Elektronická spisová služba ASAS v rezortu Ministerstva Obrany na pracovištích ochrany informací

Electronic service record ASAS the Ministri of Defense in the workplace information protection

Bc. Dušan Ház

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Dušan HÁZ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Elektronická spisová služba ASAS v resortu Ministerstva Obrany na pracovištích ochrany informací**

Zásady pro vypracování:

1. **V práci analyzujte hodnotící kritéria pro zavedení a používání elektronické spisové, datové a archivní služby v rámci resortu MO.**
2. **Analyzujte možnost integrace s jinými IS používanými v rámci AČR.**
3. **V práci zhodnoťte službu ASAS z pohledu integrace na každý IS v resortu AČR.**
4. **Zpracujte anylýzu na službu ASAS z pohledu tvůrce a dodavatele flexibilního software.**
5. **Zhodnoťte dosažené výsledky**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Datové schránky v právním řádu ČR, nakladatel: ABF, a.s. Praha**
2. **Zákon o archivnictví, spisová služba, nakladatel: Poradce s.r.o.**
3. **Elektronický podpis 2008 a jeho aplikace v praxi, nakladatel: Anag**
4. **Spisová a archivní služba ve státní správě, 3. vydání, nakladatel: Linde Praha, a.s.**

Vedoucí diplomové práce: **RNDr. Ing. Miloš Krčmář**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Páteří resortu Ministerstva Obrany z pohledu informačních systémů, stejně jako každé jiné organizace, musí být sledování a řízení toku dokumentů a informací bez ohledu na agendovou či oborovou příslušnost.

Současná informační infrastruktura resortu je však tvořena mnoha dílčími informačními systémy, které nejsou schopni efektivně vzájemně data sdílet nebo poskytovat informační podporu ostatním procesům. Ambice na zastřešení a vytvoření jednotného prostředí v resortu MO má projekt Průřezového informačního systému Ministerstva obrany.

Jedním z pilířů při realizaci takového řešení z pohledu sjednocení informačních toků mezi jednotlivými informačními systémy je projekt ASAS (Automatizovaná spisová a archivní služba), kterým resort obrany vstoupil do kvalitně nové fáze správy dokumentů. Projekt ASAS je realizován prostřednictvím informačního systému GINIS® který byl v některých ohledech přizpůsoben specifickým potřebám resortu MO.

Klíčová slova:

Elektronická spisová, datová a archivní služba, ISL, FIS, ŠIS, SEPO, ISMP, ISSP, PRIS, ASAS, GINIS®

ABSTRACT

The backbone of the Ministry of Defense in terms of information systems, as well as any other organization, must monitor and control the flow of documents and information regardless of the multidisciplinary agendovou or jurisdiction.

The current information infrastructure sector is composed of many sub-information systems that are able to efficiently share data with each other or to provide information support to other processes. Ambitions for the roof and create

a single environment in the MoD, the project transversal information system of the Ministryof Defense.

One of the pillars in the implementation of such solutions from the perspective of unification of the information flow between information systems is a project of ASAS (Automated archival filing and service), which the defense department entered a new phase of quality management documents. ASAS project is implemented through the information system ® GINIS who was in some respects adapted to the specific needs of the MoD.

Keywords:

E-File, data and archival services, ISL, FIS, SIS, SEPO, ISMP, ISSP, PRIS, ASAS, GINIS ®

Motto:

……data, která administrativní či řídicí pracovník potřebuje, jsou k dispozici prostřednictvím počítačů, telefonů či jiných forem elektronické komunikace. Mezi velké omyly 20. století patřila představa kanceláře bez papíru. Stalo se něco, co málokdo očekával: požadavky na tištěné výstupy a papírové dokumenty naopak neuvěřitelně narostly. Spotřeba papíru stoupá, a tento trend bude v nejbližší budoucnosti pokračovat.

Posun v digitalizaci nastal v okamžiku, kdy se vyspělé technologie začaly přibližovat běžnému uživateli. Nejvýrazněji se tento trend projevil v digitalizaci zpracování obrazu. Díky pokročilým technologiím, uživatelsky přívětivému softwaru a využívání dokončovacích funkcí dnes téměř každý uživatel dokáže vytvářet tiskoviny profesionálního vzhledu vlastními silami. Budoucnost moderní digitální kanceláře je především ve schopnosti rychle a přesně komunikovat nejen uvnitř společnosti, ale i s vnějšími partnery a zákazníky……

Neil McAllister, technolog a analytik se sídlem v San Franciscu, Kalifornie
(InfoWorld 2005)

Poděkování:

Rád bych touto cestou poděkoval svému vedoucímu mé diplomové práce panu RNDr. Ing. Miloši Krčmářovi za rady a vstřícnou pomoc při jejím zpracovávání. Dále pánům Ing. Stanislavu Simbartlovi ze Sekce personální MO, Ing. Františku Macháčkovi a RNDr. Ing. Jaroslavu Mirovskému ze spol. GORDIC s r.o. za poskytnutí velmi cenných informací a materiálů. Moje poděkování také patří mé rodině, která mě usilovně podporovala po celou dobu studia a v neposlední řadě patří můj dík všem akademickým pracovníkům FAI UTB ve Zlíně.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD **11**

I TEORETICKÁ ČÁST **12**

1 INFORMAČNÍ SYSTÉMY MO **13**

1.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ SOUVISEJÍCÍCH S INFORMAČNÍM SYSTÉMEM 13

1.1.1 Komu jsou určeny 14

1.1.2 Bezpečnost informačních systémů 14

1.2 SOUČASNÝ STAV INFORMAČNÍCH SYSTÉMŮ 15

1.2.1 Stávající platformy 15

1.2.1.1 Software 15

1.2.1.2 Hardware 16

1.2.1.3 Komunikace 17

1.3 PRŮŘEZOVÝ INFORMAČNÍ SYSTÉM MO – PRIS MO 22

1.3.1 Historie a vývoj 22

1.3.2 Funkční vazby na ostatní IS 22

1.3.3 Problémy se zaváděním IS v resortu MO 24

1.3.4 Specifikace hlavních funkcí PRIS MO 24

1.3.4.1 Problémově orientované služby (FAS) 25

1.3.4.2 Společné služby 25

1.3.4.3 Hlavní funkce PRIS MO 25

2 ANALÝZA HODNOTÍCÍCH KRITÉRIÍ PRO ZAVEDENÍ A POUŽÍVÁNÍ ELEKTRONICKÉ SPISOVÉ, DATOVÉ A ARCHIVNÍ SLUŽBY V RÁMCI RESORTU MO **28**

2.1 HODNOTÍCÍ KRITÉRIA 28

2.2 ANALÝZA SOUČASNÉHO STAVU 30

2.2.1 Jednotlivá pracoviště a jejich činnosti 31

2.2.1.1 Podací místo MO 31

2.2.1.2 Útvarová podatelna POI/ROI (podání) 31

2.2.1.3 Vedoucí, Sekretariát, Referent (USU) 31

2.2.1.4 Útvarová výpravna POI/ROI (expedice zásilek) 31

2.2.1.5 Spisovna 32

2.2.2 Elektronické dokumenty 32

2.2.3 Stávající databázové prostředí ASAS 33

2.2.4 Stávající úložiště pro elektronické dokumenty ASAS 34

2.2.5 Specifikace hardwarové konfigurace systému ASAS 35

2.2.6 Specifikace konfigurace koncových stanic ASAS 38

2.2.7 Záloha a obnova serverové části systému ASAS 38

2.2.8 Nastavení plánu bezpečnostní zálohy na datové pásky 38

II PRAKTICKÁ ČÁST **39**

3 ANALÝZA MOŽNOSTÍ INTEGRACE S JINÝMI IS POUŽÍVANÝMI V RÁMCI AČR **40**

3.1 TERMINOLOGIE 42
3.2 PŘÍJEM DOKUMENTŮ 44
3.3 DORUČENÍ, REGISTRACE A EVIDENCE DOKUMENTU 47
3.4 ROZDĚLENÍ A OBĚH DOKUMENTŮ 51
3.5 VYŘIZOVÁNÍ DOKUMENTŮ 54
3.6 VYHOTOVOVÁNÍ DOKUMENTŮ, PODEPISOVÁNÍ DOKUMENTŮ A UŽÍVÁNÍ RAZÍTEK 54
3.7 ODESÍLÁNÍ DOKUMENTŮ 56
3.8 UKLÁDÁNÍ A VYŘIZOVÁNÍ DOKUMENTŮ 62

4 ZHODNOCENÍ SLUŽBY ASAS S POHLEDU INTEGRACE NA KAŽDÝ IS V RÁMCI RESORTU AČR 64

4.1 POSOUZENÍ INTEGRACE NA INTERNET VS. INTRANET 64
4.2 POSOUZENÍ PROPOJENÍ ASAS NA ISDS 64
4.3 DISTRIBUCE ELEKTRONICKÝCH DATOVÝCH ZPRÁV S VYUŽITÍM DOSTUPNÝCH KIS (ŠIS, ISL) 65
4.4 INTERFACE NA AGENDOVÉ SYSTÉMY 65

5 ANALÝZA NA SLUŽBU ASAS S POHLEDU TVŮRCE A PROVOZOVATELE FLEXIBILNÍHO SW 68

5.1 NÁVRH OPATŘENÍ K REALIZACI ZÁKONA Č. 300/2008 SB. PROSTŘEDKY ASAS 68
5.1.1 Okamžitá opatření k zajištění naplnění zákona k datu účinnosti 71
5.1.2 Přechodné období do dosažení cílového stavu 72
5.1.3 Cílové řešení 73
5.2 INTERFACE NA INFORMAČNÍ SYSTÉM DATOVÝCH SCHRÁNEK 74
5.3 KONVERZNÍ PRACOVIŠTĚ (AUTORIZOVANÁ KONVERZE) 74
5.3.1 Autorizovaná konverze do dokumentu obsaženého v datové zprávě 75
5.3.2 Autorizovaná konverze z dokumentu obsaženého v datové zprávě 76
5.3.3 Registr autorizovaných konverzí – RAK 79
5.3.4 Konverzní pracoviště (neautorizovaná konverze) 80
5.4 NÁVRHY ZMĚN INTERNÍCH NOREM 82
5.5 METODIKA, BEZPEČNOST, INA 84
5.6 PODPORA UŽIVATELŮ 87
5.7 PODPORA KONCOVÝCH UŽIVATELŮ 91
5.8 HARDWARE 92
5.8.1 Architektura řešení 93
5.8.2 Nároky na komunikační datovou síť 95
5.8.3 Eliminace rizik v oblasti zabezpečení náhradního provozu 95
5.8.4 Využití geoclusteru pro bezpečné provozování systému GINIS-SSL (ASAS) 96
5.8.5 Stanovení požadavků na centrální úložiště elektronických dokumentů 97

5.8.6 Organizační a personální opatření 99
5.8.7 Analýza finanční náročnosti 101
6 ZHODNOCENÍ DOSAŽENÝCH VÝSLEDKŮ 103
6.1 ZHODNOCENÍ JEDNOTLIVÝCH NABÍZENÝCH FUNKCÍ ASAS 104
ZÁVĚR 112
ZÁVĚR V ANGLIČTINĚ 113
SEZNAM POUŽITÉ LITERATURY 114
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 116
SEZNAM OBRÁZKŮ 118
SEZNAM TABULEK 119

ÚVOD

Systém Spisové služby umožňuje evidenci veškerých údajů o dokumentech i spisech včetně sledování pohybu dokumentů v dané organizaci. Je určen pro kompletní správu dokumentů. Systém činnosti Spisové služby plně vyhovuje platné legislativě a je možno jej použít jako výkonného a efektivního nástroje pro zajištění odborné správy dokumentů došlých a vzešlých z činnosti původce.

Spisová služba pracuje naprosto rovnocenně s analogovými i elektronickými dokumenty. Je možné tedy evidovat jak papírový, tak elektronický dokument i např. obrazový nebo zvukový záznam. Údaje o jednotlivých dokumentech se do systému pořizují ručním zadáváním, elektronickým vstupem nebo lze načíst data z jiných programů (systémů). Systém umožňuje splnit zákonné požadavky na řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení.

V současné době se produkt Spisové služby vyznačuje zejména silnou metodickou stabilitou, která vychází právě z praxí prověřených zkušeností a několikaleté spolupráce s úřady a centrálními institucemi, které jsou ochotny problematiku vedení spisové služby řešit.

Nasazení informačního systému ASAS není postačující podmínkou pro eliminaci rizik. Musí být zabezpečeno důsledné provozování tohoto systému na podkladě platných metodik činností, jež je vhodné doplnit odpovídající formou a četností kontrolní činnosti.

Oběh jednotlivých dokumentů mezi moduly Spisové služby je závislý na vykonávaném procesu (předání k vyřízení, stornování, vrácení k doplnění, předání do předarchivní péče atd.), který je řízen metodikou Spisové služby a interními normami organizace (zejména Spisovým a skartačním řádem). [14]

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ SYSTÉMY MO

Stacionární komunikační infrastruktura v současnosti zahrnuje transportní síť, globální datovou síť, distribuční sítě, telefonní síť a stacionární vojenskou radiovou síť. Základním prvkem je transportní síť, která má zabezpečit výkonné a spolehlivé přenosové prostředí pro hlasové a datové komunikace resortu obrany. Transportní síť byla vybudována na bázi technologií dostupných v době svého vzniku a pokrývala tehdejší potřeby AČR. Poskytované služby jsou v rozsahu a kvalitě poplatné době výstavby. Použitá mikrovlnná technologie již nevyhovuje současným a hlavně definovaným budoucím potřebám IS, zejména z pohledu celkových možností přenosového prostředí, kapacit, zálohování a dohledu. [12]

Komunikační služby pro IS v mírových podmínkách a krizových situacích v současnosti s problémy zabezpečuje celoarmádní datová síť (dále jen „CADS“), která je součástí globální datové sítě. CADS nebyla průběžně rozvíjena, v současné době nesplňuje narůstající požadavky na přenosovou kapacitu a dostupnost, její komplikovaná architektura má negativní vliv na průchodnost sítě a provozní náklady.

Projekt „Modernizace a dostavba komunikační infrastruktury“ je klasifikován jako prioritní pro rozvoj informatizace resortu obrany. Po jeho dokončení v roce 2012 má stacionární komunikační infrastruktura zabezpečit poskytování všech hlasových, datových a multimediálních služeb v jednotné síti a pokrýt potřeby systémů velení a řízení resortu obrany a požadavky PRIS MO v mírových podmínkách a krizových situacích ve všech místech dislokace útvarů a zařízení MO a AČR. [13]

1.1 Vymezení základních pojmů souvisejících s informačním systémem

Resort MO provozuje v současné době tyto informační systémy: Štábní informační systém, Informační systém logistiky, Finanční informační systém, Informační systém o službě a personálu, Digitální vojenský informační systém o území, Informační systém mobilizačních příprav, Informační systém Vojenské policie, Informační systém vojenského zdravotnictví, Informační systém University obrany a Systém elektronické podpory obchodování, Internet MO, Operačně-taktický systém velení a řízení pozemních sil a Operačně taktický systém velení a řízení vzdušných sil. Všechny výše uvedené informační systémy jsou resortní. [13] [18]

V současné době resort připravuje průřezový informační systém (PRIS MO), který nahradí doposud fungující informační systémy.

1.1.1 Komu jsou určeny

Výše uvedené informační systémy podporují řízení činnosti resortu MO včetně administrativních a štábních činností, řízení resortních zdrojů (personálních, finančních a materiálních), dále pak podporují činnost vojenských služeb, velení a řízení v operacích.

Rozvoj resortu obrany vyžaduje zvýšené nároky na hlavní a řídící procesy (k dosažení počátečních a cílových operačních schopností AČR, schopností NEC, rozšíření a zkvalitnění výkonu misí AČR v zahraničí apod.), a tím i zvýšené nároky na jejich podpůrné procesy.

K informačnímu zabezpečení bude nezbytné využití moderních integrovaných KIS.

Prostředkem k dosažení požadovaných cílů jsou strategické projekty:

- průřezový informační systém MO (PRIS MO);
- modernizace a dostavba komunikační infrastruktury;
- operačně-taktické systémy velení a řízení pozemních a vzdušných sil.

Vzhledem k provázanosti je pouze vzájemná součinnost všech uvedených strategických projektů předpokladem úspěšného splnění „Koncepce výstavby profesionální Armády České republiky a mobilizace ozbrojených sil České republiky přepracovaná na změněný zdrojový rámec“, přijaté vládou dne 12. 11. 2003 usnesením č. 1154. [13] [18]

1.1.2 Bezpečnost informačních systémů

Z hlediska požadavků na bezpečnost zpracovávaných informaci je PRIS MO členěn na tři relativně samostatné subsystémy „Tajný“, „Vyhrazený“ a „Internet MO“.

Základní prvky pro řízení bezpečnosti informatizace jsou vytvořeny prakticky na všech stupních řízení, avšak většina úkolů spjatých se zabezpečením zpracovávání a komplexního využívání utajovaných informací uživateli příslušných IS nebyla splněna podle původních záměrů. Zatím není provozován žádný IS, který by komplexně průřezově zabezpečoval zpracování a přenos utajených dat pro podporu hlavních a řídících procesů.

Zásadním problémem je zabezpečení komunikační infrastruktury, která musí být řešena individuálně v rámci jednotlivých IS. Komplexní řešení problému bezpečnosti informací u IS lze zřejmě očekávat až s konečnou realizací projektu PRIS MO. Pro tento projekt byl už v únoru roku 2003 schválen „Bezpečnostní záměr Průřezového informačního systému MO“ v souladu s legislativou ČR a NATO. [13] [18]

1.2 Současný stav informačních systémů

V současné době je informační infrastruktura resortu MO tvořena řadou autonomních informačních systémů s vlastní technologickou základnou, aplikačním programovým vybavením, bezpečnostní politikou a datovými zdroji. Částečná integrace těchto systémů je nyní prováděna na bázi propojení elektronických pošt a zabezpečení omezené výměny dat prostřednictvím CADS, nebo Štábního informačního systému, případně na datových médiích.

Současná funkcionalita informačních systémů v rámci resortu MO řeší nejenom specifické požadavky dané potřebami v jednotlivých částech resortu MO, ale také obecné služby (email, kancelářský software, Intranet, atd.). Tyto služby bohužel nejsou poskytovány prostřednictvím jednoho informačního systému, ale každý IS řeší tyto služby vlastní cestou. Vzniká tak multiplatformní prostředí vzájemně ne zcela kompatibilních služeb, poskytujících obdobnou funkcionalitu. Ve svém důsledku to ve většině případů pro uživatele znamená, že pokud má přístup do více informačních systémů, musí mít zároveň ke každému zvláštní pracovní stanici. [14]

1.2.1 Stávající platformy

Stávající IS, nebyly budovány na jednotné platformě. Z tohoto stavu vychází i nedostatky stávajících systémů, obtíže s podporou velkého množství různých platforem, problémy vzájemné kompatibility poskytovaných služeb, atd.

1.2.1.1 Software

Informační systémy pracují na operačních systémech:

- Rodina Microsoft Windows – NT4.0 server, Windows 2000 server.
- UNIX – HP Unix (HP-UX), SCO Unix, AIX, IRIX, další klony Unixu.

Pracovní stanice pracují v drtivé většině na operačních systémech rodiny Microsoft Windows, ve verzích od Windows 95 až po Windows XP Professional. Většina stanic má instalován OS Windows 2000 Professional. Databázové systémy pracují na platformách Oracle, Informix, Microsoft SQL 2000, Lotus Notes, Caché, Sybase. Elektronická pošta je řešena technologií Microsoft Exchange, v jednom případě je použito prostředků Lotus Notes. Některá řešení jsou opatřena antivirovým softwarem, nasazeným buď na serverech, nebo i na pracovních stanicích. [14]

Při hodnocení současného stavu v souvislosti s požadovanou interoperabilitou se systémy Aliance (Bi-SC AIS), je třeba vycházet z dokumentů Aliance, popisujících bázi produktů instalovaných a doporučených pro instalaci v rámci informačních systémů Aliance. Jde zejména o dokument „NC3TA Volume 5 verze 5 NC3 Common Operating Environment“, popisující ve své příloze „A. NCOE basket of products“ strukturovaný seznam produktů certifikovaných aliancí pro implementaci v rámci Bi-SC AIS. Tento seznam produktů značným způsobem limituje počet platforem využitelných pro budování informačních systémů založených na modelu Bi-SC AIS. Produkty, které nejsou v této kapitole přímo vyjmenovány, musí buď úspěšně projít NCOE výběrem produktů (NC3TA Volume 5 verze 5 NC3 Common Operating Environment - NCOE Product Selection Process), nebo nemohou být pro implementaci v rámci NATO Bi-SC AIS systémů použity.

Vzhledem ke zdlouhavému procesu schvalování výběru technologií pro zařazení na seznam schválených produktů, doporučujeme v rámci budování PRIS MO a dalšího rozvoje informačních systémů používat výhradně produkty již schválené.

V případě uplatnění výše uvedené selekce na přehled software instalovaného v rámci existujících systémů dojdeme ke zjištění, že bez dalšího schválení systémů lze použít operační systémy Windows 2000 a výhledově Windows XP, databázové servery Oracle 9i a Microsoft SQL Server 2000. Po provedení kompletního auditu softwarových licencí v resortu MO lze přesně stanovit počty a typy licencí použitelných při implementaci systému PRIS MO. [14]

1.2.1.2 Hardware

Většina informačních systémů je provozována na hardwarové platformě Intel serverů různých výrobců. Další platformy, které jsou v rámci stávajících IS zastoupeny: IBM RISC, HP RISC a SGI. Část systémů používá disková pole EMC Symmetrix.

Jako pracovní stanice jsou v naprosté většině využívány PC Intel. V několika případech je instalován terminál RDP/ICA.

Hardwarové platformy použitelné pro budování infrastruktury na modelu Bi-SC AIS musí hostovat operační systémy a aplikační software zmíněné v předchozí kapitole. Zároveň musí opět splňovat minimální a doporučené konfigurace, uvedené v dokumentu „MHWPS: SERVERS & SERVER STORAGE“. [14]

Po aplikování výše uvedených podmínek na stávající platformy informačních systémů vyplývá, že pro využití v nově budovaných systémech připadají v úvahu servery na platformě Intel, na kterou jsou portovány operační systémy Microsoft Windows nebo platformy, na které je portován operační systém Sun Solaris 9.0.

Pracovní stanice jsou vesměs v konfiguracích, které splňují současné nároky na minimální konfiguraci pracovní stanice. Stanice, které tyto parametry (viz. následující výčet) nesplňují, bude nutné postupně nahradit. [14]

- PC s taktovací frekvencí procesoru 300 megahertz nebo vyšší; nejmenší požadovaná frekvence je 233 MHz (jednoduchý nebo duální procesor).
- Doporučená RAM 128 megabytů (MB) a vyšší (nejnižší požadovaná operační paměť 64 MB; může však omezovat výkon a některé funkce).
- 1,5 gigabytů (GB) volného místa na harddisku.
- Video adaptér a monitor Super VGA s rozlišením (800 × 600) nebo vyšším.
- CD-ROM nebo DVD drive.
- Klávesnice a myš.

1.2.1.3 Komunikace

Při vyhodnocení současného stavu IS z pohledu komunikací je zřejmé, že tato oblast není vytvářena dle jednotné koncepce. U IS se použité komunikační prostření značně liší a lze je v zásadě rozdělit na dvě skupiny:

- IS, které mají vybudované vlastní komunikační prostředí, které je spravováno skupinou administrátorů v rámci samotného IS.
- IS, které plně spoléhají na subjekt KI jakožto poskytovatele komunikačních prostředků a služeb v resortu MO.

IS s vlastním komunikačním prostředím

IS s vlastním vybudovaným komunikačním prostředím mohou mít formu uzavřeného IS, který je striktně oddělen od komunikačních sítí resortu MO. Jedná se o fyzicky oddělené IS typu ISVP, ISVZ. Striktní oddělení platí především u IS, které pracují s citlivými informacemi a které nejsou z principu vázány na jiné IS.

IS s vybudovaným komunikačním prostředím jsou i IS, které jsou odděleny od komunikačních sítí resortu MO pomocí vlastního bezpečnostního prvku. IS oddělené od KI pomocí bezpečnostního prvku jsou IS FIS, PIS (ISSP), DVISÚ, ISMP, ISUO, ISVP, ISVZ, OTS VŘ. [14]

Charakteristika IS s vlastním komunikačním prostředím:

- IS s vlastní komunikační infrastrukturou jsou odvozeny od vytvořeného distribuovaného systému, který byl vytvořen z důvodu soustředění určitého počtu uživatelů IS do skupin v místech po České republice.
- IS si vytvořil na straně uživatelů tzv. pobočku s kompletní množinou uživatelských služeb, které jim v rámci IS poskytuje.
- Na straně uživatelů jsou i lokální servery IS, stanice IS a také i aktivní síťové prvky IS.
- Tento typ systému vytváří jak na straně uživatelů, tak i centra zcela autonomní prostředí, které využívá CADS pouze jako transportní spojovací síť.
- Omezené kapacitní možnosti mají na svědomí vznik poboček IS, použití distribuovaného systému pak podstatně snižuje nároky na přenosovou kapacitu přidělenou ze strany CADS.

IS závislé na KI

Jedná se o IS, které plně spoléhají na subjekt KI jakožto poskytovatele komunikačních prostředků a služeb v resortu MO a které využívají kompletní komunikační prostředí jako „end-to-end“ službu. Tato služba zahrnuje vše od rozhraní na straně IS, včetně komunikačního prostředí typu LAN a WAN, až po rozhraní na straně uživatele. Jedná se o IS ISL a ŠIS. V tomto případě je KI přímo zodpovědná za zajištění potřebných

komunikačních a bezpečnostních prostředků, nesplnění požadavků stranou KI je pro IS limitujícím faktorem jak v provozu, tak i případné certifikaci NBÚ. [14]

Charakteristika IS závislého na KI:

- Tento typ IS je ve většině případů důsledkem centrálně řešeného systému.
- Administrátoři IS soustředili kompletní sadu služeb na straně centra.
- Uživatelé jsou jednotlivě rozmístěni po území České republiky.
- Uživatelé používají pouze určené unifikované PC s tenkým nebo i tlustým klientem.

Hodnocení současného stavu KI v rámci IS

Po vyhodnocení zjištěných faktů lze říci, že důsledkem nejednotného komunikačního prostředí v rámci IS, je především nedostatečné pokrytí komunikačních a bezpečnostních požadavků kladených na poskytovatele komunikačních služeb a prostředků v resortu MO, tj. na stranu KI. [14]

Vyhodnocení stavu v bodech:

- IS jsou nuceny si zajišťovat vlastní komunikační prostředky a služby kvůli nedostatkům v KI.
- IS, které mají blíže k finančním zdrojům, si dokáží získat snadněji prostředky ke svému provozu a řeší bezpečnostní a komunikační nedostatky vlastními silami.
- Technologie a služby v IS pak mohou být na vyšší technické úrovni (například FIS) než v nosné síti KI.
- Část IS využívá komunikační infrastrukturu typu WAN od veřejných poskytovatelů (SP). Jedná se o komunikaci v rámci částí ISVZ, dále o spoje v rámci FIS, kde není přípojka CADS. Výsledným jevem je nejednotná implementace komunikačního a bezpečnostního prostředí jak v rámci IS, tak i v samotném resortu MO.

Hodnocení komunikačního prostředí IS z pohledu integrace

Z pohledu hodnocení komunikačního prostředí IS a procesu integrace je zřejmé, že vývoj IS musí postupovat k jednotnému komunikačnímu prostředí jak na straně centra, transportního prostředí v rámci WAN, tak i na straně uživatelské části. Základním předpokladem je cesta k centralizovanému modelu, omezení společných duplicitních služeb v rámci IS, s tím, že IS jsou postupně transformovány do FAS. [14]

Tento směr je dle mého názoru možný pouze za předpokladu zajištění následujících kroků:

- sjednotit geografické rozložení IS, pokud je to možné,
- posun z distribuovaného modelu na model centralizovaný,
- použití jednotného tenkého klienta pro prostředí resortu MO,
- použití jednotných nástrojů a komunikačních prostředků v resortu MO,
- jednotná správa nástrojů a komunikačních prostředků pod správou KI resortu MO,
- zajištění dostatečného přenosového pásma od uživatelů na systém,
- subjekt KI musí fungovat jako poskytovatel služeb (SP) v rámci resortu MO,
- KI musí zajišťovat adekvátní komunikační služby vyplývající z jeho role,
- v prostředí KI musí být zajištěna zabezpečená výměna informací.

