**TECHNICKÉ ZADÁNÍ**

# Systémové prostředí ČNB

Systém SDAT musí akceptovat standardní systémové prostředí ČNB a musí být snadno do tohoto prostředí implementovatelný. Následující kapitoly jsou popisem tohoto systémového prostředí.

## Serverová část

Serverové prostředí (databázový či aplikační server) je tvořeno:

* HW platformou x86/x64 serverů s OS MS Windows Server 2008R2, cp 1250 nebo Red Hat Linux v. 6.5 jako alternativní prostředí,
* nebo virtualizovanými verzemi serverů na platformách VMWare vSphere 5.x nebo Oracle VM 3.x.

Operační systémy jsou:

* monitorovány a sběr logů je zabezpečen systémem MS SCOM 2007 SP1,
* pravidelně skenovány na zranitelnosti systémem QUALYS.

## Databázová a aplikační platforma

Databázová platforma ČNB je postavena na databázi ORACLE, pro jejíž správu má ČNB vyškolené specialisty. Je možné využít Oracle nadstavbu Oracle Business Intelligence 11g Enterprise Edition pro tvorbu sestav.

Databázový server:

* Oracle RDBMS 11g a vyšší (standard/enterprise edition),
* protokol Oracle Net.

Aplikační a WWW server:

* Oracle WebLogic Server 11g,
* JBoss,
* Microsoft IIS 6.0 a vyšší.

## Klientská část

Klientská část je založena na OS:

* MS Windows 7 Professional (64bit), cp 1250, Service Pack 1 (operační systém) + aktuální aktualizace a
* na publikovaném vDesktopu prostřednictvím Citrix XenApp 6.5 na MS Windows 2008 Server R2 (virtuální desktop využívající MS terminálové služby).

SDAT musí fungovat v obou typech klientského prostředí.

Další SW na klientské části je:

* TCP/IP síťové služby (DHCP klient, SNMP klient),
* MS Office 2010 Professional Plus CZ + Service Pack 2
* MS Internet Explorer 10 CZ (aktuální SP),
* Adobe Acrobat Reader 10 CZ – prohlížeč souborů ve formátu PDF,
* Java JRE 7.x
* Symantec EndPoint Protection v.12.1 - antivirový program.

Instalace další provozní platformy na klientskou stanici není preferována. Instalace programového vybavení na klientskou stanici je prováděna především prostřednictvím vzdálené automatické instalace. Instalace musí být kompatibilní se službou  MS Installer (standardní služba operačního systému). Instalace programového vybavení na vDesktop je prováděna centrálně pomocí tzv. image z provisioning serverů.

Není přípustné ukládat na klientskou stanici/vDesktop data trvalé hodnoty, taková data je nutno ukládat na centrální diskové kapacity. Na klientské stanici nesmí být prováděno dávkové zpracování dat IS.

Dávkové zpracování centrálně uložených dat je přípustné spouštět a provádět pouze na databázovém serveru nebo případně na aplikačním serveru.

Uživatel nebo aplikace mohou ukládat na klientskou stanici dočasná data a programové komponenty, které jsou odvozeny z centrálně uložených dat, mohou také provádět lokální zpracování dat. Pro případné vytváření dočasných souborů a ukládání dat při činnosti komponent je třeba využívat předdefinované adresáře dostupné přes proměnné prostředí (USERPROFILE, TEMP, TMP, APPDATA). V případě vDesktop jsou data na lokálním disku po restartu serveru smazána.

Přístupová práva na klientských stanicích a vDesktop odpovídají defaultnímu nastavení od firmy Microsoft po instalaci MS Windows 7 Professional (v případě vDesktop se jedná o MS Windows 2008R2). Výjimky pro potřeby aplikací je v nezbytných případech možné povolit po přesném definování potřebných změn v adresářích a v registrech a po náležitém zdůvodnění požadovaných změn. Výjimky jsou centrálně řízeny a aplikovány na klientské stanice a vDesktop prostřednictvím GPO (politiky v Active Directory). Obdobné požadavky platí i pro registrování knihoven a vytváření nebo změny hodnot klíčů v registrech.

