

Příloha č. 5

ČÁST D

Předmět plnění části D veřejné zakázky, s názvem **Zajištění služeb datového centra pro IS CERTIS**

1. Předmět plnění

Předmětem plnění této části veřejné zakázky je zajištění služeb provozu technické infrastruktury nezbytných pro provoz informačního a komunikačního systému zadavatele (IS CERTIS), který bude využíván pro realizaci společné části maturitní zkoušky (SČ MZ).

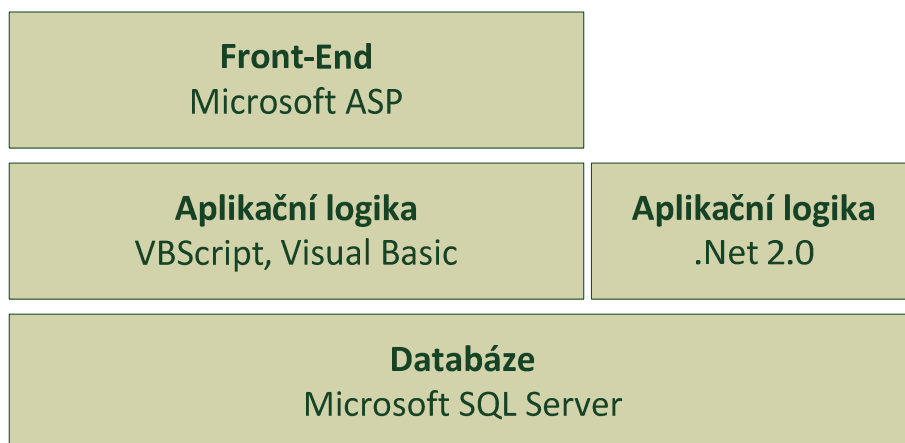
Jedná se o zajištění hardware (HW) a software (SW), instalace HW a SW, umístění v hostingovém centru určeném zadavatelem a následné provozování včetně dohledu a monitoringu této technické infrastruktury formou služby.

Technická infrastruktura a její provozní parametry musí splňovat požadavky vysoké bezpečnosti, dostupnosti a výkonu, a to zejména v období kritické služby definované v SLA. Infrastruktura musí umožňovat vertikální i horizontální škálování podle reálných potřeb, jejich postupného upřesňování a nárůstu. Dalším požadavkem je zajištění kompletního provozního a bezpečnostního dohledu a monitorování.

2. Specifikace požadovaných služeb

2.1 Charakteristika provozovaného IS CERTIS

A) Aplikační architektura (blokový model aplikační architektury)



B) Kapacitní specifikace

Počet lokalit přístupujících uživatelů IS CERTIS	1.500
Počet ředitelů škol	1.500
Počet zástupců ředitelů škol	1.500
Počet školních maturitních komisařů	2.000
Počet evidovaných hodnotitelů (ČJL, CJ apod.)	5.000
Počet raterů (hodnotitelů otevřených otázek didaktických testů)	5.000
Odhad počtu uživatelů pro zpracování dat MZ	10.000
Předpokládaný počet současně přihlášených externích uživatelů	3.000
Celkový počet otevřených úloh pro hodnocení	2.000.000
Počet úloh (dokumentů) celkem	6.000.000
Předpokládaná průměrná velikost naskenované části (výstřižku) záznamového archu s odpovědí na otevřenou otázku	50 kB
Předpokládaná velikost naskenované strany dokumentu A4	150 kB
Průměrná doba hodnocení jedné otevřené úlohy vzdáleným hodnotitelem – raterem (ČJL, CJ)	10 sekund
Průměrná doba hodnocení jedné otevřené úlohy vzdáleným hodnotitelem – raterem (MAT)	180 sekund
Počet maturujících žáků v jednom ročníku	110.000
Počet tříd v jednom ročníku	4.000
Počet učeben	10.000
Velikost záznamového archu – počet listů	Max 20
Celkový počet stran A4 záznamových archů pro jedno provedení MZ	2.500.000
Počet výčetek na učebny	30.000
Prezenční listiny	30.000
Doba přenosu dat z digitalizačního centra v hodinách	Max 24
Doba automatického vyhodnocení jednoho předmětu (hodin)	Max 72

Význam zkratk:

ČJL-český jazyk a literatura, CJ-cizí jazyk, MZ-maturitní zkouška, SČ MZ-společná část maturitní zkoušky

C) Charakter zátěže a její rozdělení v čase

Zkoušky SČ MZ se konají v jarním zkušebním období a podzimním zkušebním období.

Konkrétní termíny konání didaktických testů a písemných prací a termíny ústních zkoušek SČ MZ v roce 2010 jsou již známy, pro rok 2011 je určí MŠMT nejpozději do 31. 3. 2010.

Příprava a realizace SČ MZ se dělí na jednotlivé časové úseky, pro které je charakteristická konkrétní aktivita specifické skupiny uživatelů a/nebo samotného systému. Specifickým faktorem, který ovlivňuje technologickou infrastrukturu, je extrémně vysoký nárok na

spolehlivost a výkonnost v některých časových úsecích, které jsou na kritické cestě maturitního schématu a nemají žádnou vnitřní časovou rezervu.

