SMLOUVA NA VYTVOŘENÍ SYSTÉMU „DIGITÁLNÍ ARCHIV MO“ č. 195310197

Smluvní strany

Česká republika – Ministerstvo obrany

se sídlem: Tychonova 1, 160 01 Praha 6
jejímž jménem jedná: Ing. Petr ZÁBOREC, ředitel odboru vyzbrojování pozemních sil a KIS Sekce vyzbrojování a akvizic MO
se sídlem kanceláře: nám. Svobody 471/4, 160 01 Praha 6
IČO: 60162694
DIČ: CZ60162694
bankovní spojení: Česká národní banka, pobočka 701, Na Příkopě 864/28, 115 03 Praha 1
číslo účtu: 404881/0710
Informační systém datových schránek (dále jen „ISDS“):
Identifikátor datové schránky: **hjyaavk**
kontaktní osoby: [redacted]
Ing. Miroslav VRBENÍK, [redacted]
adresa pro doručování korespondence:
Sekce vyzbrojování a akvizic MO
odbor vyzbrojování pozemních sil a KIS
nám. Svobody 471/4
160 01 Praha 6

(dále jen **„nabyvatel“**)

a

IBM Česká republika, spol. s r.o.

zapsána v obchodním rejstříku u Městského soudu v Praze, oddíl C, vložka 692
se sídlem: V parku 2294/4, Chodov, 148 00 Praha 4
jejímž jménem jedná: Ing. Petr HAVLÍK, jednatel
IČO: 14890992
DIČ: CZ14890992
bankovní spojení: Raiffeisenbank a.s., Hvězdova 1716/2b, 140 78 Praha 4
číslo účtu: 1001042725/5500
oprávněn ve věcech smluvních a ekonomických:
Karim IFRAH, tel. [redacted]
e-mail: [redacted]
oprávněn ve věcech technických:
[redacted]
nebo jím písemně pověřená osoba
adresa pro doručování korespondence:
IBM Česká republika, spol. s r.o.
V parku 2294/4,
148 00 Praha 4 Chodov

(dále jen **„poskytovatel“**)

uzavírají v souladu s ustanovením § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“) a příslušných ustanovení zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „AZ“), tuto smlouvu na vytvoření systému „Digitální archiv MO“ (dále jen „smlouva“):

Článek 1
ÚČEL SMLOUVY

Účelem této smlouvy je 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.

Článek 2
PŘEDMĚT SMLOUVY

Předmětem smlouvy je:

1. závazek poskytovatele zpracovat před-implementační analýzu prostředí nabyvatele a na jejím základě vypracovat detailní návrh řešení včetně požadavků na poskytnutí součinnosti nabyvatele. Výstupem bude akceptovaný a oboustranně schválený závazný detailní návrh řešení, postup, způsob a harmonogram implementace navrženého řešení, seznam požadavků poskytovatele na součinnost nabyvatele, a vlastní technický popis řešení systému „Digitální archiv MO“ (dále jen „DA MO“),
2. závazek poskytovatele v souladu s požadavky specifikovanými podrobně ve Specifikaci předmětu plnění uvedené v Příloze 1, Příloze 2 a v Příloze 3 této smlouvy vytvořit, dodat, instalovat, předat, provést zaškolení a proškolování obsluhy a zabezpečit servis a legislativní upgrade systému DA MO, který se skládá z následujících částí:

   - **Softwarové licence:**
     - poskytnutí SW licencí a práv užití potřebných pro zhotovení a provoz DA MO
   - **Hardwarové komponenty:**
     - hardware potřebný pro dlouhodobé garantované uložení archiválií a provoz řešení DA MO,
     - PC digitalizačního pracoviště a místnosti „Badatelna“.
   - **Dokumentace DA MO**
   - **Služby:**
     - před-implementační analýza a detailní návrh řešení,
     - implementace DA MO,
     - akceptační testy
     - zaškolení obsluh
     - migrace obsahu ze stávajícího DMS systému Documentum.
   - **Záruční servis a technická podpora:**
     - záruční servis po dobu 60 měsíců od podpisu akceptačního protokolu smluvními stranami,
     - technická podpora hardwarových a softwarových komponent po dobu 60 měsíců od podpisu akceptačního protokolu smluvními stranami,
     - legislativní upgrade po dobu 60 měsíců od podpisu akceptačního protokolu smluvními stranami,
     - proškolování obsluh.

3. závazek poskytovatele zhotovit, dodat, instalovat, předat, provést zaškolení a proškolování obsluhy a zabezpečit servis a legislativní upgrade systému DA MO v souladu akceptovaným a oboustranně schváleným detailním návrhem řešení a dalšími akceptovanými dokumenty, které budou jeho součástí,
4. závazek poskytovatele provést systém DA MO v souladu s požadavky a postupy uvedenými v Příloze 1, Příloze 2 a v Příloze 3 této smlouvy (Specifikace předmětu plnění), ledaže není daný požadavek nebo postup kompatibilní s akceptovaným a oboustranně schváleným detailním návrhem řešení, jehož zpracování je stanoveno dle článku 2 odst. 1 této smlouvy,
5. závazek nabyvatele řádně poskytnuté plnění dle odst. 1 - 4 tohoto čl. smlouvy převzít a zaplatit dohodnutou cenu dle čl. 3 této smlouvy.

Článek 3
CENA

1. Nabyvatel se zavazuje zaplatit za řádné splnění závazků dle čl. 2 odst. 1 - 4 této smlouvy cenu, která je sjednána dohodou smluvních stran dle § 2 zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů.
2. Cenový rozklad po jednotlivých samostatných funkčních celcích ve struktuře: komodita, jednotková cena v Kč bez DPH a s DPH, počet měrných jednotek, celková cena za komoditu v Kč bez DPH a s DPH je uveden v Příloze 4 této smlouvy.
3. **a) Celková cena za plnění bez DPH** činí **33.300.000,00 Kč**
   (slovy: třicet tři milionů tři sta tisíc korun českých),

   b) DPH ve výši 21 % činí **6.993.000,00 Kč**
   (slovy: šest milionů devět set devadesát tři tisíc korun českých),

   c) Celková cena včetně DPH (dále jen „celková cena“), **činí 40.293.000,00 Kč**
   (slovy: čtyřicet milionů dvě stě devadesát tři tisíc korun českých).
4. Celková cena zahrnuje veškeré náklady poskytovatele spojené s plněním jeho závazků dle čl. 2 odst. 1 - 4 této smlouvy.
5. Celková cena bez DPH zahrnuje odměnu za poskytnutí licence i případnou přiměřenou dodatečnou odměnu autorovi dle § 2374 odst. 1 OZ.
6. Cena bez DPH je cenou nejvýše přípustnou a není možno ji překročit.
7. K celkové ceně bez DPH bude připočtena DPH dle aktuálně účinných právních předpisů.

Článek 4
DOBA A MÍSTO PLNĚNÍ

1. Poskytovatele je povinen zpracovat před-implementační analýzu prostředí nabyvatele a na jejím základě vypracovat detailní návrh řešení, včetně požadavků na poskytnutí součinnosti nabyvatele, a to nejpozději **do 60 dní** od nabytí účinnosti smlouvy. Pokud zástupce nabyvatele neposkytne součinnost poskytovateli, doba se prodlužuje o dobu neposkytnutí součinnosti zástupce nabyvatele.
2. Poskytovatel je povinen vytvořit, dodat, instalovat a předat systém DA MO včetně zaškolení nejpozději do **30. září 2021** a následně ode dne předání a převzetí systému DA MO poskytnout technickou podporu včetně proškolování obsluhy po dobu 60 měsíců od podpisu akceptačního protokolu smluvními stranami, a legislativní upgrade po dobu 60 měsíců od podpisu akceptačního protokolu smluvními stranami.

3. Místem dodání systému DA MO s primárním digitálním úložištěm je VZ 2111 Praha, Pilotů 217/12, 161 00 Praha 6 – Ruzyně, osoba odpovědná převzetím plnění je ředitel VZ 2111 Praha, [redacted], nebo jím písemně pověřená osoba, kterou je pro převzetí prvotní instalace, provedení funkčních testů a zaškolení obsluhy [redacted] (dále jen „pověřená osoba“). Místem dodání záložního digitálního úložiště systému DA MO je VZ 2111 Olomouc, Kasárna Bystrovany, ulice Libušina 646/78, 779 00 Olomouc, osoba odpovědná převzetím plnění je ředitel VZ 2111 Praha, [redacted], nebo jím písemně pověřená osoba, kterou je pro prvotní akceptaci dodávky [redacted], nebo jím písemně pověřená osoba. Pro konečnou akceptaci je to pověřená osoba.

Článek 5
PŘEVZETÍ PLNĚNÍ

1. Poskytovatel se zavazuje předat závazný detailní návrh řešení včetně postupu, způsobu a harmonogramu implementace navrženého řešení, seznamu požadavků poskytovatele na součinnost nabyvatele a vlastního technického popisu řešení systému DA MO podle článku 2 odst. 1 této smlouvy. Z detailního návrhu řešení musí být nabyvatel schopen ověřit, že jím stanovené požadavky budou splněny a systém DA MO bude vyhovovat potřebám nabyvatele a provozním zvyklostem, že systém DA MO bude implementován v dohodnutých lhůtách uvedených v detailním návrhu řešení a zda a jaké funkcionality je případně třeba realizovat dodatečně nebo odlišně od Přílohy 1, Přílohy 2 a Přílohy 3 této smlouvy (Specifikace předmětu plnění). Po akceptaci detailního návrhu řešení se tento dokument stává závazným pro smluvní strany při další realizaci systému DA MO dle této smlouvy.
2. Poskytovatel instaluje, nakonfiguruje a předá k užití systém DA MO v souladu s požadavky uvedenými v Příloze 1, v Příloze 2 a v Příloze 3 této smlouvy v místě plnění dle čl. 4 odst. 3 této smlouvy. Poskytovatel je povinen písemně uvědomit nabyvatele nejméně 10 pracovních dnů předem o připravenosti předat plnění.
3. Poskytovatel je povinen předat plnění pověřené osobě, a to v době a místě plnění v této smlouvě uvedené.
4. O předání a převzetí plnění je poskytovatel povinen vyhotovit 2 dodací listy ve třech výtiscích, podepsané poskytovatelem. Dodací list dodání v lokalitě Olomouc podepíše pověřená osoba nabyvatele v Olomouci, která současně na něj doplní číslo IDED. Dodací list dodání v lokalitě Praha podepíše pověřená osoba nabyvatele v Praze, která současně na něj doplní číslo IDED. Oba dodací listy budou přiloženy k Akceptačnímu protokolu, který zpracuje poskytovatel po splnění úplné dodávky systému DA MO (kromě záručního servisu, proškolování obsluh, technické podpory a legislativního upgrade). Poskytovatel na Akceptačním protokolu uvede čísla dodacích listů, IDED a den dodávky do Olomouce a do Prahy, termíny provedení zaškolení, instalace, migrace dat, implementace a uvedení do provozu. Poskytovatel je povinen jej označit číslem této smlouvy uvedeným v jejím záhlaví. Jeden výtisk Akceptačního protokolu včetně dodacích listů obdrží pověřená osoba nabyvatele a dva výtisky obdrží poskytovatel s tím, že jeden výtisk je poskytovatel povinen přiložit k faktuře – daňovému dokladu (dále jen „faktura“).
5. Vystavení dodacích listů je podmíněno provedením prvotní instalace systému DA MO a úspěšným provedením funkčních testů v souladu s požadavky uvedenými v Příloze 1, v Příloze 2 a v Příloze 3 této smlouvy. Akceptační protokol podepisuje zástupce poskytovatele a pověřená osoba nabyvatele nebo jím písemně pověřená osoba ve třech výtiscích. V případě nefunkčnosti zařízení či jiné zjevné vady pověřená osoba vyznačí na akceptačním protokolu tento důvod odmítnutí převzetí a zástupce poskytovatele a pověřená osoba do akceptačního protokolu uvedou vzájemně dohodnutý nový termín převzetí plnění po odstranění vad.

6. Pověřená osoba nepřevezme vadné plnění. Převzetí odmítne písemně spolu s uvedením důvodů.
7. Poskytovatel je povinen písemně dohodnout s pověřenou osobou nabyvatele termín zaškolení obsluh minimálně 20 pracovních dnů před jeho konáním. O provedení zaškolení podepíší zástupci obou smluvních stran protokol ve třech výtiscích s tím, že jeden výtisk je poskytovatel povinen přiložit k faktuře. Za nabyvatele podepíše protokol [redacted] nebo jím písemně pověřená osoba.

Článek 6
POVINNOSTI SMLUVNÍCH STRAN

1. Poskytovatel je povinen:
   a) pro DA MO použít HW zařízení pouze nová (vyrobená ne dříve než 1 rok před dobou dodání), nerepasovaná, nepoškozená, nepoužívaná, odpovídající v této smlouvě neuvedeným obecně platným technickým normám, právním předpisům a předpisům výrobce, v množství, termínu, požadovaném provedení, jakosti a balení v souladu s touto smlouvou,
   b) zabezpečit po celou dobu plnění předmětu smlouvy komunikaci s nabyvatelem výhradně v českém jazyce,
   c) umožnit nabyvateli kdykoli kontrolovat plnění smlouvy poskytovatelem - za nabyvatele toto právo má [redacted] ředitel VÚA Praha, VZ 2111 Praha, [redacted] e-mail: [redacted] nebo jím písemně pověřená osoba.
2. Nabyvatel je povinen:
   a) zabezpečit převzetí DA MO pověřenou osobou,
   b) ve sjednané lhůtě splatnosti uhradit poskytovateli celkovou cenu dle čl. 3 odst. 3 písm. c) této smlouvy.

Článek 7
PLATEBNÍ A FAKTURAČNÍ PODMÍNKY

1. Poskytovatel je oprávněn vystavit fakturu po řádném splnění dodávky systému DA MO. Poskytovatel je povinen vyhotovit fakturu – daňový doklad (dále jen „faktura“) ve 3 výtiscích (originál a 2 kopie).
2. Nabyvatel neposkytuje zálohové platby.
3. Na faktuře bude uvedena tato adresa nabyvatele:
   Česká republika – Ministerstvo obrany
   Tychonova 1
   160 00 Praha 6
   IČ: 60162694, DIČ: CZ60162694
   V zastoupení
   Sekce vyzbrojování a akvizic MO,
   odbor vyzbrojování pozemních sil a KIS,
   nám. Svobody 471/4
   160 01 Praha 6.
4. Faktura musí obsahovat všechny náležitosti řádného daňového dokladu podle platné právní úpravy, zejména podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a podle § 435 OZ. Kromě toho musí obsahovat tyto údaje a náležitosti:

- označení dokladu jako faktura,
- číslo smlouvy uvedené nabyvatelem v záhlaví smlouvy,
- počet příloh a razítko poskytovatele s podpisem poskytovatele,
- číslo bankovního účtu poskytovatele,
- v příloze faktury poskytovatel přiloží **originál podepsaného akceptačního protokolu, protokolu o zaškolení, stanoviska Úř OSK SOJ dle čl. 12 této smlouvy a dodacích listů.**

5. Splatnost faktury je 30 dnů ode dne jejího doručení nabyvateli. Bude-li faktura doručena nabyvateli z důvodu skluzu doby plnění z viny poskytovatele v období od 15. prosince do 15. ledna následujícího roku, poskytovatel souhlasí s prodlužením splatnosti takové faktury o 30 dnů z důvodu procesů na straně nabyvatele v období přechodu na nový rozpočtový rok, které brání nabyvateli, aby dodržel splatnost faktury 30 dnů. Faktura je považována za uhrazenou dnem odepsání příslušné fakturované částky z účtu nabyvatele se směrováním na účet určený poskytovatelem na faktuře.
6. Případný opravný daňový doklad je poskytovatel povinen vystavit a doručit nabyvateli do 14 dnů od vyžádání nabyvatelem. Doba splatnosti opravného daňového dokladu, tj. den připsání příslušné částky na účet nabyvatele, je 30 dnů ode dne jeho doručení.
7. Nabyvatel je oprávněn vrátit fakturu před uplynutím lhůty její splatnosti, neobsahuje-li některý výše uvedený údaj nebo má jiné závady v obsahu nebo není doručena v požadovaném množství výtisků. Ve vrácené faktuře nabyvatel musí vyznačit důvod jejího vrácení. V případě oprávněného vrácení poskytovatel vystaví novou fakturu. Vrácením faktury přestává běžet původní lhůta splatnosti a běží znovu ode dne doručení nové faktury nabyvateli. Poskytovatel je povinen novou fakturu doručit nabyvateli na adresu pro doručování korespondence uvedenou v záhlaví této smlouvy, a to do 5 pracovních dnů ode dne doručení oprávněně vrácené faktury poskytovateli. Vrácení faktury ve lhůtě její splatnosti je splněno, byla-li v uvedené lhůtě odeslána nabyvateli.
8. Všechny částky v Kč poukazované mezi poskytovatelem a nabyvatelem na základě této smlouvy musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů spojených s převodem na jejich účty.
9. Pokud budou u poskytovatele zdanitelného plnění shledány důvody k naplnění institutu ručení za daň podle § 109 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude nabyvatel při zasílání úplaty vždy postupovat zvláštním způsobem zajištění daně podle § 109a tohoto zákona. Smluvní strany berou na vědomí a souhlasí, že takovém případě bude platba poskytovateli za předmět smlouvy snížena o daň z přidané hodnoty, která bude odvedena nabyvatelem na účet správce daně místně příslušného poskytovateli. Poskytovatel obdrží úhradu za předmět smlouvy ve výši částky odpovídající základu daně a nebude nárokovat úhradu ve výši daně z přidané hodnoty odvedené na účet jemu místně příslušnému správci daně.

Článek 8
LICENČNÍ USTANOVENÍ

1. Bude-li součástí plnění této smlouvy nebo výsledkem činnosti poskytovatele prováděné dle této smlouvy předmět požívající ochrany autorského díla podle AZ (dále jen „**autorské dílo**“), nabývá nabyvatel dnem poskytnutí autorského díla nabyvateli k užívání, nejpozději však dnem podpisu akceptačního protokolu dle článku 5 odst. 4 této smlouvy, nevýhradní právo užít a po skončení poskytování služeb záruky a podpory dle této smlouvy dále modifikovat a upravovat takovéto autorské dílo všemi způsoby nezbytnými k naplnění účelu vyplývajícímu z této

smlouvy, a to po celou dobu trvání autorského práva k autorskému dílu, resp. po dobu autorskoprávní ochrany, bez omezení množstevního rozsahu, s územně neomezeným rozsahem (dále jen „**Licence**“), a to i prostřednictvím třetích osob odlišných od poskytovatele a nabyvatele. Licence se automaticky vztahuje i na všechny nové standardní verze, aktualizované verze, i na úpravy a překlady autorského díla, dodané poskytovatelem.

2. Není-li v této smlouvě stanoveno jinak je poskytovatel povinen předat nabyvateli nejpozději při předání plnění nebo její části veškerá technická řešení, koncepce, know-how, postupy či metody zpracování dat, analytické nástroje, pracovní dokumentaci, diagramy, schémata a koncepty, pokud jsou vyvinuty poskytovatelem výlučně pro plnění této smlouvy, které nemají charakter autorského díla.
3. Není-li v této smlouvě stanoveno jinak, zavazuje se poskytovatel ke každé uzavřené verzi počítačových programů v případě (na základě) požadavku nabyvatele bezplatně dodat zdrojové texty programů (v běžném textovém formátu) včetně komentářů a schéma datového modelu (tabulky, formáty dat, vazby) a to v elektronické a tištěné podobě.
4. Součástí Licence je rovněž neomezené právo nabyvatele Licenci převést nebo poskytnout podlicenci k užití autorského díla v rozsahu shodném s rozsahem Licence v souladu s účelem této smlouvy pro veškeré uživatele dle určení nabyvatele. Licence se automaticky vztahuje i na všechny nové verze, aktualizované verze, i na úpravy a překlady autorského díla, dodané poskytovatelem.
5. V případě, že z důvodu použití produktů třetích stran nebo standardních produktů poskytovatele není obvyklé a nelze po poskytovateli spravedlivě požadovat, aby poskytovatel poskytl k takovýmto autorským dílům Licenci a související oprávnění a další plnění dle článku 8 odstavce 1. až 4. výše, platí následující ustanovení:
   - jakýkoliv počítačový program, produkt, modul nebo jiné autorské dílo, ke kterému nelze poskytnout Licenci, musí být výslovně uveden v Příloze 2 a v Příloze 3 této smlouvy - Specifikaci předmětu plnění nebo v oboustranně schváleném detailním návrhu řešení;
   - k takovémuto autorskému dílu musí být poskytnuta alespoň nevýhradní uživatelská licence v rozsahu umožňujícím řádné užívání komponenty, která je součástí plnění této smlouvy, dalšími osobami oprávněnými na základě licence, včetně osob, kterým nabyvatel udělí podlicenci;
6. Smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle této smlouvy vznikne činností poskytovatele a nabyvatele dílo spoluautorů a nedohodnou-li se smluvní strany výslovně jinak, bude se mít za to, že je nabyvatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že poskytovatel udělil nabyvateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů.
7. Poskytovatel je povinen postupovat tak, aby udělení Licence k autorskému dílu dle této smlouvy včetně oprávnění udělit podlicenci zabezpečil, a to bez újmy na právech třetích osob.
8. Bude-li autorské dílo vytvořeno činností poskytovatele, smluvní strany činí nesporným, že jakékoliv takovéto autorské dílo vzniklo z podnětu a pod vedením nabyvatele.
9. Práva získaná v rámci plnění této smlouvy přechází i na případného právního nástupce nabyvatele. Případná změna v osobě poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této smlouvy poskytovatelem nabyvateli.
10. Odměna za poskytnutí, zprostředkování nebo postoupení Licence k autorskému dílu je plně zahrnuta v ceně za plnění ve smyslu článku 3 této smlouvy.
11. Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorským dílům a že má souhlas autorů k uzavření licenčních ujednání dle této smlouvy a že toto prohlášení zahrnuje i taková práva autorů, která by vytvořením autorského díla teprve vznikla.

Článek 9
ZÁRUČNÍ PODMÍNKY A NÁROKY Z VAD PLNĚNÍ

1. Poskytovatel poskytuje nabyvateli záruku za jakost systému DA MO dle ustanovení § 2113 a násl. OZ, tj. především za funkčnost a možnost jeho použití v délce 60 měsíců na HW a SW od doby převzetí systému DA MO pověřenou osobou. Záruční doba počíná běžet okamžikem řádného převzetí systému DA MO dle smlouvy a podpisu dodacího listu dle čl. 5 odst. 4 této smlouvy.
2. Pověřená osoba nabyvatele bude nároky z vad v záruce uplatňovat telefonicky, datovou zprávou nebo písemně, a to na tel. [redacted], do datové schránky **e69bcfy** nebo na adrese: **IBM Česká republika, spol. s r.o., V parku 2294/4, 148 00 Praha 4 Chodov**. V případě telefonického uplatnění zašle pověřená osoba nabyvatele poskytovateli do tří dnů písemné hlášení o tom, že byly uplatněny nároky z vad plnění. Nahlásit vady může jen určená osoba nabyvatele – pověřená osoba uvedená v čl. 4 odst. 3 této smlouvy.
3. Poskytovatel zajistí dostupnost celého systému pro dlouhodobé uchovávání neutajovaných elektronických dokumentů 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 je 10% během kalendářního roku. O závažnosti poruchy rozhoduje výhradně nabyvatel.
4. Poskytovatel bude trvale udržovat v pohotovosti pracovníky pro zásahy v rámci záručních oprav, jejichž seznam je povinen předat nabyvateli bezprostředně po nabytí účinnosti smlouvy (s osobními údaji nutnými k zabezpečení vstupu do objektu).
5. Servisní zásah v rámci záruky je ukončen znovuuvedením systému DA MO, do plného provozního stavu, který musí být akceptován pověřenou osobou.
6. Součástí záručního servisu je i zabezpečení telefonického a emailového Helpdesku pro pracovníky centrálního dohledu nabyvatele. Kontaktní údaje Helpdesku poskytovatele: [redacted]
7. Po dobu záruky je poskytovatel povinen poskytovat nabyvateli technickou a servisní podporu v délce 60 měsíců od podpisu akceptačního protokolu k systému DA MO dle čl. 5 této smlouvy 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).
8. Součástí technické a servisní podpory 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).
9. Vady plnění budou posuzovány v souladu s § 2099 a násl. OZ.

