 Provozní program a rozsah činností

Centrální místo služeb slouží k připojení subjektu státní správy, vzájemnému propojení komunikace mezi sebou, řízeným přístupem k Internetu nebo jiných síti (např. TESTA, ...).

CMS tvoří geograficky redundantní komunikační infrastruktura, která slouží k řízenému bezpečnému propojování subjektu veřejné a státní správy mezi sebou a ke komunikaci těchto subjektu s jinými subjekty ve vnějších veřejných či neveřejných sítích, jako jsou Internet nebo komunikační infrastruktura EU (TESTA-II, připravovaná s-TESTA, dále jen „TESTA“).

CMS umožňuje dělení podle druhu provozu a požadovaného stupně zabezpečení minimálně do dvou bezpečnostních zón s možností nastavení různých bezpečnostních politik. Komunikace z vnitřního IT prostředí Uživatele do vnějšího prostředí (např. Internet) prochází u obou bezpečnostních zón nejméně dvěma firewally od různých výrobců.

Prostředí CMS splňuje následující požadavky:
- Jediné místo garantovaného, bezpečného a auditovatelného propojení jednotlivých orgánů veřejné správy (dále jen „VS“) v rámci KIVS.
- Jediné místo umožňující připojení agend a aplikací uživatelů KIVS
- Jediné místo propojení do sítí EU a Internetu
- Řízení adresního prostoru, řízení sítových služeb (QoS, DNS, NTP, mail, AAA,...) v rámci KIVS
- redundantní datová konektivita min. 1 Gb/s propojená do dvou nezávislých směru zakončených na oddělené technologii v různých objektech,
- komunikační infrastruktura CMS, na které jsou poskytované datové služby, je technicky a geograficky redundantní,
- komunikační infrastruktura CMS je umístěna v bezpečném prostředí datových sálů CMS,
- k systému správy prvku a služeb je řízený přístup (místní i vzdálený) v prostředí odděleném od uživatelského prostředí (out-of-band management)
- Podpora pro externí monitoring a dohled celé KIVS
- Udržování provozní dokumentace
- SLA, monitoring SLA dodavatelů
- Požadovaná dostupnost alespoň 99,9%
- Řízení bezpečnosti v rámci KIVS, bezpečnostní autorita
- Oddělené vývojové a testovací prostředí od produkčního prostředí

Provoz CMS je zajištěn v souladu s CSN ISO/IEC 17799:2005 Informační technologie – Soubor postupu pro řízení informační bezpečnosti.

Poskytovatel má propracovaný a vyřešený systém bezpečnosti informací na základě normy ISO/IEC 17799, včetně bezpečnosti poskytovaných služeb.

2.1 Datové sály CMS

Prostory, kde jsou jednotlivé části CMS umístěny, odpovídají následujícím požadavkům:

a) teplota prostředí se pohybuje v rozmezí od 19°C do 25°C, relativní vlhkost v rozmezí 35% - 65%,
b) v místnostech, kde je CMS umístěno, jsou instalována požární čidla na kouř a teplotu,
c) tyto prostory jsou napojeny na systém elektronické protipožární signalizace a elektronické zabezpečovací signalizace,
d) v prostorách je zajištěn rozvod elektrické energie 230/50 V s bez-výpadkovým zálohováním, samostatně jištěnými rozvaděči a jsou rovněž zajištěny diesel agregáty,
e) je zajištěna vnější ochrana budovy bezpečnostní službou nepřetržitě 24 hodin denně a 7 dní v týdnu, přičemž jsou prokazatelně evidovány osoby vstupující do objektu, v němž se prostory s CMS nacházejí,
f) datové sály CMS splňují podmínky Vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. pro stupeň utajení Důvěrné
g) prostory, v nichž se CMS nachází, leží mimo zátopovou oblast tzv. stoleté vody.

Geograficky redundantní infrastrukturou se rozumí zálohování všech produkčních prvků CMS ve dvou identických větvích umístěných ve dvou různých lokalitách, které splňují podmínku, že jsou od sebe vzdáleny více než 6000 metrů a jsou napájeny z různých rozvoden elektrické energie.

3 Základní charakteristika řešení CMS

3.1 Stručná charakteristika řešení infrastruktury CMS:

- Infrastruktura CMS je navržena jako redundantní infrastruktura s možností dislokace do dvou geograficky rozdílných a vzájemně oddělených, vzdálených, nezávislých a neovlivnitelných lokalit (napájení, topologická nezávislost přípojných a propojovacích optických tras apod.)
- Infrastruktura je logicky rozčleněna do základních šesti funkčních celků (propojovací síť poskytovatelů „InterConnect-I“, bezpečné propojení resortních VPN „Central Firewall“, sdílené služby „Shared Services“, externí firewall „External Firewall“ připojení k externím sítím „InterConnect-E a nezávislá administrátorská síť „Management“) každý z funkčních celků je řešen redundantně.
- Redundance napříč funkčními celky CMS je řešena v režimu Active-Standby. Redundance je realizována prostřednictvím rapid spanning tree protokolu na úrovni druhé vrstvy dle OSI modelu. Na třetí vrstvě dle OSI protokolu je redundance v páteřní síti CMS řešena vlastnostmi firewall modulu FWSM resp. ASA5580, ACE modulu pro balancování provozu a HSRP protokolem na úrovni MSFC modulu přepínačů Catalyst 6500. Redundance na úrovni páteřních MPLS uzlů sítě InterConnect-I je řešena prostřednictvím dynamického směrovacího protokolu bgp. Redundance pro „čistý internet“ je realizována dynamickým směrovacím protokolem is-is. Redundance do Internetu je řešena prostředky bgp protokolu v rámci přiděleného veřejného autonomního systému
- Vzájemné propojení topologicky nezávislých lokalit CMS je řešeno prostřednictvím DWDM technologie přes „dark fiber“ trasy. V současnosti jsou přes DWDM technologii propojeny pouze páteřní uzly sítě InterConnect-I (Olšanská 4 – HC Nagano), ostatní bloky redundantní infrastruktury jsou dislokovány do výpočetního sálu v lokalitě Olšanská 4, Praha 3 a propojeny lokálně metalickými a multi-mode optickými spoji. Přenosová kapacita prostředí CMS na úrovni fyzických rozhraní je 1 Gbit/s.
- Jednotlivým subjektům resp. sdíleným aplikacím v příslušných logických funkčních celcích je přidělena IP adresa z bloku privátních adres dle RFC1918 (10.240.0.0 /12). Případný konflikt v bloku adres 10.240.0.0 /12 je ošetřen administrativně v gesci MVČR. Adresní prostory jednotlivých subjektů KIVS mohou být překryvné. Překryv adres je řešen prostřednictvím překladu adres do konsolidovaného adresního prostoru CMS 10.252.0.0 /14.
- Veřejný IP adresní prostor je registrován u RIPE jako „provider independent“ blok adres 94.199.40.0 /21 s vlastním autonomním systémem 48298.
- Každý subjekt KIVS je při průchodu http/http proxy resp. smtp proxy jednoznačně identifikován napříč celou infrastrukturou CMS až do Internetu resp. sítě sTESTA

