**TECHNICKÉ ZADÁNÍ**

1. [Systémové prostředí ČNB](#_SYSTÉMOVÉ_PROSTŘEDÍ_ČNB)
2. [Bezpečnost IT](#_BEZPEČNOST_IT)
3. [Vazby na interní/externí IS](#_Vazby_na_interní/externí_1)
4. [Migrace dat](#_Migrace_dat)
5. [Specifické požadavky](#_Katalog_Ttechnickéých_požadavkyů)

**DMS musí být realizován jako webová aplikace přístupná minimálně z prostředí Microsoft Internet Explorer 11.**

# Systémové prostředí ČNB

SW řešení DMS musí akceptovat standardní systémové prostředí ČNB a musí být snadno do tohoto prostředí implementovatelné.

### Prostředí datové sítě

* Klientské stanice připojeny rychlostí 1000 Mbps
* Servery připojeny typicky rychlostí 1 až 10 Gb
* Adresace dle RFC 1918 (10.x.y.z, 172.16-31.x.y, 192.168.x.y)

### Serverová část

Serverové prostředí (databázový či aplikační server):

* Platforma architektury x86 - MS Windows Server 2008R2 Server, cp 1250
* Platforma Red Hat Linux ver. 6 nebo 7
* Platforma VMware vSphere ver 5 a vyšší
* Platforma Oracle VM 3.4 a vyšší

### Databázové servery

Data standardních IS jsou uložena v databázích Oracle:

* Oracle RDBMS 12c EE provozovaný na dvou Oracle Exadata Quatter Rack X6-2, v primární a záložní budově, každý vybavený licencemi pro 40 jader (Intel Core), 1,5 TB RAM, 85 TB HDD, technologií RAC, Partitioning, Diagnostic a Tunning Pack.
* Protokol Oracle SQL Net

Databázová platforma ČNB je postavena na databázi ORACLE, pro jejíž správu má ČNB vyškolené specialisty a je možné využít Oracle nadstavbu Oracle Business Intelligence 12c Enterprise Edition pro tvorbu sestav.

## V případě, že řešení bude využívat jinou databázi, poskytne objednatel pro DB prostředí následující konfiguraci virtuálních serverů na platformě VMware:

1. Primární DB server
   1. 2 až 4 VCPU (virtuálních CPU)
   2. 8 až 16 GB RAM
   3. vzdálené úložiště prostřednictvím sítě SAN – 500 GB
   4. konektivita min. 1 Gbps
   5. operační systém RedHat nebo Windows Server (viz. odst. 1.2)
2. Záložní DB server
   1. stejná konfigurace
   2. data se synchronizují na úrovni diskového pole

**Poskytovatel je povinen zahrnout do nabídky veškeré náklady na pořízení a provoz SW licencí.**

### Aplikační a WWW servery

* Oracle Web Logic Server 12c,
* Microsoft IIS v roli MS Server 2008R2

Objednatel poskytne následující konfiguraci pro provoz virtuálních aplikačních a WWW serverů na platformě Oracle VM (v případě Oracle Web Logic) nebo VMware:

1. Primární aplikační server
   * 2 VCPU (virtuálních CPU)
   * 8 GB RAM
   * vzdálené úložiště prostřednictvím sítě SAN – 250 GB
   * konektivita min. 1 Gbps
   * operační systém RedHat nebo Windows Server (viz. odst. 1.2)
2. Záložní aplikační server
   * stejná konfigurace
   * data se synchronizují na úrovni diskového pole
3. Primární WWW server
   * 2 VCPU (virtuálních CPU)
   * 8 GB RAM
   * vzdálené úložiště prostřednictvím sítě SAN – 100 GB
   * konektivita min. 1 Gbps
   * operační systém RedHat nebo Windows Server (viz. odst. 1.2)
4. Záložní WWW server
   * stejná konfigurace
   * data se synchronizují na úrovni diskového pole

**Účastník je povinen zahrnout do nabídky veškeré náklady na pořízení a provoz SW licencí.**

### Monitoring systémů

* System Center Operations Manager 2012 R2 – centrální sběr logů
* QUALYS Guard – monitoring zranitelností
* SIEM HP ArcSight– sběr bezpečnostních logů
* Oracle Enterprise Manager (sledování provozu databázového prostředí a aplikačních serverů)
* Oracle Diagnostic Pack, Tunning Pack, Partitioning