Článek 10
OCHRANA UTAJOVANÝCH INFORMACÍ

1. Poskytovatel je povinen zabezpečit ochranu utajovaných informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon 412/2005 Sb.“) a souvisejících prováděcích právních předpisů.
2. Poskytovatel je povinen do 5 pracovních dnů oznámit bezpečnostnímu řediteli MO (dále jen „BŘ MO“) všechny změny v zákonných podmínkách uvedených v § 17 zákona č. 412/2005 Sb., které by mohly vést k ohrožení jeho ekonomické stability.
3. Poskytovatel je povinen neprodleně písemně oznámit bezpečnostnímu řediteli nezpůsobilost ve vztahu k utajovaným informacím podle § 19 zákona č. 412/2005 Sb.
4. Poskytovatel je povinen současně se splněním příslušných zákonných povinností neprodleně písemně oznámit BŘ MO jakékoliv neoprávněné nakládání s utajovanými informacemi nebo ztrátu utajovaných informací rezortu Ministerstva obrany.
5. Poskytovatel je povinen umožnit odborným orgánům nabyvatele, resp. Odboru bezpečnosti MO, kontrolovat na základě písemného pověření BŘ MO nakládání s utajovanými informacemi resortu MO v rámci své osoby a svých subdodavatelů.
6. Poskytovatel má podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb. přístup k utajovaným informacím, přičemž tyto utajované informace jsou specifikovány v souladu se seznamem utajovaných informací stanoveným nařízením vlády č. 522/2005 Sb., ve znění nařízení vlády č. 240/2008 Sb. a tvoří Přílohu 5 této smlouvy.
7. Poskytovatel je povinen v rámci smluvních vztahů se svými subdodavateli, pro tyto stanovit zákaz poskytování utajovaných informací dalším subjektům.
8. Úkoly v oblasti ochrany utajovaných informací ve vztahu k podnikateli a to v souladu s článkem č. 34 RMO (Rozkaz ministra obrany) č. 14/2013 bude plnit [redacted] VZ 2111 Praha, [redacted] („bezpečnostní manažer“).

Článek 11
KATALOGIZAČNÍ DOLOŽKA

1. Poskytovatel souhlasí s tím, že na položku a její komponenty pod názvem „DIGITÁLNÍ ARCHIV MO“ bude uplatněna katalogizační doložka podle § 9 a následujících zákona č. 309/2000 Sb., o obranné standardizaci, katalogizaci a státním ověřování jakosti výrobků a služeb určených k zajištění obrany státu a o změně živnostenského zákona, ve znění pozdějších předpisů (dále jen „zákon č. 309/2000 Sb.“) a STANAG 4177. Poskytovatel se zavazuje, že dodá Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti (dále jen „Úř OSK SOJ“) údaje nezbytné pro katalogizaci, zpřístupní (zabezpečí zpřístupnění) dokumentaci k ověření a doplnění dodaných údajů po uzavření smlouvy. Rozsah a podmínky katalogizace majetku jsou Přílohou 6 této smlouvy. Bez stanoviska Úř OSK SOJ k naplnění katalogizační doložky nelze nabyvateli fakturovat.
2. Předmětem katalogizace je „DIGITÁLNÍ ARCHIV MO“, JKM 7010, TPP 0 (položka nestandardní), účtová třída „0“, druh položky 3 (soubor movitých věcí), účetní zatřídění 222 (dlouhodobý hmotný majetek), které zahrnuje i související programové vybavení.

Článek 12
SANKČNÍ UJEDNÁNÍ

1. Nepředá-li poskytovatel nabyvateli řádně systém DA MO v době a místě plnění dle čl. 4 této smlouvy, zaplatí nabyvateli za každý započatý den prodlení smluvní pokutu ve výši 0,2 % z celkové ceny bez DPH dle čl. 3 odst. 3, a to až do úplného splnění závazku nebo do zániku

smluvního vztahu. Tím nejsou dotčena ustanovení čl. 13 smlouvy. Okamžik práva fakturace vzniká prvním dnem prodlení.

2. V případě porušení povinnosti poskytovatele dle čl. 9 odst. 3 této smlouvy, zaplatí poskytovatel nabyvateli za každý rok, kdy nebyl dodržen maximální parametr 10% nedostupnosti funkcionalit (downtime) systému DA MO, jednorázovou smluvní pokutu ve výši 200 000 Kč.

3. V případě prodlení poskytovatele se zabezpečením služeb HelpDesku, poskytnutím technické podpory a úprav programového vybavení dle čl. 9 odst. 7 a odst. 8 této smlouvy zaplatí poskytovatel nabyvateli za každý započatý den prodlení smluvní pokutu ve výši 0,2 % z ceny bez DPH předmětného plnění dle cenového rozkladu uvedeného v Příloze 4 této smlouvy za každý i započatý den prodlení až do řádného splnění závazku, nebo do odstoupení nabyvatele od smlouvy.

4. V případě prodlení nabyvatele s úhradou faktury zaplatí nabyvatel poskytovateli úrok z prodlení v zákonné výši stanovené nařízením vlády za každý i započatý den prodlení až do úplného zaplacení dlužné částky.

5. Právo vymáhat a fakturovat smluvní pokuty a úrok z prodlení vzniká poskytovateli a nabyvateli prvním dnem následujícím po marném uplynutí lhůty. Smluvní pokuty jsou splatné do 30 dnů od doručení jejich vyúčtování povinné straně.

6. Smluvní pokuty hradí povinná strana bez ohledu na to, v jaké výši vznikla druhé straně škoda. Náhrada škody je vymahatelná samostatně v plné výši vedle smluvní pokuty nebo úroku z prodlení.

Článek 13
ZÁNIK ZÁVAZKU ZE SMLOUVY

1. Závazek ze smlouvy zaniká:
   a) splněním předmětu smlouvy
   b) písemnou dohodou smluvních stran spojenou se vzájemným vypořádáním závazků,
   c) jednostranným odstoupením nabyvatele od smlouvy dle § 2002 OZ pro její podstatné porušení poskytovatelem s tím, že podstatným porušením smlouvy se rozumí:
      - nedodání předmětu smlouvy dle čl. 2 odst. 1 - 4 této smlouvy řádně a včas (řádně a včas znamená v souladu se článkem 2 odst. 1 - 4 a článkem 4 smlouvy - „řádně“ vyjadřuje předání bez vad (akceptovatelné), „včas“ vyjadřuje předání v časovém rozmezí definovaném touto smlouvou), pokud prodlení poskytovatele i po urgencích ze strany nabyvatele přesáhne 30 kalendářních dní,
      - nesplnění povinností vyplývajících z čl. 9 této smlouvy, pokud prodlení poskytovatele i po urgencích ze strany nabyvatele přesáhne 30 kalendářních dní,
      - nesplnění povinností vyplývajících z čl. 10 této smlouvy.
   d) jednostranným odstoupením nabyvatele od smlouvy v případě, že bude vůči majetku poskytovatele vyhlášeno insolvenční řízení, v němž bude vydáno rozhodnutí o úpadku nebo byl-li vůči poskytovateli insolvenční návrh zamítnut pro nedostatek majetku k úhradě nákladů insolvenčního řízení,
   e) jednostranným odstoupením nabyvatele od smlouvy, pokud poskytovatel uvedl v nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek zadávacího řízení.

Článek 14
ZVLÁŠTNÍ UJEDNÁNÍ

1. Nejpozději do deseti pracovních dnů před zánikem této smlouvy uplynutím doby jejího trvání, resp. do deseti pracovních dnů od zániku této smlouvy jiným způsobem, sepíší smluvní strany protokol o ukončení poskytování záručního servisu a technické podpory, ve kterém uvedou okolnosti podstatné pro další podporu, provoz a údržbu a servis systému DA MO.
2. Poskytovatel je povinen dle pokynů nabyvatele poskytnout v celkovém rozsahu do 30 člověkodnů veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s nabyvatelem a popřípadě s třetími osobami za účelem plynulého a řádného převedení všech činností spojených s poskytováním plnění dle této smlouvy na nabyvatele a/nebo nového poskytovatele, ke kterému dojde po skončení účinnosti této smlouvy (dále jen "Exit"). Uvedená povinnost poskytovatele se uplatní i pro případ dohody smluvních stran na ukončení této smlouvy, pokud smluvní strany v rámci dohody nestanoví jinak.
3. Za data, která budou dle tohoto článku smlouvy předávána poskytovatelem nabyvateli nebo jím určené třetí osobě, jsou považována veškerá data, zejména pak data do systému DA MO zadaná a vložená, data zpracovaná v systému DA MO a data konfigurací.
4. Poskytovatel je povinen dopracovat nebo aktualizovat na základě pokynu nabyvatele existující dokumentaci vymezující postup provedení Exitu (dále jen "Exit plán") s úpravou dle aktuální znalosti plynoucí z plnění této smlouvy, a poskytne plnění nezbytná k realizaci Exit plánu za přiměřeného použití vhodných ustanovení této smlouvy. Nabyvatel je oprávněn požádat o dopracování/aktualizaci Exit plánu nejdříve 12 měsíců před řádným ukončením této smlouvy, kdykoliv spolu s odstoupením nabyvatele od této smlouvy. Závazek dle tohoto ustanovení platí i po uplynutí doby trvání této smlouvy, a to maximálně do 3 měsíců po jejím ukončení. Poskytovatel se zavazuje provést dopracování a aktualizaci Exit plánu a poskytnout nezbytná plnění pro jeho realizaci do 2 měsíců od doručení takového požadavku nabyvatele, nestanoví-li nabyvatel jinak.

Článek 15
ZÁVĚREČNÁ USTANOVENÍ

1. Smlouva je vyhotovena elektronicky o 12 stranách a 6 přílohách.
2. Veškeré změny a doplňky této smlouvy je možno provádět jen se souhlasem obou smluvních stran, a to pouze formou písemných, vzestupně číslovaných a takto označených dodatků, které se stávají nedílnou součástí smlouvy. Za změnu smlouvy se nepovažuje změna identifikačních údajů některé ze smluvních stran, kontaktních údajů nebo odpovědných osob. Tato změna bude druhé smluvní straně písemně oznámena prostřednictvím ISDS.
3. Smluvní strany prohlašují, že jim nejsou známy žádné skutečnosti, které by uzavření smlouvy vylučovaly a berou na vědomí, že v plném rozsahu nesou veškeré právní důsledky plynoucí z vědomě jimi udaných nepravdivých údajů. Na důkaz svého souhlasu s obsahem smlouvy připojují pod ní své podpisy.
4. Pokud tato smlouva nestanoví jinak, řídí se tento smluvní vztah příslušnými ustanoveními OZ a AZ.
5. Poskytovatel souhlasí, aby smlouva po jejím podpisu byla zveřejněna.
6. Smlouva nabývá platnosti dnem jejího podpisu poslední smluvní stranou a účinnosti dnem uveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

7. Nedílnou součástí smlouvy jsou níže uvedené přílohy:

Příloha 1 – Specifikace předmětu plnění	- 45 stran
Příloha 2 – Specifikace předmětu plnění IBM	- 42 stran
Příloha 3 – Objasnění a doplnění dokladů k nabídce IBM (bez přílohy č.1)	- 43 stran
Příloha 4 – Cenový rozklad IBM	- 1 strana
Příloha 5 – Specifikace utajovaných informací	- 1 strana
Příloha 6 – Katalogizační doložka	- 1 strana

Za nabyvatele:

Ing. Petr ZÁBOREC
ředitel odboru vyzbrojování pozemních sil
a KIS SVA MO

podepsáno elektronicky

Za poskytovatele:

Ing. Petr HAVLÍK
jednatel společnosti

podepsáno elektronicky

Ing. Petr Havlík

Digitálně podepsal:
16.04.2021 20:03
Lokace: Praha
Kontakt:
petr_havlik@cz.ibm.com

Příloha 1 smlouvy č. 195310197
Výtisk č. 1
Počet stran: 45

Specifikace požadavků na předmět plnění veřejné zakázky

Digitální archiv MO – nákup

Název pro katalogizaci: DIGITÁLNÍ ARCHIV MO

PŘEDMĚT VEŘEJNÉ ZAKÁZKY

Navrhované řešení musí být realizováno v souladu s platnými právními normami:

- nařízením eIDAS (910/2014/ES) o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, včetně navazujících prováděcích předpisů (zákonu č. 297/2016 Sb., zákonu č. 298/2016 Sb., příp. dalším),
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 110/2019 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
- Případné další předpisy a normy platné v době dodání a záruky.

Předmětem veřejné zakázky je zhotovení, dodání, instalace, předání, zaškolení a proškolování obsluhy, servis a legislativní upgrade systému „Digitální archiv MO“ (dále jen DA MO), který se skládá z následujících částí:

- **Softwarové licence:**
  -poskytnutí SW licencí a práv užití potřebných pro zhotovení a provoz DA MO
- **Hardwarové komponenty:**
  - hardware potřebný pro dlouhodobé garantované uložení archiválií a provoz řešení DA MO,
  - PC digitalizačního pracoviště a místnosti „Badatelna“.
- **Dokumentace DA MO**
- **Služby:**
  -řízení projektu DA MO:
    - ▪předimplementační analýza a Detailní návrh řešení,
    - ▪implementace DA MO – instalace, konfigurace, integrace,
    - ▪akceptační procesy – funkční a integrační testy,
    - ▪zaškolení obsluh,

  -migrace obsahu ze stávajícího DMS systému Documentum.
- **Záruční servis a technická podpora:**
  - záruční servis po dobu 60 měsíců,
  - technická podpora hardwarových a softwarových komponent po dobu 60 měsíců,
  - legislativní upgrade po dobu 60 měsíců,

- proškolování obsluh.

Zadavatel požaduje řešení sestavené z produktů, které jsou v době podání nabídky běžně na trhu a pro které na trhu existuje technická podpora, kterou může poskytnout více dodavatelů.
Dále požaduje, aby navržené řešení přímo logicky, koncepčně i technologicky navazovalo na již realizovaný projekt implementace Elektronického správního archivu MO (dále také ESA MO).
DA MO musí v intencích navrženého řešení v co největší možné míře zachovat kontinuitu po stránce aplikačního programového vybavení i navrženého hardware a musí také přímo navazovat na fungující systémy neutajovaných IS resortu MO. Dodavatel je povinen na výzvu zadavatele připravit ve spolupráci s ním potřebné podklady, nezbytné pro podání žádosti zadavatele o získání souhlasného stanoviska OHA Ministerstva vnitra ve smyslu zákona 365/2000 Sb.

1 Všeobecné informace pro dodavatele

1.1 Návaznost na ESA MO

DA MO bude realizován s přímou logickou, koncepční a technologickou návazností na ESA MO, jako jeho rozšíření. Je proto nutné v intencích navrženého řešení DA MO v co největší možné míře zachovat kontinuitu po stránce aplikačního programového vybavení i navrženého hardware.
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.
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 jsou využity rozhraní LDAP, TSP, OCSP, SOAP a REST a je též využita sdílená složka pravidelně kontrolována skenerem souborového systému.

1.2 Všeobecné požadavky

Pro vyloučení pochybností zadavatel explicitně požaduje splnění následujících všeobecných požadavků, které mohou být upřesněny v dalším popisu řešení níže:

- Zadavatel trvá na tom, aby součástí nabídkové ceny byly všechny služby, licence i HW komponenty tvořící řešení.
- Zadavatel nepřipouští možnost využití stávajících HW a SW komponent ve vlastnictví zadavatele s výjimkou těch, které jsou vyjmenovány v části „Popis současného prostředí" - kap. 16.
- Zadavatel trvá na tom, aby všechny součásti řešení byly v době dodání nové (ne starší než rok) a nepoužité.
- Zadavatel požaduje, aby úložiště systému v každé ze dvou lokalit bylo realizováno prostřednictvím zařízení typu Content-Addressed Storage (CAS)/Fixed Content Storage (FCS).
- Řešení musí být navrženo takovým způsobem, aby uložené dokumenty, archiválie ani jiná data neopustila infrastrukturu a zázemí zadavatele s výjimkou certifikátů pro potřeby ověření jejich platnosti. Zadavatel požaduje použití certifikátů vydaných kvalifikovanými poskytovateli certifikačních služeb dle Ministerstva vnitra ČR. Shoda je požadována minimálně v rozsahu požadavků na prostředky a data pro elektronický podpis a na dokumenty v digitální podobě definovaných v zákoně č. 499/2004 Sb., v zákoně č. 297/2016 Sb. a v zákoně č. 298/2016 Sb. Seznam certifikačních autorit bude vytvářen v průběhu provozu, avšak řešení musí být připraveno i na rozšíření certifikátů. Toto rozšíření však nesmí být řešeno automatickým způsobem, tato funkce musí být závislá na manuální akceptaci administrátorem.

2 Výchozí stav a požadavky na DA MO

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.

- 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.

2.1 Funkční požadavky

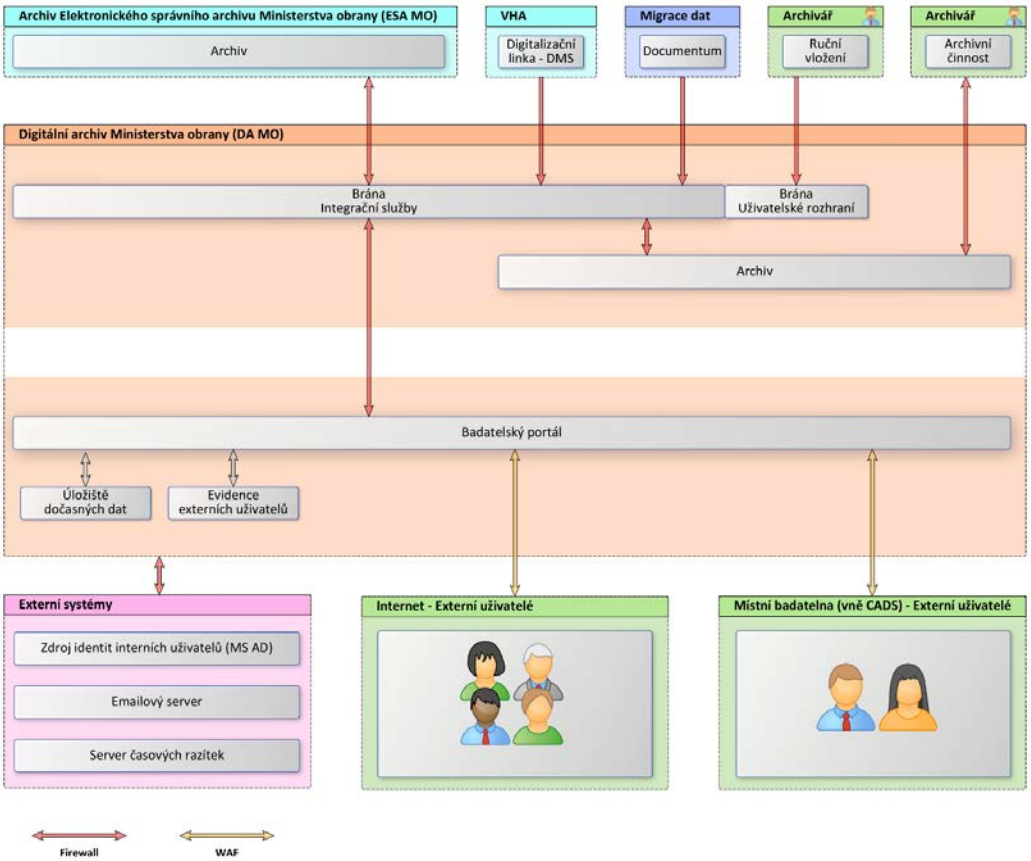
- Systém DA MO zabezpečí dlouhodobou/trvalou garantovanou archivaci neutajovaných archiválií, které se do archivu přesunou:
  - ze systému ESA MO po uplynutí maximálně třiceti let od ukončení skartačního řízení u původce dokumentu. Dokumenty mohou být do DA MO přesunuty dříve, a to na základě skartačního 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 výběrové skartace (např. v případech přehodnocení významu archiválií).

2.2 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.
- 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 interního uživatele proběhne formou autentizace vůči AD CADS. Přihlášení interního uživatele DA MO proběhne jménem a heslem vůči internímu LDAP DA MO. Integrace s JIP KAAS není plánována, jedná se o čistě lokální IS MO bez napojení na veřejné eGov prostředí státu.
- 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 prostředky tohoto Portálu. Systém DA MO musí být připraven na způsob řízení přístupu externích uživatelů do Badatelského portálu s užitím Národního bodu pro el. identifikaci fyzických osob dle zákona č. 250/2017 Sb., aby bylo zajištěno nezpochybnitelné ztotožnění uživatele. Národní identitní autorita (NIA) pro uvedenou elektronickou identifikaci a autentizaci se skládá z těchto komponent - Národní bod, Kvalifikovaný správce, Základní registry a Národní uzel eIDAS. S připraveností na využití NIA tak bude zajištěna státem garantovaná služba identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principu Single Sign-On.
- Webový portál DA MO musí být připraven na propojení s Portálem občana MV odkazovou dlaždicí.

2.3 Popis řešení DA MO

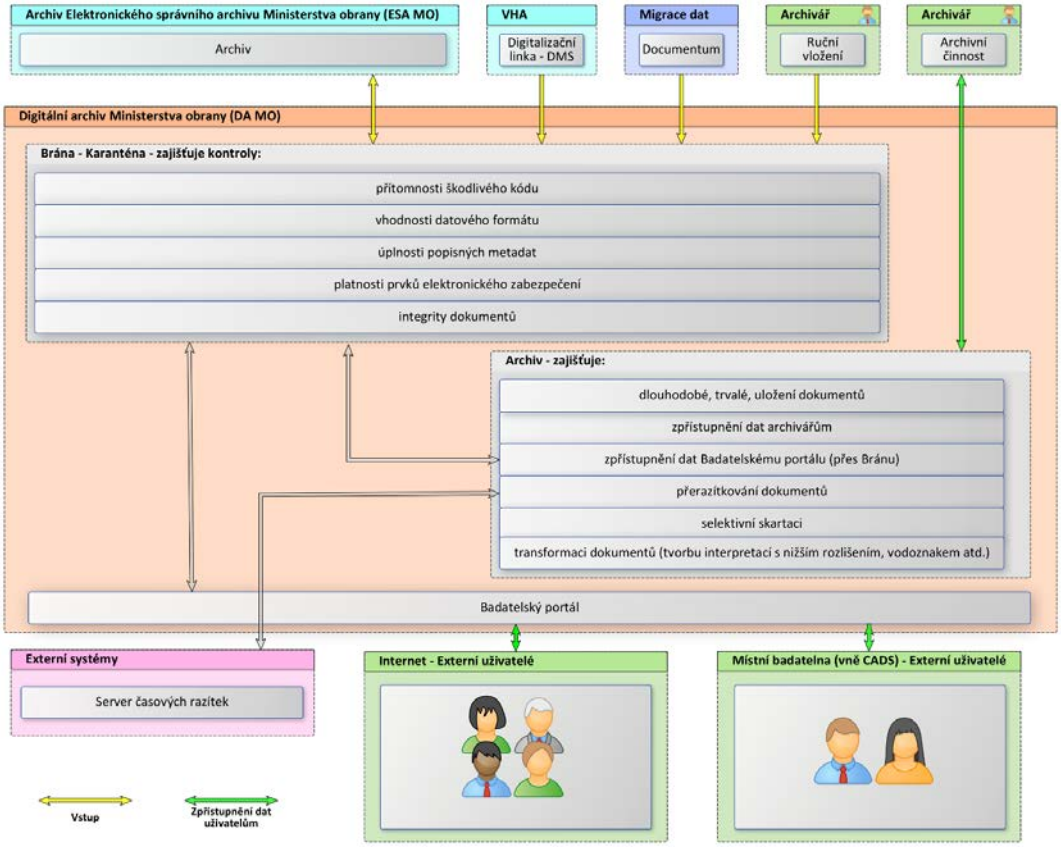
Níže na obrázku je schematicky zobrazen návrh DA MO.



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 balíčky 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



3 Brána DA MO

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:
  - 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 a ZFO (formát zpráv datových schránek).
- 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.

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.

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 výběrové skartace.