IS CERTIS je evidenční informační systém, s přístupem uživatelů pomocí webového front-endu a využívající silný databázový stroj. Využívá přitom třívrstvou architekturu (databázová vrstva – aplikační vrstva – portál).

S ohledem na záměry a koncepci řešení, spočívající v upgrade a nutných úpravách stávající verze IS CERTIS, při dodržení požadavku na minimalizaci změn, nedojde k zásadním změnám v koncepci stávajícího informačního systému. S tím je nutné počítat zejména při návrhu možného škálování a při výkonovém dimenzování jednotlivých komponent.

D) Požadavky na IS CERTIS podle období v roce 2009 a 2010

Období	Počet současně pracujících uživatelů	Činnost	Poznámka
15.11.09 - 30.11.09	1 500	Ředitelé škol zadávají údaje z vyplněných přihlášek žáků do systému CERTIS	Předpokládá se zvýšený nápor během pracovní doby a v závěru období.
1.12.09 – 10.12.09	1 500	IS CERTIS generuje opis přihlášek s vyplněnými údaji a zpřístupní je školám k tisku a distribuci. Ředitelé škol provádějí případné opravy a změny administrativních údajů přihlášek.	Předpokládá se zvýšený nápor během pracovní doby a v závěru období.
1.12.09 – 10.12.09	1 500	IS CERTIS provede pro každou školu výpočet rozdělení přihlášených žáků do jednotlivých zkušebních učeben podle předmětů a dalších podmínek (max. 17 žáků, rovnoměrné využití učeben)	Předpokládá se zvýšený nápor během pracovní doby a v závěru období.
10.12.09	-	Tvorba výrobního a kompletačního schématu.	
21.1.10. - 25.1.10	1 500	IS CERTIS vygeneruje pro všechny žáky individuální	

		pozvánky k SČ MZ.	
25.1.10	1 500	IS CERTIS zpřístupní pozvánky školám k tisku a distribuci žákům. Ředitelé pozvánky (včetně předmětu, místa, času a učebny) vytisknou a předají žákům.	
1.2.10 – 1.3.10	2 000	Jmenování školních maturitních komisařů pro jednotlivé školy s podporou IS CERTIS.	
12.4.10 – 3.5.10	1 500	Ředitelé denně zadávají informace o průběhu SČ MZ na dané škole (didaktické testy a písemné práce).	
24.5.10 – 4.6.10	1 500	Ředitelé denně zadávají informace o průběhu SČ MZ na dané škole (dílní ústní zkoušky).	
18.4.10 – 27.4.10	-	IS CERTIS přebírá z digitalizačního pracoviště digitalizovaná data didaktických testů (ČJL, AJ, NJ) včetně kontrol. IS CERTIS vypočítává bodové ohodnocení uzavřených úloh a do fronty k bodování řadí „výřezy“ úloh otevřených.	ČJL je pro všechny žáky povinným předmětem.
18.4.10 – 9.5.10	1 000	Rateři v IS CERTIS vzdáleně hodnotí (bodují) otevřené úlohy didaktických testů (ČJL, AJ, NJ) podle „výřezů“ z didaktických testů.	Každou odpověď hodnotí nezávisle na sobě dva rateři a v případě kolize určí výsledek třetí rater (senior).
24.4.10 – 29.4.10	-	IS CERTIS přebírá z digitalizačního pracoviště digitalizovaná data didaktických testů (FJ, ŠJ, RJ)	

		včetně kontrol. IS CERTIS vypočítává bodové ohodnocení uzavřených úloh a do fronty k bodování řadí „výřezy“ úloh otevřených.	
30.4.10 – 9.5.10	800	Rateři v IS CERTIS vzdáleně hodnotí (bodují) otevřené úlohy didaktických testů (FJ, ŠJ, RJ) podle „výřezů“ z didaktických testů.	Každou odpověď hodnotí nezávisle na sobě dva rateři a v případě kolize určí výsledek třetí rater (senior).
17.4.10 – 4.6.10	-	IS CERTIS přebírá z digitalizačního pracoviště digitalizovaná data didaktických testů (MA a ostatní) včetně kontrol. IS CERTIS vypočítává bodové ohodnocení uzavřených úloh a do fronty k bodování řadí „výřezy“ úloh otevřených.	
17.4.10 – 9.5.10	1200	Rateři v IS CERTIS vzdáleně hodnotí (bodují) otevřené úlohy didaktických testů (MA a ostatní) podle „výřezů“ z didaktických testů.	Každou odpověď hodnotí nezávisle na sobě dva rateři a v případě kolize určí výsledek třetí rater (senior).
9.5.10 - 10.5.10	-	IS CERTIS vypočte vyhodnocení výsledků maturitní zkoušky včetně podkladů pro potřeby ústřední maturitní komise s použitím základní prahové hodnoty (hranice úspěšnosti) jako podklad pro její úpravu.	
11.5.10 – 12.5.10	-	IS CERTIS vypočte vyhodnocení výsledků maturitní zkoušky včetně podkladů pro potřeby ústřední maturitní komise s použitím upravené prahové hodnoty	