Při implementaci FAS na stávající IS musí také dojít k přesunu, případně rozdělení IS do zajištěných segmentů typu T-LAN, V-LAN, I-LAN, které jsou pod jednotnou správou subjektu KI. Segmenty mohou být dle požadavků IS dále členěny a zabezpečeny. Při procesu implementace FAS na stávajících IS doporučuji vyhodnotit použité aktivní prvky včetně jejich hardwarové a softwarové konfigurace. [14]

Důležité parametry komunikačních prvků k jejich vyhodnocení:

- schopnosti, požadované funkce,
- kompatibilita s ostatními prvky,

- výkonnost přenosu dat ve vrstvách L2/L3 ISO OSI modelu,
- stáří a podpora výrobcem (EoL/EoS1),
- technologie, podpora standardů NATO.

Tím, že KI převezme správu prostředků, stane se také i orgánem, který musí sledovat a vyhodnocovat parametry provozu včetně zajištění výměny dosluhujících prvků za prvky nové. Lze očekávat, že v procesu integrace vzniknou požadavky na výměnu komunikačních prvků. [14]

Doporučuji v rámci integrace provést sjednocení již konkrétních komunikačních prostředků typu:

- Prostředky LAN, které využívají ke komunikaci technologie postavené na standardech IEEE 802.3, konkrétně přepínaný Ethernet o rychlostech 10/100/1000 Mbit/s. Volba rychlosti a výkonnosti se přímo odvíjí od požadavků na přenos dat. Volba typu média se odvíjí od požadavků na vzdálenost, případně na splnění požadavků norem TEMPEST.
- Prostředky WAN v rámci IS doporučuji sjednotit s prostředky CADS. Důvodem je zajištění centralizované správy a dohledu přes jednotné nástroje pro správu, podpora standardů v prostředí WAN a jejich vzájemná kompatibilita.

Varianty integrace komunikační infrastruktury v rámci IS

Ze zjištěných skutečností vyplývají dvě možné varianty integrace:

Varianta A: IS plně závislý na KI:

- komunikační prostředky IS plně podléhají správě a dohledu KI,

Varianta B: IS vlastní omezené prostředky:

- IS má část vlastních komunikačních a bezpečnostních prostředků,
- použití komunikačních prostředků podléhá schválení subjektu KI,
- následnou konfiguraci a správu prostředků IS provádí vlastními silami.

Dle mého názoru jsou si obě varianty ve výsledku navzájem podobné. U obou variant dojde k sjednocení a následné řádné kontrole prostředků. Druhá varianta poskytuje navíc omezené prvky autonomie. Varianta B je vhodná především pro systémy typu ISVZ nebo ISVP, které musí přiměřeně chránit své citlivé zdroje i v rámci stejné úrovně subsystému. [14]

Závěr

Integrace komunikační infrastruktury IS do jednotného prostředí KI je možná, a to za podmínek dodržení provozních požadavků IS. Je nutné zachovat stávající kvalitu a pružnost správy i po převedení pod jednotnou správu pracovníky KI.

Dle mého názoru musí mít prioritu dokončení již nastartovaného procesu modernizace a dostavby KI resortu MO s tím, že musí být zohledněny komunikační požadavky kladené na zajištění provozu PRIS MO a stávajících IS. [14]

1.3 Průřezový informační systém MO – PRIS MO

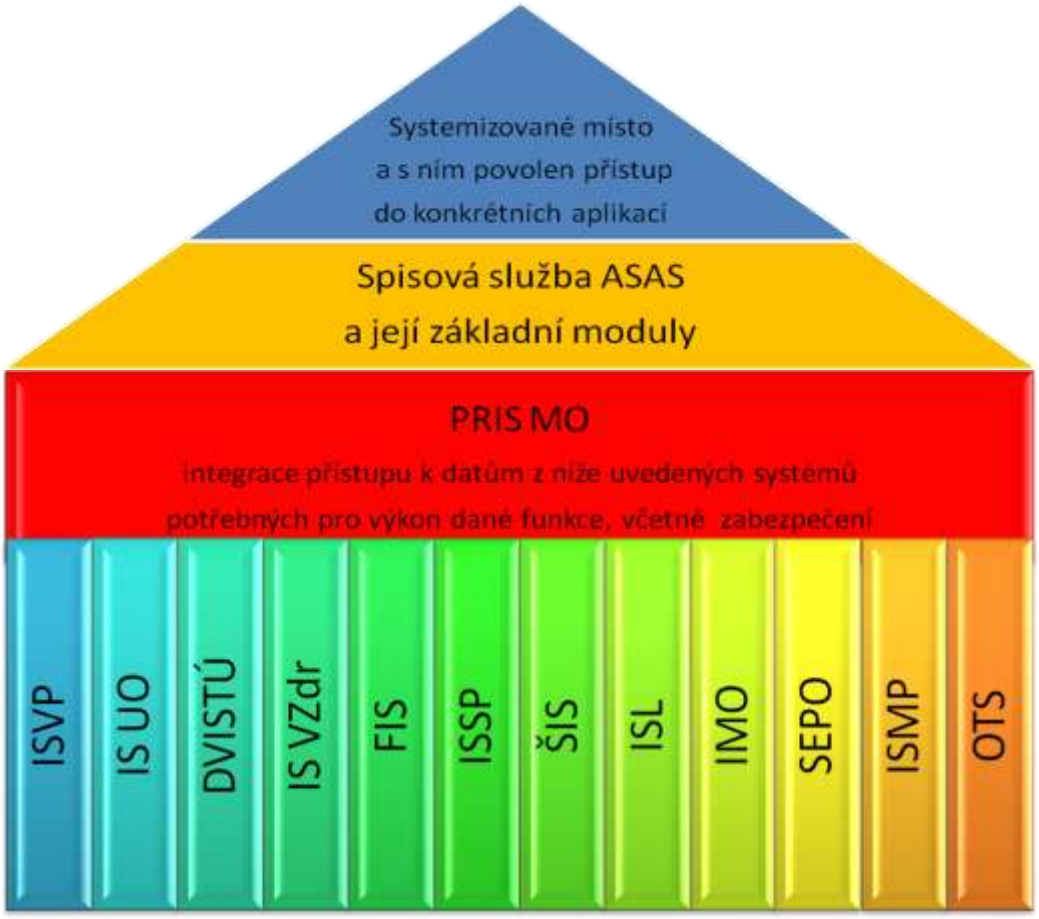
1.3.1 Historie a vývoj

Hlavním důvodem nutnosti realizace PRIS MO (průřezový informační systém Ministerstva obrany), je skutečnost, že všechny stávající stacionární IS, nejsou budovány na jednotné platformě. Nejedná se o výstavbu nového IS, ale o integraci stávajících IS na bázi společných služeb a aplikací, s maximálním využitím již dříve vynaložených investic. Přestože PRIS MO představuje prioritu v úkolech dosažení cílových operačních schopností AČR, jeho výstavba se opožďuje.

1.3.2 Funkční vazby na ostatní IS

Přidělením systemizovaného místa vojáku z povolání nebo občanskému zaměstnanci se zároveň otvírá přístup k datům čerpajících ze stávajících informačních systémů. Toto je možné zabezpečit právě pomocí první ***integrační vrstvy*** „Spisové služby ASAS“ a jejích modulů, na kterou navazuje druhá vrstva PRIS MO, která nejen že zabezpečuje přístup pouze k určitým systémům, ale i informacím (podle funkce, stupně utajení apod.). Toto rozvrstvení má ještě další úkol a to, zabezpečit že všechny informace v obou směrech (od uživatele k uloženým datům a naopak), budou za pomocí PRIS MO dostupné v on-line režimu. [13]

Při myšlence vzniku ***integrační vrstvy*** resort obrany vycházel nejen z analýzy současného stavu v resortu, ale také se inspiroval zkušenostmi jiných institucí, které potřebovaly zajistit průřezový IS, nebo integrační vrstvu např. ČSSZ (Česká správa sociálního zabezpečení), pro kterou vytvořila Projekt AAA portálu společnost Siemens IT Solutions and Services spol. s r.o., a následně jej také u ní implementovala. Význam tří áček: A jako ***Autentizace*** – do této kategorie spadá práce s identitou uživatele tzv. Identity Management a také SingleSingOn – jednotná identifikace uživatele. A jako ***Autorizace*** – správa uživatelských oprávnění a systém jejich přidělování – tzv. Access Manager. A jako ***Audit*** – systém zaznamenávání toho, co se v AAA portálu děje a tvorba reportů a statistik. [14]



Obr. 1. Dostupnost IS za pomoci integrační vrstvy spisové služby ASAS a PRIS MO

1.3.3 Problémy se zaváděním IS v resortu MO

V prvopočátku vzniku PRIS MO byly provedeny hloubkové analýzy, které nechala vyhotovit Sekce KIS. Na základě těchto analýz bylo zjištěno, že průřezový informační systém je nutný, nicméně od začátku se musí počítat s různými problémy při jeho vývoji i implementaci. Nejdiskutabilnější oblasti při vývoji a vzniku PRIS MO:

- nutnost společného managementu;
- nutnost některých společných služeb (identity management, portálový přístup, e – mailové služby, podpora Microsoft Office aj.);
- nutnost propojení databází u některých systémů (např. SEPO nepotřebuje tak objemné databáze, naopak pro jiné systémy jsou databáze stěžejní např. ISSP, ISL, DVISTÚ apod.);
- vytvoření sjednocovací vrstvy (ISL – SGI severy, FIS – IBM servery apod.);
- zabezpečení napříč všemi systémy;
- nutnost třídění informací (z pohledu stupně utajení „V“; „D“; „T“; „PT“, dále ochrany osobních dat, neporušení zákonů a INA);
- nutnost komunikace mezi IS, mezi jednotlivými útvary resortu a zároveň komunikace mimo resort;
- nutnost implementace Zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů a Zákona 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů;
- financování celého projektu.

V současné době je gestorem tohoto projektu Sekce KIS (SKIS), k dnešnímu dni je PRIS MO v implementační fázi, kdy se postupuje tzv. přírůstkovou metodou, která je závislá především na finančním rozpočtu pro tento účel vyhrazeném a zároveň aktuálních potřebách gestorů (náměstků) jednotlivých IS. [13] [14]

1.3.4 Specifikace hlavních funkcí PRIS MO

Tato kapitola specifikuje hlavní funkce systému PRIS MO.

Při specifikaci PRIS MO vycházíme z předpokladu, že ***systém má svému uživateli zajistit jednotné integrované prostředí pro přístup ke společným a problémově orientovaným službám*** (FAS) sloužícím jako informační podpora procesů. Systém PRIS MO je navržen pro zajišťování informační podpory pro správní a administrativní procesy a dále pro procesy velení a řízení při jejich realizaci v míru a v krizových situacích. [14]

1.3.4.1 Problémově orientované služby (FAS)

FAS, jsou organizovaným a integrovaným souborem systémových aplikačních služeb, integrovaných databází a asociovaných nástrojů pro podporu rozhodování. FAS, jsou společně navrženy tak, aby odpovídaly operačním požadavkům konkrétních organizačních jednotek resortu MO. Problémově orientované služby (FAS) jsou systémové aplikační služby jak systémů PRIS MO, tak NATO Bi-SC automatizovaného informačního systému (AIS). [14]

1.3.4.2 Společné služby

Společnými službami nazýváme služby automatizovaného informačního systému (AIS) ke zpracování a prohlížení dat standardním způsobem, za použití síťového připojení. ***Tyto služby zahrnují databázový přístup, předávání zpráv, automatizaci kancelářských prací, správu dokumentů, archivaci, publikaci dokumentů, atd.*** [14]

1.3.4.3 Hlavní funkce PRIS MO

Doporučuji, aby systém PRIS MO zajišťoval následující hlavní funkce:

- ***Jednotná identifikace uživatele*** – Uživatel se proti systému identifikuje pomocí svého uživatelského certifikátu nebo jména/hesla (dle bezpečnostní úrovně daného subsystému). Tato identifikace je pro přihlášeného uživatele udržována Portálem a je předávána dalším službám, ke kterým uživatel přistupuje.
- ***Jednotný přístupový bod do PRIS MO*** - Přístup k informacím zajišťuje PRIS MO pomocí web portálu PRIS MO. Tento Portál zprostředkovává uživatelům přístup k jednotnému uživatelskému rozhraní služeb

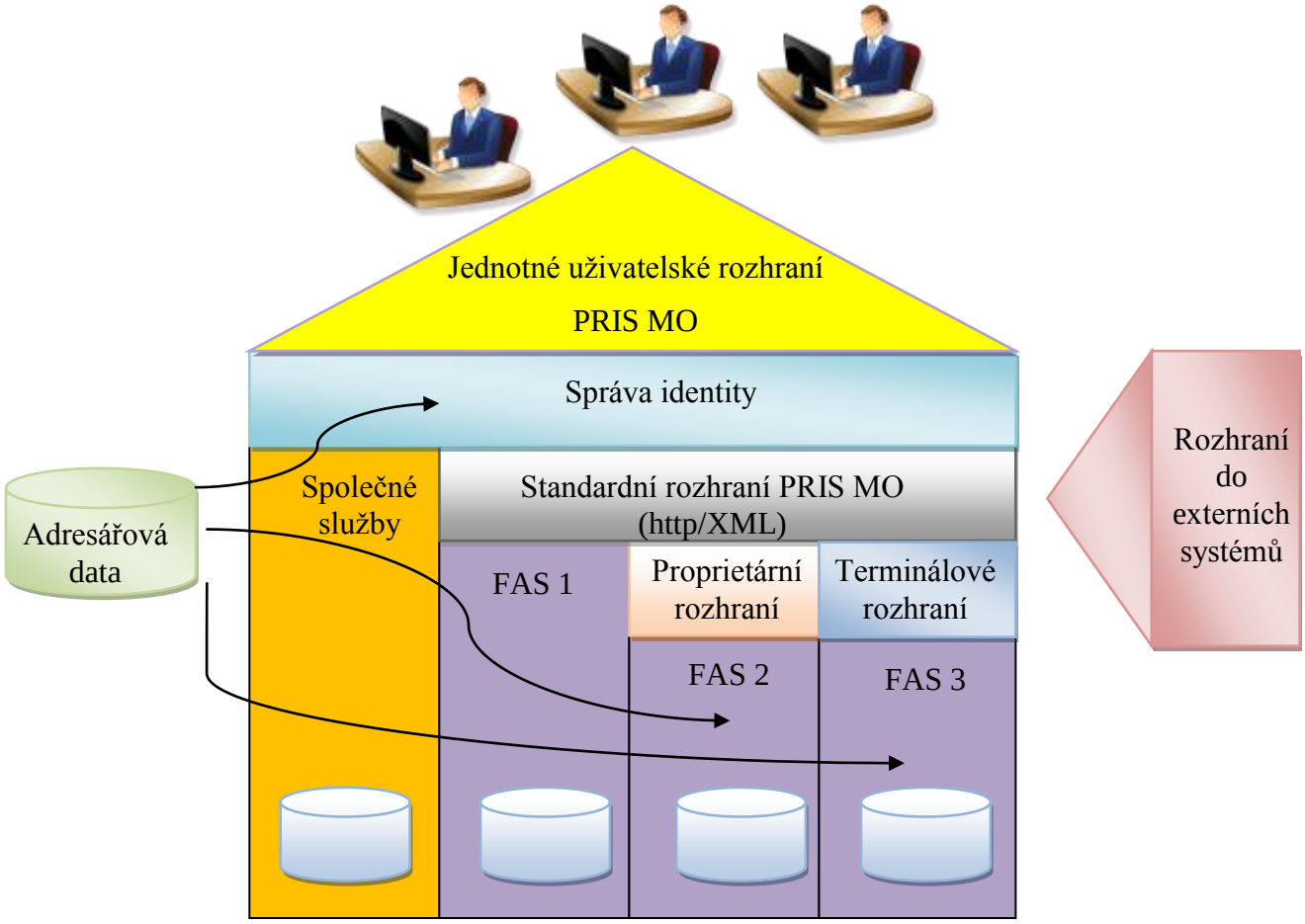
a zajišťuje další nezbytné služby pro fungování navazujících společných a problémově orientovaných služeb.

- ***Jednotné uživatelské rozhraní*** – Portál uživateli poskytuje informace v jednotné formě, která může být uživatelem nebo administrátorem modifikována podle aktuálních potřeb.
- ***Rozdělení služeb do subsystémů*** – PRIS MO bude zajišťovat bezpečné oddělení služeb v jednotlivých subsystémech (Internet MO, Vyhrazený, Tajný)
- ***Zajištění jednotného aplikačního rozhraní*** – Infrastruktura portálu bude navržena pro zajištění jednotného aplikačního rozhraní (standardní rozhraní PRIS MO) jak mezi uživatelem a službami, tak mezi službami samotnými. Toto rozhraní bude zároveň poskytovat jednotné napojení na IS externích subjektů. Doporučuji, aby při napojení PRIS MO mimo resort MO bylo vždy použito prostředků k bezpečnému oddělení subjektů. V budoucnosti by se také mohlo zvážit nasazení jednosměrného rozhraní k bezpečnému propojení vnitřních subsystémů PRIS MO (datové diody).
- ***Zajištění výměny a agregace dat*** – Systém PRIS MO bude prostřednictvím standardního rozhraní zajišťovat datovou komunikaci mezi jednotlivými službami a datovými zdroji. Dále bude provádět agregaci dat z jednotlivých informačních systémů do datového skladu za účelem možnosti dalšího využití nástroji pro podporu rozhodovacích procesů.
- ***Audit činnosti uživatele a systému*** – Systém PRIS MO bude uchovávat auditní záznamy o činnosti prováděné nad systémem PRIS MO a umožní tato data příslušným způsobem vyhodnocovat a provádět protiopatření.
- ***Zajištění vysoké dostupnosti služeb*** – Doporučujeme systém PRIS MO budovat v redundantní konfiguraci tak, aby možné krizové stavy neovlivnily zásadním způsobem běh systému.

Na následujícím obrázku obr. 2 – Základní koncept architektury PRIS MO je znázorněn základní pohled na koncepci systému PRIS MO. Tento základní pohled zobrazuje pouze jediný subsystém PRIS MO. Tento princip je pro každý bezpečnostní

subsystémy aplikován obdobným způsobem (jednotné uživatelské rozhraní – Portál, správa identity, standardizované rozhraní, společné služby, problémově orientované služby (FAS) a datové zdroje). [14]

Obrázek popisuje základní princip PRIS MO, tj. přístup uživatele skrz jednotné uživatelské rozhraní ke všem společným službám a FAS, ke kterým má nárok přistupovat.



Obr. 2. Základní koncept architektury PRIS MO

2 ANALÝZA HODNOTÍCÍCH KRITÉRIÍ PRO ZAVEDENÍ A POUŽÍVÁNÍ ELEKTRONICKÉ SPISOVÉ, DATOVÉ A ARCHIVNÍ SLUŽBY V RÁMCI RESORTU MO

2.1 Hodnotící kritéria

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů v okamžiku své účinnosti od 1. 7. 2009 způsobil „revoluci v úřadování“ a vyžaduje po Ministerstvu obrany ČR, jakožto veřejnoprávním původci (§ 63 zákona 499/2004 Sb., o archivnictví a spisové službě), ***organizační zajištění příjmu a odesílání datových zpráv, jejich oběh, vyřizování a následně ukládání.***

Od roku 2005 je v prostředí Ministerstva obrany ČR úspěšně provozována a dále rozvíjena elektronická automatizovaná spisová a archivní služba ASAS MO (dále jen ASAS). ***Základ ASAS byl vybudován na produktu Spisová služba GINIS®–SSL firmy GORDIC spol. s r. o a na jeho metodických základech.***

Aktuálně je v systému ASAS administrováno 3105 pracovníků MO. V lokalitách implementace ASAS systém zabezpečuje svým rozsahem kompletní výkon spisové služby úřadu do pozice referent. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, má dopady především na výkon metodiky spisové služby. Metodickou podporu projektu ASAS zabezpečuje na Ministerstvu obrany ČR Odbor bezpečnosti MO. ***V souvislosti s dopady uvedeného zákona musí být tedy zabezpečena zejména změna výkonu metodiky spisové služby MO ČR, novela spisového a skartačního řádu MO (ADM 1-1), podpora koncových uživatelů a případně i personální otázka projektu ASAS a související technologické provozní předpoklady***.

Významným úkolem projektu je interface na informační systém datových schránek (dále jen ISDS) a integrace s ostatními (agentovými) informačními systémy rezortu MO.

Předpoklady pro úspěšné vyřešení dopadů zákona č. 300/2008 Sb. a zvládnutí skokového nárůstu elektronických dokumentů v systému spisové služby v rezortu MO lze identifikovat zejména v těchto oblastech:

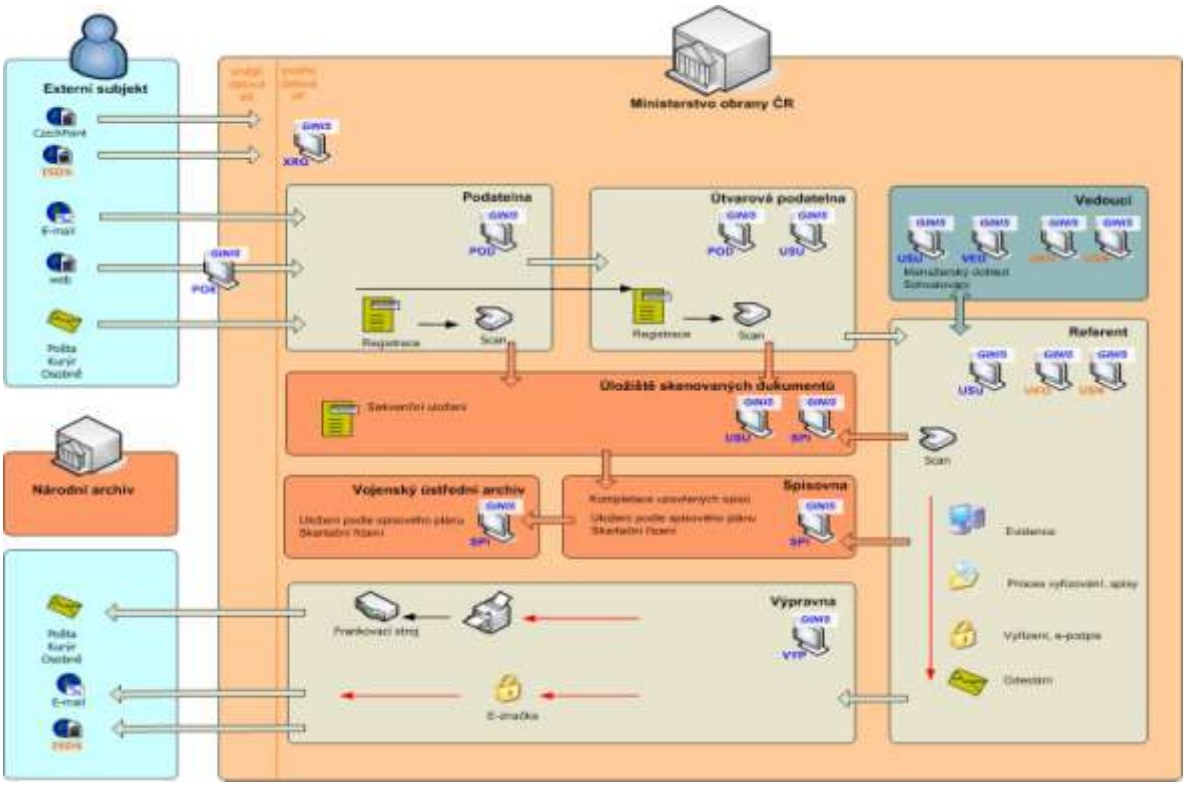
- zprovoznění rozhraní ASAS na Informační systém datových schránek (ISDS);
- autorizované konverze dokumentů;
- úprava výkonu metodiky spisové služby MO;
- zprovoznění rozhraní na agendové informační systémy;
- zajištění plné podpory elektronického úřadování, metodiky ASAS pro výhradně elektronické dokumenty.

Cílový stav, zahrnující dopady zákona č. 300/2008 Sb. a návazných kroků v oblasti eGovernmentu, je charakterizován ***rozšířením o další komponenty ve vztahu k okolním systémům***. Návrh cílového stavu je zobrazen na následujícím obrázku a dále je podrobně popsán v kapitole 5. Návrh řešení a návrh implementace opatření k realizaci zákona č. 300/2008 Sb. v resortu MO prostředky ASAS. [13] [14]

Současně je nutné se připravit na řešení následných úkolů v dalších letech, zejména na vytvoření interface na základní registry a interface na digitální archiv rezortu MO.

Předložený dokument přináší analýzu současného stavu a rozbor dopadů zákona. Současně poskytuje konkrétní návrhy řešení a odhaduje finanční náročnost jednotlivých oblastí. Vzhledem k dynamickému vývoji v oblasti elektronizace veřejné správy (eGovernmentu) předkládaný dokument není dokumentem statickým, ale dokumentem se kterým je nezbytné pracovat a v pravidelných intervalech jej aktualizovat v souladu s vývojem jak vnějšího prostředí a jeho legislativy, tak s vývojem informatizace rezortu MO. [14]

Vzhledem ke kriticky krátkému období na realizaci zákona a k složitosti a velmi širokému rozsahu vzájemně provázaných oblastí je pro úspěšné zvládnutí legislativních požadavků nezbytný rychlý a koordinovaný postup všech zodpovědných složek rezortu.



Obr. 3. Základní blokové schéma SSL – popis cílového stavu [14]

2.2 Analýza současného stavu

V rámci ***I. etapy ASAS*** v roce 2005 byly vybaveny tři OC (Kancelář MO, Kancelář náčelníka GŠ, OB MO) SW GINIS®-SSL pro tři evidenční místa a 200 klientů (uživatelů). SW je u těchto OC využíván.

Ve ***II. etapě ASAS*** v roce 2006 bylo dodáno SW vybavení pro 20 evidenčních míst a 2500 klientů. Do provozu jej uvedl pouze jeden OC (sekce personální MO), u ostatních plánovaných OC se implementace nezdařila především z důvodů metodických (nevhodná organizace školení uživatelů a absence metodického vedení ze strany OB MO) a technologických (absence dostatečného technologického zázemí pro plnohodnotný provoz ASAS).

Během ***III. etapy ASAS*** v roce 2008 byl nakoupen SW pro jedno evidenční místo a 45 klientů, v současné době probíhá jeho nasazení u jednoho OC (34. základna KIS).

V rámci projektu FIS bylo dále pořízeno SW vybavení pro dvě evidenční místa a 200 klientů. [13] [14]

V rámci projektu UKO bylo dále pořízeno SW vybavení pro pět evidenční místa a 160 klientů.

Celkově má tedy rezort MO k dispozici SW vybavení pro 31 evidenčních míst a 3105 klientů za více než 33 mil. Kč. Reálně je však využíváno asi 600 klientů a pět evidenčních míst, což je cca 15 % z předpokládaných cílových počtů uživatelů. [13]

2.2.1 Jednotlivá pracoviště a jejich činnosti

2.2.1.1 Podací místo MO

Elektronická podatelna MO – slouží pro příjem a odesílání datové zprávy při korespondenci s občany nebo organizacemi České republiky, které za použití zaručeného elektronického podpisu požívají stejnou právní kvalifikaci, jako dokumenty v listinné formě, jež obsahují notářsky ověřený/é podpis/y.

Elektronická podatelna MO slouží pro příjem elektronických podání od občanů ČR a organizací ČR ve smyslu nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů a vyhlášky č. 496/2004 Sb. o elektronických podatelnách. [13] [17]

2.2.1.2 Útvarová podatelna POI/ROI (podání)

Podatelna – slouží pro příjem, označování, registraci dokumentů (včetně zachycení základních i rozšířených evidenčních údajů), jejich základní třídění a přidělení spisovým uzlům. Dokumentu je jejím prostřednictvím přiřazen prvotní identifikátor dokumentu.