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).
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 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 archiválií uložených v Archivu v rámci uživatelského prostředí Brány bez nutnosti stahovat archiválii 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

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 archiválii 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 archiválii důkazní materiál, obsahující všechny nezbytné informace pro prokázání důvěryhodnosti archiválie.
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 archiválií. 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 archiválií 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 archiválií také vodoznak). Dále musí umožnit kromě individuálního zveřejnění i hromadný výběr archiválií (resp. jejich interpretací) na základě uživatelem zadaných metadat. V rámci procesu zveřejnění archiválií na Portál musí být možnost nastavit k nim úroveň přístupových oprávnění pro jednotlivé skupiny externích uživatelů (registrovaní/ztotožnění).

3.2.5 Skartace archiválií

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

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) 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.

3.3 Statistika

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

- 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, výběrové skartaci mimo skartační řízení.

- 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 ke skartaci - pro příležitostnou skartaci mimo skartační řízení.

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 Archiv

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.
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. V případě změny metadat nebo archiválie (verze, anonymizace) v Archivu musí tento o takové změně informovat Bránu.

5 Badatelský portál

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. Portál bude připraven na propojení s Portálem občana MV odkazovou dlaždicí.
Způsob řízení přístupu externích uživatelů do Badatelského portálu bude připraven na užití Národního bodu pro el. identifikaci fyzických osob (NIA) dle zákona č. 250/2017 Sb., aby bylo zajištěno nezpochybnitelné ztotožnění uživatele. V návaznosti na autentizaci NIA portál umožní registraci a správu externích uživatelů pro 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.

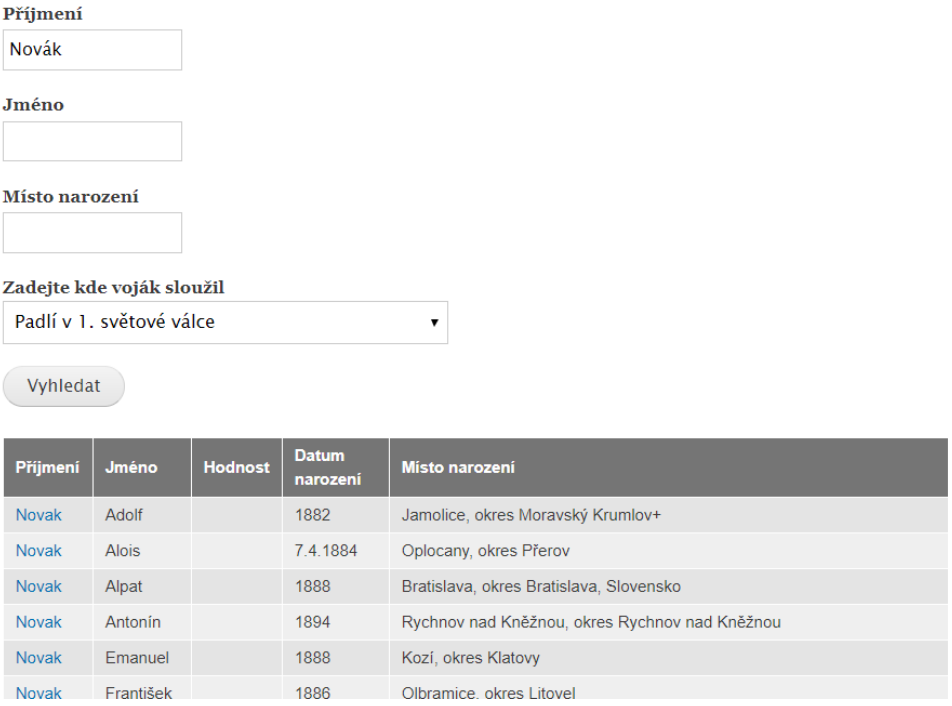
O nastavení úrovně přístupových práv k jednotlivým zveřejňovaným archiváliím rozhoduje archivář.
Badatelský portál bude obsahovat minimálně:

- 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,
  - 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) s vazbou na užití NIA,
  - 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“, rozlišení alespoň 2560x1440, OS Windows 10 OEM.

6 Digitalizace

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 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, v konfiguraci minimálně: CPU Intel i7, 16GB RAM, SSD disk 128GB, HDD 1TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440
- 2ks PC určených k verifikaci digitalizovaných dat v optimální konfiguraci k této činnosti, v konfiguraci minimálně: CPU Intel i7, 16GB RAM, SSD disk 128GB, HDD 1TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440
- 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+

- Implementace systému v rozsahu do 140 člověkodní a roční podpora 25 člověkodní.
- Samotný SW ELZA není předmětem dodávky.

Součástí dodávky je pořízení – lokalita Praha:

- 1ks APC Symmetra LX 12kVA Scalable to 16kVA N+1 Rack-mount 220/230/240V nebo 380/400/415V
- 1ks APC Symmetra LX Battery Module
- 8ks Rack PDU, 1U, 16A, 8x230V
- 1ks Jistič 3x20A
- 15ks Kabel 1-CXHK-R-J 5 x 4/O/-/B2 CAS 1dO
- 2ks Pomocný a montážní materiál (pro rack, pro UPS)

Součástí dodávky je pořízení – lokalita Olomouc-Bystrovany:

- 1ks APC Symmetra LX 8kVA Scalable to 16kVA N+1 Rack-mount 220/230/240V nebo 380/400/415V
- 1ks APC Symmetra LX Battery Module
- 8ks Rack PDU, 1U, 16A, 8x230V
- 1ks Jistič 3x20A
- 15ks Kabel 1-CXHK-R-J 5 x 4/O/-/B2 CAS 1dO
- 2ks 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.

- **Garantované smazání** – V případě požadavku na smazání archiválie z úložiště, musí být tato smazána takovým způsobem, který garantuje, že soubor ani žádnou z jeho částí není možné žádným způsobem obnovit.
- **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 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

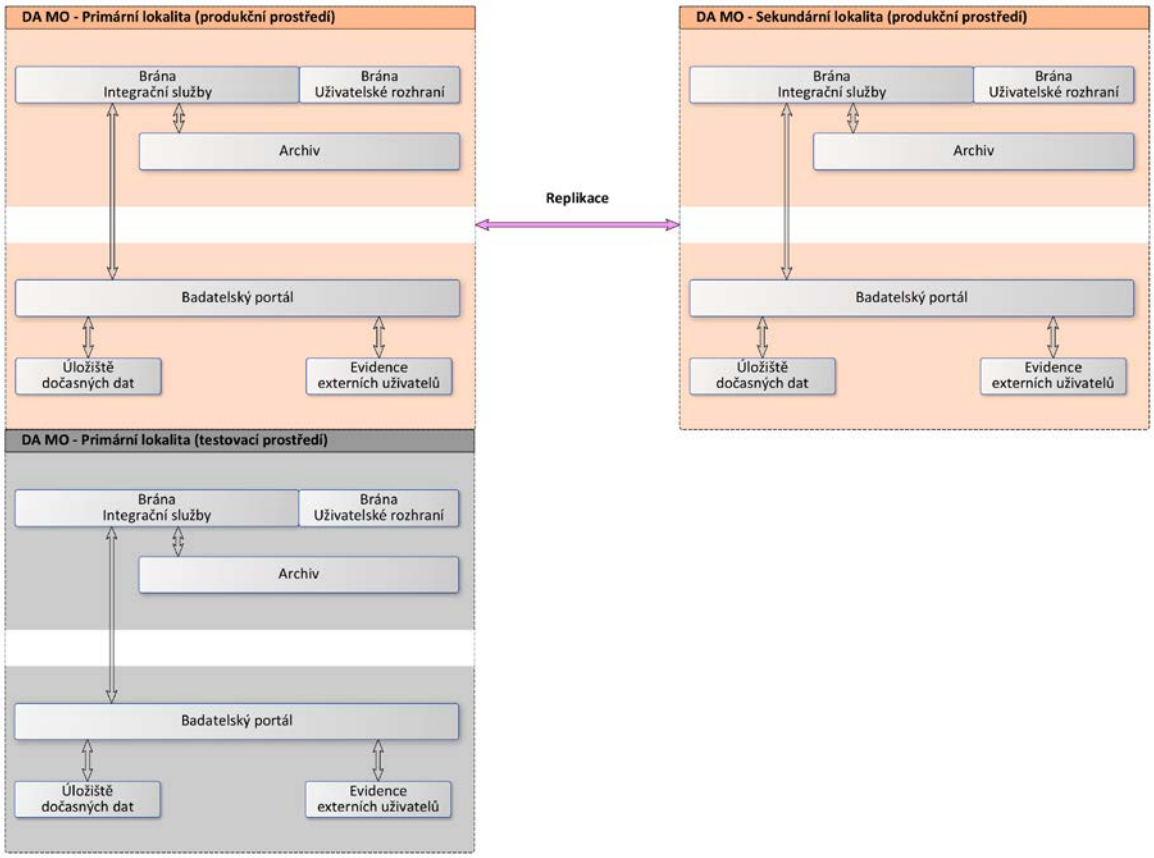
DA MO musí být navržen a realizován tak, aby nemohlo dojít ke ztrátě dat. Po dobu podpory systému dodavatel ručí za jejich ztrátu.
Jedná se o dodávku, nastavení a implementaci zálohování dat celého ESA MO, DA MO, DMS digitalizační linky, Archivu, systému ELZA, Badatelského portálu i jeho součásti v podobě 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.



11 Integrace

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

AtributDatový typ
hodnotaString(60)
typ_slozkyString(1)

Typ mo a_doc
AtributDatový typ
cislo_krabiceInteger
fondString(60)
inventarni_cisloInteger

poznamkaString(255)
rejstrikString(255)
signaturaString(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,
- 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. Vhodné je použít řešení, které nespoléhá pouze na detekci podle známých signatur, ale provádí pokročilejší behaviorální analýzu chování souboru v různých situacích.

14.5 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.

14.5.1 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. Na provozních databázích nebude umožněna lokální OS autentizace, ani vzdálená OS autentizace.

14.5.2 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 by měl být minimálně neúspěšný pokus o jakékoli operace, přístup privilegovaných uživatelů, a veškeré servisní operace nad databází. Auditní záznamy by mělo být možné ukládat, pořizovat a přistupovat k nim 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.

14.5.3 Databázové zálohy

Provozní databáze budou v pravidelných intervalech zálohovány.

14.6 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.

14.7 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.

14.8 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.

14.9 Síťová bezpečnost

14.9.1 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,
- mezi Archivem a externími systémy nesmí probíhat žádná přímá komunikace s výjimkou zabezpečené komunikace s TSA.

14.9.2 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.
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):

- 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).

16 Popis současného prostředí

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

16.1 Hardware

- 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.

16.2 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.

16.2.1 Použitý HW a SW u ESA MO

16.2.1.1 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

16.2.1.2 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

16.2.1.3 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

16.2.1.4 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

16.2.1.5 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

16.2.1.6 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
- HPE iLO

16.2.2 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).

16.2.3 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.
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).

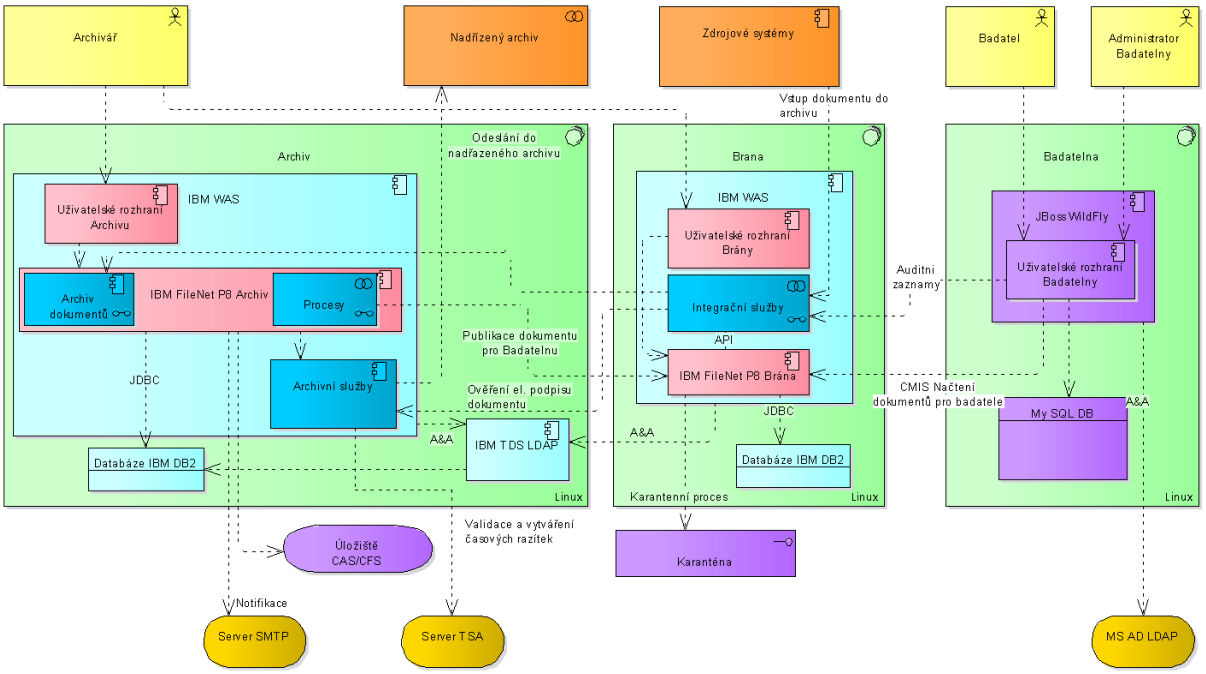
16.3 Výchozí stav

16.3.1 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. 499/2004 Sb., 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).

16.3.2 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.



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. 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:

- 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).

16.4 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.

16.4.1 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
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.

16.4.2 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 útvarčíselník útvarů**
- **Druh dokumentu výčet (Dokument NATO,..)**
- **Původní stupeň utajenívýčet**
- **Původcečíselník útvarů**
- **Kód autorařetězec**
- **Názevřetězec**
- Datum vytvořenídatum
- **Rok (myšleno vytvoření)rok**
- Originálboolena
- **Charakter dokumentuvýčet (Spis,..)**
- **Počet listůčíslo**
- Arch. Sk ozn. Pův.
- **Fondčíselník ? výčet ?**
- **Kartonyčíselník**
- **P.č. kartonuřetězec**
- Identifikace u útvaruřetězec
- Vstupní poznámkařetězec
- Protokolčíselník
- Zeměčísleník
- **Aktuální stupeň utajení:výčet**
- **Médiumvýčet (papír,..)**
- Označení výtiskuřetězec

16.5 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.

16.5.1 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..)
(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 2-místný 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).

16.5.2 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
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
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
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

17 Rámcový harmonogram realizace plnění

Předávání dodávky při plnění smlouvy dodavatel/poskytovatel dohodne minimálně 20 dní předem s osobou oprávněnou jednat ve věcech technických uvedenou ve smlouvě a provede je v následujících fázích:

17.1 Start projektu "Pořízení DA MO"

Tato aktivita začíná v okamžiku podpisu smlouvy na dodávku řešení Digitálního archivu MO (DA MO).

17.2 Předimplementační analýza a návrh

Dodavatel/poskytovatel provede detailní předimplementační analýzu prostředí nabyvatele a na jejím základě provede detailní návrh řešení včetně požadavků na nabyvatele týkající se jeho součinností. K tomu obdrží od nabyvatele (pověřené osoby) potřebné podklady a informace (včetně datového modelu pro migraci dat). V této aktivitě dojde především k

- technickému návrhu způsobu propojení DA MO na ESA MO,
- technickému návrhu propojení na externí zdroje informací jako jsou externí systémy poskytující časová razítka, CRL, certifikáty,
- technickému návrhu propojení na interní systémy pro autentizaci uživatelů a emailovou komunikaci.

Výsledkem této projektové části je oboustranně schválený Detailní návrh řešení (obsahující reálný harmonogram projektu, požadavky na součinnost nabyvatele a vlastní technický návrh řešení DA MO).

17.3 Implementace DA MO

Je rozdělena na implementaci Brány DA MO, implementaci Archivu DA MO, implementaci Badatelského portálu, implementaci DMS skenovací linky a implementaci propojení primární a záložní lokality, které zabezpečí DA MO proti výpadku nebo i zničení dat / informací v jedné lokalitě.

17.4 Akceptace – převzetí plnění

Budou postupně samostatně prováděny akceptace funkčních částí řešení, jak je navrženo v implementační části, kterými jsou:

- Dílčí akceptace DMS Digitalizačního pracoviště,
- Dílčí akceptace části Brána DA MO,
- Dílčí akceptace části Archiv DA MO,
- Dílčí akceptace části Badatelský portál vč. nové webové prezentace VHU,
- Dílčí akceptace systému ELZA,
- Dílčí akceptace komunikace primární a záložní lokalitou.

Při dílčí akceptaci DMS Digitalizačního pracoviště dojde k ověření všech specifikovaných a objednaných HW a SW prvků a k ověření jejich správné funkcionality.
U části dílčích akceptací Brána, Badatelský portál a Archiv DA MO, komunikace s primární a záložní lokalitou dojde postupně k provedení:

- Funkčních testů pro ověření objednaných funkcionalit,

- Integračních testů pro ověření zda dílčí část komunikuje správně se svým okolím.

Nakonec bude provedeno vyhodnocení všech provedených testů, a pokud výsledky těchto testů dopadnou dle připravených kritérií, bude dílčí část akceptována.
Jako závěrečná, ale také nejdůležitější část akceptací je provedení celkové Akceptace systému DA MO. Tato celková akceptace zahrnuje provedení:

- generálního funkčního testu,
- generálního integračního testu,

které otestují systém DA MO jako celek včetně všech integračních vazeb.
Výsledkem je pak celková akceptace řešení DA MO, které umožní následně spuštění Zkušebního provozu.

17.5 Vytvoření dokumentace řešení

Součástí dodávky řešení DA MO je dodávka kompletní dokumentace, která zahrnuje vytvoření kompletního popisu řešení, kompletní provozní dokumentaci včetně popisu praktické údržby, řešení, příprava strategických plánů podle metodiky PLATTER (Planning Tool for Trusted Electronic Repositoriem) „Plán důvěryhodného digitálního repozitáře“.
Dodavatel/poskytovatel předá k dílu kompletní projektovou dokumentaci dle platných norem a předpisů, včetně doporučení k provozu, údržby, návodu k obsluze, seznamů předmětů v soupravách s jejich označením a popisem (součástí je i položkový rozpočet) vše v českém jazyce. Dokumentaci předá ve vázané knize a doplní DVD v elektronické podobě ve formátu PDF a doc. Součástí dokumentace bude doporučení pro snížení rizik a návod pro obnovu funkčnosti po havárii. Součástí dokumentace bude doporučení pro zabezpečení optimálního způsobu pozáručního servisu.

17.6 Zaškolení pracovníků DA MO

Součástí této projektové části jsou zaškolení pracovníků podle jejich rolí a pracovního zaměření:

- 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.

17.7 Zkušební provoz DA MO (zajišťuje provozovatel/nabyvatel)

V rámci zkušebního provozu dojde nejprve k provedení migrace dat ze systému Documentum. Následně po provedení migrace dat bude spuštěn zkušební provoz, který prověří funkčnost systému DA MO, ELZA a DMS digitalizačního pracoviště včetně HW a SW prvků. Cílem bude prověřit funkčnost dodaného systému, návrh řešení architektury, prověření dob odezvy primárního a záložního datového úložiště, migrace dat mezi oběma datovými úložišti a způsob poskytování podpory Helpdesku. Součástí zkušebního provozu bude minimálně 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. Samostatně bude ověřena funkcionalita systému ELZA.

18 Zkratky a pojmy

Zkratka	Popis
AdES	Advanced Electronic Signature

Zkratka	Popis
AIP	Archival Information Package
API	Application Programming Interface
BA	Bezpečnostní archiv
BASE64	Schéma pro kódování binárního obsahu do ASCII
CA	Certifikační autorita
CAdES	Cryptographic Message Syntax Advanced Electronic Signature
CADS	Celoarmádní datová síť
CRL	Certificate revocation list
CSV	Comma Separated Values
DA	Digitální archiv
DEA	Důvěryhodný elektronický archiv
DIP	Dissemination Information Package
DMS	Document Management System
DRAMBORA	Digital Repository Audit Method Based on Risk Assessment
ECM	Enterprise Content Management
ED	Elektronický dokument
eIDAS	Electronic Identification and Signature
ELZA	Pořádací software archiválií
ESA	Elektronický správní archiv
ESSS	Elektronický systém spisové služby
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation (Obecné nařízení o ochr. osobních údajů)
ISDS	Informační systém datových schránek
ISMS	Information Security Management Systém
LTP	Long Therm Preversation (dlouhodobá/trvalá péče)
MD	Man-Day, "člověkoden" práce
METS	Metadata Encoding and Transmission Standard
MO	Ministerstvo obrany
MS AD	Microsoft Active Directory
MTOM	Message Transmission Optimization Mechanism
OAI - PHM	Open Archives Initiative - Protocol for Metadata Harvesting
OAIS	Open Archival Information System
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
ODF	OpenDocument Format
OOXML	Office Open XML
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
Zkratka	Popis
PDÚ	Primární datové úložiště
PNG	Portable Network Graphics

Zkratka	Popis
POST	Jedna z metod HTTP protokolu
REST	Representational State Transfer
SA AČR	Správní archiv Armády České republiky
SA MO	Správní archiv Ministerstva obrany
SIP	Submission Information Package
SOAP	Simple Object Access Protocol
SVG	Scalable Vector Graphics
TIFF	Tagged Image File Format
TRAC	Trustworthy Repositories Audit & Certification
TSA	Autorita časových razítek
TSL	Trusted Service List
UAT	User Acceptance Testing - uživatelské akceptační testování
VHA	Vojenský historický archiv
VZ	Veřejná zakázka
WAF	Web Application Firewall
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
ZDÚ	Záložní datové úložiště
ZFO	Formát zpráv datových schránek

Příloha 2 smlouvy č. 195310197

Počet stran: 42

Specifikace předmětu plnění IBM veřejné zakázky *Digitální archiv MO – nákup*

Název pro katalogizaci: DIGITÁLNÍ ARCHIV MO

OBSAH

1. PŘEDMĚT VEŘEJNÉ ZAKÁZKY

Navržené řešení uvedené v kap.2 a dále, které Poskytovatel níže popisuje, bude Poskytovatel realizovat řešením s přímou logickou, koncepční a technologickou návazností na provozovaný systém ESA MO, a tím zajistí jeho rozšíření. V intencích nutného je navržené řešení DA MO v co největší možné míře připraveno zachovat kontinuitu po stránce aplikačního programového vybavení i navrženého a použitého hardware a uživatelského rozhraní.

Řešení DA MO použije komponenty a technologie, které Nabyvatel uvedl v rámci popisu aktuálního řešení a doplňujících odpovědí. Zároveň však staví systém DA MO vedle aktuálního systému, a používá pouze systémové a technologické komponenty, jež slouží pro dodatečné využití stávajících zdrojů (HW a SW) a jejich efektivnější použití.

1.1. Popis prostředí Nabyvatele

Poskytoval uvádí popis Nabyvatele uvedeného aktuálního stavu. Poskytoval zároveň uvádí, že řešení, které dodá, je připraveno naplnit všechny požadavky (funkční i nefunkční, další), a zároveň respektuje aktuální stav a poskytnuté zařízení a technologie Nabyvatelem.

Současný stav

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.
- 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.

1.2. Požadavky Nabyvatele na systém DA MO

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, i přesto, že většina dokumentů by měla vstupovat do systému prostřednictvím automaticky.
- 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 výběrové skartace (např. v případech přehodnocení významu archiválií).

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.
- 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).
- 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 interního uživatele proběhne formou autentizace vůči AD CADS. Přihlášení interního uživatele DA MO proběhne jménem a heslem vůči internímu LDAP DA MO. Integrace s JIP KAAS není plánována, jedná se o čistě lokální IS MO bez napojení na veřejné eGov prostředí státu.
- 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 prostředky tohoto Portálu. Systém DA MO musí být připraven na způsob řízení přístupu externích uživatelů do Badatelského portálu s užitím Národního bodu pro el. identifikaci fyzických osob dle zákona č. 250/2017 Sb., aby bylo zajištěno nezpochybnitelné ztotožnění uživatele. Národní identitní autorita (NIA) pro uvedenou elektronickou identifikaci a autentizaci se skládá z těchto komponent - Národní bod, Kvalifikovaný správce, Základní registry a Národní uzel eIDAS. S připraveností na využití NIA tak bude zajištěna státem garantovaná služba identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principu Single Sign-On.
- Webový portál DA MO musí být připraven na propojení s Portálem občana MV odkazovou dlaždicí.