		(hranice úspěšnosti).	
24.5.10 – 7.6.10	1500	Ředitelé průběžně vkládají výsledky ústních zkoušek	
24.5.10 – 7.6.10	-	IS CERTIS zpracuje výsledky dílčích ústních zkoušek společné části MZ	
8.6.10 – 9.6.10	-	IS CERTIS provede analytické zpracování celkových výsledků zkoušek SČ MZ	
10.6.10 – 11.6.10	-	IS CERTIS provede na základě případného rozhodnutí MŠMT analytické zpracování celkových výsledků zkoušek SČ MZ s upravenou hranicí úspěšnosti.	
12.6.10 – 13.6.10	-	IS CERTIS vygeneruje pro všechny žáky Protokol o výsledcích žáka u zkoušek SČ MZ	
14.6.10	1500	IS CERTIS zpřístupní ředitelům škol Protokoly o výsledcích žáků u zkoušek SČ MZ.	
25.6.10 – 30.6.10		Přihlášení žáků ředitelem SŠ k MZ do IS CERTIS k podzimnímu zkušebnímu termínu	
1.7.10 – 7.7.10		Zpracování dat/přihlášek žáků k danému termínu MZ – fáze 1	
7.8.10 – 8.8.10		Zpracování dat/přihlášek žáků k danému termínu MZ – fáze 2	
6.9.10 – 14.9.10		Konání písemných zkoušek společné části MZ ve škole k podzimnímu zkušebnímu termínu	

6.9.10 – 15.9.10		Hodnocení písemných prací ve školách	
6.9.10 – 29.9.10		Zadání výsledků hodnocení PP ředitelem školy do IS CERTIS	
27.9.10 – 4.10.10		Vyhodnocení a zpracování výsledků DT z ČJL, AJ, NJ	
27.9.10 – 4.10.10		Vyhodnocení a zpracování výsledků DT z FJ, ŠJ, RJ	
27.9.10 – 8.10.10		Vyhodnocení a zpracování výsledků MA	
27.9.10 – 4.10.10		Vyhodnocení a zpracování výsledků ostatních zkoušek	
20.9.10 – 29.10.10		Konání profilové části maturitní zkoušky	
20.9.10 – 4.10.10		Zadání výsledků hodnocení ÚZ (SČ MZ) ředitelem školy do IS CERTIS k podzimnímu zkušebnímu termínu	
20.9.10 – 4.10.10		Zpracování výsledků dílčích ústních zkoušek společné části MZ k podzimnímu zkušebnímu termínu	
5.10.10 – 6.10.10		Analytické zpracování celkových výsledků zkoušek SČ MZ k podzimnímu zkušebnímu termínu	
9.10.10 – 10.10.10		Generování Protokolů o výsledcích žáka u zkoušek SČ MZ k podzimnímu zkušebnímu termínu	
11.10.10 – 11.10.10		Protokoly o výsledcích žáků u zkoušek SČ MZ v daném termínu – zpřístupnění ředitelům škol (elektronicky)	

Význam zkratk:

ČJL-český jazyk a literatura, AJ-anglický jazyk, NJ-německý jazyk, FJ-francouzský jazyk, ŠJ-španělský jazyk, RJ-ruský jazyk, MA-matematika, Dě-dějepis, CJ-cizí jazyk, ZA-záznamový arch

DT-didaktický test, ÚZ-ústní zkouška

E) Požadavky na IS CERTIS v kalendářním roce 2011

Budou vycházet z termínů konání písemných a ústních zkoušek SČ MZ, které určí Ministerstvo školství mládeže a tělovýchovy nejpozději do 31. 3. 2010. Lze předpokládat, že odchylky od výše uvedených období v r. 2010 by se měly pohybovat nejvýše v řádu dnů.