- Prostředí CMS poskytuje bezpečné propojovací prostředí mezi subjekty KIVS, mezi jednotlivými subjekty KIVS a Internetem resp. mezi jednotlivými subjekty KIVS a externími sítěmi jako je např. síť sTESTA. Každý subjekt KIVS může být připojen do Internetu mimo bezpečnostní prvky CMS přes dedikovanou MPLS VPN sít (tzv. „čistý internet“).
- Prostředí CMS poskytuje celkem 13 služeb, ze kterých bude subjektu KIVS sestaveno řešení na míru:
  služba č. 1 „Základní služba CMS – centrální firewall“
  služba č. 2 „Přímé připojení k Internetu“
  služba č. 3 „Bezpečné připojení k Internetu“
  služba č. 4 „Přístup subjektů KIVS do zákaznické VPN přes Internet“
  služba č. 5 „Přístup koncových uživatelů subjektů KIVS do zákaznické VPN přes Internet“
  služba č. 6 „Služby S-TESTA“
  služba č. 7 „Propojení s jiným subjektem KIVS“
  služba č. 8 „Služby DNS Internet“
  služba č. 9 „Služby MTA“
  služba č. 10 „Služba Mail Storage“
  služba č. 11 „Služba DMZ1“
  služba č. 12 „Služba DMZ2“
  služba č. 13 „Provozní a servisní služby CMS“
- Bezpečný internet je realizován dvěma firewally (centrální firewall, internet firewall) a soustavou prostředků pro proxy služby (http/http proxy, ftp proxy, smtp proxy, pop3/pop3s proxy, imap4/imap4s proxy, dns, ntp). Oddělení jednotlivých bezpečnostních zón CMS je realizováno VLAN sítěmi dle 802.1q na druhé vrstvě dle OSI modelu, na třetí vrstvě dle OSI je pak řešeno virtuálními routing kontexty, virtuálním firewall kontexty resp. virtuálními balancovacími kontexty a IPSec protokolem.
- Pro správu technickým prostředků CMS resp. technických prostředků subjektu KIVS v prostředí demilitarizovaných zón DMZ1 a DMZ2 (resp. DMZVPN) je vytvořena samostatná nezávislá administrativní síť.
- Správný chod sítě CMS je monitorován management nástroji SNMPc, Nagios, MARS a správa sítě CMS je realizována prostředky ACS, LMS, ANM, CSM.
- přístup k administrativní síti je možný prostřednictvím VPN IPSec klienta z internetu nebo z VPN sítě jednotlivých subjektů KIVS. Přístup k administrativní síti je autentizován/autorizován prostředky AAA.

InterConnect-E

- InterConnect-E je peeringový přístupový uzel do sítě Internet a do externích sítí jako je např. sTESTA.
- Funkční blok InterConnect-E je realizován prostřednictvím dvou routerů Cisco7609.

- Chassis Cisco 7609 je vybaven dvěma supervizor moduly RSP720-3CXL-GE s MSFC4 routing sub-modulem pro řízení přepínání na L2 a L3, jedním LAN modulem WS-6724-SFP pro připojení k okolním funkčním blokům a dvěma moduly pro identifikaci DDoS útoků (Anomally Detector Module WS-SVC-ADM-1-K9 a Anomally Guard Module WS-SVC-AGM-1-K9).
- Připojení k Internetu je realizováno redundantně vždy jedním okruhem z každého peeringového uzlu k ISP T-System pro odbavení mezinárodního internetového provozu, pro odbavení národního internetového provozu jsou uzly připojeny do NIXu a to vždy jedním okruhem z každého peeringového uzlu CMS (v současnosti k 2.4.2009 je realizován pouze jeden okruh do NIXu).
- Evropská síť sTESTA je připojena ke každému peeringovému uzlu jedním 2.048 Mbit/s okruhem. Redundantní připojení je provozováno v režmu Active-Standby tj. kapacita připojení je 2,048 Mbit/s.
- Propojení routerů Cisco7609 je realizováno čtyřmi gigabitovými okruhy (2x 1000Base-SX, 2x1000Base-TX spojenými do EtherChannel logického okruhu (PortChannel1).

- Peeringové routery jsou připojeny na funkční blok Internet Firewall prostřednictvím rozhraní 1000Base-TX v tagovaném režimu dle 802.1Q.
- Peeringové routery jsou navíc připojeny do funkčního bloku InterConnect-I pro realizaci služby „čistý internet“.

Externí FW (Internet)

- Externí firewall představuje perimetrovou ochranu prostředí, jde o redundantní instalaci 2 dedikovaných boxů Cisco ASA 5580-40 v multikontextovém režimu active/active.
- Oba boxy jsou propojené přes interface Redundant1, sloužící k přenosu failover a stavových informací.
- Na každém z obou boxů jsou vytvořeny kromě systémového kontextu (system) 3 kontexty: admin, FWIV1 a FWIV2. Každý kontext představuje virtuální firewall, kontexty stejného pojmenování existují na obou boxech, používají shodnou konfiguraci a zálohují se dle schematu active/standby. Pouze systémový kontext obsahuje odlišnost v konfiguraci, spočívající v určení role boxů primary/secondary. Jednotlivé kontexty pak mohou být ve stavu active nebo standby nezávisle na jiném kontextu. Prakticky ovšem existují 2 fail-over skupiny (Group 1 a Group 2), nastavené tak, aby v klidovém provozu jim přiřazené kontexty byly active v prvním případě na primárním boxu V1 a ve druhém případě na sekundárním boxu V2. Kontexty admin a FWIV1 primárně existují na boxu V1 a kontext FWIV2 na boxu V2. V případě kolapsu jednoho z boxů se všechny kontexty „přestěhují“ jako aktivní na funkční box.
- Konfigurace se synchronizují a stavy předávají přes dedikovaný interface Redundant1. Administrativní kontext admin slouží pro management firewallu, kontexty FWIV1 a FWIV2 jsou určeny pro vlastní provoz, který v případě kontextu FWIV1 primárně protéká přes box V1 a v případě kontextu FWIV2 přes box V2. Tím také dochází k rozdělení zátěže a je možné boxy lépe využít.

Sdílené služby

Základním úkolem tohoto funkčního bloku je realizace tzv. sdílených služeb, které představují další bezpečnostní stupeň v prostředí sítě CMS (Centrální místo služeb). Blok sdílených služeb řeší následující funkce:

