Formulář žádosti

o stanovisko Hlavního architekta eGovernmentu k plánovanému ICT projektu – typ A

Odbor Hlavního architekta eGovernmentu MV

Praha, leden 2019
verze 6.0.1

UPOZORNĚNÍ: Přestože je formulář zveřejněn ve formátu umožňujícím změny, žadatel není oprávněn měnit strukturu vybraných otázek, či předepsaných odpovědí. Pokud se tak stane, Odbor Hlavního architekta eGovernmentu vyhodnotí takovou změnu jako porušení pravidel při schvalování a formulář bude vrácen bez vydání stanoviska.

1. ZÁKLADNÍ PODMÍNKY PROJEKTU

1.1. Úvodní informace o žadateli o stanovisko k projektu

Tabulka 1: **Úvodní informace o žadateli projektu:**				
Organizace žadatele	Ministerstvo obrany ČR		Praha 6 Tychonova 1	60162694
Ředitel pro informatiku nebo Statutární zástupce	Mgr. ŽIKEŠ Josef	Ředitel Vojenského ústředního archivu Praha	zikesj@army.cz	973 213 301 606 620 020
Kontaktní osoba projektu	Ing. VRBENÍK Miroslav	Vedoucí oddělení informačních a komunikačních systémů	vrbenikm@army.cz	973 213 303 724 380 203
Architekt projektu	Ing. VRBENÍK Miroslav	Projektant informačních a komunikačních systémů	vrbenikm@army.cz	973 213 303 724 380 203
Datum vypracování žádosti:			28. 2. 2020	

Tabulka 2: **Druh žádosti (žádost o stanovisko dle):**	
Usnesení vlády č. 86 ze dne 27. ledna 2020, ve znění pozdějších předpisů	***Ano***
Zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů	***Ano***
Výzev v Integrovaném regionálním operačním programu (IROP), **vypište číslo výzvy**	*<číslo výzvy>*

1.2. Shrnutí charakteristik projektu

Tabulka 3: **Shrnutí charakteristik projektu:**	
Název projektu:	Digitální archiv MO – nákup
Hlavní předmět projektu:	Předmětem veřejné zakázky je zhotovení, dodání, instalace, předání, zaškolení a proškolování obsluhy, servis a legislativní upgrade systému „Digitální archiv MO“, který se skládá z následujících částí: softwarové licence, hardwarové komponenty, dokumentace DA MO, služby, záruční servis a technická podpora. Hlavním cílem projektu je řádná a bezpečná archivace zpracovaných fondů (klíčových historických archiválií) v souladu se zákonnými požadavky a jejich následné zpřístupnění badatelům i veřejnosti. Prostřednictvím jednotného uživatelského prostředí bude možné nahlížet do zpracovaných fondů, ve kterých se bude badatel orientovat prostřednictvím archivních pomůcek - inventářů, katalogů a soupisů. Dalším významným přínosem projektu je obrovský počin vůči veřejnosti, která prostřednictvím portálu Badatelny dostává možnost prohlížet ve velmi vysoké kvalitě digitalizované fondy vojenského dědictví spjaté s regionem a historií České republiky. Uložené klíčové historické archiválie může využívat badatel nebo veřejnost pro další badatelskou činnost a zároveň mohou být využity jako nedílná součást nástrojů odborné veřejnosti (vědečtí pracovníci). V rámci legislativních podmínek, platného znění autorského zákona, určujícího možnosti pro zveřejnění a zpřístupnění obsahu veřejnosti a citlivosti materiálu, dojde i k anonymizaci dokumentů. Nedílnou součástí archivu bude badatelská místnost, která umožní studium přímo v prostředí VUA k tomu vyhrazenému. Portál Badatelny bude uživatelům nabízet možnost komfortně vyhledávat dokumenty nebo archiválie na základě fulltextového vyhledávače, zadaného časového období nebo dle zařazení do kategorií (např. knihy, mapy, listiny apod.) a prohlížet je v různých režimech včetně jejich stažení nebo exportování do formátu PDF. Badatelnu archivu může navštívit každý zájemce o studium archiválií, který při své první návštěvě vyplní badatelský list a poté bude dbát pokynů badatelského řádu. Při dalším rozvoji archivu je záměrem poskytovat i placené služby veřejnosti (např. xerokopie černobílé i barevné, skenování dokumentů apod.), nebo příprava a zpracování odborných rešerší.

Tabulka 3: **Shrnutí charakteristik projektu:**			
Termín plánovaného zahájení realizace projektu (zahájení výstavby, je-li součástí)**:**			1. 5. 2020
Termín plánovaného dokončení realizace projektu (akceptace a uvedení do produkčního provozu)**:**			15. 9. 2020
Termín plánovaného zahájení provozu (spuštění produkčního provozu)**:**			1. 1. 2021
Termín plánovaného ukončení provozu (konec smluvního vztahu s dodavatelem)**:**			15. 9. 2025
Předpokládaný počet let využívání výstupů projektu (počet let od začátku využívání do konce využívání)**:**			Více než 5.
Možnost zveřejnění formuláře:	*Možno zveřejnit bez omezení*	**V případě požadované anonymizace (nebo nemožnosti zveřejnění) vypište údaje a úpravy, aby bylo zveřejnění možné (případně proč není možné):**	
Shrnutí shody se základními principy a standardy českého eGovernmentu:			
Žádáte výjimku(y)?	***Ne***	**Počet žádostí o výjimku v přílohách:**	
Komentář k výjimkám:			
Určení: věcného správce, technického správce a provozovatele (pokud je předmětem více IS, klasifikujte hlavní a ostatní vysvětlete v tabulce 8)			
Věcný správce:	**Vojenský ústřední archiv Praha**		
Technický správce:	**Vojenský ústřední archiv Praha**		
Provozovatel:	**Vojenský ústřední archiv Praha**		
Realizační (implementační) **výdaje v rámci projektu** (součet hodnot ve sloupci 1 tabulky 58 v kapitole 3.2.1) **v Kč bez DPH:**			**38,025 mil. Kč bez DPH.**
Provozní výdaje plánované v rámci projektu (součet hodnot ve sloupci 2 tabulky 58 v kapitole 3.2.1) **v Kč bez DPH:**			**19,000 mil. Kč bez DPH.**
5 letá TCO (součet hodnot ve sloupci 3 tabulky 58 v kapitole 3.2.1) **v Kč bez DPH:**			**57,025 mil. Kč bez DPH.**

1.3. Popis, potřebnost a výstupy projektu

Tabulka 4: **Popis projektu:**
Popis výchozí situace projektu (tzv. As-Is)**:**
DA MO bude realizován s přímou logickou, koncepční a technologickou návazností na ESA MO, jako jeho rozšíření. Z důvodů maximální ochrany investic je proto nutné v intencích navrženého řešení DA MO v co největší možné míře zachovat kontinuitu po stránce aplikačního programového vybavení i navrženého hardware. Vzhledem k očekávanému významu DA MO jsou stanoveny s ohledem na funkční a další požadavky tyto prerekvizity návrhu: • Z hlediska terminologie jsou elektronické soubory vstupující do DA MO nazývány jako dokumenty. Jakmile jsou uloženy v DA MO, stávají se z nich archiválie. • V DA MO budou dlouhodobě a trvale uloženy neutajované elektronické archiválie, které budou přijímány: - Z ESA MO – Elektronického správního archivu MO. Jedná se o archiv elektronických neutajovaných dokumentů pocházejících převážně ze správních činností, zejména z informačních systémů integrovaných s ESSS Defence a z informačních systémů bez integrace s ESSS Defence. Dokumenty jsou v ESA MO archivovány po středně dlouhou dobu, zpravidla od 6 do 30 let. Po uplynutí doby archivace v ESA MO se na základě archivního příznaku dokument přesune do DA MO nebo skartuje. - Z digitalizační linky provozované VHA. - Jednorázovou migrací ze systému Documentum, v němž jsou uloženy digitalizované archiválie. - Ručním vstupem na základě rozhodnutí archiváře.

Tabulka 4: **Popis projektu:**

- Dokumenty vstupující do systému DA MO musí mít platné prvky elektronického zabezpečení, aby mohly být ověřeny a DA MO mohl pokračovat v udržování jejich důvěryhodnosti.
- Systém DA MO udržuje důvěryhodnost a legislativní platnost archiválií pomocí mechanismu elektronické značky a časového razítka.
- Dlouhodobá a trvalá platnost prvků elektrického zabezpečení archiválií je udržována pomocí procesu přerazítkovávání archivních balíčků.
- Systém DA MO bude kontaktovat služby kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovatelů časových razítek v síti Internet pro potřeby ověřování platnosti kvalifikovaných certifikátů a označování archivních balíčků elektronických časovým razítkem.
- Pro dlouhodobé a trvalé uložení dat je využito úložiště splňující požadavky na dlouhodobé garantované uložení dat s funkcemi pro ochranu dat před ztrátou a změnou.

1.1 Funkční požadavky

- Systém DA MO zabezpečí dlouhodobou/trvalou garantovanou archivaci neutajovaných archiválií, které se do archivu přesunou:
  - ze systému ESA MO po uplynutí maximálně třiceti let od ukončení skartačního řízení u původce dokumentu. Dokumenty mohou být do DA MO přesunuty dříve, a to na základě skartačního znaku a lhůty, stanovené původcem. Přesun se koná na základě ukončeného skartačního řízení v ESA MO. Vstup dokumentů z ESA MO bude realizován na základě automatického návrhu ESA MO.
  - z digitalizační linky - po deseti letech digitalizace ve VHA je nutné celý proces upravit a zrychlit. Vybrané prvky digitalizační linky budou součástí dodávky DA MO a budou obsahovat technické prvky pro digitalizaci dokumentů a fotoarchivu.
- Systém DA MO umožní také manuální příjem dokumentů.
- Systém DA MO umožní příjem vstupních archivních balíčků, jejich prověření v rámci karantény, dlouhodobé/trvalé garantované uložení a opětovné poskytnutí archiválií badatelům.
- Ke každé archiválii v DA MO bude veden transakční log zachycující veškeré prováděné operace.
- Evidence a editace metadatových položek u jednotlivých archiválií včetně zachycení historie prováděných změn.
- Vyhledávání archiválií podle metadatových položek.
- Vyhledávání archiválií fulltextovým vyhledáváním u archiválií, které obsahují textovou vrstvu.
- Zpřístupnění archiválií interním archivářům bude řešeno přímým zabezpečeným přístupem do DA MO.
- Zpřístupnění archiválií badatelům bude řešeno prostřednictvím Badatelského portálu (dále též Portál), který bude bezpečně oddělený od vlastního DA MO a bude vyhovovat pravidlům přístupnosti webu (tzn. dle vyhlášky č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením).
- Ve zvláštních případech systém DA MO zajistí podporu procesů spojených s vyřazováním dokumentů z archivu procesem výběrového vyřazení archviálie(např. v případech přehodnocení významu archiválií).

1.2 Další požadavky

- Navrhované řešení musí být v souladu s nařízením eIDAS (910/2014/ES) o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
- Návrh musí vycházet ze standardu OAIS – ISO 14 721 (Open Archival Infomation System).
- Navrhované řešení systému DA MO musí zajistit neměnné, trvalé, důvěryhodné a právně závazné garantované uložení archiválií. Po celou dobu uložení musí být zachována jejich použitelnost, čitelnost a integrita.
- Důvěryhodnost archiválií bude zajištěna pomocí technologií kvalifikované elektronické značky a elektronického časového razítka.
- Systém DA MO je určen pro dlouhodobé garantované uchovávání pouze neutajovaných archiválií. Může nastat situace, kdy původně utajované dokumenty uložené v BA MO mohou být v průběhu životního cyklu odtajněny a mohou přejít prostřednictvím ESA MO do DA MO.
- Součástí DA MO je také vytvoření technických předpokladů pro implementaci systému ELZA – pořádací software archiválií.

Tabulka 4: **Popis projektu:**

- Systém DA MO se bude skládat ze dvou nezávislých lokalit. Primární provozní lokalita se bude nacházet v Praze - Ruzyni. Záložní lokalita se bude nacházet v Olomouci - Bystrovany.
- Data do systému DA MO budou primárně přenášena pomocí automatizovaného elektronického rozhraní, které DA MO poskytne a které bude plně v souladu s NSESSS (Národní standard pro elektronické systémy spisové služby dle zákona č. 365/2000 Sb).
- Požadovaná dostupnost celého systému pro dlouhodobé uchovávání neutajovaných elektronických archiválií je v pracovní dny a v pracovní době od 08.00 do 16.00 hod (doba provádění servisních zásahů). Maximální možná nedostupnost funkcionality (downtime) celého systému z důvodů na straně dodavatele je 10% během kalendářního roku.
- Primární přihlášení do PC uživatele proběhne formou autentizace vůči AD CADS. Přihlášení uživatele DA MO proběhne jménem a heslem vůči internímu LDAP DA MO.
- Zabezpečení obsahu - navržená platforma musí umožňovat zabezpečení uloženého obsahu (dokumentů, složek, vlastních objektů) pomocí přiřazení konkrétních přístupových oprávnění (čtení, zápis/modifikace, mazání) odděleně k metadatům a k obsahu pro konkrétní uživatele nebo jejich skupiny v tzv. seznamech oprávnění.

Správa účtů externích uživatelů Badatelského portálu bude zajištěna přímo prostředky tohoto Portálu.

2 POPIS SOUČASNÉHO PROSTŘEDÍ

V obou lokalitách, které mají být zahrnuty do řešení DA MO, může dodavatel využít následující prostředky, které zajistí zadavatel:

2.1 Hadware

- síťová konektivita, datové a telefonní sítě zahrnující:
  - propojení hlavní a záložní lokality.
  - připojení do Internetu (připojení mimo infrastrukturu MO je umožněno pouze v odůvodněných případech);
- napájení,
- chlazení,
- switch napojený na infrastrukturu,
- rack skříně.

2.2 Software, služby

- zdroj uživatelských účtů MS AD,
- služby TSA (autority časových razítek),
- emailový (SMTP) server.

Zadavatel u těchto součástí řešení přebírá odpovědnost za jejich připravenost, kvalitu služby a jejich provoz. Zadavatel po akceptaci díla bude provozovatelem celého řešení.

2.2.1 Použitý HW a SW u ESA MO

2.2.1.1 Badatelna – 1 ks (hlavní lokalita)

- Intel Xeon Processor E5-2603
- 8GB RAM
- 2 x HDD 300GB SAS 10k
- DVD ROM
- Ethernet 1Gb 2-port
- 2 x zdroj HPE
- HPE iLO

2.2.1.2 Brána – 2ks (hlavní a záložní lokalita)

- Intel Xeon Processor E5-2603
- 16GB RAM
- 2 x HDD 300GB SAS 10k
- DVD ROM
- Ethernet 1Gb 2-port
- 2 x zdroj HPE
- HPE iLO

2.2.1.3 ARCHIV – 2ks (hlavní a záložní lokalita)

- Intel Xeon Processor E5-2620
- 64GB RAM
- 2 x HDD 120GB SATA SSD
- DVD ROM
- Ethernet 1 Gb 2-port
- 82Q 8Gb Dual Port
- 2 x zdroj HPE
- HPE iLO

2.2.1.4 TEST – 2ks (hlavní lokalita)

- Intel Xeon Processor E5-2603
- 16GB RAM
- 3 x HDD 450GB SAS 10k
- DVD ROM
- Ethernet 1Gb 2-port
- 2 x zdroj HPE
- HPE iLO

2.2.1.5 BACKUP – 1ks (hlavní lokalita)

- Intel Xeon Processor E5-2603
- 32GB RAM
- 2 x HDD 300GB 12G SAS 10k
- 2 x HDD 1TB 6G SATA 7.2k
- DVD ROM
- Ethernet 1Gb 2-port
- 2 x zdroj HPE
- HPE iLO

2.2.1.6 SPRÁVA – 1ks (hlavní lokalita)

- Intel Xeon Processor E5-2603
- 32GB RAM
- 2 x HDD 300GB SAS 10k
- 2 x HDD 1TB 6G SATA 7.2k
- DVD ROM
- Ethernet 1Gb 2-port
- 2 x zdroj HPE

Tabulka 4: **Popis projektu:**

- HPE iLO

2.2.2 Aktivní prvky

V obou lokalitách jsou implementovány shodné aktivní prvky - SWITCHe HPE 1920 24G od společnosti HPE. Záložní napájení UPS – APC Symetria LX 12kVA Scalable to 16kVA N+1 (hlavní lokalita) a APC Symetria LX 8kVA Scatable to 16kVA N+1 (záložní lokalita).

2.2.3 Digitalizační pracoviště

Řešení digitalizačního pracoviště se skládá ze 3ks kancelářských počítačů s OS Windows 10 včetně monitoru s velikostí úhlopříčky 21.5" a balíku kancelářského SW MS Office. Na počítače je záruka 5 let se servisem NBD.

Skenery EPSON WorkForce DS-60000N - A3 včetně SW Epson Document Capture Pro, slouží pro vytěžování informací dokumentů. Na skenery je záruka 5 let se servisem NBD.

Řešení funguje na principu dvou clusteru (2x2 FortiGate 300D). Na Fortigate jsou rozběhnuty 2 instance (2x VDOM). Jedna VDOM slouží jako IPS sonda, druhá VDOM jako NGFW firewall. Antimalware řešení je založeno na technologii FireEye FX.

Řešení je založeno na SW/HW produktech IBM FileNet ve spolupráci s GPFS - IBM Spectrum Scale a IBM StorWise s požadovanou kapacitou. Toto certifikované řešení slouží pro ukládání digitalizovaných dokumentů - centralizovaný digitální archiv, umožňující požadované funkcionality (indexaci, archivaci i prohledávání objektů při použití retenčních a dalších pravidel pro ochranu dat).

Technologické vybavení v lokalitách je symetrické a je založeno na robustních centrálních serverech Hewlett Packard s příslušně dimenzovanými výkony a konektivitou na kterých probíhá běh řídícího komerčního software IBM FileNet ve spolupráci s dalším komerčním software IBM GPFS Spectrum Scale.

Pro bezpečnostní monitoring a sběr logů ze systémů je použit IBM Qradar. V rámci ochrany databází a zajištění konzistence je použita technologie IBM Guardium. Zároveň je nasazena technologie na zajištění ochrany koncových zařízení, před neoprávněnou modifikací konfiguračních souborů.

Tyto centrální servery jsou po zdvojených přístupových cestách připojeny k diskovým polím s vysoce dostupnou architekturou IBM StoreWise V5010, přičemž každé z nich poskytuje předepsaných 50 TB kapacity.

Software IBM GPFS (General Parallel File Systém) Spectrum Scale plní funkce řízeného zpřístupnění datových prostor pro ukládání archivací a vazby na replikační procesy pro ukládání archivovaných dat ve druhé lokalitě. Přístup k datům je díky paralelnímu systému souborů a replikacím, možné řízeně nakonfigurovat z obou lokalit a mezi lokalitami probíhá asynchronní replikace dat.

U serverů byl použit OS RedHat Enterprise Linux (RHEL).

2.3 Výchozí stav

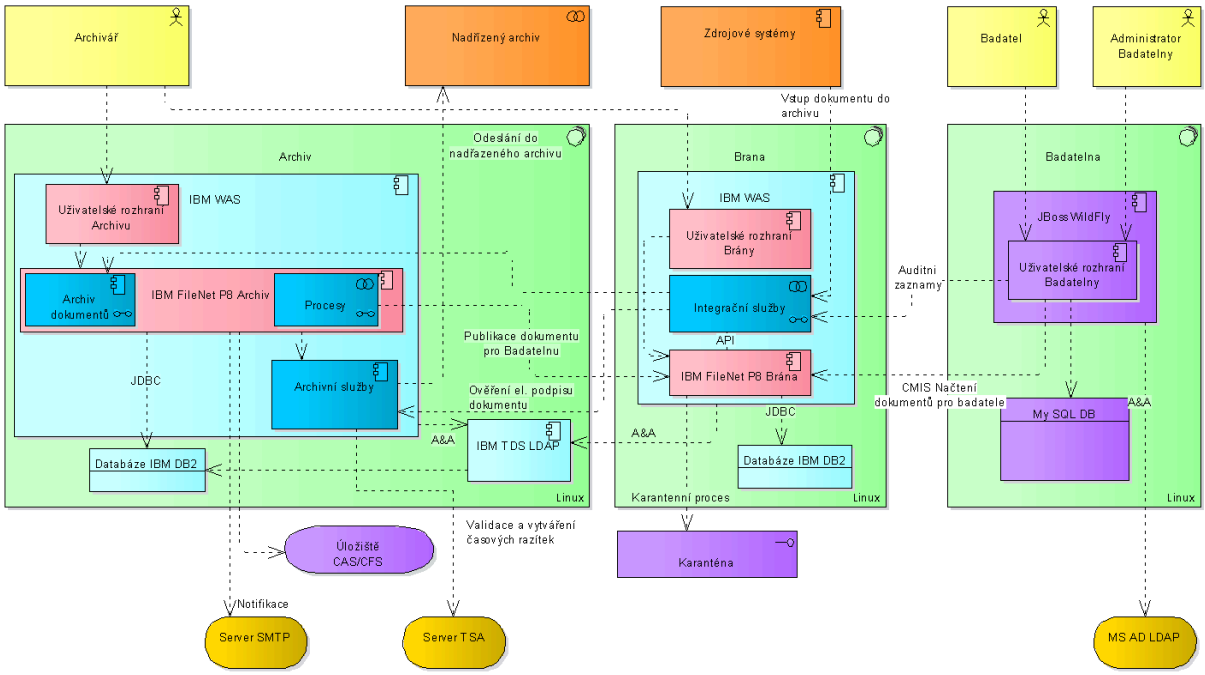
2.3.1 Zdrojové systémy

- Elektronický systém spisové služby Defence (ESSS Defence) – je ucelený systém správy dokumentů pracující v souladu s českou legislativou a umožňuje práci s dokumenty či spisy od okamžiku jejich vytvoření až po archivaci nebo skartaci. Z hlediska integrace s ESA MO se jedná o vazbu v místě skartace/archivace. Na základě zákona č. 499/2004Sb., o archivnictví, spisové službě a provádějících předpisů MV vytváří program SIP – Submission Information Package (balíčky přijímané od původců). Tyto balíčky jsou standartním formátem pro vstup do ESA MO.
- Přístup k dokumentům je rozdělen na lokality Praha a Olomouc. Rozlišení je možné na základě čísla útvaru.
- Úložiště systému ESA MO je zabezpečeno 50 TB čisté binární kapacity v každé ze dvou lokalit a je realizováno prostřednictvím řešení typu Content – Addressed Storage (CAS) Fixed Content Storage (FCS).

2.3.2 Architektura Elektronického systému spisové služby MO (ESA MO)

Řešení je rozděleno do 3 samostatně funkčních vrstev/částí (zvýrazněny zelenou barvou), které jsou odděleny fyzicky i logicky. Tyto jednotlivé části řešení jsou propojeny pouze pomocí integračních rozhraní, a jsou tak vzájemně nezávislá kromě těchto rozhraní.

Tabulka 4: **Popis projektu:**



a) Část Archiv je koncipována jako autonomní a na ostatních částech zcela nezávislá část. Je to z důvodu, aby nebyla ohrožena důvěryhodnost a platnost archivovaných dokumentů v případě, kdy dojde k napadení nebo poškození zbývajících částí řešení. Součástí Archivu je fyzické úložiště dokumentů, které je řízeno a integrováno pouze s logickou vrstvou Archivu, která spravuje metadata dokumentů ukládané do vlastní databáze a binární obsahy dokumentů ukládané do fyzického úložiště. Tato část řešení obsahuje i vlastní LDAP server, pro autorizaci a autentizaci pracovníků archivu do uživatelského rozhraní Archivu a pro řízení přístupu k jednotlivým dokumentům. Samotný Archiv dokumentů vyžaduje pro svojí plnou funkčnost přístup k akreditované TSA, která je integrována pomocí komponenty Archivní služby a slouží k ověřování a vytváření kvalifikovaných časových razítek.

Část Archiv zajišťuje klíčovou funkci řešení, a to, dlouhodobé a důvěryhodné uložení dokumentů po teoreticky neomezenou dobu. Této funkce je dosaženo pravidelným automatickým vytvářením archivních balíčků z nových dokumentů a z dokumentů, jimž se blíží termín pro přerazítkování. Doporučená doba pro přerazítkování je 2 až 4 týdny před uplynutím termínu, z důvodu zajištění platnosti dokumentu i pro případ, že dojde k výpadku služby TSA nebo jiných neočekávaných událostí.

Pro práci s archivem dokumentů je k dispozici uživatelské rozhraní Archivu, realizované jako webová aplikace pomocí technologií HTML5, CSS3 a Javascript, která poskytuje přístup k požadovaným uživatelským funkcionalitám. K jednotlivým dokumentům v archivu jsou ukládány metadata včetně evidence o fyzickém uložení analogových dokumentů. Řešení umožňuje ukládat libovolný binární obsah bez ohledu na formát dokumentu a pro jednotlivé typy dokumentů definovat různá metadata.

Logická vrstva archivu zajišťuje služby pro správu dokumentů a lze se s ní integrovat pomocí standardního rozhraní CMIS, WS-SOAP, WS-REST, Java a .NET API. Fyzická vrstva Archivu je tvořena fyzickým HW uložištěm poskytujícím souborový systém NFS a CIFS. S možností přístupu k uloženým datům na HW úložišti pomocí NFS, CIFS, HTTPS a WEBDAV.

b) V rámci Brány jsou implementovány Integrační služby, které poskytují rozhraní pro vstup dokumentů ze zdrojových systémů. Součástí Brány je i tzv. Karanténa, kde jsou všechny příchozí dokumenty podrobeny důkladné vícestupňové analýze. Brána obsahuje i tzv. dočasné úložiště, kde se ukládají dokumenty pro zpřístupnění přes Badatelnu. Část Brána je napojena na LDAP server v části Archiv pomocí standardního rozhraní LDAP, a slouží pro autorizaci a autentizaci pracovníků archivu, kteří mají právo rozhodnout o přijetí dokumentů, které neprošli validacemi a karanténou.

Část řešení Brána zajišťuje komunikaci mezi části Archiv a okolními systémy včetně části Badatelna. Součástí Brány jsou tzv. Integrační služby, které poskytují webové služby REST (Representational State Transfer) a SOAP (Simple Object Access Protocol), pro příjem vstupních dokumentů ze zdrojových systémů. Po přijetí požadavku webové služby je vstupní dokument uložen do dočasného úložiště Brány.

Uživatelské rozhraní Brány poskytuje funkci pro manuální vložení dokumentu do systému. Část Brány také poskytuje sdílenou složku, která je pravidelně kontrolována skenerem souborového systému. Skener příchozí dokument uloží do dočasného úložiště Brány.

Tabulka 4: **Popis projektu:**

Pro minimalizaci ztráty dat v případě nepředvídaných událostí je nutné, aby zdrojové systémy, které odesílají data do archivu, tato data držely ještě 24 hodin po odeslání
do archivu.

Řešení umožňuje vstup samostatných dokumentů tak i archivních balíčku SIP (implementovaných dle standardu METS) případně dokumentů ve formátu PDF/PAdES.
Po přijetí a uložení příchozího dokumentu do dočasného úložiště, je provedena 4 stupňová validace, součástí, které je i karanténa na škodlivý kód a malware.

Dokumenty, které úspěšně neprojdou všemi stupni validace, jsou uloženy do dočasného úložiště v Bráně, kde jsou připraveny k manuálnímu zpracování pracovníkem archivu, viz Zpracování nevalidních dokumentů.

V rámci Zpřístupnění dokumentu pro Badatelnu se uloží do dočasného úložiště Brány dokumenty určené pro zpřístupnění v Badatelně. Tyto dokumenty jsou označeny identifikátorem žadatele-badatele a také datem do kdy jsou dokumenty k dispozici na zpřístupnění. Po tomto datu jsou dokumenty automaticky odstraněny z dočasného úložiště, a pro opětovné zpřístupnění je nutné podat novou žádost.

c) Badatelna je vytvořena jako autonomní uživatelská aplikace, která je integrována na dočasné úložiště Brány a je napojena na LDAP server (MS Active Directory).

Badatelna je logicky členěná na administrační a prezentační část. Tyto dvě části mohou být provozovány ve dvou samostatných prostředích, jsou však na sobě datově závislé – musí být tedy datově propojeny. Badatelna podporuje provoz nad virtuální infrastrukturou a zabezpečení komunikace SSL/TLS certifikátem. Obě uživatelská rozhraní Badatelny jsou koncipované jako webové aplikace – tencí klienti. Badatelna podporuje provoz
na následujících prohlížečích v jejich nejnovějších verzích se zpětnou kompatibilitou:

- Internet Explorer (výchozí nastavení)
- Firefox
- Opera
- Chrome

Administrační část Badatelny zabezpečuje:

- Příjem dat z Brány
- Správa služebních žadatelů
- Správa přístupů do prezentační části Badatelny
- Evidence činnosti služebního žadatele v prezentační části Badatelny

Příjem dat z Brány je vyvolán ze strany Badatelny voláním REST API rozhraní Brány s dotazem na vyhledání a vrácení všech dokumentů určených pro Badatelnu. Badatelna od Brány přebere kopie všech odpovídajících dokumentů a uloží jejich binární i metadatový obsah do vlastního dokumentového repozitáře a vlastní databáze.