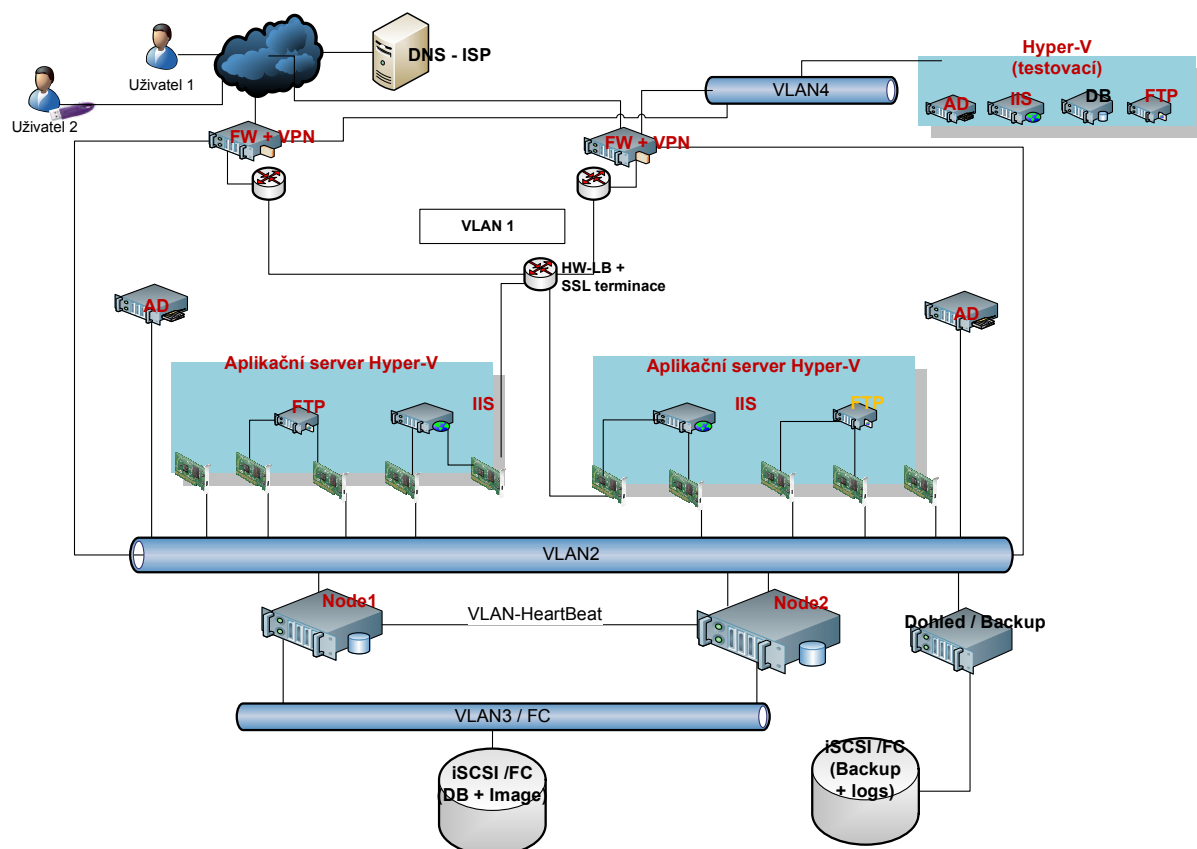
Z uvedených požadavků vyplývá, že lze předpokládat následující typické režimy ve špičkách:

- současné zadávání dat relativně malého objemu jednotlivými školami;
- vzdálené hodnocení otevřených úloh raterů, kdy rater na základě obrazu („výřez“ záznamového archu) hodnotí a zadá bodovou hodnotu výsledku odpovědi;
- výpočet výsledků pro všechny školy, žáky, zkoušky a jejich části;
- výpočet podrobných statistik;
- generování výstupních protokolů pro jednotlivé žáky a školy pro tisk na jednotlivých školách.

2.2 Architektura a základní požadavky na infrastrukturu pro IS CERTIS

A) Architektura

Schéma architektury infrastruktury IS CERTIS je následující:



Bližší popis a rozpad jednotlivých komponent je uveden v dalších kapitolách této specifikace.

Požadované vlastnosti

Pro zajištění vysokého výkonu a dostupnosti, stejně jako pro umožnění škálovatelnosti, vycházejí požadavky zadavatele z těchto parametrů:

- použití technologie určené pro 24x7 provoz s vysokou dostupností;
- dostatečně výkonné servery s možností škálování (procesory, paměť);
- oddělení kritických částí systému na samostatné specializované výkonné uzly;
- zajištění vysoké dostupnosti:
 - loadbalancing u aplikačních serverů;
 - clustering (Active/Pasiv nebo Active/Active) u databázového serveru;
 - zajištění dostatečné redundance prvků;
- nastavení dostatečné konektivity;
- zajištění dohledu a monitoringu.

Uvedené požadavky vedou k použití hardwarového load balancingu, hardwarové SSL akcelerace a k použití samostatných aplikačních serverů a databázového serveru (v clusteru Active/Pasiv nebo Active/Active).

B) Škálovatelnost

Minimální konfigurace vychází ze stávajících zkušeností se systémem IS CERTIS a bere ohled na předpokládané zvýšené nároky, kladené na upgradovaný a upravený IS CERTIS.

Zadavatel požaduje, aby po provedení testů IS CERTIS a/nebo na základě výsledků generální pilotáže SČ MZ (maturitní generálky MAG09 - 2,3) v říjnu 2009, bylo možné dále uvedené konfigurace změnit (navýšit výkon a/nebo kapacitu, případně další úpravy), pokud tato potřeba nastane.