- http/https proxy brána v routed nebo transparentním režimu (volba režimu je závislá na nastavení směrování v uživatelské VPN síti připojené k CMS a na nastavení prohlížeče uživatele). Provoz s http protokolem je podroben antivirové kontrole. Http proxy podporuje funkci IP spoofing což umožňuje přenos zdrojové adresy ze vstupu na výstup proxy brány. Tato funkcionalita zajišťuje pro http/https provoz jednoznačnou identifikaci uživatelské VPN sítě napříč celou infrastrukturou. Každý subjekt má přidělenu unikátní veřejnou IP adresu.
- ftp proxy „over http" v routed nebo transparentním režimu (volba režimu je závislá na nastavení směrování v uživatelské VPN síti připojené k CMS a na nastavení prohlížeče uživatele). Provoz „ftp over http" je podroben antivirové kontrole. Identifikace zdrojové adresy není podporována. Tento typ provozu vystupuje v Internetu pod jednou veřejnou adresou.
- ftp proxy s plnou podporou všech ftp příkazů v routed režimu. Provoz není podroben žádné kontrole na škodlivý obsah, identifikace zdrojové adresy není rovněž podporována. Tento typ provozu vystupuje v Internetu pod jednou veřejnou adresou
- smtp proxy zajišťuje relay mailového provozu mezi Internetem resp. sítí sTESTA a uživatelskými VPN sítěmi resp. mezi uživatelskými VPN sítěmi. Mailový provoz je podroben antivirové kontrole. Je možné zajistit identifikaci zdrojové adresy uživatelské VPN sítě. Tuto funkcionalitu je možné aplikovat pro maximálně 32 subjektů. Každý z 32 možných subjektů bude mít pro mailový provoz přidělenu samostatnou veřejnou IP adresu.
- pop3/po3s proxy zajišťuje přístup k mailovým schránkám umístěným v Internetu z prostředí uživatelské VPN sítě. Provoz není podroben žádné kontrole na škodlivý obsah, identifikace zdrojové adresy není podporována. Tento typ provozu vystupuje v Internetu pod jednou veřejnou adresou.
- imap4/imap4s přístup k mailovým schránkám umístěným v Internetu z prostředí uživatelské VPN sítě. Provoz není podroben žádné kontrole na škodlivý obsah, identifikace zdrojové adresy není podporována. Tento typ provozu vystupuje v Internetu pod jednou veřejnou adresou.
- dns proxy poskytuje jmenné služby jednak uživatelským VPN sítím a to jak pro resolving jmen v doménách uvnitř CMS tak pro resolving doménových jmén v externích sítích jako je internet resp. sTESTA. Současně dns proxy slouží i pro vnitřní potřeby cms tj. poskytuje služby ostatním proxy branám jako je např. http/ttp/ftp/smtp/pop3/imap4 proxy.
- ntp proxy poskytuje zdroj přesného času jednak pro subjekty KIVS připojené VPN sítí do sítě CMS ale také pro vnitřní infrastrukturu CMS
- VPN IPSec z Internetu pro přístup do VPN sítě subjektu KIVS. Služba umožňuje zakončit IPSec tunel z Internetu na VPN koncentrátoru sdílených služeb a

dešifrovaná data poslat do příslušné MPLS VPN sítě subjektu KIVS. Pro přímé směrování dešifrovaných dat do jednotlivých zákaznických VPN MPLS sítí je IPSEC koncentrátor připojen k uzlům InterConnect-I prostřednictvím mpls technologie (na portu Port-channel 41 je zprovozněn LDP protokol) a v IPSEC koncentrátoru (IPSEC_V1/V2_C7201) je spuštěn extended BGP protokol. Služba VPN IPSec zajišťuje celkem dva typy připojení a to připojení tzv. „VPN klienta“ s jedním počítačem nebo tzv. připojení „site-to-site“ pro připojení pobočkové sítě k MPLS VPN subjektu KIVS

- Balancování datového provozu sdílených služeb (každá sdílená služba je realizována několika identickými technickými prostředky jako např. server, IronPort, IPSec koncentrátor apod.) a také balancování provozu uživatelských aplikací do demilitarizováných zákaznických zón DMZ1 přístupných z prostředí Internetu, sTESTA a MPLS VPN sítí. Služba balancingu datového provozu je poskytována formou oddělených virtuálních kontextů konfigurovaných na hardwarovém modulu ACE (Application Control Engine).
- Ochrana demilitarizovaných zón DMZ1 s aplikacemi zákazníků inzerovaných do Internetu. Služba ochrany demilitarizovaných zón je poskytována formou oddělených virtuálních firewall kontextů konfigurovaných na hardwarovém modulu FWSM (Firewall Services Module).
- Chráněný resp. balancovaný segment DMZ1 je připojen přímo do sítě InterConnect –I, kde je dále zakončen lokálně přes access přepínače (v současnosti 2x C4948) nebo vzdáleně do MPLS sítě.
- Ochrana přístupové L2 vrsty sdílených služeb s připojenými technickými prostředky (server, IronPort, IPSec koncentrátor) a demilitarizovaných zón DMZ1 je realizována prostřednictvím identifikace nebezpečných útoků IPS sondou Cisco 4270.

Funkční blok sdílených služeb je umístěn v jádru sítě CMS. Je napojen na hraniční firewally sítě CMS. Jedná se o firewall připojený přes peeringový uzel do Intermetu a o Centrální firewall připojený přes síť InterConnect-I do MPLS sítí poskytovatelů.

Funkční celek sdílených služeb je tvořen dvojicí zařízení Cisco Catalyst 6509E v následující hardwarové sestavě:

- 2x řídící modul ve verzi VS-S720-10G-3C (Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C)
- 1x 24-portový Ethernet SFP modul (WS-X6724-SFP)
- 1x 48-portový Ethernet TX modul (WS-X6748-GE-TX)

- 1x ACE modul (ACE20-MOD-K9 + ACE-08G-LIC + ACE-VIRT-020 + ACE-SSL-05K-K9)
- 1x FWSM modul (WS-SVC-FWM-1-K9 + SC-SVC-FWM-3.2-K9 + FR-SVC-FWM-VC-T1)

ACE modul je vybaven licencí na celkovou propustnos 8 Gbit/s, dále pak licencí pro 20 virtuálních kontextů a licencí pro 5000 SSL spojení za sekundu.

- V současnosti jsou zkonfigurovány tři ACE kontexty (SHARED_SERVICES, SHARED_SERVICES_V2, DMZ1-MVCR). Z toho jsou v provozu dva kontexty (SHARED_SERVICES, DMZ1-MVCR). Kontext SHARED_SERVICES zajišťuje balancing provozu na servery sdílených služeb, kontext DMZ1-MVCR balancing provozu na servery portálu CZECH POINT. Kontext SHARED_SERVICES_V2 je připraven pro režim active-active přes obě větve infrastruktury CMS

FWSM modul je vybaven licencí pro 20 virtuálních kontextů.

- V současnosti jsou zkonfigurovány a provozovány tři FWSM kontexty (1x pro přístup ke sdíleným službám z admin sítě, 1x pro potřeby aplikací v DMZ1 MVČR (CzechPoint, SmartAdministration, Kivs Evidence) a 1x pro dns server CMS (ns.gov.cz).

Součástí funkčního celku sdílených služeb jsou také následující podpůrná zařízení:

- 2x Cisco Catalyst 4948
- 2x Cisco 7201

Cisco Catalyst 4948 je použit jako L2 přístupová vrstva pro připojení technických prostředků sdílených služeb (servery, IronPorty, Cisco7201)

Cisco 7201 je použit pro zakončení IPSec spojení z Internetu s přesměrováním dešifrovaných dat do MPLS VPN sítí.

Centrální firewall

Základním úkolem tohoto funkčního bloku jsou:

1. Napojení prostředí CMS k vnitřnímu propojovacímu prostředí Interconnect I, kam jsou přivedeny přípojky jednotlivých lokalit subjektů státní správy.
2. Realizace vstupních firewallů jednotlivých subjektů, přes které do prostředí vstupují.
3. Konektivita k funkčnímu bloku sdílených služeb, kde jsou zrealizovány služby prostředí CMS.