Služební žadatelé jsou evidováni v následujícím rozsahu:

- *Jméno* – povinné
- *Příjmení* - povinné
- *Číslo osobního průkazu* – povinné
- *Telefonní číslo*
- *Číslo útvaru* – výběr z číselníku útvarů přebíraného z Archivu pomocí webových služeb
- Adresa – *Ulice, Č.P., Město, PSČ*

Seznam zpřístupněných dokumentů konkrétnímu služebnímu žadateli v rámci jeho konkrétního přístupu do Badatelny je definován číslem žádosti. Číslo žádosti sděluje služební žadatel archiváři při příchodu do Badatelny a jedná se o číslo jednací dokumentu žádosti v ESSS Defense. Badatelna vyhledá ve svých datech dokumenty, které v metadatovém atributu Číslo žádosti obsahují toto číslo žádosti a přiřadí je k tomuto přístupu.

Správa přístupů do prezentační části Badatelny umožňuje archiváři sledovat seznam aktivních a platných přístupů do prezentační části Badatelny a v případě potřeby okamžitě ukončit platnost kteréhokoliv přístupového hesla.

Evidence činnosti služebního žadatele v prezentační části Badatelny je hlavním podkladem pro tvorbu badatelského listu pro prohlížení elektronických dokumentů. Archivář zde vidí podrobnou evidenci všech činností služebního žadatele v reálném čase. Seznam činností je periodicky odesílán i do Archivu prostřednictvím webových služeb za účelem tvorby badatelských listů.

Prezentační část Badatelny zabezpečuje:

Tabulka 4: **Popis projektu:**

- Přihlášení služebního žadatele pomocí vygenerovaného přístupového hesla
- Fulltextové vyhledávání v zpřístupněných dokumentech
- Prohlížení seznamu zpřístupněných dokumentů
- Prohlížení detailu zpřístupněného dokumentu - metadata
- Prohlížení detailu zpřístupněného dokumentu – obrazová data a OCR vrstva
- Odhlášení

Fulltextové vyhledávání vyhledá zadaný textový řetězec ve všech zpřístupněných dokumentech služebního žadatele, a to jak v metadatech, tak v OCR obsahu dokumentu, je-li k dispozici. Výsledný seznam výsledků zobrazí a v případě nalezení shody v OCR obsahu dokumentu zobrazí služebnímu žadateli i tuto shodu/shody včetně kontextu – okolí hledaného řetězce v textu.

Každý dokument v seznamu dokumentů je zobrazen jako náhled první stránky dokumentu a věc dokumentu.

Detail dokumentu obsahuje náhled první stránky a seznam zpřístupněných metadat dokumentu.

Tlačítkem služební žadatel otevře prohlížeč obrazového obsahu dokumentu spolu s OCR vrstvou, je-li k dispozici. Obrazová data jsou streamována ve formě malých čtvercových fragmentů s použitím technologie DeepZoom, co umožňuje plynulé prohlížení datově rozsáhlých obrazových dokumentů ve vysokém detailu.

Badatelna podporuje práci s těmito typy dokumentů: PDF, PDF/A; MS Office – DOC, DOCX, PPT, PPTX, XLS, XLSX, RTF; JPG, GIF,TIF/TIFF, PNG, XML.

Veškerá komunikace mezi těmito částmi řešení je pomocí standardních komunikačních rozhraní (např. WS-SOAP, LDAP a CMIS).

2.4 Popis programu ARCHID - implementace plněna v rámci ESA MO – datová úložiště

Účel programu:	Specializovaný evidenční program, který byl vyvinut pro potřeby evidenci Autorského fondu (dokumenty NATO) a Fondu útvarů (mise).
Kvantifikace:	Celkový objem archivu 61 000 dokumentů.
Přírůstek:	Nelze přesně specifikovat, eviduje se zpětně ručně, orientačně lze hovořit o 10 000 ročně.

2.4.1 Procesy programu

Vyhledávání:	Základní vyhledávání dle kódu autora, dle názvu dokumentu, dle stupně utajení, dle roku vytvoření, dle druhu dokumentů, dle země původů, dle původce dokumentu. Dle klíčových slov – nastavit vyhledávání dle druhu dokumentů, dle země původu, dle původce dokumentu, dle stupně utajení a dle roku vytvoření a doplnit klíčová slova.
Ruční vstup:	Rozčleněn do fází. V první fázi uživatel zadá rok, původce a protokol, na jehož základě je dokument přijat do archivu. Po zadání kódu autora dojde k porovnání kmenových dat. Toto porovnání slouží zejména k zabránění duplicit při vstupu. Následně se pokračuje novým záznamem evidenční karty, položková struktura viz datový mód.
Správa číselníků:	Systém obsahuje následující číselníky - Útvary a uživatelé a Klíčová slova Ostatní číselníky (např. země) nejsou nezávislým číselníkem, ale pouze nabídnou seznam hodnot, které byly pro danou položku vloženy. Například, mám-li evidovány dokumenty z CZ, DE a FR, nabízí číselník Země tyto 3 hodnoty a při zakládání záznamu umožní vložení nového záznamu.
Fond:	Archivní fond je souborem archiválií, jejichž autorem je jeden původce. V pojetí aliančních dokumentů jsou fondy členěny dle výborů a podvýborů NATO. Tyto fondy jsou vytvářeny a evidovány a může v nich být vyhledáváno. Fond lze považovat za strukturovaný číselník.
Protokoly:	Dokumenty jsou do archivu předávný na základě protokolů. Tyto protokoly jsou vytvářeny a evidovány a může v nich být vyhledáváno. Protokol lze považovat za strukturovaný číselník.
Zápůjčky:	Zápůjčky slouží k evidenci požadavků badatelů a k vytváření badatelských listů při poskytnutí dokumentu z archivu

Tabulka 4: **Popis projektu:**	
Inventarizace:	Specifický způsob vyhledávaní, který poskytuje seznamy dokumentů podle lokace (struktury) jednotlivých fondů.
Skartace:	V rámci skartace lze vytvářet skartační protokol, do toho protokolu zařadit dokumenty určené ke skartaci a provést vlastní skartaci.
Přesun:	Toto je proces pro přemístění dokumentu do jiného archivu. Slouží k vytvoření protokolu o odeslání (přesunu) a přidružení příslušných dokumentů, které budou daným protokolem předány.

2.4.2 Datový model

Doposud nebyl dodán, z funkčnosti programu je vidět, že nelze přímo použít standardní datový model pro dokumenty ESSS Defence.

Základní evidenční karta (analýza na základě obrazovky programu) obsahuje položky (tučně jsou povinné).

- **Předávající útvar** **číselník útvarů**
- **Druh dokumentu** **výčet (Dokument NATO,..)**
- **Původní stupeň utajení výčet**
- **Původce** **číselník útvarů**
- **Kód autora** **řetězec**
- **Název** **řetězec**
- Datum vytvoření datum
- **Rok (myšleno vytvoření)** **rok**
- Originál boolena
- **Charakter dokumentu** **výčet (Spis,..)**
- **Počet listů** **číslo**
- Arch. Sk ozn. Pův.
- **Fond** **číselník ? výčet ?**
- **Kartony** **číselník**
- **P.č. kartonu** **řetězec**
- Identifikace u útvaru řetězec
- Vstupní poznámka řetězec
- Protokol číselník
- Země čísleník
- **Aktuální stupeň utajení:** **výčet**
- **Médium** **výčet (papír,..)**
- Označení výtisku řetězec

2.5 Popis programu ARCHIV - implementace plněna v rámci ESA MO – datová úložiště

Účel programu:	Evidence fyzické dokumentace o vojácích a pracovnicích MO.
Kvantifikace:	Celkový objem archivu 4 000 000 dokumentů, ne všechny jsou však evidovány.
Přírůstek:	Ročně cca 60 000 až 70 000 tisíc dokumentů.

2.5.1 Procesy programu

Vyhledávání:	Podle příjmení, podle jména, podle rodného čísla. Kritéria jsou implicitně nastavena „pole začíná na“ a ignoruje se interpunkce. (Dotaz Mat znamená Mat*, najde Mates, Matěj, Matylda, Mánes, Maťkovič). Vyplnění více položek znamená spojení „AND“ (dotaz Jméno=“Karel“ a Příjmení „Nov“ najde Karel Novák, Karel Nový, atd..)

Tabulka 4: **Popis projektu:**	
	(dotaz Příjmení = „Mal“ a RČ = „54“ najde Malý, Marek, Maleček narozený v roce 1954 (*). Pozn: Najde stejně i osobu narozenou 1854 a v budoucnosti 2054 (tzv. problém roku 2000 – systém používá pouze 2místný rok narození). Data jsou zobrazena „po stránkách“.
Editace:	Vybraný záznam lze editovat, tedy zejména doplnit „Balík“ = místo uložení a případně opravit položky. Pro specifické případy umožní editace přidat „další příjmení“, „další jméno“ a „poznámka“. Přes tyto položky však nelze vyhledávat. Doplněné položky nejsou příliš přehledné, často se další jméno doplní do primární položky. Pravidla nejsou jednotná. Příklad: Osoba má jména „Petr Pavel“ Do systému lze zadat: A Jméno = „Petr Pavel“ B Jméno = „Petr“ Další jméno = „Pavel“ Problém: současný způsob vyhledávání neumožňuje vyhledat „Pavel“ bez ohledu na způsob zadání, resp. Pouze vyhledá dotaz Jméno = „Petr Pavel“ pro variantu A.
Import:	Data standardně přicházejí z jednotlivých krajských správ (celkem 15) jednou ročně. Fyzická dodávka je doprovázena CSV souborem o následující struktuře: Pořadové číslo Hodnost Příjmení Jméno Rodné číslo Osobní spis (1/0) Osobní karta (1/0) Zdravotní doklady (1/0) Jiné doklady (1/0) Svazek (1/0) Data musí v CSV, pokud přijdou v XLS, jsou na externím počítači převedena na CSV. Data v CSV nerespektují datový model Archiv z hlediska délky a musí se upravit (oříznout). Data z CSV upozorňují na duplicity dle RČ, umožní „merge“ záznamů, tedy k jedné osobě (jednomu RČ) mít více záznamů. CSV (či XLS) soubory se předávají na Flash disku, protože obsahují osobní data (RČ(, nesmí být posílána elektronicky).
Číselníky:	Systém používá dva číselníky Útvar (strukturovaný) Číslo, Název, Zkratka, PlatnostOd, PlatnostDo, Dislokace (č), Fond, Poznámka Dislokace (jednopoložkový, součást Útvaru)
Role:	Admin - může vše (editace, import, správa číselníků). User - pouze vyhledávat.
Tisk:	Existuje (obsah aktuální obrazovky), ale není využíván, protože žádné PC s programem Archiv nemá tiskárnu (není pro toto plánována). Případný interní tisk (výhradně pro vedoucího) realizována jako PrintScreen a obrázek přes flashdisk přenesen na jiné PC.
Specifika:	Položka hodnost používána i pro jiné účely (Čj, odlišení osoby z 19. století atd).

2.5.2 Datový model

Table CJ

1	id	ID	i	10
2	id_utvar	id_utvar	i	10
3	cj	CJ	c	20
4	datum	Datum	d	14

Tabulka 4: **Popis projektu:**

5	poznamka	Poznamka	c	50
101	kc	Krycí-číslo	c	20
102	fond	Fond	c	50
103	nazev	Nazev	c	50

Table Dislokace

1	id	ID	i	10
2	dislokace	Dislokace	c	30

Table Field

1	id	ID	i	10
2	field	Nazev	c	16

Table import_file

2	hodnost	Hodnost	c	20
3	primeni	Příjmenímeno	c	25
4	jmeno	Jmeno	c	25
5	rc	Rodné číslo	c	30
6	OS	Os.Spis	i	10
7	OK	Os.karta	i	10
8	ZdrD	Zdr.dokl.	i	10
9	jine	Jiné	i	10
10	svazek	Svazek	i	10
11	rc_ok	RC OK	c	10
12	import	Importovano	c	10
13	zmeneno	Změněno	c	10

Table import_new

1	id	ID	i	10
2	upload_file	Zdrojový soubor	c	50
3	upload_date	Datum upload	d	20
4	upload_pocet	počet vět	i	10
5	import_file	Soubor pro import	c	50
6	import_date	Datum importu	d	20
7	import_pocet	počet vět	i	10
8	ukonceno	Import ukončen	b	10
9	id_cj	CJ	i	10
10	poznamka	Poznámka	c	240
101	cj	CJ	c	15

Table import_new_data

1	id	ID	i	10
2	id_import	id_import	i	10
3	poradi	Počadí	i	10
4	hodnost	Hodnost	c	10

Tabulka 4: **Popis projektu:**

5	jmeno	Jméno	c	40
6	prijmeni	Prijmeni	c	40
7	rc	RC	c	30
8	osobni_spis	OSp	i	10
9	osobni_karta	OsK	i	10
10	zdrav_dok	Zdr.D	i	10
11	jine	Jiné	i	10
12	svazek	Svazek	i	10
13	rc_ok	RC OK	b	10
14	import	Import	b	10
15	zmeneno	Zm	b	10
16	id_osoby	id_osoby	i	10
17	id_osoby_data	id_os_data	i	10

Table osoby

1	id	ID	i	10
2	hodnost	Hodnost	c	15
3	jmeno	Jméno	c	30
4	prijmeni	Příjmení	c	30
5	rc	Rodné číslo	c	20
6	osobni_spis	OS	i	10
7	ev_list	EL	i	10
8	osobni_karta	OsK	i	10
9	dotaznik	Dot	i	10
10	zdravotni_dok	ZK	i	10
11	jine	Jiné	i	10
12	rc_ok	O/1	b	4
201	cj	CJ | útvar | fond | balik	c	30
202	id_field	další záznam	c	30

Table osoby_data

1	id	ID	i	10
2	id_osoba	ID_osoba	i	10
3	id_utvar	ID_utvar	i	10
4	cj	číslo jednací	c	20
5	datum	Datum	d	14

Table rc

1	id	ID	i	10
2	hodnost	Hodnost	c	15
3	jmeno	Jméno	c	30
4	prijmeni	Příjmení	c	30
5	rc	Rodné číslo	c	20
12	rc_ok	O/1	b	4

Tabulka 4: **Popis projektu:**

202	id_field	Další záznam	c	30

Table skupina

1	id	ID	i	10
2	nazev	Název	c	16
3	poznamka	Poznámka	c	50

Table útvary

1	id	ID	i	10
2	kc	KČ	c	16
3	nazev	Název	c	50
4	zkratka	Zkratka	c	16
5	plat_od	Platnost OD	d	14
6	plat_do	Platnost DO	d	14
7	dsc1	DSC1	i	14
8	id_dislokace	ID Dislokace	i	14
101	dislokace	Dislokace	c	20
9	fond	Fond	i	14
10	poznamka	Poznamka	c	50

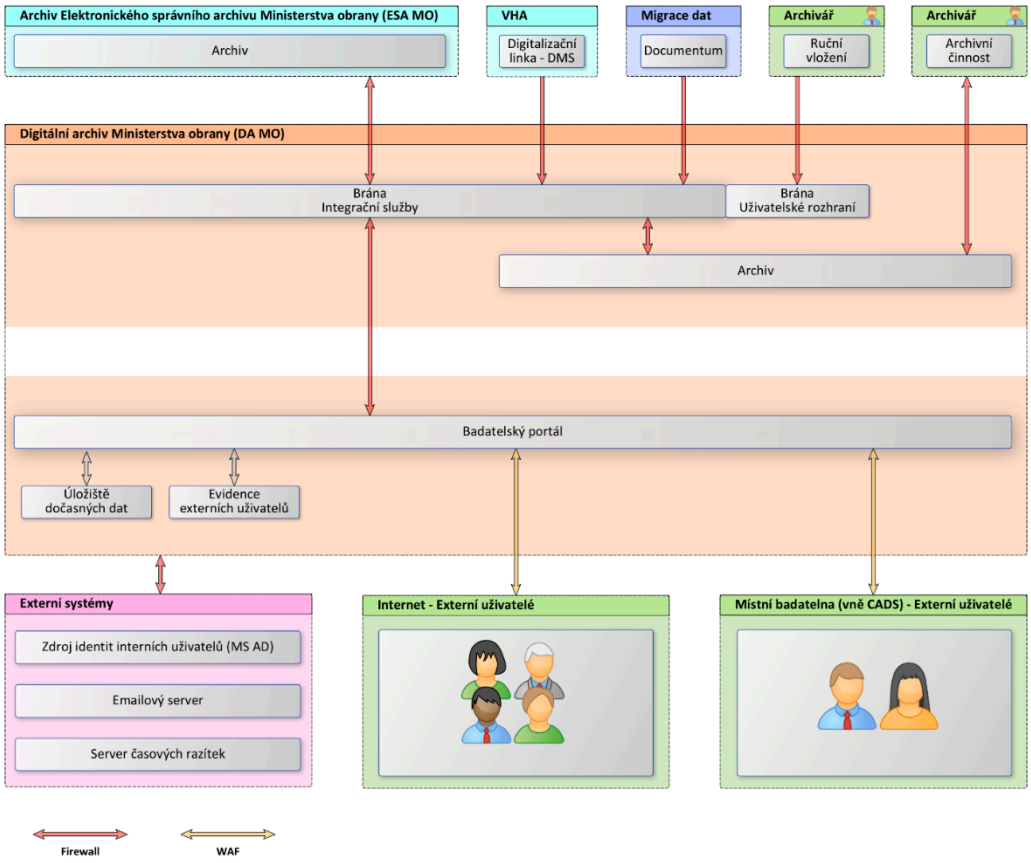
Table uživatel

1	id	ID	i	10
2	jmeno	Jméno	c	16
3	prijmeni	Příjmení	c	50
4	login	Login	c	16
5	heslo	Heslo	c	16

Popis projektu (tzv. To-Be)**:**

Níže na obrázku je schematicky zobrazen návrh DA MO.

Tabulka 4: **Popis projektu:**



Řešení musí být realizováno v souladu s referenčním modelem OAIS a standardem METS. Podle tohoto standardu jsou zpracovávány vstupní archivní balíčky SIP a vytvářeny výstupní archivní baličky DIP pro poskytování právně závazných informací. Dále je požadován soulad se standardy ETSI pro vytváření a validaci elektronických podpisů a časových razítek. Dalším požadavkem je integrace na akreditovanou TSA, která slouží pro vytváření časových razítek při označování archivních balíčků elektronickým časovým razítkem. S ohledem na požadavky standardu eIDAS bude řešení vytvářet pouze uznávané systémové elektronické podpisy a kvalifikované časové razítka od akreditované TSA. Pomocí těchto časových razítek a periodického přerazítkování archivních balíčků je udržována dlouhodobá/trvalá důvěryhodnost archiválií, umožňující uchování platnosti archiválií po neomezenou dobu.

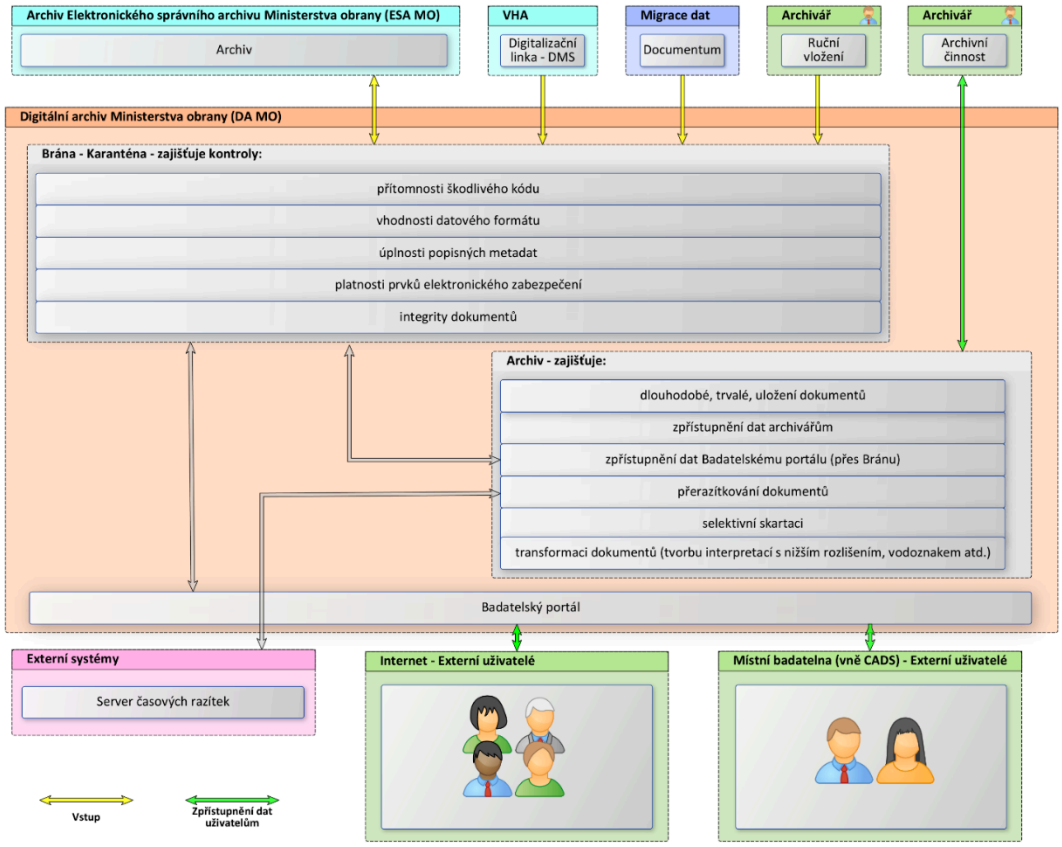
Všechny části řešení (Brána, Archiv, Portál) podporují práci minimálně s formáty PDF, PDF/A, MS Office – DOC, DOCX, PPT, PPTX, XLS, XLSX, RTF, JPG, GIF, TIF/TIFF, PNG a XML.

Základem funkčního návrhu řešení je rozdělení systému DA MO na část ***Brána DA MO, vlastní Archiv a Badatelský portál DA MO***.

- **Brána** představuje viditelnou část archivu a poskytuje jak automatizované rozhraní pro integraci systémů, tak i grafické uživatelské rozhraní pro práci uživatelů.
- Druhou komponentou je samotný **Archiv**, který se skládá z logické (softwarové) části starající se o procesy v archivu a fyzické (hardwarové) části starající se o bezpečné garantované uložení dat. Brána je s Archivem integrována pomocí definovaného rozhraní. Mimo toto rozhraní neprobíhá mezi těmito komponentami žádná jiná komunikace.
- **Badatelský portál** slouží k přístupu k archiváliím všem uživatelům, kteří se zaregistrují. Dále slouží ztotožněným badatelům. Badatelský portál je bezpečně oddělen od vlastního Archivu a jsou v něm uloženy kopie metadat a interpretací archiválií s vodoznakem. Elektronické originály a právně závazné archiválie jsou z Archivu poskytována oprávněným (pouze ztotožněným) uživatelům na základě jejich požadavků, přičemž správu těchto požadavků realizuje Portál.

Níže na obrázku je znázorněn přehled funkcí DA-MO

Tabulka 4: **Popis projektu:**



3 B R Á N A D A M O

Brána DA MO je rozhraním DA MO, které odděluje zdrojové systémy, uživatele a Archiv. Brána poskytuje komunikační rozhraní pro vstup dokumentů, funkce pro práci archivářů, funkce badatelny a přehledové a statistické funkce poskytující informace o stavu archivu. Brána může být tvořena jednou nebo více vzájemně integrovanými aplikacemi, které implementují požadované funkce.

Oddělení Brány a vyčlenění určitých funkcí mimo samotný Archiv má následující přínosy:

- Brána a vlastní Archiv bude oddělen pomocí firewallu, tak mohou být přesně definovány komunikační prostředky.
- Otevřené spojení archivu a zdrojových systémů. Zdrojové systémy nejsou integrovány přímo s archivní částí. V případě změn v archivní části tak nedochází k ovlivnění integrace zdrojových systémů a naopak.
- Prostředky pro práci uživatelů mohou být v průběhu času upravovány. To je výhodné z pohledu budoucích technologií v oblasti klientských prostředků (pracovní stanice, mobilní zařízení, softwarová výbava, standardy) bez nutnosti zásahu do archivní části.

3.1 Vstup dokumentů

Brána poskytuje prostředky pro automatický příjem dokumentů ze zdrojových systémů i funkce pro ruční vkládání dokumentů existujících nebo nově vzniklých z činnosti specializovaného digitalizačního pracoviště. Veškeré vkládané dokumenty jsou vždy přijímány do karanténní části archivu, kde jsou podrobeny zkoumání z pohledu vhodného formátu, úplnosti metadat, platnosti prvků elektronického zabezpečení a přítomnosti škodlivého kódu. Bude zajištěn vstup samostatných dokumentů i archivních balíčku SIP (implementovaných dle standardu METS) případně dokumentů ve formátu PAdES. Dokument se vstupem do DA MO a jeho zaevidováním stává archiváliı.

Pokud dokumenty nejsou na vstupu do DA MO opatřeny elektronickým podpisem a časovým razítkem (typicky dokumenty z migrace dat), zajistí Brána jejich opatření elektronickým podpisem a časovým razítkem. Tato funkce musí být automatická pro vybrané skupiny dokumentů (typicky dokumenty z migrace dat) nebo volitelná, závislá na rozhodnutí archiváře. Časovým razítkem se opatřuje více souborů současně, a to zpravidla 1x denně.

Musí být zajištěno fyzické i logické oddělení Brány a vyčlenění určitých funkcí mimo samotný Archiv:

- Vstupy do Brány ze všech systémů musí být chráněny firewallem:

Tabulka 4: **Popis projektu:**

- ESA MO,
- DMS digitalizační linky,
- migrační nástroj,
- přístup k uživatelskému rozhraní pro archivní činnost.

- Oddělení Brány a Archivu pomocí firewallu, který jasně definuje možné komunikační prostředky.
- Oddělení Brány a Badatelského portálu pomocí firewallu, který jasně definuje možné komunikační prostředky.
- Zajištění bezpečnosti, kdy případné útoky nebo jiné pokusy o napadení či průnik budou vedeny na Bránu, nikoliv na samotný Archiv.
- Volné spojení archivu a zdrojových systémů. Zdrojové systémy nejsou integrovány přímo s archivní částí. V případě změn v archivní části tak nedochází k ovlivnění integrace zdrojových systémů a naopak.

3.1.1 Automatický příjem dokumentů

Automatický příjem dokumentů probíhá pomocí jasně definovaného rozhraní. Brána bude podporovat tyto možnosti automatického příjmu dokumentů:

- Skener souborového systému – Brána poskytne pro každý systém, který není schopen integrace pomocí pokročilejších technologií, složku na vyhrazeném souborovém systému.
  Do této složky zapisuje zdrojový systém data spolu s popisnými metadaty ve formě SIP balíčků. Brána (nebo její externí součást) tyto složky pravidelně monitoruje a nově přidané soubory předává archivu k dalšímu zpracování.
- Webové služby typu SOAP – Standardní prostředek pro systémovou integraci. Data k archivaci jsou zasílána jako příloha (např. pomocí standardu MTOM). Pokud by data k archivaci byla zasílána v těle zprávy, docházelo by ke zbytečnému nárůstu datového toku z důvodu BASE64 kódování binárních dat. Metadata jsou zaslána uvnitř SOAP zprávy jako parametry volání.
- Webové služby typu REST – Standardní prostředek pro systémovou integraci. Data k archivaci jsou zasílána v těle POST požadavku.

Všechna zpřístupněná rozhraní musí být zabezpečena takovým způsobem, aby mohla být dostupná pouze oprávněným subjektům. Vždy musí být jasné, jaký zdrojový systém požadavek do archivu zaslal.

SOAP/REST požadavek splňuje požadavky na SIP balíček kladený standardem OAIS – jedná se o otevřený strukturovaný formát.

Po přijetí požadavku webové služby je vstupní dokument uložen do dočasného úložiště Brány. Data ze zdrojových systémů odesílaná do DA MO budou ve zdrojových systémech uložena ještě minimálně 24 hodin z důvodu eliminace rizika ztráty dat při nepředvídatelné události.

3.1.2 Ruční vstup dokumentů

Systém musí podporovat ruční vstup dokumentů přes uživatelské rozhraní Brány, v rámci které probíhá běžná práce archivářů. Proces následného zpracování dokumentu se neliší od dokumentu vstupujícího prostřednictvím automatického rozhraní.

3.1.3 Karanténa dokumentů

V rámci karantény budou u dokumentu provedeny následující kontroly:

- Přítomnost škodlivého kódu – dokument je testován na přítomnost škodlivého kódu, který by mohl ohrozit nejen bezpečnost archivu, ale také koncové příjemce.
- Vhodnost datového formátu – Do archivu jsou přijímány pouze soubory definovaných datových typů. Z pohledu dlouhodobého uchování hodnoty jsou některé formáty vhodnější než jiné:
- Úplnost popisných metadat – Vstupující dokument musí být popsán množinou definovaných metadat. Tato metadata se dle modelu OAIS archivují spolu s dokumentem.
- Platnost prvků elektronického zabezpečení dokumentů – U souborů vybraných datových typů, které podporují elektronické bezpečnostní prvky (elektronický podpis/značka, elektronické časové razítko), jsou tyto prvky validovány. Typicky se jedná o formáty PDF
- Integrita dokumentů – Stejně jako platnost elektronického podpisu/značky je kontrolována i integrita samotného dokumentu, zda v době od vytvoření podpisu dokumentu nedošlo k jeho modifikaci.