2. NÁVRH ŘEŠENÍ

2.1. Legislativní a normativní požadavky

Archiv je navržen, aby splňoval požadavky na dlouhodobé ukládání a archivaci informací dle referenčního modelu OAIS (Open archival information system) a standardem METS. Pro uchování dlouhodobé důvěryhodnosti archiválií je použito elektronického podpisu a časového razítka v souladu s ETSI standardy elektronického podpisu XAdES.

Řešení splňuje požadavky Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (Nařízení eIDAS) o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu včetně následně přijatých a v době podání nabídky platných prováděcích předpisů (zákon č. 297/2016 Sb., zákon č. 298/2016 Sb.). Dále řešení splňuje:

- zákon č.499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č.300/2008Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- zákon č.365/2000Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 110/2019 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
- případné související předpisy a normy platné v době dodání a záruky.

Elektronické podpisy, časová razítka a kvalifikované certifikáty odpovídají normě ETSI a to v oblastech:

- Ověření platnosti elektronických podpisů a jejich kontrola u archiválií, včetně neporušení kontrolního součtu a platnost certifikátu.
- Připojení technických metadat k archiválii. CRL (seznam zneplatněných certifikátů), OCSP odpovědi, případně další.
- Připojení časového razítka. Kontrolní součet tak chrání nejen samotnou archiválii, ale i její metadata.
- Zajištění pravidelného připojení dalších časových razítek před vypršením platnosti předchozího.

Automatizované elektronické rozhraní, které DA MO poskytne pro přenos dat do DA MO, bude plně v souladu s NSESSS (Národní standard pro elektronické systémy spisové služby dle zákona č. 365/2000 Sb).

DA MO bude připraven na způsob řízení přístupu externích uživatelů do Badatelského portálu s užitím Národního bodu pro el. identifikaci fyzických osob dle zákona č. 250/2017 Sb., aby bylo zajištěno nezpochybnitelné ztotožnění uživatele. Národní identitní autorita (NIA) pro uvedenou elektronickou identifikaci a autentizaci se skládá z těchto komponent - Národní bod, Kvalifikovaný správce, Základní registry a Národní uzel eIDAS. S připraveností na využití NIA tak bude zajištěna státem garantovaná služba identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principu Single Sign-On. Webový portál DA MO bude také připraven na propojení s Portálem občana MV odkazovou dlaždicí.

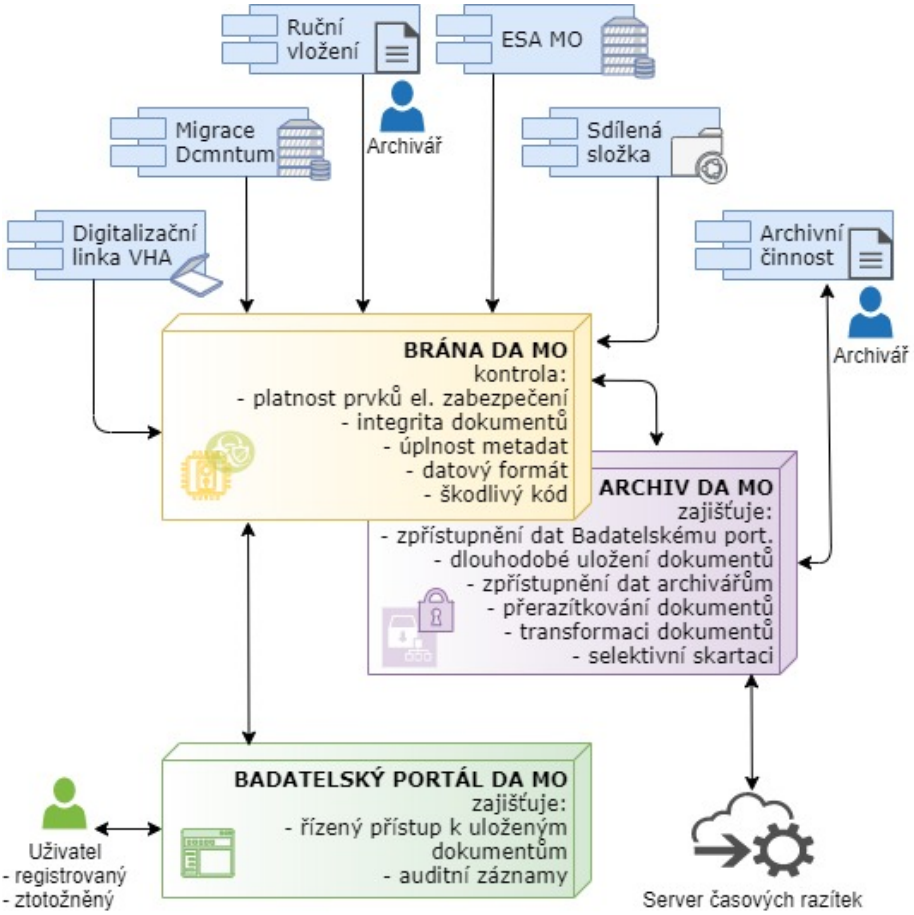
2.2. Architektura navrženého řešení

Navržené řešení přímo logicky, koncepčně i technologicky navazuje na již realizovaný projekt implementace Elektronického správního archivu MO (ESA MO).

Hlavní funkční celky jsou:

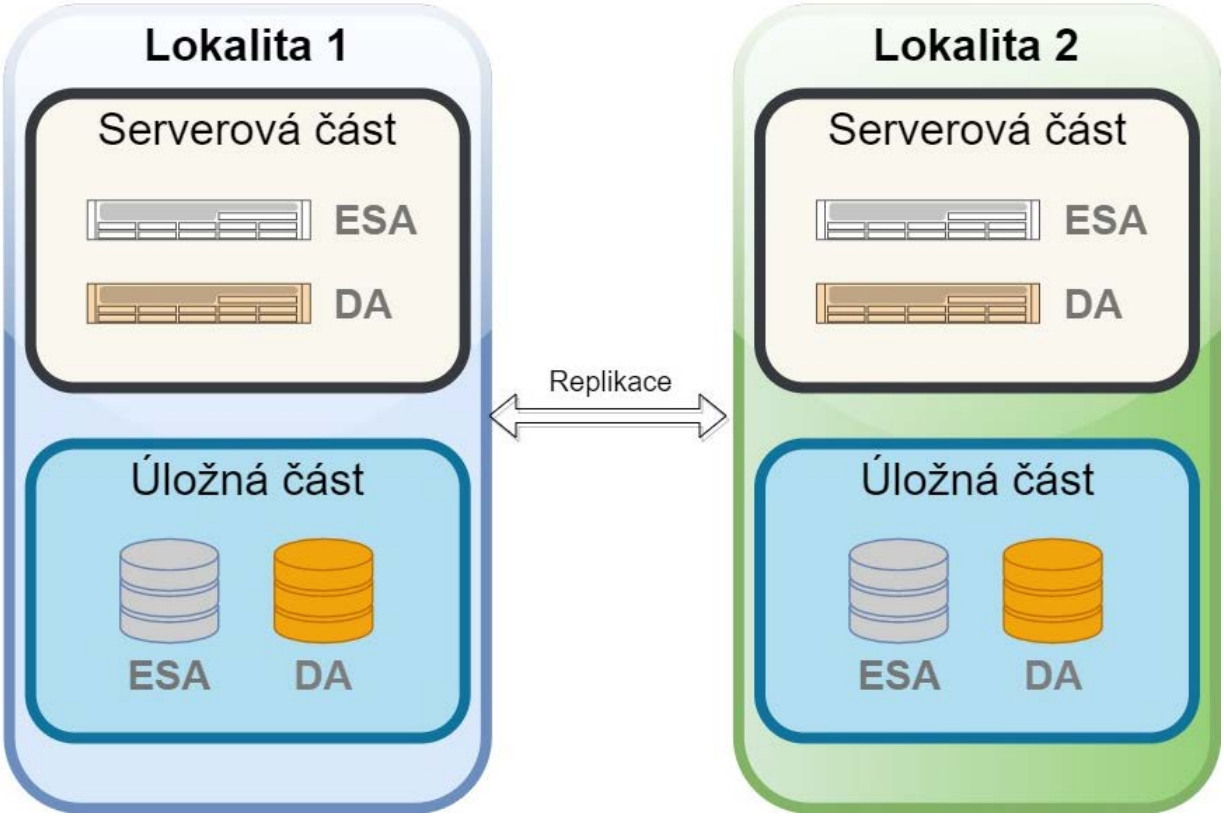
- Brána
- Archiv
- Badatelský portál

Pokud je textu zmíněn archiv s malým „a“, pak má poskytovatel na mysli archiv obecně, je-li zmíněn s velkým „A“, pak se jedná o konkrétní funkční celek DA MO.



Funkční model systému DA MO

Funkční celky jsou od sebe odděleny firewallem (firewally) a komunikace probíhá pomocí jasně definovaných kanálů (WS/SOAP, REST). Zdrojové systémy (tj. systémy, ze kterých pocházejí elektronické dokumenty) jsou s DA MO integrovány pomocí standardních rozhraní (např. WS/SAOP, WS/REST).



Lokality:

Systém je provozován v primární a záložní lokalitě, testovací instance všech požadovaných částí systému DA MO je pouze v primární lokalitě. Pro replikace budou použity technologie poskytované Nabyvatelem, případně pak rsync a nativní součást replikačních mechanismů databázového systému DB2 (DB2 HADR), tak, že bude naplněn požadavek pro RTO a RPO.

Jednotlivé části systému DA MO (Brána, Archiv, Badatelna), jsou segmentovány a odděleny firewallem. Je možné zde nastavovat pravidla, deep packet inspection, ACL nebo analyzovat data na aplikační vrstvě. Pro jednotlivé části, jejich ochranu, kontrolu a sledování dat, jsou použity sondy jak na firewallu, tak jsou i schopné ze switchů, které mají konfigurovány porty k zrcadlení provozu, sledovat provoz na úrovni datových toků a analyzovat tento provoz na základě signatur nebo i behaviorální analýzy, případně prostřednictvím definovaných pravidel. Vlastní nastavení je velmi variabilní a dokáže definovat jednotlivá pravidla nebo politiky, dle topologie. Inspekce je možné provádět i pro SSL provoz, jestliže budou poskytnuty a nastaveny klíče pro dešifrování takového provozu.

Systém DA MO je připraven k napojení na SIEM a tím poskytnout tak data pro další zpracování formou syslog-u. Zálohy jsou postaveny na osvědčené technologii známého výrobce a je možné pořizovat a kompletně spravovat prostřednictvím technologie, která zajistí komplexní zálohování všech požadovaných systémů, dotyčných serverů a jejich dat. Zálohy provozních dat z DB je možné ukládat v šifrované podobě.

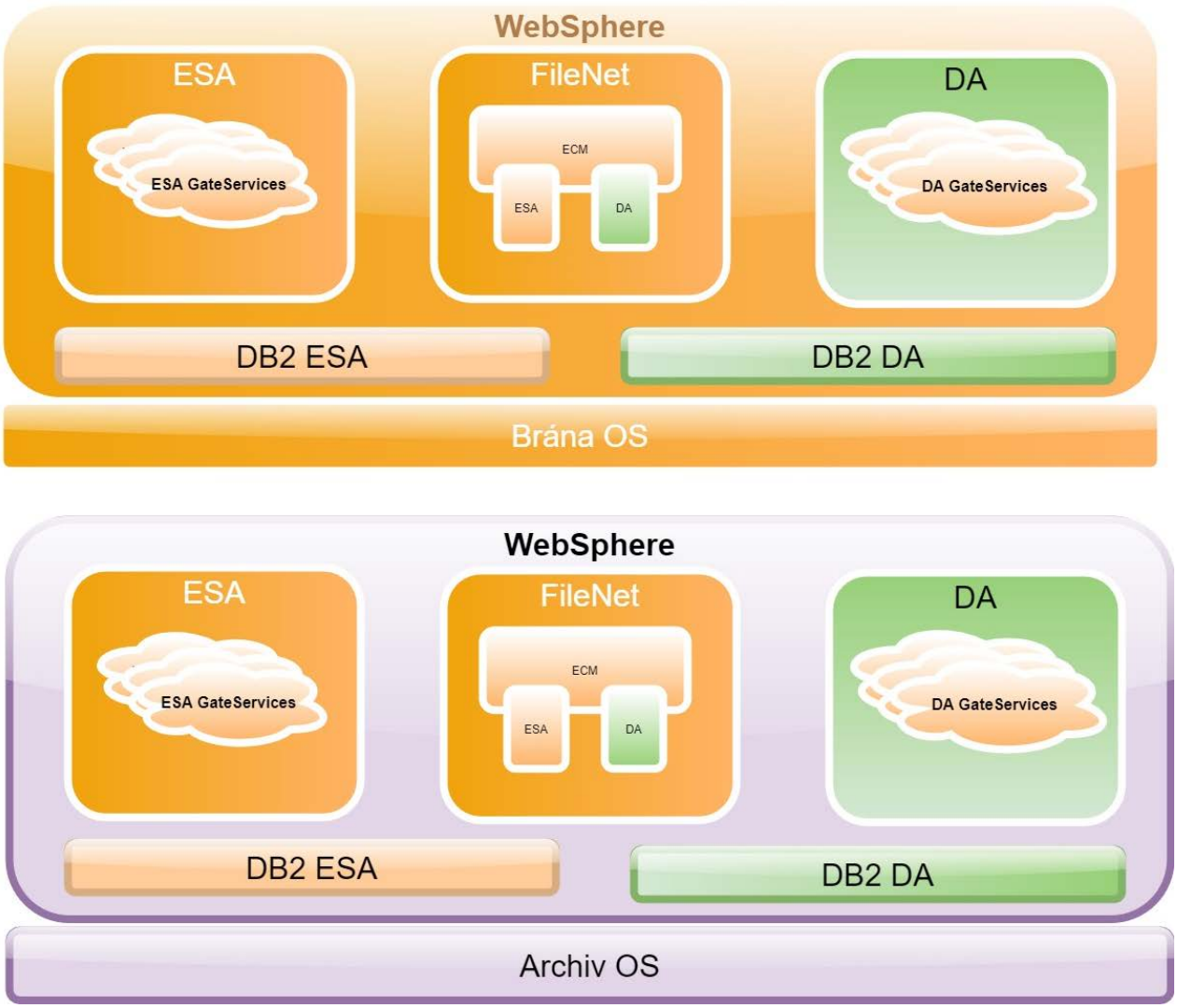
Garantované úložiště DA MO je realizováno nad stejnou technologickou platformou jako garantované úložiště, které využívá ESA MO. Toto je zajištěno použitím stávající technologií IBM FileNet a použitím stávajícího diskového pole, a stejnými programovými prostředky. Proto

garantované úložiště veškeré požadavky pro uložení dat a jejich ochranu před ztrátou, zajišťuje virtuální prostory, detailní audit mazání dat (retenční doba) a umožňuje replikaci dat. Zároveň je schopno prostřednictvím API komunikovat s Archivem.

Níže je zjednodušeně znázorněno, jak je nasazením systému DA MO realizováno rozšíření ESA MO z pohledu aplikačního SW Filenet a Websphere a technologického. Toto je také podrobněji popsáno dále v textu. Jednotlivé komponenty a technologie co možné v největší míře využívají stávající technologie proto, aby odpovídaly naplnění požadavků Nabyvatele. Zároveň jsou funkční celky systému DA MO a ESA MO odděleny, tak aby nemohlo dojít k záměně jejich prostředí.

Poskytovatel navrhl maximální možnou míru využití současného prostředí a prostředků Nabyvatele pro splnění cíle Nabyvatele uvedených v rámci ZD.

Základní komponentový model DA a ESA v jedné lokalitě:



2.2.1. Základní popis

2.2.1.1. FileNet

Základními komponenty pro Bránu a Archiv jsou FileNet Content Engine a FileNet BPM Engine.

Obě komponenty jsou logicky i fyzicky oddělené (Brána, Archiv). Technologie FileNet Content Engine umožňuje ukládání obsahu dokumentů, jejich metadat a řízení přístupu, a to i v logických prostorech s oddělenou správou. Lze vytvářet strukturu složek a vazeb mezi jednotlivými dokumentů. Tento návrh je a použité technologie jsou plně v souladu s modelem OAIS.

Na Bráně budou uložené dokumenty a balíčky čekající na import do Archivu. V Archivu se daná archiválie zpracuje dle příslušných tříd a uloží dle balíčků, razítek a certifikátů, aby uložená archiválie byla zcela jednoznačně identifikovatelná a za každých okolností integritní. Content engine má široké možnosti vyhledávání pomocí webového klienta. Je možné vytvářet i uložené hledání a to jak v rámci aplikace, tak si uživatel může vytvořit vlastní. Vyhledávání najde pouze obsah, ke kterému má daný uživatel dostatečná oprávnění. Vyhledávat lze fulltextově nebo podle metadat. Je možné nastavit formát zobrazení výsledku. Vyhledané dokumenty lze prohlížet případně exportovat.

FileNet umožňuje definovat vlastnosti dokumentů ve všech požadovaných formátech - lze ukládat různá metadata, minimálně v rozsahu typů text, celé číslo, číslo s desetinou čárkou, logická hodnota a datum) včetně vícehodnotových metadat.

Klient Content Enginu je webová aplikace, ze které bude vycházet uživatelské rozhraní. Součástí klienta je prohlížeč Daeja ViewONE. V prohlížeči je možné zobrazit, zvětšit, stránkovat, otáčet a tisknout zobrazený dokument. Umožňuje vytváření grafických anotací dokumentů. Prohlížené dokumenty se zobrazí přímo v prohlížeči, není nutné je tedy stahovat a ukládat na pracovní stanici uživatele a v případě nutnosti je možné toto zakázat a vynutit tak zamezení možnosti stažení dokumentu.

FileNet BPM Engine obsahuje nástroje pro automatické a manuální spouštění a řízení procesů. Procesy jsou řízeny pomocí Workflow. Předdefinované procesy budou v rámci Brány řídit vstup dokumentů a balíčků, spouštění a orchestraci služeb. V Archivu budou přednastavené procesy řídit přerazítkování, generování kopií pro Badatelský portál a skartační procesy. FileNet BPM Engine obsahuje pro vytváření uživatelských workflow a jejich spouštění.

Součástí FileNetu je i možnost určit, kde bude fyzicky uložen obsah dokumentu. U existujících dokumentů lze měnit jejich fyzické uložení.

Ukládaný obsah je možné šifrovat a zabezpečit tak uložení data. FileNet obsah automaticky dešifruje při přístupu přes rozhraní. Je také možné využít komprese a deduplikace dat.

Uživatelská vrstva je realizovaná jako webová aplikace (lehký klient) pomocí současných technologií (HTML, CSS, Javascript a potřebné serverové technologie). Uživatelskou vrstvu pro práci koncových uživatelů lze modifikovat, přizpůsobit nebo doplnit o nové funkcionality řízeným a zdokumentovaným způsobem.

2.2.1.2. Řízení přístupu

Navržený systém zajišťuje splnění předem definovaných heslových politik. Nastavení oprávnění, rolí a skupin je možné ve velmi širokém rozsahu – širším, než je požadováno zadávací dokumentací. Konkrétní způsob řešení bude přesněji stanoven v implementační analýze. Nicméně hlavním zdrojem oprávnění pro dokument, bude přiřazení oprávnění na základě třídy dokumentu a

uživatele nebo šablony, které dokument získá při jeho založení nebo nastavením administrátora systému.

Před přístupem uživatele k DA MO je ověřena jeho identita. Pro řízení přístupových práv k archiváliím využívá systém možnosti platformy FileNet v oblasti interní evidence uživatelských účtů. Uživatelé jsou autorizováni vůči internímu nebo externímu LDAP. Práva lze definovat i pro skupiny a role (Administrátoři, Analytici, Operátoři, Auditoři a případně i další), do kterých lze zařadit uživatele nebo servery a jejich služby. Přístup lze přidělit i speciálním rolím jako autor dokumentu nebo autorizovaný uživatel.

U strukturovaných dat lze nastavit dědičnost sad oprávnění. To funguje pro složky i pro složené dokumenty. Lze určit i hloubku zanoření, pokud bude dědičnost práv platit. Další úroveň řízení přístupu lze aplikovat na přístup k vybraným metadatům dokumentu.

K řízení přístupu k dokumentům bude využito také technologie „Marking set“. Ta umožňuje pomocí speciálního atributu řídit přístup k dokumentu na základě jeho hodnoty, nikoliv však konkrétní oprávnění. Každá hodnota definuje role (skupiny), které mají přístup k dokumentu. Konkrétní typ oprávnění se vyhodnocuje až na základě listu přístupových oprávnění dokumentu. Tato funkcionalita dále určuje, která role má oprávnění dokument vložit

Řízení oprávnění k dokumentům bude dále možné spravovat na základě složkové struktury. Každý uzel má právě jednoho rodiče a každý rodič má 1-n potomků. Listy stromů již potomky nemají. Na každém uzlu jsou jasně definovány role (skupiny) s patřičným oprávněním. Dokument může být následně zařazen do kteréhokoliv adresáře (maximálně vždy právě do jednoho) ze kterého zdědí oprávnění uvedených na všech nadřazených složkách včetně kořenové.

2.2.1.3. Audit

Auditní log lze nastavit detailně na jednotlivé třídy, dokonce na vlastnosti. Zároveň jsou logovány detaily umožňující identifikaci, kdo daný prostředek použil nebo použít chtěl, výsledek, samozřejmě datum a čas a vlastní požadavek identifikované operace. Popřípadě může být nastaveno logování mazání záznamů nebo neoprávněné operace, především s ohledem na šetrné využití zdrojů.

Služby a workflow mají své vlastní auditní logy, které mohou sledovat jednotlivé operace.

Auditní logy umožňují napojení na systém dohledu (SIEM). Vybrané auditní logy lze poslat i pomocí: emailu, http, rsyslog, snmp. Integraci s existujícími systémy pro monitorování zabezpečení je možné využít formáty rsyslog: CEF, LEEF, JSON, XML.

V případě výpadku jakékoliv bezpečnostní komponenty v systému není narušena dostupnost služeb. Součástí řešení jsou nástroje pro monitorování jednotlivých komponent a služeb, včetně modulu pro výstrahu správců.

2.2.1.4. Technické požadavky

Webové aplikace jsou optimalizované pro aktuální verze webových prohlížečů: Chrome, Edge, Opera, Firefox i Internet Explorer (se zpětnou kompatibilitou nejméně o jednu verzi oproti aktuální v době nasazení systému). Lze očekávat, že v dohledné budoucnosti nebude výrobcem podporován Internet Explorer a původní verze Edge. Lze použít všechny prohlížeče, které splňují bezpečnostní kritéria v předepsané konfiguraci, zejména bez schválených pluginů. Výkon některých částí aplikací se může pro různé prohlížeče lišit.

Veškerá komunikace mezi těmito částmi řešení je pomocí standardních komunikačních rozhraní (např. WS-SOAP, LDAP a CMIS, podporovány jsou protokoly HTTPS, WEBDAV, NFS a CIFS). Obdobně budou pro komunikaci s externími systémy, ze kterých budou data (el. dokumenty) do DA MO zasílána, implementována standardní rozhraní WS-SOAP a WS-REST.

Navržené řešení disponuje nástroji pro tvorbu, údržbu a správu workflow, umožňující posílat e-mailové notifikace pro nastavené situace (např. příjem nevalidního dokumentu) a obsahující workflow systém a nástroje pro definování, spouštění, reporting a správu workflow, umožňující ad-hoc definování úloh koncovým uživatelem v průběhu zpracování konkrétní instance workflow, podporující přidělování úkolů na konkrétního uživatele nebo na celou roli v rámci řešení konkrétních úkolů. Součástí řešení je administrační prostředí pro návrh a správu workflow realizované formou webové aplikace.

Všechny části řešení (Brána, Archiv, Badatelský portál, GUI atd.) podporují práci s požadovanými formáty PDF, PDF/A; MS Office – DOC, DOCX, PPT, PPTX, XLS, XLSX, RTF; JPG, GIF,TIF/TIFF, PNG, XML.

Systém je možné provozovat jak na fyzickém hardware, tak i s využitím virtualizačního prostředí.