**Z důvodu koncepční konsolidace datové základny v prostředí DB Oracle preferujeme řešení realizované nad touto platformou. Potřebné licence Oracle RDBMS 12c EE zajistí objednatel. Pro tuto platformu jsou zajištěny návazné procesy zálohování dat a replikace do záložního střediska, monitoring zranitelností a pravidelné aktualizace SW.**

**Pokud je SW řešení DMS dodáno s využitím výše uvedených platforem, může dle možností zajistit licence ČNB. Je-li dodáno SW řešení s využitím jiných platforem, je poskytovatel zavázán dodat i potřebné licence.** **V každém případě cena SW řešení obsahuje všechny potřebné licence k provozu SW řešení.**

**Podle technologické platformy SW řešení DMS bude implementace do systémového prostředí objednatele a následný provoz probíhat za podmínek uvedených ve variantě … v příloze č.12 smlouvy.**

*(bude doplněno při uzavření smlouvy s vybraným účastníkem)*

### Klientské stanice

Osobní počítače typu IBM-PC kompatibilní (x86) nebo virtuální desktop

OS:

* MS Windows 7 Professional 64bitCZ, cp 1250, Service Pack 1 (8GB RAM). Nutno počítat i s budoucím upgradem na MS Windows 10.
* Notebooky s MS Windows 10 Pro 64bit CZ
* Citrix XenApp 6.5 na MS Windows 2008 Server R2 (virtuální desktop využívající MS terminálové služby).

Další SW na klientské části je:

* TCP/IP síťové služby (DHCP klient, SNMP klient),
* MS Office 2010 Professional Plus CZ + SP 2, nutno počítat i budoucím upgradem na MS Office 2016.
* MS Internet Explorer 11 CZ (aktuální SP),
* Adobe Acrobat Reader 10 CZ nebo vyšší.
* Symantec EndPoint Protection v aktuální verzi.

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“.

**Při realizaci SW řešení DMS je nutné zajistit, aby programové komponenty realizovaného IS nebyly v rozporu s komponentami dalších provozovaných IS. Realizovaný IS tedy musí být provozovatelný v systémovém prostředí ČNB a současně nesmí narušovat funkčnost ostatních IS.**

### Systémové služby



1. Single Sign-On

U informačních systémů ČNB je realizována funkce Single Sign-On s využitím služby Microsoft Active Directory (autentizační protokol Kerberos) a OID Oracle Internet Directory. 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.

Další podmínky jsou uvedeny v kapitole 2 [Bezpečnost IT](#_BEZPEČNOST_IT).

1. Zálohování IS a dat

Zálohování SW řešení DMS a jeho dat je v ČNB řešeno centrálně, pokud bude databáze DMS typu Oracle. Zálohována jsou pouze data uložená na centrálních kapacitách ve správě sekce informatiky. Zálohování databázového prostředí probíhá pomocí nástroje Oracle RMAN. Pro zálohování je určen zálohovací systém HP Data Protector 9.07.

SW řešení DMS bude instalováno a provozováno v prostředí Microsoft Cluster Server (Windows 2008). Mimo jiné musí být schopno automatického zotavení po havárii serveru a zároveň po zotavení musí mít zajištěnu konzistenci dat. Instalaci do prostředí Microsoft Cluster Server zajišťuje poskytovatel.

Integraci do prostředí geografického clusteru (tj. start DMS na druhém node clusteru v jiné lokalitě) zajišťuje objednatel.

**Pokud využívá SW řešení DMS jiný typ databáze, pak poskytovatel musí dodat současně  s dodávkou systému DMS skripty (sadu příkazů), které uvedou DMS (jeho data) do konzistentního stavu vhodného k zálohování a ČNB zajistí zálohu určených souborů.**

**Poskytovatel dodá skript, který na konci zálohy opět vrátí IS do provozního stavu a stejně tak umožní jeho obnovu z těchto záloh v případě havárie.**

1. SIEM (Sběr bezpečnostních logů)

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

SW řešení DMS musí podporovat některý z následujících způsobů logování a sběru logů:

* zaznamenávat logy ve strojově čitelné a zpracovatelné podobě, tzn. logy musí mít jednotnou strukturu, do souboru v operačním systému a tento v realtime sdílet pro systém SIEM. Soubor může rotovat, ale musí být zachováno jeho jméno
* zaznamenávat logy ve strojově čitelné podobě do DB a umožnit realtime přístup systému SIEM k daným tabulkám,
* odesílat logy ve strojově čitelné podobě na vzdálený server např. syslogem.