Funkční celek cetrální firewall (dále jen CFW) je dvořen dvojící zařízení Cisco Catalyst 6509-E v následující hardwarové sestavě:

- 2x řídící modul ve verzi 720 10GE (VS-S720-10GE)
- 1x 24-portový Ethernet SFP modul
- 1x 48-portový 10/100/1000 Ethernet (RJ-45) modul
- 1x Firewall module
- 1x Application Control Engine (ACE) modul

Vstupní Layer-3 rozhraní každého subjektu připojujícího se do prostředí CMS je zrealizováno na pro tento subjekt vyhrazeném virtuálním firewallu (dále jen VFW), jakákoliv komunikace směrující ze subjektu do prostředí či naopak tedy musí projít tímto VFW.

VFW jednotlivých subjektů jsou přes své vnitřní rozhraní napojení na řídící modul zařízení CFW, který zajišťuje směrování provozu dále do prostředí.

Virtuální firewall jako vstupní prvek každého zákazníka do prostředí CMS bude vždy obsahovat minimálně 3 základní Layer-3 rozhraní:

- Vstupní rozhraní od zákazníka (ve směru od funkčního bloku IC-I)
- Přes toto rozhraní budou směrovány adresní rozsahy zákazníka, které využívá ve své vnitřní síti
- Vstupní rozhraní do prostředí CMS (směrem ke sdíleným službám a ostatním zákazníkům prostředí)
- Směrována výchozí cesta (default route) či konsolidovaný adresní rozsah (10.240.0.0/12)
- Management rozhraní (přístup management nástrojů prostředí a administrace)
- Směrován adresní rozsah managementu prostředí CMS (10.251.0.0/16)

Dále pak mohou na tomto VFW mohou být vytvořena další rozhraní dle individuálních potřeb jednotlivých zákazníků – nejčastěji se bude jednat o:

- Demilitarizované zóny DMZ2
  Zóny pro umístění zákaznických zařízení v hostingových centrech, která budou obsahovat služby, které chtějí zákazníci sdílet s dalšími subjekty připojenými do prostředí či případně budou soužit jako backend pro zařízení umístěná v demilitarizovaných zónách DMZ1 (t.j. pro zdroje primárně publikované do internetu).

  Těchto zón může být na VFW vytvořeno v závislosti na preferencích zákazníka
- Komunikační spojky mezi funkčními bloky
  Nejčastěji pro provoz, který nelze provozovat přes sdílené služby či například jeho provoz přes proxy servery nedovolují bezpečností požadavky apod.

InterConnect –I (MPLS)

- InterConnect-I slouží k propojení páteřní infrastruktury poskytovatelů, kteří poskytují své služby pod rámcovou smlouvou KIVS 2007 tak, aby se docílilo maximální možnosti volby jednotlivých dílčích služeb dle výhodnosti od různých operátorů.
- InterConnect-I je vybudován jako plně geograficky redundantní propojovací uzel páteřních sítí operátorů. InterConnect-I je budován jako propojení dvou dílčích geograficky redundantních uzlů s redundantním napojením jednotlivých zúčastněných poskytovatelů.

Do propojovací sítě InterConnect-I jsou připojeni následující poskytovatelé služeb:
Telefónica O2, GTS Novera, ČD Telematika, Ministerstvo vnitra ČR .

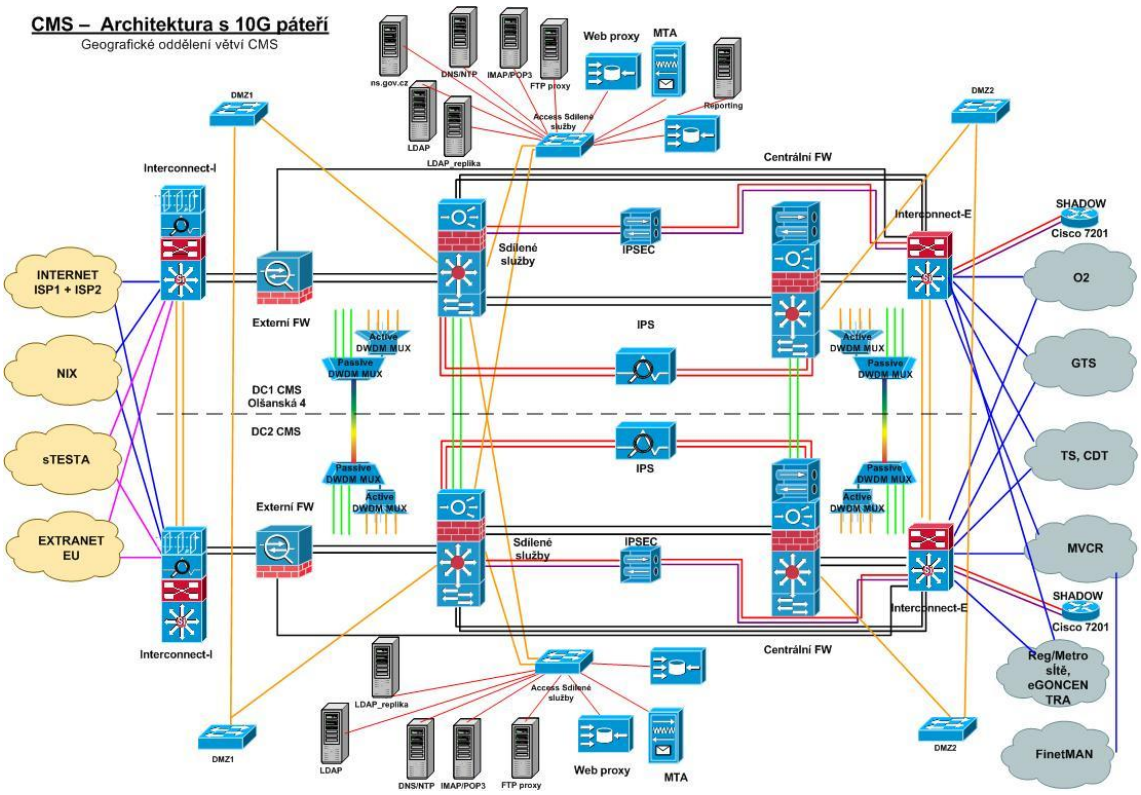
- Poskytovatelé budou k PSP připojeni přímo vždy 2 WAN spoji (v rámci každého dílčího uzlu 2 WAN porty k centrálnímu boxu). Standardně je uvažováno s tím, že:
  1 spoj (port) bude určen pro účely poskytování VPN konektivity poskytovatelem.

  1 spoj (port) bude určen pro účely připojení Housingových center poskytovatelem.
- V rámci sítě InterConnect-I bude cílově použita WAN technologie Cisco na bázi WAN karet typové řady 7609.

- Rozhraní InterConnect-I bude vůči operátorům řešeno s propustností (resp. na rozhraních) 1GB na každém spoji. Každý poskytovatel připojovaný k PSP odpovídá za dodání příslušného koncového zařízení SFP GBIC do obou centrálních boxů dílčích uzlů PSP s tím, že tato zařízení musí být kompatibilní s použitou technologií centrálních boxů a typově vhodné dle charakteru poskytovatelem použitého spoje (ve smyslu přenosové trasy).