V případě problémů s propustností systému je, kromě vertikálního upsizingu jednotlivých kritických uzlů nutné předpokládat další opatření:

Potřeba navýšení	Opatření
Propustnost na vstupu do FW	Zajistit a nastavit rychlejší konektivitu u poskytovatele služeb. Zadavatel požaduje zajistit a nastavit rychlejší konektivitu v průběhu zkušebního provozu a maturit.
Propustnost FW	Přidat další FW do LoadBalancingu
Propustnost IIS – Aplikačního serveru	<p>Přidání 2 serverů a přidání do loadbalancingu (pokud bude nutné zvýšit propustnost o hodnotu do 50%)</p> <p>Pokud bude 100% vytíženost aplikačních serverů, bude třeba přidat 1 server v režimu „Hot Standby,, pro okamžité řešení výpadku některého serveru v průběhu kritického období.</p> <p>V případě 75% vytížení připravit i 1 virtuální server umístěný na Hyper-V server, který v případě výpadku jednoho IIS serveru bude aktivován a přidán do LB</p>
Propustnost DB	<p>Rozdělení DB na více DB a přejít z režimu Active/Pasiv na režim Active/Active.</p> <p>Doplnit 1 - 2 servery a upravit databázovou konfiguraci na replikace databází.</p>

V případě prokázané potřeby provádět upsizing HW a provádět zásadnější změny v konfiguraci zadavatel předpokládá, že tyto činnosti budou prováděny mimo krizová období. Dále akceptuje fakt, že požadované úpravy budou časově náročné (cca jednotky dnů), což by bylo řešeno jednorázovou úpravou SLA podmínek.

Za předpokladu, že pro zadavatele bude nezbytné příslušné konfigurace změnit (navýšit výkon a/nebo kapacitu, případně další úpravy), bude takové plnění zadavatelem poptáno v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách, v platném znění.

2.3 Podrobná specifikace požadovaných služeb

Zadavatel požaduje, aby vybraný uchazeč zajistil následující třídy služeb:

- zadavatel požaduje pro služby datového centra pro IS CERTIS zřízení služby tj. zajištění dále popsané HW konfigurace a SW komponent včetně implementačních, instalačních a konfiguračních prací. Požadavky jsou členěny na oblast serverů, databáze, síťových služeb a konektivity;
- zadavatel požaduje instalaci a konfiguraci systémů a relevantního SW nejpozději do 1. 10. 2009;
- zadavatel dále požaduje pro zajištění provozu IS CERTIS níže specifikované služby.

A. Zřízení služby

Minimální požadavky na konfiguraci HW

Minimální konfigurace vychází ze stávajících zkušeností s IS CERTIS a bere ohled na předpokládané zvýšené nároky, kladené na upgradovaný a upravený IS CERTIS.

Procesory:

Všechny servery budou osazeny procesory min. Quad-Core x64 (64 bitová technologie s podporou virtualizace)

Rychlost odezvy:

U celé aplikace je zásadní dostatečná rychlost odezvy z pohledu uživatele. Jestliže uživatel, při svém dostatečně rychlém připojení na internet, bude na zobrazení stránky čekat déle než několik sekund, bude pokládat aplikaci za nefunkční. V současné době

nelze sice v této oblasti přesně specifikovat výkonové požadavky, je však možno vyjít z představy hromadného přístupu cca 1500 uživatelů, stahujících stránky o velikosti cca 300 kB, přičemž tyto stránky jsou dynamicky generovány na základě dat v databázi. Nezbytný je dostatečný výkon celého řetězce (databáze - IIS - SSL - Firewall - internet). Jako nejkritičtější se jeví především nároky během procesu vzdáleného hodnocení otevřených otázek ratery. Je skutečností, že při stávajícím vybavení zadavatele nedošlo v rámci testování "maturity nanečisto" k zásadním problémům s pomalostí odezvy při práci raterů, ovšem pro relativně malý počet současně hodnotících (cca několik desítek). V každém případě je třeba orientovat se na takové technologie, které umožní měření kritických parametrů a pak v případě potřeby optimalizaci a scale-up v závislosti na zjištěních, získaných během maturitní generální zkoušky a výkonnostních testů.

a) Výkonnost webového (IIS) serveru, cache:

Výkonnost webového (IIS) serveru může být v kladném i záporném směru ovlivněna také způsobem nastavení a využití (či nevyužití) cache, přičemž IIS v.7 pro tento účel nabízí celou řadu možností, včetně tzv. Smart-Cache. S ohledem na to, že se v rámci aplikace CERTIS jedná převážně o dynamické stránky, bude využití cache IIS spíše výjimečné. Optimalizaci bude možné provést až po zjištění a rozboru úzkých míst v průběhu MAG09 – 2,3. V každém případě je nutno počítat s tím, že právě oblast IIS Cache bude nutné průběžně sledovat a vyhodnocovat - jak ze strany autorů aplikace, tak ze strany poskytovatele a správce systému.

b) Databázový server

4 procesory, 64 GB RAM, min 4x HD SAS disky s 15000 otáčkami, konstrukce odpovídající požadavkům na vysokou dostupnost v režimu 24 x 7 (redundance klíčových prvků), dostatečná rezerva na scale-up (zvýšení počtu procesorů, rozšíření paměti). Odpovídající počet síťových karet pro realizaci clusteru a v případě použití iSCSI diskového pole zajištění dostatečné propustnosti (min 4GB/s).

c) Aplikační Hyper-V server

4 procesory, 32 GB RAM, konstrukce odpovídající požadavkům na vysokou dostupnost v režimu 24 x 7 (redundance klíčových prvků), dostatečná rezerva na scale-up (zvýšení počtu procesorů, rozšíření paměti).

d) Testovací server

V podstatě totožný server jako server databázový, s dostatečnou kapacitou disku, 4 procesory, 32 GB RAM, HD SAS disky 4x300 GB s 15000 otáčkami.