1. 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

1. Tisková zařízení

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

1. 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.

1. 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.

1. Synchronizace času

Čas na všech komponentách sítě ČNB mimo stanic uživatelů je synchronizován se zdrojem přesného času (pro zajištění správného vyhodnocení auditních záznamů) 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. 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 DMS zabezpečen proti hrozbám ohrožujícím jeho dostupnost, důvěrnost, integritu a auditovatelnost.

### 2.1 Zajištění bezpečnosti v ČNB:

|  |  |
| --- | --- |
| **Dostupnost** | Dostupnost je zajišťována také prostřednictvím 2 geograficky vzdálených středisek v lokalitě Praha v režimu „split-site“. |
| **Důvěrnost** | Řízený přístup (práva přístupu dle rolí). |
| **Integrita** | Použití https protokolu a databázové transakce |
| **Autentizace** | Primárně užitím čipové karty, pouze ve výjimečných a řádně zdůvodněných případech jménem a heslem OS Windows (SSO ve spolupráci s Active Directory). |
| **Prokazatelnost** | Záznam v auditním logu. |

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.)**

**Poskytovatel nemá ze svých sítí jiný přístup k systému.**

### 2.2 Zabezpečení dokumentů v systému

Vzhledem k nutnosti býti v souladu s požadavky ESCB, které jsou stanoveny v dokumentu „Jednotná pravidla a minimální standardy pro nakládání s citlivými informacemi ESCB a SSM“, musí být data v DMS zabezpečena dle požadavků uvedených níže:

1. **Statická data**

(míněno data ukládaná na servery, pracovní stanice, vyjímatelná media a mobilní zařízení)

|  |  | **Použití šifrovací metody** | | |
| --- | --- | --- | --- | --- |
| **Klasifikace ESCB** | **Klasifikace ČNB**  **(dle Pokynů ČNB č. 38/2015)** | **Servery** | **Pracovní stanice** | **Vyjímatelné disky a mobilní zařízení** |
| **ECB-SECRET** | ***Přísně chráněno*** | ***M*** | ***M*** | ***M*** |
| **ECB-CONFIDENTIAL** | ***Chráněno*** | ***R*** | ***M*** | ***M*** |
| **ECB-RESTRICTED** | ***Omezený přístup*** | *NA* | *NA* | ***M*** |

1. **Dynamická data:**

(míněno data putující mezi klientskými stanicemi, servery a ostatními zařízeními, stejně jako elektronické transakce přes telekomunikační sítě operátorů)

|  |  | **Použití šifrovací metody** | | | |
| --- | --- | --- | --- | --- | --- |
| **Klasifikace ESCB** | **Klasifikace ČNB**  **(dle Pokynů ČNB č. 38/2015)** | **Interní**  **e-mail** | **Externí**  **e-mail** | **Interní přenosy[[1]](#footnote-1)** | **Externí přenosy[[2]](#footnote-2)** |
| **ECB-SECRET** | ***Přísně chráněno*** | ***M*** | ***M*** | ***M*** | ***M*** |
| **ECB-CONFIDENTIAL** | ***Chráněno*** | ***R\**** | ***M*** | ***R\**** | ***M*** |
| **ECB-RESTRICTED** | ***Omezený přístup*** | *NA* | ***R*** | *NA* | ***R*** |

Vysvětlivky k hodnotám v tabulce:

M  - musí být šifrováno nebo použity kompenzační zabezpečovací prvky pro zmírnění příslušných rizik

R - šifrování je doporučeno

R\*- šifrování je velmi důrazně doporučeno

NA - není třeba šifrovat

### 2.3 Vzdálený přístup k dokumentům v systému

ČNB připojuje uživatele do sítě prostřednictvím vzdálené plochy realizované pomocí klientského SW Citrix Receiver.