Služby a webové aplikace využijí existující instalaci aplikačního serveru WebSphere, kde bude vytvořen nový profil a do něj instalovány potřebné služby DA MO. Služby FileNetu mají ve Websphere ESA vlastní oddělený profil a tuto instalaci využije i DA MO. Do FileNetu bude přidán nový Object Store pro ukládání aplikačních dat a dokumentů. Pro vytvoření nového Object Store bude založena příslušná databáze.

Lze také vytvářet politiky ukládání, které umožní automatický výběr a změnu fyzického úložiště dle definovatelných kritérií v průběhu životního cyklu dokumentu. Prostřednictvím rozšíření stávajícího úložiště dojde k provedení upgrade tohoto úložiště a zvětšení celkové kapacity úložiště. Je zcela zřejmé, že existuje životnost každého zařízení, nicméně Poskytovatel možností rozšířením stávajícího úložiště poskytl doložení, že provozované úložiště je možné rozšiřovat. Detailní popis o další rozšíření je možné zajistit na webových stránkách výrobce nebo tyto doloží Poskytovatel na vyžádání.

Toto úložiště je chráněno několika stupňovou ochranou minimalizující ztrátu dat. Na diskových úložištích jsou použity svazky RAID, které zajišťují v případě výpadku disku nebo několika disků, dostupnost dat. Zároveň je zajištěna vysoká dostupnost prostřednictvím více přístupových cest na toto úložiště. Samozřejmostí tohoto pole je výměna disků (použití technologie hot-swap = vytažení disku z běžícího systému, bez ztráty dat a ohrožení jejich integrity) a jejich nahrazení za chodu, zcela bez výpadku. Uvedené diskové pole je v porovnání s odpovídajícími v dané kategorii, vybaveno lepšími možnosti rozšíření optických rozhraní (HBA), jednodušší licencování rozšiřujících funkcionalit a akceleraci ukládání za pomocí SSD disků s možností využití metro/global replikací, apod. Vlastní diskové pole zároveň disponuje funkcionalitou postupného upgrade microcode jednotlivých disků, jež zajistí bezvýpadkový provoz. S využitím přepínaných logických jednotek a logických replikací, je možné využít jednoduché a cenově efektivní řešení. Z výše uvedených důvodů Poskytovatel považuje uvedená a Nabyvatelem provozovaná, disková pole, v kombinaci s technologií FileNet za ekonomicky výhodná, přičemž poskytují z pohledu rozšíření a provozu v delším časovém horizontu možnost úspory. Použití vlastního diskového pole není limitujícím prvkem a dává možnost do budoucna připojovat disková pole i jiných výrobců těchto technologií.

2.2.2. Brána

V rámci Brány jsou implementovány Integrační služby, které poskytují rozhraní pro vstup dokumentů ze zdrojových systémů. Součástí Brány je i tzv. Karanténa (poskytovaná Nabyvatelem),

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.

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

Veškerá komunikace mezi těmito částmi řešení je pomocí standardních komunikačních rozhraní (např. WS-SOAP, LDAP a CMIS). Část Archiv a Brána jsou vytvořeny s pomocí produktu IBM FileNet P8, který kromě funkcionalit pro archiv dokumentů poskytuje i nástroje pro tvorbu a správu workflow. Jako součást modelovaných procesů je možné využít širokou škálu integračních prvků, uživatelských a systémových úkolů, přidělování úkolů konkrétním uživatelům nebo rolím, atd. V případě uživatelských úkolů je možné zastupování a přeřazování úkolů, eskalace úkolů na nadřízenou roli nebo také odesílání emailových notifikací

Pro minimalizaci ztráty dat v případě nepředvídaných událostí budou zdrojové systémy, které odesílají data do archivu, tato data držet ještě 24 hodin po odeslání do archivu, resp. na rozhraní Brána.

V rámci Websphere bude na stávající instalaci Brány ESA (která aktuálně používá dva profily) vytvořen další profil pro DA, který zabezpečí služby Brány DA. Služby pro FileNet budou i pro Bránu DA pokryty bez rizika stávajícím profilem Brány ESA.

FileNet - stávající instalace Brány ESA používá dva object stores pro workflow, dokumenty s definicí dokumentových tříd a Sweep Jobs. Na Bráně DA bude vytvořen jeden nový object store pro workflow Brány DA i nová databáze v rámci stávající instance pro dočasné úložiště Brány DA.

Tímto návrhem řešení Brány DA se optimálním způsobem pokračuje v logice, koncepci a technologii stávajícího řešení ESA. Přidáním profilu do Websphere a object store do Filenetu se snižuje riziko chybovosti, které by mohlo nastat při použití pouze stávajících komponent ESA. Takovéto rozšíření navíc nepřináší potřebu doplnění nebo modifikace stávajících licencí Websphere a Filenet použitých pro ESA.

2.2.2.1. Služby

- Služba FileNet
  - FileNet Content engine pro ukládání obsahu.
- Služba FileNet BPM engine
  - který řídí a orchestruje ostatní služby a požadavky. Například proces poskytnutí informací z archivu a další.
- Služba pro vstup SIP balíčků
  - Služba pro vstup SIP balíčků dle NSESSS, dle standardu METS. Pokud jsou součástí obsahu elektronicky podpesané PDF dokumenty ve formátu PAdES, bude v rámci validací provedeno ověření el. podpisu. Po přijetí příchozího dokumentu se uloží do dočasného úložiště. Předáním na další služby je provedena 4 stupňová validace, součástí, které je i karanténa na škodlivý kód a malware.
- Služba pro vstup samostatných dokumentů

  - Služba pro vstup samostatných dokumentů i archivních balíčků SIP v případě potřeby doplní metadata do třídy dokumentů ve Filenetu. Pro účely skenování souborů se používá samostatné rozhraní Ethernet.

- Služba ruční vložení
  - Ruční vložení přes webové rozhraní využije služby pro vstup samostatných dokumentů i archivních balíčků SIP v případě potřeby doplní metadata do třídy dokumentů ve Filenetu. Takto vložený dokument prochází stejným procesem, jako vstupní dokument zaslaný jiným systémem prostřednictvím rozhraní.
- Služba rozhraní pro pracovníky archivu
  - Rozhraní pro pracovníky archivu, kteří rozhodují o přijetí dokumentů do archivu, které neprošly kontrolou. Autentizace a autorizace je napojena na LDAP server Archivu.
- Služba scanner filesystému
  - Scanner filesystému bude sledovat složku na filesystému, odkud převezme SIP balíček, nebo samostatný obsah a metadata.
- Služba pro základní kontrolu integrity
  - Služba pro základní kontrolu integrity dokumentu a metadat. Dokument, který nevyhoví v rámci kontrol definovaným kritériím, je zařazen do seznamu problematických dokumentů. Další postup je na rozhodnutí archiváře.
- Služba pro předání obsahu do karantény.
  - Zajistí rozbalení obsahu SIP balíčku a předání do karantény, kde jsou všechny příchozí dokumenty podrobeny důkladné vícestupňové analýze. Asynchronně vyhodnotí výsledek kontroly v karanténě.
- Služba pro komunikaci s Badatelským portálem
  - Služba předá Badatelskému portálu kopii archiválie (případně transformovanou) s metadaty. Data zpřístupněných kopií archiválií krátkodobě poskytovaných plných kopií a důkazního materiálu v Badatelském portálu jsou striktně oddělena od originálních archiválií.
  - Zpracovává žádosti o založení a schválení požadavku na poskytnutí informací z Archivu.
- Archiváři jsou v rozsahu jeho oprávnění k dispozici statistické informace o archivu a jeho využití, např.:
  - celkový objem archiválií v archivu,
  - objem archiválií daného typu,
  - přírůstek archiválií za dané období,
  - zbývající dostupný prostor v archivu
  - počty archiválií, u kterých se vyřizuje žádost o zpřístupnění

Kompletní seznam všech statistik bude předmětem analýzy.

2.2.2.2. Karanténa

Pro řešení DA bude použita stejná Karanténa, která je již provozována v ESA. Její kapacita je dostačující pro pokrytí běžného provozu ESA MO a plánovaného běžného provozu DA MO společně.

Vstup dokumentů do karantény je řešený pomocí několika monitorovaných složek sdílených pomocí protokolu Samba (sdílení souborů ve Windows). Po přijetí z Brány a uložení příchozího/každého dokumentu do dočasného úložiště, je provedena 5 stupňová validace, součástí, které je i karanténa na škodlivý kód a malware. Karanténa jej odtud převezme a po kontrole je vloží do výstupních složek s příznakem „Validní“ nebo „Chybové“ – podle výsledku testů. Soubor bude mít stejný název jako na vstupu. Systém DA MO automaticky vygeneruje název souboru a přiřadí jednoznačný prefix, podle kterého na výstupu rozpozná dokument příslušející DA MO. V rámci implementační analýzy budou doporučeny a následně realizovány příslušné úpravy stávající konfigurace Karantény.

Analýza všech souborů se provádí v prostorách Nabyvatele. Žádné údaje Nabyvatele jako jsou soubory nebo jiné objekty nejsou odesílány do cloudu pro provádění dynamické analýzy útoku.

V rámci nabídky navrhujeme tyto kontroly v rámci Karantény (upřesnění bude součástí implementační analýzy):

- Vhodnost datového formátu – Do Archivu jsou přijímány pouze soubory definovaných datových typů. Z pohledu dlouhodobého uchování 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/pečeť, elektronické časové razítko), jsou tyto prvky validovány. Při kontrole platnosti elektronických podpisů a časových razítek je ověřena platnost kvalifikovaných certifikátů vydaných kvalifikovanými poskytovateli služeb vytvářejících důvěru, které poskytují služby v rámci Evropské unie. Typicky se jedná o formáty PDF;
- Integrita dokumentů – Stejně jako platnost elektronického podpisu/značky je kontrolována i integrita samotného dokumentu, zda od podpisu dokumentu nedošlo k jeho modifikaci;
- Přítomnost škodlivého kódu – Dokument je testován na přítomnost škodlivého kódu, který by mohl ohrozit bezpečnost Archivu, ale především ohrozit koncové příjemce dokumentu. Řešení umožňuje automatizované vyřazení dokumentů ze zpracování pokud představují jakoukoliv hrozbu pro celé řešení nebo jeho část.
    - Dokumenty vyřazené ze zpracování jsou bezpečně uloženy mimo ostatní dokumenty a je zamezeno možnosti ohrožení systému nebo jeho části.

2.2.3. Archiv

Část Archiv DA, je stejně jako část Brána DA, navržen jako rozšíření ESA.

V rámci Websphere má stávající Archiv ESA vytvořeny dva profily – jeden slouží pro komponenty s FileNetu a druhý pro služby Archivu ESA. Pro Archiv DA bude ve Filenetu vytvořen další profil pro služby Archivu DA. Na služby pro FileNet bude použitý stávající profil Archivu ESA.

Filenet - Archiv ESA má nastaveny 2 object stores, které slouží pro workflow, dokumenty s definicí dokumentových tříd a sweep joby). Pro Archiv DA bude vytvořen jeden nový object store, sloužící pro úložiště Archivu a nová databáze v rámci stávající instance.

Tímto návrhem řešení Archivu DA se optimálním způsobem pokračuje v logice, koncepci a technologii stávajícího řešení ESA. Přidáním profilu do Websphere a object store do Filenetu se snižuje riziko chybovosti, které by mohlo nastat při použití pouze stávajících komponent ESA. Takovéto rozšíření navíc nepřináší potřebu doplnění nebo modifikace stávajících licencí Websphere a Filenet použitých pro ESA.

Archiv je koncipován jako autonomní a na ostatních částech 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. V případě, že dokument neobsahuje potřebné informace (metadata) je na pracovníkovi Archivu, aby tyto informace doplnil, nebo byl dokument odmítnut jako neúplný.

Samotný Archiv dokumentů vyžaduje pro svou plnou funkčnost přístup k akreditované TSA, která je integrována pomocí komponenty Archivní služby a slouží k ověřování a vytváření kvalifikovaných časových razítek. (CRL)

Archiv má svůj LDAP server vyhrazený pouze pro Archiváře a Administrátory Archivu. Uživatelé jsou spravováni odděleně, včetně skupin a rolí. LDAP poskytuje autorizaci a autentizaci pro archiváře pro schvalování dokumentů, u kterých neproběhla validace atributů nebo kontrola v karanténě.

Archiv je založen na instanci FileNet Content engine, který zajišťuje ukládání archiválií, spravuje přístupová práva.

Zajišťuje klíčovou funkci řešení - udržuje dlouhodobou platnost důvěryhodných elektronických prvků a garantované dlouhodobé uložení dat. Řešení je schopno důvěryhodně ukládat elektronické archiválie po neomezenou dobu (z pohledu aktuálních technologií, legislativy). Zajišťuje tedy trvalé, neměnné a důvěryhodné uložení archivovaných elektronických archiválií. Dlouhodobá platnost elektronických archiválií je udržována pomocí přerazítkování archivních balíčků. Řešení umožňuje řízení procesu tvorby balíčků dle různých archivačních politik a umožňuje nastavit archivační politiky s ohledem na optimalizaci procesu razítkování.

FileNet BPM engine má na starosti přerazítkování pro dlouhodobé důvěryhodné ověřování archiválií a životní cykly (procesy spojené s vyřazováním archiválií z archivu procesem výběrové skartace, skartaci nebo trvalou archivaci). Dlouhodobá platnost elektronických archiválií je udržována pomocí přerazítkování archivních balíčků. Řídí proces tvorby balíčků dle různých archivačních politik a umožňuje nastavit archivační politiky s ohledem na optimalizaci procesu razítkování. Této funkce je dosaženo pravidelným automatickým vytvářením archivních balíčků z nových dokumentů a z dokumentů, jimž se blíží termín pro přerazítkování. Elektronické archiválie je možné balíčkovat nezávisle na jejich typu, významu, různých přístupových právech a bez jejich vzájemného vztahu. Řešení tedy umožňuje tvorbu archivních balíčků zajišťujících dlouhodobou platnost celé sady elektronických archiválií. Skartace dokumentu neovlivní možnost ověřit ostatní dokumenty ve stejném balíčku.

Dále FileNet BPM engine vytváří kopie pro Badatelský portál. Předává kopie na Bránu DA MO, kde probíhá anonymizace kopií pro badatele. Řídí procesy spojené s vyřazováním archiválií z archivu. V případě, že archiválie prošla procesem vyřazení a byla určena k odstranění, systém umožní mazání jednotlivých archiválií z balíčku bez narušení možnosti prokázat důvěryhodnost ostatních archiválií z balíčku. Je také vedena evidence v rámci, které jsou vedeny informace o dokumentech, u nichž došlo k vyřazení z archivu a informace o výběrových skartacích.

Uložené elektronické archiválie jsou periodicky kontrolovány na platnosti certifikátů časových razítek a provádí se automatická obnova časových razítek. 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. Řešení ověřuje při kontrole platnosti elektronických podpisů a časových razítek platnost kvalifikovaných certifikátů vydaných kvalifikovanými poskytovateli služeb vytvářejících důvěru, které poskytují služby v rámci Evropské unie.
Ukládány jsou veškeré informace nutné pro ověření/prokázání právní platnosti archiválií, a to i po vypršení platnosti certifikátů, na kterých jsou založeny elektronické podpisy. Pakliže je požadován elektronický originál elektronické archiválie jako důkazní materiál, pak je poskytován k jednotlivým elektronickým archiváliím bez ohledu na ostatní dokumenty v balíčku, bez jejich kompromitace a bez ohledu zda v čase poskytnutí důkazního materiálu existují. Toho je dosaženo tak, že bude podepsán balíček obsahující kontrolní součty jednotlivých dokumentů v tomto balíčku. Jako důkaz bude poskytnut tento soubor, takže nebudou kompromitovány ostatní dokumenty.

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 úložištěm poskytujícím souborový systém NFS a CIFS. Archivní balíčky a jejich důvěryhodnost jsou nezávislé na vlastnostech archivního úložiště.

K jednotlivým dokumentům v Archivu jsou ukládána 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, minimálně v rozsahu typů text, celé číslo, číslo s desetinnou čárkou, logická hodnota a datum včetně vícehodnotových metadat. Množiny evidovaných metadat je možné konfigurovat zvlášť pro různé typy archiválií. Konfiguraci metadat je možné měnit v průběhu života systému.

2.2.3.1. Práce archiváře

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 funkcím pomocí rozhraní na bráně a přímým přístupem do webového klienta v rámci prostředí Archivu. Vybraným uživatelům – archivářům – je umožněn přístup přímo do části Archivu prostřednictvím uživatelského rozhraní Archivu. Logická vrstva Archivu poskytuje služby DMS pro práci s archiváliemi a umožňuje editaci metadat prostřednictvím formuláře systému. Tyto metadata a případně další doplněná technická metadata jsou určená pro vyhledávání a následné zobrazení.

U vybraných typů dokumentů je možné nastavit, aby si jej uživatel nemohl přímo stáhnout na PC, ale aby byl pouze zobrazen v prostředí prohlížeče internetu.

Zobrazení vybraných formátů dokumentů v podobě náhledu je možné v prohlížeči Daeja ViewONE (Office View – součást dodávky licencí systému DA MO), který je součástí webové aplikace, bez nutnosti stažení celého dokumentu na pracovní stanici uživatele, a to v těchto formátech: PDF, PDF/A, Office dokumenty (DOC, DOCX, XLS, XLSX, PPT, PPTX, ODT, ODS, ODP), RTF, Rastrové obrázky (TIFF včetně vícestránkového TIFF, JPEG, BMP, PNG, GIF, XML), HTML soubory. Systém obsahuje prohlížeč dokumentů, který umožňuje přidávat k zobrazenému dokumentu popisky, poznámky, grafické symboly (čáry, šipky, geometrické obrazce) – tzv. anotace a anotace lze uložit bez modifikace zobrazeného dokumentu. Prohlížeč také umožňuje stránkovat, zvětšovat/zmenšovat, otáčet a tisknout zobrazené dokumenty včetně jejich anotací.

Archiváři jsou v rozsahu jeho oprávnění k dispozici statistické informace o archivu a jeho využití, např.:

- celkový objem archiválií v archivu,
- objem archiválií daného typu,
- přírůstek archiválií za dané období,

Tyto informace jsou dostupné v podobě standardizovaných reportů. Archivář si ale může vytvořit sestavu podle vlastních potřeb.

V rámci práce archiváře může oprávněný uživatel editovat vybraná metadata archiválie. Je také možné archiválie vyhledávat, a to pomocí metadatových položek, fulltextově, nebo kombinací obou způsobů. Podoba výsledků vyhledávání je uživatelsky konfigurovatelná (ve smyslu zobrazených dat ve výsledkové sadě - např. řazení, množina zobrazených metadat). Výsledky vyhledávání jsou omezeny přístupovými právy uživatele a lze je exportovat ve vhodném formátu. K vybrané položce výsledku vyhledávání je možné si zobrazit detailní informace.

Archiváři s příslušnou rolí je umožněno také garantované smazání, tedy takové odstranění dat, že archiválii ani žádnou z jejich částí není možné obnovit.

2.2.3.2. Anonymizace

Součástí DA MO je SW pro anonymizaci archiválií. Tento SW zajistí převod dokumentu na obrazovou podobu (v případě textových formátů (např. pdf) i odstranění případné textové vrstvy) a následnou co nejefektivnější anonymizaci v okně prohlížeče vč. možnosti automatizace. Tím bude zajištěno, že archivář nemusí daný dokument stahovat do PC a že dojde k trvalé anonymizaci dat (nebude se jednat o oddělitelnou vrstvu). Webová aplikace pro anonymizaci je na bráně. Kopii archiválie je možné anonymizovat. Jednu anonymizovanou verzi lze poskytnout více badatelům nebo je možné vytvořit různé anonymizované verze pro různé badatele. Archivář rozhoduje, kterou verzi kterému poskytne badateli.

Pro anonymizaci bude využita komponenta Filenetu – DejaViewPRO (Redakce), která je s FileNetem webovým klientem integrovaná.

2.2.3.3. Monitoring, audit

Systém obsahuje monitoring operací zachycující veškeré operace s archiváliı:

- Ukládání záznamů o veškerých operacích s archiváliı, které byly platformou provedeny nebo které byly požadovány a z důvodu nedostatečných přístupových oprávnění nebyly provedeny.
- Rozhraní pro zobrazení záznamů o operacích s konkrétní archiváliı.
- Rozhraní pro vyhledávání v těchto záznamech napříč všemi archiváliemi, vytváření sestav, reporting a varovné mechanismy upozorňující na nestandardní nebo podezřelé chování.

Je možné definovat, které operace mají být takto a jak detailní má audit být.

2.2.3.4. Služby

V Archivu jsou k dispozici tyto služby:

- FileNet Content Engine

  pro ukládání archiválií a metadat. Je napojen na LDAP server archivu.
- FileNet BPM

FileNet BPM Engine pro řízení přerazítkování a životního cyklu dokumentů. Orchestruje ostatní služby a požadavky brány.

- LDAP server Archivu

  Udržuje odděleně seznam uživatelů archivu, jejich role.

- Služba pro vytváření náhledů

  Zajistí vytvoření rastrové verzované kopie dokumentu včetně vodoznaku pro použití v Badatelském portálu. Služba poběží na pozadí a bude spouštěna pomocí Workflow nebo Sweep Jobu. Pro převod dokumentů budou využity vhodné knihovny. Konkrétní typy budou stanoveny v implementační analýze. Bude zajištěn převod rastrových dokumentů, MS Office dokumentů, převod PDF na raster. Uložení anonymizované verze kopie bude ošetřeno v rámci workflow, kde uživatel anonymizuje dokument pomocí komponenty DeajaView PRO (Redakce -součást dodávky licencí po systém DA MO).

- Služba vytváření archivačních balíčků a přerazítkování

  Služba vytváří archivní balíčky ve formátu XAdES LTA s použitím kvalifikovaného elektronického podpisu a kvalifikovaného časového razítka dle normy ETSI TS 101 903 V1.4.2. Na straně FileNet je nastavení úloh pro výběr dokumentů, generace hash, volání SOAP služby, dále sledování platnosti a zajištění včasného provolání přerazítkování.
  Přerazítkování je plně automatický proces, který vyhledá archivní balíčky a dokumenty, u kterých končí platnost časového razítka (výběr prostřednictvím parametrů počet dnů před vypršením, které je nastavitelné administrátorem archivu). Proces provede vytvoření nového balíčku obsahujícího stávající balíčky a nové dokumenty. Pokud bude skartována některá archiválie z balíčku, neovlivní to možnost ověřit ostatní archiválie. Archivní balíčky jsou trvale uloženy jako součást archivních dat a lze z nich zjistit a vytvořit důkazní materiál s informacemi, kdy a jaké dokumenty byly přerazítkovány bez narušení možnosti prokázat důvěryhodnost ostatních archiválií z balíčku.

- Služba pro sestavení důkazního materiálu.

  Vytvoří DIP balíček, který obsahuje kopie vybraných dokumentů a metadat včetně důkazního materiálu, obsahující potřebné elektronické informace pro dokázání důvěryhodnosti dokumentu. Formát DIP je dle standardu METS a je v souladu s národním standardem pro elektronické systémy spisové služby NSESSS. Poskytoval očekává, že Nabyvatel poskytne takové informace, které jsou nutné pro vytvoření DIP balíčku dle standardu METS.

- Služba ověření dokumentu

  Služba ověřuje 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 a ZFO (formát zpráv datových schránek). Ověření platnosti elektronického podpisu dokumentu je v souladu se standardem ETSI EN 319 102-1 V1.1.1. Pro úplnost uvádíme další implementované standardy pro jednotlivé formáty (XAdES, PAdES, CAdES, ASiC) ETSI EN 319 132, ETSI EN 319 122, ETSI EN 319 142, ETSI EN 319 162. Dále potom standard ETSI TS 119 612 Trusted Lists.

- Služba statistiky

Služba pro výpočet statistiky archivu. Sleduje celkový objem archiválií, objem podle jednotlivých typů archiválií, přírůstek za dané období. Archivář si může v rámci svých oprávnění definovat vlastní sestavu, na základě které se vygeneruje report.

- Webový klient Archivu

  Webový klient pro přímý přístup do archivu. Přístupný pouze pro uživatele archivu.