Tabulka 4: **Popis projektu:**

Dokumenty, které nevyhoví v rámci kontrol definovaným kritériím, jsou zařazeny do seznamu problematických dokumentů. Další postup jejich zpracování je na rozhodnutí archiváře.

Souborová karanténa v tradičním pojetí v kombinaci s antivirovou ochranou nemusí být dostatečnou ochranou před moderními hrozbami a malware. Některé typy malware není možné v karanténě detekovat ani po opakovaném antivirovém skenu, jedná se např. o:

- Malware zneužívající zero-day zranitelností – tedy malware, pro který ještě neexistují antivirové signatury.
- Polymorfní malware výrazně měnící svoje chování a strukturu.
- Malware, který se aktivuje na základě uživatelské interakce (kliknutí myší, zobrazení a interakce s dialogovým oknem, scrollování apod.).
- Multivektorový malware, tedy malware pozůstávající z několika nezávislých komponent, které mohou být distribuovány různými způsoby (typicky webový exploit + spear-phishing email), k jehož aktivaci dojde až po stažení všech komponent na koncovou stanici.
- Malware, který se aktivuje až po určitém předem definovaném datu.
- Malware, který je distribuován ve formě downloaderu, který neobsahuje škodlivý kód a jehož jedinou úlohou je stáhnout samotné tělo malware. V izolovaném prostředí karantény nedojde ke stažení těla malware a škodlivé chování je tak nedetekovatelné.

Pro eliminaci těchto hrozeb bude použitý systém pracující na základě behaviorální analýzy, který umožní detekovat běžně rozšířený malware a zároveň další typy malware, například malware pro který nebyly vytvořeny signatury, polymorfní malware, Zero-day útoky a APT (označení pro skupinu útočníků která cíleně napadá konkrétní společnosti s cílem získat úplný přístup k celé síti a všem jejím datům) již při jejich prvním výskytu, malware s podmíněnou aktivací (např. předem stanovené datum, specifická akce uživatele, apod.)

Do okamžiku vložení dokumentu do Archivu nebo rozhodnutí archiváře o odmítnutí zpracování problematického dokumentu musí být tento dokument dostupný i ze zdrojového systému. Ke každému souboru, který je zkontrolován musí existovat detailní informace, kdy byl testován a jaký byl výsledek. Tento přehled bude součástí každého balíčku a bude součástí metadat.

3.2 Archivní činnosti

Tento funkční modul pokrývá svými funkcionalitami veškerou běžnou práci zaměstnanců archivu, v rámci které mohou archiválie vyhledávat, prohlížet, upravovat metadata (vyjma metadat týkajících se bezpečnosti archiválie, časový razítek, provozních záznamů a badatelského listu), poskytovat kopie archiválie dalším subjektům zpřístupnit archiválii jako důkazní materiál nebo archiválii z archivu vyřadit v rámci výběrového vyřazení archiválie.

3.2.1 Vyhledání archiválií

Vyhledání musí být možné podle všech definovaných metadatových položek. U položek, které mají číselníkový charakter, musí být ve formuláři nabídka položek číselníku. Podoba výsledků vyhledávání musí být uživatelsky konfigurovatelná, aby si mohl uživatel zobrazit přehled takových metadatových položek, které jsou smysluplné pro jeho práci. Seznam musí být možné exportovat ze systému ve vhodném datovém formátu (např. Excel).

K libovolné položce v seznamu výsledků vyhledávání je možné si zobrazit detailní náhled se všemi evidovanými informacemi k archiválii. V případě potřeby je možné stáhnout si kopii elektronické archiválie, nebo kopii archiválie nebo důkazního materiálu odeslat do Badatelského portálu (viz funkce Zpřístupnění archiválií).

Výsledky vyhledávání jsou omezeny oprávněními uživatele. Pokud nemá uživatel přístupové právo, nezobrazuje se vyhledaná archiválie ve výsledcích a neexistuje žádný jiný způsob, kterým by se uživatel k archiválii mohl dostat.

3.2.2 Editace/doplnění metadat

Každá položka evidovaná v Archivu je popsána sadou definovaných archivních metadat (definováno v rámci konfigurace systému). Dokument do archivu vstupuje již s nejnutnější sadou metadat, která jej jednoznačně identifikují (např. mezi povinná metadata z ESA MO patří: původce, zdrojový systém, a číslo jednací). Pokud dokument při vstupu do archivu neobsahuje veškeré povinné metadatové položky, může být na základě rozhodnutí archiváře nebo na základě konfigurace systému odmítnut. V opačném případě má archivář možnost povinná metadata doplnit. Kromě povinných metadat může být archiválie popsána další řadou nepovinných metadatových položek, které mohou být doplněny později. Editace metadat probíhá prostřednictvím formuláře systému po vyhledání konkrétní archiválie (viz funkce Vyhledání archiválií).

Tabulka 4: **Popis projektu:**

Metadata se kterými dokument do archivu vstupuje, jsou archivována spolu s archiváliĺ. Další metadata jsou ukládána v rámci provozní databáze Archivu a slouží pro usnadnění práce archivářů. Kromě archivních metadat, mohou být k archiváliĺ uložené v DA připojeny i technická metadata, která jsou v režii systému a uživatel je běžně needituje (může si je však zobrazit).

3.2.3 Náhled na archiválie

Systém umožňuje archivářům prohlížet obsah elektronických archiváliĺ uložených v Archivu v rámci uživatelského prostředí Brány bez nutnosti stahovat archiváliĺ na pracovní stanici archiváře a použití dalšího softwaru. Tato funkce je dostupná pro běžně používané formáty elektronických dokumentů (minimálně formáty PDF, PDF/A; MS Office – DOC, DOCX, PPT, PPTX, XLS, XLSX, RTF; JPG, GIF,TIF/TIFF, PNG, XML). Funkce je dostupná v rámci detailu archiválie po jejím vyhledání (viz funkce Vyhledání archiválie - kap. 3.2.1).

3.2.4 Zpřístupnění elektronické archiválie/ důkazního materiálu

K elektronické žádosti může připojit samotný dokument žádosti, ten je archivován v systému a propojen se zaevidovanou žádostí. Tím se spustí proces, v rámci kterého systém čeká na vložení povolení ke zpřístupnění. Každý archivář má k dispozici seznam takto zpracovávaných archiváliĺ. Po zaevidování povolení ke zpřístupnění dá archivář pokyn systému ke zpřístupnění „kopie“ archiválie v rámci Badatelského portálu. V případě důkazního materiálu systém umožní stáhnout jeho „kopii“, aby mohla být zaslána žádajícímu subjektu (ztotožněnému badateli) prostřednictvím kanálu, zaručujícího platné, důvěryhodné doručení.

Systém musí podporovat zveřejnění příslušné interpretace archivářem vybraných archiváliĺ opatřených vodoznakem na Badatelský portál. Interpretací se rozumí kopie dané archiválie ve formátu vhodném k uveřejnění na Portálu nebo ve formátu vhodném k poskytnutí žádajícímu subjektu (např. změna formátu z TIFF na komprimovaný pdf, případná anonymizace, u hromadně zveřejněných archiváliĺ také vodoznak). Dále musí umožnit kromě individuálního zveřejnění i hromadný výběr archiváliĺ (resp. jejich interpretací) na základě uživatelem zadaných metadat. V rámci procesu zveřejnění archiváliĺ na Portál musí být možnost nastavit k nim úroveň přístupových oprávnění pro jednotlivé skupiny externích uživatelů (registrovaní/ztotožnění).

Žádost o zpřístupnění elektronické archiválie/důkazního materiálu obdrží archivář prostřednictvím Portálu do uživatelského rozhraní Brány. Tuto žádost může vystavit pouze ztotožněný uživatel Portálu. Po přijetí žádosti o zpřístupnění archiválie vyhledá archivář tuto archiváliĺ v Archivu a pomocí připraveného formuláře zaeviduje žádost o zpřístupnění. Součástí požadavku na poskytnutí archiválie může být i požadavek na prokázání její důvěryhodnosti a poskytnutí k tomu potřebných materiálů. Pro tyto potřeby musí být systém schopen vygenerovat ke konkrétní archiváliĺ důkazní materiál, obsahující všechny nezbytné informace pro prokázání důvěryhodnosti archiválie.

3.2.5 Vyřazení archiváliĺ

Je-li dokument určen k vyřazení, pak skartační řízení proběhne v ESA MO. Do DA MO postoupí pouze dokumenty vybrané zde za archiválie. V DA MO může dojít k vyřazení archiválie pouze výjimečně (přehodnocení významu, poškození apod.), ale ne na základě skartačního řízení. Namísto zpracování protokolu apod. musí být zabezpečeno zaznamenání takového vyřazení v evidenci archiváliĺ. V tom případě musí být zahrnuta do evidence archiváliĺ v DA MO i tzv. NAD – zákonem předepsaná základní evidence archiváliĺ.

3.2.6 Administrace a konfigurace archivu

Data v DA MO jsou rozdělena do pracovních prostorů, kde každý prostor má svého správce, který může dalším uživatelům přidělovat právo práce v tomto pracovním prostoru.

Systém bude konfigurovatelný z pohledu metadatových položek. V rámci systému je možné vytvářet třídy (typy) archiváliĺ a jim přidělovat různé množiny povinných a nepovinných metadat. Samotné metadatové položky jsou předmětem konfigurace. Definice metadatové položky obsahuje nejméně: datový typ (znak, řetězec, číslo, logická hodnota), název, popis, forma pořízení. Forma pořízení může být textové pole, výběr z číselníku, checkbox, případně další možnosti.

3.3 Statistika

Software DA MO bude pro uživatele/archiváře poskytovat alespoň tyto provozní a statistické informace:

- Celkový objem archiváliĺ v Archivu – počet archiváliĺ, celková velikost.

Tabulka 4: **Popis projektu:**

- Zbývající dostupný prostor v archivu – velikost a odhadovaný počet archiválií (na základě průměrné velikosti archiválií v archivu). Odhad doby, po kterou bude stačit stávající kapacita archivu.
- Přírůstek archiválií za daný interval (den, týden, měsíc, rok). Systém může zobrazovat např. graf přijatých archiválií v definované agregaci.
- Počty problematických archiválií.
- Počty archiválií navržených k příležitostné, výběrové vyřazení.
- Počty archiválií, u kterých se vyřizuje žádost o zpřístupnění.

Dále systém pro každého uživatele zobrazuje následující seznamy:

- Seznam všech archiválií aktivních v zadaném období (např. včera, tento týden, minulý týden, tento měsíc...).
- Seznam problematických archiválií, které vyžadují zásah archiváře.
- Seznam archiválií, u kterých se vyřizuje žádost o zpřístupnění.
- Seznam archiválií navržených k vyřazení - pro příležitostné vyřazení

3.4 Další služby Brány

Po validním příjmu dokumentu do DA MO Brána zajistí předání kompletní archiválie do Archivu.

Brána musí zabezpečit realizaci požadavků ztotožněných uživatelů Portálu týkajících se poskytnutí plné elektronické kopie původní archiválie nebo důkazního materiálu:

- příjem žádosti,
- vyřízení žádosti,
- zápis dat do badatelského listu.

V případě změny archiválie (verze, interpretace…) nebo jejích metadat v Archivu musí Brána zajistit jejich synchronizaci do Portálu. O takové změně musí Archiv informovat Bránu.

4 A R C H I V

Je tvořen komponentou důvěryhodného elektronického archivu, který se stará o zachování důvěryhodnosti uložených elektronických archiválií. Elektronicky uložená archiválie se dá, dle evropské i české legislativy, pokládat za důvěryhodnou, je-li opatřena platným elektronickým podpisem a kvalifikovaným časovým razítkem. Při zachování platnosti těchto prvků elektronického zabezpečení a neporušenosti datové integrity, tj. kontrolní součty vypočtené z obsahu odpovídají kontrolním součtům vypočteným v době podpisu, se dá takováto archiválie pokládat za důvěryhodnou bez ohledu na formu jeho fyzického uložení.

4.1 Vstup dokumentu

Do Archivu se dokument dostává prostřednictvím Brány DA MO chráněným firewallem.

Při vstupu dokumentu do Archivu bude vytvořena interpretace dokumentu ve formátu vhodném pro uveřejnění na Portálu. Tato interpretace vznikne jako výstup transformační služby Archivu a bude plně parametrizovatelná na základě metadat vstupního dokumentu (např. na základě zdroje dokumentu, požadovaného rozlišení, formátu souboru atd.) včetně možnosti opatřit všechny strany této interpretace vodoznakem. Vodoznak nesmí být vložen jako oddělitelná vrstva, ale musí trvale označit zobrazitelná data.

4.2 Digitální kontinuita a důvěryhodnost

Dlouhodobé a trvalé uložení elektronických archiválií podepsaných elektronickým podpisem, založeném na kvalifikovaném certifikátu generuje potřebu řešit problém omezené platnosti tohoto certifikátu. V době, kdy je potřeba prokázat důvěryhodnost archiválie, může být certifikát, na kterém je podpis založen, již neplatný (ať už z důvodu vypršené stanovené platnosti nebo předčasné revokace z důvodu kompromitace samotného certifikátu). Při současném využití elektronického časového razítka je však možné platnost certifikátu podpisu prokazovat k času orazítkování, kdy byl certifikát ještě platný.

Kvalifikovaný certifikát, na kterém je založeno časové razítko má však také omezenou platnost. Toto omezení lze spolehlivě řešit procesem přerazítkování, kdy je archiválie opatřena novým časovým razítkem vždy před vypršením platnosti certifikátu posledního časového razítka.

Tabulka 4: **Popis projektu:**

Ani tím však není zcela zaručena prokazatelnost důvěryhodnosti archiválie. Informace použité pro ověření archiválie v čase označení časovým razítkem mají také omezenou platnost. Jedná se především o CRL seznamy kvalifikovaných poskytovatelů služeb vytvářejících důvěru, odpovědi OCSP služeb, použité certifikáty a jejich hierarchická struktura. Řešením je uložení všech informací použitých pro ověření spolu s ověřovanou archiválií do struktury k tomu určené – archivního balíčku. Vhodné datové struktury definují ETSI standardy rozšířeného elektronického podpisu AdES. Tyto datové struktury zároveň odpovídají požadavkům na AIP balíček standardu OAIS.

Těmito **referenčními** (rozhodnutí Evropské komise 2011/130/EU) formáty jsou **CAdES, PAdES a XAdES**. Jedná se o formáty, které vznikly v rámci Evropského institutu pro telekomunikační standardy (ETSI – European Telecommunications Standard Institute). Tyto ETSI normy detailně definují, jak má být připojen elektronický podpis a časové razítko (výpočty kontrolních součtů (hashů), šifrování, opatřování metadaty apod.).

- ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES) – připojování podpisu k libovolnému formátu.
- ETSI TS 102 778 PDF Advanced Electronic Signatures (PAdES) – připojování podpisu k PDF dokumentům
- ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) – připojování podpisu k XML datům

Z norem ETSI také jednoznačně vyplývá, jak má proces dlouhodobé archivace dokumentu probíhat:

1. Kontrola platnosti elektronických podpisů připojených k archiválii. To zahrnuje neporušenost kontrolního součtu a platnost certifikátu.
2. Připojení metadat: aktuální verze CRL (seznam zneplatněných certifikátů), OCSP odpovědi, případně další.
3. Připojení časového razítka tak, aby kontrolní součet chránil nejen samotnou archiválii, ale i její metadata.
4. Periodické připojování dalších časových razítek tak, aby každé další bylo připojeno před vypršením platnosti předchozího.

Způsob provedení každého z těchto úkonů je detailně specifikován ve zmíněných normách ETSI.

Nové nařízení eIDAS, kromě oblasti elektronické identifikace a výše zmiňované oblasti elektronického podpisu a jeho dlouhodobé udržitelnosti, které již v české legislativě alespoň částečně obsaženy byly, zavádí i zcela nové oblasti nazývané **„služby vytvářející důvěru“.**

Mezi tyto služby patří i „služby elektronického doporučeného doručování“, které definují způsob **důvěryhodného doručení**. Mezi takovéto způsoby by se dal zařadit systém datových schránek (ISDS), který ovšem pracuje s pojmem „datová schránka“, zatímco nařízení eIDAS zná pouze „odesílatel“ a „příjemce“.

4.3 Validace

Archiválie podepsaná osobním elektronickým podpisem založeným na kvalifikovaném certifikátu nebo označena elektronickou systémovou značkou založenou na kvalifikovaném certifikátu je tímto bezpečnostním prvkem zafixována. Systém musí kontrolovat platnost certifikátu, na kterém je podpis založen. Validace certifikátu spočívá v kontrole, zda jej vydal kvalifikovaný poskytovatel služeb vytvářejících důvěru a zda je certifikát platný a nebyl uveden na seznamu zneplatněných certifikátů. V rámci kontroly je provedeno porovnání s CRL seznamy kvalifikovaných poskytovatelů služeb vytvářejících důvěru a vyhodnocení, zda použité certifikáty jsou k testovanému datu platné. Vzhledem k časové prodlevě mezi odvoláním certifikátu a vydáním a zpracováním CRL je nutné pro rozhodnutí o platnosti certifikátu vyčkat tak, aby byly vráceny údaje o platnosti založené na CRL listu, jehož *platnost od* je až po čase, ke kterému se o platnosti certifikátu rozhoduje. Systém musí podporovat nejméně validaci certifikátů akreditovaných kvalifikovaných poskytovatelů služeb vytvářejících důvěru vedených v Trusted Service List (TSL) příslušných států Evropské unie.

4.4 Balíčkování

Systém podporuje tvorbu archivních balíčků zajišťujících dlouhodobou platnost celé sady archiválií, což vede k optimalizaci procesu razítkování a přerazítkování archiválií tak, aby byly minimalizovány náklady za razítka od časové autority. Systém balíčkování musí splňovat minimálně následující vlastnosti:

- Možnost balíčkování archiválií nezávisle na jejich typu, významu, různých přístupových právech a bez jejich vzájemného vztahu.
- Poskytování důkazních informací k jednotlivým archiváliím bez nutnosti znalosti obsahu ostatních archiválií ve stejném archivním balíčku.

4.5 Evidence a další funkce

Aplikační vrstva Archivu si vede index obsahu uloženého ve fyzické vrstvě nezávislý na Bráně DA MO.

5 B A D A T E L S K Ý P O R T Á L

Badatelský portál zajistí veřejnou prezentaci archiválií uložených v DA MO. Zajistí se tak možnost prezentace všech archiválií ukládaných v digitální podobě v rámci VHA. Jsou v něm uloženy kopie metadat a vybraných interpretací archiválií s vodoznakem. Zásadní důraz je kladen na zabezpečené oddělení Badatelského portálu od vlastního Archivu.

Dále bude součástí tohoto portálu webová prezentace Vojenského ústředního archivu s novým grafickým návrhem a s obsahem obdobným, jako je ve stávající podobě dostupný na adrese http://www.vuapraha.cz/. Webová prezentace musí být vícejazyčná (umožnění překladu do angličtiny, němčiny, ruštiny, francouzštiny a italštiny). Bude také obsahovat volně přístupnou (bez registrace uživatele) databázi VHA (viz níže).

Dodávaný systém musí umožnit rozšíření funkčnosti pomocí pluginů, které zajistí úpravu funkčnosti či změny vzhledu, přičemž ale nebude vyžadován zásah do samotného jádra systému. Dále musí obsahovat funkční bloky – „portlety“, které se mohou mezi sebou provázat a sdílet vybraná data.

Tento Portál bude umístěn v doméně army.cz a bude provozován na síťové infrastruktuře zadavatele. Součástí plnění je dodávka potřebného HW, SW a implementace řešení. Bude oddělen firewallem od Brány DA MO. Místní badatelna a síť internet bude od Portálu oddělena pomocí WAF. WAF není součástí dodávky.

Portál umožní registraci a správu externích uživatelů, včetně řízení přístupových oprávnění do těchto skupin:

- **registrovaní uživatelé** – této skupině bude umožněn přístup k metadatům všech archiválií a interpretacím vybraných archiválií opatřených vodoznakem, včetně možnosti jejich stažení,
- **ztotožnění uživatelé** (uživatelé s jednoznačně ověřenou identitou) – této skupině bude umožněn přístup stejně jako registrovaným uživatelům a navíc budou moci zadávat požadavky na poskytnutí důkazních materiálů nebo elektronických originálů archiválií bez vodoznaku určených např. ke zveřejnění do publikací a podobně, včetně možnosti jejich stažení (neplatí pro důkazní materiál, který bude poskytnut formou důvěryhodného doručení).
    - Ke každému elektronickému originálu archiválie zpřístupněnému tomuto uživateli bude v rámci Archivu veden Elektronický badatelský list, kde budou vedeny záznamy o poskytnutí kopie archiválie včetně žádostí.
    - Tento uživatel bude mít přístup k dané kopii archiválie prostřednictvím Badatelského portálu, a to po omezeně dlouhou dobu (např. 30 dní). V případě požadavku na důkazní materiál bude tento poskytnut danému uživateli způsobem důvěryhodného doručení.

O nastavení úrovně přístupových práv k jednotlivým zveřejňovaným archiváliím rozhoduje archivář.

Badatelský portál bude obsahovat minimálně:

- Webovou prezentaci VHA,
- volně přístupné nahlížení do databáze VHA,
- část pro selektivní autentifikaci (přihlášení a ztotožnění uživatelé),
- selektivní přístup uživatelů k informacím dle úrovně autentifikace,
- funkci pro vyhledávání archiválií, včetně historie hledání pro aktuální sezení,
- listování v seznamu vyhledaných archiválií,
- zobrazení náhledů na archiválie s vodoznakem ve webovém prohlížeči, zobrazení příslušných metadat,
- formuláře pro žádosti o poskytnutí elektronické kopie původní archiválie v původním rozlišení, případně elektronické kopie s právní závazností (důkazní materiál),
- pracovní prostor pro ztotožněné uživatele s možností stáhnout si vyžádané archiválie,
- uživatelské statistiky pro ztotožněné uživatele (např. seznam realizovaných/běžících žádostí o poskytnutí kopie původních archiválií s časovým rozlišením a podobně),
- možnost zobrazení (ve webovém prohlížeči – bez nutnosti stažení) anonymizované verze (např. za účelem nezveřejnění osobních dat) poskytnuté kopie elektronické archiválie,
    - vlastní anonymizaci provádí archivář v rámci DA MO, archiválie nebude při procesu anonymizace stažena na PC archiváře,
    - archivář, který provádí anonymizaci, v dokumentu označí oblasti, které je třeba anonymizovat, jejich překrytím černými obdélníky pomocí myši. Stiskem tlačítka se provede vygenerování nového dokumentu (nové interpretace dokumentu), který neobsahuje text označených údajů a který z vizuálního pohledu ve všech místech výskytu relevantních údajů osahuje černé obdélníky, jež nesmí být vloženy do dokumentu jako oddělitelná vrstva, ale musí trvale znečitelnit zobrazitelná data,

Tabulka 4: **Popis projektu:**

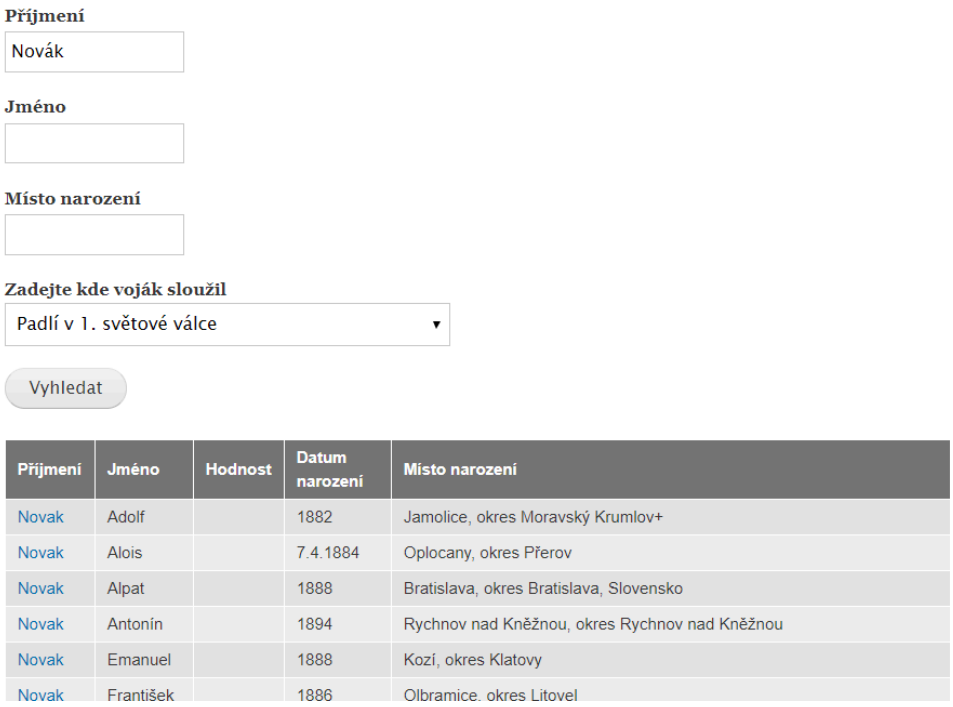
- takto anonymizovaná archiválie bude uložena v Archivu jako interpretace originální archiválie pro případné opakované zpřístupnění nebo za účelem prokázání, že archiválie byla zpřístupněna v anonymizované podobě,
- součástí požadavků na dodávku DA MO je licence SW pro anonymizaci pro práci 10 archivářů. Tento SW musí umožnit co nejefektivnější práci vč. možnosti automatizace,

- část administrace,
  - vytváření a správu účtů externích uživatelů (dle možností přístupu),
  - zakládání ztotožněných uživatelů,
  - statistické údaje – souhrnně pro přihlášené uživatele, selektivně pro ztotožněné uživatele,
- diskusní fórum.

5.1 Databáze VHA

Databáze VHA se vytváří ve Vojenském historickém archivu od roku 1997. Údaje v databázi jsou průběžně doplňovány ručním přepisováním z karet do samostatné aplikace v MS Access, která zůstane zachována. Z této aplikace je nepravidelně, vždy po zpracování určité části karet, vytvořen exportní soubor ve formátu *.csv a tento bude importován do Portálu (bez jeho uložení v Archivu) standardní cestou prostřednictvím Brány.

Portál bude svými prostředky udržovat tuto databázi (postupně aktualizovanou pomocí csv importů) a bude umožňovat ji zpřístupnit tak, že uživatel (libovolný návštěvník webových stránek VHA na adrese http://www.vuapraha.cz/) bude mít možnost vyhledat konkrétní osobu pomocí zadání alespoň jednoho kompletního údaje (příjmení, jméno, místo narození) a výběru z číselníku u údaje, kde voják sloužil (legionáři, padlí v 1. světové válce, padlí ve 2. světové válce, příslušníci čs. Vojenských jednotek v zahraničí). Přestože přístup bude uživatelům umožněn bez registrace, musí být mimo jiné zabezpečen proti strojovému zneužití, např. Turingovým testem.



Příjmení	Jméno	Hodnost	Datum narození	Místo narození
Novak	Adolf		1882	Jamolice, okres Moravský Krumlov+
Novak	Alois		7.4.1884	Oplocany, okres Přerov
Novak	Alpat		1888	Bratislava, okres Bratislava, Slovensko
Novak	Antonín		1894	Rychnov nad Kněžnou, okres Rychnov nad Kněžnou
Novak	Emanuel		1888	Kozí, okres Klatovy
Novak	František		1886	Olbramice, okres Litovel

Na obrázku výše je uveden stávající stav – viz link: http://www.vuapraha.cz/fallensoldierdatabase

5.2 Badatelna a HW

V této interpretaci je míněna badatelna jako existující samostatná místnost, určená zejména (ale ne výhradně) badatelům ke studiu fyzických originálů archiválií v analogové podobě, kterou je v rámci dodávky DA MO potřebné dovybavit 6 ks počítačů v konfiguraci standardního kancelářského PC. Tyto počítače budou zapojeny do lokální sítě místní badatelny DA MO s připojením k internetu. Pro dovybavení sítě místní badatelny je dále požadováno dodat 24-portový switch v provedení Rack-mount 19“ a optický převodník.

5.2.1 HW Badatelny

Součástí plnění je dodávka výše definovaných síťových prvků a 6 ks PC v konfiguraci pro standardní kancelářskou práci vč. klávesnice a myši, monitor 27“.

6 D I G I T A L I Z A C E

Součástí plnění je dodávka samostatného DMS řešení pro digitalizační linku, které bude zajišťovat uložení skenů, doplnění metadat, jednoduché schvalovací workflow a předání dat Bráně DA MO. Toto DMS musí mít vícevrstvou architekturu s přístupem přes tenkého klienta. Součástí plnění je dodávka potřebného HW, OS, aplikačního SW, implementace tohoto DMS a dále dodávka pracovních stanic a periferií.