2.2.1.3 Vedoucí, Sekretariát, Referent (USU)

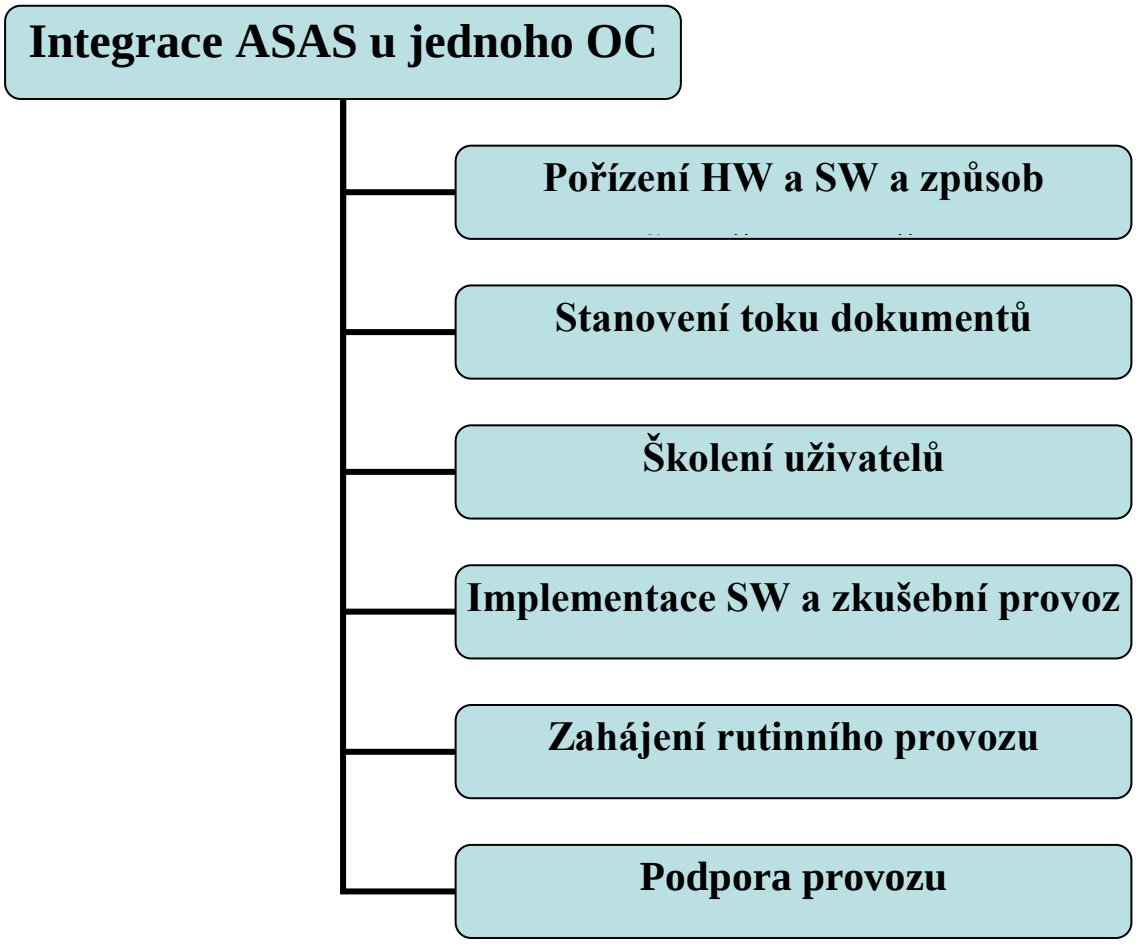
Univerzální spisový uzel – slouží k převzetí dokumentů z podatelny, dokončení evidence, vytvoření spisu, jeho vyřízení, přípravě k vypravení, případně stornování zápisu. Jeho prostřednictvím je rovněž sledován pohyb dokumentu.

2.2.1.4 Útvarová výpravna POI/ROI (expedice zásilek)

Výpravna – slouží k převzetí odesílaných zásilek od jednotlivých spisových uzlů, jejich označení podacím číslem, vytvoření poštovního podacího archu, případně ofrankování a následnému předání k přepravě držitelem poštovní licence.

2.2.1.5 Spisovna

Spisovna – slouží pro správu spisoven a evidenci spisů v rámci předarchivní péče. Uložené dokumenty již nevstupují do oběhu, k základním evidenčním údajům jsou přidávány informace o lokaci (místě uložení) a případných výpůjčkách. Modul podporuje rovněž tvorbu skartačních návrhů. [14] [17]



Obr. 4. Integrace ASAS u jednoho organizačního celku

2.2.2 Elektronické dokumenty

V současné době nejsou elektronické dokumenty v ASAS v resortu MO plošně využívány. Pracuje se s pojmy evidenční karta dokumentu/spisu (EKD/EKS), což jsou elektronické záznamy vzniklé registrací/evidencí především listinného dokumentu. U pracoviště KaMO, probíhá proces skenování příchozích dokumentů v listinné podobě

a jejich elektronický obraz ve formátu TIFF je přiřazen k EKD. Základem současné spisové služby je listinný dokument.

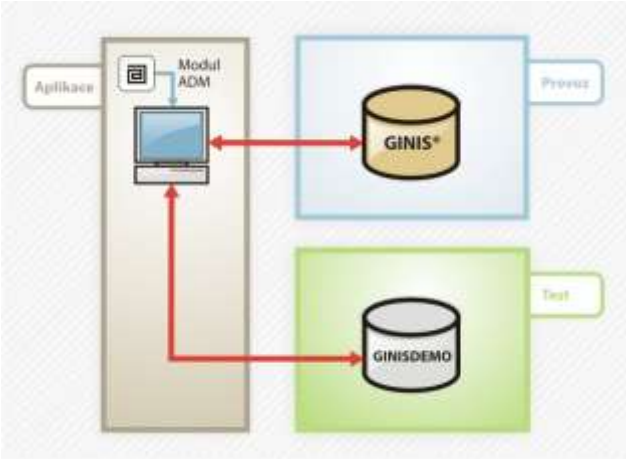
- rozdělení dokumentů není definováno;
- formáty nejsou stanoveny, na pracovišti KaMO, je užíván formát TIFF.

2.2.3 Stávající databázové prostředí ASAS

V současné době se veškerá evidenční data pořízená do systému GINIS–SSL (ASAS) ukládají do společné centrální databáze v prostředí databázového serveru (MS SQL). Existuje jednoduchý databázový model pro sběr ostrých a testovacích dat. Pro sběr ostrých dat slouží jedna samostatná provozní databáze (pod názvem GINIS) a pro sběr testovacích dat slouží samostatná testovací databáze (pod názvem TEST).

Jednotlivé databáze jsou uloženy na samostatném paměťovém svazku připojeného diskového pole. Architektura jedné provozní centrální databáze má za následek pořizování veškerých údajů pouze jednou, pořádek v datech, efektivní vyhledávání a možnost věrohodných přehledů o veškeré činnosti.

Veškeré administrační nastavení (např. změna organizační struktury, změna úrovně oprávnění, nastavení globálních parametrů apod.) se provádí prostřednictvím centrální administrace systému (modul ADM), která je zakomponována v provozní i testovací databázi samostatně. Synchronizace administračních dat a nastavení mezi provozní a testovací databází probíhá manuálně dle požadavku.



Obr. 5. Stávající databázové prostředí systému SSL

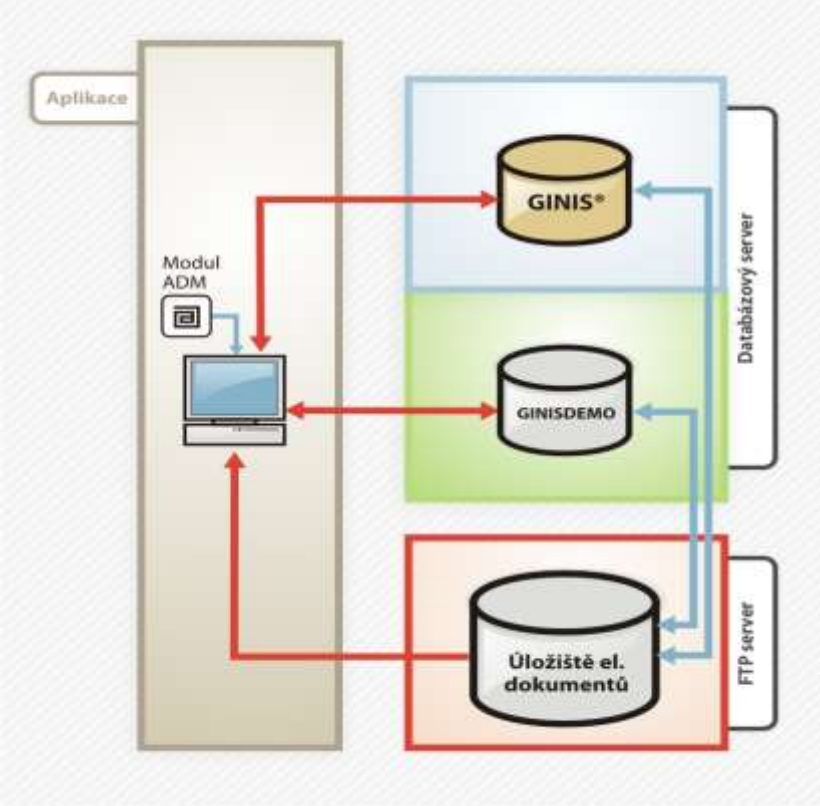
Databázové jádro programového vybavení GINIS® (ASAS) je v provozním prostředí resortu MO provozováno na databázových serverech ŠIS - lokalita MO-VALY.

Databázový stroj: Microsoft SQL Server 2000. [14]

2.2.4 Stávající úložiště pro elektronické dokumenty ASAS

V současné době se veškeré elektronické dokumenty (tj. elektronické obrazy dokumentů a elektronické přílohy) ukládají pomocí aplikační programového vybavení GINIS® (ASAS) – WS ELE01 pro elektronické dokumenty.

Veškeré administrační nastavení (např. definování serverů pro ukládání elektronických dokumentů, definovaní disků pro ukládání elektronických dokumentů, kontrola obsazeného a zároveň volného místa na definovaném úložišti apod.) se provádí prostřednictvím centrální administrace systému (modul ADM), která je zakomponována v provozní i testovací databázi samostatně.



Obr. 6. Stávající databázové prostředí s úložištěm elektronických dokumentů systému SSL

Databázové úložiště a úložiště elektronických dokumentů ASAS je realizováno diskovým polem ŠIS lokality MO-VALY. [14]

2.2.5 Specifikace hardwarové konfigurace systému ASAS

Systém GINIS® (ASAS) vyžaduje pro provoz:

- databázový server (v případě resortu z rodiny MS SQL);
- aplikační server MS IIS pro ASAS services a případný provoz tenkého klienta;
- diskové úložiště odpovídající kapacity.

Pro případ využití terminálového přístupu je dále nutné zabezpečit

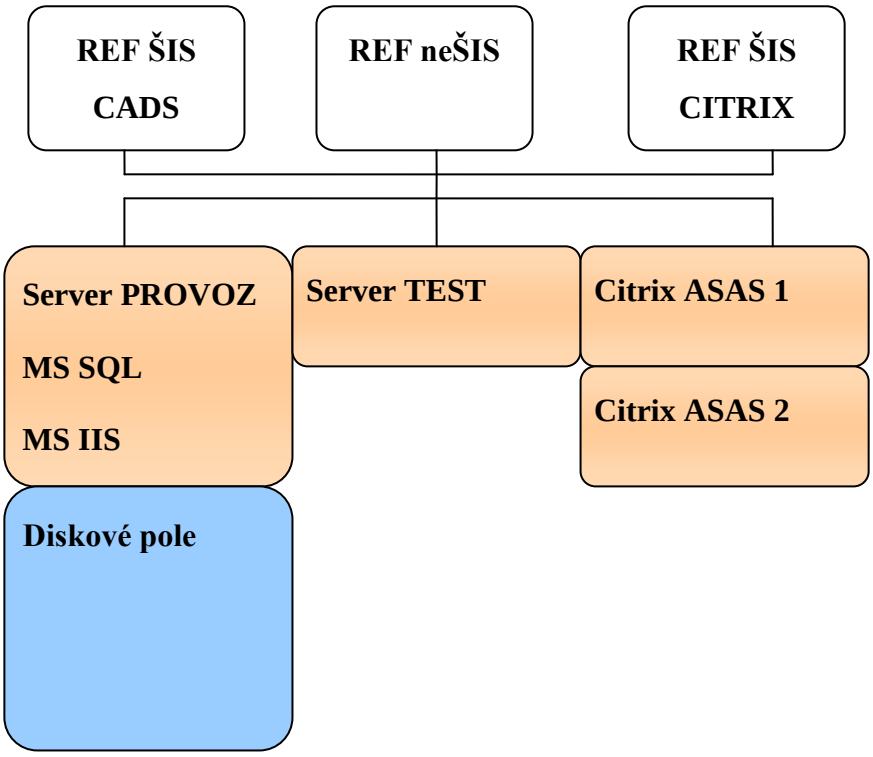
- servery CITRIX v odpovídajícím množství dle počtu uživatelů.

Další požadavky vyplývají z provozu pracoviště pro skenování dokumentů. Pro toto pracoviště je nezbytné vhodné vstupně-výstupní zařízení.

Popis provozního prostředí GINIS® (ASAS): 34.ZKIS - provozní lokalita MO-Valy

1. Provozní prostředí GINIS® - Databázový server (PROVOZ)
   - HP DL380 G5
   - 2/Dual-Core Intel Xeon 5140, 2,33GHz
   - 4x1GB PC2-5300 DDR2, HDD 8 x 146,8 GB
   - LAN #1: HP NC373i Multifunction Gigabit Server Adapter,
   - LAN #2: HP NC373i Multifunction Gigabit Server Adapter
   - OEM Microsoft Windows 2003 Server EN + SP2-R2
   - Microsoft SQL Server 2000 SP4
   - Microsoft IIS 6.0 s podporou ASP.NET 2.0
2. Provozní prostředí GINIS® - Databázový server (TEST)
   - HP DL380 G
   - Dual-Core Intel Xeon 5140, 3,2GHz
   - 3,5GB DDR2, HDD 6 x 72,8 GB
   - LAN #1: HP NC373i Multifunction Gigabit Server Adapter,
   - LAN #2: HP NC373i Multifunction Gigabit Server Adapter
3. Provozní prostředí GINIS® - Terminálový server CITRIX
   - Compaq Proliant DL380 G4
   - 2x Intel Xeon 3.2 GHz,
   - 2GB RAM, 2x72,8 GB 10k-ULTRA320 SCSI,
   - LAN #1: HP NC7782 Gigabit Server Adapter,
   - LAN #2: HP NC7782 Gigabit Server Adapter
   - Microsoft Windows 2000 Server EN + SP4
   - CITRIX MetaFrame 4.0

4. Provozní prostředí GINIS® - Server úložiště elektronických dokumentů
   - (server je provozován na databázovém serveru PROVOZ)
5. Provozní prostředí GINIS® - Server pro provoz testovacích databází
   - (server je provozován na databázovém serveru PROVOZ)
6. Provozní prostředí GINIS® - Diskové pole pro bezpečné uložení dat
   - MSA 1000 14x146 GB
   - (pole je přímo opticky napojeno na databázový server PROVOZ a TEST a terminálový server)
7. Provozní prostředí GINIS® - Systém zálohování
   - HP StorageWorks MSL6000
   - Zálohovací knihovna 6030
   - UPS HP 5500 XR + RM



Obr. 7. Schéma hardwarové konfigurace systému ASAS

2.2.6 Specifikace konfigurace koncových stanic ASAS

V současné době je pro uživatelský přístup k ASAS využíváno pracovních stanic ŠIS, FIS a ISSP. Na pracovních stanicích je provozován buď tlustý klient – klientské APV, nebo Citrix terminál, pro přístup na Citrix farmu, kde je „virtuálně“ provozován tlustý klient – klientské APV. [14] [18] [19] [20]

Pro budoucí použití se předpokládá využití uživatelských stanic s

- tlustým klientem pro pracovní stanice v doméně ŠIS, resp. u takových pracovních stanic, kde je možno nástroji SZP zajistit vzdálenou konfiguraci a aktualizaci software. Další podmínkou pro instalaci tlustého klienta je též dostatečně robustní komunikační kanál;
- terminálovým klientem Citrix pro pracovní stanice mimo doménu ŠIS, resp. mimo dohled nástrojů SZP, případně pro pracovní stanice v doméně ŠIS s nedostatečným komunikačním kanálem pro provoz tlustého klienta.

2.2.7 Záloha a obnova serverové části systému ASAS

Databáze jsou zálohovány podle schématu zálohování ŠIS (po-pá incr, so full). Podobně SystemState serverů (so full). Pro stanovení požadovaných parametrů pro zálohování a obnovu serverové části systému ASAS je nutné stanovit v součinnosti s hlavním uživatelem ASAS následující parametry:

- garantovaná provozní doba;
- garantované úroveň dostupnosti služeb ASAS;
- Recovery Time Objective;
- Recovery Point Objective.

2.2.8 Nastavení plánu bezpečnostní zálohy na datové pásky

Zálohování probíhá podle schématu zálohování ŠIS.

Plán bezpečnosti pro datové pásky ASAS (budou-li využívány) bude nutné nastavit dle požadavků hlavního uživatele. V případě absence přesného zadání doporučuji vycházet z best-practice, zejména u FIS a ISL. [14]

II. PRAKTICKÁ ČÁST

3 ANALÝZA MOŽNOSTÍ INTEGRACE S JINÝMI IS POUŽÍVANÝMI V RÁMCI AČR

Cílem této kapitoly je popsat dopady, ale i požadavky zákona č. 300/2008 Sb. na základní zákonné a metodické požadavky výkonu spisové služby na jednotlivé IS resortu MO, a to zejména v částech:

- Příjem dokumentů

  (§ 1vyhlášky 646/2004 Sb. o podrobnostech výkonu spisové služby).

- Evidence dokumentů

  (§ 2 vyhlášky 646/2004 Sb. o podrobnostech výkonu spisové služby).

- Rozdělování a oběh dokumentů

  (§ 3 vyhlášky 646/2004 Sb. o podrobnostech výkonu spisové služby).

- Vyřizování dokumentů

  (§ 4 vyhlášky 646/2004 Sb. Sb. o podrobnostech výkonu spisové služby).

- Vyhotovování dokumentů

  (§ 5 vyhlášky 646/2004 Sb. Sb. o podrobnostech výkonu spisové služby).

- Podepisování dokumentů a užívání razítek

  (§ 6 vyhlášky 646/2004 Sb., o podrobnostech výkonu spisové služby).

- Odesílání dokumentů

  (§ 7 vyhlášky 646/2004 Sb. o podrobnostech výkonu spisové služby).

- Ukládání dokumentů

  (§ 8 vyhlášky 646/2004 Sb. o podrobnostech výkonu spisové služby).

- Vyřazování dokumentů

  (§ 9 vyhlášky 646/2004 Sb. o podrobnostech výkonu spisové služby).

V úvodní části této analýzy je osvětlena použitá terminologie, která je dále využívána v obsahu této a dalších kapitol. Obsahem druhé části této kapitoly je metodický popis dopadů zákona č. 300/2008 Sb. na výkon metodiky spisové služby úřadu (resortu MO).

V současné době je v legislativním schvalovacím procesu novela vybraných částí zákona č. 300/2008 Sb., která však zásadním způsobem nemění dopady jmenované v tomto dokumentu.

Předpokladem úspěšného vyřešení dopadů zákona č.300/2008 Sb. je zajištění galvanického bezpečného propojení mezi systémem datových schránek a ASAS (sítě internet a intranet).

Tento axiom je podporován nejen zněním zákona č.300/2008 Sb. který hovoří o přímém napojení v § 29, ale nalezneme jej v celém koncepčním záměru e-Governmentu a samozřejmě také v připravovaných novelách souvisejících zákonů (např. aktuálně schvalovaná novela zákona č.300/2008, 499/2004, aj.). [17]

Krom těchto předpokladů hovoří pro tento předpoklad také argumenty technologické a procesní. Vzhledem k předpokládanému vysokému objemu přenášených dokumentů (dle současných kvalifikovaných odhadů až 3000 dokumentů za den) by jejich přenos mezi oddělenými sítěmi na pomocném pracovním médiu byl nejen velmi problematický, ale představoval by i zásadní riziko ztráty či zanedbání se všemi právními důsledky pro organizaci (zejména nedodržení zákonných lhůt od data přijetí datové zprávy adresátem doručení).

Dále během příjmu datových zpráv probíhá několik zásadních kroků, které bez spojení na příslušné autority vůbec nelze realizovat, zejména ověřování stažení a uložení doručené datové zprávy, kontrola elektronického podpisu a časového razítka, v případě odesílání je to především komunikace se systémem DS ohledně existence DS adresáta (činnost vykonává referent organizace – tedy prakticky každý uživatel ASAS) a dále činnosti v souvislosti s výkonem procesu autorizované konverze. Tyto činnosti jsou vykonávány současně na řadě pracovišť ASAS. [14]

V této souvislosti je třeba zmínit také institut schvalovacího procesu a především jeho zásadní část, kterou je elektronické podepisování vyhotovených elektronických dokumentů a jejich následné odeslání do datové schránky adresáta, které bude probíhat opět v celé šíři organizační struktury resortu MO a o jehož vykonání musí být veden jednoznačný záznam v ASAS, jakožto nástroji spisové služby.

Návrh bezpečného interface ISDS na ASAS je řešen Ř ARI ve spolupráci s SKIS MO a PPÚZ. Výchozím předpokladem je použití technologií s dosaženým stupněm

certifikace EAL 4, tj. technologie navržené, testované a hodnocené metodicky s ohledem na maximální zajištění bezpečnosti. Pro propojení ASAS s certifikační autoritou a ISDS budou dle návrhu použity buď pronajaté okruhy, nebo spojení prostřednictvím Internetu. Omezujícím východiskem je definice provozního prostředí CADS, která je uvedena v certifikačních zprávách ISL a FIS.

Návrh řešení předpokládá distribuci přijatých a vypravovaných elektronických datových zpráv výhradně prostředky ASAS od / do útvarů ve stávající KIS ŠIS, ve které je systém ASAS rutinně provozován. Po definování přístupových pravidel mohou s ASAS pracovat také uživatelé jiných domén v rámci MO (dnes např. FIS). [14] [18]

3.1 Terminologie

Datová schránka (§ 17 odstavce 7 zákona č. 300/2008 Sb.)

Datová schránka je elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci. Datové schránky zřizuje a spravuje Ministerstvo vnitra. [9] [17]

- Datová schránka fyzické osoby je datová schránka zřízená ministerstvem, a to na základě žádosti fyzické osoby, která je plně způsobilá k právním úkonům.
- Datová schránka podnikající fyzické osoby je datová schránka zřízená ministerstvem, a to na základě žádosti podnikající fyzické osoby. Datová schránka podnikající fyzické osoby bude zřízena ministerstvem bezplatně advokátu, daňovému poradci a insolvenčnímu správci bezodkladně poté, co obdrží informaci o jejich zapsání do zákonem stanovené evidence.
- Datová schránka právnické osoby je datová schránka zřízená ministerstvem bezplatně právnické osobě zřízené zákonem, právnické osobě zapsané v obchodním rejstříku a organizační složce podniku zahraniční právnické osoby zapsané v obchodním rejstříku, a to v případě právnické osoby zřízené zákonem bezodkladně po jejím vzniku, v případě právnické osoby zapsané v obchodním rejstříku a organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku bezodkladně poté, co obdrží informaci o jejím zapsání do obchodního rejstříku. Právnické osobě, která

není uvedena v předchozím popisu, zřídí ministerstvo datovou schránku právnické osoby bezplatně na žádost této osoby

- Datová schránka orgánu veřejné moci je ta datová schránka, která byla zřízena ministerstvem bezodkladně po vzniku orgánu veřejné moci, v případě notářů a soudních exekutorů bezodkladně poté, co obdrželo informaci o jejich zapsání do zákonem stanovené evidence.

Doručení datové zprávy (§ 17 odstavec 3 a 4 zákona č. 300/2008 Sb.)

Doručení datové zprávy nastává dvěma možnými způsoby:

- Doručení nastane v okamžiku, kdy se do datové schránky přihlásí osoba oprávněná k přístupu do datové schránky.
- Nepřihlásí-li se do datové schránky osoba oprávněná k přístupu do datové schránky ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty.

Konverze (§ 22 odstavec 1. zákona č. 300/2008 Sb.)

- Úplné převedení dokumentu z analogové podoby do digitální podoby, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.
- Úplné převedení dokumentu z digitální podoby do podoby analogové, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.

Technické náležitosti provádění konverze, vstupu a výstupu stanoví Ministerstvo vnitra vyhláškou. Osoby oprávněné k přístupu do datové schránky orgánu veřejné moci

K přístupu do datové schránky orgánu veřejné moci je oprávněn vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena, případně fyzická osoba určená vedoucím orgánu veřejné moci, pro který byla datová schránka zřízena, a to v rozsahu jím stanoveném. [9] [11] [17]

3.2 Příjem dokumentů

§ 2 odstavce 1 zákona č. 300/2008 Sb. definuje pojem *datová schránka následně* ***„Datová schránka je elektronické úložiště, které je určeno k***

a) doručování orgány veřejné moci,

b) provádění úkonů vůči orgánům veřejné moci.“

Příjem elektronických dokumentů prostřednictvím datové schránky je v zásadě možný dvěma základními způsoby.

Prvním způsobem je využití standardního aplikačního programového vybavení, tj. přístup k datové schránce prostřednictvím aplikace informačního systému datových schránek. Příjem podání v tomto případě bude zřejmě probíhat následujícím způsobem. ***„Osoba oprávněná k přístupu do datové schránky se do ní přihlašuje prostřednictvím přístupových údajů“*** (§ 9 odstavec 1 zákona č. 300/2008 Sb.). Po autorizaci a přihlášení do systému datových schránek oprávněná osoba „vyzvedne“ datové zprávy a uloží do vlastního chráněného úložiště elektronických dokumentů. Tento postup je použitelný pro menší a malé původce, nebo v případě nutnosti zabezpečit „náhradní provoz“, tj. zejména v případech výpadku aplikačního programového interface (dále též API), informačního systému datových schránek (dále též ISDS) či výpadku systému elektronické spisové služby MO (dále též ASAS). S ohledem na denní množství přijímaných datových zpráv je tento způsob příjmu pro rutinní potřebu Ministerstva obrany naprosto nevhodný.

Druhým, daleko efektivnějším způsobem přístupu do datové schránky je využití API ISDS. I při tomto způsobu přístupu k datové schránce platí požadavek § 9 odstavce 1 zákona č. 300/2008 Sb. Příjem podání v tomto případě bude probíhat následujícím způsobem: [3] [9]

- Osoba oprávněná k přístupu do datové schránky se přihlásí do příslušné části systému elektronické spisové služby (ASAS).
- Osoba oprávněná k přístupu do datové schránky musí mít nastaven přístup do příslušné části (modulu) systému elektronické spisové služby umožňující komunikaci se systémem datových schránek (modul POD rozšířený o funkcionalitu ePOD-DS).

- Po přihlášení systém ASAS kontroluje, zda je u této osoby nastaven příznak, že je oprávněnou osobou k přístupu do datové schránky orgánu veřejné moci, viz § 8 odstavce 4 zákona č. 300/2008 Sb., případně § 8 odstavce 6 písmeno c) zákona č. 300/2008 Sb.
- ***„K přístupu do datové schránky orgánu veřejné moci je oprávněn vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena.“*** (§ 8 odstavce 4 zákona č. 300/2008 Sb.)
- Osobou oprávněnou k přístupu do datové schránky orgánu veřejné moci je fyzická osoba určená vedoucím orgánu veřejné moci, pro který byla datová schránka zřízena, a to v rozsahu jím stanoveném (§ 8 odstavce 6 písmeno c) zákona č. 300/2008 Sb.).

Informace o datové schránce orgánu veřejné moci jsou dostupné v informačním systému datových schránek v souladu s § 14 odstavce 3 písmeno i) zákona č. 300/2008 Sb.