2.2.4. Badatelský portál

Badatelský portál postavený na standardním produktu badatelny iQ Discovery je součástí řešení DA MO. Je poskytovaný jako portálové řešení pro specializované archivy a splňuje všechny požadavky dané zadávací dokumentací. Portál obsahuje veřejnou i interní část a je oddělen od ostatních komponent Firewallem s jasně definovanými prostupy a prostřednictvím WAF, zajišťující ochranu před útoky typu SQL Injection, Cross-site Scripting, Cross-site Request Forgery a dalšími. Do veřejné části je umožněn přístup laické i odborné veřejnosti, a to buď anonymní nebo autorizované (na základě registrace, případně ověření přes MojeID nebo NIA). Interní část je určena administrátorům Badatelského portálu a expertním pracovníkům archivu. Další vlastností je funkce pro ztotožněné uživatele k prohlížení neveřejných částí archivního spisu na základě schválené žádosti. Přístup může být umožněn i anonymním uživatelům ale jen k velmi omezené množině informací. Po důvěryhodném ztotožnění uživatele je možnost podání oprávněné žádosti pro zpřístupnění neveřejné části spisu. Oprávněná žádost obsahuje prostor pro definici pozice žádajícího, důvod, účel a další Nabyvatelem definované atributy nutné k posouzení žádosti. Komunikace a žádosti o archiválie jsou odeslány z Portálu prostřednictvím požadavků na rozhraní Brány, tak aby nemohlo dojít k narušení bezpečnosti vlastního Archivu. Tyto požadavky jsou po odbavení na Bráně zpracovány v rámci workflow a následně je zpět na Portál odeslán požadovaný dokument, nebo poskytnuta jiná informace, opět komponentou Brána. Dynamický formulář žádosti umožnuje vyžádání odlišné sady atributů nebo podkladových dokumentů na základě vložených uživatelských dat (např. důvodu žádosti nebo pozice žádajícího). Systém obsahuje komplexní statistiky a webovou prezentaci archivu.

Badatelský 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 a činnosti uživatele s danou archiválií.
  - 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. Aktivita všech typů uživatelů (registrovaní uživatelé, ztotožnění uživatelé a administrátoři badatelny) nad archiváliemi je detailně logována tak, aby bylo zpětně zřejmé, kdo a jakým způsobem s dokumenty pracoval.

Dále bude Badatelský portál obsahovat vícejazyčnou prezentaci VHA a volné nahlížení do databáze VHA v rozsahu daném zadávací dokumentací. Cizojazyčné texty pro vícejazyčnou prezentaci budou poskytnuty Nabyvatelem během implementační analýzy.

Badatelský portál podporuje funkce:

- 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).

Licence, které jsou poskytnuty na Badatelský portál, nejsou omezeny počtem uživatelů nebo počtem zpracovaných dokumentů.

2.2.4.1. Interní část

V rámci tohoto administrátorského rozhraní můžou dále oprávněný uživatelé spravovat uživatelské účty, udělovat ad-hoc přístupové oprávnění a spravovat žádosti badatelů o nahlížení.

Administrátoři mají k dispozici přehled dávek k zpřístupnění a žádostí o nahlížení do spisu:

- Seznam dávek k zpřístupnění.
- Detail dávky k zpřístupnění.
- Seznam žádostí o nahlížení spisů z archivu.
- V detailu Žádosti je viditelný účel žádosti, titul na základě, kterého badatel žádá a připojené podkladové dokumenty.

Dále mají administrátoři k dispozici doplňkové funkcionality:

- Statistiky užívání portálů (v členění na archiválie a uživatele).
- Seznam a správa badatelů (schvalování uživatelských účtů, přidělování přístupových údajů).

2.2.4.2. Veřejná část

Veřejná část Badatelského portálu obsahuje úvodní stránku pro širokou veřejnost Integrovanou součástí je vícejazyčná webová prezentace Vojenského ústředního archivu, koncipována tak, aby přirozeným způsobem podporovala uživatelský komfort z používání samotného Badatelského portálu. Badatelský portál umožňuje vložení tzv. portletů za účelem rozšíření funkčnosti a zpravidla obsahuje textové části (případně doplněny o grafické prvky) pro lepší navigaci uživatele.

Portlety umožňují vzájemné provázání a sdílení vybraných dat. Konkrétní portlety nejsou součástí této nabídky, portál ale jejich realizaci, konfiguraci a customizaci plně podporuje. Dominantní funkcionalitou portálu je možnost přihlášení, resp. registrace uživatele, a to v rozlišení na běžnou a důvěryhodnou registraci, jejíž výsledkem je ztotožněný uživatel (např. prostřednictvím NIA). Přihlášený uživatel vidí historii svého bádání, statistiky bádání, žádost o zpřístupnění archiválie nebo modul vyhledávání v zpřístupněných archiváliích. V databázové vrstvě jsou uložení digitální kopie (anonymizované interpretace) archiválií opatřeny vodoznakem spolu se souvisejícími metadaty. Bezpečnostní vrstva Badatelského portálu umožňuje pro archiváře řídit přístup k archiváliím pro tyto vrstvy uživatelů:

- Anonymní uživatel
- Registrovaný uživatel
- Ztotožněný uživatel

Toto řízení přístupu probíhá na úrovni samotné archiválie a dále na úrovni konkrétních metadat. Badatelský portál pro jednotlivá bádání a činnosti ztotožněného uživatele s vyžádanou poskytnutou kopií archiválie předává informace do Badatelského listu, který je veden v Archivu. Pro přihlášené uživatele bude v rámci prostředí Badatelského portálu dostupné i diskuzní fórum.

2.3. Migrace

Předmětem dodávky je jednorázová migrace dat ze stávajícího DMS systému Documentum. Bude vytvořen jednorázový migrační nástroj pro převod dat vyexportovaných z DMS Documentum a následně bude proveden import do systému DA MO. Celkový počet archiválií ke konverzi je cca 2 miliony.

Součástí plnění je:

- analýza požadovaných vlastností, příslušných norem a standardů, struktury zdrojových dat, přesná definice zadání a její odsouhlasení,
- programování aplikace,
- testování, ladění,
- validace vzorku migrovaných dat, spuštění migrace v místě Nabyvatele, zaškolení obsluhy,
- podpora Nabyvatele v průběhu migrace (telefon, e-mail, omezený rozsah),
- tvorba dokumentace.

Výchozí stav.

Předpokladem je, že Nabyvatel zajistí export dat ve formě .zip souborů v definované složce v rámci lokálně dostupného filesystému. Pro každou verzi každého dokumentu zde existuje jeden .zip balíček, jehož obsahem je samotný dokument v příslušné jeho verzi, a dále .xml dokument obsahující metadata, vztahující se k tomuto dokumentu. Celkový počet dokumentů ke konverzi je cca 2 miliony.

Předpokládaný cílový stav

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

Konverzní nástroj

Pro převod původních exportních .zip balíčků na výstupní SIP balíčky určené k importu do systému DA MO bude vytvořena jednoúčelová konzolová konverzní aplikace. Parametry pro korektní běh této aplikace (vstupní/výstupní adresář a podobně) budou zadány v textovém konfiguračním souboru. Konverzní nástroj bude vytvářet podrobné logy, které budou obsahovat informace o jednotlivých konvertovaných dokumentech a výsledcích konverze. Pokud se vyskytne v průběhu zpracování některého dokumentu chyba, bude tento dokument zapsán do samostatného seznamu dokumentů, které nebylo možno konvertovat. Konverzní nástroj si bude také evidovat informace o všech zpracovaných dokumentech, aby v případě přerušení jeho činnosti mohla konverze pokračovat od místa, kde předtím skončila.

Aby mohl být konverzní nástroj vytvořen a otestován, je ze strany Nabyvatele nezbytné poskytnout několik vzorků exportovaných dat, z kterých bude možné jednoznačně odvodit veškeré závislosti typů obsahů původních .zip balíčků a logiku tvorby jejich názvů.

Konverze a validace obsahu zvolených metadat

V průběhu konverze do SIP balíčků může být kontrolován obsah některých položek metadat. Typicky jde o kontrolu rozsahu číselných údajů a 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 dodaných Nabyvatelem a podobně. Pro potřeby takových kontrol se předpokládá, že Nabyvatel specifikuje, o které položky se má jednat, jakým způsobem mají být ověřovány, a jaké výchozí hodnoty mají být dosazeny v případě, že původní hodnota je mimo povolený rozsah, nebo není zadána.

V tomto návrhu se předpokládá, že podobným způsobem nebude kontrolováno více než pět jednotlivých položek metadat.

Provedení konverze

Vlastní konverze bude provedena na infrastruktuře Nabyvatele v místě plnění. Je třeba vzít v úvahu časovou náročnost při daném počtu dokumentů.

Postup provedení migrace:

- nastavení parametrů pro běh konverzního nástroje,
- provedení konverze na testovacím vzorku dat,
- kontrola a validace výsledků testu,
- odsouhlasení výsledků testu,
- spuštění konverzního nástroje do ostrého provozu a provedení vlastní konverze.

Informace o průběhu konverze jednotlivých dokumentů a počtu již zpracovaných dokumentů budou vypisovány do konzole. Po skončení konverze se běh konverzního nástroje automaticky zastaví a na konzoli bude vypsána informace o jejím ukončení a celkovém počtu zpracovaných dokumentů.

2.4. DMS skenovací linky

Implementace DMS skenovací linky bude implementováno jako samostatná část. Má vícevrstvou architekturu s přístupem přes tenkého klienta.

Bude zabezpečen 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 archiválie, vyhledávání podle metadat, jejich hromadné zadání a podpora workflow.

DMS pro skenovací linku je navrženo tak, aby bylo zamezeno ztrátě dat, má řízení přístupu uživatelů k digitalizovaným archiváliím, doplnění metadat včetně automatického vložení systémového data a jména pracovníka, přičemž tyto dvě metadata není možno uživatelsky změnit.

K systému DMS bude přistupovat max. 15 pojmenovaných uživatelů a kapacita úložiště je navržena na min. 10TB.

Počítače digitalizační linky jsou ve vlastní uzavřené síti a uživatelé budou ověřováni prostředky tohoto DMS a budou dostupné prostřednictvím ethernet rozhraní. 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 umožní:

- 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 nebude 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.

2.5. Bezpečnost prostředí archivu, bezpečnost dokumentů

Řešení pro zajištění a ochranu dat je pro digitální archiv klíčovou komponentou. Jako takové je třeba věnovat velké úsilí ochraně takových dat a zajištění konzistence a integrity.

Behaviorální analýza dokumentů probíhá ve specializovaném virtualizačním prostředí, které je postaveno na řešení předního výrobce těchto technologií, které je plně integrováno do celkového řešení, a bude v rámci dodávky řešení Nabyvateli integrováno. Celkové řešení a jeho komponenty jsou segmentovány do jednotlivých zón a jejich komunikace je striktně oddělena firewallem (firewall cluster), který umožňuje pokročilé kontroly (deep packet a statefull inspection, ACL, virtual patching, včetně kontrolu na aplikační vrstvě, apod..). Součástí řešení je zároveň použití stávajícího řešení SIEM napojení a pro sběr logů z komponent navrhovaného prostředí DA MO a ochranu dat prostřednictvím technologie Guardium. Tyto řešení je možné integrovat na další komponenty a zajistit tak komplexitu přehledu a detekci kybernetických hrozeb.

Poskytované řešení Poskytovatele naplňuje požadavky Nabyvatele z pohledu bezpečnosti a provozu takových systémů, dle příslušných předpisů požadovaných v rámci ZD. Stejně tak je zajištěno, že při výpadku těchto bezpečnostních komponent, nebude narušen provoz a dostupnost služeb vlastního řešení DA MO.

2.5.1. Vlastnosti karantény

Navrhované řešení je velice flexibilní v rámci konfigurace virtuálního stroje, kde je možné instalovat a konfigurovat různé aplikace, včetně specifických aplikací Nabyvatele případně aplikací třetích stran. Tato flexibilita umožňuje testovat dokumenty v prostředí, které je pokud možno, co nejpodobnější prostředí Nabyvatele. Standardně se používá tzv. gold image, která je používána jako standardní image pro instalaci pracovních stanic u Nabyvatele. To zaručuje maximální bezpečnost v případě, že dochází k pokusům o útok s využitím interních informací o infrastruktuře Nabyvatele, používaných aplikací, typických konfigurací aplikací apod. Pro prostředí VHA však budou použity již vestavěné a customizované images, které používá i ESA MO nad technologií, která naplňuje požadavky pro takové využití. Poskytovatel použije prostředky Nabyvatele, které jsou použity v současně provozovaném prostředí, které na ně Nabyvatel klade.

Vlastní testovací prostředí běží ve specifickém frameworku, v kterém je provozován vlastní sandbox. Tím je zajištěna vlastní bezpečnost a nemožnost kompromitace vlastního prostředí karantény, neboť pro odeslání do takto připraveného prostředí jsou připravené činnosti, které nemohou vlastní firmware zařízení kompromitovat ani detekovat, čímž se eliminuje možnost odhalení běhu ve vnitřním prostředí karantény.

Dokumenty k testování zasílá do karanténního řešení systém DA MO prostřednictvím sdílených složek. Pro testovaný dokument je v rámci řešení spuštěna instance virtuálního stroje, ve kterém probíhá behaviorální analýza testovaného dokumentu včetně případných souvisejících souborů a objektů. Karanténa provádí v rámci spuštění testovaného dokumentu ve virtuálním stroji analýzu bez nutnosti disponovat příslušnou virovou signaturou a to na základě chování testovaného dokumentu. Nicméně je vhodné provést komplexní hodnocení testovaného dokumentu, tj. včetně kontroly vůči známým signaturám. V takto dedikovaném a zcela izolovaném prostředí při testování dokumentu ve virtuálním stroji je zachyceno i případné polymorfní chování malware.

Zároveň je možné této flexibility využít i pro paralelní testování v méně zabezpečených virtuálních strojích (např. WinXP) tak, aby bylo co nejrychleji a nejefektivněji odhalit, že dochází k pokusům o útok na infrastrukturu Nabyvatele (jako jsou Zero-Day attacks nebo APT, podmíněné aktivace, apod.), které by se nemusely u standardně nakonfigurovaným virtuálním strojům projevit díky vyššímu zabezpečení těchto standardních virtuálních strojů. V rámci analýzy chování testovaných dokumentů ve virtuálním stroji jsou detekovány činnosti procesů a prováděny další simulace, které mohou nastat v reálném prostředí (posun času apod.)

Pro kontrolu obsahu souborů je v karanténě navrženo řešení, které podporuje požadované verze OS a aplikací při využití stávajícího řešení společnosti FireEye. (Windows 7, Windows 7 SP1, Windows XP, Windows XP SP2, Windows XP SP3, Mac OS X. Aplikace: MS Office 2003 a novější, Adobe Reader 9 a novější (v souladu se standardně vybavenými PC).

Standardně jsou podporovány přílohy, které jsou současně použity v rámci prostředků ESA MO. Tyto přílohy budou testovány v prostředí Nabyvatele a analýza se bude provádět v infrastruktuře Nabyvatele., tak jak vyžaduje ZD. Je možné zapnout i další pokročilé funkce, které mohou přinést další úroveň bezpečnosti a které mohou eliminovat některé další false/positive incidenty. Zároveň je možné poskytovat a provádět testování zcela bez přístupu na internet.

2.5.2. Detailní popis prostředí karanténa

Navržené řešení DA MO je propojené systémem prostřednictvím sdílených složek a po dokončení inspekce poskytuje výsledky testování. Systém DA MO na základě těchto výsledků a umístěné do

složky, rozhodne o dalším způsobu zpracování testovaných dokumentů. Testování dokumentů na přítomnost malware jsou prováděna před vlastní archivací dokumentu a vlastní systém tedy není nijak ohrožen. Na základě výsledků tohoto testování je teprve rozhodnuto, jestli daný dokument bude dál puštěn do standardního procesu archivace, případně bude vyřazen z tohoto procesu (nebude propuštěn do prostředí Archivu). V případě detekce závadného obsahu v testovaném dokumentu přesune systém karantény dokument do příslušné složky. Na základě tohoto bude daný dokument, případně soubor, vyřazen ze standardního zpracování v rámci systému DA MO. Takto detekované dokumenty jsou uloženy v prostoru, který nemůže nijak ohrozit další dokumenty ani vlastní prostředí karantény. Uživatel DA MO má možnost rozhodnout, jak s daným dokumentem bude naloženo. Toto testování, jak již bylo uvedeno, je prováděno na prostředcích Nabyvatele a soubory nebo objekty nejsou odesílány na cloudu pro dynamickou analýzu. V případě detekce malware systém poskytuje v rámci dodávaného řešení detailní reporting a podrobnou analýzu. Systém tento report generuje ke každému zpracovanému souboru.

Podrobné a komplexní výsledky testů behaviorální analýzy testovaných dokumentů jsou dostupné v prostředí konzole FireEye FX, která je dostupná přes šifrované web rozhraní z prohlížeče uživatele. Výsledky obsahují podrobný popis chování škodlivého software, včetně síťové komunikace, manipulace s registry, změny na úrovni souborového systému, manipulace s běžícími procesy apod.

Řešení na platformě FireEye FX poskytuje podrobnou analýzu o chování škodlivého software ve virtuálním testovacím prostředí včetně souvisejících ostatních objektů, jako jsou webové odkazy, IP adresy a identifikace dalších případných objektů / souborů (prostřednictvím hash id).

Zároveň podporuje současnou analýzu více souborů, které jsou součástí vícefázových a vícenásobných útoků. Typicky se jedná o situaci, kdy zaváděcí modul malware zavádí a spouští další moduly, které vyžaduje pro svou další činnost. Ideální pro detekci těchto typů útoků je umožnit malware komunikovat do Internetu po tzv. "dirty line". Pro zpracování a vyhodnocení vícefázových a vícenásobných útoků je možné zajistit paralelní zpracování. Níže jsou uvedeny základní typy souborů, které jsou vhodné pro takový typ zpracování:

a. Office dokumenty (DOC, DOCX, XLS, XLSX, PPT, PPTX, ODT, ODS, ODP), PDF dokumenty, Rastrové obrázky (TIFF včetně vícestránového TIFF, JPEG, BMP, PNG, GIF), HTML soubory
b. Kromě archivu, či jednotlivých souborů, lze vložit i „bundle“ souborů (např. spustitelné soubory, které mají být v dané adresářové struktuře.

Typicky je Karanténa zapojena tak, že komunikuje jednosměrně s update serverem přes web proxy, která dovoluje pouze tento druh komunikace (aktualizace), případně je možné provádět aktualizace vlastních reputačních a hash databází ručně. Případně je možné toto řešení napojit na vlastní management server, který Karanténě poskytuje zdroj „updates“. Navrhovaná řešení naplňují požadavky na přepnutí do režimu “offline”.

2.6. Bezpečnost dat a informací

Jako součást nabídky je integrace s technologií IBM Guardium, kterou Nabyvatel dovolil použít pro zajištění ochrany dat. A jako součást zajištění komplexní ochrany informací a dat uložených v systému DA MO. Tato přináší osvědčenou technologii, která je použita u mnoha poskytovatelů a zpracovatelů osobních a citlivých informací. Je samozřejmé, že data jsou provozována na databases prostředí plně podporovaných výrobcem, včetně posledních bezpečnostních aktualizací.

Právě z důvodu, že data jsou jedním z nejcennějších majetků firem, je potřeba tyto data chránit, ovšem tak, aby to neomezilo zaměstnance a funkčnost vlastních systémů. Celé řešení systému DA MO, je dle požadavku postaveno na logicky oddělených komponentách Brána, Archiv, Badatelna, které běží v různých bezpečnostních zónách a jsou oddělené prostřednictvím firewallu. Na serverech jsou agenti pro zajištění integrity a ochrany dat, stejně tak jsou příslušné operace monitorovány v reálném čase a to i privilegovaných uživatelů. Toto sledování může být založeno na mnoha atributech a hodnotách (ip adresy, uživatelského jména, tabulek, jména souborů, cesty, klíče v registru nebo sloupce či názvu tabulky). Všechny logy jsou vyhodnocovány v centrálním SIEM, tedy mimo prostředí, kde by s nimi mohl správce systémů, jakkoliv manipulovat.

Databázová data jsou chráněna prostřednictvím produktu IBM Guardium. Řešení IBM Security Guardium poskytuje centralizovaný monitoring, ochranu, automatickou analýzu dat a jejich kategorizaci, vysokou škálovatelnost, vytváření a uchovávání auditních záznamů a mnoho dalšího, a to vše v reálném čase jak nad strukturovanými, tak i nestrukturovanými daty. Řešení umožňuje posílat poplachy událostí přes syslog (stejně jako ostatní komponenty DA MO), email, snmp, ticketovací systém a i možnost vytvořit si vlastní poplach v programovacím jazyku java využívající API externích systémů.

Řešení umožňuje možnosti vybírat si z předdefinovaných reportů anebo vytvářet vlastní reporty, případně kopírovat stávající, a ty libovolně upravovat. Je možné měnit zobrazení z pohledu sloupců, nastavovat podmínky zobrazení, časové intervaly, řazení dat, apod.

Použité a již používané řešení Nabyvatelem, se skládá z modulů pro ochranu databází, souborů a vyhledávání zranitelností.

2.6.1. Modul ochrany databází

V databázích jsou uložené údaje o dokumentech, obchodních transakcích a další důležité firemní informace. Jedná se o jedny z nejcennějších informací ve firmě.

Řešení ochrany databází umožňuje zaznamenávat, co se děje v databázi bez toho, aby to výrazně ovlivnilo výkon databáze. Zaznamenané informace jsou poté v reálném čase analyzovány. Pokud dojde k podezřelé události, je zasláno upozornění na příslušná místa, případně dojde k blokaci akce, která může vést k úniku dat. Veškerou monitorovanou aktivitu a detekované podezřelé události si mohou pověření pracovníci prohlédnout v přehledné webové konzoli, kde mohou také nastavovat bezpečnostní politiky, tvořit reporty a třeba i definovat citlivá data, kterým má být věnována speciální pozornost během monitoringu.

Kontrola provozu je prováděna v reálném čase. IBM Guardium podporuje mnoho různých typů databází, je tedy možné na jednom místě monitorovat aktivitu nad všemi firemními databázemi. Konkrétně řešení je dáno implementací a bude použito v již existujícím prostředí. Výhodou tohoto přístupu je to, že Guardium dokáže odhalit i útoky a příkazy (případně je omezit nebo zakázat) od privilegovaných uživatelů, kteří se mohou do databáze připojit přímo a nepřistupují k ní přes aplikaci nebo přes síť. Záznamy o takových aktivitách nejsou uloženy na DB serverech a tudíž je znemožněn zásah takového privilegovaného uživatele do logu.

Dalšími funckionalitami v modulu ochrany databází je behaviorální analýza uživatelů (Risk Spotter), která dokáže upozornit na anomálie v chování jednotlivých uživatelů s využitím strojového učení. Je možné s ní detekovat nové uživatele, nové objekty v provozní komunikaci, změny chování jednotlivých uživatelů z pohledu pracovní doby. Funkcionalita Aktivní analýzy hrozeb je zase určená pro detekci kybernetických útoků na databáze (SQL injection a další typy útoků).

Funkcionalita Aktivní analytiky hrozeb je zase zaměřená na detekci kybernetických útoků typu SQL injection další (např ACL - Na základě ACL seznamů je možné automaticky vytvořit baseline pravidla v řešení IBM Guardium, apod.).

Používaná IBM Guardium appliance umí korelovat data z většiny komerčně používaných databází a big data řešení, například Oracle, IBM DB2 nebo Hadoop, tudíž bude vhodně použita pro nasazený systém DA MO.

Pro potřeby auditingu má uvedená technologie předpřipravenou širokou škálu reportů a umožňuje pokročilé vyhledávání v záznamech. Záznam a vyhodnocení auditních záznamů je možné napojit a integrovat se systémy SIEM, které jsou zcela mimo prostředí správců a které logy sbírá a ukládá. (syslog formát). Zároveň je může být napojen na LDAP nebo používat interní uživatele. Zároveň je možné pro testovací databáze nastavit maskovací či redakční politiky, které dokáží zneviditelnit nebo pozměnit obsah jednotlivých dat v rámci testování. Je možné definovat variabilní politiky, u kterých lze nastavit flexibilně pro jaké atributy komunikace bude maskování probíhat

2.6.2. Modul ochrany souborů, integrita

Modul ochrany souborů dokáže monitorovat a kontrolovat přístup k souborům v celém prostředí firmy, díky tomu získají Nabyvatel přehled o tom kdo, kam, kdy a jak přistupoval k souborům. Systém dokáže tyto informace využít a dát je do vzájemných souvislostí a upozorňovat na případné podezřelé aktivity uživatelů.