# Vazby na interní IS

##### Seznam vazeb – základní přehled

| **Systém** | **Popis využití** |
| --- | --- |
| DMS - MS Office plug-in | Předpokládaný plug-in do aplikace MS Office zajišťující integraci mezi MS Office (včetně plug-in do MS Outlook) a DMS. |
| Microsoft AD RMS | Microsoft AD Rights Management System systém pro zabezpečení informací v elektronických dokumentech před neautorizovaným přístupem. Umožňuje zašifrovat jednotlivé dokumenty již u původce a zpřístupnit informace v dokumentu pak jen předem definovaným uživatelům. Systém DMS musí umožnit standardní správu dokumentů obsahujících klasifikované informace, které jsou chráněny šifrováním. |
| MS Exchange | Microsoft Exchange Server je SW produkt společnosti Microsoft, který bude využit pro zasílání e-mailových notifikací generovaných v systému DMS z úložiště dokumentů nebo z workflow na určené uživatele v rámci ČNB. |
| ŘDB | Informační systém pro správu řízení přístupu uživatelů a skupin uživatelů domény ms.cnb.cz k IS ČNB a pro správu nastavení zařízení zapojených do LAN sítě ČNB. Nový systém DMS bude denně aktualizovat z ŘDB/Active Directory uživatele a uživatelské a organizační skupiny. |
| IS e-Spis | Systém elektronické spisové služby, ve kterém jsou evidovány dokumenty v podatelně/výpravně ČNB a spisových uzlech jednotlivých sekcí. Systém splňuje všechny náležitosti spisové služby v souladu s Národním standardem (tvorba spisu, ukládání spisu, skartační řízení atd.) a zajišťuje také archivaci spisů v souladu se zákonem č. 499/2004 Sb. o archivnictví a spisové službě. |
| IS HRIS | Informační systém HRIS pro řízení lidských zdrojů, který bude pro systém DMS poskytovat údaje o nepřítomnosti zaměstnance (dovolená, volno, nemoc, služební cesta). |
| IBIS | Intranet ČNB (IBIS) |
| SIEM | Systém pro centrální sběr bezpečnostních logů (Security Information and Event Management), kde jsou ukládány detailní záznamy o přístupech uživatelů do systémů, popř. jejich dalších aktivitách v systému. |
| DMS web services | Webové služby systému DMS zajišťující možnost napojení a využití služeb DMS pro okolní systémy a systému DMS umožňující napojení se na služby externích systémů. |
| Klientská stanice, domácí klientská stanice, notebook, iPad | Uživatelská zařízení pro přístup do systému. |
| Firewall | Síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi externími sítěmi a interní sítí ČNB. Zabezpečuje komunikaci pro domácí klientské stanice, mobilní zařízení uživatelů (zaměstnanců ČNB) přes VPN. |
| IS Obelisk | Stávající úložiště dokumentů, ze kterého bude provedena migrace relevantních dokumentů do DMS |
| Software 602 Signer | Aplikace zajišťuje převody dokumentů do formátu PDF a PDF/A, možnost podepsání dokumentu elektronickým certifikátem, včetně vložení časového razítka. Je implementována jako plug-in do MS Office. |

##### Detailní popis některých vazeb

##### Integrace s MS Office – Word, Excel, Powerpoint, Outlook aj.

Plug-in do MS Office umožní využít základní operace vytvoření/úpravy dokumentu a připomínkování.

Uživatel vytvoří v MS Office nový dokument a pomocí funkcionality „Uložit“ vybere cílové úložiště v adresáři systému DMS, poté potvrdí uložení nového dokumentu. Systém DMS ověří přístupová oprávnění a přidělí automaticky hodnoty přednastavených metadat a v případě, kdy identifikuje potřebu vložení uživatelských metadat vyzve uživatele k jejich doplnění. Pokud uživatel nevyplní povinná metadata, systém neumožní uložení souboru. Stejný postup bude v případě otevření existujícího souboru (uloženého mimo úložiště DMS) v MS Office, pokud jej bude uživatel chtít uložit do DMS.

Při otevírání již vytvořeného dokumentu uloženého v DMS uživatel vybere soubor z cílového úložiště systému DMS a potvrdí jeho otevření. Systém DMS vyhodnotí přístupová oprávnění a provede otevření souboru v příslušné aplikaci.