“V informačním systému datových schránek se vedou tyto informace o datových schránkách: název orgánu veřejné moci, pro nějž byla zřízena datová schránka, sídlo a identifikační číslo ekonomického subjektu, bylo-li přiděleno,“ Lze předpokládat, že tyto údaje budou dostupné prostřednictvím aplikačního programového vybavení informačního systému datových schránek, a to pouze jednotlivě na konkrétní dotaz, tj. nebude možné získat ucelený seznam všech subjektů, které mají DS vytvořenu viz odpověď na otázku ***„Bude existovat něco jak „telefonní“ seznam datových schránek?“*** Odpověď: ***Nebude existovat žádný oficiální seznam datových schránek, do kterého by bylo možné se podívat a zjistit, kdo má a kdo nemá datovou schránku. Informační systém datových schránek bude fungovat opačně, bude možné se „zeptat“, zda příslušná osoba má datovou schránku. Pokud ano, bude možné do ní zprávu odeslat. Důvodem pro tuto formu je ochrana dat a především skutečnost, že seznam schránek se může měnit.***

Speciálně fyzické osoby si mohou schránky zřizovat, ale i rušit. To, že jsme někomu odesílali do jeho datové schránky elektronickou zprávu před týdnem, neznamená automaticky, že tuto schránku ještě dnes vlastní. Proto je nutné pokaždé učinit dotaz, který vrátí odezvu s aktuálním stavem. [17]

Zdroj: http://www.egovernment.cz/schranky/otazky/5.htm

- Osoba oprávněná k přístupu do datové schránky provede spuštění příslušné aplikace ePOD-DS a s využitím API ISDS se autorizuje do informačního systému datových schránek. Pomocí API ISDS následně „vyzvedne“ obsah datové schránky (četnost případně časy přístupů do ISDS by měly být ve Spisovém a skartačním řádu MO určeny).
- Spisový a skartační řád dané organizace musí stanovit organizační, technické podmínky a bezpečnostní zásady přístupu do datové schránky. Podmínky v budoucnu stanoví prováděcí vyhláška Ministerstva vnitra. Podle § 9 odstavce 3 zákona č. 300/2000 Sb. Ministerstvo stanoví vyhláškou technické podmínky a bezpečnostní zásady přístupu do datové schránky.
- Přihlášení osoby oprávněné k přístupu do datové schránky je realizováno prostřednictvím přístupových údajů nebo elektronických prostředků, které vydává Ministerstvo vnitra. Podrobnosti jsou popsány v § 9 odstavce 3 zákona č. 300/2008 Sb.: ***„Přihlášení podle odstavce 1 zajišťuje ministerstvo prostřednictvím jím vydaných přístupových údajů nebo elektronických prostředků anebo prostřednictvím elektronických prostředků třetích osob. Náležitosti přístupových údajů a elektronické prostředky k přihlášení stanoví ministerstvo vyhláškou. Ustanovení o přístupových údajích se použijí obdobně i pro elektronické prostředky podle věty první.“***
- Informace o přihlášení osoby oprávněné k přístupu do datové schránky jsou uchovány v ISDS viz § 14 odstavce 3 písmeno c) zákona č. 300/2008 Sb.: ***„V informačním systému datových schránek se vedou tyto informace o datových schránkách: datum přihlášení osoby oprávněné k přístupu do datové schránky do této datové schránky s uvedením hodiny, minuty a sekundy a údaj identifikující tuto osobu“***. Uvedené informace budou dostupné pouze prostřednictvím aplikačního programového vybavení informačního systému datových schránek.
- Osoba oprávněná k přístupu do datové schránky provede pomocí aplikace ePOD-DS (přes API ISDS) potvrzení „úspěšné vyzvednutí“ datových zpráv.

Informační systém datových schránek vyrozumí adresáta o dodání datové zprávy do jeho datové schránky – dle podrobností uvedených v § 20 odstavce 1 písmeno d) zákona č. 300/2008 Sb.: ***„Ministerstvo vyrozumí adresáta o dodání datové zprávy do jeho datové schránky na jím zvolenou elektronickou adresu nebo jiný technický prostředek pro vyrozumění; adresát je v tomto případě povinen uhradit náklady, které ministerstvu v souvislosti s vyrozuměním vznikly, s výjimkou, bylo-li vyrozumění učiněno na adresátem zvolenou elektronickou adresu“***. S ohledem na velké denní množství přijímaných emailových zpráv bude vhodné nastavit zvolenou emailovou schránku tak, aby bylo možné dohledat 5 dní staré doručené e-maily. Na uvedené schránce je vhodné realizovat kontrolní činnost například pomocí SW služby, SW komponenty či mechanismu nastavení schránky. Cílem kontroly je včas avizovat chybové stavy například „za posledních 48 hodin nebyla doručena žádná datová zpráva“. [14] [17]

3.3 Doručení, Registrace a Evidence dokumentu

Doručení datové zprávy – § 17 odstavec 3 a 4 zákona č. 300/2008 Sb. definuje okamžik doručení dvěma možnými způsoby:

- ***„Dokument, který byl dodán do datové schránky, je doručen okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu“*** (§ 17 odstavec 3 zákona č. 300/2008 Sb.).
- ***„Nepřihlásí-li se do datové schránky osoba podle odstavce 3 ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty; to neplatí, vylučuje-li jiný právní předpis náhradní doručení“*** (§ 17 odstavec 4 zákona č. 300/2008 Sb.).

Přičemž podstatné je uvedeno i v odstavci 6 téhož paragrafu: ***„Doručení dokumentu podle odstavce 3 nebo 4 má stejné právní účinky jako doručení do vlastních rukou.“***

Na jednání pracovní skupiny, které se uskutečnilo v budově Ministerstva vnitra (nám. Hrdinů 1634/3, Praha 4), bylo ze strany MV (Členové pracovní skupiny: MV: Mgr.

Zdeněk Zajíček, Ing. Jindřich Kolář, JUDr. Václav Henych, Ing. Oskar Macek) deklarováno následující: [4] [14]

- Systém datových schránek nebude žádným způsobem podporovat vnitřní adresování dokumentů uvnitř – v rámci jednotlivých organizací. Systém datových schránek pouze dopraví dokument do organizace, co se děje dále ISDS neřeší.
- Pro prokazatelnost autentičnosti a neporušenosti odeslané zprávy dodá systém datových schránek své nástroje. Není věcí spisových služeb prokazovat původnost zpráv.
- Interface nebude podporovat a standardizovat podporu šifrování na straně odesilatele a tím pádem ani na straně příjemce. Zprávy budou šifrovány pouze interně uvnitř systému datových schránek. Toto šifrování však navenek nebude vůbec patrné. Podle vyjádření MV ČR si odesilatel může tělo zprávy zašifrovat, ale pouze pokud učiní individuální dohodu s příjemcem, který takto šifrovanou zprávu bude ochoten akceptovat.
- Datové zprávy budou omezeny určitou zadanou maximální velikostí.

Důležité je také ustanovení § 20 odstavce 3 zákona č. 300/2008 Sb. věta druhá: ***„Ministerstvo zveřejní přípustné formáty datových zpráv a seznam možných technických prostředků pro vyrozumění o dodání datové zprávy do datové schránky v provozní dokumentaci informačního systému datových schránek“***. Ministerstvem vnitra byl zveřejněn „Draft Provozního řádu ISDS“ ve kterém je uvedeno „Obsahem zprávy může být jedna či více příloh v libovolném počítačovém formátu, s výjimkou spustitelných souborů jako je např. exe a komprimovaných souborů typu zip, arc, arj, cab, rar, tar, sfx, lha, lzh, hqx, btoa, bz2, tbz, cpt, tgz, bin, sit, sitx, taz, ync.“

Dokud Ministerstvo vnitra oficiálně nezveřejní přípustné formáty je možné vývoj věcí budoucích pouze předpokládat a vycházet i z dalších veřejných informací například z odpovědi na otázku ***„V jakých formátech bude možné s datovou zprávou posílat přílohy?“*** Odpověď: ***„ Přesně bude formáty stanovovat prováděcí vyhláška, která nyní prochází tzv. vnitroresortním připomínkovým řízením. S největší pravděpodobností by se ale mělo jednat o formáty PDF, TIF a PNG.“***

Zdroj: http://www.egovernment.cz/schranky/otazky/8.htm

Je tedy logické a možné, že Ministerstvo vnitra zveřejní přípustné formáty v souladu s usnesením vlády České republiky ze dne 3. listopadu 2008 č. 1338. Dle tohoto usnesení jsou schváleny jako výstupní datové formáty statických dokumentů v digitální podobě ze systémů elektronických spisových služeb následující formáty: [14] [17]

- formát PDF/A-1a (ISO 19005-1 – Portable Document Format – Electronic document file format for long-term preservation) pro statické textové, obrazové a kombinované dokumenty v digitální podobě,
- formáty PNG (ISO/IEC 15948:2004 – Portable Network Graphics) pro statické obrazové dokumenty v digitální podobě;
- TIFF (Tagged Image File Format – revize 6 – nekomprimovaný) pro statické obrazové dokumenty v digitální podobě.

Registrace dokumentů

Registrací je chápáno prvotní zapsání informací o doručeném dokumentu, tj. metadat, o elektronickém dokumentu a o uložení elektronického dokumentu do chráněného úložiště. Při příjmu datové zprávy by tedy měla být uložena celá datová zpráva, ze které bude při registraci využit elektronický dokument a popisná data dokumentu (rozsah těchto popisných dat by měl být součástí API informačního systému datových schránek. Doručená datová zpráva se ukládá včetně připojeného kvalifikovaného časového razítka. Po registraci je tedy možno vyhledat dokument podle identifikačních údajů, kterými jsou například identifikace datové zprávy, datum odeslání atp.

Registrovat bude nutné všechny doručené datové zprávy bez ohledu na agendovou příslušnost (věcný obsah) doručeného dokumentu.

Podle ustanovení § 29 odstavec 1 zákona č. 300/2008 Sb.: ***„Vedou-li orgány veřejné moci spisovou službu elektronicky, činí tak způsobem umožňujícím doručování dokumentů a provádění úkonů prostřednictvím datové schránky, ledaže je z bezpečnostních důvodů nezbytné vést spisovou službu odděleně“*** a s ohledem na skutečnost, že Ministerstvo obrany vede spisovou službu elektronicky, musí být

zajištěna vazba ASAS na informační systém datových schránek pomocí vydefinovaného API ISDS rozhranní.

Podle ustanovení § 29 odstavec 2 zákona č. 300/2008 Sb.: ***„Zřizují-li orgány veřejné moci elektronickou podatelnu, elektronická podatelna umožňuje doručování dokumentů a provádění úkonů prostřednictvím datové schránky.“***

S ohledem na skutečnost, že Ministerstvo obrany tuto povinnost zřídit a provozovat (podle § 1 nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů) elektronickou podatelnu má, je doporučeno doručování realizovat prostřednictvím elektronické podatelny ASAS MO. [1] [9]

Registrace dokumentů tímto bude realizována vždy nástroji elektronické spisové služby ASAS MO.

Evidence dokumentů

Problematiku evidence dokumentů (ať již elektronických, nebo listinných) řeší § 2 vyhlášky 646/2004 Sb., o podrobnostech výkonu spisové služby. Vyhláška v tomto paragrafu definuje, kam a v jakém rozsahu se evidence dokumentu provádí:

- Dokumenty doručené a dokumenty vzniklé z vlastní činnosti MO se evidují v podacím deníku vedeném prostředky elektronické spisové služby ASAS. Vyřízení doručeného dokumentu se vloží do stejného spisu spolu s podáním (dokumentem do organizace doručeným). Spis je veden pod číslem jednacím.
- Dokumenty podléhající samostatné evidenci jsou evidovány mimo ASAS ručně, tj. jsou součástí ručně vedených agendových knih. Výčet těchto druhů dokumentů podléhajících samostatné evidenci by měl být uveden ve Spisovém a skartačním řádu MO.
- Dokumenty se evidují v podacím deníku v číselném pořadí, v němž byly určeným původcem evidovány.

Doručený elektronický dokument, který byl zaregistrován do systému elektronické spisové služby, může být tedy zaevidován do podacího deníku. Pokud elektronický

dokument svou povahou a obsaženými informacemi patří do specializované agendy (podle samostatného právního předpisu) musí být evidován v agendové knize, např. pokud bude Ministerstvo obrany doručena datovou schránkou faktura, bude elektronickou podatelnou přijata a zaregistrována.

Tyto dokumenty musí pomocí API ASAS přejít do evidence dané agendy. V této agendě musí dojít ke zpracování a „agendovému vyřízení" elektronického dokumentu. Požadavky na odeslání, uložení do spisovny a předání na jiný útvar resortu MO jsou prostřednictvím API ASAS MO vyřizovány v systému ASAS. U již zmíněné faktury musí dojít k převzetí do „EKO agendy" a dojde ze zákona k evidenci do knihy došlých faktur.

Dokumenty vedené mimo ASAS se musí vést v centrálním podacím deníku tak, aby bylo možné je vyřizovat elektronicky. V opačném případě se musí dořešit způsob autorizované konverze nejprve z digitální podoby a po vyřízení z analogové do digitální podoby tak, aby bylo možné vytvořit datovou zprávu a zabezpečit její odeslání. Řešení musí zohlednit i požadavky § 24 odstavec 5 zákona č. 300/2008 Sb., kde je uveden výčet situací, kdy se autorizovaná konverze neprovádí. [4] [14]

3.4 Rozdělení a oběh dokumentů

Oběh dokumentů je sledován v systému ASAS MO. Při oběhu dokumentu je zajištěno a zabezpečeno předávání a přebírání dokumentu. Při oběhu dokumentu je zaručena průkaznost předávání a přebírání zachycující jmenovitě a časově veškerou manipulaci s dokumentem.

Oběh elektronického dokumentu s ohledem na skutečnost, že nemá fyzickou podobu, musí být o to pečlivější a je vhodné jej podpořit „avizací" systémovou či mailovou. Právě tato skutečnost bude nejčastějším důvodem problémů s řádným a včasným vyřizováním dokumentů.

Zaregistrované, případně zaevidované dokumenty se předávají k vyřízení příslušné organizační jednotce (odboru, oddělení), případně zaměstnanci určenému k vyřízení.

Rozdělování doručených a registrovaných dokumentů provádí podatelna podle ustanovení Spisového a skartačního řádu MO.

Pokud bude z organizačních, technických, metodických či jiných důvodů nezbytné zabezpečit autorizovanou konverzi dokumentu do listinné podoby, pak se to musí dít

v souladu s podmínkami uvedenými § 24, § 25 a § 26 zákona č. 300/2008 Sb., jinak řečeno postup při konverzi musí být plně v souladu s požadavky § 24, § 25 a § 26 zákona č. 300/2008 Sb.: [6] [14]

- Při konverzi do dokumentu v listinné podobě pracovník provádějící konverzi
  - „ověří platnost kvalifikovaného časového razítka“,
  - „ověří, že je kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb“,
  - „ověří platnost zaručeného elektronického podpisu“,
  - „ihned po provedení konverze ověří shodu výstupu se vstupem“,
  - „po ověření shody připojí k výstupu ověřovací doložku“.
- Konverzi pracovník neprovede v případě, že:
  - „je požadována konverze dokumentu, který je již výstupem konverze“,
  - „nebylo-li k dokumentu obsažené v datové zprávě připojeno kvalifikované časové razítko“,
  - „nebyl dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil“,
  - „byl dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem oprávněné osoby nebo označen uznávanou elektronickou značkou toho, kdo příslušnou datovou zprávu vydal nebo vytvořil, a nebyla-li shledána shoda tohoto dokumentu s výstupem“,
  - „jde o dokument, který nelze konvertovat do listinné podoby, například zvukový nebo audiovizuální záznam“,
  - „pokud dokument obsažený v datové zprávě nesplňuje technické náležitosti“.

- Ověřovací doložka konverze dokumentu do v listinné podoby je součástí výstupu a obsahuje:
  - „název subjektu, který konverzi provedl“,
  - „pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí“,
  - „údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu“,
  - „údaj o tom, z kolika listů se skládá výstup“,
  - „datum vyhotovení ověřovací doložky“,
  - „údaj o tom, zda byl vstup podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou, číslo kvalifikovaného certifikátu, na němž je uznávaný elektronický podpis založen, nebo číslo kvalifikovaného systémového certifikátu, na němž je uznávaná elektronická značka založena, a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydal“,
  - „datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal“,
  - „otisk úředního razítka, jméno, popřípadě jména, příjmení a podpis osoby, která konverzi provedla“.
- Pracovník provádějící konverzi vede evidenci provedených konverzí. Evidenční záznamy jsou minimálně v následujícím rozsahu
  - „pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí“,
  - „datum provedení konverze“,
  - „konkrétní označení vstupu a datum jeho sepsání, je-li datum ve vstupu obsaženo“.

Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy.

3.5 Vyřizování dokumentů

Dokument vyřizuje určený zaměstnanec, tzv. zpracovatel. Zpracovatel vyřizuje podání v systému ASAS. Údaje do podacího deníku jsou zaznamenány automaticky během vyřízení, které zadává příslušná zodpovědná osoba a to zejména, jak byl dokument vyřízen, kdy a komu bylo odesláno vyřízení dokumentu.

Všechny dokumenty týkající se téže věci se spojují ve spis. Spis musí obsahovat soupis všech dokumentů, jež jsou jeho součástí. Návaznost připojovaných dokumentů se projeví v podacím deníku.

Součástí vyřízeného spisu je vždy vyřizující dokument v analogové, nebo digitální podobě. Pokud je vyřízení dokumentu v digitální podobě, musí být tento elektronický dokument uložen v chráněném úložišti elektronických dokumentů systému ASAS.

Zpracovatel, který dokument vyřídil, jej označí spisovým znakem, skartačním znakem a skartační lhůtou v souladu s požadavky a podmínkami stanovenými ve Spisovém a skartačním řádu MO. [11] [16]

V případě, že vyřízení dokumentu bylo vyhotoveno v listinné podobě a má li dojít k odeslání prostřednictvím informačního systému datových schránek, musí toto listinné vyhotovení být autorizovaně konverzováno do digitální podoby.

V případě, že vyřízení dokumentu bylo vyhotoveno v jiném než schváleném formátu (usnesení vlády České republiky ze dne 3. listopadu 2008 č. 1338), musí dojít k neautorizované konverzi z původního neschváleného formátu do jednoho ze schválených formátů například PDF/A-1a (ISO 19005–1), PNG (ISO/IEC 15948:2004), TIFF (Tagged Image File Format – revize 6 – nekomprimovaný).

3.6 Vyhotovování dokumentů, podepisování dokumentů a užívání razítek

Podoba při vyhotovování dokumentů bude dána způsobem odeslání, tj. pokud dokument bude (podle ustanovení zákona č. 300/2008 Sb.) odesílán prostřednictvím

informačního systému datových schránek, bude prvoplánově vyhotovován v digitální podobě. Pokud z organizačních, technických či jiných důvodů bude dokument vyhotovován v analogové podobě, musí být autorizovaně konvertován do podoby digitální.

Postup při konverzi musí být plně v souladu s požadavky §24, §25 a §26 zákona č. 300/2008 Sb.:

- Při konverzi listinného dokumentu do dokumentu obsaženého v datové zprávě opatří subjekt, který konverzi provedl, výstup svou uznávanou elektronickou značkou nebo uznávaným elektronickým podpisem osoby, která konverzi provedla, a zajistí, aby byl výstup opatřen kvalifikovaným časovým razítkem.
- Konverzi pracovník neprovede v případě, že:
  - je dokument v jiné než v listinné podobě či v podobě datové zprávy,
  - jde o dokument v listinné podobě, jehož jedinečnost nelze konverzí nahradit, zejména se jedná o občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los, sázenku, geometrický plán, rysy a technické kresby,
  - jsou-li v dokumentu v listinné podobě změny, doplňky, vsuvky nebo škrty, které by mohly zeslabit jeho věrohodnost,
  - není-li z dokumentu v listinné podobě patrné, zda se jedná o prvopis, vidimovaný dokument, opis nebo kopii pořízenou ze spisu, nebo stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle jiného právního předpisu,
  - je-li dokument v listinné podobě opatřen plastickým textem nebo otiskem plastického razítka.
- Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě je součástí výstupu a obsahuje:

- název subjektu, který konverzi provedl,
- pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,
- údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,
- údaj o tom, z kolika listů se skládá vstup,
- údaj o tom, zda vstup obsahuje vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky variabilní prvek nebo jiný zajišťovací prvek,
- datum vyhotovení ověřovací doložky,
- jméno, případně jména, a příjmení osoby, která konverzi provedla.

- Pracovník provádějící konverzi vede evidenci provedených konverzí. Evidenční záznamy jsou minimálně v následujícím rozsahu:
  - pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,
  - datum provedení konverze,
  - konkrétní označení vstupu a datum jeho sepsání, je-li datum ve vstupu obsaženo

Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy.

Za povšimnutí dále stojí i znění § 22 odstavec 3 zákona č. 300/2008 Sb.: ***„Má-li být podle jiného právního předpisu předložen dokument v listinné podobě správnímu orgánu, nebo soudu anebo jinému státnímu orgánu, zejména aby byl užit jako podklad pro vydání rozhodnutí, je tato povinnost splněna předložením jeho výstupu.“*** [9] [21]

3.7 Odesílání dokumentů

Zadat údaje o odeslání, včetně určení způsobu odeslání a druhu zacházení je plně v kompetenci zpracovatele spisu (odborného referenta). Zpracovatel je právě osoba odpovědná a kompetentní posoudit ustanovení § 17 odstavce 1 zákona č. 300/2008 Sb., ve kterém se uvádí: „Umožňuje-li to povaha dokumentu, orgán veřejné moci jej doručuje

jinému orgánu veřejné moci prostřednictvím datové schránky, pokud se nedoručuje na místě. Umožňuje-li to povaha dokumentu a má-li fyzická osoba, podnikající fyzická osoba nebo právnická osoba zpřístupněnu svou datovou schránku, orgán veřejné moci doručuje dokument této osobě prostřednictvím datové schránky, pokud se nedoručuje veřejnou vyhláškou nebo na místě. Doručuje-li se způsobem podle tohoto zákona, ustanovení jiných právních předpisů upravující způsob doručení se nepoužijí.“ Na § 17 odstavce 1 zákona č.300/2008 Sb. se odkazuje i v odstavci 2 téhož paragrafu: „Připouštějí-li jiné právní předpisy doručování prostřednictvím datových schránek, pořadí způsobů doručování stanovené těmito právními předpisy zůstává ustanovením odstavce 1 nedotčeno“. [9] [16]

Požadované vlastnosti systému ASAS:

- Zpracovatel při odesílání předpokládá, že všechny právnické osoby a orgány veřejné moci mají DS zřízenu a „umožňuje-li to povaha dokumentu“ zadá zpracovatel požadavek na odeslání před ISDS. Údaje o odeslání zadává příslušný zpracovatel. Systém ASAS by měl uživateli při odeslání poskytnout informaci o tom, zda daný subjekt (fyzická osoba, podnikající fyzická osoba nebo právnická osoba) má zpřístupněnu svou datovou schránku.
- Přes definované API ISDS by mělo docházet k aktualizaci informací o tom, zda subjekt má zřízenou datovou schránku, kontaktní adresa, identifikátor datové schránky a další veřejné informace, které ze zákona mohou být systémem datových schránek poskytnuty.
- Systém ASAS by měl být upraven v částech informujících o stavu odeslání, vypravení a doručení. Zejména s ohledem na následující ustanovení zákona:
    - Systém ASAS by měl odesílat elektronické dokumenty formou datové zprávy a to na základě ustanovení § 19 odstavce 1 zákona č. 300/2008 Sb.: „Dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky a úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky mají formu datové zprávy.“ S ohledem na ustanovení § 29 odstavec 1 zákona č. 300/2008 Sb.: ***„Vedou-li orgány veřejné moci spisovou službu***

elektronicky, činí tak způsobem umožňujícím doručování dokumentů a provádění úkonů prostřednictvím datové schránky, …“

- § 20 odstavec 1 písmeno c) zákona č. 300/2008 Sb.: ***„Ministerstvo oznámí odesílateli, že datová zpráva, kterou odeslal, byla dodána do datové schránky adresáta, a toto oznámení označí elektronickou značkou ministerstva založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaná elektronická značka“)“***: Tento údaj je v ASAS uveden jako stav doručeno s datem doručení, resp. datem uložení.
- § 20 odstavec 1 písmeno f) zákona č. 300/2008 Sb.: ***„Ministerstvo oznámí odesílateli, že datová schránka, do které odeslal datovou zprávu, neexistuje“***. Tento údaj je v ASAS uveden jako stav nedoručeno s informací (důvodem) vráceno-adresát neznámý.
- § 20 odstavec 1 písmeno g) zákona č. 300/2008 Sb.: ***„Ministerstvo oznámí odesílateli, že datová schránka, do které odeslal datovou zprávu, je znepřístupněna, a to i zpětně"***. Tento údaj je v ASAS uveden jako stav nedoručeno s informací Vráceno-nepřijato.
- § 20 odstavec 1 písmeno h) zákona č. 300/2008 Sb.: ***„Ministerstvo oznámí odesílateli, že datová schránka, do které odeslal datovou zprávu, byla zrušena“.*** Tento údaj je v ASAS uveden jako stav nedoručeno s informací (důvodem) vráceno-jiný důvod.
- § 20 odstavec 2 zákona č. 300/2008 Sb.: ***„Ministerstvo je oprávněno datovou zprávu zničit, pokud u ní zjistí výskyt chybného formátu nebo počítačového programu, které jsou způsobilé přivodit škodu na informačním systému datových schránek nebo na informacích v tomto informačním systému. O zničení datové zprávy ministerstvo neprodleně vyrozumí odesílatele.“*** Tento údaj je v ASAS uveden jako stav nedoručeno s informací (důvodem) stornováno. Na posledním jednání pracovní skupiny MV

se skupinou sedmi dodavatelů spisových služeb bylo sděleno, že uvedené ustanovení není povinností, ale možností. ISDA nebude v žádném případě analyzovat obsah DS a to ani výskyt škodlivého kódu, datový typ souboru obsažený v DS atp.

- V § 20 odstavci 1 písmenu a) zákona č. 300/2008 Sb. je uvedeno: ***„Ministerstvo zajistí připojení kvalifikovaného časového razítka k datové zprávě odeslané z datové schránky“***. A v písmenu i) téhož odstavce je popsáno, jaké informace systém datových schránek uchovává: ***„Ministerstvo vede evidenci o datu a času událostí podle tohoto odstavce včetně identifikace datové zprávy, odesílatele a adresáta“.*** V § 20 ani jiné části zákona není uvedeno, jakým způsobem ministerstvo zasílá oznámení uvedená v předchozím odstavci. Uvedené nejasnosti mají být upřesněny podle § 20 odstavce 3 zákona č. 300/2008 Sb., kde je ve větě druhé uvedeno: ***„Ministerstvo zveřejní……seznam možných technických prostředků pro vyrozumění o dodání datové zprávy do datové schránky v provozní dokumentaci …“.***
- Osobě zodpovědné za vyřízení (zpracovateli daného spisu) by měla být dostupná informace o tom, že jím odeslaný dokument nebyl doručen. Po obdržení či zjištění této skutečnosti je osoba zodpovědné za vyřízení povinna zajistit odeslání dokumentu jiným způsobem. Tuto požadovanou informaci může uživatel získat aktivním dotazem do systému ASAS nebo systém poskytne informaci aktivně formou avíza.
- Opětovně je nutné upozornit na velmi podstatné ustanovení § 20 odstavce 3 zákona č. 300/2008 Sb. věta druhá: ***„Ministerstvo zveřejní přípustné formáty datových zpráv, seznam možných technických prostředků pro vyrozumění o dodání datové zprávy do datové schránky v provozní dokumentaci informačního systému datových schránek.“*** S ohledem na neexistenci této prováděcí vyhlášky lze požadavky a návrh pouze předpokládat případně odvodit. Popis v následujících odrážkách je tedy odhadem věcí možných:

- Zástupci MV na předchozích veřejných setkáních konstatovali, že ISDS nebude zasahovat ani kontrolovat obsah datové zprávy. Z uvedeného lze odvodit, že Ministerstvo vnitra (ISDS) nebude oznamovat odesílateli, že datová zpráva není v přípustném formátu a že jako takovou ji tedy není možné doručit zadanému adresátovi. Uvedenou skutečnost bude ověřovat až adresát, který datovou zprávu příjme a bude ji vyřizovat. Ve stanovisku MV k Interpretaci ustanovení § 17 odst. 1 a § 17 odst. 7 zákona č. 300/2008 Sb. je konstatováno: ***„Co se týče formy dokumentu, s výhradou doručování dokumentů na místě, by měly být datovými schránkami doručovány všechny dokumenty orgánů veřejné moci, s nimiž je informační systém datových schránek schopen pracovat. Takovéto dokumenty předně musí být v podobě datové zprávy, a to ve formátu a velikosti, které budou stanoveny v provozní dokumentaci informačního systému datových schránek. Nebude-li dokument splňovat tyto požadavky, tj. nebude-li možno převést jej do datové zprávy formátu a velikosti požadované právním předpisem, bude jej nutno zaslat jiným způsobem. Dále nebude možné, respektive žádoucí využít datových schránek v případě, kdy samotný dokument sice bude ve formě datové zprávy splňující požadavky provozní dokumentace, avšak jeho přílohy již nikoliv. Datové schránky patrně nebudou vhodné pro zasílání dokumentů v podobě strukturovaných dat či složky strukturovaných dat formovaných dle požadavků zvláštních komunikačních aplikací typu daňového portálu (a jeho funkcionality Elektronické podání).“*** Při autorizované konverzi by mělo dojít ke kontrole formátu a velikosti. Tyto kontroly může zabezpečit ASAS modulem RAK.
- Ministerstvo oznámí odesílateli, že velikost datové zprávy je nad maximální stanovený limit a jako takovou ji není možné doručit zadanému adresátovi. Tento údaj je v ASAS uveden jako stav nevypraveno s informací (důvodem) vráceno-nepřípustná velikost.