- Optická trasa single-mode 9/125µm s konektorem E2000 na straně optického patch panelu.
- Připojení ke *koncovému zařízení duplexním single mode (9/125µm) optickým patch kabelem s konektory E2000/APC a LC (bude použit na straně InterConnect a na straně SP pokud používá SFP GBIC na koncovém zařízení) resp. E2000/APC a SC (pokud SP používá GBIC na koncovém zařízení).*

Schématické zobrazení CMS (bez OOB Managementu)



4 Provozní a výkonnostní parametry infrastruktury KIVS

Infrastruktura KIVS obsahuje komunikační a datové služby.

4.1 Parametry komunikačních služeb KIVS

Komunikační služby slouží pro připojení jednotlivých subjektů k prostředí CMS

Typ služby	Rychlost	Dostupnost
VPN DSL	64Kbit- 8Mbit	99.00%
VPN do 8Mbit	128Kbit -8Mbit	99.00%-99.99%
VPN nad 10 Mbit	10Mbit – 10Gbit+	99.00%-99.99%
INTRA DSL	64Kbit- 8Mbit	99.00%
INTRA do 8Mbit	128Kbit -8Mbit	99.00%-99.90%
INTRA nad 8Mbit	10Mbit – 10Gbit+	99.00%-99.99%
DARK FIBRE		99.00%-99.50%
HOUSING		99.90%-99.99%

4.2 Datové služby CMS

4.2.1 VPN služba CMS „CMS-0-1“

Služba slouží pro zakončení jednotlivých linek a vytvoření jedné či více VPN nad jednotlivými linkami od providerů. Subjekt může mít jednu či více VPN. Na základě požadavku zákazníka mohou být VPN zakončeny pouze na definovaných přípojkách, nebo na všech přípojkách subjektu.

4.2.2 Základní služba CMS “CMS-1-1“

V rámci realizace IP VPN přípojky KIVS je VPN každého subjektu propojena přes Interconnect-I – tato konfigurace je automatická při zřizování každé KIVS přípojky.

Realizace „Základní služby CMS“ znamená pro každou takto vytvořenou IP VPN aktivovat a alokovat na Centrálním FW CMS (dále CFW) samostatný virtuální FW daného subjektu.

Realizace této služby je základní podmínkou, kterou musí subjekt splnit, pokud chce odebírat některé další služby CMS.

V rámci této služby je dále poskytováno bezpečné garantované připojení na Informační systém datových schránek a na portál Testa.

4.2.3 Přímé připojení k Internetu “CMS-2-1“

Jedná se o službu připojení centrálního sdíleného nekontrolovaného Internetu do IP VPN přípojky subjektu KIVS. Připojený Internet není žádným způsobem filtrován a kontrolován.

Adresní rozsahy služby „Přímé připojení k Internetu“ mohou být přiděleny z rozsahu adres CMS, nebo z adresního rozsahu vlastněného subjektem, pokud má „provider independent adresy“.

4.2.4 Bezpečné připojení k Internetu “CMS-3-1“

Jedná se o službu připojení centrálního sdíleného kontrolovaného Internetu do zákaznické VPN přípojky KIVS. Připojení má následující vlastnosti:

- veškerý provoz z/do Internetu je překládán,
- pro odchozí provoz bude dedikována pro každý subjekt 1 veřejná IP adresa z rozsahu přiděleného CMS,
- v rámci komunikace do Internetu budou nativně povoleny následující protokoly:
  - HTTP/HTTPS/FTP přes HTTP,
  - IMAP4/IMAP4S,
  - POP3/POP3S,
  - FTP

4.2.5 Přístup subjektů KIVS do zákaznické VPN přes Internet “CMS-4-1“

Služba slouží k zajištění připojení LAN sítí daného subjektu KIVS do jeho IP VPN přípojky KIVS přes Internet. Služba je určena rozsáhlým subjektům KIVS zejména pro připojení jejich regionálních pracovišť/poboček/lokalit.

Takto připojená síť má stejná přístupová práva jako standardní uživatel VPN KIVS. Přístup je realizován na bázi SSL/IPSec tunelů přes prostředí Internet.

4.2.6 Přístup koncových uživatelů subjektů KIVS do zákaznické VPN přes Internet “CMS-5-1“

Služba slouží k zajištění přístupu koncových uživatelů daného subjektu KIVS do VPN prostředí jeho přípojky KIVS.

Takto připojený uživatel má stejná přístupová práva jako standardní uživatel VPN KIVS. Přístup je realizován na bázi SSL/IPSec tunelů přes prostředí Internet.

4.2.7 Služby S-TESTA “CMS-6-1“

Jedná se o zákaznickou službu přístupu do sítě EU. Služba je vždy zřizována na základě individuálního zákaznického projektu v souladu s požadavky EU pro provoz této sítě.

4.2.8 Propojení s jiným subjektem KIVS “CMS-7-1“

Služba je určená pro vzájemnou komunikaci jednotlivých subjektů mezi sebou. Pro zřízení služby je nutný písemný souhlas obou propojovaných subjektů, až na jeho základě může být služba zřízena.

4.2.9 Služby DNS Internet “CMS-8-1“

Jedná se o jmenné služby směrem do Internetu. Služby DNS Internet jsou rozděleny do dvou oblastí:

- Služba „Primární DNS“
- Služba „Záložní DNS“

Jedná se o volitelnou službu pro subjekty, které potřebují zajistit jmenné služby v této oblasti.

4.2.10 Služby MTA "CMS-9-1"

Služba elektronické pošty zajišťuje předávání zpráv elektronické pošty jak mezi jednotlivými subjekty KIVS, tak mezi subjekty KIVS a uživateli sítě Internet. Jedná se o službu Mail Transfer Agent (MTA) – služba bude zajišťovat pouze předávání zpráv, služba nezajišťuje funkcionalitu mailových schránek.

Služba bude poskytována v rozsahu:

- Primární MTA server
- Záložní MTA server
- veškerý provoz elektronické pošty je kontrolován na přítomnost škodlivého kódu,
- subjekt má možnost zřízení karantény pro infikovaná data a zajištění přístupu do této karantény,
- subjekt má pro lepší fungování antispamové ochrany možnost využití služby LDAP CMS pro uložení všech platných emailových adres.

4.2.11 Služby DMZ1 "CMS-11-1"

Služba DMZ1 je vytvoření prostředí pro publikaci služeb subjektů KIVS do Internetu. V rámci této službu bude subjektu poskytnuto:

- vlastní virtuální FW pro vytvoření DMZ1 daného subjektu,
- konektivita této DMZ1 do Internetu,

4.2.12 Služby DMZ2 "CMS-12-1"

Služba DMZ2 je vytvoření prostředí pro publikaci služeb subjektů KIVS do CMS, nebo pro umístění back-end serverů pro publikaci aplikaci/služeb do internetu (front-end servery jsou v tomto případě v DMZ1). Službu DMZ2 je také dále možné využít pro umístění serverů subjektu bez jejich publikace do CMS (bezpečné oddělení aplikací a aplikačních serverů subjektu od jeho uživatelů).