Na klientské stanici a vDesktop pracuje uživatel standardně pod právy přidělené skupině „Users“.

Tisk z klientské stanice je umožněn výhradně po síti přes centrální spool servery.

## Datová síť

Datová síť ČNB má následující parametry:

* Klientské stanice jsou připojeny rychlostí typicky 100/1000 Mbsec-1 100/1000 Base-T.
* Servery jsou připojeny typicky rychlostí 1/10 Gb 1000/10.000 Base-T.
* Mezi servery a klientskými stanicemi je pouze L3 konektivita, mezi servery možná L2 nebo L3 konektivita.
* Adresace dle RFC 1918 (10.x.y.z 172.16-31.y.z, 192.168.y.z).
* Datová síť je plně přepínaná s redundantním jádrem.

## Systémové služby

**Single Sign-On**

U informačních systémů ČNB je realizována pro interní uživatele informačních systémů funkce Single Sign-On s využitím služby Microsoft Active Directory (autentizační protokol Kerberos). Uživatel se autentizuje pouze jednou do domény „CNB“ (typicky s využitím certifikátu na čipové kartě), při vyvolání libovolné aplikace již pak není zadávání jména/hesla nutné, ani žádná další autentizace uživatele není požadována.

**Zálohování IS a dat**

Zálohování SDAT a jeho dat je v ČNB řešeno centrálně, pokud je databáze SDAT typu Oracle. Zálohována jsou pouze data uložená na centrálních kapacitách ve správě sekce informatiky. Pro zálohování je určen zálohovací systém HP Data Protector 6.0 nebo vyšší.

**Zajištění vysoké dostupnosti HA**

Pro zajištění vysoké dostupnosti může SDAT využít jednou z následujících technik:

1. virtualizace VMware nebo OVM,
2. MS Cluster Server. Systém bude funkční ve dvou lokalitách (CVS Senovážná, ZVS Zličín) s tím, že aktivní systém bude mít připojené disky z diskového pole v režimu ReadWrite, zatímco záložní systém bude mít zrcadlené disky připojené v režimu ReadOnly.

**SIEM (Sběr bezpečnostních logů)**

Sběr a vyhodnocování bezpečnostních logů je v ČNB řešen centrálně systémem SIEM ArcSight od firmy HP.

Systém SDAT musí podporovat některý z následujících způsobů logování a sběru logů:

* zaznamenávat logy ve strojově čitelné podobě do souboru v operačním systému a tento sdílet pro systém SIEM,
* zaznamenávat logy ve strojově čitelné podobě do DB a umožnit přístup systému SIEM k daným tabulkám,
* odesílat logy ve strojově čitelné podobě na vzdálený server např. syslogem.

Pro správnou interpretaci a syntaktickou analýzu (parsing) je nutný popis struktury logu.

**Elektronická pošta**

* Server elektronické pošty - MS Exchange 2010.
* Klient elektronické pošty - MS Outlook 2010.

Tisková zařízení

* Síťová tisková zařízení.
* Komunikační protokol – TCP/IP.
* Podporované síťové služby – SNMP, DHCP, DNS, NTP

Centrální diskové kapacity

K dispozici jsou „fault“ tolerantní disková pole pro ukládání dat spravovaných databázovými systémy, pro sdílení programového vybavení a dat organizačních útvarů ČNB. Zálohování dat centrálních diskových kapacit je zajištěno objednatelem.

**Internet (DMZ)**

* E-mail je povolen všem uživatelům prostřednictvím poštovny Exchange a MTA serverů. Maximální velikost zprávy je však omezena na 30 MB a může být zablokována antivirovým systémem.
* Neaktivní spojení jsou po jedné hodině přerušena.
* Služby provozované v rámci aplikací nebo IS jsou registrovány a povolovány zvlášť v souladu se systémovou bezpečnostní politikou DMZ na základě schválené žádosti.
* Přístup z Internetu je omezen pouze na dedikované servery v určené části DMZ.