Počítače digitalizační linky jsou ve vlastní uzavřené síti a uživatelé budou ověřováni prostředky tohoto DMS. Server DMS poskytne integrační rozhraní pro přenos digitalizovaných archiválií do DA MO prostřednictvím Brány DA MO, od které bude oddělen firewallem.

DMS pro digitalizační linku musí umožnit:

- ruční i hromadný vstup digitalizovaných archiválií ze skeneru včetně načtení a zpracování metadat,
- automatické vytěžení OCR (zónové čtení a následné vytvoření atributů),
- náhledy na uložené digitalizované archiválie,
- možnost přidat komentář ke zvolené digitalizované archiválii,
- vyhledávání podle metadat,
- řízení přístupu uživatelů k digitalizovaným archiváliím,
- doplnění metadat včetně automatického vložení systémového data a jména pracovníka, přičemž tato dvě metadata nesmí být možno uživatelsky změnit,
- možnost hromadného zadání metadat k více digitalizovaným archiváliím,
- zabránění ztráty dat v DMS,
- zajištění základního workflow: skenování - verifikace - předání do DA MO včetně řízení přístupových oprávnění uživatelů k jednotlivým krokům workflow,
- smazání digitalizované archiválie po potvrzení prostřednictvím Brány DA MO, že Archiv DA MO převzal danou digitalizovanou archiválii.

Předpokládá se, že k tomuto DMS bude přistupovat max. 15 pojmenovaných uživatelů, kapacita úložiště je požadována alespoň 10TB.

6.1 Digitalizace listinných archiválií

Prezentace archiválií v digitální podobě – původně archiválií VHA v analogové podobě – úzce souvisí s procesem digitalizace těchto archiválií. Součástí plnění je upgrade stávající digitalizační linky o koncové stanice a její napojení na samostatné DMS řešení pro digitalizační linku.

6.2 Digitalizace fotoarchivu

S řešením prezentace archiválií v digitální podobě souvisí i rozšíření pracoviště pro digitalizaci specifických archiválií – fotografií, jež je také součástí plnění. Jedná se o samostatné pracoviště s možností vlastní digitalizace, s vlastní tvorbou metadat. Skenovány budou fotografie, negativy i pozitivy. Fotografie i ve formátu větším, než A4, ale nikoli větším, než A3.

V rámci digitalizačního procesu musí být umožněna organizace, prohlížení, a úprava naskenovaných souborů ve fotoeditoru včetně možnosti hromadného doplnění metadat, která následně budou využita při importu do DA MO. Pro evidenci metadat lze využít např. standardy IPTC či XMP.

Digitalizovaná data budou ukládána do formátu TIF/TIFF bez interní komprese nebo s interní kompresí typu ZIP.

Součástí plnění je dodávka koncové stanice vč. periferií a SW a napojení na samostatné DMS řešení pro digitalizační linku.

6.3 Systém ELZA

Systém ELZA je připravovaný pořádací software archiválií v gesci Technologické agentury České republiky a bude poskytovaný bezplatně. Součástí plnění je vytvoření technických předpokladů pro jeho implementaci. Zadavatel bude

Tabulka 4: **Popis projektu:**

tento software využívat, jakmile bude dokončen jeho vývoj a budou splněny interní technické a organizační předpoklady, tj. předběžně po roce 2019. Primárním účelem aplikace ELZA je pořádání archiválií v souladu se Základními pravidly pro zpracování archiválií – popsáno v publikaci: WANNER, Michal a kol. Základní pravidla pro zpracování archiválií. Druhé, doplněné a rozšířené vydání. Praha: Odbor archivní správy a spisové služby MV, 2015. ISBN 978-80- 86466-78-1. Další informace k ELZA:

- slouží k evidenci analogových dokumentů,
- vytváří principy tvorby metadat,
- slouží k vytváření indexů a metadat,

Server ELZA bude připojen k CADS/ŠIS.

6.4 Hardware a implementace

Součástí plnění je dodávka serveru pro DMS digitalizační linky v konfiguraci, kterou navrhne dodavatel dle požadavků navrženého DMS řešení.

Součástí dodávky je rozšíření digitalizačního **pracoviště listinných archiválií** o:

- 4ks PC určených k digitalizaci v optimální konfiguraci vzhledem k výše uvedenému určení, monitor 27“
- 2ks PC určených k verifikaci digitalizovaných dat v optimální konfiguraci k této činnosti, monitor 27“
- 1x barevná laserová tiskárna A4, samostatné tonery, duplex, síťové rozhraní
- 1x barevná laserová tiskárna A3, samostatné tonery, duplex, síťové rozhraní

Součástí dodávky je rozšíření specializovaného **digitalizačního pracoviště fotoarchivu** o:

- 1ks PC v konfiguraci CPU Intel i7, 16GB RAM, SSD disk 512GB, HDD 2TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440
- Skenery včetně skenovacího SW:
  - 1x Skener fotografií – formát A3, optické rozlišení min. 600 dpi, barevná hloubka 48 bitů, optická hustota Dmax alespoň 2,4. vč. skenovacího SW.
  - 1x Skener negativů/pozitivů – rozměr předlohy minimálně 20x25 cm, optické rozlišení min. 4000 dpi, barevná hloubka 48 bitů, optická hustota Dmax alespoň 3,6; skener musí umožnit skenování negativů atypických formátů či skleněných desek.

Součástí dodávky je vytvoření technických předpokladů pro **implementaci systému ELZA**:

- Dodávka serverů v konfiguraci alespoň:
  - Aplikační server
    - HW: RAM 8GB, HDD 1TB, CPU min. 2x XEON,
    - SW: Java 1.8 kompatibilní OS (Windows Server nebo Unix/Linux)
  - Databázový server
    - HW: RAM 2GB, CPU 1x XEON, HDD 300GB
    - SW: OS Windows Server nebo Linux, PostgreSQL 9.4+
- Podpora implementace systému v rozsahu do 140 člověkodní a roční podpora 25 člověkodní.
- Samotný SW ELZA není předmětem dodávky.

Součástí dodávky je pořízení – lokalita Praha:

- UPS
- Battery Module
- Jistič
- Pomocný a montážní materiál (pro rack, pro UPS)

Součástí dodávky je pořízení – lokalita Olomouc-Bystrovany:

- UPS
- Battery Module
- Jistič

Tabulka 4: **Popis projektu:**

- Pomocný a montážní materiál (pro rack, pro UPS)
- 2ks RACK TRITON 32U 600x900, nosnost 400kg
- 2ks Podstavec pod RACK 600x900
- 2ks Ventilační jednotka 600x900

7 INFRASTRUKTURA

Fyzická (hardwarová) vrstva je tvořena, diskovým polem, které poskytuje samotnou úložnou kapacitu a servery pro provoz aplikačních komponent celého řešení.

7.1 Garantované úložiště

Garantované úložiště DA MO bude realizováno nad stejnou technologickou platformou jako garantované úložiště, které využívá ESA MO. Předmětem dodávky bude rozšíření tohoto úložiště, které bude oddělené od ESA MO. Stávající řešení ESA MO je postavené na technologické platformě IBM FileNet.

Garantované úložiště celému řešení dodává následující vlastnosti nutné pro uložení archiválií:

- **Zabezpečení dat před ztrátou a změnou** – Data v úložišti musí být chráněna proti ztrátě minimálně metodou existence více nezávislých kopií v zařízení. V lepším případě jsou pak aplikovány další mechanismy zabraňující ztrátě, nebo změně dat způsobené technickou chybou, jako jsou např. paritní a cyklické kódy. Dále musí zařízení podporovat definovatelné intervaly, po které je garantováno, že uložená archiválie nemůže být uživatelským zásahem smazána a ani nijak pozměněna (retenční doba). Doba retence musí být nastavitelná také na základě definované události. Mazání archiválie z úložiště musí být auditovaný proces, který podléhá definovaným pravidlům. Dále musí úložiště garantovat, že nelze vnějším zásahem manipulovat se systémovým časem a ovlivnit tak nastavené retenční doby.
- **Dlouhodobá a bezproblémová rozšiřitelnost** – Vzhledem k době plánovaného provozu DA MO, musí být zajištěna dlouhodobá podpora provozu a rozšiřitelnost bez negativního vlivu na uložená data. Zároveň musí být jasně definovatelný proces migrace dat v případě upgradu na novější verze.
- **Podpora replikace do dalších lokalit** – Úložiště musí podporovat synchronizaci více geograficky vzdálených lokalit tak, aby bylo minimalizováno riziko ztráty dat při ohrožení jedné lokality. Záložní lokalita musí být schopna v každém časovém bodě provozu převzít zodpovědnost primární lokality.
- **Pokročilá organizace dat** – Data v úložišti musí být možné organizovat do virtuálních prostorů s odděleným nastavením. Dále by mělo úložiště podporovat mechanismy deduplikace, komprese a ideálně v případě budoucí potřeby i šifrování dat.

7.2 Diskové pole

Předmětem dodávky je rozšíření stávajícího diskového pole ESA MO. Diskové pole poskytuje úložný prostor pro garantované úložiště a databáze aplikačních komponent řešení archivu. Musí být, stejně jako garantované úložiště, snadno a dlouhodobě rozšiřitelné.

Požadovaná kapacita pro každou lokalitu DA MO musí být minimálně 75 TB s možností dalšího rozšíření.

7.3 Nasazení a integrace DA MO

Stejně jako v řešení ESA MO, tak i DA MO bude provozováno ve dvou lokalitách, primární provozní lokalitou v Praze - Ruzyni a záložní lokalitou v Olomouci - Bystrovanech. S ohledem na odhadovanou zátěž archivu a vzdálenost obou lokalit počítá návrh s režimem Failover/Disaster Recovery, kdy je běžný provoz směrován pouze na primární lokalitu. Veškeré změny v primární lokalitě jsou s menším zpožděním replikovány do sekundární lokality, která je připravená převzít běžný provoz v případě výpadku primární lokality.

8 TESTOVACÍ PROSTŘEDÍ

Kromě provozního prostředí je požadováno také prostředí testovací, které je instalováno pouze v primární lokalitě. Testovací prostředí má svoje aplikační a databázové servery, může však využívat úložný hardware produkčního prostředí, kde má vytvořený oddělený prostor. Pokud technologie garantovaného úložiště podporuje

Tabulka 4: **Popis projektu:**

virtualizaci, lze vybudovat virtualizované úložiště pro potřeby testování. Testovací prostředí slouží pro ověřování veškerých změn před jejich aplikací na provozní prostředí.

Součástí plnění je dodávka testovacího prostředí všech komponent DA MO, s výjimkou pracovních stanic.

9 ZÁLOHOVÁNÍ

DA MO musí být navržen a realizován tak, aby nemohlo dojít ke ztrátě dat. Po dobu podpory systému dodavatel ručí za jejich ztrátu.

Jedná se o dodávku, nastavení a implementaci zálohování dat celého ESA MO, DA MO, DMS digitalizační linky, Archivu, systému ELZA, Badatelského portálu i jeho součásti v podobě webových stránek VHA včetně databáze VHA (legionáři, padlí v 1. světové válce, padlí ve 2. světové válce, příslušníci čs. Vojenských jednotek v zahraničí).

10 ŘEŠENÍ SEKUNDÁRNÍ LOKALITY

Pro DA MO je použito řešení s jednou aktivní a jednou pasivní lokalitou. Veškerý produkční provoz probíhá v rámci primární lokality, kde jsou dostatečně dimenzované hardwarové prostředky, aby tento provoz zvládly. Případný load balancing probíhá v rámci jedné lokality. Veškeré změny v primární lokalitě jsou se zpožděním (v řádu minut až hodin) replikovány do pasivní sekundární lokality. Sekundární lokalita je vybavena obdobnou množinou hardwarových prostředků tak, aby byla schopna v případě vyřazení primární lokality převzít veškerý provoz s možností snížení výkonu o max. 50%, ale bez snížení bezpečnosti řešení.

Součástí sekundární lokality není DMS skenovací linky ani dodávka pracovních stanic.

Replikace dat může probíhat na několika úrovních:

- **virtualizace** – pokud bude řešení využívat virtualizaci, může být replikace řešena na úrovni virtuálních strojů,
- **databáze** – většina databázových systémů podporuje replikaci dat do jedné i více pasivních i aktivních instancí.
- **garantovaného úložiště** – většina garantovaných úložišť podporuje replikaci do jedné i více pasivních i aktivních instancí.

Z pohledu kontinuity provozu je kritická především replikace databází a garantovaného úložiště. Ostatní části archivu mají z časového pohledu spíše statický charakter (instalace, konfigurace) a jejich replikace do sekundární lokality nemusí probíhat se stejnou intenzitou, jako u databází a úložiště archivních dat.

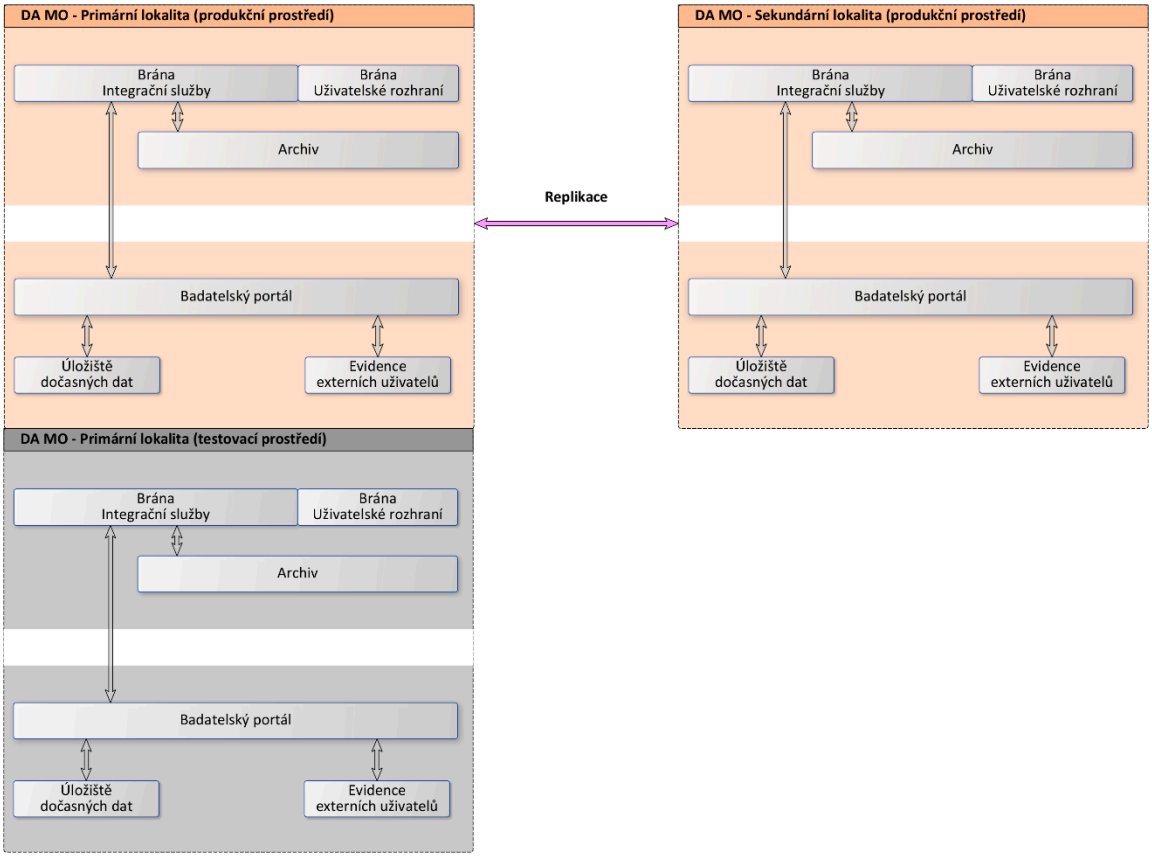
Možná ztráta dat v uvažované variantě: data zpracovaná archivem v řádu minut až jednotek hodin od vyřazení primární lokality.

Doba přepnutí do záložní lokality v uvažované variantě: v řádu hodin až jednotek dnů od vyřazení primární lokality.

Přepnutí primární a sekundární lokality: musí být realizováno synchronizovaně s přepnutím ESA MO.

Níže na obrázku je schematicky zobrazen návrh řešení lokalit DA MO.

Tabulka 4: **Popis projektu:**



1 1 I N T E G R A C E

Modul Archivu poskytuje služby, které modulu Brány umožňují ukládat nové dokumenty do Archivu, získat již archivované soubory případně i s důkazním materiálem o jejich autenticitě a dát pokyn k vymazání Archiválie z Archivu. Komunikace Brány a Archivu probíhá prostřednictvím zabezpečeného transportního protokolu po interní síti DA MO. Oba moduly jsou odděleny firewallem, který umožňuje pouze tuto komunikaci. Modul Archivu je integrován s garantovaným úložištěm pomocí API, které úložiště poskytuje. Žádný jiný modul s garantovaným úložištěm přímo nekomunikuje, pouze prostřednictvím služby logické vrstvy. Modul Archivu není přímo integrován s žádnou interní, nebo externí službou. Pokud potřebuje funkcionality takové služby, jsou zprostředkovány prostřednictvím Brány.

Brána má vlastní diskové pole pro uložení konfiguračních a aplikačně provozních dat, která však nemají archivní charakter.

11.1 Externí služby

Pro zajištění správné funkčnosti potřebuje navržené řešení externí služby, které jsou zde uvedené spolu s požadavky na funkce a způsob integrace. Komunikace se všemi externími službami bude vždy chráněna firewallem.

11.1.1 Emailový server

Emailový server je využíván pro odesílání notifikací interním zaměstnancům archivu a garantům jednotlivých zdrojových systémů. Archiv s emailovým serverem komunikuje pomocí protokolu SMTP.

11.1.2 Zdroj uživatelských účtů interních uživatelů

K přihlášení (autentizaci) je použit doménový zdroj identit MS AD. DA MO může mít i vlastní LDAP, v němž budou definovány jednotlivé uživatelské role.

11.1.3 Kvalifikovaní poskytovatelé služeb vytvářejících důvěru

Služby kvalifikovaných poskytovatelů služeb vytvářejících důvěru se využívají pro ověřování platnosti kvalifikovaných certifikátů. Ověřování probíhá buď pomocí protokolu OCSP nebo stažením CRL a porovnáním certifikátu s tímto seznamem.

11.1.4 Autorita časových razítek

Pro zafixování archivních balíků v čase jsou využívána časová razítka poskytována autoritou časových razítek. Archiv s touto službou komunikuje pomocí protokolu TSP (transportní protokol je HTTPS).

12 MIGRACE

Součástí dodávky DA MO bude jednorázová migrace dat. Předmětem migrace budou digitalizované archiválie, které jsou v současné době uloženy v DMS systému Documentum. Zadavatel zajistí export dat ve formě .zip souborů v definované složce v rámci lokálně dostupného filesystému. Existují – li verze, pak pro každou verzi každé archiválie existuje jeden .zip balíček, jehož obsahem je samotná archiválie v příslušné verzi, a dále .xml dokument obsahující metadata, vztahující se k této archiválii. Celkový počet archiválií ke konverzi je cca 2 miliony.

Dodavatel zajistí migrační nástroj a odpovídá za provedení migrace těchto dat do DA MO.

12.1 Požadovaný cílový stav

Archiválie budou po provedené konverzi ukládány ve formě SIP balíčků organizovaných dle standardů METS do definované složky v rámci lokálně dostupného filesystému. Při konverzi budou vytvořeny logy, které budou obsahovat podrobné informace o jednotlivých konvertovaných archiváliích a výsledcích konverze.

12.2 Konverze a validace obsahu zvolených metadat

V průběhu konverze do SIP balíčků bude kontrolován obsah vybraných položek metadat. Typicky jde o kontrolu rozsahu číselných údajů, ověření zda položky typu datum obsahují smysluplné datum spadající do období od-do, ověření vyplnění povinných položek, případné nahrazení původních hodnot metadat novými na základě konverzních tabulek.

O způsobu zpracování nevalidních dat rozhodne archivář.

12.2.1 Metadata v systému Documentum

Atribut	**Datový typ**
hodnota	String(60)
typ_slozky	String(1)

Typ mo a_doc

Atribut	**Datový typ**
cislo_krabice	Integer
fond	String(60)
inventarni_cislo	Integer
poznamka	String(255)
rejstrik	String(255)
signatura	String(60)

13 OBJEMY DAT A POČTY UŽIVATELŮ

Níže jsou uvedeny předpokládané počty uživatelů jednotlivých komponent DA MO a odhadované potřebné kapacity datových úložišť. Celý systém musí být dodavatelem vhodně navržen, dimenzován a dodán tak, aby zajistil plynulý běh a pružné reakce na uživatelské požadavky.

Záložní lokalita i testovací systém mají stejný počet uživatelů jako hlavní. Testovací prostředí bude navrženo a dodáno tak, aby bylo možno otestovat veškerou požadovanou funkčnost i zátěž.

13.1 Kapacita úložiště

- Archiv a Brána DA MO – 75TB v každé z lokalit
- Portál – 20 TB v každé z lokalit (archiválie zde budou mít menší velikost – konverze do pdf)
- DMS skenovací linky – 10TB (pravděpodobně může být i menší)

13.2 Uživatelé

- přístup přes Bránu – 10
- admin Brány - 2
- přístup přímo do Archivu – 5
- admin Archivu - 2
- DMS pro skenovací linku – 15
- SW pro anonymizaci – 10
- interních uživatelé Portálu
  - archiváři – 15
  - admin - 2
- externí uživatelé Portálu
  - registrovaní uživatelé – 10.000, současně pracujících cca 200
  - ztotožnění uživatelé – 1.000, současně pracujících cca 20

13.3 Kapacita linky

- kapacita linky pro Portál (připojení k internetu není předmětem dodávky)
  - interní síť (komunikace s Bránou) 1 Gb (co největší – dle propustnosti sítě)
  - internet – download/upload z pohledu Portálu 10/50 Mb

14 BEZPEČNOST DA

Návrh řešení bezpečnosti systému DA MO vychází z aktuálních trendů na poli zajištění kybernetické a organizační i fyzické bezpečnosti. Je vyžadováno splnění ustanovení vyplývajících ze zákona č. 101/2000 sb. o ochraně osobních údajů, respektování opatření informační bezpečnosti ze zákona č. 365/2000 Sb. o informačních systémech veřejné správy a rovněž zabezpečí přípravu na provedení interního auditu úložiště podle metodiky DRAMBORA.

Řešení musí být připraveno k pravidelnému testování na bezpečnostní hrozby a zranitelnost.

14.1 Organizační bezpečnost

Systém DA MO a jeho jednotlivé části představují rozšířená informační aktiva MO, která by měla být zařazena do systému řízení bezpečnosti informací, procesu řízení aktiv a analýzy rizik, a měl by pro ně být vypracován plán zvládání rizik.

Pro přístup externích uživatelů k archiváliím prostřednictvím Portálu musí byt předem stanovena pravidla. Při každém přístupu ztotožněného badatele musí být vhodnými prostředky ověřena jeho totožnost.

14.2 Fyzická bezpečnost

DA MO bude provozován v prostředí, které uplatňuje prostředky fyzické bezpečnosti:

- pro zajištění ochrany na úrovni objektů,
- pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěná technická aktiva systému,
- pro ochranu informací a jednotlivých technických aktiv systému,

v souladu s interními předpisy.

14.3 Technická opatření

Je potřebné přijmout technická opatření pro zajištění informační bezpečnosti v souladu s interními předpisy, zajišťující zejména:

- integritu komunikačních sítí,
- ověření identity uživatelů a možnost definice požadovaných heslových politik,
- řízení přístupových oprávnění,

Tabulka 4: **Popis projektu:**

- ochranu před škodlivým kódem,
- aplikační bezpečnost,
- využívaní vhodných kryptografických prostředků zejména v oblasti databází např. z důvodu ochrany osobních dat,
- dostupnost informací,
- zaznamenávaní činností systému a uživatelů,
- napojení na systémy monitorování a dohledu v obou lokalitách a síťový dohled a monitorování až na vnější interface firewallu u obou lokalit, tak aby bylo možné detekovat a vyhodnotit kybernetické bezpečnostní události.

V následujících podkapitolách jsou uvedena technická opatření, která je vhodné zajistit vzhledem k povaze a architektuře systému DA MO.

14.4 Bezpečnost uložených archiválií

Všechny archivované soubory musí být před samotnou archivací zkontrolovány na přítomnost malware. Musí být použito řešení, které nespoléhá pouze na detekci podle známých signatur, ale provádí pokročilejší behaviorální analýzu chování souboru v různých situacích. (viz popis výše)

14.5 Bezpečnostní monitoring

Předpokladem je, že součástí řešení musí být napojení a dodávka SIEM řešení, případně rozšíření a integrace do současného řešení, jestliže to současné řešení umožní. Nástroj bezpečnostního dohledu je nástroj, který dokáže sbírat, monitorovat, ukládat, vyhodnocovat a upozorňovat na neobvyklé chování a hrozby. Součástí celé zakázky musí být dodávka, implementace a technická podpora systémového řešení SIEM (Security, Information and Event Management).

Tento systém bezpečnostního dohledu a správy musí umožňovat shromažďování informací o událostech z různých systémů, sjednocovat je do jednoho místa a následně je korelačně vyhodnocovat. Systém musí pomáhat a umožňovat analytikům nejen efektivně reagovat na vzniklé incidenty, ale tyto incidenty i předvídat a předcházet jim. Implementace musí být schopna integrovat interní i externí systémy zadavatele. Řešení musí pomáhat naplňovat požadavek na detekci bezpečnostních událostí a následného hlášení bezpečnostního incidentu v rámci 7 a 8 zákona č.181 / 2014Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů. Tento systém musí zajišťovat centrální a komplexní bod monitoringu bezpečnostních událostí, a musí být připraven na co možná největší míru autonomie a automatičnosti (možnost blokovat zařízení v síti na základě popsaných use cases, zakládání bezpečnostních incidentů v HelpDesk systému, apod.) Musí také umět integrovat další nástroje prostřednictvím vlastního programovatelného prostředí (API, nebo built-in příprava na integraci). Navržená technologie musí patřit ke špičkám ve svém oboru.
Systém musí poskytovat nejen standardní log management, event management, reporting a analýzy chování pro sítě a aplikace nebo uživatele, ale i funkcionality v podobě komplexního chápání různých zdrojů relevantních bezpečnostních informací. Společně s modulem pro detekci zranitelností, musí být schopen efektivně určit a korelovat informace a eliminovat prodlevu od vzniku incidentu po jeho vyřešení.

14.6 Bezpečnost databází

Provozní databáze budou respektovat doporučení výrobce databáze a související best practice v oblasti zabezpečení databází. Základní body zabezpečení lze rozdělit do několika oblastí.
Požadované řešení musí být dodáno nebo připojeno k řešení provozovanému v současné době na ESA MO. Při pohledu na řešení jako celek, musí sloužit jako stěžejní prvek pro udržení integrity dat uložených v databázích. Zároveň musí být schopno jednoduše udržovat ochranu dat v souladu s již platnými normami a nařízeními pro tuto oblast (a to jak v rámci legislativního právního rámce dané země, tak i v rámci platné legislativy EU). Vytváření automatizovaných a customizovatelných reportů a udržování auditních záznamů je nedílnou součástí takového řešení.
Neméně důležitá je také možnost plné integrace požadovaného řešení na další prvky bezpečnostní infrastruktury již existující, nebo v rámci řešení nově dodaného.
Přínosem řešení musí být nepřetržitý monitoring všech chráněných databází a to včetně automatického odhalování anomálií či případného blokování neoprávněných operací s daty. Stejně tak musí být jeho součástí i jednoduchá správa a možnost modifikace politik a pravidel pro konkrétní účely a související automatizace ochrany dat s možnostmi informování administrátorů o případných incidentech.

14.6.1 Autentizace a autorizace

Databázové účty budou respektovat platná doporučení ohledně komplexity hesla. To se týká nejen databázových účtů nutných pro provoz samotných aplikací a elektronického archivu, ale všech dalších účtů ve stejné databázi. To je důležité z pohledu omezení kompromitace účtů vlastního archivu prostřednictvím jiných, méně zabezpečených databázových uživatelů. Všechny databázové účty budou také respektovat politiku minimálních nutných oprávnění, tedy budou mít přístup pouze k takovým funkcím a objektům databáze, které nezbytně potřebují. Toto se týká i případných veřejných (PUBLIC) rolí v databázi, kterým budou odebrána veškerá nepotřebná oprávnění. Nepotřebné implicitní databázové účty budou v provozních databázích uzamknuty, servisní a další potřebné účty nebudou mít výchozí hesla, nýbrž hesla podle platných doporučení jako účty ostatní. Všechny neoprávněné aktivity uživatelů, musí být zákázány a auditovány.