e) Služby sítě

Aplikační Hyper-V server bude hostit virtuální servery IIS a FTP.

f) Dohledový / Backup server

2 procesory, 4 GB RAM, konstrukce odpovídající požadavkům na vysokou dostupnost v režimu 24 x 7 (redundance klíčových prvků). Slouží pro monitorování a měření výkonu a dostupnosti a k provádění zálohování.

g) AD server

2 procesory, 4 GB RAM, konstrukce odpovídající požadavkům na vysokou dostupnost v režimu 24 x 7 (redundance klíčových prvků). Slouží k autentizaci a autorizaci uživatelů IS CERTIS.

h) Disková pole

iSCSI /FC - BD +Image

Diskové pole pro databázový server a ukládání digitalizovaných dat a obrazů naskenovaných úloh.

Konfigurace diskového pole: kapacita min. 2 TB, cache 2GB/řadič, vysoká dostupnost a redundance + failover (řadič, procesor, zdroje a chlazení) včetně dual RAID. Nezbytná je rychlá I/O odezva.

iSCSI /FC – Backup +logs

Diskové pole pro operativní zálohování a ukládání auditů informací z jednotlivých serverů sítě CERTIS

Konfigurace diskového pole: kapacita min. 2 TB, cache 2GB/řadič, vysoká dostupnost a redundance + failover (řadič, procesor, zdroje a chlazení) včetně dual RAID. Nezbytná je rychlá I/O odezva.

Požadavky na produkční prostředí

a) Prezentační a aplikační vrstva

Je primárně řešena pomocí minimálně 2 IIS serverů s podporou SSL akcelerace. Síťový provoz na tyto servery je rozdělován předřazeným hardware Load Balancerem. Pro autentizace jsou využívány služby AD.

b) Databázová vrstva

Dva uzly clusteru Windows Server 2008, ve kterém je provozován databázový server MS SQL v režimu active-passive. Ve schématu označeno jako NODE1,2. Vzhledem k dosud hůře odhadnutelné zátěži je nutné, aby tento server měl dostatečné kapacitní rezervy, které lze využít pouze přidáním CPU a paměti.

c) FTP server

slouží k ukládání digitalizovaných dat do datového úložiště diskového pole.

d) Doménové řadiče (AD)

Dva doménové řadiče, které slouží k autorizaci a autentizaci uživatelů, administrátorů a pracovníků digitalizačního pracoviště k prostředkům sítě IS CERTIS na základě výslovných oprávnění, které jsou jednotlivým účtům uživatelů sítě přiděleny k příslušným prostředkům.

Předpokládá se, že do sítě IS CERTIS budou převedeny stávající účty uživatelů IS CERTIS upgradem stávající Active Directory 2003 na Active Directory 2008 s využitím současného doménového řadiče sítě IS CERTIS.

e) IIS server

Dva virtuální webové servery, provozované v Hyper-V a využívající dva síťové porty:

- první síťový port (Cluster adapter) je připojen do VLAN1, která poskytuje konektivitu uživatelům aplikace IS CERTIS k aplikačním serverům.
- druhý síťový port (Management adapter) je připojen do VLAN2, která slouží pro správu serveru a zpřístupňuje IIS ostatním serverům sítě

f) Dohledový server

vybavený SMS bránou sloužící k průběžné kontrole parametrů dostupnosti a kapacity.

Požadavky na testovací prostředí

Testovací server bude realizován v rámci jednoho serveru, s využitím virtualizační technologie Microsoft Hyper-V. Bude obsahovat všechny potřebné prvky sítě IS CERTIS, tedy AD, IIS, DB, FTP.

Ukládání dat

Databázové servery budou doplněny o vhodnou variantu diskového pole, které bude sloužit k ukládání digitalizovaných dat a obrazů naskenovaných úloh.

Dále se diskové pole bude využívat pro ukládání auditních informací ze všech prvků systémů a ukládání operativních záloh (image serverů).

B. Zajištění provozu technické infrastruktury

Zadavatel požaduje kompletní technické zajištění služeb provozu technické infrastruktury nezbytných pro provoz IS CERTIS, tedy poskytování níže vyjmenovaných služeb s uvedenými parametry.

Služba podpory provozu je poskytována pro:

- instalace HW a SW včetně konfigurace
- zajištění provozu technické infrastruktury pro IS CERTIS
- zajištění podpory pro vývoj a implementaci IS CERTIS
- zajištění zálohování serverů IS CERTIS
- správa systémů a monitoring

ad Zajištění provozu technické infrastruktury pro IS CERTIS

- zajištění dohledu nad systémy (monitoring)
- zajištění administrace systémů
- odstraňování problémů na systémech
- zajištění změn konfigurací – Change Request
- profylaxe systémů
- správa a zálohování dat
- tvorba a údržba provozní dokumentace
- evidence Change Requestů a Activity reportů, provázání na uživatelskou podporu
- pravidelné vykazování provozních statistik zadavateli
- podpora administrace databáze systému CERTIS

Podpora bude poskytována pro prostředí (SW, HW, aplikace) a systémy dle této specifikace, rozprostřené ve dvou lokalitách.