4.3 Parametry datových služeb CMS:

Označení služby	Dostupnost	Odstranění závady
CMS-0-1	99.9%	do 4 hodin při plném výpadku
CMS-1-1	99.9%	do 4 hodin při plném výpadku
CMS-2-1	99.9%	do 4 hodin při plném výpadku
CMS-3-1	99.9%	do 4 hodin při plném výpadku
CMS-4-1	99.9%	do 4 hodin při plném výpadku
CMS-5-1	99.9%	do 4 hodin při plném výpadku
CMS-6-1	99.9%	do 4 hodin při plném výpadku
CMS-7-1	99.9%	do 4 hodin při plném výpadku
CMS-8-1	99.9%	do 4 hodin při plném výpadku
CMS-9-1	99.9%	do 4 hodin při plném výpadku
CMS-11-1	99.9%	do 4 hodin při plném výpadku
CMS-12-1	99.9%	do 4 hodin při plném výpadku

4.4 Celá infrastruktura CMS má následující technologické parametry

Název parametru	Hodnota	Popis
Propustnost core	Nx1Gbit	Možnost využít provozu v obou větvích
Propustnost do MPLS	Nx1Gbit	Každý provider má dedikován samostatný port s kapacitou 1Gbit
Propustnost do Internetu	2x1Gbit + 1x 300Mbit	Je použito připojení do NIX (český internet), s rozdělením zátěže. Takže do českého internetu je možné docílit kapacity 2Gbit Do zahraničí je připojeno pomocí samostatné linky o kapacitě 300Mbit, Celková teoretická propustnost do internetu je tedy 2.3Gbit
Propustnost do TESTA	1x2Mbit	Spojení do TESTA, je realizováno pomocí 2 linek, každá o rychlosti 2Mbit. Není nasazeno vyvažování zátěže, proto je možná kapacita do TESTA, jen poloviční kapacitou přípojných linek
Počet uživatelů pro ochranu před škodlivým kódem	unlimited	Stávající licence neomezují počet chráněných počítačů, a počet chráněných poštovních schránek
Konvergence L2	do 2 vteřin	pomocí protokolu rapid spanning tree
Konvergence L3 HSRP	do 3 vteřin	
Konvergence L3 IS-IS	do 30 vteřin	
Konvergence L3 BGP	do 180 vteřin	
Dostupnost	99.99%	Infrastruktura je redundantní, jsou 2 zařízení v jedné lokalitě. MV hledá druhou lokalitu pro oddělení větví infrastruktury

5 Definice a podmínky pro umístění systémů eGoverment do prostředí CMS a datových sálů CMS

5.1 Vlastnosti prostředí DMZ1

DMZ1 jsou tvořeny v rámci infrastruktury sdílených služeb na technologii Cisco 6509.

- Reálné adresy serverů mohou být z libovolného adresního rozsahu
  - Mohou být z privátního rozsahu (192.168, 172.17,)
  - Mohou být z veřejného rozsahu (62.168,)
  - Více zákazníků může používat stejné adresní rozsahy reálných serverů
- Realizace DMZ1 může být ve dvou variantách:
  - S překladem do internetu
  - Bez překladu do internetu (veřejné adresy na reálných serverech)
- Při využití DMZ1 jako „*frontend*“ mají systémy umístěné v DMZ1 reálnou adresu, která bude překládána:
  - Na veřejnou adresu směrem do internetu
  - Na konsolidovanou adresu (10.255-10.240) pro komunikaci s DMZ2 (backend)
  - Na konsolidovanou adresu (10.255-10.240) pro přístup subjektů KIVS z jejich VPN přes prostředí CMS

5.2 Vlastnosti prostředí DMZ2

DMZ2 jsou tvořeny v rámci infrastruktury centrálního propojovacího prostředí na technologii Cisco 6509.

- Reálné adresy serverů mohou být z libovolného adresního rozsahu
  - Mohou být z privátního rozsahu (192.168, 172.17,)
  - Mohou být z veřejného rozsahu (62.168,)
  - Více zákazníků může používat stejné adresní rozsahy reálných serverů
- Realizace DMZ2 je s překladem jen v případě, že služby jsou publikovány z DMZ2 směrem do CMS a do DMZ1. Jinak nedochází k překladu a ani k publikaci do CMS.

- Při využití DMZ2 jako „*backend*“ mají systémy umístěné v DMZ2 reálnou adresu, která bude překládána:
  - Na konsolidovanou adresu (10.255-10.240) pro komunikaci s DMZ1 (frontend)
  - Na konsolidovanou adresu (10.255-10.240) pro přístup subjektů KIVS z jejich VPN na tyto služby
- K překladu nemusí docházet jen za podmínky, že reálné adresy serverů v DMZ2 jsou již z adresního prostoru CMS (10.255-10.240)

5.3 Sdílené služby v prostředí DMZ1 a DMZ2

V prostředí DMZ1 a DMZ2 je možné využití následujících sdílených služeb:

- *L2/L3 přepínače a loadbalancery pro připojení serverů realizujících služby*
  - Switching (L2/L3)
    - 1000Base-TX, rozšiřitelná
    - 1000Base-SX/LX/ZX (GBIC nebo SFP mini GBIC), rozšiřitelná non-blocking přepínací kapacita chassis
    - podpora standardních L2 funkcí (RPST, port security, 802.1q VLAN,

        - podpora standardních L3 funkcí (VRRP/HSRP, routing static/OSPF/BGP4)
    - Aplikační load balancing (L3-L7)
        - balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů typu až do 7. vrstvy OSI (ftp, dns, http/https spod.)
        - propustnost 4 – 10 Gbit/s, rozšiřitelnost přidáním dalších modulů
        - podpora 802.1Q virtuálních rozhraní na fyzických portech
        - bridging/routing balancovací mód
        - Client/Server NAT
        - SSL hardwarová akcelerace
        - podpora režimu redundance se synchronizaci stavových tabulek
        - propustnost až 1,000,000 TCP spojení
        - podpora až 150,000 nových sestavených spojení/s
        - podporované metody pro vyvažování zátěže
            - Kruhová metoda s vážením
            - Podle počtu navázaných spojení
            - Podle otisku zdrojové a cílové adresy
            - Podle URL a cookie
        - sledování dostupnosti
- Firewalling
    - fyzická rozhraní firewallu virtualizovatelná pomocí 802.1q
    - statefull firewall, protokolová pravidla
    - zpracování překryvných adresních prostorů na jednotlivých vstupních rozhraních (fyzické resp. virtuální) do konsolidovaného adresního prostoru
    - překlady a pravidla definovatelná do samostatných vzájemně od sebe oddělených skupin (softwarové virtuální firewally)
    - až 100 virtuálních systémů (firewallů) dále rozšiřitelných v případě potřeby
    - centrální správa a úložiště pravidel na externím serveru (2x v redundantním uspořádání)
    - vzdálená konzole pro zákaznickou správu jednotlivých virtuálních systémů
    - vestavěné funkce IDS/IPS/DDoS
    - nadstavbové analytické nástroje pro vyhodnocování provozu (statistiky typů provozu, identifikace nežádoucího provozu, alarmy na přednastavené události apod.
    - podpora pro ukončení IPSec provozu na firewallu, IPSec hardwarové akcelerátory
    - podpora syslog rozhraní pro zasílání logů do centrální syslog databáze
- SSL terminace, offloading
- Využití out-of-band management sítě
- DNS
- NTP
- MTA
- Bezpečný přístup do internetu – přes proxy
- Přístup do ISDS
- Konektivita k jednotlivým subjektům a ISVS veřejné správy