Při odesílání odkazu na uložený dokument v DMS jiným uživatelům e-mailovou zprávou se oprávněnému koncovému uživateli otevře odkazovaný soubor/složka souborů v novém okně/záložce. Adresátem může být osoba, organizační struktura nebo aplikační skupina nebo jejich kombinace.

Rozšíření MS Office plně podporuje procesy uvedené v příloze č.1 Věcné zadání – kapitola 9 Popis vzorového procesu ČNB, která je nedílnou součástí smlouvy.

Integrace s MS Outlook zajišťuje příjem notifikací generovaných systémem DMS v rámci workflow, tj. při přidělení úkolu, při upomínce termínu zpracování úkolu, nebo příjem avíz/notifikací o vložení nového dokumentu do úložiště DMS a/nebo o jeho změnách.

Z prostředí MS Outlook je možné uložit přílohy z doručené zprávy do úložiště DMS. Systém vybídne uživatele k volbě umístění v systému a v případě potřeby doplnění metadat. Uživatel vyplní povinná i nepovinná metadata a potvrzením tyto přílohy uloží. Pokud uživatel nevyplní povinná metadata, systém neumožní uložení přílohy.

##### Integrace s Microsoft AD RMS

V současné době je používán pro šifrování dokumentů Microsoft AD RMS - Active Directory Rights Management.

Systém DMS umožní uložení těchto dokumentů do příslušné složky ve struktuře úložiště DMS, včetně možnosti spuštění workflow nad těmito dokumenty. Samotný systém DMS nedisponuje funkcionalitou šifrování dokumentů.

S ohledem na šifrování je počítáno s omezenou funkcionalitou systému v oblasti fulltextového vyhledávání.

##### Integrace s MS Exchange

Integrace s MS Exchange je na úrovni odesílání e-mailů zaměstnancům ČNB na základě avíz/notifikací generovaných ze systému DMS.

##### Integrace s ŘDB

Integrace s ŘDB zajišťuje aktualizaci uživatelů a skupin z domény ms.cnb.cz. Na základě existence uživatele v aplikačních a organizačních skupinách vedených v ŘDB je uživatel autorizován pro vstup do systému DMS.

V současném systému pro správu dokumentů IS Obelisk dochází k synchronizaci uživatelů a uživatelských skupin s databází personálních údajů zaměstnanců ČNB prostřednictvím ŘDB. Využívá přitom tabulek ŘDB „ZAMEST“ (obsahuje informace o zaměstnancích – jméno, titul, příjmení, status, příslušnost k org. útvaru apod.), „ORG2“ (údaje o základních organizačních jednotkách) a „ORG3“ (členění organizačních jednotek). Aktualizovaná data z ŘDB jsou poskytnuta 1x denně prostřednictvím synchronizační procedury. O provedení synchronizace je proveden zápis v databázi systému.

Tento princip se přebírá pro základní nastavení oprávnění v SW řešení DMS.

ŘDB poskytuje aktuální interní e-mailové adresy zaměstnanců ve vazbě na osobní číslo ve formátu [**jmeno.prijmeni@cnb.cz**](mailto:jmeno.prijmeni@cnb.cz)**.**

##### Integrace s e-Spis

Pro integraci DMS a e-Spis se využijí webové služby, jejichž popis nabízí dodavatel IS e-Spis společnost ICZ, a.s. stránkách <https://dms-support.i.cz> nebo jej poskytne na vyžádání objednatel. Základní komunikace mezi oběma systémy se řídí standardy popisovanými v dokumentu „Obecné rozhraní pro komunikaci mezi elektronickými systémy spisových služeb a agentovými informačními systémy (Best-practises)“, který vydalo Ministerstvo vnitra ČR (pokud jím poskytovatel nedisponuje, objednatel dokument poskytne na vyžádání).

###### Předání dokumentu z IS e-Spis do DMS

Do systému DMS IS e-Spis předá celý dokument včetně atributů (zejména atribut číslo jednací dokumentu v e-Spis a číslo jednací spisu v e-Spis), a ten je dále zpracováván v DMS (přiřazení UID, uložení do příslušné složky, spuštění workflow).