14.6.2 Provoz a audit

Celé řešení bude funkční na podporovaných verzích databáze příslušného výrobce, včetně nainstalovaných posledních vydaných bezpečnostních balíčků. Po příslušném otestování bude možný upgrade na vyšší verzi databáze, stejně jako instalace potřebných opravných a bezpečnostních balíčků. Mimo standardní ošetření zranitelností prostřednictvím bezpečnostních záplat by řešení mělo umožnovat pokročilou ochranu před cíleným útokem na zveřejňované zranitelnosti databází včetně proaktivního monitoringu provozu nad databází tak, aby bylo možné podezřelou aktivitu včas vyhodnotit a zamezit případnému útoku. Auditován musí být jakákoliv neúspěšný pokus o operace, přístup privilegovaných uživatelů, a veškeré servisní operace nad databází. Auditní záznamy musí být ukládány, pořizovány mimo vlastní server a přistupovat k nim lze, pouze nezávisle tak, aby nebyla možná jejich kompromitace ze strany databázového správce.

Testovací prostředí bude respektovat stejné politiky jako prostředí produkční. Pokud bude vyžadován přístup širšího okruhu uživatelů, případně by z testovacích důvodů nebylo možné dodržet některá bezpečnostní pravidla, musí být možné při zachování funkčnosti provozovat toto prostředí bez obsahu, nebo s účinně pozměněnými citlivými daty.

14.6.3 Databázové zálohy

Provozní databáze budou v pravidelných intervalech zálohovány.

14.7 Kontrola změn a integrity prostředí

Součástí řešení by měl být nástroj umožňující nastavení politik pro přístup ke konfiguračním souborům a registrům pro prevenci neoprávněných zásahů. Veškeré změny v těchto souborech by měly být monitorovány.

Pro zachování integrity prostředí by řešení dále mělo umožňovat zamezení spouštění veškerých neautorizovaných a neznámých aplikací v prostředí DA MO.

14.8 Zabezpečení Badatelského portálu

Na Badatelském portálu budou vždy a zásadně vystaveny pouze kopie archiválií i metadat. Tyto kopie budou uloženy a spravovány v rámci tohoto Portálu.

Badatelský portál bude zabezpečen proti automatizovanému přístupu, často opakovaným dotazům/požadavkům a strojovému vytěžování dat.

Veškerá komunikace bude probíhat prostřednictvím zabezpečeného protokolu https, přičemž jednotlivé části DA MO budou odděleny firewallem. Nezbytné certifikáty budou poskytnuty na základě žádosti přímo VHA, který toto vystavení zajistí.

14.9 Zabezpečení webového front-endu

Webový front-end musí být zabezpečen především proti útokům typu SQL Injection, Cross-site Scripting, Cross-site Request Forgery, ale i dalším známým typům útoků, které by mohly ohrozit důvěrnost, integritu, případně dostupnost systému DA MO. WAF není součástí dodávky.

14.10 Síťová bezpečnost

14.10.1 Segmentace sítě

Síť musí být vhodně segmentovaná a přístup mezi Archivem, Bránou a externími systémy musí být bezpečně řízen:

- komunikace mezi Bránou a Archivem musí být omezena na minimum nezbytných služeb,

Tabulka 4: **Popis projektu:**

- mezi Archivem a externími systémy nesmí probíhat žádná přímá komunikace s výjimkou zabezpečené komunikace s TSA.

14.10.2 Analýza síťového provozu

Veškerý síťový provoz v prostředí DA MO musí být monitorován, tak aby bylo možné detekovat pokusy o neautorizovanou a škodlivou činnost. Systém bude dodavatelem monitorován v rámci jednotlivých lokalit. Monitorování nebude povoleno z CADS. Kromě detekce škodlivých aktivit na základě pravidel a signatur by řešení mělo podporovat i pokročilejší detekci založenou na heuristice a behaviorální analýze. V případě, že řešení bude využívat virtualizaci, měl by být monitorován i provoz mezi jednotlivými virtuálními servery.

Servery hostující jednotlivé součástí DA MO musí být proaktivně chráněny před kybernetickými hrozbami a útoky. Řešení by proto mělo podporovat funkcionality jako detekce a blokace neautorizovaných síťových požadavků, blokace nevyužívaných portů, aplikační monitoring, ochrana před exploity a ochrana před dalšími relevantními hrozbami.

15 SLUŽBY SERVISNÍ A TECHNICKÉ PODPORY

15.1 Dostupnost systému DA MO

Požadovaná dostupnost celého systému DA MO včetně systému ELZA, vyjma Badatelského portálu, je v pracovní dny a v pracovní době od 08:00 do 16:00 hod (doba provádění servisních zásahů). Maximální možná nedostupnost funkcionality (downtime) celého systému s výjimkou Badatelského portálu z důvodů na straně dodavatele je 10% během kalendářního roku.

Požadovaná dostupnost Badatelského portálu je 24x7. Dostupností je míněno:

- dostupnost webové prezentace VUA,
- funkční přihlášení uživatele na Portál,
- funkční vyhledávání a prohlížení archiválií a metadat.

Funkcionalita Portálu, která se váže na dostupnost služeb dalších částí DA MO, se řídí požadavkem na dostupnost těchto částí. Typicky se jedná o služby typu změna v Badatelském listu nebo Žádosti o zpřístupnění archiválie v plném rozlišení. Uživatel musí být o nedostupnosti těchto služeb informován prostředky Portálu.

Maximální okamžitá nedostupnost funkcionality Badatelského portálu je 24 hodin, maximální kumulovaná nedostupnost funkcionality Badatelského portálu z důvodů na straně dodavatele je 2,5% během kalendářního roku.

15.2 Záruční servis

Dodavatel/poskytovatel zajistí záruční servis po dobu 60 měsíců od okamžiku převzetí dodávky příjemcem v souladu s požadavky na dostupnost systému. Zadavatel v době záruky nebude používat zdrojové kódy k změnám programového vybavení. Oprávněná osoba zadavatele/nabyvatele (obsluha DA MO) nahlásí na základě dohodnutých SLA dodavateli/poskytovateli incident a dodavatel/poskytovatel jej následně bude podle těchto SLA řešit.

Záruční doba neběží po dobu, po kterou nabyvatel nemůže užívat zboží pro jeho zjevné vady, za které odpovídá dodavatel/poskytovatel. Dodavatel/poskytovatel zajistí nabyvateli záruční servis včetně dodávky potřebných náhradních dílů dle smluvního ujednání. Případná výměna pevných disků bude prováděna na místě plnění s tím, že nefunkční vadné disky zůstávají natrvalo v majetku AČR. Odstranění vad v záruční době dodavatel/poskytovatel provede ve lhůtách stanovených smlouvou.

Předmětem záručního servisu se rozumí:

- Dodavatel/poskytovatel bude trvale udržovat v pohotovosti potřebný počet vlastních pracovníků pro zásahy v rámci záručních oprav, jejichž seznam je povinen předat objednateli (s osobními údaji nutnými k zabezpečení vstupu do objektu).
- Záruční opravy hardwarových komponent a firmware dodaného řešení.
- Služby údržby SW licencí (maintenance),
- Legislativně-právní upgrade řešení.

Servisní zásah v rámci záruky je ukončen znovuuvedením zařízení do plného provozního stavu odsouhlaseným určeným pracovníkem objednatele.

Tabulka 4: **Popis projektu:**

Součástí záručního servisu je i zabezpečení telefonického a emailového Helpdesku pro pracovníky centrálního dohledu objednavatele (kontaktní údaje vyplní dodavatel do smlouvy).

Po dobu záruky je dodavatel/poskytovatel povinen poskytnout nabyvateli záruční servisní podporu na dodaný HW, SW, konfigurace a implementaci v délce 60 měsíců od akceptace dodávky DA MO s těmito parametry doby poskytování:

- 7x24 pro registraci požadavků přes internet (Helpdesk),
- reakční doba do 2 hodin od nahlášení vady v pracovní době,
- 5x8 (pracovní dny 8:00 – 16:00) pro dobu odezvy,
- režim počátku zásahu Next Business Day (následující pracovní den).

Příklad:

- Pátek 16:30 (mimo pracovní dobu) je hlášen incident/ požadavek na zásah (jedná se o hlášení v režimu 7x24, které nesmí být odmítnuto.
- V pondělí v 8:00 -10:00 - musí dodavatel/poskytovatel reagovat na uvedené hlášení = dodržení reakční doby aniž by došlo k porušení SLA.
- V úterý v 8:00 (ne později) se musí dodavatel/poskytovatel dostavit k zásahu, a tím bude dodržen požadavek Next Business Day.

15.3 Technická podpora hardwarových a softwarových komponent

V rámci technické podpory dodavatel/poskytovatel zajistí odstranění zjištěných vad (poruch) na konkrétním místě a opětovné uvedení zařízení do provozu v těchto lhůtách:

- **havarijní porucha** (způsobí přerušení celkového provozu) - odstranění poruchy do 24 hodin od nahlášení objednatelem,
- **běžná porucha** (omezení funkčnosti jednotlivých zařízení) - odstranění poruchy do 80 hodin od nahlášení objednatelem,
- **poškození nebo drobné poruchy** (nemají vliv na schopnost zařízení plnit požadované funkce ve vyhovující kvalitě) – zahájení opravy do 80 hodin od nahlášení objednatelem.

O závažnosti poruchy rozhoduje výhradně objednatel.

Součástí technické a servisní podpory (u SW se jedná o komerční programové vybavení, nebo i speciálně vyvinuté aplikační programové vybavení, pokud bude součástí řešení DA MO) je zajištění:

- Údržby SW licencí (maintenance) v délce 60 měsíců od data předání SW licencí
- Hardwarové a softwarové servisní podpory v délce 60 měsíců s těmito parametry:
- Doba poskytování:
  - 5x8 (pracovní dny 8:00 – 16:00) pro dobu odezvy,
  - 7x24 pro registraci požadavků přes internet,
  - reakční doba do 2 hodin od nahlášení vady v pracovní době,
  - režim zásahu Next Business Day (následující pracovní den).
- Služby Media Retention (vyměněné nosiče dat se při opravě nevracejí).

Provozní zajištění vychází ze standardů ISO 20000 a ISO 27002.

15.4 Legislativně technický upgrade

Požaduje se bezplatný legislativně technický upgrade, tzn. zapracování případných změn zákonných norem týkajících se předmětu plnění po dobu 60 měsíců do souvisejících změn aplikačního programového vybavení DA MO.

15.5 Zaškolení zaměstnanců VHA na DA MO

Dodavatel/poskytovatel zajistí plnou metodickou a technickou podporu po dobu realizace projektu včetně zaškolení obsluh správy úložiště a uživatelů v rozsahu nezbytném pro uvedení DA MO do provozu po dobu nejvýše 2 dny pro nejvýš 20 osob – administrátorů, archivářů, uživatelů jednotlivých pracovišť DA MO (jedná se o prvotní školení k pořizovanému systému DA MO po splnění implementační fáze DA MO jako jedna z nutných podmínek pro akceptaci plnění smlouvy a převzetí DA MO):

Tabulka 4: **Popis projektu:**

- zaškolení administrátorů DA MO
- zaškolení uživatelů DA MO
- zaškolení archivářů pro práci s DA MO
- zaškolení uživatelů na obsluhu Badatelského portálu
- zaškolení uživatelů na obsluhu DMS Digitalizačního pracoviště.

Dále dodavatel/poskytovatel zajistí pravidelné opakované proškolování do 15 uživatelů a 5 administrátorů (tzn. do 20 zaměstnanců VHA) na |DA MO po celou dobu trvání smlouvy (tzn. v rámci pětileté podpory), přičemž opakované proškolování nebude častější než 1x ročně v rozsahu 1-2 dny. Při stanovení časového rozsahu školení musí dodavatel/poskytovatel s pověřenou osobou dojednat detailní rozsah (zejména u administrátorů zohlednit komplexnost proškolení na celý systém DA MO).

Důvod změny – označte všechny relevantní			
Legislativní důvody	☒	Konec licencí	☐
Modernizace, optimalizace řešení (výsledky business analýz)	☒	Lepší nabídka trhu	☐
Požadavky zaměstnanců, uživatelů	☒	Konec podpory od dodavatele	☐
Konec podpory produktu	☐	Jiné (vysvětlete v tabulce 8)	☐

Přehled případných alternativ řešení rozdílných od „Popis projektu (tzv. To-Be)“ specifikovaném výše

Tabulka 5: **Přehled výstupů projektu:**

Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Vysvětlení výstupu**	**Rozsah změny pro SW**
Úvodní analýza a cílový koncept implementace	1	1 600 000		*Nový*
Aplikační SW - Filenet	2 licence	11 000 000	Primární a sekundární lokalita	*Nový*
Úložiště - diskové pole	2 ks	1 200 000	Primární a sekundární lokalita	*Nový*
Servery	11 ks	1 200 000	Po 3 ks Brána, Archiv, Badatelský portál (primární a sekundární lokalita, testovací prostředí), Backup server, management server	*Nový*
Počítače	13 ks	375 000	6 PC Badatelna, 6 PC Digitalizační linka, 1 PC Fotoarchiv	*Nový*
Implementace	1	1 100 000	140 člověkodnů	*Nový*
Tiskárny	2 ks	100 000		*Nový*
Skenery	2 ks	100 000		*Nový*
Firewally	6 ks	1 600 000	Oddělují Bránu, Archiv a Portál, Web aplikační firewall	*Nový*
Racky, montážní materiál, prvky sítě	1 soubor	250 000		*Nový*
Bezpečnostní prvky HW/SW	1 soubor	11 000 000	Rozšíření stávajícího řešení ESA MO	*Rozšířený*
UPS	1	900 000		*Nový*

Tabulka 5: **Přehled výstupů projektu:**				
Označení výstupu	**Množství a jednotka**	**Celková cena výstupu** [Kč]	**Vysvětlení výstupu**	**Rozsah změny pro SW**
Instalace a konfigurace	1	7 600 000		*Nový*
SW maintenance	1	11 000 000	Na 60 měsíců	*Nový*
Údržba a servis	1	8 000 000	Na 60 měsíců	*Nový*

1.4. Právní klasifikace předmětu projektu

Tabulka 6: **Klasifikace předmětu projektu dle zákonů eGovernmentu (pokud je předmětem více IS, klasifikujte hlavní a ostatní vysvětlete):**	
Klasifikace	**Vyberte**
Druh informačního systému dle klasifikace zák. č. 365/2000 Sb., o informačních systémech VS	**Provozní informační systém podléhající zák. 365/2000 Sb.**
Je projektem agendový informační systém dle zák. 111/2009 Sb., o základních registrech	**Ne**
Budou předmětem projektu přijímány a odesílány datové zprávy dle zák. č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů?	**Ne**
Druh informačního/komunikačního systému dle klasifikace zák. č. 181/2014 Sb., o kybernetické bezpečnosti	**Významný informační systém**

Tabulka 7: **Vazba projektu na informace v Portálu veřejné správy**		
Klasifikace	**Vyberte**	**Vysvětlete**
Budou v Portálu veřejné správy (resp. v Portálu občana) **popsány všechny související životní situace v souladu s vyhláškou č. 442/2006 Sb.?**	**Ano**	DA MO lze ve struktuře Portálu veřejné správy zařadit pod položku „Občan a stát / Archivy a statistiky / Využívání archivních informací“. Zde je možné příslušnou „životní situaci“ popsat.
Bude pro přístup občanů k el. službám úřadu využita struktura služeb v Portálu veřejné správy (resp. v Portálu občana)**?**	**Ne**	Občané budou ke službám DA MO přistupovat prostřednictvím samostatného webového portálu.
Budou projektem využívané formuláře při el. komunikaci s klienty VS dostupné s využitím struktury služeb v Portálu veřejné správy (resp. Portálu občana)**?**	**Ne**	Řešeno samostatně mimo strukturu Portálu veřejné správy

Tabulka 8: **Vysvětlení k základním podmínkám (nutným předpokladům dosažení cílů) projektu:**

2. ARCHITEKTONICKÉ INFORMACE O PROJEKTU

2.1. Dodržení architektonických principů NA VS ČR

Odbor Hlavního architekta eGovernmentu MV předpokládá soulad projektu s principy Národní architektury veřejné správy ČR tak, jak jsou popsány v metodickém pokynu k formuláři. Případný nesoulad v návrhu je možný výhradně, pokud je k němu vyplněna žádost o výjimku, jejíž schválení bude rovněž předmětem posouzení. Otázky na doložení souladu s architektonickými principy jsou obsaženy průběžně v celém formuláři.

2.2. Enterprise architektura projektu a její kontext

Tabulka 9: **Architektonický model:**	
V rámci Enterprise Architektury projektu přiložte jako přílohu model exportovaný ve standardizovaném výměnném formátu The Open Group ArchiMate Model Exchange File Format	**Ne, model nemohl být z objektivních důvodů přiložen**
Případně vysvětlete, proč není model přiložen ve standardizovaném formátu či není přiložen vůbec.	SW ArchiMate nevyužíváme, v současné době nemáme k dispozici Architektonický model v žádné podobě. Vše co bylo dodáno je vloženo v rámci obrázků a schémat. Architektonické principy NA VS ČR (Dostupnost, Použitelnost, Důvěryhodnost, Transparentnost, Bezpečnost, Spolupráce a sdílení, Udržitelnost, Technologická neutralita) budou v rámci projektu dodrženy.

2.2.1. Motivační architektura - strategie a směrování

Tabulka 10: **Vysvětlete, proč projekt realizujete v této podobě a čeho jím chcete dosáhnout. Pro vysvětlení motivace použijte zejména pojmy z odpovídajícího modelu motivační architektury (motivátory, zainteresované, cíle, principy, podmínky, architektonické požadavky):**
Požadované řešení má naplnit cíl „Zabezpečit archivní a dokumentační činnost v rezortu MO“ pořízením systému pro dlouhodobé uchování digitálních záznamů MO splňujícího požadavky standardu OAIS – ISO 14 721 (Open Archival Infomation System) a nařízení eIDAS (910/2014/ES) o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, podle kterých budou budovány všechny elektronické archivy a digitální spisovny na území ČR.

2.2.2. Efektivita projektu – výkonnostní architektura

Tabulka 11: **Vysvětlete dopad projektu na hospodárnost, účelnost, účinnost, časovou a kvalifikační náročnost a na kvalitu služeb v organizaci** (viz metodika TCO zveřejněná zde):
V rámci hospodárnosti byly v maximální možné míře minimalizovány vstupní náklady se zřetelem na odpovídající kvalitu. Především se to týká vstupů, kde dílčími hodnotícími kritérii je nabídková cena s váhou kritéria 60 % a úroveň splnění technických požadavků s váhou kritéria 40 %. Bylo nutné zohlednit stanovené cíle s nutností minimalizovat provozní náklady (personální, finanční, časové) v průběhu celého cyklu při současném dodržení kvality z hlediska daných potřeb. V rámci účelnosti byly porovnány očekávané cíle se skutečně dosaženými výstupy s přihlédnutím na kvantitativní kritéria, tj. nejlepší hodnota dané nabídky a kvalita ve vztahu se zásadami transparentnosti, rovného zacházení a zákazu diskriminace. Největším dopadem projektu je časová a kvalifikační náročnost s důvodu složitých kontrol procesů, které se stávají značnou překážkou především pro zdárné ukončení realizace projektu z důvodu časového omezení.

Tabulka 12: **Přehled požadovaných cílových parametrů SLA nových nebo měněných služeb:**			
Název v rámci projektu nově zřizované nebo měněné služby	**Specifikace SLA parametru služby**	**Sjednaná mezní hodnota SLA parametru**	**Sjednaný způsob měření hodnoty SLA**
DA MO včetně systému ELZA (webová prezentace VÚA, vyhledávání a prohlížení archiválií)	Dostupnost	V pracovní dny a v pracovní době od 08:00 do 16:00	Maximální možná nedostupnost funkcionality (downtime) celého systému je 10% během kalendářního roku.
Badatelský portál	Dostupnost	24x7	Maximální okamžitá nedostupnost funkcionality je 24 hodin, maximální kumulovaná nedostupnost funkcionality z důvodů na

			straně dodavatele je 2,5% během kalendářního roku.
Helpdesk dodavatele	Dostupnost	24x7	Pro registraci požadavků přes internet.
Záruční servisní podpora	Reakční doba na nahlášení vady	2 hodiny	
Záruční servisní podpora Legislativní upgrade není rozvoj IS. Lze použít opci, nikoliv mandatorní plnění dodavatele, plnění pouze na základě požadavku MO. Rozvoj by mohl být v rozsahu cca 300 MD ročně s cenou cca 3 mil. ročně.	Doba odezvy	5x8 (pracovní dny 8:00 – 16:00)	Režim počátku zásahu Next Business Day (následující pracovní den).

Tabulka 13: **Popis klíčových měřitelných ukazatelů výkonnosti (KPI):**

Název v rámci projektu nově zřizované nebo měněné služby vůči koncovému klientovi	**Předpokládaný počet transakcí za rok**	**Kolik stojí každá ukončená transakce bez DPH?** [Kč]	**Jaké % uživatelů je spokojeno s poskytovanou službou?**	**Jaké % transakcí je úspěšně dokončeno?**	**Jaké % uživatelů si zvolí raději elektronickou formu služby než ne-elektronickou?**
KPI zde nemá relevantní oporu, protože se zde nejedná o posuzování rozdílu ve zpřístupnění papírové archiválie místo elektronické. KPI je garance bezpečného uložení dokumentů v archivu v definovaném počtu kopi a zajištění jeho čitelnosti v čase,					

2.2.3. Byznys architektura - poskytování veřejných služeb

Tabulka 14: **Katalog organizačních jednotek, aktérů a rolí:**

Název objektu	**Počet uživatelů služby / IS**	**Vysvětlení významu objektu**
Aktér (organizace, organizační jednotky / úředníci, klienti veřejné správy)		
Brána	10	Brána představuje viditelnou část archivu a poskytuje jak automatizované rozhraní pro integraci systémů, tak i grafické uživatelské rozhraní pro práci uživatelů.
Archiv	5	Přímý přístup do archivu
DMS pro digitalizační linku	15	Bude zajišťovat uložení skenů, doplnění metadat, jednoduché schvalovací workflow a předání dat Bráně DA MO.
Anonymizace	10	Modul pro archiváře vytvářející anonymizované (např. za účelem nezveřejnění osobních dat) kopie elektronických archiválií.

Tabulka 14: **Katalog organizačních jednotek, aktérů a rolí:**		
Název objektu	**Počet uživatelů služby / IS**	**Vysvětlení významu objektu**
Portál interní	15	Přístup pro interní pracovníky – archiváře.
Portál externí	10000 1000	Registrovaní uživatelé, současně pracujících cca 200 Ztotožnění uživatelé, současně pracujících cca 20
Role aktérů při výkonu a příjmu služby		
Archivář	15	Interní pracovníci archivu.
Administrátor	2	Správce HW a SW technologií.
Registrovaný uživatel	10000	Běžný uživatel požadující přístup k archiváliím.
Ztotožněný uživatel	0	Napojení na JIP nebude.

Tabulka 15: **Katalog funkcí a procesů veřejné správy a ve veřejné správě:**	
Název objektu	**Vysvětlení významu objektu**
Agendové funkce (agendy dle RPP, a dále neregistrované, podpůrné a provozní agendy nebo funkční oblasti)	
Obslužné funkce	Pracovník badatelny
Odborné funkce	Archivář
Funkce společného zázemí agend	Pracovník digitalizační linky
Procesy v agendách nebo funkčních oblastech	
Automatický příjem dokumentu	Funkce Brány pro příjem dokumentů ze zdrojových systémů ze skeneru souborového systému, webové služby typu SOAP, webové služby typu REST.
Ruční vstup dokumentu přes uživatelské rozhraní Brány	Vstup v rámci Brány, kde probíhá běžná práce archivářů. Proces následného zpracování dokumentu se neliší od dokumentu vstupujícího prostřednictvím automatického rozhraní.
Anonymizace	Anonymizované verze (např. za účelem nezveřejnění osobních dat) kopie elektronické archiválie vytváří archivář v rámci DA MO, archiválie nebude při procesu anonymizace stažena na PC archiváře. Archivář, který provádí anonymizaci, v dokumentu označí oblasti, které je třeba anonymizovat, jejich překrytím černými obdélníky, provede vygenerování nového dokumentu (nové interpretace dokumentu), který neobsahuje text označených údajů a který z vizuálního pohledu ve všech místech výskytu relevantních údajů osahuje černé obdélníky. Takto anonymizovaná archiválie bude uložena v Archivu jako interpretace originální archiválie pro případné opakované zpřístupnění nebo za účelem prokázání, že archiválie byla zpřístupněna v anonymizované podobě.
Vyhledání/zpřístupnění archiválie	Vyhledání podle všech definovaných metadatových položek nebo systémem fulltextového hledání.
Editace/doplnění metadat	Každá položka evidovaná v Archivu je popsána sadou definovaných archivních metadat, která jej jednoznačně identifikují. Archivář má možnost povinná metadata doplnit. Kromě povinných metadat může být archiválie popsána další řadou nepovinných metadatových položek, které mohou být doplněny později. Editace metadat probíhá prostřednictvím formuláře systému po vyhledání konkrétní archiválie. Metadata, se kterými dokument do archivu vstupuje, jsou archivována spolu s archiválií. Další metadata jsou ukládána v rámci provozní databáze Archivu a slouží pro usnadnění práce archivářů. Kromě archivních metadat, mohou být k archiválii uložené v DA MO připojena i technická metadata, která jsou v režii systému a uživatel je běžně needituje.

Tabulka 15: **Katalog funkcí a procesů veřejné správy a ve veřejné správě:**	
Název objektu	**Vysvětlení významu objektu**
Administrace a konfigurace archivu	Data v DA MO jsou rozdělena do pracovních prostorů, kde každý prostor má svého správce, který může dalším uživatelům přidělovat právo práce v tomto pracovním prostoru. Systém bude konfigurovatelný z pohledu metadatových položek. V rámci systému je možné vytvářet třídy (typy) archiválií a jim přidělovat různé množiny povinných a nepovinných metadat. Samotné metadatové položky jsou předmětem konfigurace. Definice metadatové položky obsahuje nejméně: datový typ (znak, řetězec, číslo, logická hodnota), název, popis, forma pořízení. Forma pořízení může být textové pole, výběr z číselníku, checkbox, případně další možnosti.
Funkce (činnosti) **zařazené v procesu nebo samostatně existující na podporu agend / funkčních oblastí** (NEPOVINNÉ)	

Tabulka 16: **Katalog (interních a externích) služeb:**			
Název služby	**Kdo poskytuje službu**	**Kdo je konzumentem služby**	**Výčet použitých obslužných rozhraní služby**
Interní služby veřejné správy (dovnitř úřadu či subjektu VS)			
Příjem dokumentu do archivu	Archivář	Interní IS resortu MO	Brána DA
Externí služby veřejné správy (vně úřadu či subjektu VS)			
Vyhledání/zpřístupnění archiválie	Archivář	Registrovaný/ztotožněný uživatel	Portál DA

Tabulka 17: **Využití front-office rozhraní předmětem projektu:**		
Rozhraní	**Využití**	**Popis využití rozhraní v projektu**
Asistovaná přepážka	**Ano**	Využití služeb Badatelny VHA.
Webový portál	**Ano**	Standardní přístup přes portál www.vuapraha.cz.
Datová zpráva (ISDS)	**Ano**	Zaslání požadavku do datové schránky MO ČR.
Elektronicky podepsaný dokument do e-Podatelny	**Ano**	Zaslání požadavku do e-Podatelny MO ČR.
Listinnou cestou do podatelny	**Ano**	Zaslání požadavku do Podatelny MO ČR.