**Synchronizace času**

Čas na všech komponentách sítě ČNB mimo stanic uživatelů je synchronizován se zdrojem přesného času (pro zajištění správného vyhodnocení auditních záznamů). Přesný čas je distribuován protokolem NTP.

## Řízení přístupu k IT

Ke všem funkcím, programovému vybavení či službám systémového prostředí a obvykle i DB rolím je řízen přístup prostřednictvím interně vyvinuté aplikace „ŘDB – Řídicí databáze“ (aplikace nad DB Oracle), která uchovává seznam uživatelů a jejich skupin a tyto informace jsou pak propagovány např. do Microsoft Active Directory nebo zpřístupněny přes LDAP z Active Directory či z tabulek aplikace ŘDB prostřednictvím views do jiných systémů a aplikací dle jejich potřeb. Ke každému aktivu (aplikace, zdroj, funkce, privilegium atd.) je vytvořena tzv. aplikační skupina, do které jsou pak zařazovány uživatelské účty či účty klientských stanic a tím jsou jim dané komponenty, služby či funkce systémového prostředí ČNB zpřístupněny.

# Bezpečnost IT

V souladu s bezpečnostní politikou České národní banky v oblasti informačních technologií je informační systém SDAT zabezpečen proti hrozbám ohrožujícím jeho dostupnost, důvěrnost, integritu a auditovatelnost.

Zajištění bezpečnosti v ČNB::

|  |  |
| --- | --- |
| **Dostupnost**  | Max. doba výpadku 24 hodin. Dostupnost je zajišťována také prostřednictvím 2 geograficky vzdálených středisek v lokalitě Praha v režimu „split-site“.  |
| **Důvěrnost**  | Řízený přístup (práva přístupu dle rolí).  |
| **Integrita**  | Databázová transakce.  |
| **Autentizace interní uživatelé** | Primárně užitím čipové karty, pouze ve výjimečných a řádně zdůvodněných případech jménem a heslem OS Windows (SSO ve spolupráci s Active Directory a OID).  |
| **Autentizace externí uživatelé** | Primárně komerčním osobním nebo serverovým certifikátem popřípadě jménem heslem nebo jednorázovou pass-klauzulí  |
| **Prokazatelnost**  | Záznam v auditním logu.  |
| **Nepopiratelnost** | Elektronický podpis kvalifikovaným osobním nebo systémovým certifikátem  |

Servery a na nich instalované SW produkty jsou pravidelně monitorovány a skenovány produktem QUALYS (http://www.qualys.com/). Pokud jsou nalezeny zranitelnosti u instalovaných produktů hodnoty 4 a vyšší (hodnoty výstupu ze systému Qualys), jsou neprodleně odstraněny a to formou aplikací patchů či jiným doporučeným postupem.

Součástí akceptace systému je provedení penetračního testu a skenu známých zranitelností. Testována jsou rozhraní dostupná z internetu, interním uživatelům i případná další (propojení s jinými systémy).

Všechna datová média (především pevné disky) použitá v informačním systému jsou před přemístěním mimo prostory ČNB bezpečně smazána nebo zničena.

**K funkcím pro správu, změny, diagnostiku apod. systému je přístup pouze ze sítě ČNB (příp. prostřednictvím běžného vzdáleného přístupu zaměstnance ČNB do této sítě.) Poskytovatelé nemají ze svých sítí jiný přístup k systému než veřejnost**.