- Ministerstvo oznámí odesílateli, že při ukládání datové zprávy do datové schránky došlo k chybě s tím, že datová zpráva do datové schránky vložena nebyla. K doručení datové zprávy nedošlo. Tento údaj je v ASAS uveden jako stav nevypraveno.
- API informačního systému datových schránek musí povinně poskytnout základní údaje, mezi které patří: identifikace datové zprávy, stav (dle § 20 odstavce 1 písmena c), e), f), g), h) zákona č. 300/2008 Sb.) a datum (doručení/nedoručení) datové zprávy.
- API informačního systému datových schránek musí povinně poskytnout základní údaje o cenách (výplatě poštovného) dle § 14 odstavce 2 zákona č. 300/2008 Sb. a Zákona č. 526/1990 Sb. o cenách, ve znění pozdějších předpisů.
- Informační systém datových schránek musí být po celou dobu existence datové schránky k dispozici a poskytnout informace v rozsahu § 20 odstavce 1 písmene i) zákona č. 300/2008 Sb.

- Zpracovatel daného spisu je jedinou osobou odpovědnou posoudit ustanovení § 17 odstavce 7 zákona č. 300/2008 Sb., ve kterém je uvedeno: ***"Doručování mezi orgány veřejné moci prostřednictvím datové schránky se nepoužije, pokud je z bezpečnostních důvodů mezi těmito orgány zavedena jiná forma elektronické komunikace"***. Uvedené platí např. v případech žádosti cizinecké policie o poskytnutí rodného čísla pro cizince.
- Zpracovatel daného spisu je jedinou osobou odpovědnou posoudit, zda nelze realizovat autorizovanou konverzi v souladu s § 24 odstavec 5 zákona č. 300/2008 Sb., a z těchto důvodů nelze vytvořit datovou zprávu dle § 19 odstavce 1 zákona č. 300/2008 Sb.

Odeslanou zprávu z datové schránky odesilatele ministerstvo dodá do datové schránky osoby, která je odesílatelem označena jako adresát, přesně v souladu s § 20 odstavec 1 písmeno c) zákona č. 300/2008 Sb.: ***„Ministerstvo dodá datovou zprávu odeslanou z datové schránky do datové schránky osoby, která je odesílatelem označena jako adresát"*** a podle ustanovení § 20 odstavec 1 písmeno a) zákona č. 300/2008 Sb.

zajistí připojení kvalifikovaného časového razítka k datové zprávě odeslané z datové schránky odesilatele. [14] [18]

3.8 Ukládání a vyřizování dokumentů

Problematiku ukládání dokumentů bez ohledu na jejich podobu obecně řeší § 8 vyhlášky 646/2004 Sb., o podrobnostech výkonu spisové služby:

- Postup při ukládání vyřízených a uzavřených dokumentů do spisovny nebo do digitální spisovny musí být obsažen ve Spisovém a skartačním řádu MO.
- Zaměstnanec pověřený vedením spisovny (digitální spisovny) přezkoumá, zda ukládané dokumenty jsou úplné, a uloží je (listinné dokumenty do spisovny, elektronické dokumenty do digitální spisovny). O uložených dokumentech je nutné vést evidenci.
- O zapůjčených dokumentech vede spisovna evidenci. Postup při zapůjčování dokumentů a jejich evidenci je nezbytné upřesnit ve Spisovém a skartačním řádu MO.
- Dokumenty v digitální podobě se skartačními znaky "A" a "V" musí být v souladu s usnesením vlády České republiky ze dne 3. listopadu 2008 č. 1338 převedeny do schváleného formátu, tj. formát PDF/A-1a (ISO 19005–1), PNG (ISO/IEC 15948:2004), TIFF (Tagged Image File Format – revize 6 – nekomprimovaný).
- Zaměstnanec pověřený vedením spisovny, případně správního archivu připravuje dokumenty ke skartačnímu řízení. V seznamech dokumentů navrhovaných ke skartačnímu řízení uvede zvlášť dokumenty se skartačním znakem "A", zvlášť dokumenty se skartačním znakem "S". Dokumenty se skartačním znakem "V" skartační komise posoudí a zařadí je buď k dokumentům se skartačním znakem "A", nebo k dokumentům se skartačním znakem "S".
- Určený vedoucí zaměstnanec zašle skartační návrh na vyřazení dokumentů a razítek příslušnému archivu. Skartační návrh je zaslán v digitální podobě prostřednictvím informačního systému datových schránek.

- U elektronických dokumentů se znakem „A“ zaměstnanec elektronické dokumenty zkontroluje, zkompletuje a opatří je definovanou sadou popisných údajů, tj. metadata
- Každý dokument spolu s jeho s množinou metadat zabalí do informačního balíčku SIP (Submission Information Package).
- S pracovníkem digitálního archivu provede zaměstnanec odsouhlasení seznamu elektronických dokumentů předpokládaného objemu a navzájem se případně dohodne technický nosič dat, čas a způsob přenosu. Z určitého množství SIP balíčků (zabalených dokumentů) se vytvoří dávka, která bude přenesena pomocí schválených nosičů dat médií do Národního digitálního archivu.

Skartační návrh, protokol o skartačním řízení, protokol o předání archiválií a potvrzení archivu (digitálního archivu) o jejich převzetí se ukládají na MO a také v archivu, ve kterém jsou archiválie uloženy. [2] [11]

4 ZHODNOCENÍ SLUŽBY ASAS S POHLEDU INTEGRACE NA KAŽDÝ IS V RÁMCI RESORTU AČR

4.1 Posouzení integrace na Internet vs. Intranet

Předpokladem úspěšného vyřešení dopadů zákona č.300/2008 Sb. je zajištění galvanického bezpečného propojení mezi systémem datových schránek a ASAS (sítě internet a intranet). Tento axiom je podporován nejen zněním zákona č.300/2008 Sb. který hovoří o přímém napojení v § 29, ale nalezneme jej v celém koncepčním záměru e-Governmentu a samozřejmě také v připravovaných novelách souvisejících zákonů (např. aktuálně schvalovaná novela zákona č.300/2008, 499/2004, aj.). [3] [11]

Krom těchto předpokladů hovoří pro tento předpoklad také argumenty technologické a procesní. Vzhledem k předpokládanému vysokému objemu přenášených dokumentů (dle současných kvalifikovaných odhadů až 3000 dokumentů za den) by jejich přenos mezi oddělenými sítěmi na pomocném pracovním médiu byl nejen velmi problematický, ale představoval by i zásadní riziko ztráty či zanedbání se všemi právními důsledky pro organizaci (zejména nedodržení zákonných lhůt od data přijetí datové zprávy adresátem doručení). [17]

4.2 Posouzení propojení ASAS na ISDS

Během příjmu datových zpráv probíhá několik zásadních kroků, které bez spojení na příslušné autority vůbec nelze realizovat, zejména ověřování stažení a uložení doručené datové zprávy, kontrola elektronického podpisu a časového razítka, v případě odesílání je to především komunikace se systémem DS ohledně existence DS adresáta (činnost vykonává referent organizace – tedy prakticky každý uživatel ASAS) a dále činnosti v souvislosti s výkonem procesu autorizované konverze. Tyto činnosti jsou vykonávány současně na řadě pracovišť ASAS.

V této souvislosti je třeba zmínit také institut schvalovacího procesu a především jeho zásadní část, kterou je elektronické podepisování vyhotovených elektronických dokumentů a jejich následné odeslání do datové schránky adresáta, které bude probíhat opět v celé šíři organizační struktury resortu MO a o jehož vykonání musí být veden jednoznačný záznam v ASAS, jakožto nástroji spisové služby. [14]

4.3 Distribuce elektronických datových zpráv s využitím dostupných KIS (ŠIS, ISL)

Návrh řešení předpokládá distribuci přijatých a vypravovaných elektronických datových zpráv výhradně prostředky ASAS od / do útvarů ve stávající KIS ŠIS, ve které je systém ASAS rutinně provozován. Po definování přístupových pravidel mohou s ASAS pracovat také uživatelé jiných domén v rámci MO (dnes např. FIS).

Návrh bezpečného interface ISDS na ASAS je řešen Ř ARI ve spolupráci s SKIS MO. ***Výchozím předpokladem je použití technologií s dosaženým stupněm certifikace EAL 4, tj. technologie navržené, testované a hodnocené metodicky s ohledem na maximální zajištění bezpečnosti***. Pro propojení ASAS s certifikační autoritou a ISDS budou dle návrhu použity buď pronajaté okruhy, nebo spojení prostřednictvím Internetu. Omezujícím východiskem je definice provozního prostředí CADS, která je uvedena v certifikačních zprávách ISL a FIS. [13] [20]

4.4 Interface na agendové systémy

Toto rozhraní není přímo vynucené zákonem č. 300/2008 Sb., nesouvisí s rozhraním na datové schránky, ale nepřímo podmiňuje úspěšnost eGovernmentu. Jeho opodstatnění se opírá především o novelu zákona č. 499/2004 Sb., jehož prováděcí vyhláška bude zavádět do naší legislativy mezinárodní standard MoReq2 ve formě tzv. Národního standardu. Konkrétní řešení musí vycházet z reality současných informačních systémů ve veřejné správě a jejich praktického rozšíření. [9] [17]

Pracovní skupina na tvorbu Národního standardu, svolaná a koordinovaná Odborem archivní správy a spisové služby, má za úkol především dodefinování metadat, která se ve standardu MoReq2 nevyskytují a jsou pro české prostředí potřebná. Na základě dílčích závěrů je možné již nyní navrhnout řešení, které je, na základě dosud známých skutečností, v souladu s tímto připravovaným Národním standardem.

Interface systému ASAS na agendové systémy, případně také na jiné systémy spisových služeb, zabezpečuje tzv. ***Integrační platforma systému GINIS®*** (licenčně označována GINIS-XRG). [14]

Toto řešení je v současné době nejen nejrozsáhlejší definicí rozhraní spisových služeb ve veřejné správě ČR, ale je podložené jeho dlouholetým praktickým používáním

v mnoha integračních projektech, je metodicky kompaktní a v souladu s legislativou a dosud známými návrhy legislativních novel. Toto řešení dnes již představuje přirozený standard v komunikaci spisová služba – agenda, resp. spisová služba – spisová služba.

Základní komponenty Integrační platformy GINIS®

- ***XML rozhraní systému GINIS®*** - rozhraní založené na zpracování a distribuci dat ve formátu XML. Jedná se o otevřenou aplikační platformu, která je interně využívána všemi webovými službami, komponentami datově orientovaného rozhraní INT a dalšími aplikacemi systému.
- ***Webové služby rozhraní XRG*** - kategorizovaná sada webových metod umožňujících integrovaným aplikacím ustavit vzájemnou komunikaci probíhající v reálném čase metodou dotaz-odpověď. Jednotlivé metody jsou cíleně orientovány na poskytování služeb pro externí systémy tak, aby toto rozhraní bylo slučitelné s koncepty SOA.
- ***Datově orientované rozhraní INT*** - je určeno pro datovou komunikaci s externími systémy přes import a export asynchronně zpracovávaných datových dávek. Tento způsob integrace je primárně vhodný pro velmi velké objemy přenášených dat.
- ***Nástroje pro komunikaci se specializovanými rozhraními třetích stran*** - jedná se o řešení pro přístup k obecně vyhlášeným nebo dlouhodobě provozovaným systémům. Namátkou lze zmínit podporu obousměrné komunikace s portálem veřejné správy nebo implementaci rozhraní pro elektronickou komunikaci s různými komerčními bankami.
- ***Portál pro sdílení a řízenou distribuci technologických a provozních informací*** - sjednocuje informace o různých integračních projektech a aplikacích do jediného webového zdroje. Plní rovněž funkci komunitního portálu pro osoby zainteresované na realizaci konkrétního integračního řešení.
- ***Centrální řízení přístupů a zabezpečení systému*** - realizováno pomocí aplikace Autorizační služba pro GINIS®, která se jako služba operačního systému instaluje přímo na aplikační server. Její primární funkcí je

zabezpečení centrální správy profilů pro přístup do systému a optimalizace vyhodnocení předané sady uživatelských oprávnění za pomoci vstupenek.

- ***Aktivní integrace na základě vzniku systémových událostí*** - doplňuje možnost jednotlivých komponent integrační platformy GINIS® vystupovat v roli aktivního člena v rámci daného integračního řešení a nahrazovat tak významnou část funkcionality integračního brokeru v situacích, kdy není nasazen.

Přehled agentových informačních systémů MO: [13] [18]

- Finanční informační systém (FIS)
- Informační systém logistiky (ISL)
- Informační systém o službě a personálu (ISSP)
- Štábní informační systém AČR (ŠIS AČR)
- Digitální vojenský informační systém o území (DVISÚ)
- Informační systém plánování sil (ISPS) - dříve Modul centrální databáze projektů (MCDP)
- Informační systém mobilizačních příprav (ISMP)
- Informační systém Vojenské policie (ISVP)
- Automatizovaný IS vojenského zdravotnictví (ZDRAVIS)
- Systém elektronické podpory obchodování (SEPO)
- Informační systém vyzbrojování (ISV)
- Informační systém standardizace (IS STAN) – samostatný modul ISL
- Automatizovaná spisová a archivní služba (ASAS)
- Czech NATO Secret – NATO Office Automation Network (CZ NS NOAN)
- Systém utajeného vládního spojení (IS VEGA)
- Internet MO (IMO)

5 ANALÝZA NA SLUŽBU ASAS S POHLEDU TVŮRCE A PROVOZOVATELE FLEXIBILNÍHO SW

Požadavky zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, kladou požadavky na další rozvoj ASAS. *Dílčí analýza je popsána níže, přičemž je rozdělena do dvou základních skupin na přímo respektive nepřímo vyplývající požadavky, tedy nutné a další vhodné.*

Vhodnou kombinací těchto bodů lze dosáhnout maximálního naplnění požadavků zákona č. 300/2008 Sb. Řešení popsané v kapitole 5.1 je pak nutnou podmínkou pro splnění minimálních požadavků. [9] [14]

5.1 Návrh opatření k realizaci zákona č. 300/2008 Sb. prostředky ASAS

Dopady na SSL přímo vyplývající ze zákona č. 300/2008 Sb.

- Interface na informační systém datových schránek (ISDS) zahrnuje rozšíření ASAS o oblasti:
  - Rozšíření funkčnosti podatelny ASAS o interface na ISDS (předpoklad – zřízení centrálního příjmového místa)
  - Vazba kartotéky externích subjektů ASAS na datové schránky
  - Rozšíření funkčnosti výpravny ASAS o interface na ISDS (předpoklad – zřízení centrálního vypravovacího místa)
  - Administrace přístupu ASAS k ISDS
  - Využití elektronického podpisu v ASAS ve vztahu k ISDS
- Konverzní pracoviště pro zajištění autorizované konverze zahrnuje rozšíření ASAS o oblast:
  - Konverzní pracoviště pro autorizovanou konverzi
- Návrhy změn interních norem:
  - Změny ve Spisovém a skartačním řádu MO a příp. dalších souvisejících interních normách

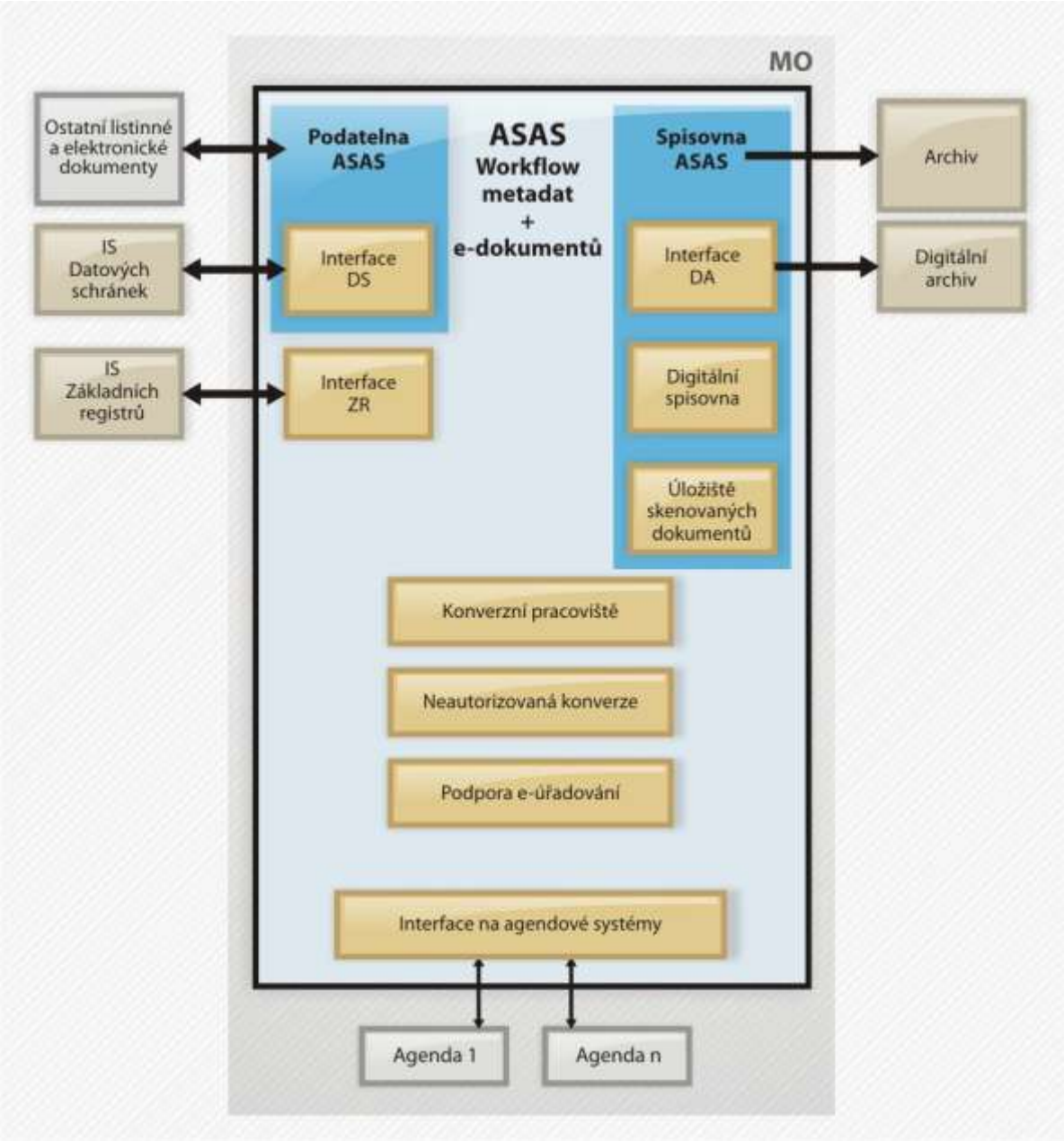
- Metodika zahrnuje rozšíření ASAS o oblast:
  - Metodika zacházení s dokumenty v elektronické podobě, tvorba workflow elektronických dokumentů
- Interface na agendové systémy zahrnuje rozšíření ASAS o oblast:
  - XRG Integrační platforma, INT
- Neautorizovaná konverze dokumentů zahrnuje rozšíření ASAS o oblast:
  - Centrální skenovací pracoviště / digitalizace dokumentů.
  - Skenování na OC
- Zajištění podpory koncových uživatelů je nutné v oblastech:
  - Elektronický vzdělávací systém
  - Podpora koncových uživatelů
- Hardware
  - Architektura řešení
  - Nároky na komunikační datovou síť
  - Eliminace rizik v oblasti zabezpečení náhradního provozu
  - Využití geoclusteru pro bezpečné provozování systému GINIS-SSL (ASAS)
  - Stanovení požadavků na centrální úložiště elektronických dokumentů
- Úložiště elektronických dokumentů
  - Rozšíření úložiště elektronických dokumentů ASAS, DMS

Dopady na SSL nepřímo vyplývající ze zákona č. 300/2008 Sb., nebo očekávaných v rámci eGovernmentu (v průběhu let 2009 až 2011)

- Podpora elektronického úřadování zahrnuje rozšíření ASAS v oblastech:
  - Trasování dokumentů – definice workflow dokumentů

- Vlastnosti dokumentů – rozšíření evidenčního profilu
- Avizační a událostní systém
- Vytěžování e-formulářů
- Vazba na frankovací stroje
- Manažerské a informační moduly
- Interface CP (Czech POINT)

- Interface na digitální archiv
  - Předpokládaný rozvoj v propojení na digitální archiv a předávání dokumentů
- Interface na základní registry
  - Předpokládaný rozvoj v oblasti napojení na základní registry
- Digitální spisovna
  - Úložiště skenovaných dokumentů
  - Podpora fulltextového vyhledávání



Obr. 8. Blokové schéma vztahu ASAS k okolním systémům

5.1.1 Okamžitá opatření k zajištění naplnění zákona k datu účinnosti

- Interface na informační systém datových schránek (ISDS)
  - Rozšíření funkčnosti podatelny ASAS o interface na ISDS (předpoklad – zřízení centrálního příjmového místa)
  - Vazba kartotéky externích subjektů ASAS na datové schránky
  - Rozšíření funkčnosti výpravny ASAS o interface na ISDS (předpoklad – zřízení centrálního vypravovacího místa)

- Administrace přístupu ASAS k ISDS
- Využití elektronického podpisu v ASAS ve vztahu k ISDS

- Konverzní pracoviště pro zajištění autorizované konverze
  - Konverzní pracoviště pro autorizovanou konverzi
- Návrhy změn interních norem
  - Změny ve Spisovém a skartačním řádu MO a příp. dalších souvisejících interních normách
- Metodika
  - Metodika zacházení s dokumenty v elektronické podobě, tvorba workflow elektronických dokumentů
- Hardware
  - Architektura řešení
  - Nároky na komunikační datovou síť
  - Eliminace rizik v oblasti zabezpečení náhradního provozu
  - Využití geoclusteru pro bezpečné provozování systému GINIS-SSL (ASAS)
  - Stanovení požadavků na centrální úložiště elektronických dokumentů
- Úložiště elektronických dokumentů
  - Rozšíření úložiště elektronických dokumentů ASAS, DMS

5.1.2 Přechodné období do dosažení cílového stavu

- Neautorizovaná konverze dokumentů
  - Centrální skenovací pracoviště / digitalizace dokumentů.
  - Skenování na OC
- Podpora elektronického úřadování
  - Vlastnosti dokumentů – rozšíření evidenčního profilu

- Avizační a událostní systém

- Zajištění podpory koncových uživatelů
  - Elektronický vzdělávací systém
  - Podpora koncových uživatelů

5.1.3 Cílové řešení

- interface na agendové systémy zahrnuje rozšíření ASAS o oblast
  - XRG Integrační platforma, INT
- interface na digitální archiv
  - Předpokládaný rozvoj v propojení na digitální archiv a předávání dokumentů
- interface na základní registry
  - Předpokládaný rozvoj v oblasti napojení na základní registry
- podpora elektronického úřadování zahrnuje rozšíření ASAS v oblastech
  - Trasování dokumentů – definice workflow dokumentů
  - Vytěžování e-formulářů
  - Vazba na frankovací stroje
  - Manažerské a informační moduly
  - Interface CP (Czech POINT)
- digitální spisovna
  - Úložiště skenovaných dokumentů
  - Podpora fulltextového vyhledávání

Dále je popsán návrh řešení napojení ASAS na systém datových schránek, které jsou propojením IS v rámci Ministerstva obrany.

5.2 Interface na Informační systém datových schránek

S ohledem na skutečnost, že doposud nedošlo ze strany MV ČR ke zveřejnění popisu rozhraní Informačního systému datových schránek (dále ISDS), přikládáme možný návrh řešení „Interface na Informační systém datových schránek“ – dále API na ISDS. Návrh vychází z pracovní skupiny vzniklé podpisem Memoranda o spolupráci mezi MV ČR a významnými dodavateli Spisové služby, kterým je též GORDIC spol. s r.o.. [14] [16]

Elektronické dokumenty jsou v informačních systémech evidovány různým způsobem. Nicméně zřejmě nejrozšířenějším případem je uložení elektronický dokumentu ve formě datového souboru, který lze zobrazit a editovat pomocí běžně užívaných kancelářských aplikací. *Podobně jako je tomu u klasických dokumentů v papírové formě, rovněž pro elektronické dokumenty je nezbytné zabezpečit možnost jejich výměny mezi různými orgány veřejné správy. Výměna dokumentů přitom svým rozsahem zpravidla přesahuje hranice jednoho orgánu veřejné správy a tím i hranice jednoho informačního systému.*

Tato část materiálu si klade za cíl formalizovat vzájemnou výměnu elektronických dokumentů mezi různými subjekty veřejné správy. Elektronický dokument je v tomto smyslu každý záznam či informace předávaná mezi informačními systémy. Závazná formalizace vzájemné výměny elektronických dokumentů je nutnou podmínkou a povinným základním kamenem pro referenční rozhraní informačních systémů veřejné správy. Vzájemnou výměnu dalších tzv. agendových záznamů mezi informačními systémy je nutné realizovat ve stejných standardech a struktuře, není však již předmětem tohoto dokumentu.

Za předmět této výměny je přitom považován přímo vlastní datový soubor, ve kterém je elektronický dokument fyzicky uložen na záznamovém médiu. Není zde tedy řešena komunikace spočívající v předávání jakýchkoliv generalizovaných datových struktur získaných pomocí abstrakce či transformace původního elektronického dokumentu.

5.3 Konverzní pracoviště (autorizovaná konverze)

Dle §22 Zákona č. 300/2008 Sb. se konverzí rozumí:

- Úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky, nebo
- Úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.

Datová zpráva

- Zpráva doručená prostřednictvím datové schránky,
- 1 nebo více elektronických souborů, které tvoří z hlediska informační hodnoty jeden celek. Tyto soubory byly uloženy v některém z definovaných formátů (PDF/A, PNG, TIFF).

Zákon taxativně vymezuje případy, ve kterých není možné realizovat konverzi dokumentů.