Tabulka 18: **Využití propojeného datového fondu:**				
Služba	**Použito**	**Č. žádosti o výjimku**	**Vysvětlení**	**Zákonné zmocnění k přístupu**
Čtení referenčních údajů FO (ROB)	Nerelevantní			
Zápis nových FO (ROB)	Nerelevantní			
Editace referenčních údajů FO (ROB)	Nerelevantní			
Čtení referenčních údajů PO (ROS)	Nerelevantní			

Tabulka 18: **Využití propojeného datového fondu:**				
Služba	**Použito**	**Č. žádosti o výjimku**	**Vysvětlení**	**Zákonné zmocnění k přístupu**
Zápis nových organizací (ROS)	Nerelevantní			
Editace referenčních údajů PO (ROS)	Nerelevantní			
Čtení referenčních údajů míst a adres (RÚIAN)	Nerelevantní			
Zápis nových územních id. (RÚIAN)	Nerelevantní			
Editace referenčních údajů míst a adres (RÚIAN)	Nerelevantní			
Zápis a využití práv a povinností při využívání údajů agend (RPP)	Nerelevantní			
Zápis rozhodnutí o změnách údajů agend dle § 52 zák. 111/2009 Sb. (RPP)	Nerelevantní			
Čerpání informací z agend jiných úřadů (Integrační platformy, eGSB)	Nerelevantní			
Poskytování informací agendám jiných úřadů (Integrační platformy, eGSB)	Nerelevantní			

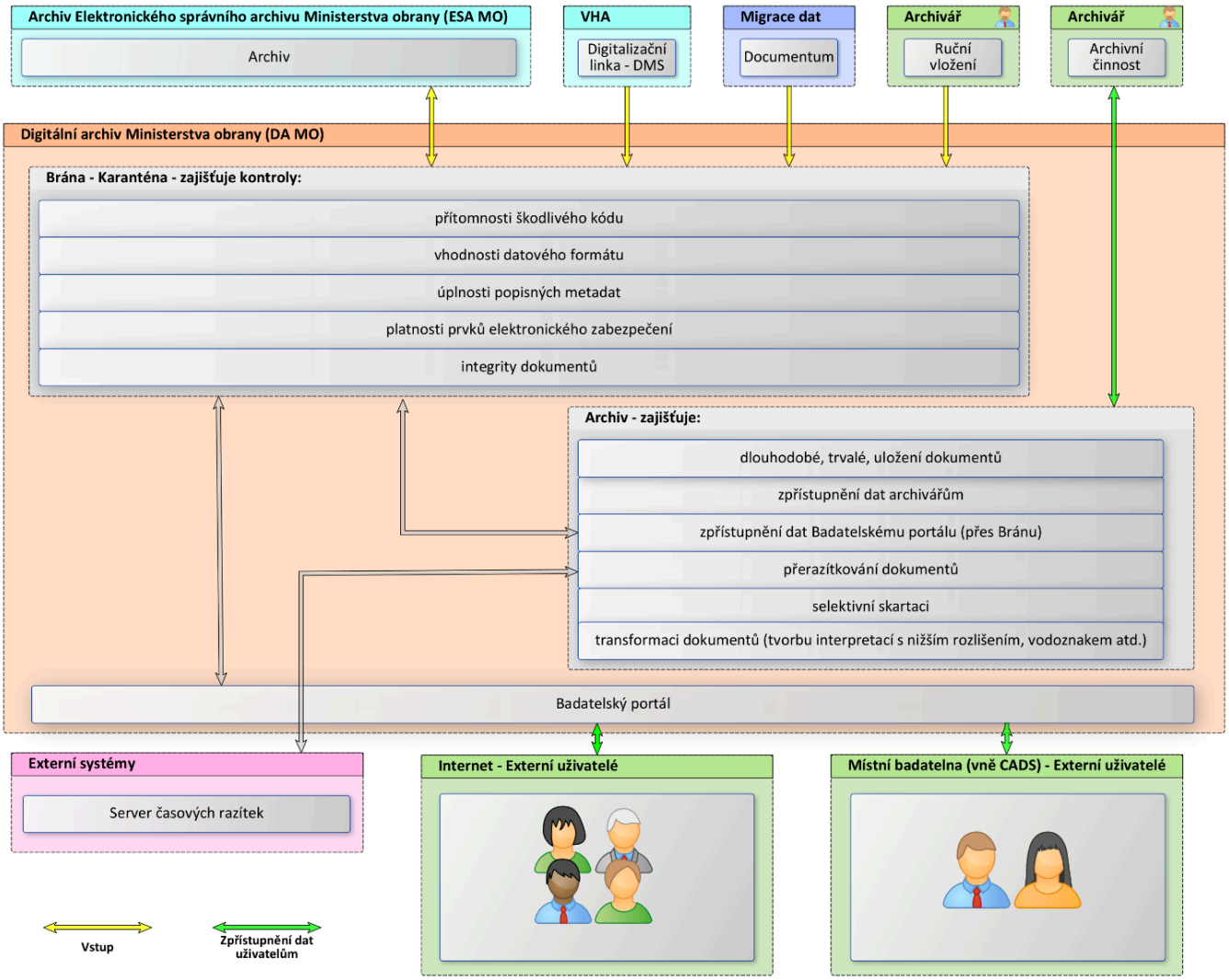
Tabulka 19: **Využití dalších klíčových prvků eGovernmentu v byznys architektuře projektu:**			
Název	**Popis**	**Použito**	**Č. žádosti o výjimku**
Identifikace, autentizace úředníka	Identifikace osob vstupujících do procesu je řešena v souladu s JIP/KAAS	Nerelevantní	
Identifikace, autentizace klienta	Identifikace osob vstupujících do procesu je řešena v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci	Ano, použito	Celý process el. identifikace bude tvořen platformou Národní identitní authority (NIA), která vykonává činnosti Národního bodu dle § 20 a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické identifikace dle nařízení Evropského parlamentu a Rady (EU) č. 910/2014. Bude zajištěna státem garantovaná služba identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity

Tabulka 19: **Využití dalších klíčových prvků eGovernmentu v byznys architektuře projektu:**			
Název	**Popis**	**Použito**	**Č. žádosti o výjimku**
			dle principu Single Sign-On.
Doručování	Využití Datových schránek pro účely doručování od OVM soukromoprávním subjektům a mezi OVM navzájem	Nerelevantní	
Dodávání	Využití datových schránek pro účely dodávání mezi soukromoprávními subjekty navzájem	Nerelevantní	
Provádění úkonů	Využití Informačního systému datových schránek pro účely příjmu úkonů učiněných soukromoprávním subjektem vůči OVM (např. podání)	Nerelevantní	

Tabulka 20: **Identifikace, autentizace a autorizace subjektů/uživatelů v jejich rolích:**		
Služba využívající identifikaci, autentizaci a autorizaci	**Vysvětlení způsobů identifikace, autentizace a autorizace**	**Použitý prostředek a druh autentizace**
Přihlášení interního uživatele DA MO	Jménem a heslem	Interní LDAP DA MO Integrace s JIP KAAS se neočekává. Jedná se o čistě lokální IS MO bez napojení na veřejné eGov prostředí státu.
Přímý přístup do Archivu	Jménem a heslem	Interní LDAP DA MO
Brána pro vstup dokumentů	Jménem a heslem	Interní LDAP DA MO
Provozní databáze	Nebude umožněna lokální OS autentizace, ani vzdálená OS autentizace	
Webový portál DA MO	Elektronická identifikace a autentizace	Národní identitní autorita (NIA) složená z těchto komponent: - Národní bod - Kvalifikovaný správce - Základní registry - Národní uzel eIDAS Webový portál DA MO bude propojen s Portálem občana MV odkazovou dlaždicí.

Model byznys architektury (výkonu veřejné správy) – pohled činnostních funkcí

zde vložte diagram(y), které odpovídají tomu, co je uvedeno výše



Model byznys architektury (výkonu veřejné správy) – pohled služeb veřejné správy

zde vložte diagram(y), které odpovídají tomu, co je uvedeno výše

Tabulka 21: **Dodržení architektonických principů byznys vrstvy:**

Princip	Požadavek	Dodrženo	Č. žádosti o výjimku	Způsob a míra naplnění
Dostupnost	Řešíte obecně přístupnost a použitelnost pro klienty se zdravotním postižením?	Ano		Dle vyhlášky č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením.
	Řešíte přístupnost u webových stránek a rozhraní pro komunikaci s klientem?	Ano		
	Bude každá nová nebo zásadně měněná služba či proces vnitřně plně elektronická?	Ano		
	Bude možné učinit podání v plně elektronické podobě	Ano		

Tabulka 21: **Dodržení architektonických principů byznys vrstvy:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
	kdekoli (bez nutnosti následného dokládání papírových dokumentů) a kdykoliv (kromě okamžiků nezbytné údržby systémů)?			
Použitelnost	Budou všechny formuláře služeb v projektu předvyplněny všemi úřadu/státu známými údaji klienta (vlastními či z PPDF)?	Nerelevantní		
	Bude klientům dostupná plná historie vzájemné komunikace s úřadem tak, aby byla využitelná pro opakované použití?	Nerelevantní		
Důvěryhodnost	Bude zajištěno oboustranné garantované doručení a platnost elektronických dokumentů?	Ano		
	Bude zajištěno průkazné doložení úkonů z minulosti?	Ano		Bude probíhat logování všech úkonů a transakcí.
Transparentnost	Byl veřejnosti představen záměr a cíle projektu?	Ano		
	Bude zajištěn přístup klientů ke všem svým řízením všemi dostupnými kanály eGovernmentu?	Nerelevantní		
Spolupráce a sdílení	Byly (budou) do návrhu služeb v projektu zapojeny ve vzájemné spolupráci odborné týmy napříč veřejnou správou?	Ano		
Udržitelnost	Představuje-li projekt nové nebo zásadně pozměněné IT řešení, bude realizováno nad procesně aktualizovanými byznys službami úřadu?	Ano		

Tabulka 22: **Vysvětlení v kontextu byznys architektury úřadu, tedy:**
a) jaké k projektu existují či vznikají duplicity a proč?
Realizací projektu nevzniknou žádné duplicity.
b) jaké jsou další souvislosti?
Projekt souvisí (přímo navazuje) na již realizovaný projekt Elektronický správní archiv, z něhož bude přebírat dokumenty, které budou mít charakter archiválie.
Vysvětlení byznys architektury projektu:

2.2.4. Aplikační architektura (aplikací a dat)

2.2.4.1. Aplikační architektura – část: Architektura informačních systémů

Tabulka 23: **Katalog všech aplikačních komponent řešení a klíčových aplikačních funkcí:**

Typ prvku	Název prvku	Vysvětlení významu aplikačních komponent, funkcí a služeb
Komponenty, funkce a aplikační služby vytvářené nebo významně měněné v rámci záměru (žádosti)		
komponenta	Brána	Komponenta, která představuje viditelnou část archivu a poskytuje jak automatizované rozhraní pro integraci systémů, tak i grafické uživatelské rozhraní pro práci uživatelů. Je rozhraním DA MO, které odděluje zdrojové systémy, uživatele a Archiv.
funkce	Karanténa dokumentů	Zajišťuje v rámci brány kontroly přítomnosti škodlivého kódu, vhodnosti datového formátu, úplnosti popisných metadat, platnosti prvků elektronického zabezpečení, integrity dokumentů.
funkce	Komunikační rozhraní	Funkce Brány, která slouží pro vstup dokumentů ze zdrojových systémů nebo pro ruční vkládání dokumentů existujících nebo nově vzniklých z činnosti specializovaného digitalizačního pracoviště.
funkce	Přehledy a statistiky	Přehledové a statistické funkce Brány poskytují tyto informace o stavu archivu: • Celkový objem archiválií v Archivu – počet archiválií, celková velikost. • Zbývající dostupný prostor v archivu – velikost a odhadovaný počet archiválií (na základě průměrné velikosti archiválií v archivu). Odhad doby, po kterou bude stačit stávající kapacita archivu. • Přírůstek archiválií za daný interval (den, týden, měsíc, rok). Systém může zobrazovat např. graf přijatých archiválií v definované agregaci. • Počty problematických archiválií. • Počty archiválií navržených k příležitostné, výběrového vyřazení archiválie. • Počty archiválií, u kterých se vyřizuje žádost o zpřístupnění.
služba	Příjem a vyřízení žádosti	Služba Brány zabezpečující realizaci požadavků ztotožněných uživatelů Portálu týkajících se poskytnutí plné elektronické kopie původní archiválie nebo důkazního materiálu.
služba	Zápis dat do badatelského listu	
komponenta	Archiv	Skládá se z logické (softwarové) části starající se o procesy v archivu a fyzické (hardwarové) části starající se o bezpečné garantované uložení dat.
funkce	Validace dokumentu	Archiválie podepsaná osobním elektronickým podpisem založeným na kvalifikovaném certifikátu nebo označená elektronickou systémovou značkou založenou na kvalifikovaném certifikátu je tímto bezpečnostním prvkem zafixována. Systém musí kontrolovat platnost certifikátu, na kterém je podpis založen. Validace certifikátu spočívá v kontrole, zda jej vydal kvalifikovaný poskytovatel služeb vytvářejících důvěru a zda je certifikát platný a nebyl uveden na seznamu zneplatněných certifikátů. V rámci kontroly je provedeno porovnání s CRL seznamy kvalifikovaných poskytovatelů služeb vytvářejících důvěru a vyhodnocení, zda použité certifikáty jsou k testovanému datu platné.
funkce	Ukládání dokumentů	Funkce Archivu, zajišťující dlouhodobé, trvalé uložení archiválií v elektronické podobě.
funkce	Balíčkování	Funkce Archivu pro tvorbu archivních balíčků zajišťujících dlouhodobou platnost celé sady archiválií, což vede k optimalizaci procesu razítkování a přerazítkování archiválií tak, aby byly minimalizovány náklady za razítka od časové autority.

Tabulka 23: **Katalog všech aplikačních komponent řešení a klíčových aplikačních funkcí:**		
Typ prvku	**Název prvku**	**Vysvětlení významu aplikačních komponent, funkcí a služeb**
funkce	Zpřístupnění dat	Funkce Archivu, zajišťující přístup k uloženým dokumentům pro archiváře a Badatelskému portálu přes Bránu, vyhledání archiválií, editaci a doplňování metadat.
funkce	Selektivní vyřazení archiválie	Funkce Archivu, zajišťující skartaci dokumentů. Skartační řízení standardně probíhá v ESA MO. Do DA MO postoupí pouze dokumenty vybrané zde za archiválie. V DA MO může dojít ke k vyřazení pouze výjimečně (přehodnocení významu, poškození apod.), ale ne na základě skartačního řízení.
funkce	Transformace dokumentů	Funkce Archivu, zajišťující tvorbu interpretací dokumentů s nižším rozlišením, opatření vodoznakem, anonymizaci apod.
funkce	Administrace a konfigurace	Data v DA MO jsou rozdělena do pracovních prostorů, kde každý prostor má svého správce, který může dalším uživatelům přidělovat právo práce v tomto pracovním prostoru.
komponenta	Badatelský portál	Komponenta, která zajišťuje přístup k archiváliím všem uživatelům, kteří se zaregistrují. Dále slouží ztotožněným badatelům. Badatelský portál je bezpečně oddělen od vlastního Archivu a jsou v něm uloženy kopie metadat a interpretací archiválií s vodoznakem. Elektronické originály a právně závazné archiválie jsou z Archivu poskytovány oprávněným (pouze ztotožněným) uživatelům na základě jejich požadavků, přičemž správu těchto požadavků realizuje Portál.
komponenta	Webová prezentace VHA	Veřejný přístup je na stránkách www.vuapraha.cz. V rámci DA MO bude rozšířen o prezentaci Badatelského portálu. DA MO nebude součástí federované knihovní identity v ČR.
funkce	Přihlášení a ztotožnění uživatele	Funkce portálu zajišťující selektivní přístup uživatelů k informacím dle úrovně autentifikace.
funkce	Přístup k archiváliím	Funkce portálu zajišťující přihlášeným externím uživatelům vyhledávání archiválií, včetně historie hledání pro aktuální sezení, listování v seznamu vyhledaných archiválií, zobrazení náhledů na archiválie s vodoznakem ve webovém prohlížeči, zobrazení příslušných metadat. Poskytuje pracovní prostor pro ztotožněné uživatele s možností stáhnout si vyžádané archiválie.
funkce	Uživatelské statistiky	Funkce portálu zajišťující ztotožněným uživatelům zobrazení statistických údajů (seznam realizovaných/běžících žádostí o poskytnutí kopie původních archiválií s časovým rozlišením apod.).
funkce	Administrace	Funkce portálu zajišťující administrátorům vytváření a správu účtů externích uživatelů, zakládání ztotožněných uživatelů, zobrazení statistických údajů.
funkce	Diskusní fórum	
Ostatní komponenty, funkce a aplikační služby integrované na výše uvedené nebo jinak podstatné pro žádost		
Zvolte položku.		
Zvolte položku.		

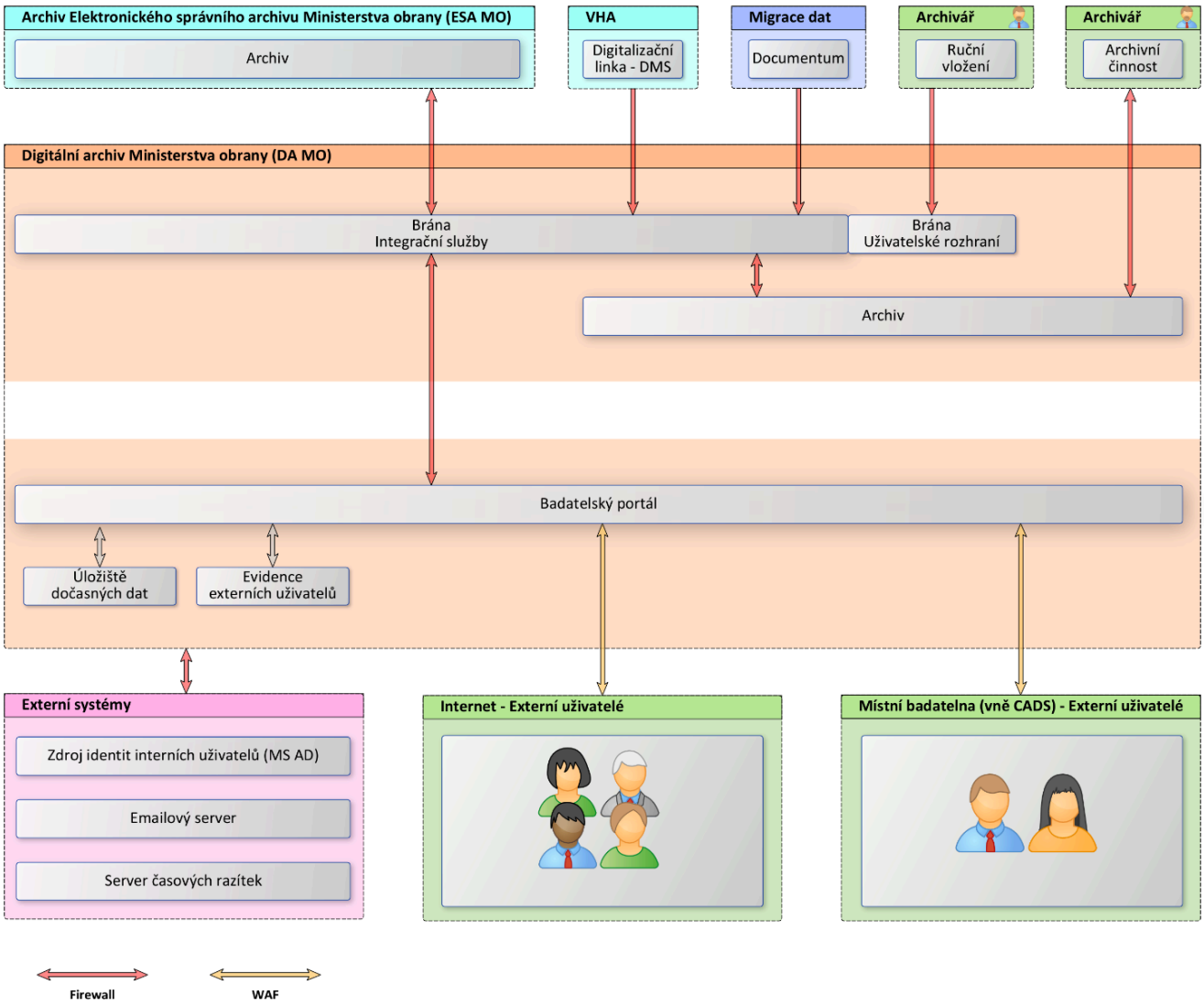
Tabulka 24: **Katalog aplikačních rozhraní** (mezi dvěma různými komponentami A, B):			
Název aplikačního rozhraní	**Komponenta A**	**Komponenta B**	**Vysvětlení obsahu a významu rozhraní aplikačních komponent**
Interní rozhraní (aplikací řešení mezi sebou, na aplikace uvnitř úřadu, případně resortu, krajské korporace, apod.)			

Tabulka 24: **Katalog aplikačních rozhraní** (mezi dvěma různými komponentami A, B):			
Název aplikačního rozhraní	**Komponenta A**	**Komponenta B**	**Vysvětlení obsahu a významu rozhraní aplikačních komponent**
Brána DA MO	ESA MO	Archiv	Rozhraní pro přijímání dokumentů charakteru archiválie z Elektronického správního archivu.
Badatelský portál	Badatelna	Archiv	Rozhraní pro přístup k archiváliím pro uživatele přihlášené na pracovišti místní badatelny VÚA.
Autentizační rozhraní DA MO	Přístupová brána	MS AD	Zdrojem identit interních uživatelů je Active Directory Štábního informačního systému AČR.
Externí rozhraní (na aplikace eGovernmentu a jiných úřadů, případně jiná rozhraní)			
Webové rozhraní VÚA	Webový prohlížeč	DA MO	Webové stránky VÚA, pomocí kterých lze přistupovat k některým funkcím DA MO.
Autentizační rozhraní DA MO	Přístupová brána	Externí identity	Rozhraní pro autentizaci a autorizaci externích uživatelů.
Brána DA MO	Server časových razítek	Archiv	Zajišťuje přerazítkování dokumentů pro udržení dlouhodobé, trvalé platnosti prvků elektrického zabezpečení archiválií.
Replikace	Primární lokalita	Sekundární lokalita	Úložiště DA MO bude podporovat synchronizaci dat do geograficky vzdálené lokality tak, aby bylo minimalizováno riziko ztráty dat při ohrožení jedné lokality.

Tabulka 25: **Katalog aplikacemi podporovaných agend (vazební tabulka aplikací na katalog agendových funkcí v kapitole 2.2.3 - Byznys architektura):**	
Realizovaný systém	**Agenda**
DA MO	A1343 Archivnictví a spisová služba

Model aplikační architektury – pohled struktury aplikací

zde vložte diagram(y), které odpovídají tomu, co je uvedeno výše



Model aplikační architektury – pohled komunikace aplikací

zde vložte diagram(y), které odpovídají tomu, co je uvedeno výše

Tabulka 26: **Katalog komunikačních (obslužných) rozhraní, kanálů koncových klientů:**				
Rozhraní	**Využití**	**Počet uživatelských přístupů ročně**	**Č. žádosti o výjimku**	**Popis využití rozhraní v projektu**
Asistovaná přepážka				
Přepážka úřadu	Ano	2300		Badatelé mohou navštívit VHA a zde mohou na základě povolení do badatelské místnosti využít prostředků poskytnutých k zajištění přístupu do Badatelského portálu.
CzechPOINT (přepážka)	Nerelevantní			„Systém ze zákona neobsahuje proces elektronického podání od veřejnosti“.
Call-centrum	Nerelevantní			„Systém ze zákona neobsahuje proces elektronického podání od veřejnosti“.
Webový portál				

Tabulka 26: **Katalog komunikačních (obslužných) rozhraní, kanálů koncových klientů:**				
Rozhraní	**Využití**	**Počet uživatelských přístupů ročně**	**Č. žádosti o výjimku**	**Popis využití rozhraní v projektu**
Aplikace v portálu úřadu s autentizovaným klientem	Nerelevantní			„Systém ze zákona neobsahuje proces elektronického podání od veřejnosti“.
Aplikace v Portálu občana jako střechovém portálu VS	Nerelevantní			„Systém ze zákona neobsahuje proces elektronického podání od veřejnosti“.
Tlustý aplikační klient	Ne			
Mobilní aplikace	Ne			
CzechPOINT@office	Nerelevantní			„Systém ze zákona neobsahuje proces elektronického podání od veřejnosti“.
Datová zpráva (ISDS)				
Formulář v DS	Nerelevantní			„Systém ze zákona neobsahuje proces elektronického podání od veřejnosti“.
Elektronicky podepsaný dokument do e-Podatelny				
E-mail s elektronicky podepsaným formulářem	Ano			
Webová aplikace pro zaslání elektronicky podepsaného dokumentu do e-Podatelny	Ano			
Listinnou cestou do podatelny				
Formulář listinou poštou	Ano			
Formulář na listinnou podatelnu (osobně)	Ano			
Jiné				
E-mail s formulářem bez elektronického podpisu	Ano			
Aplikace v portálu úřadu s neautentizovaným klientem	Ano			
Aplikační rozhraní pro externí systémy	Ano			Propojení s Portálem Národního digitálního archivu. Výstupy z interních aplikací PEvA a ELZA budou předávány do druhotné a ústřední evidence.

Tabulka 27: **Dodržení architektonických principů aplikační vrstvy:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
Použitelnost	Umožní design služeb i systému, v případě spolupráce	Ano		

Tabulka 27: **Dodržení architektonických principů aplikační vrstvy:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
	úřadů na řešení životní situace/události klienta, řazení (orchestrování) do komplexního automatizovaného řešení?			
Transparentnost	Počítá projekt s prostředky pro zveřejňování měření a auditů výkonnosti poskytovaných služeb?	Ano		Předpokládá se automatické zveřejňování základních statistických dat o celkovém objemu počtech archivovaných dokumentů, roční přírůstky archiválií a další požadované a zveřejnitelné statistiky ve formě otevřených údajů.
Bezpečnost	Počítá projekt s auditovatelností a průkazností služeb veřejné správy a vytvářením auditní stopy (provozních logů) pro tento účel?	Ano		Veškeré přístupy do úložiště a nakládání s dokumenty budou standardně logovány. Auditní záznamy bude možné ukládat, pořizovat a přistupovat k nim nezávisle tak, aby nebyla možná jejich kompromitace ze strany databázového správce.
Udržitelnost	Byl upřednostněn nákup a implementace standardní služby před vývojem vlastního řešení?	Ano		Řešení je poptáváno na základě veřejné zakázky zadané v otevřeném řízení.
	Umožní otevřená modulární architektura projektu vyměňovat jednotlivé prvky řešení bez nutnosti měnit jejich okolí?	Ano		Projekt je navrhován jako modulární a škálovatelné řešení, složené ze samostatných hardwarových a aplikačních komponent, které mezi sebou komunikují. Výměna jednotlivých prvků neovlivní ostatní komponenty. Integrace vlastních komponent bude umožněna přes API.
Technologická neutralita	Budou elektronické služby veřejné správy v projektu dostupné na všech běžně používaných klientských platformách?	Ano		Webové rozhraní VÚA je platformově nezávislé. OpenSource komponenty mohou být v řešení použity. Předpokladem je technologická neutralita.

Tabulka 28: **Vysvětlení v kontextu aplikační architektury úřadu, tedy:**
a) jaké k projektu existují či vznikají duplicity?
V rámci primární lokality nezavádí navrhované řešení žádné duplicitní technologické komponenty. V maximální míře budou využity existující hardwarové prostředky VÚA. Vybudování sekundární lokality sice znamená vytvoření duplicitních technologických komponent, tato duplicita je však žádoucí (a nutná) z pohledu zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
b) proč a jaké jsou další souvislosti?
Vysvětlení aplikační architektury projektu:
Řešení je tvořeno těmito základními aplikačními komponentami: • Brána DA MO – je rozhraním DA MO, které odděluje zdrojové systémy, uživatele a Archiv. Brána poskytuje komunikační rozhraní pro vstup dokumentů, funkce pro práci archivářů, funkce badatelny a přehledové a statistické funkce poskytující informace o stavu archivu.

Tabulka 28: **Vysvětlení v kontextu aplikační architektury úřadu, tedy:**
• Badatelský portál – zajistí veřejnou prezentaci archiválií uložených v DA MO. Zajistí se tak možnost prezentace všech archiválií ukládaných v digitální podobě v rámci Vojenského historického archivu. Jsou v něm uloženy kopie metadat a vybraných interpretací archiválií s vodoznakem. Zásadní důraz je kladen na zabezpečené oddělení Badatelského portálu od vlastního Archivu. Dále bude součástí tohoto portálu webová prezentace Vojenského ústředního archivu s novým grafickým návrhem a s obsahem obdobným, jako je ve stávající podobě dostupný na adrese www.vuapraha.cz. Webová prezentace bude vícejazyčná (umožnění překladu do angličtiny, němčiny, ruštiny, francouzštiny a italštiny). Bude také obsahovat volně přístupnou (bez registrace uživatele) databázi VHA. • Archiv – je tvořen komponentou důvěryhodného elektronického archivu, který se stará o zachování důvěryhodnosti uložených elektronických archiválií. Popis komunikačních rozhraní: Komunikace mezi jednotlivými částmi stávajícího řešení (Archiv, Brána, Badatelna) je realizována pomocí standardních komunikačních rozhraní WS-SOAP, REST, EJB, LDAP a CMIS. Při komunikaci s vnějšími systémy jsou využity rozhraní LDAP, TSP, OCSP, SOAP a REST a je též využita sdílená složka pravidelně kontrolována skenerem souborového systému. • Brána DA MO – zajišťuje komunikaci mezi části Archiv a okolními systémy včetně části Badatelna. Mimo toto rozhraní neprobíhá mezi těmito komponentami žádná jiná komunikace. Brána poskytuje komunikační rozhraní pro vstup dokumentů, funkce pro práci archivářů, funkce badatelny a přehledové a statistické funkce poskytující informace o stavu archivu. Komunikace Brány a Archivu probíhá prostřednictvím zabezpečeného transportního protokolu po interní síti DA MO. Oba moduly jsou odděleny firewallem, který umožňuje pouze tuto komunikaci. Modul Archivu je integrován s garantovaným úložištěm pomocí API, které úložiště poskytuje. Žádný jiný modul s garantovaným úložištěm přímo nekomunikuje, pouze prostřednictvím služby logické vrstvy. Modul Archivu není přímo integrován s žádnou interní, nebo externí službou. Pokud potřebuje funkcionality takové služby, jsou zprostředkovány prostřednictvím Brány. Popis komunikace s externími systémy: • Zdroj identit externích uživatelů - k přihlášení (autentizaci) bude použit doménový zdroj identit MS AD. DA MO bude mít vlastní LDAP, v němž budou definovány jednotlivé uživatelské role. • Emailový server – bude využíván pro odesílání notifikací interním zaměstnancům archivu a garantům jednotlivých zdrojových systémů. Archiv s emailovým serverem komunikuje pomocí protokolu SMTP. • Kvalifikovaný poskytovatel služeb vytvářejících důvěru - služby těchto poskytovatelů budou využívány pro ověřování platnosti kvalifikovaných certifikátů. Ověřování probíhá buď pomocí protokolu OCSP nebo stažením CRL a porovnáním certifikátu s tímto seznamem. • Autorita časových razítek – pro zafixování archivních balíků v čase budou využívána časová razítka poskytována akreditovanou autoritou časových razítek (TSA). Archiv s touto službou komunikuje pomocí protokolu TSP (transportní protokol je HTTPS).

