



Příloha č. 1 – Technická specifikace

1. Rozšíření B2B kanálu

1.1.1 Popis B2B kanálu

Infrastruktura B2B doplňuje funkcionalitu aplikační vrstvy datových center ČSSZ o komunikační kanál na externí systémy umístěné jak v Extranetu prostřednictvím VPN, GovNet či GovBone tak i v Internetu. Infrastruktura B2B centralizuje bezpečnostní standardy pro komunikaci s externími subjekty a zajišťuje plné oddělení aplikační vrstvy. B2B kanál zajišťuje publikování interní VIP pro jednotlivé externí zdroje, filtrování provozu na http proxy serveru a navazování zabezpečeného SSL spojení autentifikovaného pomocí klientských certifikátů. Stávající infrastruktura B2B kanálu byla navržena pro zajištění odchozí komunikace založené na HTTP/HTTPS protokolu.

Stávající infrastruktura B2B kanálu má být nahrazena univerzálním komunikačním kanálem v projektu 159.

1.1.2 Požadavky na rozšíření B2B

V průběhu integrace systémů komunikujících na agendy základních registrů vznikly požadavky na rozšíření B2B kanálu o funkcionalitu:

- Zpracování klientských certifikátů podepsaných hash funkcí SHA-2
- Podpora protokolu FTP

Klientské certifikáty poskytují základní bezpečnostní prvek pro autentifikaci klientského přístupu na portálové aplikace pomocí protokolu SSL. Na základě požadavku MV ČR mají od 1.1.2010 tvůrci aplikací, ve kterých je elektronický podpis používán, využívat hash funkce třídy SHA-2. Pro vytváření elektronického podpisu je možné po přechodnou dobu nadále používat algoritmus SHA-1, nejdéle však do 31. 12. 2010. SHA-2 je rodina čtyř hashovacích funkcí (SHA-224, SHA-256, SHA-384 a SHA-512), které jsou součástí standardu FIPS PUB 180-2 a u kterých dosud nebyly nalezeny bezpečnostní slabiny. Stávající infrastruktura B2B kanálu nepodporuje zpracování klientských certifikátů s elektronickým podpisem SHA-2 a vzhledem k životnímu cyklu zařízení již nebude tato hash funkce do zařízení implementována výrobcem.

1.1.3 Návrh na rozšíření B2B

Doplnění požadovaných funkcionalit do B2B kanálu navrhujeme realizovat náhradou Cisco CSS v B2B kanálu aplikační vrstvy za virtuální HTTP/HTTPS/FTP proxy servery a úpravou jejich programového vybavení.

Požadavky na 2x virtuální servery:

- 1 GB RAM
- 20 GB HDD
- Bez OS

Navrhovaná řešení jsou cenově efektivní bez investic do nových zařízení zachovávající centrální správu bezpečnostních standardů pro komunikaci na externí subjekty.

Naše nabídka neobsahuje:

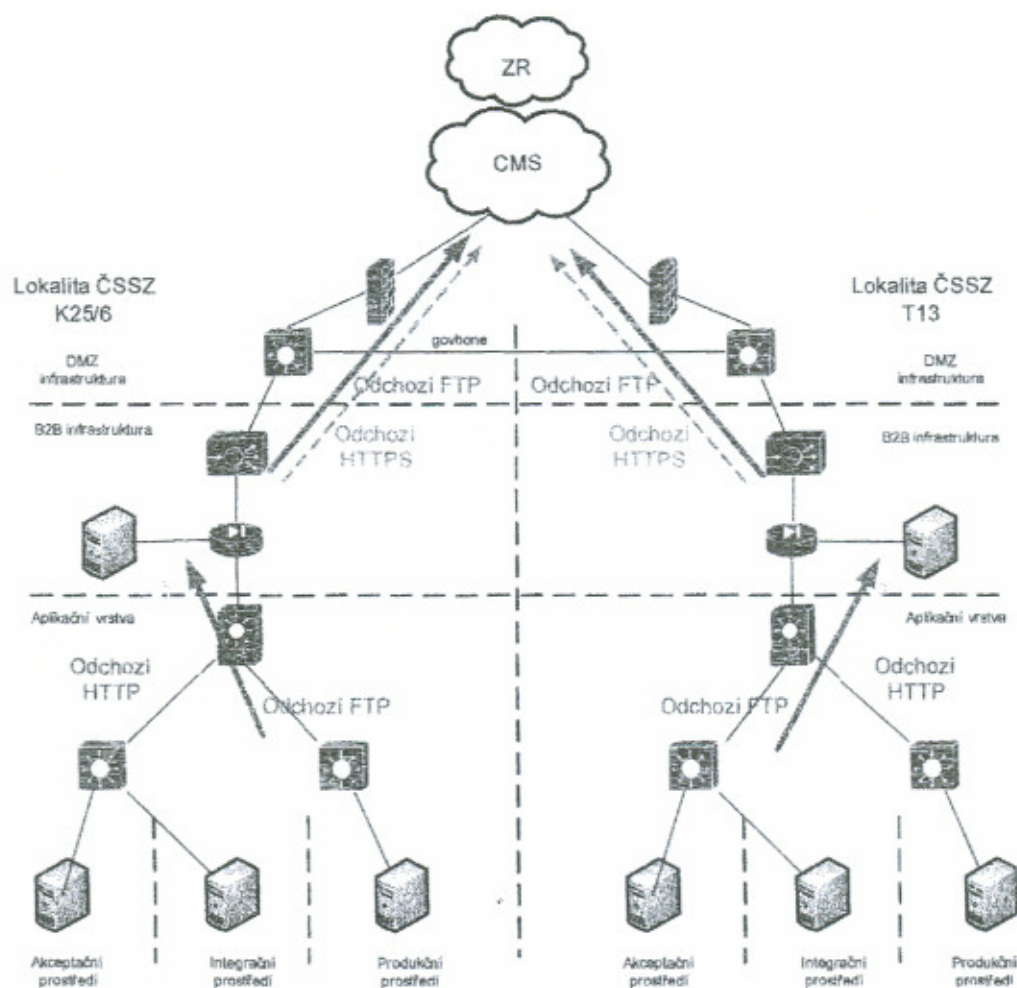
Dodávku HW či SW komponent.



Smlouva na rozšíření B2B kanálu a Provisioning systému



1.1.4 Schéma řešení





Smlouva na rozšíření B2B kanálu a Provisioning systému



2. Rozšíření Provisioning systému

2.1.1 Popis Provisioning systému

Vzhledem k centralizaci aplikací je pro ČSSZ infrastruktura datových center jednou z kritických oblastí. Provisioning systém umožňuje administrátorům ČSSZ konfigurační správu infrastruktury datových center, přepínačů, loadbalancerů, serverů a aplikací umístěných v jednotlivých prostředích aplikační vrstvy datových center, změnu jejich administrativního stavu a začlenění do provozu.

Provisioning systém zajišťuje nastavení síťového prostředí dle požadavků specifikovaných v předpřipraveném schématu. Tento systém nastavuje konfiguraci síťových přepínačů v aplikační vrstvě, nastavuje konfiguraci load balancing ACE modulů a jeho kontextů. Všechna tato nastavení se týkají všech virtuálních prostředí v ČSSZ.

Důležitou součástí celého systému je i správa adresního prostoru a síťových parametrů všech aplikací. K jeho dalším funkcionalitám patří nastavení RSPAN pro troubleshooting serverů či aplikačního rozhraní.

Celý systém je základním pilířem pro nasazení nových aplikací či jejich funkcionalit / změn do aplikačního prostředí.

Stávající instalace provisioning systému podporuje správu maximálně 400 fyzických či virtuálních zařízení umístěných v datacentrech, přičemž limit již byl dosažen.

2.1.2 Návrh na rozšíření Provisioning systému

Navrhujeme rozšíření Provisioning systému o možnost přidávání dalších serverů, přepínačů a spravovaných zařízení s celkovým počtem spravovaných zařízení 1.000.

Dodávka neobsahuje:

Dodávku HW či SW komponent.