5.3.1 Autorizovaná konverze do dokumentu obsaženého v datové zprávě

Digitalizace dokumentu na vhodném zařízení

- Digitalizace (skenování), doporučené parametry pro skenování:

  Barevný režim: černobílý

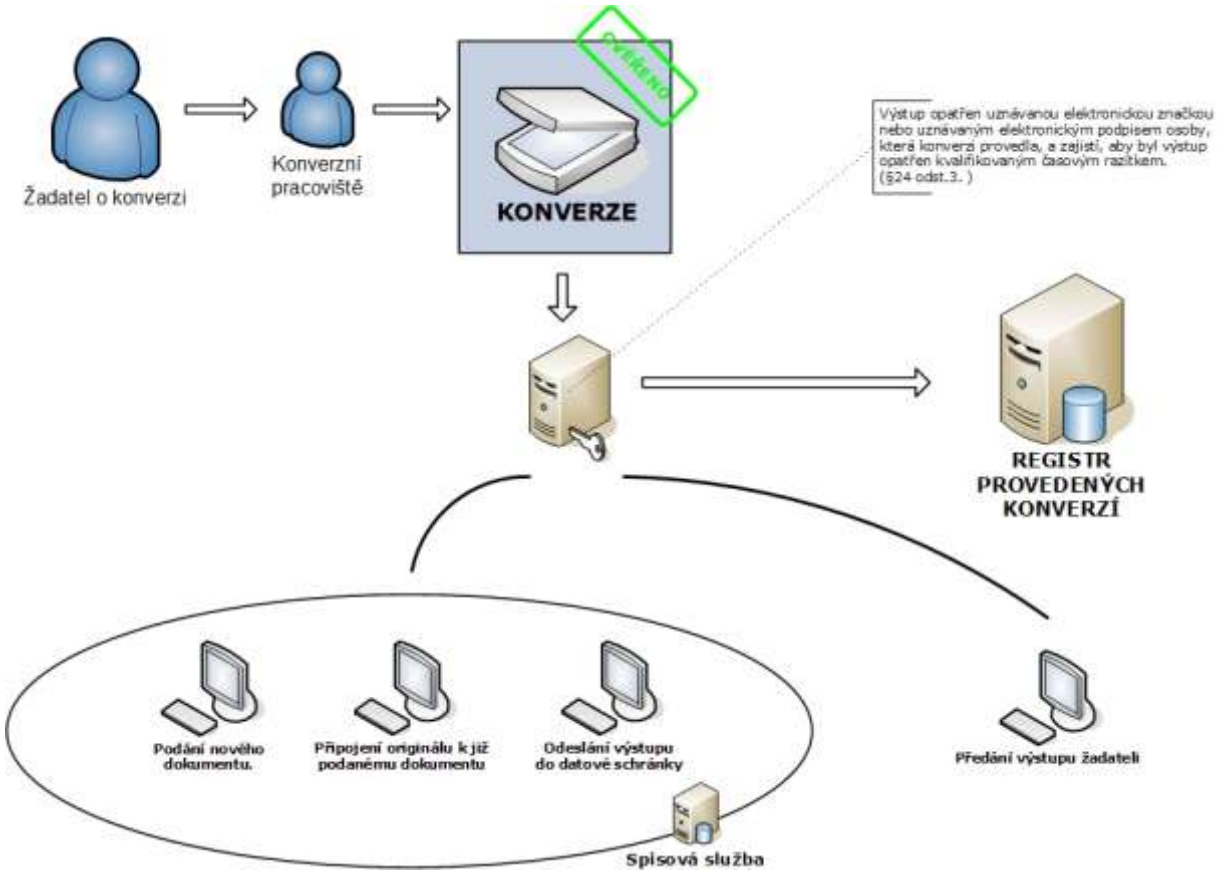
  Formát souboru: TIFF G4 (jednostránkové dokumenty)

  MTIFF G4 (vícestránkové dokumenty) revize 1.2 a vyšší

  PDF

  Rozlišení: 200 nebo 300 dpi

- Převod do jednoho z definovaných formátů (PDF/A, PNG, TIFF).
  - Opatří výstup uznávanou elektronickou značkou nebo uznávaným elektronickým podpisem osoby, která konverzi provedla
  - Zajistí, aby součástí výstupu bylo kvalifikované časové razítko
  - Zajistí předání výstupu prostřednictvím datové zprávy (datové schránky, mailu nebo na datovém médiu)

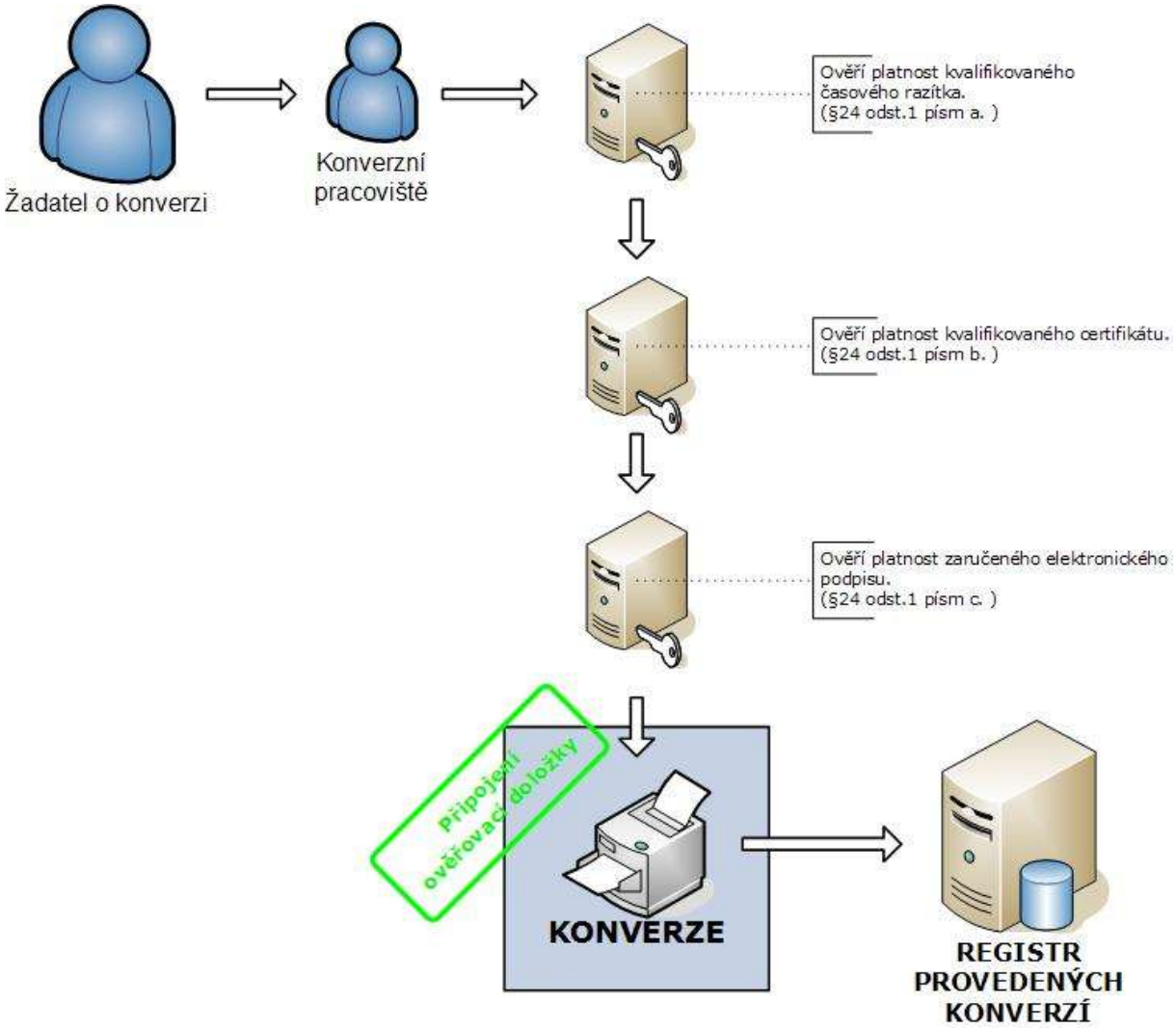


Obr. 9. Schéma postupu konverze do dokumentu obsaženého v datové zprávě

5.3.2 Autorizovaná konverze z dokumentu obsaženého v datové zprávě

- Ověření platnosti kvalifikovaného časového razítka vstupu,
- Ověření, že kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založen zaručený elektronický podpis, kterým je podepsán vstup, nebo kvalifikovaný systémový certifikát vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založena elektronická značka, kterou je označen vstup, nebyly před okamžikem uvedeným v kvalifikovaném časovém razítku zneplatněny,
- Ověření platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaný elektronický podpis“) nebo platnost uznávané elektronické značky.

- Vytvoření výstupu. Výstup je vytvořen tiskem vstupu na zařízení k tomu určenému. Technické parametry tisku a vlastnosti papíru určí prováděcí vyhláška k Zákonu č. 300/2008 Sb.
- Bezodkladně po ověření shody výstupu se vstupem, a shoduje-li se výstup se vstupem, je k výstupu připojena ověřovací doložka.



Obr. 10. Schéma postupu konverze z dokumentu obsaženého v datové zprávě

Autorizovaná konverze z dokumentu obsaženého v datové zprávě do dokumentu obsaženého v datové zprávě je upravena v návrhu Zákona č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů. V tomto případě se jedná např. o autorizovanou konverzi dokumentů mezi jednotlivými datovými formáty nebo při změně

média. Autorizovaná konverze se neprovádí v případech specifikovaných v Zákoně č. 300/2008 Sb., §24, odst. 5. Ověřovací doložka je součástí výstupu a její náležitosti upravuje §25 Zákona č. 300/2008 Sb., obsahuje tedy: [9] [11]

Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě:

- Název subjektu, který konverzi provedl,
- Pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,
- Údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,
- Údaj o tom, z kolika listů se skládá vstup,
- Údaj o tom, zda vstup obsahuje vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky variabilní prvek nebo jiný zajišťovací prvek,
- Datum vyhotovení ověřovací doložky,
- Jméno, případně jména, a příjmení osoby, která konverzi provedla.

Ověřovací doložka konverze do dokumentu v listinné podobě:

- Název subjektu, který konverzi provedl,
- Pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,
- Údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,
- Údaj o tom, z kolika listů se skládá výstup,
- Datum vyhotovení ověřovací doložky,
- Údaj o tom, zda byl vstup podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou, číslo kvalifikovaného certifikátu, na němž je uznávaný elektronický podpis založen, nebo číslo kvalifikovaného systémového certifikátu, na němž je uznávaná elektronická značka založena, a obchodní firmu akreditovaného

poskytovatele certifikačních služeb, který kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydal,

- Datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal,
- Otisk úředního razítka, jméno, popřípadě jména, příjmení a podpis osoby, která konverzi provedla.

5.3.3 Registr autorizovaných konverzí – RAK

Účelem modulu GINIS® - RAK je správa a bezpečné vedení evidence provedených konverzí dle zákona č. 300/2008 Sb. Koncepčně je navržen jako samostatný nástroj využívající společné vrstvy spisové služby, registrů a ekonomiky. [14]

Modul obsahuje tyto registry a podregistry :

Registry

Registr konverzí dokumentů v listinné podobě do dokumentů obsažených v datové zprávě Registr konverzí dokumentů obsažených v datové zprávě do dokumentů v listinné podobě Registr doložek.

Podregistr

Správních poplatků.

Centralizace

Všechny provedené konverze se evidují v centrální klientské databázi. Díky tomuto řešení pak všechna konverzní pracoviště postupují podle jednotné metodiky a současně využívají jedno centrálně spravované a zabezpečené úložiště.

Doložky

Tvorba doložky je realizována formou tisku samolepících štítků, případně tisku papírových doložek. Samotná technologie zpracování pak umožňuje:

- Návrh centrální šablony pro tvorbu doložek.
- Návrh uživatelské šablony pro tvorbu doložek.

Spisová služba

Koncepčně modul navazuje na procesy aplikované ve spisové službě a je plně připraven na (pokud to proces vidimace vyžaduje) on-line spolupráci s vrstvou spisové služby. Díky tomu je pak možné:

- Podat dokument – výsledek konverze současně evidovat jak do spisové služby, tak do registru konverzí (vidimací),
- Připojit originál k existujícímu dokumentu – výsledek konverze evidovat a připojit k existujícímu dokumentu a současně provést zápis do registru konverzí (vidimací),
- Odeslat konvertovaný dokument do datové schránky.

Datové schránky

Díky integraci komponent ze spisové služby modul umožňuje přímé odeslání výstupu konverze do datové schránky. V tento okamžik je vytvořen zápis o odeslání do spisové služby a podniknuty kroky k okamžitému odeslání výstupu do datové schránky.

Správní poplatky

Modul zahrnuje registr odbavených správních poplatků a spolu s nástroji na tvorbu výběrů a tisku přehledových sestav.

Nedílnou součástí je přímá integrace EKO vrstvy pro správu správních poplatků prostřednictvím modulů POK, BUC atd. Integrace je postavena na jednotné metodice tvorby WS pro úspěšné párování odbavených poplatků. Celý systém je nezávislý na způsobu úhrady (hotovostně, bezhotovostně, platy platebními kartami).

Automatizace

Díky připraveným komponentám je možné přímo ze skenovací linky (s využitím OCR) provést současné zápisy jak do Spisové služby, tak do registru konverzí.

5.3.4 Konverzní pracoviště (neautorizovaná konverze)

Neautorizovaná konverze dokumentů – digitalizace z listinné podoby

Jako zařízení pro neautorizovanou konverzi (digitalizaci) dokumentů je možno použít dokumentový skener s denní zatížitelností, která koresponduje s objemem

zpracovávaných dokumentů. Výhodné je využití multifunkčních zařízení, jako jsou např. digitální kopírky, které v sobě zahrnují dokumentový skener dobré kvality většinou s možností kvalitního (nejlépe duplexního) podávání papíru (oboustranné skenování). Použitelné jsou produkty většiny hlavních světových dodavatelů, jako jsou Ricoh, Canon, Xerox, Minolta, apod. Multifunkční digitální stroje navíc poskytují velmi praktické funkce pro síťové skenování, takže je možné celý proces digitalizace zautomatizovat a obsluhovat z ovládacího panelu multifunkčního stroje.

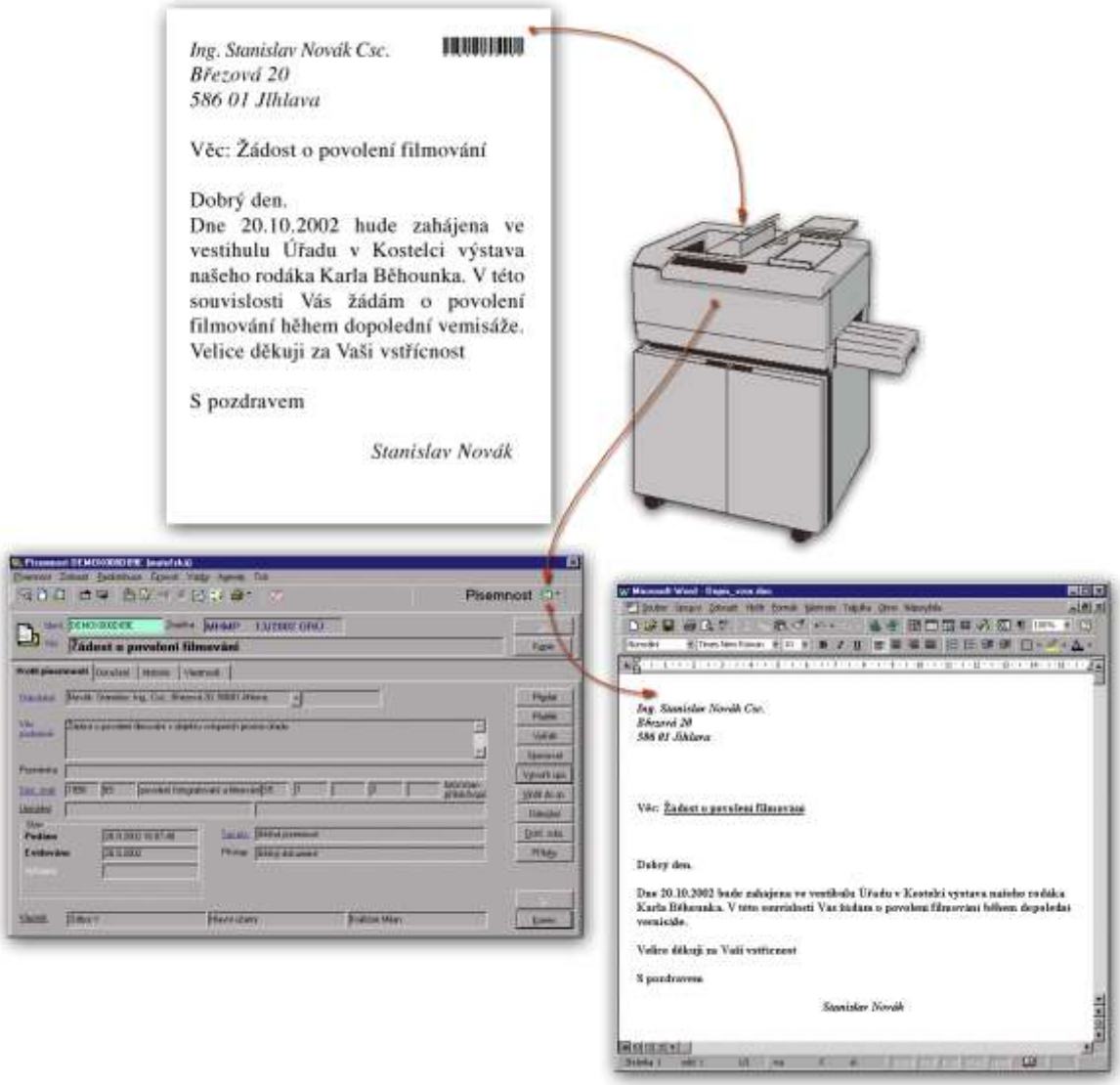
Digitalizované dokumenty jsou přebírány z multifunkčních strojů pomocí inteligentního monitorování stanovených síťových prostředků organizace.

S funkčními moduly lze přijímat do systému i dokumenty přijaté v elektronické podobě z jiných systémů buďto z paměťových medií, nebo transportovaných komunikačními nástroji, např. elektronickou poštou.

Základní konfigurace systému by měla být rozšiřitelná (nutno konzultovat s konkrétním dodavatelem) o další funkční moduly, které kromě digitalizace dokumentů, komprese, spojování do vícestránkových digitálních dokumentů a zpracování čárového kódu dovolují další funkce pro práci s dokumenty a digitálním archivem, jako jsou např. celodokumentové OCR, zpracování formulářů se zónovým čtením, vytěžování dat z dokumentů a jejich převod do systému elektronické spisové služby nebo do databáze, fulltextové vyhledávání v dokumentech apod.

Digitální dokument je optimálně zkomprimován do souboru ve formátu TIFF nebo PDF, označen „přečteným“ identifikátorem a předán systému elektronické spisové služby.

V ASAS je příchozí dokument ze skenovací linky automaticky „připojen“ jako elektronický obraz k evidenční kartě dokumentu. Některé evidenční položky je možné automaticky vyplnit podle předem zadaného popisu, klíčových slov nebo indexů. Veškeré další činnosti s dokumentem (řízený oběh, vyřizování, archivace...), jsou již záležitostí ASAS. Elektronické dokumenty jsou bezpečně uložené v úložišti elektronických dokumentů ASAS. [14]



Obr. 11. Skenovací linka

5.4 Návrhy změn interních norem

Spisový řád MO a další interní směrnice související s výkonem spisové služby a obsluhy datových schránek musí být v návaznosti na dopady zákona č. 300/2008 Sb. doplněny nebo upraveny zejména v následujících oblastech: [14]

- Spisový řád MO musí stanovit, kdo je odpovědný za včasné vyzvedávání zpráv z datové schránky. Nevyzvednutí zprávy může mít pro organizaci negativní právní dopady.

- Spisový řád MO musí stanovit seznam pracovníků pověřených vyzvedáváním pošty. Za každého takového pracovníka musí být stanoven zástupce v případě, že svou funkci nemůže vykonávat.
- Protože přístupové údaje jsou mezi osobami nepřenositelné, musí se dopředu počítat např. s nenadálou nutností zastoupit odpovědné pracovníky. Proto musí i zástupci mít vždy aktuálně platné přístupové údaje do systému datových schránek.
- Vnitřní předpisy organizace musí zajistit, že pracovník, který např. ukončil pracovní poměr, nebude mít nadále platné přístupové údaje vztažené ke schránce organizace. I tato skutečnost by měla být zohledněna ve Spisovém řádu MO. Zanedbání této povinnosti by mohlo vést k zneužití informací anebo k neoprávněnému právnímu vystupování dané osoby za organizaci. K zajištění této oblasti je vhodná i úprava organizačního řádu a ***je nutná úzká spolupráce personálního oddělení a správce systému.***
- Vnitřní směrnice MO musí stanovit, že ***všechny přístupy k datové schránce organizace budou realizovány výhradně prostřednictvím ASAS, a to aplikací elektronická podatelna pro datové schránky***. Přístupy mimo takto stanovený systém by nebyly ze strany MO přímo kontrolovatelné a přímo dohledatelné v historii záznamů ASAS.
- Avizační systém spisové služby je možné využít také jako bezpečnostní funkci, která na zadané e-mailové adresy ohlásí upozornění v případě, že zadaný počet dní žádný pracovník organizace nepřistoupil do datové schránky organizace. Tento avizační systém takto zabezpečí, že nedojde při přebírání pošty k prodlení a zanedbání ze strany pověřených pracovníků MO.
- Veškeré manipulace s datovou schránkou organizace budou na straně MO zaznamenávány do systému ASAS. Tím bude možné, i bez ověřeného přístupu do datových schránek, získat přehled historie odesílání, doručování odeslaných zásilek, vyzvedávání a i samotného přihlašování pověřených pracovníků k datovým schránkám.

Rizika v oblasti metodického zabezpečení provozu

Z metodického a organizačního hlediska mohou nastat zejména tyto rizikové situace:

- Výpadek dodávky el. proudu (stanice),
- Výpadek síťové konektivity (stanice),
- Došlo ke zneplatnění přístupových údajů,
- Nedošlo ke zneplatnění přístupových údajů,
- Zahájení/ukončení pracovního poměru, určení osoby oprávněné k přístupu do ISDS, zastupitelnost,
- Nedošlo k přihlášení do datové schránky,
- Jiná chyba uživatele.

5.5 Metodika, bezpečnost, INA

Navržené řešení je nutné koncipovat v souladu s domácí legislativou i zahraničními obecně uznávanými standardy.

Kromě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který přináší většinu změn, jichž se dotýká tento dokument, ***je nutné respektovat také ostatní platnou legislativu***, která s danou problematikou přímo či nepřímo souvisí. [14] [17]

Jedná se zejména o zákon č. 499/2004 Sb., o archivnictví a spisové službě, který nyní prochází rozsáhlou novelizací. Bohužel, k současnému datu není příslušná novela ještě schválena, není možné proto detailněji řešit její důsledky. Jednou ze základních očekávaných změn je definice tzv. neautorizované konverze dokumentů. Novelizace je očekávána také u Vyhlášky 646/2004 Sb., o podrobnostech výkonu spisové služby. Bohužel ani v tomto případě není dosud její definitivní znění známo. Z pohledu evidence dokumentů ve správním řízení je nutné respektovat zákon 500/2004 Sb., správní řád.

Z dalších dotčených zákonů a vyhlášek, které je nutné respektovat v oblasti práce s elektronickými dokumenty, lze uvést zejména zákon č. 227/2000 Sb., o elektronickém

podpisu (ve znění pozdějších novel). Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb. a Vyhláška č. 496/2004Sb., o elektronických podatelnách.

Z pohledu osobní bezpečnosti se jedná především o zákon č. 101/2000 Sb., o ochraně osobních údajů, a zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Na mezinárodním poli jde především o mezinárodní standard MoReq2, který byl připraven mezinárodním sdružením DLM Forum. Jedinými členy tohoto sdružení za Českou republiku je Ministerstvo vnitra ČR a firma GORDIC spol. s r. o. Další standardy na mezinárodní úrovni jsou zejména ISO 15489, Records Management a ISO 14721, Open Archival Information System, Reference Model (OAIS).

Důsledky plynoucí z uvedených zákonů, vyhlášek, norem a standardů musí být promítnuty a zohledněny ve všech interních normativech. Zejména se jedná o Spisový a skartační řád MO. [11] [13]

Přehled základní dotčené legislativy České republiky (vždy ve znění všech pozdějších novel):

- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě,
- Vyhláška č. 646/2004 Sb., o podrobnostech výkonu spisové služby,
- Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě,
- Zákon č. 500/2004 Sb., správní řád,
- Zákon č. 227/2000 Sb., o elektronickém podpisu,
- Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu,
- Vyhláška č. 496/2004 Sb., o elektronických podatelnách,
- Zákon č. 480/2004 Sb., o některých službách informační společnosti (tzv. antispamový zákon),

- Zákon č. 101/2000 Sb., o ochraně osobních údajů,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech,
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích,
- Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy,
- Zákon č. 29/2000 Sb., zákon o poštovních službách.

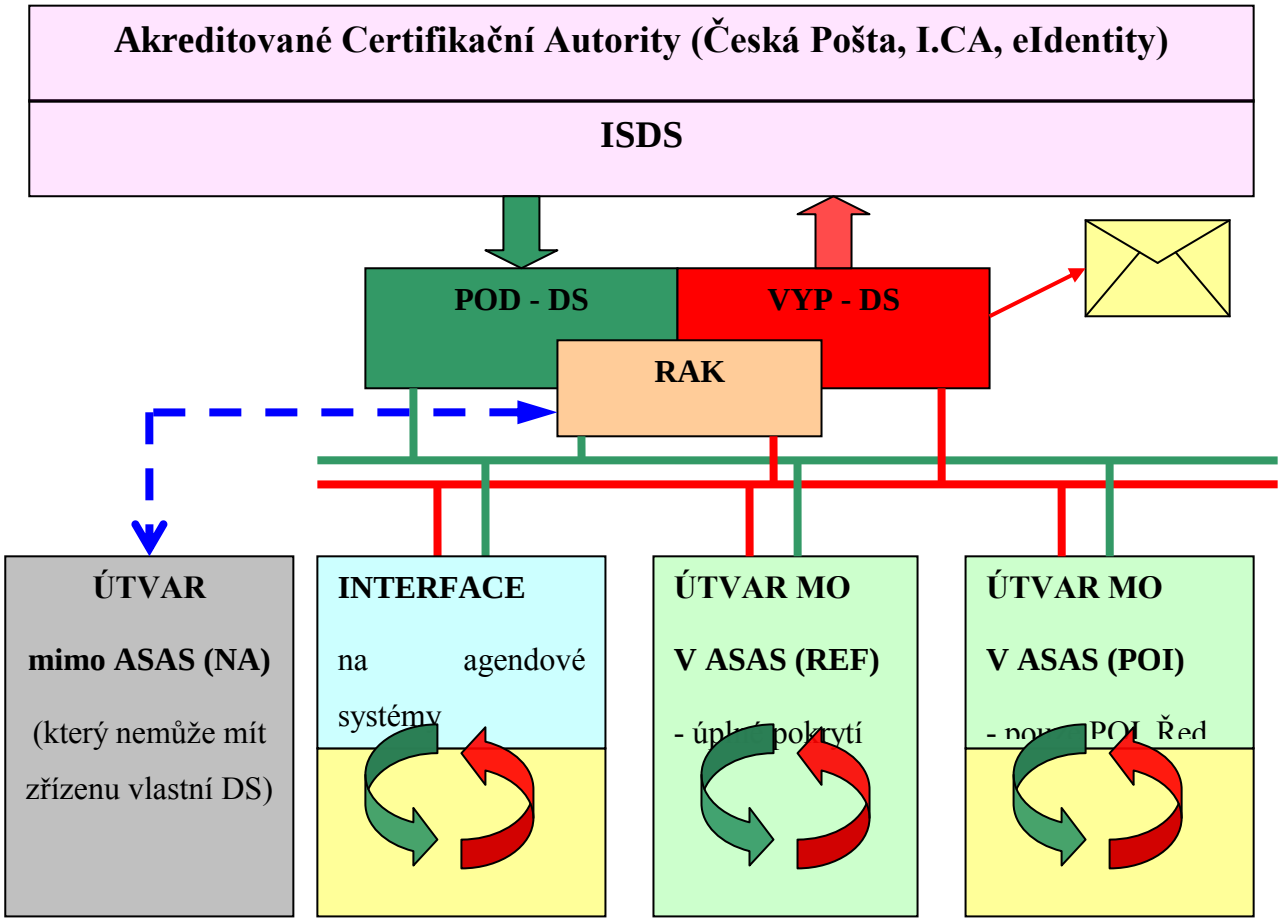
Přehled základních dotčených mezinárodních standardů

- MoReq2, Model Requirements for the Management of Electronic Records,
- ISO 15489, Records Management,
- ISO 14721, Open Archival Information System, Reference Model (OAIS).

Z provozně technického hlediska se jako perspektivní jeví možnost zavedení samostatného elektronického jednacího protokolu pro dokumenty doručené prostřednictvím datové schránky. Toto řešení předpokládá rozšíření ASAS v minimálním rozsahu POI + Velitel / Ředitel na všechny útvary MO tak, aby bylo možné cestou ASAS v reálném čase distribuovat podání k internímu adresátovy. Tak bude zajištěna maximální rychlost komunikace a sníží se na minimum riziko neopodstatněného zkrácení zákonných lhůt na vyřízení doručených dokumentů.