*2.2.4.2. Aplikační architektura – část: **Datová** architektura*

Tabulka 29: **Katalog základních datových entit projektu:**		
Objekt reálného světa, který je předmětem evidence	**Vysvětlení objektu**	**Je objekt čerpán nebo poskytován jiným subjektům?**
Archiválie	Dokument, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiválií.	Je poskytován jiným subjektům
Fyzická osoba	Na základě podané žádosti registrovaný/ztotožněný uživatel Badatelského portálu.	Je čerpán od jiného subjektu

Tabulka 30: **Využití datového fondu základních registrů a dalších agend:**			
Název	**Použito**		**Vysvětlení**
Základní registry			
Způsob vedení datového kmene	Nerelevantní		
Evidujeme subjekty práva, které nejsou vedeny v ZR (např. zahraniční)	Ne		
Evidujeme fyzické osoby, které nejsou vedeny v ROB	Ne		
Využití údajů publikovaných prostřednictvím kompozitních služeb editorů Základních registrů			
Evidence obyvatel (ISEO)	Nerelevantní		
	Č. žádosti o výjimku:		
Cizinecký informační systém (CIS)	Nerelevantní		
	Č. žádosti o výjimku:		
eGon Service Bus			
Čerpání dat přes eGSB	Nerelevantní		
	Č. žádosti o výjimku:		
Publikování vlastních dat přes eGSB	Nerelevantní		
	Č. žádosti o výjimku:		

Tabulka 31: **Způsob zajištění vedení dat s ohledem na otevřená data veřejné správy:**			
Požadavek	**Použito**		**Vysvětlení**
Zajištění přístupu k datům			
Budete mít zajištěn přístup k veškerým datům vedeným v databázích dotčených předmětem projektu ve strojově čitelném a otevřeném formátu?	Ano		Přístup k datům bude zajištěn prostřednictvím API, které budeme moci kdykoliv využívat k získání veškerých údajů ze všech databází dotčených předmětem projektu ve strojově čitelném a otevřeném formátu ve smyslu § 3 odst. 7 a 8 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. K API budeme mít k dispozici dokumentaci popisující syntaxi a sémantiku jeho datových struktur a syntaxi, sémantiku a způsob přístupu k operacím, které API nabízí.
	Č. žádosti o výjimku:		
Budete mít výše popsaný přístup k datům zajištěn bez dodatečných finančních nákladů?	Ano		Přístup k datům budeme moci využívat bez dodatečných nákladů, dodavatelem nebudou zpoplatňovány ani přístupy k API ani provádění jednotlivých exportů obsahu databází.
	Č. žádosti o výjimku:		
Budete moci se zpřístupněnými daty libovolně nakládat?	Ano		Nebudeme žádným způsobem, s výjimkou právních předpisů, omezeni v nakládání se získanými daty.
	Č. žádosti o výjimku:		

Tabulka 31: **Způsob zajištění vedení dat s ohledem na otevřená data veřejné správy:**			
Požadavek	**Použito**		**Vysvětlení**
Publikace výstupů ve formátu otevřených dat. Všechna digitální díla v majetku knihovny MO ČR.			
Budou data vedená v databázích dotčených předmětem projektu zveřejňována jako otevřená data?	Ano		Souhrnné statistiky budou zveřejňovány jako otevřená data dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
	Č. žádosti o výjimku:		
Jaké datové oblasti plánujete zveřejňovat jako otevřená data, kdy a na jakém stupni otevřenosti?			Projekt předpokládá sdílení generovaných základních statistických údajů, které budou poskytovány v souladu s podmínkami pro otevřená data státní správy.

Tabulka 32: **Nakládání s osobními a citlivými údaji**	
Způsoby identifikace subjektů (FO, PO) v informačním systému (AIFO, IČO, rodné číslo nebo jiný identifikátor)	
Primární přihlášení interního uživatele proběhne formou autentizace (jménem a heslem) vůči Active Directory CADS. Registrovaní a ztotožnění uživatelé DA MO se autentizují jménem a heslem vůči internímu LDAP DA MO.	
Způsoby zavedení základních principů práce s osobními a citlivými údaji dle GDPR:	
Zabezpečení zpracování:	Některé osobní údaje v souborech budou odstraněny, případně se jen nahradí jinými a to takovým způsobem, že identifikace konkrétní fyzické osoby bude po přiřazení dodatečných údajů možná. Pojmově se tedy nejedná o nevratný proces, ale jen o dočasné funkční oddělení určitého „podsouboru údajů“ od ostatních údajů, které společně identifikaci umožňují.
Právo na přístup:	Pokud se bude jednat o žádost podle čl. 15, bude informace o přijatých opatřeních poskytnuta bez zbytečného odkladu a v každém případě do 1 měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení, a to v době jednoho měsíce od podání žádosti.
Právo na opravu:	Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho budou týkat. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů a to i poskytnutím dodatečného prohlášení.
Právo na výmaz:	Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat.
Právo na omezení zpracování:	Subjekt údajů má právo na to, aby správce omezil zpracování případech, kdy subjekt popírá přesnost osobních údajů, zpracování je protiprávní a subjekt odmítá výmaz osobních údajů, správce údaje již nepotřebuje pro účely zpracování, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků, subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, že důvody správce převažují nad oprávněnými důvody subjektu údajů. Pokud bylo zpracování omezeno, mohou být osobní údaje s výjimkou jejich uložení zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné osoby nebo důležitého veřejného zájmu.
Právo na oznamovací povinnost:	Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s čl.16, čl.17 a čl.18 s výjimkou případů, kde se ukáže jako nemožné, nebo to vyžaduje nepřiměřené úsilí.
Právo na přenositelnost:	Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci v běžně používaném čitelném formátu a právo předat tyto údaje jinému správci aniž by tomu správce, kterému byly osobní údaje poskytnuty bránil.

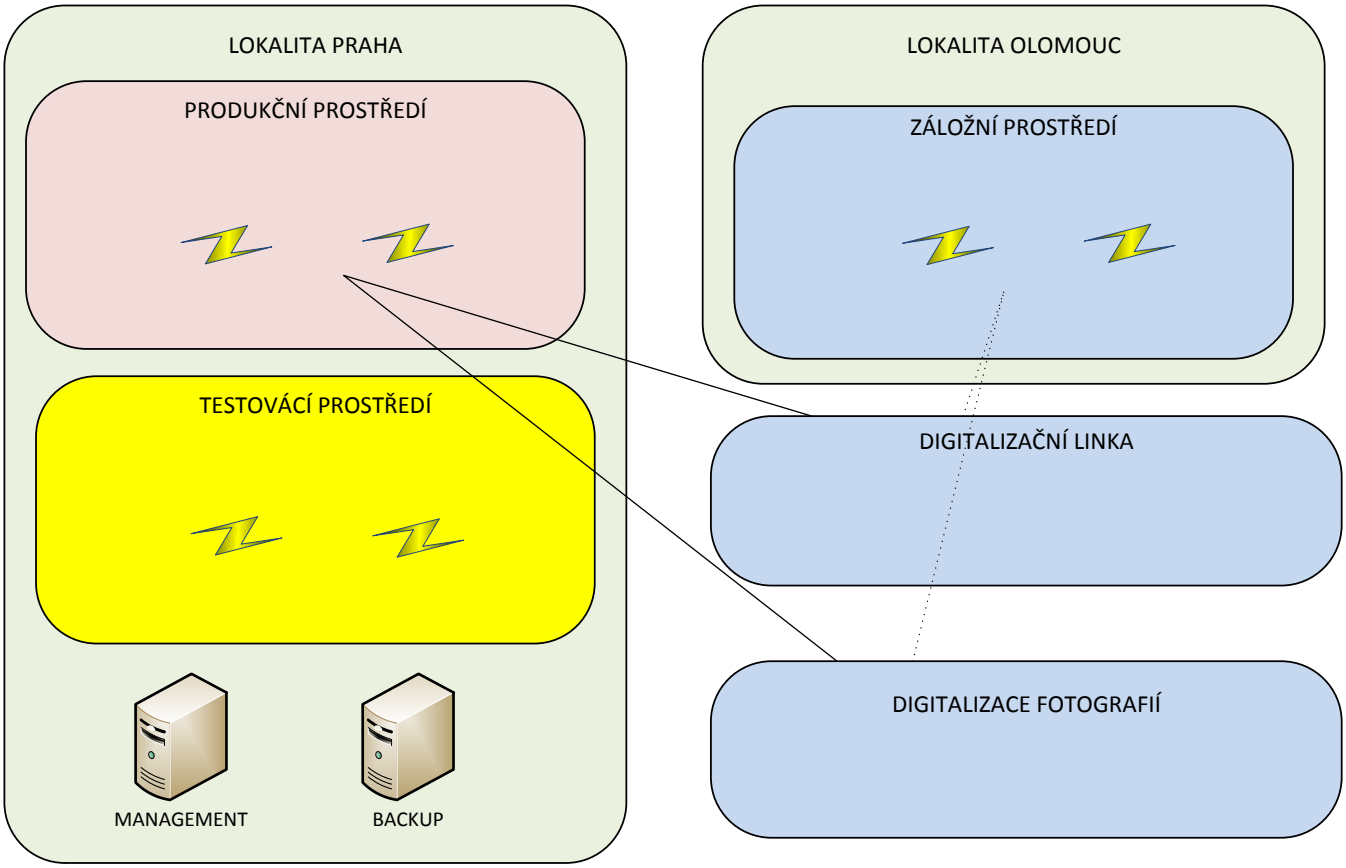
Tabulka 33: **Dodržení architektonických principů datové vrstvy:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
Důvěryhodnost	Jakým způsobem zajistíte, aby vzájemně vyměňované informace byly spolehlivé, přesné, relevantní a aktuální a aby klienti elektronické komunikaci důvěřovali?	Ano		Přístup k systému bude zajištěn pomocí šifrovaného protokolu, údaje budou on-line ověřovány vůči referenčním údajům a číselníkům.
Bezpečnost	Jakým způsobem zajistíte, aby v projektu byla zajištěna adekvátní ochrana osobních údajů a utajovaných informací?	Ano		Veřejné elektronické služby budou poskytovány výlučně za podmínek, které jsou pro tyto služby předepsány. Zneužití služeb je vyloučeno nezbytnou identifikací.

Tabulka 34: **Vysvětlení v kontextu datové architektury úřadu, tedy:**
a) jaké k projektu existují či vznikají duplicity?
K archiváliím budou uživatelé přistupovat prostřednictvím Badatelského portálu, na kterém budou pracovníky archivu zveřejňovány interpretace vybraných archiválií. Interpretací se rozumí kopie dané archiválie ve formátu vhodném k uveřejnění na portálu nebo ve formátu vhodném k poskytnutí žádajícímu subjektu (např. změna formátu z TIFF na komprimovaný pdf, případná anonymizace, u hromadně zveřejněných archiválií také vodoznak). Uživatelé nebudou přistupovat přímo k archiváliím uloženým v archivu, ale k takto duplicitně vytvořeným interpretacím. Vybudování sekundární lokality znamená vytvoření kompletní datové duplicity uložených archiválií. Tato duplicita je však žádoucí (a nutná) z pohledu zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
b) proč a jaké jsou další souvislosti?
Vysvětlení aplikační architektury projektu:

2.2.5. Technologická architektura – vrstva IT technologie (HW a SW)

Tabulka 35: **Katalog uzlů a klíčových funkcí nebo služeb:**		
Typ prvku	**Název prvku**	**Vysvětlení významu uzlu, funkce nebo služby**
Technologický uzel	Server Brány	2 servery (pro primární a sekundární lokalitu), OS RHEL 6.9, databáze DB2.
Technologický uzel	Server Archivu	2 servery (pro primární a sekundární lokalitu), OS RHEL 6.9, databáze DB2.
Technologický uzel	Server Badatelského portálu	2 servery (pro primární a sekundární lokalitu), OS RHEL 6.9, databáze DB2.
Technologický uzel	Servery Testovacího prostředí	3 servery (Brána, Archiv, Badatelský portál pouze pro primární lokalitu), OS RHEL 6.9, databáze DB2.
Technologický uzel	Server Backup	Zálohovací server OS WIN 2016 Server.
Technologický uzel	Server Správa	Server pro management, OS RHEL 6.9, databáze DB2.
Technologický uzel	Garantované úložiště	Totožné pro primární a sekundární lokalitu. Založeno na SW/HW produktech IBM FileNet ve spolupráci s GPFS - IBM Spectrum Scale a IBM StorWise s požadovanou kapacitou.
Technologická služba	Digitalizace	Modul pro digitalizaci papírových dokumentů a fotoarchivu.

Model technologické architektury – pohled struktury IT technologické architektury



Tabulka 36: **Využití sdílených IT technologických a platformových služeb:**		
Název	**Popis**	**Použito**
PaaS	Pronájem technologií v datovém centru externího subjektu	Ne
DC eGOV	Využití centrálních prvků provozního a bezpečnostního monitoringu Dohledového centra eGOV (MV)	Ne

Tabulka 37: **Vysvětlení v kontextu technologické architektury úřadu, tedy:**
a) jaké k funkčnímu celku existují či vznikají duplicity?
Realizací projektu nevzniknou žádné duplicity k existujícím technologiím. Vznikne pouze vnitřní duplicita budovaného funkčního celku – primární a sekundární lokalita.
b) proč a jaké jsou další souvislosti?
Vybudování sekundární lokality sice znamená vytvoření duplicitních technologických komponent, tato duplicita je však žádoucí (a nutná) z pohledu zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
Vysvětlení technologické architektury funkčního celku:

2.2.6. Technologická architektura – vrstva komunikační infrastruktury

Tabulka 38: **Katalog infrastrukturních komunikačních funkcí, sítí, cest a klíčových služeb:**		
Typ prvku	**Název prvku**	**Vysvětlení významu infrastrukturních funkcí, sítí, cest a služeb**
Uzel		
Komunikační síť		

Model technologické architektury – pohled struktury komunikační infrastruktury

<zde vložte diagram(y)>

V projektu DA MO budou využity síťové komponenty stávajícího systému ESA MO.

Tabulka 39: **Využití sdílených služeb komunikační infrastruktury:**			
Název	**Popis**	**Použito**	**Č. žádosti o výjimku**
CMS	Pro publikaci a přístup k vytvářeným službám je využito Centrální místo služeb – aplikace jsou publikovány prostřednictvím CMS	Nerelevantní	
KIVS	Využití komunikační infrastruktury veřejné správy, tj. fyzického propojení infrastruktury úřadů nebo VPN připojení k CMS	Nerelevantní	
NDC	Umístění technologií do Národních datových center v perimetru CMS	Ne	
Housing (IaaS)	Využití umístění vlastní HW infrastruktury do prostor datového centra třetí strany	Ne	

Tabulka 40: **Vysvětlení v kontextu architektury komunikační infrastruktury úřadu, tedy:**
a) jaké k projektu existují či vznikají duplicity a proč?
Realizací projektu nevzniknou žádné duplicity k existujícím technologiím. V projektu DA MO budou využity síťové komponenty stávajícího systému ESA MO.
b) jaké jsou další souvislosti?
Vysvětlení architektury komunikační infrastruktury projektu:

2.2.7. Bezpečnostní architektura

Tabulka 41: **Katalog bezpečnostní architektury projektu:**		
Dotčený nebo bezpečnostní prvek	**Hrozba / riziko**	**Vysvětlení způsobu zmírnění hrozby / rizika prvkem architektury**
Rizika zadavatele	Vnější změny podmínek zakázky	Změna legislativy ČR nebo EU s dopadem na rozsah a obsah plnění veřejné zakázky – V1, D4, ZR4. Správní nebo soudní rozhodnutí ve věci zakázky - např. Zrušení veřejné zakázky – V1, D5, ZR5.
	Sponzorství projektu	Nedostatečná podpora vedení – V2, D3, ZR6.
	Zadání identifikace předmětu	Změna rozsahu – V1,D4,ZR4. Nesprávné nebo nedostatečně vyjednané smluvní podmínky – V1, D2,ZR2.
	Řízení projektu	Nevyhovující řízení projektu plnění veřejné zakázky – V3, D3, ZR9. Nedodržení projektových milníků – V3, D3, ZR9. Nevyhovující řízení kvality plnění veřejné zakázky – V3, D3, ZR9. Nesoučinnost třetích stran – V4, D4, ZR16. Nesoučinnost vlastní. Nedostatečné znalosti uživatelů řešení ze strany zadavatele, např. z důvodu fluktuace pracovníků – V3, D2, ZR6. Nedostatečná informovanost v rámci projektu (případně nízká kvalita předávaných informací) – V4, D2, ZR8. Nedostatečná koordinace s ostatními projekty – V2, D2, ZR4.
Rizika dodavatele	Sponzorství projektu	Nedostatečná podpora vedení – V2, D2, ZR4.

Tabulka 41: **Katalog bezpečnostní architektury projektu:**		
Dotčený nebo bezpečnostní prvek	**Hrozba / riziko**	**Vysvětlení způsobu zmírnění hrozby / rizika prvkem architektury**
	Zadání identifikace předmětu Řízení projektu	Nesprávné nebo nedostatečně vyjednané smluvní podmínky – V1, D2,ZR2. Nevyhovující řízení projektu plnění veřejné zakázky – V3, D3, ZR9. Nedodržení projektových milníků - V3, D3, ZR9. Nevyhovující řízení kvality plnění veřejné zakázky - V3, D3, ZR9. Nevyhovující řízení rizik plnění veřejné zakázky - V3, D3, ZR9. Nesoučinnost třetích stran – V4, D4, ZR16. Nesoučinnost vlastní. dodavatele, např. z důvodu fluktuace pracovníků – V3, D4, ZR12. Nedostatečná informovanost v rámci projektu (případně nízká kvalita předávaných informací) – V3, D3, ZR9. Nedostatečná koordinace s ostatními projekty – V3, D3, ZR9. **Vysvětlivky**: Výskyt rizika – V Dopad – D Závažnost rizika – ZR Závažnost nízká – 1 až 4 Závažnost střední – 5 až 9 Závažnost vysoká – >10

Tabulka 42: **Dodržení architektonických principů bezpečnostní architektury:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
Bezpečnost	Ochrání projekt prostředky poskytování elektronických služeb veřejné správy před poškozením a zneužitím?	Ano		Navržené řešení bude nakonfigurováno podle obecných doporučení pro bezpečný vývoj. Jednotlivé komponenty řešení, vč. Brány a Archivu, budou odděleny firewallem s bezpečně definovanými pravidly komunikace. Součástí zabezpečení je i segmentace sítě, ACL, statefull inspekce. Součástí řešení je i IPS sonda, která provádí skenování provozu na základě signatur i chování, Virtual patching,

Tabulka 43: **Vysvětlení bezpečnostní architektury projektu:**
Kontrola přístupu do databáze a auditní záznamy Navržené řešení obsahuje nástroje, které poskytují informace o veškerých aktivitách prováděných s databází včetně těch, které jsou spuštěny pod privilegovanými účty. Veškeré aktivity s databází jsou ukládány v auditním záznamu, jehož součástí jsou i veškeré transakce, které během spojení proběhly. Auditní záznamy jsou oddělené od správy databáze, a tak není možná modifikace ze strany databázového správce nebo privilegovaných uživatelů databáze. Další formou ochrany je možnost nastavit bezpečnostní pravidla pro přístup do databáze, kterými lze kontrolovat jednotlivé přístupy. **Zabezpečení databází** Řešení je navrženo tak, že uživatelé nemají žádné práva a přímé přístupy do databází, a lze je tak bezpečně chránit před útoky pomocí pravidel na firewallu. Řešení poskytuje další možnosti ochrany i tzv. Virtual Patching, který chrání citlivá data v období, kdy je známá určitá zranitelnost databáze, ale ještě nedošlo k instalaci bezpečnostního updatu. Řešení poskytuje několik úrovní zabezpečení přístupu uživatelů k datům. Na úrovni uložiště v částech Brány a Archivu je možné řídit přístup uživatelů pomocí tzv. ACL (Access Control List). Obdobným způsob lze řídit oprávnění i na úrovni databáze. Řešení obsahuje mechanismy, jak nezávisle na DB správci a zásahu do databáze kontrolovat přístup a provoz nad databází, včetně možnosti omezení přístupu k databázi mimo standardní pracovní okno či okruh uživatelů. Řešení umožňuje pořizovat auditní záznamy vč. privilegovaných uživatelů a nelze je měnit. Auditní záznamy jsou ukládány odděleně od databáze v prostředí specializovaného nástroje. Řešení umožňuje pravidelně automaticky provádět bezpečnostní testy s účelem odhalit zranitelnosti a hrozby. Řešení umožňuje nepřetržitý monitoring používání a toku citlivých údajů uložených v databázích. Nástroj poskytuje možnosti blokování provozu na základě IP adres, uživatelských jmen, tabulek apod. a dále je schopné identifikovat anomálie. Je možné klasifikovat citlivá data a nastavovat politiky pro jejich maskování. Nástroj umí zasílat alerty při porušení předdefinovaných pravidel. Řešení obsahuje vzorové sady pravidel pro požadavky GDPR a poskytuje možnost vytvoření klasifikačních pravidle např. Podle regulárních výrazů, porovnání se slovníkem, programovatelného API rozhraní. Je možné také sestavit různé reporty. **Zaručení integrity prostředí** Bude umožněno vytvoření white-listu softwarového vybavení, které nepovolí změnu softwarového vybavení kromě jasně definovaných výjimek pro určité aplikace. Dále toto řešení poskytuje kontrolu a monitorování změn v konfiguračních souborech. Veškeré operace budou logovány a tím bude udržován auditní záznam změn. Produkty pro zajištění bezpečnosti umožňují připojení na SIEM systémy a jejich výpadek neohrozí funkčnost celého řešení. **WAF** Pro ochranu Portálu bude nainstalován web aplikační firewall, který poskytuje i funkcionalitu dešifrování SSL provozu. Webový aplikační firewall umožňuje detekci a eliminaci nejrůznějších typů útoků, ať již běžných, tak i sofistikovanějších - např. XSS, Injection [SQL,OS, XML, HTML apod.] útoky, upload útoky, Clickjacking a celá řada dalších útoků.

2.2.8. Shoda s pravidly, standardizace a dlouhodobá udržitelnost

Tabulka 44: **Uveďte, které licence standardizovaných SW produktů budete pořizovat formou centrálních rámcových smluv zajištěných Ministerstvem vnitra. Pokud tento instrument nevyužijete, vysvětlete proč:**
Nákup SW formou centrálních rámcových smluv zajištěných Ministerstvem vnitra závisí na výběru konkrétního dodavatele DA MO a jím navrženého řešení. V úvahu připadá nákup virtualizačního SW VMware, serverových a databázových produktů Microsoft nebo IBM. Další pořizovaný SW jsou specifické produkty mimo oblast standardizovaného SW.

Tabulka 45: **Shoda se strategickými dokumenty:**			
Požadavek	**Odpověď**	**Č. žádosti o výjimku**	**Vysvětlení**
Je řešení v souladu s Informační koncepcí úřadu?	Ano		
Je řešení v souladu s Informační koncepcí ČR a cíli či principy Digitálního Česka?	Ano		Který z následujících podcílů IKČR projekt naplňuje? ☑ 1.4 Rozvoj on-line „front-office“ služeb jednotlivých rezortů ☐ 1.5 Zlepšení národního katalogu otevřených dat ☑ 3.3 Digitalizace dosud nedigitalizovaného obsahu ☑ 3.4 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu ☐ 3.7 Zavedení systému důvěryhodné elektronické identifikace do praxe ☑ 3.8 Vytvoření základních služeb sdílení dat ☐ 5.7 Podpora budování sdílených agendových systémů v přenesené působnosti ☐ 5.9 Propojený datový fond ☐ 5.10 Veřejný datový fond ☐ 5.11 Geoinformace ☐ Nemá vazbu na cíle IKČR
Je řešení v souladu s NAP?	**NEPOVINNÉ**		

Tabulka 46: **Dodržení architektonických principů architektury shody s pravidly:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
Udržitelnost	Je řešení navrženo pro efektivní údržbu a rozvoj, tj. jako standardizované, rozšiřitelné, integrovatelné, upgradovatelné a podporovatelné i vlastními silami úřadu?	Ano		Řešení je sice navrženo pro efektivní údržbu a rozvoj, jako standardizované, rozšiřitelné, integrovatelné, upgradovatelné a podporovatelné i vlastními silami úřadu. Nicméně není předpoklad, že pracovníci VÚA budou tyto činnosti provádět sami. V rámci projektu je požadována technická podpora HW a SW komponent a legislativní upgrade po dobu 60 měsíců s předpokladem uzavření

Tabulka 46: **Dodržení architektonických principů architektury shody s pravidly:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
				následných smluv na tuto činnost.
Spolupráce a sdílení	Jsou nové služby (nebo jejich součásti) koncipovány jako opakovatelné a komplementární ke sdíleným službám eGovernmentu?	Nerelevantní		
Udržitelnost	Je zajištěno, že je návrh byznys i IT řešení natolik robustní, modulární, škálovatelný, flexibilní a parametrizovatelný, aby se přizpůsobil očekávaným změnám za dobu jeho životnosti?	Ano		

Tabulka 47: **Vysvětlení standardizace a udržitelnosti architektury projektu:**

2.2.9. Přehled služeb čtyřvrstvé architektury

Model služeb v čtyřvrstvé vizi architektury veřejné správy nebo jednotlivé modely využití každé vrstvy vrstvou vyšší

<zde vložte diagram(y)>

Tabulka 48: **Dodržení architektonických principů 4 vrstvé architektury:**				
Princip	**Požadavek**	**Dodrženo**	**Č. žádosti o výjimku**	**Způsob a míra naplnění**
Technologická neutralita	Jsou odděleny jednotlivé vrstvy architektury řešení systémem služeb poskytovaných navzájem mezi vrstvami?	Ano		
	Je zajištěna separátní správa, dohled a provoz služeb na jednotlivých vrstvách?	Ano		

Tabulka 49: **Vysvětlení čtyřvrstvé architektury služeb projektu:**

2.3. Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu

Tabulka 50: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu:**			
Název architektonického vzoru eGovernmentu	**Byl dodržen vzor?**	**Č. žádosti o výjimku**	**Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu**
Centrální místo služeb			
Publikujete aplikační služby řešené tímto projektem do CMS druhé generace?	Nerelevantní		
Přistupujete ke službám Propojeného datového	Nerelevantní		

Tabulka 50: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu:**			
Název architektonického vzoru eGovernmentu	**Byl dodržen vzor?**	**Č. žádosti o výjimku**	**Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu**
fondu prostřednictvím CMS druhé generace?			
Jakým způsobem přistupujete do CMS druhé generace?	IPSec		
Univerzální kontaktní místo			
Publikujete na CzechPOINT všechny své samoobslužné služby tak, aby mohly být přístupné i asistovaně?	Nerelevantní		
Jste na centrálu CzechPOINT připojeni skrze systém CMS?	Nerelevantní		
Rozšířený backoffice úředníka			
Máte služby CzechPOINT@office integrovány do svých systémů?	Nerelevantní		
Budou všechny interní aplikace dostupné z intranetu úřadu/resortu?	Ano		
Bude využito principu Single Sign-On?	Nerelevantní		
ÚEP včetně eFakturace			
Máte zajištěno předvyplňování formulářů ÚEP všemi státu známými údaji subjektu?	Nerelevantní		
Máte zajištěn příjem a zpracování el. faktur?	Nerelevantní		
Elektronický systém spisové služby			
Je realizace propojení systému se spisovou službou vytvořena dle rozhraní definovaného v kapitole 9 Národního standardu?	Ano		Data do systému DA MO budou primárně přenášena pomocí automatizovaného elektronického rozhraní, které DA MO poskytne a které bude plně v souladu s NSESSS (Národní standard pro elektronické systémy spisové služby dle zákona č. 365/2000 Sb).
Informační systém datových schránek			
Je prováděno automatické vytěžování přijatých formulářů do informačního systému?	Nerelevantní		
Propojený datový fond			
Jste ke službám PPDF připojeni skrze CMS?	Nerelevantní		
Využíváte pro překlad identity mezi agendami služby ISZR?	Nerelevantní		
Využíváte pouze údaje, které máte explicitně uvedeny v daném zákoně?	Nerelevantní		

Tabulka 50: **Kontrola shody architektury řešení projektu se vzory sdílených služeb eGovernmentu:**			
Název architektonického vzoru eGovernmentu	**Byl dodržen vzor?**	**Č. žádosti o výjimku**	**Podrobný popis způsobu a míry dodržení vzorů návrhem řešení projektu**
Odebíráte na údaje PPDF notifikace skrze služby ISZR?	Nerelevantní		
Elektronická identita			
Využíváte služeb Národního bodu pro identifikaci a autentizaci?	Nerelevantní		
Používáte pro překlad identifikátoru identity do své agendy (BSI na AIFO) služeb ISZR?	Nerelevantní		
Využíváte při obsazení identifikované a autentizované osoby do role úředníka systém JIP/KAAS?	Nerelevantní		

2.4. Plán projektu

Tabulka 51: **Hrubý harmonogram předloženého projektu:**				
Fáze / milník	**Začátek**	**Konec**	**Základní náplň**	**Navazuje na**
Výběrové řízení	1. 2. 2020	30. 4. 2020	Výběr dodavatele podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek.	
Realizace projektu	**1. 5. 2020**	**15. 9. 2020**		Podpis smlouvy s vybraným dodavatelem
- Analýza	1. 5. 2020	1. 6. 2020	Zpracování Plánu projektu, analýzy, návrh řešení.	
- Dodávka	1. 5. 2020	15. 7. 2020	Dodávka HW a SW.	
- Implementace	1. 7. 2020	15. 9. 2020	Implementace HW a SW, konfigurace a testování SW, zaškolení, zpracování dokumentace.	
- Akceptace	1. 9. 2020	15. 9. 2020	Akceptační testy, předání díla.	
- Ukončení realizace projektu		15. 9. 2020	Závěrečná zpráva projektu.	
Zkušební provoz	16. 9. 2020	31. 12. 2020	Nejprve bude provedena migrace dat ze systému Documentum. Následně zkušební provoz prověří funkčnost systému DA MO, ELZA a DMS digitalizačního pracoviště, funkčnost dodaného systému, návrh řešení architektury, prověření dob odezvy primárního a záložního datového úložiště, migrace dat mezi oběma datovými úložišti a	Ukončení výstavby DA MO dodavatelem

Tabulka 51: **Hrubý harmonogram předloženého projektu:**				
Fáze / milník	**Začátek**	**Konec**	**Základní náplň**	**Navazuje na**
			způsob poskytování podpory Helpdesku. Součástí zkušebního provozu bude prověření přebírání neutajovaných elektronických dokumentů a digitalizovaných archiválií od původců z ESA MO a z DMS digitalizační linky a předávání uložených elektronických archiválií v rámci DA MO na Badatelský portál.	
Ostrý provoz s technickou podporou dodavatele DA MO	1. 1. 2021	15. 9. 2025	Standardní provoz s technickou podporou dodavatele řešení po dobu 60 měsíců.	Úspěšné ukončení zkušebního provozu
Pokračování provozu s TP vybraného dodavatele	16. 9. 2025			Návaznost na smlouvu o TP dodavatele řešení DA MO.