5.4 Technologické podmínky pro umístění systémů eGovernment v Datových sálech CMS

5.4.1 Podmínky pro umístění technologií do datových sálů CMS

- jsou poskytovány RACKy pro systémy umístěné v datových sálech CMS na základě požadavků na napájení/chlazení (RACKy Rittal, základní rozměr je 80x100), racky je možné osadit kontrolou teploty a otevření
- zátěž podlahy je dimenzována na 850 kg/m2, při požadavku na vyšší nosnost nutno využít roznášecích roštů (zajistí provozovatel datového sálu)
- všechna zařízení musí obsahovat 2 zdroje, CMS poskytuje 2 nezávislé okruhy napájení
- realizace fyzické bezpečnosti – způsob zónování (klece, CCTV, kartový přístup...)
- metody vzdáleného přístupu (IPSEC, dial-up) přes OOB Management
- out-of-band management, technologie umístěné v CMS musí mít dedikované síťové rozhraní pro komunikaci v rámci OOB Managementu
- datové sály CMS poskytují infrastrukturu aktivních prvků (access) pro přípojení do DMZ1 a DMZ2 a OOB Managementu (rozhraní je poskytováno dle požadavků na optických nebo metalických rozhraních typu ethernet o rychlostech 10,100,1000,10000 Mbit/s
- před umístěním technologií do datových sálů je nutné specifikovat počet požadovaných RACKů, příkon a jištění, vyzářený výkon, počet portů terminálové konzole, počty portů pro L2/L3 přepínače v DMZ1, DMZ2 a OOB Managementu, využití sdílených služeb zejména požadavků na Load balancing, Firewalling, SSL terminaci a offloading, nutno specifikovat nároky systémů na eventuální realizaci geografické redundance mezi datovými sály a mód realizace infrastrukturní redundance (active-pasive, active-active), dále transport mezi lokalitami pro fibre-channel (1,2,4 Gb/s)

5.4.2 Podmínky pro dohled technologií umístěných v Datových sálech CMS

U systémů provozovaných v prostředí CMS, kde je nezbytné zajištění jednotného SLA je vyžadováno zajištění následujících vlastností dohledu:

- Konsolidace a korelace událostí a incidentů v reálném čase a root-cause
- Kompletní viditelnost všech KPI a SLA napříč aplikacemi/systémy, infrastukturou a službami CMS.
- Zajištění konsolidace fault a performance dat a napojení na tzv. umbrella dohledové prostředí MV (technologie Netcool) a automatizované propojení na servicedesk (Omnitracker), tedy jednotný dohled nad celou heterogenní technologickou, komunikační a aplikační infrastrukturou

Sledování násleujících KPI:

- Aktuální stav SLA
- Procentuální poměr, kdy je služba dostupná
- Celkový down-time služby pro dané SLA
- Zbývající čas do překročení SLA

5.4.3 Pravidla pro užívání datových sálů CMS

Využívání datových sálů CMS je podmíněno dodržováním následujících platných normativů:

1. Provozní řád datových sálu CMS
2. Pravidla KIVS a provozu Interconnectu - Procesy a Technická specifikace *(zpřístupnění na základě NDA s MVČR)*
3. Bezpečnostní politikou CMS *(zpřístupnění na základě NDA s MVČR)*
4. Závaznými procesy ServiceDesku CMS pro systémy umístěné v prostředí CMS *(zpřístupnění na základě NDA s MVČR)*
5. Pravidly jednotného monitoringu provozovaných technologií a ITIL procesů *(zpřístupnění na základě NDA s MVČR)*
6. Pravidly jednotné dokumentace provozovaných systémů a značení umístěné technologie a kabeláže *(zpřístupnění na základě NDA s MVČR)*

6 Příloha 1 – Provozní řád Datového sálu CMS

Provozní řád HC CMS

umístěného v objektu areálu MV ČR, Olšanská 4

Obsah:

Za poskytovatele : .....

Zodpovídá : .....

Schválil : .....

Za objednatele: .....

Zodpovídá : .....

Schválil : .....

Platnost od 1. 3. 2009

Vydání 5.0

1) Úvod

Provozní řád CMS upravuje provozní podmínky pro prostory HC CMS (místnosti č. 113, 114, 132) v objektu MV, Olšanská 4, Praha 3. Tyto slouží především k poskytování telehousingových služeb.

2) Oblast působnosti

Zabezpečení objektu Olšanská 4 je stanoveno samostatným předpisem, jehož vybrané části jsou uvedeny v příloze A (Dokumentace bezpečnostní ochrany objektu Olšanská 4) a odpovídá standardním podmínkám zabezpečení objektů MV a PP ČR. Vstup do prostor CMS je zabezpečen vstupním systémem napojeným na systém elektronické kontroly vstupu MV.
Pro vstup do technologických prostor HC CMS jsou určeny okruhy osob, které za dále definovaných podmínek mají oprávnění ke vstupu:

- Osoby, jež mají *oprávnění vstupu* bez nutnosti další kontroly
  i. určení zaměstnanci ČP
  ii. určení pracovníci SLZ PP ČR (správa logistického zabezpečení)
    - určení pracovníci Sekce rozvoje a projektového řízení ICT v oblasti vnitřní bezpečnosti MV ČR

- Osoby, jež mají *oprávnění ke vstupu pouze v doprovodu* oprávněné osoby
  - obslužné činnosti prostor (ostraha, úklid, údržba)

i. smluvně sjednaní dodavatelé pro servisní činnost nainstalovaných technologií HC CMS případně smluvně sjednaní dodavatelé pro instalaci nových technologií
ii. zákazníci

3) Obecné povinnosti

Všechny osoby pohybující se uvnitř prostor CMS musí dodržovat následující zásady:

- Povinností každé vstupující osoby nebo obsluhy je udržovat čistotu a pořádek.
- V prostorech CMS je zakázáno:
  i. kouřit, manipulovat s otevřeným ohněm, jíst a vykonávat další činnosti, které mohou ohrozit bezpečnost práce, apod.
  ii. řezat, pilovat a provádět jiné obdobné mechanické činnosti, při kterých vzniká prach a nečistoty
  iii. provádět činnosti, při kterých dochází k ionizaci vzduchu
- V prostorech CMS nesmí být ponechávány předměty nesouvisející s jejich provozem (papírové či dřevěné krabice, nepoužité boky rozvaděčů atd.). Za odklizení těchto předmětů zodpovídá jejich původce.
- Všechny osoby jsou povinny při pohybu v prostorách CMS používat návleky.
- Osoby provádějící v prostorách CMS montážní anebo servisní činnost musí být vybaveny vhodným a bezpečným nářadím. Elektrické ruční nářadí musí být revidováno a kontrolováno ve smyslu ČSN 331600.
- Pro připojení elektrického ručního nářadí, měřících přístrojů a počítačů používaných pro servisní činnosti musí být použity zásuvky nezálohovaného napájení 230V, které jsou umístěny po obvodech místností.