Zároveň bude možné v ASAS sledovat lhůty a termíny a prostřednictvím avizačního automatu na jejich překročení automatizovaně upozorňovat. Systém ISDS v současné době nepočítá s podporou vnitřní adresace u subjektů s rozsáhlou organizační strukturou. Z toho důvodu je nutné předpokládat nutnost zřízení centrálního podacího a vypravovacího místa v resortu MO, které primárně bude zabezpečovat činnosti spojené s příjmem, interní distribucí a odesíláním datových zpráv.

Toto pracovní místo je zároveň také ideálním pro zřízení centrálního pracoviště autorizované konverze a tak budou minimalizovány nároky na technickou vybavenost a školení obsluhy. Zároveň toto pracovní místo může být hlavním pracovištěm pro odesílání obvyklých listovních zásilek v resortu MO. [12] [14]



Obr. 12. Schéma zpracování doručení datových zpráv

5.6 Podpora uživatelů

Cílem této kapitoly je návrh způsobu podpory a vzdělávání koncových uživatelů pro pokrytí požadavků zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Vzdělávání navrhujeme provádět v rámci školení, seminářů, sebevzdělávání a školením uživatelů ASAS a jejich zástupů. Jako nezbytné shledáváme jedno speciální školení zaměstnanců realizujících autorizovanou konverzi. [14]

Vzdělávání

Vzdělávání koncových uživatelů je nutné rozdělit do několika základních oblastí“ školení, tematické semináře a sebevzdělávání. V následujících odstavcích je uveden návrh vzdělávání koncových uživatelů.

Doškolení zaměstnanců pracujících s modulem USU *na útvarových podatelnách*, případně na dalších podacích místech:

- Základní seznámení se systémem ASAS v oblasti práce s elektronickými dokumenty.
- Seznámení s metodikou vedení elektronického podacího deníku.
- Praktické procvičení základních úkonů při práci s elektronickými dokumenty.
- Základní seznámení s informačními zdroji k programu ASAS.

Proškolení zaměstnanců pracujících s modulem USU *na úrovni zástup referenta útvaru*:

- Základní seznámení se systémem ASAS a modulem USU.
- Seznámení s metodikou výkonu spisové služby pomocí ASAS v rozsahu práce referenta a rozdělení činností s útvarovou podatelnou.
- Praktické procvičení základních úkonů referenta při práci s modulem USU.
- Základní seznámení s informačními zdroji k programu ASAS (odkazy na intranetu, procesní scénáře, příručky apod.).

Doškolení *referentů útvarů* (tzv. osob zodpovědných za SU) pracujících s modulem USU:

- Základní seznámení se skladbou modulů ASAS.
- Seznámení s metodikou výkonu spisové služby pomocí ASAS na celém útvaru; rozdělení činností mezi jednotlivé zaměstnance se zaměřením

na oblasti příjmu, vyřizování, ukládání a odesílání elektronických dokumentů (referent, útvarová podatelna, výpravna, spisovna).

- Prohloubení znalostí při práci s modulem USU; praktické cvičení při práci s tímto modulem podle individuálních potřeb posluchačů, případně v méně využívaných oblastech (skupiny externích subjektů, trasy redistribucí a další.).
- Praktická cvičení (odpovědi na nejčastěji kladené dotazy a další).

Proškolení administrátora datové schránky

- Základní seznámení s legislativou a metodikou výkonu spisové služby ASAS na MO.
- Seznámení s prostředím a ovládáním ISDS a administrace DS.
- Praktická cvičení (odpovědi na nejčastěji kladené dotazy a další).

Proškolení *zaměstnanců realizující autorizovanou konverzi* (tzv. zaměstnanců RAK):

- Základní seznámení s možnostmi SW/HW.
- Seznámení s metodikou výkonu spisové služby.
- Evidence konverzí (technologie, nástroje možnosti).

Tematické *účelové semináře zaměstnanců*:

- Význam a přínos ASAS.
- Legislativní požadavky.
- Interní normy metodika.
- Možnosti a nástroje ASAS.

Sebevzdělávání (samostudium):

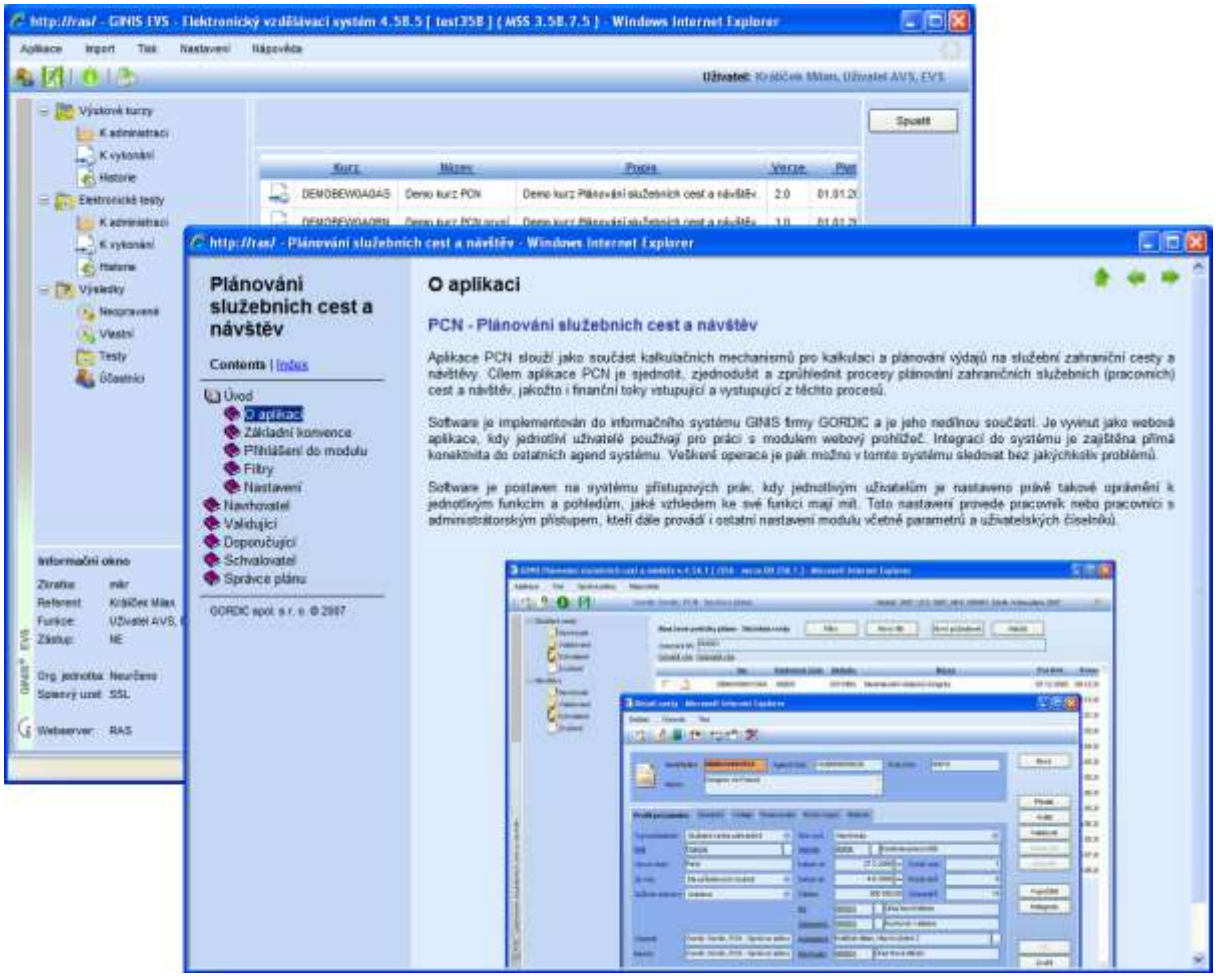
- Procesní scénáře.
- Metodická doporučení.
- Dokumentace.
- Elektronické vzdělávací kurzy.

Školení uvedené v tomto bodu a realizace účelových tematicky zaměřených seminářů (v průběhu roku 2010) doporučujeme realizovat vlastními silami zákazníka. Navržená školení mimo školení uvedeného v bodě 5 nejsou nezbytná, ale je vhodné je realizovat. V opačném případě musí být kladen větší důraz na dokumentaci a podporu koncových uživatelů.

Přístup k sebevzdělávání je doposud pasivní, tj. očekává se, že uživatel má snahu se sebevzdělávat. Doplňkem a aktivním prvkem sebevzdělávání je elektronický vzdělávací systém (modul EVS), který je složen z následujících částí:

- Výukové kurzy. Výuková podpora je postavena na elektronických kurzech (tzv. e-learningu), který přináší řadu výhod v oblasti vzdělávání. Tato vzdělávací technologie je založena na maximálním využití všech možných technických i didaktických opor a autorského vedení, které umožní studujícímu učit se samostatně a tempem, které odpovídá jeho aktuálním časovým možnostem. Součástí výukových kurzů společnosti GORDIC® jsou pracovní postupy, např. ve formě video ukázek nebo statického textu s náhledy obrazovek. Vše je podrobně vysvětleno na praktických příkladech v přímé souvislosti s metodikou nebo příslušnou legislativou.
- Elektronické testy. Prvkem navazujícím na výukové kurzy jsou elektronické testy, v nichž si uživatel ověří znalosti, které získal. Testy obsahují několik typů otázek, které lze mezi sebou libovolně kombinovat. Každý test může obsahovat i více pokusů, může být časově omezen apod. Pomocí algoritmu pro losování otázek do testu můžeme zajistit jedinečnost vybraných otázek a jejich pořadí pro každého testovaného uživatele. Variabilita, zajištěná obsáhlým nastavením elektronického testu, dává uživateli (školiteli) mnoho

možností, jak připravit test, vypovídající o reálných znalostech testovaných uživatelů. Tyto uživatele lze pak snadno, dle vybraných filtračních kritérií, přiřadit k danému testu. Další výhodou je automatická oprava testů, která zrychluje celý vzdělávací proces a usnadňuje tak práci školitelům a autorům jednotlivých testů.



Obr. 13. Ukázka výukového kurzu

5.7 Podpora koncových uživatelů

Služby (jako např. systémové podpory APV, podpory v oblasti správy DB) a programové úpravy systému ASAS lze řešit pouze formou nakoupení této služby od výhradního držitele autorských práv. Realizaci podpory koncových uživatelů lze uskutečnit kombinací jednak vlastních sil zákazníka a jednak objednáním této služby u poskytovatele. [14]

Personální zajištění odborných činností:

- ***Administrátor systému***. Tato osoba musí mít včasný přístup k organizačním a personální datům, zajišťuje zejména: administraci systému ASAS, (modul ADM), trvalou správu administračních dat, správu číselníků, správu kartotéky externích subjektů (modul ADK), správu databáze systému v rozsahu běžné údržby Administrátor systému se musí účastnit školení administrátora systému.
- ***Ze strany MO je nutné zajistit minimálně 2 administrátory pro zajištění dostupnosti této služby a zastupitelnosti***.
- ***Konzultant spisové služby***. Tato osoba musí dobře znát metodiku vedené spisové služby, velice dobře ovládat praktické činnosti v modulech spisové služby a zajišťovat zejména: sběr připomínek uživatelů a jejich vyhodnocování, školení spisové služby pro uživatele. Je vhodné, aby konzultant spisové služby se účastnil uživatelských školení.

Domnívám se, že je nutné zajistit minimálně 1-2 konzultanty na OC v závislosti na velikosti OC, zejména pro plynulý rozjezd a zajištění individuálních konzultací s uživateli.

5.8 Hardware

Hlavní důraz při výběru vhodného hardwaru a softwaru se kladu na celkovou vhodnost nasazení v kombinaci s budoucí možnou rozšiřitelností dle potřeb MO. Dále je při výběru vhodných technologií kladen důraz na jednotnost prostředí, možnosti servisního zabezpečení a celkovou redundanci všech hlavních komponent řešení. [12] [14]

Návrh vychází zejména ze skutečnosti, že nasazením systému ISDS razantně stoupne množství elektronické komunikace MO s okolím.

Při cca 3000 příchozích dokumentech denně se očekává, že po rozběhnutí systému bude 70 procent z nich zasláno přes datovou schránku. Při průměrné velikosti elektronického dokumentu 200 kB se jen u vlastních dokumentů jedná o denní nárůst cca 0,5 GB, což při uvažování metadat, provozních kopií dělá nárůst cca 2 GB denně, 750 GB ročně. Dále vzrostou nároky na stabilitu a bezpečnost informačních systémů, které budou

zpracovávat dokumenty procházející datovými schránkami, a to v obou směrech komunikace. Důležitým parametrem je také stabilita komunikační infrastruktury.

Z výše uvedeného vyplývá, že je třeba zajistit:

- Stabilní provozní prostředí, které je schopno eliminovat rizika výpadků.
- Dostatečnou kapacitu diskového pole.

5.8.1 Architektura řešení

Řešení přístupu ke spisové službě se skládá z následujících částí:

- Databázové servery v clusteru.
- Datové úložiště.
- Úložiště dokumentů.
- Aplikační servery.
- Terminálová farma.
- Záložní lokalita.
- Testovací a školící prostředí.

Základními parametry navrhovaného řešení jsou:

- Vysoká dostupnost.
- Robustnost.
- Rozšiřitelnost.
- Ochrana investic.

Databázovou platformu doporučuji budovat plně 64bitovou robustní architekturou. Plně redundantní hardware s možností online servisovatelnosti a rozšiřitelnosti serveru za běhu operačního systému od úrovně disků, systémových zdrojů a ventilátorů až po redundantní připojení serverů k datovým sítím (LAN i SAN) zjednodušuje správu a minimalizuje servisní odstávky. Jak databázové servery, tak servery pro přenos dat doporučuji stejné či obdobné technologie z důvodů nižších nákladů při správě prostředí.

Na servery zajišťující přenos dat ovšem nejsou kladeny takové nároky na výpočetní výkonnost a jejich dodatečné rozšiřování jako na databázové.

Vzhledem k požadavku na dostupnost celého řešení se předpokládá implementace serverů do clusterového prostředí. Databázový cluster může být nasazen v typu active-active, tj. databázová aplikace běží v reálném čase paralelně na obou uzlech cluster, nebo v typu active-pasive, tj. databázová aplikace běží pouze na jednom uzlu cluster a v případě problému automaticky nebo manuálně migruje na druhý zdravý uzel.

Clusterový framework musí podporovat nebo být rozšiřitelný na geocluster tak, aby byla zajištěna dostupnost i v případě výpadku lokality. V tomto případě musí umožňovat testování krizových scénářů bez dopadu na produkční prostředí nebo konfiguraci záložní lokality.

Pro připojení serverů k datové síti Ethernet musí mít servery vhodný počet portů a celková topologie musí být plně redundantní.

Propojení serverů, diskových polí a zálohovací knihovny doporučuji realizovat technologií SAN s přenosovým protokolem FibreChannel. Jde o jedinou vhodnou možnost propojení třídy Enterprise v dnešní době s rychlostí přenosu 4Gbps. Samozřejmostí je vybudování plně redundantní topologie SAN sítě s neblokovanou rychlostí přenosu pro všechny členy sítě rychlostí 4Gbps a s podporou připojení všech komponent duální cestou.

Pro zálohování celého systému doporučuji využít některý z Enterprise zálohovacích Softwarů. Samozřejmostí je podpora Online zálohování databází, operačních systémů s možností jejich rychlé obnovy a dalších komponent řešení a šifrování dat. Vhodná je také podpora záloh z kopií vytvořených diskovým polem tak, aby dopad na provoz byl minimální.

Zálohovací knihovnu je možné zvolit s připojením do SAN sítě a minimalizovat tak zpoždění a přenosy dat po Ethernet síti. Vše se bude zálohovat přímo po rychlé SAN síti. Knihovna by měla mít nejméně dvě zálohovací mechaniky a nabízet dostatečnou rozšiřitelnost jak kapacity, tak propustnosti. Rozšiřování kapacity a propustnosti nemá být realizováno přidáváním nových nezávislých knihoven, ale rozšiřováním slotů a mechanik na „jednom robotu“. [14]

5.8.2 Nároky na komunikační datovou síť

Popisovaný informační systém předpokládá využití architektury tlustého klienta v kombinaci s terminálovým klientem Citrix XenApp. Provozní bezpečnost (zejména dostupnost IS) navrhujeme podpořit využitím clusterového řešení.

Standardně se budou klientské stanice připojovat k serverům hlavní lokality. V případě výpadku hlavní lokality budou přesměrovány na servery záložní lokality.

5.8.3 Eliminace rizik v oblasti zabezpečení náhradního provozu

Z technického hlediska mohou nastat zejména tyto rizikové situace:

- Výpadek dodávky el. proudu.
- Výpadek síťové konektivity.
- Výpadek databázového serveru.
- Výpadek serveru úložiště elektronických dokumentů a serveru pro fulltext.
- Výpadek diskového pole.
- Chyba uživatele.

Tab. 1. Návrhy opatření pro eliminaci rizik

Riziko	**Bezpečnostní opatření**	**Upřesnění**
Výpadek dodávky el. proudu	Použití záložních baterií	UPS
	Použití záložních zdrojů el. proudu	diesel-agregáty
	Využití alternativního dodavatele el. energie	je-li to v dané lokalitě možné
Výpadek síťové konektivity	Zdvojení komunikačních kanálů	Vybudování záložních datových linek
	Zdvojení aktivních prvků	
	Zdvojení síťových adapterů serverů	

Výpadek databázového serveru	Clusterové řešení	Použití clusteru v režimu active-active pro hlavní lokalitu, cluster active-passive mezi hlavní a záložní lokalitou
Výpadek serveru úložiště elektronických dokumentů a serveru pro fulltext	Clusterové řešení	Použití clusteru v režimu active-active pro hlavní lokalitu, cluster active-passive mezi hlavní a záložní lokalitou
Výpadek diskového pole	Použití diskového pole podporujícího snapshot zálohy	
	Provozní zálohování dat pole na jiná média (záloha D2D, D2D2T)	
Chyba uživatele	Možnost obnovy dat ze záloh	Obnova ze snapshot záloh diskového pole, případně z provozních záloh

5.8.4 Využití geoclusteru pro bezpečné provozování systému GINIS-SSL (ASAS)

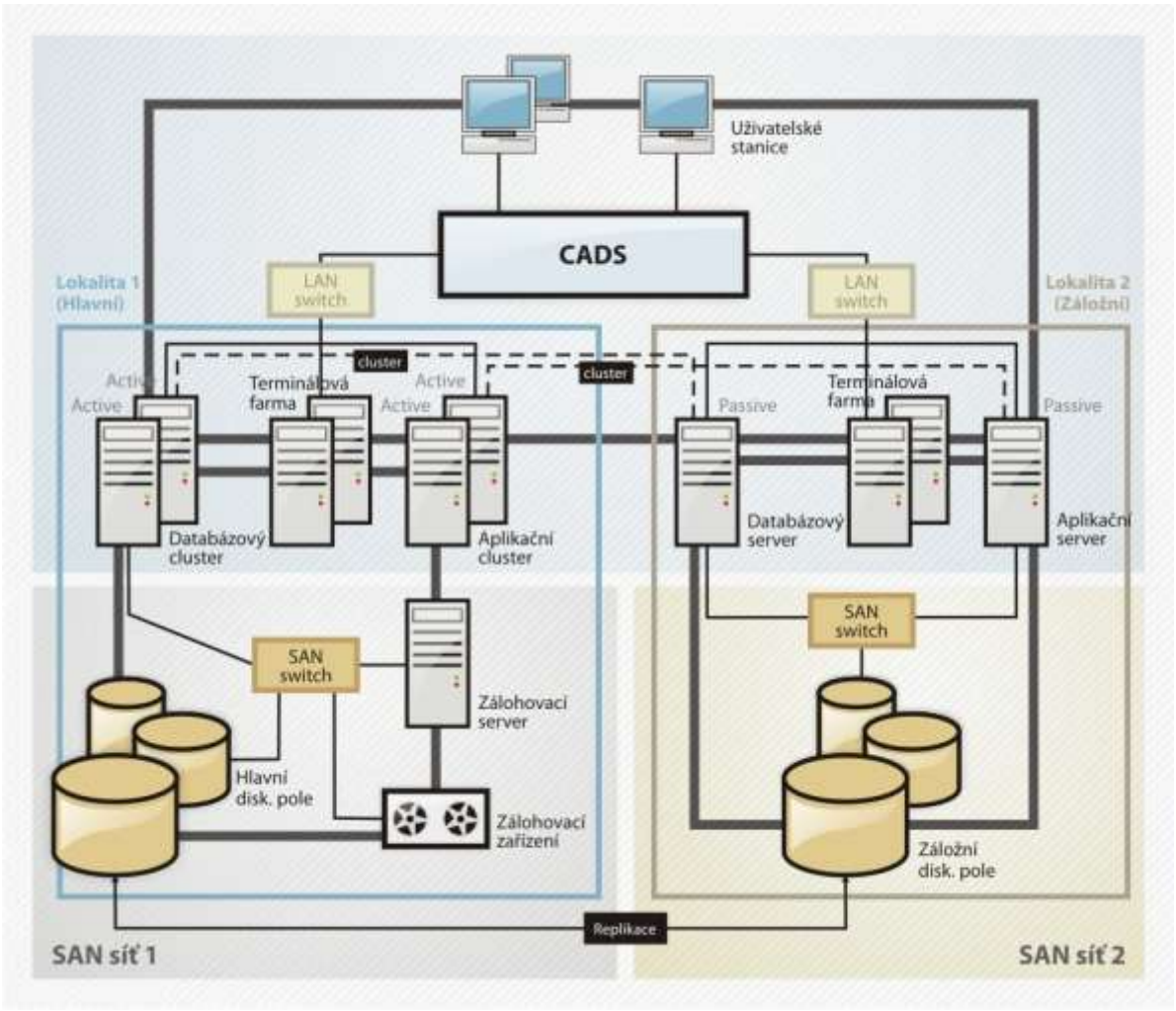
Jelikož ***systém GINIS-SSL je základem elektronické spisové a archivní služby MO, je třeba zajistit, aby bylo dosaženo maximální dostupnosti tohoto systému*** pro uživatele ASAS.

Jedním z důležitých nástrojů pro vysokou dostupnost systému je využití techniky clusterů. Navrhuji servery pro provoz systému GINIS-SSL rozložit do dvou lokalit. V obou lokalitách navrhuji vybudovat infrastrukturu sítě pro ukládání dat zpracovávaných v informačním systému.

V hlavní lokalitě navrhuji pro jednotlivé klíčové servery (tj. databázový a aplikační server) vytvořit clusterové řešení pracující v režimu active-active. Vedle nich navrhuji instalovat diskové pole a zálohovací systém.

V záložní lokalitě, která bude využívána v případě výpadku hlavní lokality, navrhuji instalovat pro jednotlivé technologické komponenty samostatné servery. Tyto servery pak

budou vůči odpovídajícím clusterům v hlavní lokalitě pracovat v režimu active-passive. Diskové pole v záložní lokalitě bude synchronizováno s polem v hlavní lokalitě prostřednictvím replikačních mechanismů. [14]



Obr. 14. Schéma využití geoclusteru v prostředí AČR

5.8.5 Stanovení požadavků na centrální úložiště elektronických dokumentů

Informační systém GINIS-SSL využívá pro ukládání elektronických obrazů a příloh dokumentů úložiště umístěná mimo relační databázi. Výběr vhodného typu úložiště závisí na mnoha okolnostech konkrétního prostředí implementace. Technologicky je úložiště od vlastního kódu aplikace odděleno specifickým konektorem. To umožňuje implementovat rozhraní na další typ úložiště elektronických dokumentů bez nutnosti zásahu do vlastní aplikace. [14]

Pro efektivní využití již vynaložených prostředků v prostředí AČR připadají v úvahu zejména tyto technologie:

WS Gordic

+ Momentálně reálně využívaná varianta v rámci ASAS

+ Technologická nenáročnost

- Slabší výkon

- Standardně bez možnosti fulltextového vyhledávání

Hitachi HCAP

+ Umožňuje fulltextové vyhledávání

+ Vysoký výkon

+ Kvalitní zabezpečení dostupnosti

- Technologicky komplikovanější, vyžaduje speciální technologie (jež AČR vlastní)

V požadavcích na centrální úložiště je nutné brát v potaz rozšiřitelnost kapacity diskových prostorů pro ukládání elektronických dokumentů v závislosti na růstu velikosti ukládaných elektronických dokumentů v čase. Tyto elektronické dokumenty jsou v systému ASAS užity jako elektronické obrazy evidovaných dokumentů anebo jako elektronické přílohy těchto dokumentů.

Tab. 2. Skladba a velikost uložených dat

Typ	Velikost	Uložení
Evidenční karta dokumentu	1- 2kB	Relační databáze
Elektronický obraz nebo elektronická příloha	Jednotky kB až desítky MB	Elektronické úložiště

Zálohování centrálního úložiště elektronických dokumentů doporučujeme provádět na připojená disková pole standardními nástroji zálohovacího serveru a zároveň na datová média konkrétního páskového zařízení s příslušným softwarem i pro případnou obnovu z těchto pásek. [14] [18]

5.8.6 Organizační a personální opatření

K zabezpečení dopadů zákona č. 300/2008 Sb. z hlediska personálních zdrojů bude třeba zohlednit zejména tyto skutečnosti: [14] [21]

- zřídit pracoviště centrální elektronické podatelny a výpravny MO pro DS;
- zřídit pracoviště autorizované konverze;
- zajistit příjem a zpracování na OC;
- vyškolit interní školitele a konzultanty ASAS se zaměřením na oblast DS;

V souvislosti s nárůstem počtu uživatelů a specifické části agendy:

- vyškolit pracovníky metodického HelpDesk v oblasti specifik obsluhy ASAS-DS;
- vyškolit pracovníky technologického HelpDesk v oblasti specifik provozu ASAS-DS;
- zvýšené nároky na metodické pracoviště ASAS na OB MO;
- zvýšené nároky na pracoviště hlavního administrátora ASAS;

Základní role ASAS v souvislosti s řešením dopadů zákona č. 300/2008 Sb.:

- ***Pracovník centrální elektronické podatelny a výpravny MO pro DS*** – zabezpečuje příjem, zpracování, prvotní registraci a ověření doručeného elektronického podání, jeho distribuci na interní řešitele a vypravování odpovědí.
- ***Pracovník autorizované konverze*** – zabezpečuje realizaci autorizované konverze dokumentů.

- ***Metodik spisové služby*** – musí mít dostatečnou pravomoc k prosazení metodiky spisové služby a to zejména s ohledem na dopad zákona 300/2008 Sb. Musí ovládat praktické činnosti v modulech spisové služby a zajišťovat zejména: průběžnou metodickou údržbu a podporu ASAS, průběžný styk se zástupci uživatelů systému, průběžnou aktualizaci interních norem (zejména Spisového a skartačního řádu a plánu) a dokumentace systému, metodická školení školitelů spisové služby.
- ***Lektor spisové služby*** – musí dobře znát metodiku vedení spisové služby, velice dobře ovládat praktické činnosti v modulech spisové služby a zajišťovat zejména: sběr připomínek uživatelů a jejich vyhodnocování, účelové semináře a odborná školeni (a to i individuální školení) pro uživatele.
- ***Administrátor systému*** - musí mít včasný přístup k organizačním a personální datům, zajišťují zejména: administraci systému ASAS, (modul ADM), trvalou správu administračních dat, správu číselníků, správu kartotéky externích subjektů (modul ADK), správu databáze systému v rozsahu běžné údržby.
- ***Mentor spisové služby*** (zástupce uživatele) - tito pracovníci jsou velmi zkušení uživatelé spisové služby, kteří poskytují podporu a rady ostatním uživatelům. Musí velmi dobře znát obsluhu všech uživatelských modulů, dobře znát metodiku vedené spisové služby a ovládat základní souvislosti v administraci systému.
- ***Kontrolor spisové služby*** - Tito pracovníci jsou velmi zkušení uživatel spisové služby, musí dobře znát metodiku vedené spisové služby, velice dobře ovládat praktické činnosti v modulech spisové služby a kontrolovat zejména: metodickou správnost výkonu uživatelů v ASAS, průběžnou kontrolu a aktualizaci interních norem (zejména Spisového a skartačního řádu a plánu) a dokumentace systému, metodická školení uživatelů spisové služby. Pozici kontrolora je možné výhodně kombinovat s pozicí mentora, případně kapacity mezi těmito pozicemi operativně přelévat podle potřeby a etapy nasazení.