Ad Zajištění podpory pro vývoj a implementaci IS CERTIS

- provoz hotline v režimu 7 x 24
- provoz zajištěn nepřetržitou přítomností kvalifikovaných pracovníků v pracovní dny od 7:30 do 20:00 hod
- provoz zajištěn každý den administrátoři na místě, administrátoři pokrývají kvalifikačně všechny použité platformy
- poskytovaná podpora je schopna vyřídit do 3.000 požadavků ročně
- hot-line systém schopen komunikace do obdobných nadřazených systémů včetně vykazování provedených služeb a zásahů

Ad Zajištění zálohování serverů IS CERTIS

Pro management záloh požaduje zadavatel vytvořit zálohovací prostředí (včetně SW) a realizaci zálohovací strategie (online záloha, image backup, záloha OS, snapshot).

Zálohování bude zajištěno na diskové pole umístěné v lokalitě zadavatele. Disková pole budou umístěna ve dvou různých lokalitách (hostingové centrum a lokalita zadavatele).

Zálohované objekty:

- Záloha OS a souborových systémů Windows
- On-line záloha IS (CERTIS) a databáze (MS SQL)
- Křížová záloha (duplikace záložních dat do vzdálené knihovny)
- Zálohování za využití instantních kopírovacích služeb diskových polí.
- Zálohování souborové nebo metodou image backup

Základní principy zálohovací politiky:

- záloha všech serverů-denně
- udržování několika verzí záloh – možnost návratu ke starší verzi dat
- on-line backup OS, IS CERTIS
- prostorová duplikace záloh (bezpečnostní kopie do jiné lokality)
- vytváření off-site kopií dat pro uchování v jiné lokalitě pro případ havárie
- vytváření dlouhodobých archivů
- použití LAN FREE Backup pro SAN architekturu

ad Správa systémů a monitoring

Pro optimální využití a efektivní bezvýpadkový a bezpečný provoz HW a SW infrastruktury požaduje zadavatel zajištění provozu software pro systémovou správu a monitoring.

Centrální systém pro dohled a automatizaci by měl zajistit sledování aplikačních a systémových logů dohled nad operačními systémy, HW, Storage, sítí, nad databázemi a IS CERTIS.

Všechny ostatní nástroje pro správu musí být do tohoto systému integrovány. Výsledkem centrálního dohledu by měla být vyhodnocená informace očištěná od opakování, nevýznamných zpráv, neškodných kombinací incidentů, apod. Požaduje se rovněž funkcionalita pro analýzu příčiny události a korelace událostí. Možnost definování korelací by měla být otevřená pro ruční definování libovolných vazeb mezi událostmi. Předpokládá se také využití integrované knowledge base.

Zásadní je možnost centrální správy a konfigurace storageových subsystému. Tedy centralizovaný nástroj pro správu SAN, disků, páskových knihoven. Základními požadavky jsou jednotná centrální správa a monitoring topologie sítě SAN, definice zón, lun management, analýza využívání a kategorizace dat, end-to-end sledování výkonu SAN, diskových polí, apod.

3. Součinnost

Zadavatel zajistí před realizací požadovaných služeb definovaných v podrobné technické specifikaci následující služby. Veškeré služby budou dodány, nebo zajištěny nejpozději 14 dní před samotnou dodávkou služeb.

3.1 Služby hostingového centra

Konektivita a síťové služby

Zadavatel zajistí konektivitu do internetu v dostatečné kvalitě a kapacitě. Síťová infrastruktura bude plně redundantní. Jednotlivé prvky IS CERTIS budou od sebe odděleny na úrovni samostatných síťových segmentů (bude realizováno jako VLAN s definovaným řízením přístupu).

DNS služby

Zadavatel zajistí DNS server pro publikaci potřebných údajů do internetu.

Firewall a VPN koncentrátor

Zadavatel zajistí v hostingovém centru dva firewally v redundantní konfiguraci, které poskytují řízení bezpečného vstupu z internetu do následujících tří sítí

- VLAN 1 – síť s aplikačními servery IS CERTIS, provozovanými v režimu Load Balancingu a distribučními servery CRL.

- VLAN2 – Administrativní síť aplikace CERTIS. Přístupná pouze administrátorům a skenovacím pracovištím pouze přes VPN server. VPN server zajistí autentizaci prostřednictvím certifikátu.
- VLAN 4 – Testovací síť přístupná testerům aplikace IS CERTIS.

SSL akcelerace

Zadavatel zajistí v hostingovém centru SSL terminaci datového provozu s dostatečnými parametry. SSL akcelérátor musí být schopen realizovat 3000 operací/sec s šifrou 1024bit RSA Trusted Path Authentication.

HW Load Balancing

Zadavatel zajistí v hostingovém centru HW Load balancing s dostatečnými parametry. Load balancing bude použit pro rozvažování zátěže na jednotlivé aplikační servery.

Segmenty sítě

VLAN 1

Redundantní síť, do které jsou připojeny v začátku dva aplikační servery IS CERTIS, které jsou z internetu přístupné pouze přes HTTPS. VLAN1 je řešena pomocí redundantních switchů, které umožní rozšiřitelnost aplikačních serverů minimálně na dvojnásobek.