Předání dokumentu do DMS je asynchronní událostí. Akci vyvolává uživatel IS e-Spis, a to tak, že dokumentu přidělí požadovaný typ dokumentu (typ spárovaný v administraci s externí aplikací) a provede předání dokumentu externí aplikaci předem definovanou webovou službouu DMS. Systém e-Spis v tuto chvíli připravuje dávku událostí „DokumentPostoupení“. Dokument je postoupen příslušnému uživateli do DMS, neurčují se však žádná další specifická kritéria agendy, kam, např. do jaké „složky“ má být postoupeno, to již rozhodne přebírající uživatel DMS. DMS zašle uživateli emailovou notifikaci o vložení dokumentu z e-Spisu do příslušné složky v DMS. Přebírající DMS zpracuje události s postoupením dokumentů z e-Spisu a dále řídí jejich zpracování na základě vlastních workflow. Podrobnosti budou obsaženy v realizační studii.

###### Předání dokumentu z  DMS do IS e-Spis

Pokud na základě procesů v DMS vznikne potřeba založení nového dokumentu do IS e-Spis, pak tento systém vyvolá synchronní událost API WS (BP) rozhraní, a to DokumentZalozeni. Založení dokumentu z DMS vyžaduje splnění některých povinných podmínek, a to zejména naplnění minimálních povinných elementů pro založení dokumentu (např. Nazev = věc dokumentu, Identifikátor = UID dokumentu ve tvaru ZdrojId a HodnotaId, TypDokumentu a SpisovyZnak, pokud nejsou součástí tzv. defaultních hodnot nastavení integračního můstku). Dokument musí být zároveň založen pod existujícím autentizovaným uživatelem IS e-spis, na jehož funkčním místě má vzniknout.

Proces vzniku dokumentu v externím DMS je zpravidla složen z více událostí, zvláště pokud součástí vzniklého záznamu o dokumentu (metadatech) má být i elektronický obsah (soubor). Sled volaných událostí vypadá následovně:

• DokumentZalozeni – založení záznamu o dokumentu (záznam o ČJ)

• SouborZalozeni – založení el. přílohy (souboru), tedy obsahu dokumentu

• SouborVlozitKDokumentu – provázání uložené el. přílohy (souboru) s evidenčním záznamem o dokumentu v systému

Vložení dokumentu do IS e-Spis nastává zpravidla v okamžiku, kdy je již k dispozici finální verze dokumentu, který má být vložen a evidován v IS e-Spis, např. po ukončení workflow, ve kterém vznikne upravený dokument nebo dokument nový. Vložení dokumentu do IS e-Spis bude prováděno jednak automaticky na základě nastavení hodnoty příslušného atributu dokumentu, jednak manuálně na základě úkonu oprávněného uživatele. Do IS e-Spis se vkládá dokument:

1. s přidělením nového čísla jednacího a uložením do již existujícího spisu (např. původního, ze kterého byl dokument předán do DMS):
   1. Synchronní událost: DokumentZalozeni
   2. Asynchronní událost:
      1. SouborZalozeni,
      2. SouborVlozitKDokumentu,
      3. DokumentVlozeniDoSpisu – vložení dokumentu s obsahem do existujícího spisu, ERMS musí znát Identifikátor (ZdrojId a HodnotaId) spisu, do něhož má být dokument vložení
2. s přidělením nového čísla jednacího a založením spisu nad tímto dokumentem
   1. Synchronní událost: DokumentZalozeni
   2. Asynchronní událost:
      1. SouborZalozeni
      2. SouborVlozitKDokumentu
      3. SpisZalozeni – odkaz na existující dokument prostřednictvím

elementu DokumentIdVlozeny

##### Integrace s IS HRIS

Informační systém HRIS pro řízení lidských zdrojů poskytuje pro systém DMS údaje o nepřítomnosti zaměstnance v tomto rozsahu:

* plánovaná a předpokládaná dovolená
* regenerace pracovní síly
* nemoc
* služební cesta
* státní svátek

Údaje jsou poskytovány prostřednictvím datového view ODY\_PLANIS\_NEPRIT, které přenáší údaje v intervalu: dnešek minus 2 měsíce, dnešek plus 6 měsíců. Data se budou synchronizovat 1x denně (nejlépe v ranních hodinách mezi 05:00-06:00).