Tabulka 52: **Projektový kontext předkládaného projektu (v rozvojovém programu, portfoliu úřadu):**	
Předchozí projekty	**Popis návaznosti na předchozí projekty**
Elektronický správní archiv MO (ESA MO)	Projekt požaduje, aby navržené řešení DA MO přímo logicky, koncepčně i technologicky navazovalo na již realizovaný projekt implementace ESA MO.
Elektronický správní archiv MO – Datová úložiště (ESA MO – DÚ)	Projekt ESA MO byl v roce 2019 technicky zhodnocen pro dlouhodobé uchování digitálních záznamů MO.
Souběžné projekty	**Popis návaznosti na souběžné projekty**
Navazující projekty	**Popis návaznosti na budoucí projekty**

Tabulka 53: **Katalog rozvojových etap (přechodových architektur) – roadmapa:**		
Etapa/ přechodová architektura	**Milník**	**Přírůstky a změny v přechodových architekturách oblastí zahrnutých do projektu**
Vyplývající z vlastního funkčního celku (např. komplexního IS)		
Vyplývající z kontextu úřadu (roadmapy úřadu)		

Tabulka 54: **Vysvětlení plánu projektu:**

3. DALŠÍ ÚDAJE O PROJEKTU

3.1. Připravenost projektu k realizaci

3.1.1. Majetkoprávní vztahy projektu

Tabulka 55: **Majetkoprávní vztahy:**

Podmínka	Odpověď	Poznámka (důvod)
Budou vám udělena výhradní práva k užívání k dodávanému produktu?	Ne	
Budou vám udělena nevýhradní práva k užívání k dodávanému produktu?	Ano	Bude-li součástí plnění smlouvy na výstavbu DA MO předmět požívající ochrany autorského díla podle Autorského zákona, nabývá nabyvatel nevýhradní právo užít a po skončení poskytování služeb záruky a podpory dle smlouvy s dodavatelem DA MO dále modifikovat a upravovat takovéto autorské dílo všemi způsoby nezbytnými k naplnění účelu vyplývajícímu z uzavřené smlouvy, a to po celou dobu trvání autorského práva k autorskému dílu, resp. po dobu autorskoprávní ochrany.
Budou práva k autorskému dílu nějak omezena (IČO, konkrétní uživatel, převoditelnost a další šíření, úpravy produktu, parametry…)?	Ne	
Budete mít přístup ke zdrojovému kódu pro čtení?	Ano	Je vyžadováno, aby dodavatel ke každé uzavřené verzi počítačových programů na základě požadavku nabyvatele bezplatně dodal zdrojové kódy programů včetně komentářů a schéma datového modelu.
Bude vám či třetímu subjektu umožněno provádět údržbu, měnit produkt, upravovat jej či rozšiřovat bez souhlasu dodavatele?	Ne	
Budete mít přístup k aktuální technické dokumentaci produktu?	Ano	Součástí dodávky řešení DA MO je dodávka kompletní dokumentace, která zahrnuje vytvoření popisu řešení, provozní dokumentaci včetně popisu praktické údržby, řešení, příprava strategických plánů podle metodiky PLATTER (Planning Tool for Trusted Electronic Repositoriem) „Plán důvěryhodného digitálního repozitáře“.
Obsahuje budoucí smlouva ujednání o vyloučení odpovědnosti za výpadky fungování?	Ne	
Budou externí nákupy veřejně soutěženy?	Ano	

3.1.2. Finanční připravenost projektu

Tabulka 56: **Finanční připravenost:**		
Druh financování	**Odpověď**	**Popis zajištění, získání financování**
Financování pomocí ESIF[1]	Ne	
Financování z vlastních zdrojů	**Ano**	
Financování pomocí jiných externích zdrojů	Ne	

3.1.3. Metodická připravenost projektu

Tabulka 57: **Metodické připravenost:**		
Metodické zajištění	**Odpověď**	**Popis**
Řízení pomocí metodiky (uveďte název)	Ano	
Podpora od projektové kanceláře úřadu/resortu	Ano	
Podpora od architektonické kanceláře úřadu/resortu	Ano	

[1] Evropské strukturální a investiční fondy

3.2. Ekonomické parametry projektu

3.2.1. Hodnota výdajů a ekonomická náročnost projektu

Hrubý odhad hodnoty záměru nákupu služeb či investic (externích výdajů)**, souvisejících s informačními a komunikačními technologiemi** (projektu).

Plán předpokládané ekonomické náročnosti projektu založené na metodologii 5 letých celkových nákladů vlastnictví (tzv. Total Costs of Ownership) **- účelové členění nákladů projektu.**

Tabulka 58: **TCO:**

Souhrnná položka modelu TCO [Kč] bez DPH	**① Výdaje na realizaci (výstavbu) projektu**	**② Výdaje na provoz a rozvoj (do konce aktuální smlouvy)**	**③ TCO 5** = ① + (②, přepočtené **na 5 let)**	**Vysvětlení k položce**
Počet měsíců trvání fáze	X1	X2	X1 + (X2 přepočtené na 5 let)	
A. Předběžné analýzy (vč. rizik), tvorba zadání, výběr řešení, výběr dodavatele – náklady nákupního procesu				
B. Nákup SW a HW pro projekt (bez SaaS či PaaS)	27 725 000,-		27 725 000,-	<uveďte do tabulky 60 nebo samostatné přílohy rozpad výdajů, pokud výdaj přesahuje 10% celkové ceny projektu a současně přesahuje 1 mil. Kč>
C. Analýza, finální projekt, vývoj, implementace, školení uživatelů, zkušební provoz a testy, případně i migrace dat a akceptační audit	10 300 000,-		10 300 000,-	<při jakékoliv částce uveďte do tabulky 60 nebo samostatné přílohy seznam rolí s počtem člověkodnů a cenu za člověkoden>
D. Provoz a podpora řešení HW a SW (bez SaaS či PaaS)		11 000 000,-	11 000 000,-	<uveďte do tabulky 60 nebo samostatné přílohy rozpad výdajů, pokud roční provoz a podpora přesahuje 20% celkové ceny řešení>
E. Hardware/Software údržba a průběžné úpravy (bez SaaS či PaaS)		8 000 000,-	8 000 000,-	<uveďte do tabulky 60 nebo samostatné přílohy rozpad výdajů, pokud roční údržba a průběžné úpravy přesahuje 20% celkové ceny řešení>
F. Projekty postupné inovace a zlepšování (plánované)				
G. Projekty upgrade (pokud jsou plánovány)				
H. Zvýšené náklady užívání řešení vč. nákladů na přechod z předchozího řešení (pokud se vyskytnou)				

Tabulka 58: **TCO:**				
Souhrnná položka modelu TCO [Kč] bez DPH	**① Výdaje na realizaci (výstavbu) projektu**	**② Výdaje na provoz a rozvoj (do konce aktuální smlouvy)**	**③ TCO 5** = ① + (②, přepočtené **na 5 let)**	**Vysvětlení k položce**
I. Útlum, konzervace a ukončení řešení				<uveďte do tabulky 60 nebo samostatné přílohy rozpad výdajů, pokud útlum, konzervace a ukončení řešení přesahuje 10% celkové ceny řešení>
X. Licence, HW, provoz, podpora, údržba, průběžný rozvoj - vše v subskripci (pouze SaaS a PaaS)				<uveďte do tabulky 60 nebo samostatné přílohy rozpad výdajů, pokud výdaj na SaaS a PaaS přesahuje 1 mil. Kč>
Z. Ostatní nerozlišené režijní náklady				<uveďte do tabulky 60 nebo samostatné přílohy rozpad výdajů, pokud výdaj na nerozlišenou režii přesahuje 0,5 mil. Kč>
Celkem	38 025 000,-	19 000 000,-	**57 025 000,-**	

Tabulka 59: **Popis funkčního celku, který je projektem rozšiřován či upravován (pokud existuje):**
DA MO bude realizován s přímou logickou, koncepční a technologickou návazností na projekt Elektronický správní archiv MO (ESA MO), jako jeho rozšíření. Pro **HW část** stávajícího řešení ESA MO jsou využity: • servery Proliant výrobce HPE, • aktivní síťové prvky (switche) výrobce HPE, • disková pole s vysoce dostupnou architekturou IBM StoreWise V5010. **Jako serverový OS** je převážně použit Red Hat Enterprise Linux 6.9, v omezené míře též CentOS Linux a Microsoft Windows Server. **Pro vlastní SW část** jsou primárně využity tyto komponenty: FileNet P8 - ECM (Enterprise Content Management), kromě funkcionalit pro archiv dokumentů poskytuje i nástroje pro tvorbu a správu workflow databáze DB2 - zajišťuje uložení metadat dokumentů, IBM GPFS (General Parallel File System) Spectrum Scale - zajišťuje funkci řízeného zpřístupnění datových prostor pro ukládání archiválií a vazby na replikační procesy pro ukládání dat v sekundární lokalitě, aplikační server WAS, LDAP server TDS, databáze MySQL. **Testování příchozích dokumentů** a požadovanou detekci na přítomnost malware na základě behaviorální analýzy (Karanténa) je zajištěna produktem FireEye. **Bezpečnost dat a monitoring** je zajištěn technologiemi Qradar a Guardium **Archiv zajišťuje služby pro správu dokumentů** prostřednictvím logické vrstvy s níž je možná integrace pomocí standardního rozhraní CMIS, WS-SOAP, WS-REST, Java a .NET API. Fyzická vrstva Archivu je tvořena fyzickým HW úložištěm poskytujícím souborový systém NFS a CIFS s možností přístupu k uloženým datům pomocí NFS, CIFS, HTTPS a WEBDAV. **Brána zajišťuje komunikaci mezi části Archiv a okolními systémy** včetně části Badatelna. Integrační služby poskytují webové služby REST (Representational State Transfer) a SOAP (Simple Object Access Protocol), pro příjem vstupních dokumentů ze zdrojových systémů a také sdílenou složku, která je pravidelně kontrolována skenerem souborového systému. **Badatelna** je vytvořena jako autonomní uživatelská aplikace s administrační a prezentační částí, přičemž komunikace s Bránou je realizována pomocí služby webové REST. **Komunikace** mezi jednotlivými částmi stávajícího řešení (Archiv, Brána, Badatelna) je realizována pomocí standardních komunikačních rozhraní WS-SOAP, REST, EJB, LDAP a CMIS. Při komunikaci s vnějšími systémy

Tabulka 59: **Popis funkčního celku, který je projektem rozšiřován či upravován (pokud existuje):**	
jsou využity rozhraní LDAP, TSP, OCSP, SOAP a REST a je též využita sdílená složka pravidelně kontrolována skenerem souborového systému.	
Plánované 5leté externí výdaje celého funkčního celku (mimo tento projekt) [tis. Kč]**:**	12 788

Tabulka 60: **Vysvětlení a komentář k souhrnu výdajů a ekonomické náročnosti projektu:**
Ekonomická náročnost projektu byla určena na základě vypracované Studie proveditelnosti pro systém "Digitální archiv MO", konkrétně v dokumentu „Analýza nákladů na pořízení DA MO - legislativně technický upgrade na období 5 let od uvedení do provozu a na jeho provozování po celou dobu životního cyklu". Analýza nákladů vychází zejména z marketingového průzkumu, který byl také součástí Studie proveditelnosti.

3.2.2. Personální náročnost projektu

Tabulka 61: **Odhady kapacitní náročnosti realizace projektu (korespondující s TCO):**

Interní / Externí zdroje	**Počet zúčast. osob**	**Počet přepočtených úvazků** (FTE)	**Vysvětlení rolí v projektu**
Interní zaměstnanci organizace	15	5	PM celého projektu pro lokalitu Praha a Bystrovany. Zastoupení v obchodní rovině Praha a Bystrovany. Zastoupení v technické rovině Praha a Bystrovany. ŘV (Bezpečnostní manažer – Praha a Bystrovany). PT (Koordinátor, zástupce PM – Praha). PT (Technická podpora IT – Praha). PT (Zabezpečení vjezdu a vstupu – Praha). PT (Řízení školení – Praha). PT (Logistické zabezpečení evidence – Praha). 2x Zastoupení v technické rovině – Bystrovany. 2x PT (Technická podpora IT – Bystrovany). PT (Zabezpečení vjezdu a vstupu – Bystrovany). PT (Řízení školení – Bystrovany).
Ostatní zaměstnanci VS			**Zatím se neuvažují, uveďte, je-li pro projekt významné**
Externí dodavatelé	5	0,1	Projekt předpokládá roční podporu dodavatele v rozsahu 25 člověkodní ročně.

Tabulka 62: **Odhady dopadů do změn počtu systemizovaných míst spojených s projektem:**

Kategorie systemizovaného místa	**Uvnitř úřadu**	**Jinde ve VS**	**Vysvětlení změny a umístění systemizovaných míst**
Pro realizaci projektu	3		Ve struktuře VÚA (v rámci Vojenského historického archivu) bylo zřízeno pracoviště Digitální archiv MO ve složení vedoucí, projektant, archivář.
Pro vlastní výkon podpořené externí veřejné služby	5		V současnosti probíhá digitalizace archiválií na VHA víceméně nárazově a v závislosti na aktuální dostupnosti finančních prostředků a je zabezpečena zejména externími pracovníky na dohodu o provedení práce. Z dlouhodobého a

Tabulka 62: **Odhady dopadů do změn počtu systemizovaných míst spojených s projektem:**			
Kategorie systemizovaného místa	**Uvnitř úřadu**	**Jinde ve VS**	**Vysvětlení změny a umístění systemizovaných míst**
			koncepčního pohledu by operátoři digitalizačního pracoviště měli být vlastními zaměstnanci zejména s ohledem na znalost obsluhy, plynulé vytížení a co nejvyšší využití digitalizační linky. Další oblastí práce prováděné pracovníky DA MO je vlastní archivní činnost, která zahrnuje vyhledávání archiválií, úpravy a doplňování již pořízených digitálních archiválií, úpravy a doplňování metadat, příprava pro zpřístupnění digitálních archiválií na Badatelském portálu, práce s elektronickými badatelskými listy, vyhodnocování, sestavy a statistiky.
Pro IT podporu provozu	3		Pracoviště DA MO bude po realizaci projektu sloužit jako IT podpora provozu.

Tabulka 63: **Vysvětlení a komentář k personální náročnosti projektu:**
Implementací DA MO vznikne pro Vojenský historický archiv nová povinnost zpracovávat kromě fyzických archiválií také elektronickou podobu archiválií. Zvýšené požadavky na personální kapacity se následně promítají do role operátorů digitalizační linky, do role archivářů při zpracovávání archiválií uložených v DA i do role archivářů zodpovědných za proces publikace archiválií. Zatížení archivářů se bude postupně zvyšovat analogicky k počtu uložených archiválií v DA MO a počtu žádostí o poskytnutí digitálních archiválií v původním rozlišení nebo jako důkazního materiálu. S ohledem na zajištění potřeb provozování DA MO je žádoucí rozšíření existující základny lidských zdrojů VHA zabezpečením nových pozic pro tvorbu dat, správu dat z pohledu archivní práce, správu dat z pohledu systémového IT, úpravu dat k jejich prezentaci na Badatelském portálu.

3.3. Analýza rizik projektu

Tabulka 64: **Přehled klíčových identifikovaných rizik neúspěchu projektu:**		
Označení rizika	**Popis rizika**	**Opatření pro snížení rizika**
a) rizika během projektové přípravy:		
Řízení projektu Zadavatele	Nedostatečná podpora vedení	Přesvědčit vrcholné vedení a zajistit jeho podporu pro projekt. Zapojit člena vrcholného vedení jako Sponzora projektu. Prosadit a stanovit projektu maximální prioritu.
	Změna rozsahu projektu	Důsledná aplikace změnového řízení s možným dopadem do základních projektových charakteristik. Podpora vrcholového vedení. Důsledná příprava zadání předmětu plnění včetně jednoznačného popisu.
	Nesprávné nebo nedostatečně vyjednané smluvní podmínky.	Podpora vrcholového vedení. Důsledná příprava zadání předmětu plnění včetně jednoznačného popisu. Důsledná příprava návrhu smlouvy ze strany Zadavatele se zapracováním předmětu plnění a vyjednávání s vybraným dodavatelem a jeho protinávrzích s cílem vyvážit smlouvu Win –Win. Důsledná aplikace dohodnuté metodiky řízení projektu.

Tabulka 64: **Přehled klíčových identifikovaných rizik neúspěchu projektu:**		
Označení rizika	**Popis rizika**	**Opatření pro snížení rizika**
	Nevyhovující řízení projektu plnění veřejné zakázky.	Postup důsledně dle Plánu projektu a Plánu kvality a Plánu řízení rizik, včetně jejich revizí a případných aktualizací. Důsledné poskytování součinností z obou stran zadavatelem i dodavatelem. Podpora vrcholového vedení.
	Nedodržení projektových milníků.	Důsledná aplikace metodiky řízení projektu a metodiky řízení kvality. Postup důsledně dle Plánu projektu a Plánu kvality a Plánu řízení rizik, včetně jejich revizí a případných aktualizací. Důsledné poskytování součinností z obou stran zadavatelem i dodavatelem. Případná aplikace změnového řízení.
	Nevyhovující řízení kvality plnění veřejné zakázky	Důsledná aplikace metodiky řízení kvality zadavatele. Postup důsledně dle Plánu kvality, včetně jeho revizí a případných aktualizací. Podpora vrcholového vedení.
	Nevyhovující řízení rizik plnění veřejné zakázky.	Důsledná aplikace metodiky řízení projektu zadavatele. Postup důsledně dle Plánu projektu a Plánu řízení rizik, včetně jejich revizí a případných aktualizací. Podpora vrcholového vedení. Podpora vrcholového vedení zadavatele.
	Nesoučinnost třetích stran	Změnové řízení s možným dopadem do harmonogramu plnění veřejné zakázky.
	Nesoučinnost vlastní – Nedostatečné znalosti uživatelů problematiky na straně zadavatele, např. v důsledku fluktuace pracovníků.	Podpora zadavatele po celou dobu realizace předmětu plnění poskytovaná dodavatelem, případné řešení změnovým řízením. Odpovídající personální politika zadavatele. Podpora vrcholového vedení.
	Nesoučinnost vlastní – Nedostatečná informovanost v rámci projektu (případně nízká kvalita předávaných informací).	Důsledná aplikace metodiky řízení projektu a postup dle Plánu projektu. Podpora vrcholového vedení.
	Nesoučinnost vlastní – Nedostatečná koordinace s ostatními projekty	Dodržování stanovené metodiky projektu a metodiky řízení kvality dodavatele. Postup důsledně dle Plánu projektu, případně jeho revize a aktualizace. Metodické řízení programu, či portfolia projektu zadavatele.
b) rizika v průběhu realizace:		
Řízení projektu Dodavatele	Nedostatečná podpora vedení	Přesvědčit vrcholné vedení a zajistit jeho podporu pro projekt. Zapojit člena vrcholného vedení jako Sponzora projektu.

Tabulka 64: **Přehled klíčových identifikovaných rizik neúspěchu projektu:**		
Označení rizika	**Popis rizika**	**Opatření pro snížení rizika**
		Prosadit a stanovit projektu maximální prioritu.
	Nesprávné nebo nedostatečně vyjednané smluvní podmínky.	Podpora vrcholového vedení. Důsledná spolupráce se strany zadavatele na jeho návrhu smlouvy, vytvoření návrhu úprav smlouvy a vyjednávání se zadavatelem o protinávrzích s cílem vyvážit smlouvu Win – Win.
	Nevyhovující řízení projektu plnění veřejné zakázky.	Důsledná aplikace dohodnuté metodiky řízení projektu. Postup důsledně dle Plánu projektu, včetně jeho revizí a případných aktualizací.
	Nedodržení projektových milníků.	Podpora vrcholového vedení. Důsledná aplikace metodiky řízení projektu a metodiky řízení kvality. Postup důsledně dle Plánu projektu a Plánu kvality a Plánu řízení rizik, včetně jejich revizí a případných aktualizací. Důsledné poskytování součinností z obou stran zadavatelem i dodavatelem. Případná aplikace změnového řízení.
	Nevyhovující řízení kvality plnění veřejné zakázky.	Důsledná aplikace metodiky řízení kvality dodavatele. Postup důsledně dle Plánu kvality, včetně jeho revizí a případných aktualizací.
	Nevyhovující řízení rizik plnění veřejné zakázky.	Podpora vrcholového vedení. Důsledná aplikace metodiky řízení projektu. Postup důsledně dle Plánu projektu a Plánu řízení rizik, včetně jejich revizí a případných aktualizací.
	Nesoučinnost třetích stran.	Podpora vrcholového vedení. Podpora vrcholového vedení dodavatele. Důsledná příprava projektu dodavatelem včetně všech jeho subdodavatelů a projednáním.
	Nesoučinnost vlastní – Nedostatečné znalosti problematiky pracovníků na straně dodavatele, např. v důsledku fluktuace pracovníků.	Podpora dodavatele po celou dobu realizace předmětu plnění, případně řešení změnovým řízením. Důsledné řízení projektu zabraňující změnám v pozicích klíčových pracovníků. Odpovídající personální politika dodavatele zabraňující fluktuaci pracovníků. Podpora vrcholového vedení.
	Nesoučinnost vlastní – Nedostatečná informovanost v rámci projektu (případně nízká kvalita předávaných informací).	Důsledná aplikace metodiky řízení projektu, případně jeho revize a aktualizace Metodické řízení programu, či portfolia projektu dodavatele.

3.4. Plán zavedení, údržby, dlouhodobá udržitelnost výstupů projektu

Tabulka 65: **Plánovaný ověřovací provoz (před akceptací) jednotlivých výstupů projektu:**	
Označení výstupu projektu	**Plánovaná doba ověřovacího provozu výstupu [týden]**

Tabulka 66: **Plánovaná životnost jednotlivých výstupů projektu:**		
Označení výstupu projektu	**Plánovaná životnost výstupu [rok]**	**Popište plánované změny**
Funkčnost a stabilita projektu	Neomezená - dlouhodobé využití projektu	

Tabulka 67: **Legislativní update:**	
Bude podpora zahrnovat rovněž udržování řešení v souladu s novými právními předpisy (tzv. legislativní update)**?** **Vysvětlete v jakém rozsahu:**	**Jakým způsobem bude legislativní update hrazen?**
V rámci služby (záručního servisu) na 5 let bude zabezpečen i legislativně – právní upgrade řešení.	Součást smlouvy o provozu a podpoře

Tabulka 68: **Jak je zajištěn další budoucí rozvoj předmětné oblasti a její ICT podpory:**
Rozvoj by měl být součástí 5 let trvání projektu formou opce. Pokračování projektu po 5 letech bude formou nového zadávacího řázení. Součástí projektu by měl být tzv, exit plán, který ale není součástí aktuálně plánovaného rozsahu projektu a jeho pracnosti i nákladů/ceny.

Tabulka 69: **Jak je zajištěno řízené ukončení životnosti jednotlivých výstupů projektu a případný přechod na další řešení, či případná výměna dodavatele nad stejným řešením** (tzv. Exit strategie)?
Do smlouvy bude zahrnuto: 1.1.8. Podle potřeb Objednatele poskytnutí služeb exitu, které jsou spojené se závěrečným ukončením poskytování služeb a dodávku DA MO podle této Smlouvy a spočívající v přípravě a předání díla a souvisejících služeb DA MO novému poskytovateli na konci smluvního vztahu podle pokynů Objednatele. V případě zájmu o poskytnutí Služeb exitu dle odst. X.X.X této Smlouvy zašle Objednatel podle odst. X.X.X této Smlouvy Poskytovateli písemnou objednávku obsahující detailní specifikaci zamýšleného obsahu a rozsahu prací. Specifikace bude obsahovat popis zadání, očekávanou pracnost v ČD (1 ČD = 8 pracovních hodin), termín dodání a fakturační milník. Objednávka musí být před započetím předmětných prací odsouhlasena Poskytovatelem. Veškeré písemné výstupy ze své činnosti bude Poskytovatel předávat v sídle Objednatele, nebude-li v konkrétním případě Smluvními stranami sjednáno jinak. Místem plnění je lokalita VÚA Zadavatele. Služby exitu můžou zahrnovat i činnosti provádění v sídle Objednatele a dále jakékoliv místo v České republice, k němuž se vztahuje či by se mohlo vztahovat poskytování Předmětu plnění dle této Smlouvy. Způsob poskytování služeb exitu Poskytovatel se zavazuje dle pokynů Objednatele poskytnout veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených <NAZEV SMLOUVY> s dodávkou DA MO na Objednatele a/nebo nového poskytovatele, ke kterému dojde po skončení účinnosti této Smlouvy, tedy poskytnout Služby exitu dle odst.1.1.8 této Smlouvy, které zahrnují:

Tabulka 69: **Jak je zajištěno řízené ukončení životnosti jednotlivých výstupů projektu a případný přechod na další řešení, či případná výměna dodavatele nad stejným řešením** (tzv. Exit strategie)?
2.1.1 vypracování plánu exitu a poskytnutí nezbytné součinnosti k jeho realizaci, 2.1.2 poskytnutí potřebné součinnosti podle pokynů Objednatele novému poskytovateli, 2.1.3 předání veškeré dokumentace a potřebných informací v aktualizované podobě, dle aktuálního stavu díla, 2.1.4 předání všech uložených dat, 2.2 Za tímto účelem se Poskytovatel zavazuje ve lhůtách dle odst. 7.3 této Smlouvy vypracovat na základě pokynu Objednatele dokumentaci vymezující postup provedení Služeb exitu (dále jen „Exitový plán“), a poskytnout plnění

4. VYJÁDŘENÍ K BEZPEČNOSTNÍM ASPEKTŮM

Tabulka 70: **Předkladatel prohlašuje, že předkládaný projekt bude realizován plně v souladu s níže uvedeným prohlášením:**
Text vyplňujte až na případnou výzvu OHA.

5. UPOZORNĚNÍ A DOPORUČENÍ

Tabulka 71:**Upozornění a doporučení:**

6. PŘÍLOHY

Tabulka 72: **Přílohy:**		
Typ	**Číslo a název přílohy**	**Upřesnění žádostí o výjimky/přílohy**
Zvolte položku.	Exit strategie	viz. Tab. 69
Zvolte položku.	Architektonický model	
Zvolte položku.	Rozpočet projektu	viz. Tab. 58
Zvolte položku.		
Celkový počet příloh:		