VLAN2

Redundantní vnitřní síť aplikace IS CERTIS.

VLAN3/FC

Redundantní síť FC nebo Ethernet, podle typů diskových polí. VLAN musí garantovat minimálně 4GB přenos mezi jednotlivými uzly clusteru s diskovým polem.

VLAN – HeartBeat

Síť sloužící ke vzájemné komunikaci mezi uzly clusteru.

VLAN 4

Testovací síť přístupná testerům aplikace IS CERTIS.

3.2 SW licence

Řešení je založeno na produktech společnosti Microsoft. Jako operační systém je navržen Microsoft Windows Server 2008 s tím, že podle účelu se jedná o edici Standard nebo Enterprise. Jako databázový stroj je využit Microsoft SQL server 2008 v edici Enterprise. Níže uvedené SW licence zajistí zadavatel.

Určeno pro:	Popis	Počet licencí	Poznámka
2 x AD 1 x Dohled a Backup	MS Windows Server 2008 Standard	3	
2 x Aplikační HV, 2 x DB (Node1, Node2), 1 x Testovací HV	MS Windows Server 2008 Enterprise	5	
2 x 4 procesory DB HV, 1 x Testovací HV	MS SQL 2008 Enterprise	9	Licence dle počtu procesorů, u testovacího serveru konfigurace pro 1 procesor
1 x Testovací HV, 2 x Aplikační HV, 2 x AD, 2 x DB HV	MS Extended Connection	7	

4. Místo plnění

Místem plnění služby bude hostingové centrum, které bude umístěno na jakémkoliv místě na území České republiky, vybavené požadovanou infrastrukturou. Uchazeč je povinen při stanovení nabídkové ceny vzít v úvahu všechny náklady spojené s touto skutečností. Konkrétní lokalitu určí zadavatel nejpozději před podpisem smlouvy s vybraným uchazečem. Jedná se o službu flore space, bude k dispozici elektrické napájení, konektivita do internetu.

Druhou lokalitou bude pracoviště zadavatele.

V každé lokalitě bude k dispozici infrastruktura zahrnující nepřetržité (zálohované) napájení s ochranou proti přepětí a dalším rušivým vlivům, chlazení a kontrola prostředí (vlhkost, prašnost, ochrana proti požáru) a zabezpečení (kontrola) fyzického přístupu k zařízením.

5. Období a termíny plnění

Realizace služeb datového centra je zadavatelem objednávana pro:

- a) maturitní generálku MAG09-2,3;
předpokládaný termín realizace: říjen 2009;
- b) společnou část maturitní zkoušky v r. 2010 (SČ MZ 2010);
- c) společnou část maturitní zkoušky v r. 2011 (SČ MZ 2011).

Pro přípravu, testování implementaci a ověření všech funkčních a výkonnostních parametrů je nutné, aby předmět této veřejné zakázky byl realizován nejpozději do 1.10.2009 tak, aby bylo možné testovat potřebné parametry v rámci maturitní generálky MAG09-2,3.

6. Bezpečnost

Důležitým parametrem zajišťovaných služeb je vysoká citlivost obsahu zadání maturitní zkoušky. Vyzrazení zkušebního tajemství (informace veřejně nepřístupné podle příslušných ustanovení zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), v platném znění (dále jen „**Školský zákon**“) by způsobilo znehodnocení vynaložených prostředků v řádu desítek až stovek miliónů korun.

Tato rizika je nutné eliminovat technicko-organizačními opatřeními.

V rámci těchto opatření musí být ze strany vybraného uchazeče kladen důraz na personální, technické, administrativní zabezpečení. V případě jakéhokoliv incidentu musí být možné dohledat nezbytně nutné množství záznamů k identifikaci důvodů vzniku incidentu. Incident bude neodkladně hlášen zadavateli stanoveným způsobem a řešen podle připravených havarijních plánů s přesně stanovenou odpovědností.

Ochrana osobních údajů

Informace uložené a zpracovávané v IS CERTIS zahrnují i osobní údaje, a proto je nutné s nimi nakládat podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění.

Zkušební tajemství

Informace uložené a zpracovávané v IS CERTIS jsou klasifikovány podle § 80 odst. 3 písm. c) a § 80b školského zákona jako informace veřejně nepřístupné.

Zmařením maturitní zkoušky je taková situace, kdy maturitní zkouška nemůže proběhnout v řádném termínu, ani za použití záložních variant, a to s ohledem na skutečnost, že takové zmaření způsobil vybraný uchazeč.

Přístup k aplikaci IS CERTIS

Uživatel

Uživatel aplikace IS CERTIS, autentizující se do aplikace jménem a heslem k IIS serverům. Komunikace s uživatelem je šifrována (SSL).

VPN uživatel

Administrátor nebo pracovník digitalizačního pracoviště, přistupující do vnitřní sítě přes VPN Server. K autentizaci je použit certifikát uložený na iKey Token. K VPN tunel bude použit L2TP (IPSec) protokol