Na základě těchto údajů přesměruje systém DMS úkoly ve workflow na nastavené zástupce uživatele po dobu jeho nepřítomnosti. Pokud nebude mít uživatel svého zástupce po dobu nepřítomnosti nastaveného, bude jeho úkol uzavřen po uplynutí termínu k vyřízení úkolu. Při zadání úkolu může v závislosti na jeho povaze a obsahu uživatel nastavit, zda bude vyžadovat od zpracovatele či připomínkového místa aktivní reakci nebo postačí pasivní neporušení tiché procedury, tedy např.  v případě schvalovacího řízení to bude uzavření úkolu s výsledkem – dokument schválen, dokument neschválen či adresát se nevyjádřil.

##### Integrace s IBIS

Pro intranet ČNB slouží DMS jako úložiště dokumentů, popř. jiných souborů s informacemi, které mají být publikovány na intranetu ČNB (IBIS). IBIS v současné době používá vlastní úložiště nebo jsou v něm uvedeny odkazy na dosud provozovaný systém IS Obelisk. Po provedení migrace dokumentů z Obelisku do nového DMS musí být odkazy na dokumenty z IBISu přesměrovány do DMS.

##### Integrace s IS SIEM

Viz kapitola 1.7.4. [SIEM (Sběr bezpečnostních logů)](#_SIEM_(Sběr_bezpečnostních).

##### IS Obelisk

Informační systém Obelisk je databázový systém využívaný v ČNB ke správě dokumentů a jejich publikování na intranetu. IS Obelisk je interní aplikace provozovaná nad Oracle DB Serverem (verze 10.2.0.5.0). Do úložiště jsou uploadovány dokumenty formátu MS Office 2010 (a v některých případech i starších verzích MS Office). Uživatelé pracují v několika rolích s oprávněním na čtení nebo vkládání a úpravy dokumentů.

Dokumenty uložené v tomto systému budou předmětem migrace.

##### Podpisová kniha

##### Systém musí umožnit napojení na interní aplikaci ČNB Podpisová kniha, který zajištuje podpis dokumentu kvalifikovaným elektronickým certifikátem.

##### 

##### Aplikace Software 602 Signer

Pro práci s dokumenty v pdf formátu využívá ČNB aplikaci Signer (dodavatel Software 602), verze 3.0.5. Pro manipulaci se soubory (otevření, editace a ukládání) mohou být využity nástroje aplikace Signer. Aplikace zajišťuje převody dokumentů word do formátu PDF a PDF/A, možnost podepsání dokumentu elektronickým certifikátem, včetně vložení časového razítka. Je implementována také jako plug-in do MS Office.

# Migrace dat

Pod pojmem „migrace dat“ jsou zahrnuty tyto akce a procesy:

1. analýza zdrojové struktury IS Obelisk, cílové struktury DMS a transformační mapování mezi oběma strukturami,
2. export objednatelem určených dat z IS Obelisk pro DMS na základě namapování dat,
3. import vyexportovaných dat z IS Obelisk do DMS.

ad a)

Analýzu a přípravu procesu uvedeného v bodu a) musí zajišťovat objednatel ve spolupráci s poskytovatelem DMS. Poskytovatel SW řešení DMS musí poskytnout datové struktury nového systému a ve spolupráci s objednatelem navrhne namapování dat z IS Obelisk a dat DMS. Popis namapování a následné migrace bude zdokumentován v realizační studii.

ad c)

Poskytovatel DMS musí připravit datové struktury a nástroje pro import vyexportovaných dat z IS Obelisk. Po importu musí být provedeno otestování komplexnosti dat (dokumenty včetně metadat), jejich správnosti a přidělení přístupových oprávnění z hlediska metodiky nového DMS.

Objednatel předpokládá, že procesy b) a c) mohou být opakovány několikrát podle specifikace objednatele, vzhledem k typu dat uložených v současném IS Obelisk. Detailní rozsah bude popsán v realizační studii.

# Specifické požadavky

Tabulka technických specifických požadavků je uvedena v příloze č. 2b smlouvy.

*V tabulce vyplňte žlutě označené sloupce.*

1. Interní komunikace – data jsou přenášena pouze důvěryhodnými sítěmi, VPN apod. [↑](#footnote-ref-1)
2. Externí komunikace – data jsou přenášena přes veřejné nebo nezabezpečené sítě (např. Internet) [↑](#footnote-ref-2)