# Vývojové prostředí informačních systémů

Pro vývoj informačních systémů jsou v ČNB používány následující frameworky

**Uživatelské rozhraní:**

* Oracle Applicacion Express (APEX)
* Oracle Applicacion Development Framework (ADF) nástroj JDeveloper

**Reporting:**

* Oracle Business Intelligence (OBIEE)
* Oracle BI Publisher

**Databázové logika**

* Uložena v Oracle PL/SQL, SQL\*Plus

# Architektura současného systému MTS-ISL-SÚD-SDNS

Základem je schéma statické architektury, které prezentuje členění systému do technologických vrstev, jednotlivé technologické komponenty systému a vazby mezi nimi.

Schéma rozhraní prezentuje současná rozhraní, která systém MTS-ISL-SÚD-SDNS (dále také jako „MTS“) používá ke komunikaci s okolím. Každé rozhraní systému je složeno ze dvou vrstev, přičemž první vrstva definuje **služby**, které systém poskytuje okolí, resp. které systém vyžaduje od okolí, zatímco druhá vrstva definuje **technologie**, které jsou pro jednotlivá rozhraní použita.

**Statická architektura současného systému MTS**



Obrázek - Statická architektura systému MTS

**Architektura rozhraní současného systému MTS**



Obrázek - Architektura rozhraní současného systému MTS

# Vazby na interní/externí IS

Systém MTS je do standardního systémového prostředí integrován prostřednictvím svého Standardního datového rozhraní, které bez výjimky používají všechny návazné aplikace, kterých je cca 15 s různou mírou komplexnosti a velikosti. Standardní datové rozhraní je tvořeno sadou databázových objektů použitelných v prostředí SQL a PL/SQL pro výběry metadat a dat ze systému MTS. Komunikace návazných informačních systému se systémem MTS a tvorba sdílených číselníků je zajištěna skrze datové API dodané společností NESS a.s.

**Z formálního hlediska je rozhraní systému MTS charakterizováno následujícími dvěma rysy:**

* Strukturou rozhraní (tj. datovým modelem) - struktura rozhraní je tvořena množinou databázových objektů, jejich vazbami a jejich fyzickou strukturou, tj. množinou atributů (sloupců) obsažených v těchto databázových objektech.
* Datovým obsahem rozhraní - datový obsah rozhraní je vlastní náplň databázových objektů rozhraní.

**Z obsahového hlediska dělíme objekty rozhraní MTS na dvě skupiny:**

* Metadata - metadata jsou všechna data a objekty určené k popisu sledovaných údajů a navigaci k údajům (metadata – data o datech).
* Vlastní data - vlastní data jsou hodnoty sledovaných veličin - údajů.

**Způsob popisu dat v rozhraní**

Rozhraní MTS obsahuje jak sémantický popis veličin (pomocí metaobjektů definovaných v MTS), tak popis tzv. výkazový, tj. souřadnicemi {řádek,sloupec} umístění dané veličiny ve struktuře datové oblasti /výkazu. Oba tyto způsoby popisu dané veličiny podléhají možným změnám při změně metodiky vykazování, výkazový popis je však méně stabilní než sémantický (nutnost změnit strukturu výkazu se jeví častější než nutnost změnit sémantický popis veličiny).

**Technologický charakter datových objektů rozhraní**

Datové objekty rozhraní jsou realizovány v databázovém prostředí RDBMS Oracle. Některé objekty jsou realizovány jako databázová views nad objekty MTS, výjimečně méně často jako samostatné fyzické databázové objekty (databázové tabulky nebo materializovaná views). Výjimečně je objektem rozhraní databázová funkce. Aktuálnost dat v objektech rozhraní je zabezpečena funkcemi rozhraní, uživatelé se tedy nemusejí o aktualizaci starat.

**Způsob práce návazných informačních systémů s daty v rozhraní**

Z hlediska další práce s daty a metadaty prostřednictvím rozhraní MTS existují tři možné koncepce:

1. Aplikace pracují přímo nad datovými objekty rozhraní.
2. Aplikace využívají mezisklad dat, který je plněn z rozhraní specifickými procedurami, aplikace pracují až nad daty v meziskladu.
3. Aplikace využívají obě kombinace.