Veškeré politiky jsou tvořeny modulárně, připojení dalších souborových systémů tedy nevyžaduje složité nastavování a politiky jsou automaticky aktivovány po instalaci agenta na souborový systém. Je zde využito nastavení prostřednictvím white-listů.

Aby řešení zjistilo, jaká data jsou na souborovém systému, spouští pravidelně na systémech neinvazivní operaci, která prohledá soubory a zašle o nich informaci. Vlastní řešení poté tato data zpracuje a vyhodnotí citlivost souborů dle předdefinovaných politik. K definici dat používá například informace o lokaci souborů, jména souborů, velikost, datum poslední modifikace, vlastník souboru, přístupová práva k souboru a další. Nastavené politiky zamezí spuštění neznámých nebo neautorizovaných aplikací nebo modifikaci. V případě výjimek, je tyto možné definovat ručně.

Modul ochrany souborů je tedy vhodný pro:

- Ochranu konfiguračních a aplikačních souborů, které jsou volně dostupné na aplikačních a databázových serverech.
- Ochranu souborů obsahujících důvěrná osobní data jako například čísla kreditních karet, čísla účtů, rodná čísla a další.
- Ochranu souborů, které mají být modifikovány pouze pomocí k tomu určených aplikací před neoprávněným přímým přístupem.
- Ochranu zdrojových kódů přístupných například na build serveru firmy.

Architektura řešení je obdobná jako architektura modulu ochrany databází a používá již aktuální řešení nasazené v prostředí Nabyvatele v systému ESA MO. Na serveru nebo klientské stanici je nainstalována takzvaná sonda nebo agent, nezávislá na operačním systému, který odesílá informace ze systému do vlastního managementu řešení, které tyto spravuje agenty spravuje. V

řešení je tento management modul umístěn na centrální konzoli. Dle pravidel pak obratem dostane informaci o možném udělení přístupu nebo jeho zamítnutím pro konkrétní proces, který o daný prostředek žádal. Je tím zajištěna integrita jak na úrovni souborů a daném operačním systému, tak i na úrovni registrů v prostředí Windows. Celý provoz může probíhat nejenom restriktivním (zakazujícím) režimem, ale i formou monitoringu daný prostředků a samozřejmě logován. Zároveň je možné dle definic, data potenciálních incidentů odesílat na SIEM, kde jsou dále korelována.

Detailní popis nasazení řešení, bude součásti analýzy, kde Poskytovatel vyspecifikuje seznam vlastních politik. V kombinaci s nasazení next-gen firewall, poskytuje toto řešení možnou blokaci portů, ochranu před kybernetickými hrozbami, monitoring a ochranu před exploity.

2.6.3. Modul vyhledávání zranitelností

Součástí řešení je použití modulu vyhledávání zranitelností. Jedná se o centralizovanou platformu pro řízení rizik spojených s datovou infrastrukturou. Guardium provádí pravidelné skenování prostředí a hledá chybějící aktualizace, slabá hesla, známé chyby v nastavení a další bezpečnostní rizika.

Skenování se neomezuje pouze na databázové systémy, ale je možné ho provádět i nad big data, data warehousech a dalších platformách pro uchovávání dat. Všechny nalezené informace jsou automaticky zpracovány v přehledném reportu spolu s doporučenými best-practices, jak nalezené zranitelnosti opravit.

Zranitelnosti jsou seřazeny dle závažnosti v závislosti na typu zranitelnosti a informacích o skenovaném zařízení, které má Guardium k dispozici. Skenování lze provádět jak pravidelně (plánovaně), tak v daném okamžiku přímo z Guardium konzole. Všechny reporty je možné exportovat v mnoha různých formátech jako například .PDF, syslog, CSV a další. Reporty je možné automaticky odesílat příslušným osobám a automatizovat tím auditní procesy.

Guardium umožňuje provádět zaměstnancům, starajícím se o bezpečnost, skenování zranitelností bez spolupráce s ostatními IT zaměstnanci. To pomáhá k menší zátěži IT a také k rozdělení jednotlivých pravomocí v rámci společnosti. Skenery Guardium jsou nastavené tak, aby minimálně zatěžovaly databázové systémy a nedocházelo k ohrožení dostupnosti. Guardium dokáže v případě, že má provádět skenování v době kdy je databáze zatížena provést pouze testy na velmi nebezpečné zranitelnosti a ostatní testy provést později. Stejně tak je možné pozastavit testování na konkrétní zranitelnost, než bude opravena. Výstupy z jednotlivých datových zdrojů je možné v reportech spojovat do logických celků pro celkové zpřehlednění reportu.

Modul vyhledávání zranitelností je tedy vhodný pro:

- Skenování jednotlivých databází a hledání zranitelností jako chybějících patchů, slabých hesel a nevhodných nastavení.
- Tvorbu a export přehledných reportů. Export do .PDF, CSV, Syslog.
- Doporučené best-practices pro opravení nalezených zranitelností
- Jednotná konzole pro kontrolu a správu všech zranitelností v databázích, big data a data warehousech.

- Eskalaci a odesílání reportů o nalezených zranitelnostech pro účely auditingu

2.6.4. Soulad s GDPR

IBM Security Guardium je platforma, která pomáhá řešit značnou část z technických požadavků regulace. Díky monitoringu databází i nestrukturovaných dat a aplikovaní behaviorální analýzy dokáže v reálném čase zjistit podezřelé chování spojené s osobními údaji i dalšími citlivými aktivy organizace. Zároveň je díky vlastním prvkům proaktivní ochrany nebo ve spoluprací s dalšími bezpečnostními prvky infrastruktury, schopna podezřelé aktivity zastavit, popřípadě podstoupit přezkoumání. Řešení obsahuje sady pravidel pro soulad s GDPR.

Platforma v sobě již nyní přímo obsahuje tzv. GDPR akcelerátor v jehož rámci jsou nastaveny odpovědi na jednotlivé požadavky Nařízení. Řešení IBM Guardium obsahuje vlastní klasifikační funkcionalitu pro rozpoznání citlivých údajů v databázích a souborech. V řešení jsou například před připravená klasifikační pravidla z pohledu souladu s GDPR. Zároveň řešení obsahuje předpřipravené klasifikační politiky, nástroje pro tvorbu vlastních klasifikačních pravidel a automatizovaně vytvářet reporty, které poskytují požadované informace v souladu s požadavky GDPR. Součástí je i prostředí API, které je zdokumentované a připravené k dalším integracím.

3. POPIS HARDWARE

3.1. Stávající servery

Stávající servery budou rozšířeny o paměť RAMM a diskový prostor, tak aby bylo možné využít stávající prostředí ESA MO (Servery - Brána, Archiv v produkční i testovacím prostředím, zároveň i servery Brána a Archiv DR lokalitě). Navržené hardware prostředky jsou dostatečně dimenzované, tak aby bylo možné zátěž zvládnout.

3.2. Firewally a další síťová infrastruktura

Redundance síťové infrastruktury –Síťová infrastruktura je doplněna o dva firewally v clusteru, v primární lokalitě, které na základě analýzy, převezmou plnou funkčnost stávajících firewallů, nebo budou kaskádovitě plnit další ochranou zeď při komunikaci s prostředím DA MO. Ostatní infrastrukturní prvky budou použity tak, jak je poskytuje Nabyvatel.

3.3. Diskové pole

Předmětem dodávky je rozšíření stávajících diskových polí ESA MO o kapacitu 75TB a to jak v lokalitě Bystrovany, tak i v lokalitě Praha. Systém je dále možné rozšířit. Bude zachována plná funkcionalita stávajícího řešení a nastavení. Druhá lokalita je použita jako Failover/Disaster Recovery a bude schopna po provedení upgrade stejných postupů a zajistí stejnou funkcionalitu, jako již použité diskové pole.

3.4. Badatelna

Pro Portál Badatelna dojde k rozšíření kapacity pro Portál o 20TB v každé lokalitě.

Pro vlastní Badatelnu (pracoviště Badatelna) bude dodáno 6ks PC v konfiguraci standardního PC. Tyto počítače budou zapojeny do lokální sítě místní badatelny DA MO s připojením k internetu v budově VHA – Ryzyně (internet neposkytuje Poskytovatel). Pro dovybavení sítě místní badatelny bude dodán 24-portový switch v provedení Rack-mount 19“ a optický převodník. Součástí těchto PC bude i monitor 27“ s rozlišením min. 2560x1440 a operačním systémem Windows 10 OEM.

Níže je uvedena specifikace

- 4ks PC určených k digitalizaci v optimální konfiguraci vzhledem k výše uvedenému určení, v konfiguraci minimálně: CPU Intel i7, 16GB RAM, SSD disk 128GB, HDD 1TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440
- 2ks PC určených k verifikaci digitalizovaných dat v optimální konfiguraci k této činnosti, v konfiguraci minimálně: CPU Intel i7, 16GB RAM, SSD disk 128GB, HDD 1TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440
- 1x barevná laserová tiskárna A4, samostatné tonery, duplex, síťové rozhraní
- 1x barevná laserová tiskárna A3, samostatné tonery, duplex, síťové rozhraní

3.5. Digitalizace

Pro systém Digitalizace bude kromě serveru pro zajištění vlastního DMS, také další prostředky:

- 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.

ELZA

Součástí dodávky je vytvoření technických předpokladů pro implementaci systému ELZA. Proto je součástí plnění dodávka serverů s následujícími konfiguracemi (nebo lepší)

- 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+

Dále pak pro jednotlivé lokality bude dodáno:

Součástí dodávky je pořízení – lokalita Praha:

- 1ks APC Symmetra LX 12kVA Scalable to 16kVA N+1 Rack-mount 220/230/240V nebo 380/400/415V
- 1ks APC Symmetra LX Battery Module
- 8ks Rack PDU, 1U, 16A, 8x230V
- 1ks Jistič 3x20A
- 15ks Kabel 1-CXHK-R-J 5 x 4/O/-/B2 CAS 1dO
- 2ks Pomocný a montážní materiál (pro rack, pro UPS)

Součástí dodávky je pořízení – lokalita Olomouc-Bystrovany:

- 1ks APC Symmetra LX 8kVA Scalable to 16kVA N+1 Rack-mount 220/230/240V nebo 380/400/415V
- 1ks APC Symmetra LX Battery Module
- 8ks Rack PDU, 1U, 16A, 8x230V
- 1ks Jistič 3x20A
- 15ks Kabel 1-CXHK-R-J 5 x 4/O/-/B2 CAS 1dO
- 2ks Pomocný a montážní materiál (pro rack, pro UPS)
- 2ks RACK TRITON 32U 600x900, nosnost 400kg
- 2ks Podstavec pod RACK 600x900
- 2ks Ventilační jednotka 600x900

4. SLUŽBY

4.1. Zálohování a Monitoring

Systém DA MO bude dodán tak, aby zajistil zálohy všech klíčových komponent a jejich dat. K tomuto účelu bude použito software předního výrobce takového řešení, který poskytuje kvalitní management pro řízení záloh, jejich retencí, stejně tak umožňuje WAN akceleraci v případě nutnosti a použití a monitoring jednotlivých komponent pro další možnost a plánování kapacit. Licence jsou součástí dodávky.

Zálohování DA MO bude modifikováno tak, aby byla zvýšena spolehlivost a bezpečnost celého systému dle pravidla 3-2-1.
3 kopie dat
2 odlišné typy médií ve 2 lokalitách
1 of-site záloha

Princip zálohování zůstává zachovaný a bude rozšířena funkcionalita zálohovacího systému s využitím licencí pro zálohování.
Budou zálohovány:

- všechny servery (nové i stávající) v lokalitě Praha a to včetně dat, aplikací a jejich nastavení a operačních systémů včetně konfigurací v produkčním prostředí.
- Data uložená na rozšířeném diskovém poli IBM V5010 v lokalitě Praha.

V rámci zálohování DA MO budou implementovány tyto funkce:

- Bare-metal recovery - obnovení na čistý server bez instalovaného OS
- Možnost obnovení celého systému/disků/oddílu/souborů ze zálohy
- Vícenásobné plánování a skripty v rámci úlohy zálohy pro aplikačně konzistentní zálohu

Součástí implementace je vypracování a nasazení DR plánu umožňující off-site management a pravidelnou recyklaci pásek a aktualizace dokumentace.

4.2. Dostupnost systému

Dostupnost celého systému pro dlouhodobé uchovávání neutajovaných elektronických dokumentů bude 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 systému s výjimkou Badatelského portálu z důvodů na straně Poskytovatele 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. Nabyvatel 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 Poskytovatele je 2,5% během kalendářního roku.

4.3. Záruční servis

Poskytovatel zajistí záruční servis po dobu 60 měsíců od okamžiku převzetí dodávky Nabyvatelem v souladu s požadavky na dostupnost systému. Nabyvatel v době záruky nebude používat zdrojové kódy k změnám programového vybavení. Oprávněná osoba 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 Poskytovatel. 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.

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).

4.4. Technická podpora hardwarových a softwarových komponent

V rámci technické podpory 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.

4.5. Legislativně technický upgrade

Poskytovatel zajistí 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.

4.6. Zaškolení zaměstnanců VHA na DA MO

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):

- 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 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 Poskytovatel s pověřenou osobou dojednat detailní rozsah (zejména u administrátorů zohlednit komplexnost proškolení na celý systém DA MO).

4.7. Zapojení digitalizačního pracoviště

Součástí plnění bude zprovoznění a implementace celého Digitalizovaného DMS řešení do prostředí Nabyvatele. A to jak pro periferie, pracovní stanice, tak i zprovoznění vlastního aplikačního SW. 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.

5. HARMONOGRAM

Předávání dodávky při plnění smlouvy dodavatel/poskytovatel dohodne minimálně 20 dní předem s osobou oprávněnou jednat ve věcech technických uvedenou ve smlouvě a provede je v následujících fázích:

5.1. Start projektu "Pořízení DA MO"

Tato aktivita začíná v okamžiku podpisu smlouvy na dodávku řešení Digitálního archivu MO (DA MO).

5.2. Předimplementační analýza a návrh

Dodavatel/poskytovatel provede detailní předimplementační analýzu prostředí nabyvatele a na jejím základě provede detailní návrh řešení včetně požadavků na nabyvatele týkající se jeho součinností. K tomu obdrží od nabyvatele (pověřené osoby) potřebné podklady a informace (včetně datového modelu pro migraci dat). V této aktivitě dojde především k

- technickému návrhu způsobu propojení DA MO na ESA MO,
- technickému návrhu propojení na externí zdroje informací jako jsou externí systémy poskytující časová razítka, CRL, certifikáty,
- technickému návrhu propojení na interní systémy pro autentizaci uživatelů a emailovou komunikaci.

Výsledkem této projektové části je oboustranně schválený Detailní návrh řešení (obsahující reálný harmonogram projektu, požadavky na součinnost nabyvatele a vlastní technický návrh řešení DA MO).

5.3. Implementace DA MO

Je rozdělena na implementaci Brány DA MO, implementaci Archivu DA MO, implementaci Badatelského portálu, implementaci DMS skenovací linky a implementaci propojení primární a záložní lokality, které zabezpečí DA MO proti výpadku nebo i zničení dat / informací v jedné lokalitě.

5.4. Akceptace – převzetí plnění

Budou postupně samostatně prováděny akceptace funkčních částí řešení, jak je navrženo v implementační části, kterými jsou:

- Dílčí akceptace DMS Digitalizačního pracoviště,
- Dílčí akceptace části Brána DA MO,
- Dílčí akceptace části Archiv DA MO,
- Dílčí akceptace části Badatelský portál vč. nové webové prezentace VHU,
- Dílčí akceptace systému ELZA,
- Dílčí akceptace komunikace primární a záložní lokalitou.

Při dílčí akceptaci DMS Digitalizačního pracoviště dojde k ověření všech specifikovaných a objednaných HW a SW prvků a k ověření jejich správné funkcionality.

U části dílčích akceptací Brána, Badatelský portál a Archiv DA MO, komunikace s primární a záložní lokalitou dojde postupně k provedení:

- Funkčních testů pro ověření objednaných funkcionalit,
- Integračních testů pro ověření zda dílčí část komunikuje správně se svým okolím.

Nakonec bude provedeno vyhodnocení všech provedených testů, a pokud výsledky těchto testů dopadnou dle připravených kritérií, bude dílčí část akceptována.

Jako závěrečná, ale také nejdůležitější část akceptací je provedení celkové Akceptace systému DA MO. Tato celková akceptace zahrnuje provedení:

- generálního funkčního testu,
- generálního integračního testu, které otestují systém DA MO jako celek včetně všech integračních vazeb.

Výsledkem je pak celková akceptace řešení DA MO, které umožní následně spuštění Zkušebního provozu.

5.5. Vytvoření dokumentace řešení

Součástí dodávky řešení DA MO je dodávka kompletní dokumentace, která zahrnuje vytvoření kompletního popisu řešení, kompletní provozní dokumentaci včetně popisu praktické údržby, řešení, příprava strategických plánů podle metodiky PLATTER (Planning Tool for Trusted Electronic Repositoriem) „Plán důvěryhodného digitálního repozitáře“.

Poskytovatel předá k dílu kompletní projektovou dokumentaci dle platných norem a předpisů, včetně doporučení k provozu, údržby, návodu k obsluze, seznamů předmětů v soupravách s jejich označením a popisem (součástí je i položkový rozpočet) vše v českém jazyce. Dokumentaci předá ve vázané knize a doplní DVD v elektronické podobě ve formátu PDF a doc. Součástí dokumentace bude doporučení pro snížení rizik a návod pro obnovu funkčnosti po havárii.

Součástí dokumentace bude doporučení pro zabezpečení optimálního způsobu pozáručního servisu.

5.6. Zaškolení pracovníků DA MO

Součástí projektové části je i zaškolení pracovníků podle jejich rolí a pracovního zaměření:

- 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.

6. LICENČNÍ PODMÍNKY LICENCE PRO SYSTÉM DA MO

6.1. Licenční model a rozsah licence Digitální archiv ministerstva obrany

6.1.1. Licenční model

Tento dokument popisuje licenční podmínky licence dodávaného řešení Digitální Archiv Ministerstva Obrany pro zadavatele Ministerstvo Obrany. Licence bude zákazníkovy poskytnuta ve formě „managed licence“ tedy licenční modelem, kdy zákazník získá stanovenou licenci k plnému užívání dle níže uvedených licenčních podmínek na dobu platnosti uzavřené smlouvy, a to včetně produktové podpory. Po uplynutí smluvní doby, po kterou má zákazník licenci k plnému užívání včetně platné produktové podpory, má zákazník možnost pokračovat v plném využívání poskytnuté licence bez produktové podpory anebo zakoupit produktovou podporu dle podmínek Passport Advantage Agreement (viz Kapitola 2 tohoto dokumentu).

Níže uvedená text uvádí seznam prvků řešení Digitálního Archivu Ministerstva Obrany, které jsou do licence zahrnuty a licenční podmínky dané části licencovaného řešení Digitálního Archivu Ministerstva Obrany.

Modul Brána

Část řešení Digitální archiv ministerstva obrany Brána je licencována na základě licenčního modelu VPC pro stanovený počet standardních autorizovaných uživatelů a archivářů, kteří mohou komponentu Brány využívat. V rámci licence řešení Digitální archiv ministerstva obrany získává zákazník k plnému užívání licenční právo pro **10000** standardních autorizovaných uživatelů a **20** archivářů využívajícím komponentu Brána. V rámci těchto licenčních podmínek získává zákazník právo k plnému využívání komponenty řešení Brána pro testovací, produkční i DR prostředí DAMO.

V případě, že počet standardních autorizovaných uživatelů nebo počet archivářů využívajících komponentu Brána překročí výše uvedené počty, je zákazník povinen konzultovat rozšíření stávající licence s dodavatelem.

Odkaz na detailní licenční podmínky: http://www-03.ibm.com/software/sla/sladb.nsf/lilookup/C790AE092CDB9E908525863B00481765?OpenDocument

Modul Archiv

Část řešení Digitální archiv ministerstva obrany Archiv je licencován na základě licenčního modelu VPC pro stanovený počet standardních autorizovaných uživatelů a archivářů, kteří mohou komponentu Archiv využívat. V rámci licence řešení Digitální archiv ministerstva obrany získává zákazník k plnému užívání licenční právo pro **10000** standardních autorizovaných uživatelů a **20** archivářů využívajícím komponentu Archiv. V rámci těchto licenčních podmínek získává zákazník právo k plnému využívání komponenty řešení Archiv pro testovací, produkční i DR prostředí DAMO.

V případě, že počet standardních autorizovaných uživatelů nebo počet archivářů využívajících komponentu Archiv překročí výše uvedené počty, je zákazník povinen konzultovat rozšíření stávající licence s dodavatelem.

Odkaz na detailní licenční podmínky: http://www-03.ibm.com/software/sla/sladb.nsf/lilookup/C790AE092CDB9E908525863B00481765?OpenDocument

Modul MS Office View

Část řešení Digitálního archivu ministerstva obrany MS Office View je licencována na základě licenčního modelu UVU (User Value Unit) pro stanovený počet standardních autorizovaných uživatelů a archivářů, kteří mohou komponentu MS Office View využívat. V rámci licence řešení Digitální archiv ministerstva obrany získává zákazník k plnému užívání licenční právo pro **10000** standardních autorizovaných uživatelů a **20** archivářů využívajících řešení MS Office View. V rámci těchto licenčních podmínek získává zákazník právo k plnému využívání komponenty řešení MS Office View pro testovací, produkční i DR prostředí DAMO.

V případě, že počet standardních autorizovaných uživatelů nebo archivářů přistupujících k řešení MS Office View překročí výše uvedené počty, je zákazník povinen zakoupit rozšíření stávající licence.

Odkaz na detailní licenční podmínky: http://www-03.ibm.com/software/sla/sladb.nsf/lilookup/851944EC4975286F8525858F007F14DC?OpenDocument

Modul Redakce

Část řešení Digitálního archivu ministerstva obrany Redakce je licencována na základě licenčního modelu UVU (User Value Unit) pro stanovený počet standardních autorizovaných uživatelů a archivářů, kteří mohou komponentu Redakce využívat. V rámci licence řešení Digitální archiv ministerstva obrany získává zákazník k plnému užívání licenční právo pro **10000** standardních autorizovaných uživatelů a **20** archivářů využívajících řešení Redakce. V rámci těchto licenčních podmínek získává zákazník právo k plnému využívání komponenty řešení Redakce pro testovací, produkční i DR prostředí DAMO.

V případě, že počet standardních autorizovaných uživatelů nebo archivářů přistupujících k řešení Redakce překročí výše uvedené počty, je zákazník povinen zakoupit rozšíření stávající licence.

Odkaz na detailní licenční podmínky: http://www-03.ibm.com/software/sla/sladb.nsf/lilookup/851944EC4975286F8525858F007F14DC?OpenDocument

Modul Digitalizační linka

Část řešení Digitálního archivu ministerstva obrany Digitalizační linka je licencována na základě licenčního modelu UVU (User Value Unit) pro stanovený počet uživatelů digitalizační linky, kteří mohou komponentu Digitalizační linka využívat. V rámci licence řešení Digitální

archiv ministerstva obrany získává zákazník k plnému užívání licenční právo pro **15** uživatelů DMS skenovací linky využívajících modul Digitalizační linka. V rámci těchto licenčních podmínek získává zákazník právo k plnému využívání komponenty řešení Digitalizační linka pro testovací, produkční i DR prostředí DAMO.

V případě, že počet uživatelů digitalizační linky přistupujících k modulu řešení Digitalizační linka překročí výše uvedené počty, je zákazník povinen zakoupit rozšíření stávající licence.