5.8.7 Analýza finanční náročnosti

Výši finančních nároků lze ovlivnit rozsahem realizace, včasností objednávky, plněním sjednaného harmonogramu projektu řešení a v neposlední řade i mírou součinnosti objednatele. Ceny licencí a souvisejících služeb stanoví obchodní zástupce GORDIC pro resort MO dle aktuálního ceníku GORDIC spol. s r. o. na základě definice rozsahu a hloubky poptávaného řešení.

Předpokladem řešení je zajištění galvanického bezpečného propojení mezi systémem datových schránek a ASAS (sítě internet a intranet) včetně zabezpečení odpovídajících HW provozních prostředků ASAS. Dalším předpokladem je plošné nasazení ASAS v rámci MO alespoň v minimálním rozsahu (POI + VEL / ŘED) na všech uvažovaných útvarech s požadavkem na připojení k systému DS. [14] [20]

Minimální doporučený rozsah komponent pro řešení dopadů zákona č. 300/2008 Sb. na resort MO:

Interface na informační systém datových schránek (ISDS) zahrnuje rozšíření ASAS o oblasti:

- Rozšíření funkčnosti podatelny ASAS o interface na ISDS (předpoklad – zřízení centrálního příjmového místa).
- Vazba kartotéky externích subjektů ASAS na datové schránky.
- Rozšíření funkčnosti výpravny ASAS o interface na ISDS (předpoklad – zřízení centrálního vypravovacího místa).
- Administrace přístupu ASAS k ISDS.
- Využití elektronického podpisu v ASAS ve vztahu k ISDS.

Konverzní pracoviště pro zajištění autorizované konverze zahrnuje rozšíření ASAS o oblast:

- Konverzní pracoviště pro autorizovanou konverzi.

Návrhy změn interních norem:

- Změny ve Spisovém a skartačním řádu MO a příp. dalších souvisejících interních normách.

Metodika zahrnuje rozšíření ASAS o oblast:

- Metodika zacházení s dokumenty v elektronické podobě, tvorba workflow elektronických dokumentů.

Neautorizovaná konverze dokumentů zahrnuje rozšíření ASAS o oblast:

- Centrální skenovací pracoviště / digitalizace dokumentů.

Hardware

- Architektura řešení.
- Nároky na komunikační datovou síť.
- Eliminace rizik v oblasti zabezpečení náhradního provozu.
- Využití geoclusteru pro bezpečné provozování systému GINIS-SSL (ASAS).
- Stanovení požadavků na centrální úložiště elektronických dokumentů.

Úložiště elektronických dokumentů

- Rozšíření úložiště elektronických dokumentů ASAS, DMS.

Podpora elektronického úřadování zahrnuje rozšíření ASAS v oblastech:

- Avizační a událostní systém.

6 ZHODNOCENÍ DOSAŽENÝCH VÝSLEDKŮ

Z hlediska zhodnocení celé služby a posouzení dle nároků a potřeb Ministerstva obrany je možné jako nejvhodnější referenci uvést vzorovou implementaci GINIS® –SSL na Ministerstvu vnitra a to včetně pilotního rozšíření GINIS® –SSL o úplnou podporu práce s datovou schránkou a činnostmi souvisejícími s autorizovanou konverzí dokumentů dle požadavků zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů. Tato implementace je vystavena okamžitému a nejpřísnějšímu dohledu ze strany legislativního garanta zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů a zákona č. 499/2004 Sb. o archivnictví a spisové službě. [9] [14]

Tisková zpráva

GORDIC® jako první komunikuje s datovými schránkami

Jihlava, 11.5.2009. Informační systém GINIS® SSL společnosti GORDIC® je prvním systémem spisové služby, který prošel úspěšně testy na komunikaci s datovými schránkami. Testování probíhá od 1. května na testovacím pracovišti Ministerstva vnitra ČR. Ministerstvo bylo spolu s dalšími 11 subjekty zařazeno do pilotního testu informačního systému datových schránek (ISDS) a systém GINIS® provozuje od roku 2008 v rámci projektu Elektronické spisové služby (eSS).

V průběhu pilotního testu na ministerstvu byly v uplynulém týdnu ověřeny funkce spojené s napojením spisové služby na ISDS, především pak přihlášení, odeslání a příjem zpráv do a ze systému datových schránek. Testování dalších rozšíření a pomocných funkcí, jako jsou například kontrola stavu doručení, přehled odeslaných nebo přijatých zpráv, nyní probíhá. Systém prokázal při testech očekávanou funkčnost.

K rychlé a úspěšné realizaci vazby přispělo předchozí testování GINIS® SSL na firemním simulátoru datových schránek. Simulátor dokázal pro účely testování nahradit všechny funkce skutečného ISDS, a tak bylo možné systém s předstihem připravit na ostré napojení.

GORDIC spol. s r. o.

Společnost GORDIC® je největším dodavatelem specializovaných informačních systémů pro oblast státní správy a samosprávy - její softwarové aplikace a služby využívá více než 6000 organizací.

Problematice řešení spisové služby se firma intenzivně věnuje již od roku 1991. Její systém Spisové služby GINIS®-SSL v současnosti používá např. Ministerstvo obrany ČR, Kancelář prezidenta republiky, Ministerstvo vnitra ČR, Ministerstvo průmyslu a obchodu, Magistrát hlavního města Prahy, Kancelář veřejného ochránce práv, osm krajských úřadů a řada dalších významných úřadů a organizací. [14]

6.1 Zhodnocení jednotlivých nabízených funkcí ASAS

- Funkce elektronického pracoviště ochrany informací (POI).

  Ano, GINIS®-SSL splňuje všechny funkce zabezpečované na pracovišti POI.

- Jednotnou registraci písemností došlých i v resortu MO vzniklých (přidělení jednoznačné identifikace a základních registračních údajů) a následnou evidenci písemností (vložení potřebných údajů do písemnosti, zadání dalších evidenčních údajů).

  Ano, tento požadavek je splněn. Každý došlý i v resortu vzniklý dokument je označen jednoznačnou identifikací, pod kterou je v systému zaregistrován (zadány základní identifikační údaje) a dále zaevidován (zadání dalších specifických evidenčních údajů o dokumentu). Systém je koncipován jako centralizovaný s možností decentrálního pořizování dat. To umožňuje výkon jednotné metodiky archivní a spisové služby a současně posílení osobní zodpovědnosti za evidenci a správu vlastních dokumentů.

- Jednotnou identifikaci písemností po celou dobu životnosti v resortu MO i při archivaci v rámci ASAS použitím jednoznačného identifikátoru v rámci celého resortu MO, kompatibilního s identifikátory používanými ekonomickými systémy (aplikacemi).

- *Ano, tento požadavek je splněn. Jednoznačná identifikace každého dokumentu je jedním z pilířů nabízeného systému GINIS®-SSL. Tento*

identifikátor vystupuje jako „rodné číslo" dokument, je neměnný po celou dobu životního cyklu dokumentu (od vzniku až po skartaci resp. archivaci), díky jednoznačné licenci je zaručena unikátnost nejen v rámci resortu, ale i v rámci všech ostatních provozovatelů tohoto systému. Ekonomické aplikace v resortu MO jsou také součástí (subsystémy) informačního systému GINIS® a proto kompatibilita používaných identifikátorů je samozřejmostí a přirozenou součástí nabízeného řešení.

- Evidenci písemností v souladu se zákonem č. 148, vyhláškou NBÚ č. 137/2003 Sb., o podrobnostech stanovení a označení stupně utajení a o zajištění administrativní bezpečnosti, a to písemností jak v „papírové", tak v elektronické podobě.

  Ano, tento požadavek je splněn. Nabízené řešení pracuje rovnocenně s papírovými i elektronickými dokumenty a umožňuje evidenci v souladu se zákonem č.148/1998 Sb. a vyhláškou NBÚ č. 137/2003 Sb.

- Podporovat práci s neutajovanými i utajovanými písemnostmi v souladu s interními normami resortu MO.

  Ano, tento požadavek je splněn, systém umožňuje pracovat s utajovanými i neutajovanými dokumenty. Systém jako celek (včetně HW, přístup osob atp.) musí však také splňovat odpovídající bezpečnostní požadavky pro práci s utajovanými dokumenty.

- Zabezpečit rovnocennou registraci a evidenci všech písemností včetně jejich řízeného oběhu – Workflow.

  Ano, tento požadavek je splněn. Systém přistupuje z pohledu registrace, evidence, oběhu, vyřizování i skartace naprosto rovnocenně ke všem dokumentům – došlým či vlastním ale i např. papírovým či elektronickým. GINIS®-SSL obsahuje vlastní workflow – řízený oběh všech dokumentů se stanovením jednoznačné osobní zodpovědnosti v reálném čase.

- Řízený proces toku a schvalování písemností uvnitř organizačního celku podle předem definovaných kritérií s možností definování stálých a dočasných vazeb pro zastupování.

  Ano, tento požadavek je splněn. Systém nabízí řízení toku dokumentů během procesu vyřizování s možností definice předání na organizační celek, funkční místo nebo konkrétní osobu s možností definice vzájemných zástupů. Stanovení toku dokumentu nebo zástupů osob je možné realizovat centrálně pro skupinu dokumentů nebo jednotlivě pro jednotlivé dokumenty. Zástupy je možné pružně měnit podle aktuálních potřeb resortu.

- Možnost definování stálých a dočasných práv na písemnost (delegování práva například formou přidělení písemnosti k řešení).

  Ano, tento požadavek je splněn. V systému je možné jednoznačně delegovat práva k dokumentu – zejména přidělením dokumentu k řešení (definice vlastníka dokumentu). Nový vlastník dokumentu jej může definovaným a jednoznačným způsobem převzít (např. pomocí e-podpisu) a tím nezpochybnitelně přebírá zodpovědnost za tento dokument od původního vlastníka. Současně lze definovat okruh dalších osob, které mohou mít k dokumentu přístup v různých úrovních (pouze čtení, zápis evidenčních údajů…).

- Jednoznačně zaznamenávat historii každého dokumentu (záznam realizovaných změn), obsahující datum a čas, jméno a funkce osoby a charakteristika realizované změny. Historie musí být uživatelsky nezávislá a neměnná (auditovatelná).

  Ano, tento požadavek je splněn. Pro každý dokument je uživatelsky neměnným způsobem zaznamenávána historie, ve které je vždy záznam o provedené změně, časovém okamžiku a osobě, která změnu realizovala. Historie je uživatelsky zobrazitelná pro každý dokument, zápisy jsou však realizovány automaticky systémem bez možnosti uživatele do tohoto procesu zasahovat.

- Umožnit současnou práci s více jednacími protokoly.

Ano, tento požadavek je splněn. Tvorba, správa a přiřazení přístupových práv k jednacím protokolům je plně záležitostí centrální uživatelské administrace systému. S více jednacími protokoly je možné pracovat současně.

- Umožnit vedení několika oddělených evidencí u jednoho organizačního celku (neutajované, utajované, NATO atd.) a garantovat jednoznačné osobní vlastnictví každého dokumentu v čase s řízeným předáváním dokumentů předdefinovaným způsobem.

  Ano, tento požadavek je splněn, viz již body výše. Je možné vést více samostatných evidencí u jednoho organizačního celku, současně pro každý dokument jednoznačně sledovat osobní vlastnictví a tím i zodpovědnost za dokument a řídit oběh dokumentů (workflow).

- Možnost vedení oddělených evidencí za více samostatných součástí na jedné pracovní stanici (centrální POI), s jednou přihlašovací procedurou (vytvoření oddělených virtuálních skupin s jasně definovanou odpovědností a strukturou). Požadavek vyplývá z právní subjektivity jednotlivých organizačních celků.

  Ano, tento požadavek je splněn. Systém umožní vytvoření stromových organizačních struktur s jednoznačně definovanou zodpovědností a strukturou a přístup centrální POI k těmto jednotlivým celkům z jedné stanice pod jedním přihlášením.

- Možnost přenesení odpovědnosti za správnou evidenci na referenty – vyřizovatele písemnosti u centralizovaných POI.

  Ano, tento požadavek je splněn. Systém nijak neomezuje delegování zodpovědnosti za správu dokumentů na referenty, naopak předpokládá rozložení jednotlivých činností (registrace, evidence, vyřizování, skartace…) právě na osoby, které tuto činnost reálně vykonávají. Referent má tedy k dispozici všechny výkonné i kontrolní nástroje pro správu svých dokumentů.

- Zabezpečit řízení přístupu (bezpečnostní funkce) k informacím uloženým v systému ASAS a ke konkrétním činnostem administrovanými přístupovými právy – auditování veškerých činností.

  Ano, tento požadavek je splněn. Přístup do systému i ke konkrétním činnostem je důsledně řízen přístupovými právy, které jsou centrálně administrovány. Uživatelský přístup je logován a tím je umožněno auditování konkrétních činností v systému.

- Vazbu systému ASAS minimálně na kancelářský systém MS Office, případně Software 602, zejména možnost generování dokumentů MS Word z evidenční karty písemnosti ASAS s předvyplněním evidenčních údajů, automatickou evidenci e-mailových zpráv v ASAS a možnost generování e-mailových zpráv ze systému ASAS.

  Ano, tento požadavek je splněn. Systém je integrován s kancelářským balíkem MS Office. Z evidenční karty každého dokumentu je možné např. generovat elektronický dokument pomocí šablon MS Word s předvyplněním požadovaných evidenčních údajů (správu a tvorbu šablon si může realizovat zákazník sám), generovat e-mailovou zprávu s volitelným obsahem příloh, je možné automatizovaně nebo uživatelsky evidovat v systému GINIS®-SSL došlé e-mailové zprávy atp.

- Možnost snadného dohledání dokumentů na základě znalosti jejich obsahu nebo částečné znalosti některého z evidenčních údajů v celé databázi systému ASAS podle různých kritérií.

  Ano, tento požadavek je splněn. Systém GINIS®-SSL obsahuje velmi silné vyhledávací a kontrolní nástroje, pomocí kterých je možné dohledat dokument nebo skupinu dokumentů na základě alespoň zlomkové znalosti některého z evidenčních údajů či datového rozsahu. Vyhledávací kritéria lze téměř libovolně křížit či seskupovat a rozšiřovat. Vyhledávací masku lze uložit pro rychlé opětovné použití v budoucnu. Kromě toho systém nabízí již vytvořené nejčastěji používané přehledy a sestavy k rychlému nahlédnutí nebo vytištění.

- Zabezpečit řízenou manipulaci s vyřízenými dokumenty a jejich systematické ukládání na pracovišti ochrany informací, evidence zápůjček, automatizované generování skartačních návrhů podle přiřazených skartačních znaků a roků skartačního řízení.

  Ano, tento požadavek je splněn. Systém obsahuje kompletní správu vyřízených dokumentů až po skartační řízení. Umožňuje systematické ukládání vyřízených dokumentů ve spisovnách (na pracovišti POI) podle zadaných spisových znaků, skartačních znaků a lhůt, a také správu uživatelsky vytvářených úložných míst, které je možné členit podle budov, místností, polic i menších celků. Dále nabízí sledování zápůjček i automatické generování archivní knihy podle zadávaných údajů. Podle zadaných skartačních znaků a lhůt jsou automaticky generovány skartační návrhy, které je možné ještě uživatelsky zpracovat (např. rozdělení dokumentů V na A a S).

- Možnost rozšíření systému ASAS o pracoviště pro digitalizaci písemností s automatickou registrací digitalizovaných písemností v systému ASAS a navázání elektronického obrazu (digitální podoby písemnosti) na evidenční kartu příslušné písemnosti.

  Ano, tento požadavek je splněn. Systém je možné rozšířit o skenovací linku, která umožňuje automatizovanou digitalizaci a následnou registraci dokumentů v GINIS®-SSL. Skenovací linka může být využita pro „prosté" oskenování a navázání elektronického obrazu k automaticky zaregistrované evidenční kartě dokumentu, nebo může být oskenovaný dokument dále rekognifikován do textové formy, případně může být ještě vytěžen obsah dokumentu a vytěžená data následně využita jako evidenční údaje při registraci a evidenci dokumentu. Skenovací linka je integrální součástí nabízeného systému a rozsah jejího nasazení je záležitostí konkrétní specifikace.

- Realizaci funkce elektronické podatelny v souladu s nařízením vlády č. 304/2001 Sb., kterým se provádí zákon č. 227/2000 Sb. jako součást

systému ASAS a požadavek na certifikát e-podatelny o shodě s požadavky Standardu ISVS.

Ano, tento požadavek je splněn. Součástí nabízeného řešení je také elektronická podatelna, která je integrální součástí GINIS®-SSL. Dokumenty podané prostřednictvím e-podatelny jsou automaticky také zaregistrovány v systému a dále se s nimi pracuje standardními mechanizmy jako s elektronickými dokumenty. E-podatelna je plně v souladu s platnou legislativou (Nařízení vlády č. 495/2004 Sb., které nahrazuje zrušené nařízení č. 304/2001 Sb., Zákon č. 227/2000Sb., Vyhláška 496/2004 Sb., o elektronických podatelnách). Systém GINIS®-SSL je certifikován na shodu s odpovídajícími standardy ISVS.

- Realizaci funkce elektronického podpisu uvnitř resortu MO.

  Ano, tento požadavek je splněn. Systém GINIS®-SSL obsahuje možnost práce s e-podpisem v souladu se zákonem č. 227/2000 Sb. a odpovídá Koncepci infrastruktury veřejného klíče v resortu obrany.

- Zabezpečit spolupráci s ostatními systémy, které provádí evidenci, na úrovni administračních dat i na úrovni práce s evidovanými písemnostmi (např. s ekonomickým systémem).

  Ano, tento požadavek je splněn. Nabízené řešení je součástí informačního systému GINIS® a přirozeně je tedy integrováno s ostatními subsystémy, které v resortu MO jsou již provozovány (zejména ekonomický subsystém a úkoly). Spolupráce s jinými informačními systémy je zabezpečena pomocí univerzálního otevřeného interface, který umožňuje oboustrannou výměnu dat ať již na úrovni administračních dat, tak i na úrovni evidovaných dokumentů.

- Zabezpečit návaznost (kompatibilitu) na funkce VÚA (správních archivů) a SW používaný v tomto archivu.

  Ano, tento požadavek je splněn. Systém umožňuje obecně výměnu dat a tím i integraci s jinými informačními systémy. Podmínkou je samozřejmě

alespoň rámcový soulad metodiky (způsob evidence a význam jednotlivých evidenčních údajů) těchto systémů.

- Snadnou modifikovatelnost dle požadavků resortu MO (typy a označování písemností, změny v legislativě).

  Ano, tento požadavek je splněn. Nabízený systém je legislativně závislým SW, je tedy pružně upravován podle platné legislativy v oblasti spisové služby. Díky tomu, že je systém důsledně modulární, je jeho nasazování možné po jednotlivých celcích, ať již z pohledu rozsahu, tak i funkčnosti. Centrální administrace GINIS®-SSL, kterou spravuje vyškolený administrátor systému, umožňuje pružně reagovat jak na organizační změny v resortu, změny v přístupových právech uživatelů či definici zástupů, tak i na měnící se nebo upřesňovanou metodiku vedení spisové a archivní služby (typy dokumentů, skartační znaky, způsoby vyřízení atp.)

- Identifikaci a autentizaci řešit s vazbou na adresářové služby a PKI resortu MO.

  Ano, tento požadavek je splněn.

- Buňkový systém (buňka = POI) s propojením jednotlivých buněk do uceleného systému s přiměřenou dobou aktualizace přírůstků.

  Ano, tento požadavek je splněn. Díky důsledné modularitě systému není problém s postupným nasazováním po jednotlivých „buňkách" a jejich následné provazování do uceleného jednotného systému. Při provázání buněk dojde k automatickému sjednocení nad společnou databází a společným workflow s okamžitým promítnutím změn kdekoliv v systému. (bude jedna databáze nebo více + sehrávání dat?)

- Možnost rozšiřování systémem postupného připojování dalších buněk.

  Ano, tento požadavek je splněn, viz předešlý bod. [14]

ZÁVĚR

Na základě posouzení možností resortu obrany, byla vyhodnocena jako nejlepší varianta zavedení systému pro podporu oběhu dokumentů nákup již hotových softwarových produktů, který bude vyhovovat požadavkům celého resortu. Resort obrany nedisponuje kapacitami pro vlastní vývoj aplikace a také vytvoření produktu na zakázku se jeví jako nákladné a zdlouhavé. Na trhu jsou dostupná hotová programová řešení pro tuto oblast.

Po posouzení vlastností a vhodnosti jednotlivých produktů, které včas reagují na legislativní změny zákonů, byl opětovně zvolen systém GINIS-SSL společnosti Gordic s. r. o. Po analýze stávajícího stavu práce s dokumenty v celém resortu, v rámci všech informačních systémů, byla navržena inovace struktury celého průřezového informačního systému a ta je podle výše uvedených pravidel nasazována do provozu. Po odstranění všech nedostatků, postupného zavádění a financování by měl plně průřezový systém s integrační vrstvou tvořenou spisovou službou ASAS a jejími aplikacemi být plně nasazen v roce 2012. Již dnes po několika měsících provozu je zřejmé, že systém Spisové služby přesahuje možnosti pouhé evidence dokumentů a zasahuje do všech oblastí resortu.

ZÁVĚR V ANGLIČTINĚ

Based on the assessment of the options the Defense Department, was evaluated as the best option to establish a system to promote circulation of documents, purchase ready-made software products that will meet the requirements of the department. MoD does not have capacity for custom application development and also create customized products appear to be costly and time consuming. Available on the market ready solution for this program area.

After examining the properties and suitability of each product to timely respond to legislative changes in the law, was re-elected system GINIS SSL GORDIC Company Ltd. After analyzing the current status of work with documents in the entire department within all information systems, innovation has been proposed structure of the whole cross - sectional information system and that under the above rules deployed into service. After removing all the shortcomings, the phasing and funding should be fully horizontal system integration layer Records Service ASAS and its applications to be fully deployed in 2012. Even now, after several months of operation, it is clear that the system of reference services beyond the capabilities of mere registration documents and extends to all areas of the resort.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. 1. vyd. Praha: ANAG, 2008. ISBN 978-80-7263-465-1.

[2] SMEJKAL, Vladimír. *Datové schránky v právním řádu ČR*. 1. vyd. Praha: ABF, a.s., 2009. ISBN 978-80-86284-78-1.

[3] TVRDÍKOVÁ, Milena. *Zavádění a inovace informačních systémů ve firmách*. 1. vyd. Praha: Grada, 2001. ISBN 80-7169-703-6.

[4] BITTNER, Ivan a kol. *Spisová a archivní služba ve státní správě, samosprávě a v podnikatelské sféře*. 3. vyd. Praha: Linde Praha a.s., 2005. ISBN 80-7201-549-4.

[5] JAŠEK, Roman a kol. *Informatika ve veřejné správě*. Zlín: Univerzita Tomáše bati, 2003. ISBN 80-7318-147-9.

[6] JANÍK, Zdeněk. *Implementace elektronické spisové služby na MěÚ Vsetín*. Zlín: Univerzita Tomáše Bati, 2008.

[7] Zákon č. 137/2006 Sb., *o veřejných zakázkách.*

[8] Zákon č. 227/2006 Sb., *o elektronickém podpisu.*

[9] Zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů.*

[10] Zákon č. 365/2000 Sb., *o informačních systémech veřejné správy.*

[11] Zákon č. 499/2004 Sb., *o archivnictví a spisové službě a o změnách některých zákonů.*

Internetové zdroje:

[12] Ministerstvo obrany ČR: *Působnost a činnosti* [online]. [cit. 2010-04-11]. Dostupný z WWW: <http://www.army.cz/>.

[13] Armáda ČR: *Armáda ČR - Struktura* [online]. [cit. 2010-03-22]. Dostupný z WWW: <http://www.army.cz/>.

[14] Gordic: *Gordic – Produkty* [online]. [cit. 2010-03-17]. Dostupný z WWW: <http://www.gordic.cz/portal/>.

[15] SEPO: *Elektronické tržiště MO – Informace o tržišti* [online]. [cit. 2010-02-16]. Dostupný z WWW: <https://sepo.army.cz/>.

[16] Ministerstvo informatiky ČR: *Výzkum počítačové gramotnosti ČR* [online]. [cit. 2010-03-08]. Dostupný z WWW: <http://www.micr.cz/>.

[17] Egovernment: *Schránky - otázky* [online]. [cit. 2010-04-08]. Dostupný z WWW: <http://www. egovernment.cz/schranky/otazky/5.htm />.

Interní zdroje:

[18] Štábní informační systém AČR: ŠIS [online]. [cit. 2010-02-13]. Dostupný z CADS: <http://www.sis.acr/>.

[19] Štábní informační systém AČR: ISL [online]. [cit. 2010-01-26]. Dostupný z CADS: <http://www.step.acr/>.

[20] Štábní informační systém AČR: FIS [online]. [cit. 2010-03-18]. Dostupný z CADS: <http://www.fis.acr/>.

[21] Informační systém o službě a personálu AČR: ISSP [online]. [cit. 2010-04-23]. Dostupný z CADS: <http://www.issp.acr/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

MO	Ministerstvo obrany.
AČR	Armáda České republiky.
NATO	North Atlantic Treaty Organisation – Severoatlantická aliance.
NAMSA	Maintenance and Supply Agency – Agentura pro údržbu a zásobování.
LOGFAS	Logistics Functional Area Sub-Systém – subsystém pro oblast logistiky NATO.
SHARE	Stock-Holding and Asset Requirements Exchange – výměna informací v ISL.
SE MO	Sekce ekonomická Ministerstva obrany.
IISSP	Integrovaného systému státní pokladny.
ISSP	Informační systém o službě a personálu.
SEPO	Systém elektronické podpory obchodování.
ISMP	Informační systém mobilizačních příprav.
ISL	Informační systém logistiky.
FIS	Finanční informační systém.
ŠIS	Štábní informační systém.
PRIS	Průřezový informační systém.
CADS	Celoarmádní datová síť.
IS	Informační systém.
VEL	Velitel.
OTS	Operačně-taktický systém.
KIS	Komunikační a informační systémy.
SGI	Flexibilní serverová platforma.
VeV-VA	Velitelství výcviku – Vojenská akademie.
VVP	Vojenský výcvikový prostor.
IS UO	Informační systém Univerzity Obrany.

DVISTÚ	Digitální vojenský informační systém o území.
INA	Interní normativní akty.
ČSSZ	Česká správa sociálního zabezpečení.
DS	Datové schránky.
SSL	Automatizovaná spisová služba.
GINIS®	GORDIC® – Integrovaný Informační Systém.
HW	Hardware.
SW	Software.
API	Application interface – Aplikační programové prostředí.
ISDS	Informační systém datových schránek.
ISZR	Informační systém základních registrů.
RÚIAN	Registr územní identifikace, adres a nemovitostí.
CP	Czech POINT.
DA	Digitální archiv.
ZR	Základní registr.
OC	Organizační celek.
KaMO	Kancelář Ministra obrany.
RAK	Registr autorizovaných konverzí.
SIP	Submission Information Package – Příslušný informační balíček.
POI	Pracoviště ochrany informací.
VÚA	Vojenský ústřední archiv.
NBÚ	Národní bezpečnostní úřad.
eSS	Elektronická spisová služba.
EVS	Elektronický vzdělávací systém.
OAIS	Open Archival Information Systém – Otevřený archivní informační systém.

SEZNAM OBRÁZKŮ

Obr. 2. Základní koncept architektury PRIS MO 27
Obr. 3. Základní blokové schéma SSL – popis cílového stavu [14] 30
Obr. 4. Integrace ASAS u jednoho organizačního celku 32
Obr. 5. Stávající databázové prostředí systému SSL 34
Obr. 6. Stávající databázové prostředí s úložištěm elektronických dokumentů systému SSL 35
Obr. 8. Blokové schéma vztahu ASAS k okolním systémům 71
Obr. 9. Schéma postupu konverze do dokumentu obsaženého v datové zprávě 76
Obr. 10. Schéma postupu konverze z dokumentu obsaženého v datové zprávě 77
Obr. 11. Skenovací linka 82
Obr. 12. Schéma zpracování doručení datových zpráv 87
Obr. 13. Ukázka výukového kurzu 91
Obr. 14. Schéma využití geoclusteru v prostředí AČR 97

SEZNAM TABULEK

Tab. 1. Návrhy opatření pro eliminaci rizik 95
Tab. 2. Skladba a velikost uložených dat 98