- Návštěvník je zodpovědný za škody vzniklé nedodržením ustanovení obsažených v pravidlech “Provozní řád HC CMS”.
- Provozovatel si vyhrazuje právo provádět změny pravidel v “Provozním řádu HC CMS”.
- Při jakýchkoli pochybnostech je zákazník povinen kontaktovat pracoviště Servicedesk MV a případné nejasnosti konzultovat. Telefonní číslo je uvedeno v příloze “Důležitá telefonní čísla”.
- Všichni pracovníci oprávnění ke vstupu do prostor CMS musí být prokazatelně poučeni o zásadách BOZP a PO v prostorách chráněných stabilním hasicím zařízením. Vstup osob bez prokazatelného poučení je možný pouze za trvalého dohledu osoby poučené.

4) Povinnosti zákazníků pro vstup do prostor CMS

- Chovat se v technologických prostorách v souladu s obecně závaznými předpisy z oblasti bezpečnosti práce a protipožární ochrany.
- Řídit se obecnými pravidly provozovatele, s nimiž byl prokazatelně seznámen.
- Umožnit zaměstnancům provozovatele a majitele kontrolu používaných prostorů.
- Havarijní stavy řešit jen za spoluúčasti zástupců provozovatele.
- Do technologických prostor vstupovat pouze po předchozím ohlášení ve středisku “ServiceDesk MV” a s jeho souhlasem.

- Vstupovat pouze do prostor souvisejících se smluvními závazky firmy.
- Předat zaměstnancům NOC aktualizovaný seznam osob oprávněných vstoupit do jejich prostor v CMS.
- Osobám neuvedených v seznamu oprávněných osob nebude vstup umožněn.

5) Povinnosti zákazníků pro práci v prostoru CMS

- Před výkonem jakýchkoli plánovaných prací v pronajatých technologických prostorách CMS toto oznámit prostřednictvím střediska ServiceDesk, předložit schválenou projektovou dokumentaci k odsouhlasení. Požadavek, dokumentace a seznam osob musí být doručena prokazatelnou formou (email, fax) nejméně 3 pracovní dny předem.
- V případě provádění takovýchto prací a rozmísťování technologie je nutné respektovat stávající systém kabeláže, jak optické, tak metalické.
- Instalovat kabely mimo prostor pronajatý zákazníkovi je zakázáno.
- V žádném případě není dovoleno zasahovat do již existující kabeláže bez předchozí konzultace s odpovědnými osobami provozovatele CMS.
- Po ukončení prováděných prací je povinností zákazníka po sobě uklidit a to jak vnitřní, tak i vnější prostory.
- Jestliže dochází při demontáži technologie k rozebírání jednotlivých dlaždic zdvojené podlahy, je z důvodů stability dovoleno rozebrat nejvíce 2 sousední dlaždice. Po skončení prací musí být dlaždice řádně upevněny.
- Činnosti jako je řezání, pilování a ostatní, při kterých vznikají prach a nečistoty, jsou zakázány v prostorech CMS.

6) Povinnosti servisního střediska provozovatele CMS

Pracovníci servisního střediska provozovatele CMS mimo své povinnosti v oblasti servisu a dohledu vykonávají veškerou činnost související s provozem technologických prostor v CMS zejména:

- Doprovází zákazníka do technologických prostorů.
- Předávají pracoviště zákazníkům, podle povahy a rozsahu činností, určí, zda budou na činnost zákazníka dohlížet nebo ne.
- Provedou záznam o provedené činnosti do provozního deníku se záznamem času, data, kdo činnost provedl a podpis, kdo záznam udělal.
- Vedou úplnou evidenci (provozní deník) o provozu v technologických prostorách CMS.
- Provádějí pravidelné kontroly prostor CMS.
- udržují trvalý přehled o osobách a jejich zamýšlené činnosti v prostorech CMS.

7) Systém vstupu do prostor CMS a hospodaření s klíči

Prostory HC CMS jsou vybaveny automatickým dveřním vstupním systémem napojeným na systém elektronické kontroly vstupu objektu MV, Olšanská 4. Oprávnění pracovníci provozovatele jsou vybaveni čipovými kartami s příslušným oprávněním.

Ke každé zámkové vložce existují tři klíče, jeden klíč je trvale umístěn v prosklené schránce napojené na systém elektronické kontroly vstupu (EKV). Schránky jsou umístěny na vnitřní straně dveří. Klíče slouží pro nouzové otevření dveří (odchod) při poruše elektrického zámku. O použití klíče (vyjmutí ze schránky) je dotyčný pracovník povinen vyrozumět ostrahu objektu, ostraha následně zajistí cestou správce objektu opravu elektrického zámku, vložení klíče do schránky a osazení nového krycího sklíčka. Zbylé dva klíče od prostor HC CMS s označením jednotlivých místností jsou uloženy v pečetěné krabičce u ostrahy objektu. Jejich použití je přípustné pouze v případě havárie. Použití klíčů a následný vstup do prostor CMS je ostraha povinná hlásit na pracoviště ServiceDesk. O použití klíčů pořizuje ostraha písemný záznam (včetně záznamu o použití klíčů pro nouzové opuštění prostor CMS) s uvedením následujících údajů:

a. Datum a čas zapůjčení klíčů
b. Které klíče byly zapůjčeny
c. Jméno a zaměstnavatel, číslo OP nebo služebního průkazu
d. Druh události
e. Datum a čas odevzdání klíčů
f. Při použití klíčů pro nouzové opuštění prostor CMS cestou správce objektu zajistit uvedení schránky s klíčem do původního stavu

8) Úklid

Úklid prostor CMS zajišťuje správa budovy. V příloze B je uveden grafický popis prostor a v příloze C je popis činností při úklidu.

9) Technologické zabezpečení prostor CMS

- Určené prostory CMS jsou vybaveny kamerovým systémem, záznamy z kamer jsou uchovávány 7 dní, podpůrné technologie (UPS, DA, chladící jednotky) mají instalován dálkový dohled, monitoring uvedených technologií zajišťuje servisní středisko.

- Místnost technologie (č. 114) je chráněna plynovým stabilním hasicím zařízením. Kromě toho je prostor CMS napojen na systém EPS instalovaný ve vybraných prostorách objektu Olšanská.
- Technologické skříně ve stojanových řadách jsou vybaveny teplotními čidly s hlídáním maximální teploty ve skříni (35°C) a dveřními kontakty (zadní i přední dveře) signalizující otevření skříně, monitoring zajišťuje servisní středisko.

10) Důležitá telefonní čísla

ServiceDesk MV:	+420 974 841 130
Správce prostor CMS (p.Fatyka):	+420 974 848 360
Vedoucí areálu Olšanská 4 (p. Medeši):	+420 974 841 271

Ostraha budovy: +420 974 841 643

11) Přílohy

A. Dokumentace bezpečnostní ochrany objektu Olšanská 4 obsahující:
- Bezpečnostní posouzení objektu
- Provozní řád objektu
- Plán obrany objektu
- Havarijní plán objektu
- Grafický popis objektu

B. Grafický popis prostor HC CMS

C. Seznam činností při úklidu v prostorech HC CMS

D. Pokyny pro ostrahu při aktivaci SHZ

Uvedené přílohy nejsou součástí hlavního dokumentu. Na vyžádání je poskytne pracoviště Servicedesku MV.