Odkaz na detailní licenční podmínky: http://www-03.ibm.com/software/sla/sladb.nsf/lilookup/C7642D9B5D4BAA50852585EB00666934?OpenDocument

http://www-03.ibm.com/software/sla/sladb.nsf/lilookup/C2E5C8F55CB41BF2852585EB0066603E?OpenDocument

6.2. Doplňující licenční podmínky

- Zákazník obdrží zdrojové kódy k částem řešení Bezpečnostní Digitální archiv, která byla vyvíjena přímo na míru zákazníkovi na základě jeho specifických požadavků
- Licence Digitální archiv ministerstva obrany je využívána pro DR prostředí pouze v případě, že nedochází k jejímu využívání v prostředí produkčním a naopak. (lze používat pouze v případě nastavení Active/Passive. Pokud přejdeme do režimu Active/Active, je nutno rozšířit stávající licenci)
- Definice typů licencovaných uživatelů v rámci řešení Digitální archiv ministerstva obrany
    - Standardní autorizovaného uživatel – V kontextu detailních licenčních podmínek je standardní autorizovaný uživatel synonymem pro pojem externí uživatel
    - Archivář – V kontextu detailních licenčních podmínek je archivář synonymem pro autorizovaného uživatele
    - Uživatel DMS skenovací linky – V kontextu detailních licenčních podmínek je uživatel DMS skenovací linky synonymem pro autorizovaného uživatele

6.3. Passport Advantage

ftp://ftp.software.ibm.com/software/passportadvantage/PA_Agreements/PA_Agreement_Czech.pdf

Příloha 3 smlouvy č. 195310197

Objasnění a doplnění dokladů k nabídce
na nadlimitní veřejnou zakázku v užším řízení
Sp. zn. SpMO 48224/2018-1350/30
(bez přílohy č.1)

Únor 2021

Digitální archiv MO - nákup

Pro:

Česká republika – Ministerstvo obrany

- ORIGINÁL

Tento dokument je odpovědí účastníka IBM Česká republika, spol. s r.o., se sídlem V parku 2294/4, 148 00 Praha 4 – Chodov, IČO 14890992 (dále jen „účastník“ , „Účastník“ nebo „IBM“), na **Žádost o objasnění a doplnění dokladů (Sp. zn. SpMO 48224/2018-1350/30) k veřejné zakázce „Digitální archiv MO – nákup“** zadavatele Česká republika – Ministerstvo obrany se sídlem Tychonova 1, 160 01 Praha 6, IČO 60162694, zastoupeného ředitelem odboru vyzbrojování pozemních sil a KIS sekce vyzbrojování a akvizic MO Ing. Petrem ZÁBORCEM, na adrese Sekce vyzbrojování a akvizic MO, odbor vyzbrojování pozemních sil a KIS, nám. Svobody 471/4, 160 01 Praha 6 (dále jen „zadavatel“, „Zadavatel“ nebo „MO“) ze dne 10.února 2021.

Tímto dokumentem účastník objasňuje vybrané části své nabídky ze dne 4.2.2021, a to na základě výše uvedené výzvy zadavatele ze dne 10. února 2021.

Popis navrženého řešení, jeho architektury, topologie či detailní specifikace konkrétních HW a SW technologií a služeb, které jsou uvedeny v tomto dokumentu, je založen na aktuální míře znalostí Účastníka ohledně prostředí Zadavatele vyplývající ze Zadávací dokumentace. Účastník si vyhrazuje právo detail řešení přizpůsobit výstupům předimplementační analýzy, při zachování finančních a smluvních aspektů uvedených v nabídce Účastníka.

Pokud v rámci tohoto dokumentu Účastník uvádí, že používá, rozšiřuje, modifikuje, atp. stávající zařízení, komponenty, atp. Zadavatele, jde výhradně o prostředky, které Zadavatel v souladu s kapitolou 16 Přílohy č. 1 zadávací dokumentace poskytuje pro využití v rámci řešení DA MO.

Dokument je členěn do jedenácti kapitol, kdy každá kapitola obsahuje:

- **resumé dotazu či požadavku na objasnění zadavatele**
- **objasnění zpracované společností IBM Česká republika, spol. s r.o.**

Obsah

1. Dotaz č.1 (Cenový rozklad)

1.1 Dotaz či požadavek zadavatele na objasnění

Cenový rozklad v nabídce účastníka považuje zadavatel za zcela nedostatečný a v rozporu s požadavky zveřejněné zadávací dokumentace (Sp. zn. SpMO 48224/2018-1350/9), (dále jen „zadávací dokumentace“ nebo „ZD“). Zadavatel nedokáže z předložených údajů žádným způsobem dovodit, jaké HW a SW komponenty, v jaké konfiguraci a jaké služby, v jakém rozsahu jsou předmětem smluvního plnění. Zadavatel žádá účastníka o předložení opraveného podrobného cenového rozkladu (položkového rozpočtu), v souladu s § 46 odst. 3 zákona, který bude obsahovat rozpad ceny návrhu řešení na jednotlivé položky za HW, SW a služby. Zadavatel upozorňuje, že cenový rozklad požaduje vypracovat s rozpadem až na jednotlivé položky smluvního plnění a jakékoliv slučování do vyšších celků bude považováno za nesplnění této žádosti o objasnění nabídky.

1.2 Objasnění účastníka IBM

Účastník dle požadavku zadavatele předkládá podrobný cenový rozklad s rozpadem na jednotlivé položky smluvního plnění vložený do původní cenové tabulky formátu Excel jako nový list ***Doplnění a objasnění***.

Původní cenové položky uvedené v cenovém rozkladu předkládaném společně s nabídkou jsou v novém cenovém rozpadu vyznačeny žlutým podbarvením. Původní položky, které byly vzhledem k podrobnějšímu členění nahrazeny, jsou vyznačeny přeškrtnutím.

Pozn.: V dokumentu je rovněž ponechán v záložce *Nabídka* původní cenový rozklad uvedený v nabídce.

Doložení dokumentu viz **Příloha 1 - Priloha 1_Cenovy_rozklad_detail_IBM.xlsx,**
list ***Doplnění a objasnění***

Účastník předkládá zmíněný cenový rozklad rovněž ve formátu .pdf, ve kterém je součástí návrhu smlouvy jako Příloha č.2.

Doložení dokumentu viz **Příloha 2 - Priloha 2_Cenovy_rozklad_detail_IBM.pdf**

2. Dotaz č. 2 (Popis návrhu řešení)

2.1 Dotaz či požadavek zadavatele na objasnění

Zadavatel konstatuje, že prakticky celá textace nabídky účastníka je sestavena z formulací uvedených v tabulce pro posouzení nabídek z hlediska technických požadavků bez bližšího popisu navrženého řešení, jeho architektury, topologie a uvedení detailní specifikace konkrétních HW a SW technologií a služeb, které jsou předmětem smluvního plnění.

Zadavatel takový přístup neakceptuje, protože podle jeho názoru nesplňuje požadavek bodu B.7. zadávací dokumentace a žádá o předložení řádného popisu architektury a topologie návrhu řešení v souladu s požadavky Přílohy č. 1 zadávací dokumentace a konkretizaci jednotlivých položek včetně popisu HW konfigurací jednotlivých komponent a typu a rozsahu SW licencí, které jsou součástí návrhu řešení a smluvního plnění, které musí být položkově uvedeny i v cenovém rozkladu.

2.2 Objasnění účastníka IBM

Níže Účastník detailně rozpracovává popis jednotlivých komponent, jejich zapojení a nasazení v rámci návaznosti na existující řešení ESA, tak jak specifikuje Zadávací dokumentace DA. V rámci maximalizace a využití současných komponent, bylo cílem Účastníka připravit v návrhu řešení takové modifikace, aby bylo zajištěno optimální ekonomické využití. Proto ty komponenty řešení ESA, které budou nahrazeny budou dále použity, pro možné rozšíření stávajících prostředků (serverů a jiných komponent), které netvoří zcela klíčovou část garantovaného úložiště. Např. pro servery prostředí Test a Backup budou další výkonnostní prostředky jenom přínosem. Celý proces doplnění jednotlivých komponent bude řízen a potvrzen Zadavatelem, tak, aby nebyly porušeny interní předpisy.

Účastník v kap. 4.1. uvedl: „Budou zálohovány: všechny servery (nové i stávající) v lokalitě Praha a to včetně dat, aplikací a jejich nastavení a operačních systémů včetně konfigurací v produkčním prostředí“
V rámci odpovědí Účastník upřesňuje, že budou dodány níže uvedené servery s uvedenými **min. parametry**, na které se bude provádět migrace ze stávajícího prostředí. Zároveň původní servery (4ks – Brána PROD, Brána DR, Archiv PROD, Archiv DR) budou použity jako zdroj komponent pro zvýšení výkonu u zbývajících neklíčových komponent, tak jak bylo uvedeno v kap.3.1 nabídky, nebo jako dedikované servery, zcela oddělené od prostředí DA prostřednictvím firewallu. (vyplyne z analýzy – požadavky na fungování v rámci DMZ):

Servery
Virtualizace1 (Virtual1)-Praha = CPU 2x16cores, 256GB RAMM, 6x1Gbit, HBA, 2x480GB, 2xZdroj
Předpokládané nasazení virtualizovaných serverů:
Badatelna Ext. Prod

Badatelna Ext. Test
Digitalizace Pha Prod
Digitalizace Pha Test
Brána (ESA, DA) - Prod
Archiv (ESA, DA) – Prod
Karanténa

Virtualizace2 (Virtual2)-Olomouc = 2xCPU 16cores, 256GB RAMM, 6x1Gbit, HBA, 2x480GB, 2xZdroj

Brána ESA, DA - DR
Archiv ESA, DA - DR
Badatelna DA - DR
Backup Proxy/DR
Karanténa

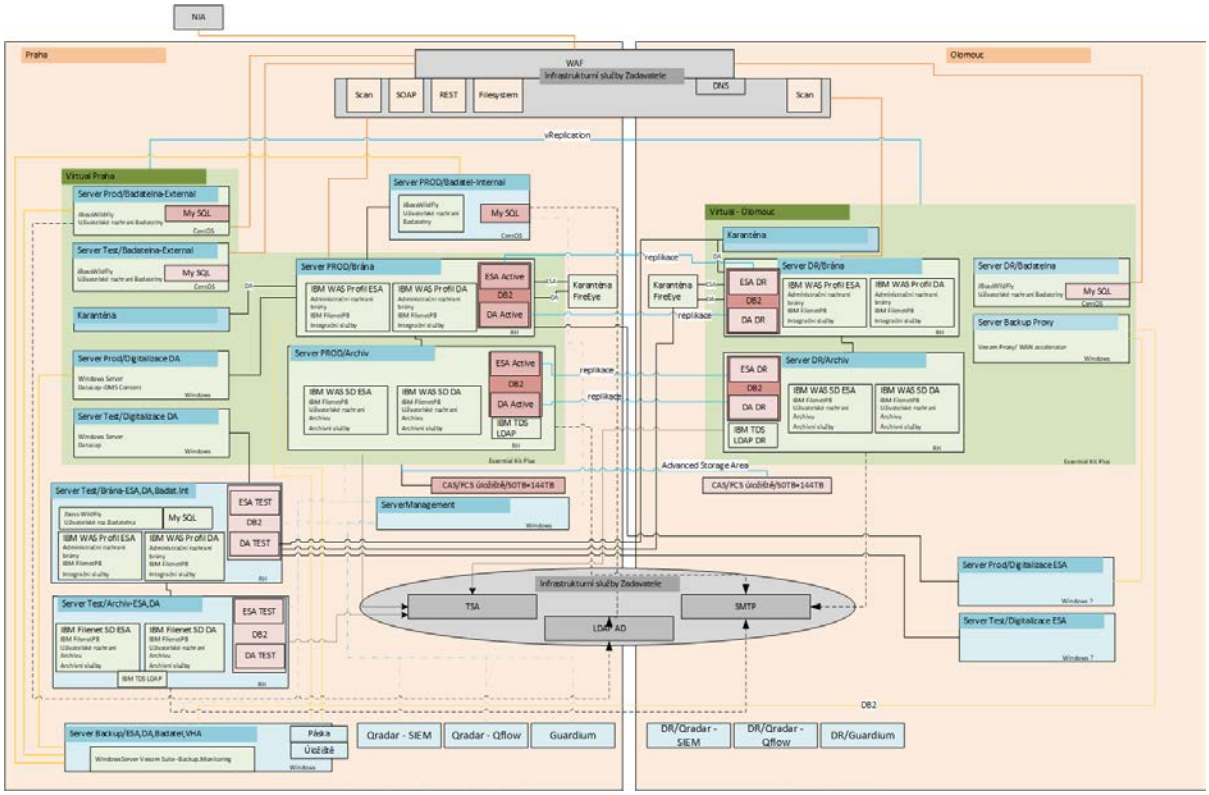
Diskový subsystém Storwize 5010 bude rozšířen celkem o expanzní jednotku, která bude osazena celkem 12ks x 12TB (144TB) v obou lokalitách. Z toho bude 75TB určeno výhradně pro účely DA pro ukládání dokumentů. Další část úložiště pak bude v každé lokalitě (20TB) dedikována pro Portál Badatelny. Další max. 10TB bude určeno pro systém DMS, resp. Digitalizační linku umístěnou v Praze, čímž je naplněn požadavek na vytvoření Digitalizačního pracoviště s DMS. Zbylá kapacita může být použita pro účely testování, navýšení kapacit výše uvedených prostředí, nebo pro účely vytváření replik.
Další hardware (např. servery ELZA, APC, apod …) byl již vyjmenován v rámci nabídky jak bylo Zadavatelem požadováno, případně upřesněn v následujících dotazech (pracovní stanice).

Návrh nasazení a umístění jednotlivých klíčových komponent, je uveden v obrázku níže. (viz obr. *Základní model deploymentu jednotlivých komponent*). Popis migrace a přesun stávajících serverů ze současného prostředí bude součástí detailního popisu v analýze, i s ohledem na možnosti odstávky prostředí ESA.

V obrázku níže jsou popsány jednotlivé komponenty a jejich umístění v rámci celé architektury. Zároveň je tento obrázek přiložen jako příloha pro lepší přehlednost. Účastník popisuje pro snazší přehlednost:

- zeleným pozadím je označena dodávaná virtuální infrastruktura (Virtual1, Virtual2) a zřejmě Digitalizační pracoviště běžící v lokalitě Olomouc
- červené čáry jsou z a do externích systémů.
- přerušované čáry jsou pro komunikaci s interními systémy Zadavatele, které budou použity, případně management
- modré čára jsou replikace dat.
- černá čára je logický spoj, že tyto komponenty spolu budou komunikovat.
- oranžová pak zálohování komponent, nebo uvedení jednotlivého zálohovacího agenta - proxy.

Pro větší přehlednost je obrázek předložen rovněž jako samostatná příloha ve formátu .pdf.
Doložení dokumentu viz **Příloha 3 - Priloha 3_ Zakladni_model_deploymentu_IBM.pdf**



Obrázek: Základní model deploymentu jednotlivých komponent

Síťová konektivita

Účastník vycházel při návrhu vlastního nasazení a integrace nové funkčnosti systému DA MO z konceptu a architektonického modelu systému ESA (viz obrázek *Základní architektonický model ESA.)*, který je na MO provozován. Jeho rozšíření a možnost využití virtuální infrastruktury bylo Zadavatelem potvrzeno v rámci ZD.

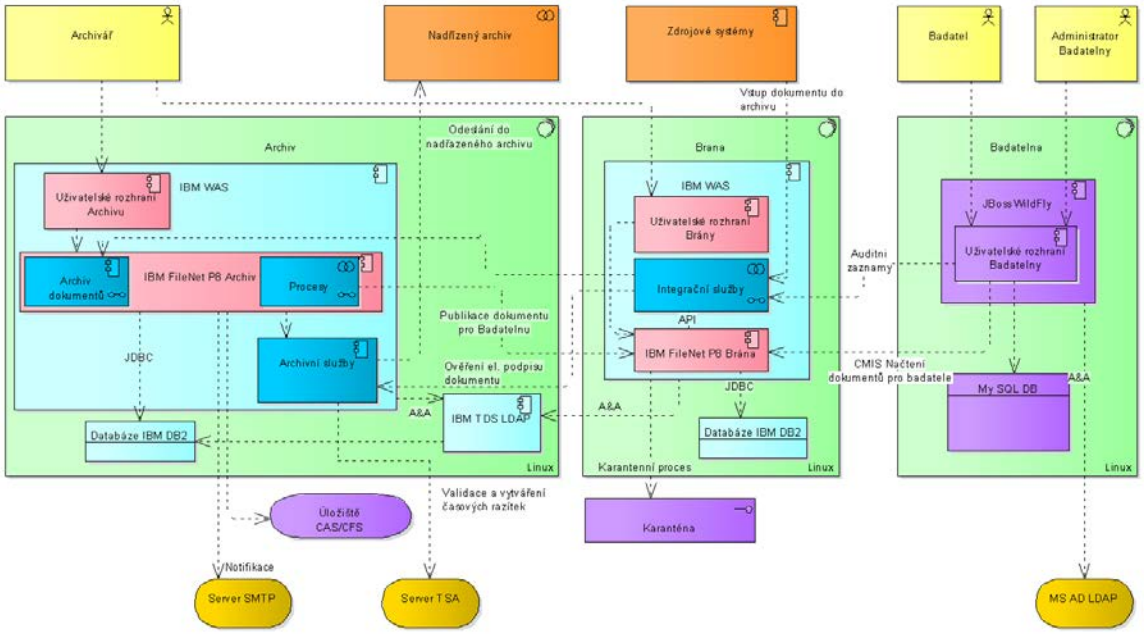
Nasazení jednotlivých komponent je navrženo tak, aby byla zajištěna segmentace jednotlivých komponent (Brána, Archiv, Badatelna) a byly zároveň zajištěny i rozdílné komunikační cesty v mezi systémy ESA a DA. (použití VLAN a jiných subnetů sítě).

Server Archiv má v návrhu dedikovány vlastní 2ks síťových karet, které jsou zapojeny do switchů sítě Archiv (následně pak konektivita do firewallu). Pro ESA i DA budou použity jiné VLANs a jiné síťové rozsahy.

V rámci serveru Brána jsou dedikovány další dvě síťové karty do switchů Brány, společně s Digitalizační linkou i jejím testovacím prostředím a Karanténou. Všechny servery budou mít nastavena pravidla na komunikaci, dle potřeb Zadavatele (Digitalizace a Brána v produkci stejná VLAN, Digitalizace v testu, separátní VLANs). Tím je zajištěno oddělení komunikace a nutnost volání služeb brány nebo archivu pouze prostřednictvím komunikačních cest, které procházejí přes firewall. Provoz bude bude monitorován, filtrován nebo i blokován nejen prostřednictvím IPS klienta, ale i vlastní IPS sondou na firewallu. (Pro doplnění Účastník uvádí, že na virtuální servery budou nasazeni IPS klienti/agenti DeepSecurity, kteří zajištují další dodatečnou ochranu, kterou Zadavatel vyžadoval v případě použití virtuální infrastruktury – popis níže.) Další doplňující informace o firewallu jsou uvedeny v upřesnění k dotazu č.11.

Virtualizace

Migrace ze stávajícího hardware na novou virtualizační platformu, dává Účastníkovi vysokou variabilitu řešení při umístění vlastní Badatelny. Tento server je prozatím plánováno nasadit ve virtuálním prostředí striktně odděleným od ostatních serverů a bude mít dedikovány svoje síťové karty (2ks) pro komunikaci s okolním prostředím (tyto jsou zapojeny přímo do firewallu). Veškerý provoz ze a na server bude procházet výhradně přes firewall a waf (přístup na rozhraní Badatelny přímo na interface firewallu bude zakázáno). Stejně tak diskový prostor bude zcela oddělen. Zadavatel v ZD nevyžadoval fyzické oddělení tohoto serveru od zbytku infrastruktury. Stejně tak bude nastaveno Test prostředí, které bude komunikovat výhradně přes stejné síťové karty jako produkce, ale přes jiné VLAN na firewall. Nastavení firewall pravidel bude zmigrováno ze stávajících firewallů a rekonfigurováno pro deployment na novém hardware (zřejmě i podrobeno kontrole a odsouhlasení Zadavatelem).



Obrázek: Základní architektonický model ESA.

Software

Níže bude popsán použitý infrastrukturní software, který bude v rámci nasazení použit a který je nezbytnou součástí pro plnohodnotné fungování systému DA MO (potažmo i ESA MO). Zároveň Účastník upřesňuje, že veškerý dodaný software (infrastrukturní i aplikační) je poskytován s podporou na 5let. (včetně veškerého aplikačního software pro modul Brána, Archiv, Digitalizační linky, Office View, modul Redakce, Badatelny)

Pro zálohování byl zvolen osvědčený software předního výrobce zálohovací technologie pro virtuální stroje Veeam Availability Suite. Dvě komponenty, které jsou v rámci tohoto bundle použity Veeam Backup and Restore a VeeamONE a nasazen bude na serveru Backup.Zajistí tím jak plnění technologických záloh systému, tak i jeho monitoring. Protože některé pevné servery (bare metal), na kterých jsou aktuálně provozovány systémy ESA MO budou zvirtualizovány a přeneseny do virtuálního prostředí VMWARE Esssential Kit Plus může tím dojít k uvolnění prostoru v daných rack-cích. Navržený hypervizor od společnosti VMWARE, který bude dodán s podporou na 5let a který naplňuje požadované

technologické a inovativní požadavky, umožňuje používat pokročilé funkce vMotion, vReplication, vDataProtection, vShield Endpoint, High Availability a mnohé další. Vzhledem k nasazení na pouze dvou serverech (licence umožňuje využívat až 3ks hosts / 1licence volná), je možné dále konsolidovat prostředí Zadavatele, nebo oddělit prostředí Badatelny na zcela oddělený server a tím nastavit ještě vyšší bezpečnost a dostupnost služeb. Stejně tak jsou navrhované servery Virtual1 a Virtual2 dostatečně dimenzovány pro možnou další budoucí migraci, v případě, že stávající (již běžící) hardware nebude možné dále provozovat.

Badatelna

Technologie Badatelny byly zvoleny s cílem dosáhnout maximální udržitelnost, nízké náklady na údržbu a rozšiřování řešení. Jádrem řešení Badatelny jsou zejména tyto open-source technologie

- Java 8
  - Java je objektově orientovaný programovací jazyk, vyvíjený společností Oracle (dříve Sun Microsystems). Od roku 2007 je vyvíjena jako open-source. Java 8 je nejnovější a nejmodernější verze tohoto jazyka, vydaná v březnu 2014
- WildFly
  - WildFly je výkonný, modulární a lehký aplikační server, který umožňuje vytvářet aplikace. Využívá další moduly k zajištění skutečné izolace aplikace, skrývání tříd. Běh vlastní aplikace se provádí pouhým propojením na JAR, který aplikace potřebuje.
- Apache Solr
  - Apache Solr je špičková indexovací technologie, která poskytuje zejména robustní funkcionalitu v oblastech fulltextového a fasetového vyhledávání
- OpenSeadragon
  - Technologie OpenSeadragon zabezpečuje zobrazování obrazového obsahu velkých rozměrů optimalizovaným způsobem. Využívá techniku tzv. tilování, u které dojde k rozdělení podkladového obrázku na mřížku a k vygenerování jednotlivých buněk mřížky v různých rozlišeních
- AngularJS, jQuery, HTML5
  - Jedná se o sadu špičkových frontendových technologií. Společně tvoří celek, pomocí kterého jsme schopni konceptuálně oddělit vývoj frontendu od backendových technologií a tím paralelizovat značnou část vývoje. Taktéž jsme schopni vnést do frontendu principy responsivního design.

Brána a Archiv

Technologie pro core komponenty digitálního archivu jsou součástí modulu Brána a modulu Archiv. Jejich jádrem jsou:

- FileNet P8
  - Filenet P8 je enetrprise platforma pro práci s dokumenty, provádění toku informací nad dokumenty (workflow) nad dokumenty, od jejich pořízení až po samotnou archivaci.
- IBM DB2
  - IBM DB2 je databáze která je nativně podporována v rámci provozu IBM Filenet P8. Byla zvolena z důvodu optimálního licenčního modelu a zajištění vysoké dostupnosti celého řešení

- IBM WAS (WebSphere Application server)
    - IBM WAS, je aplikační server, který zprostředkovává služby poskytované IBM Filenet a IBM DB2

Databáze

Součástí nabízeného řešení pro ukládání a správu metadat archívních dat je databázový systém DB2, který je součástí softwarového balíku Modul Brána, Modul Archiv, Modul Digitalizace.
Standardní DB2 jsou nástroje zálohování databází a archivních logů. Zálohování databází může probíhá jak offline (tedy bez připojení uživatelů), tak online (během práce uživatelů). Zálohuje se buď do filesystému nebo přímo do centrálního systému zálohování (Storage manager) pomocí API knihovny.
Online zálohování může být v těchto režimech:

- FULL - záloha všech dat v databázi
- INCREMENTAL – záloha jen změn od poslední zálohy FULL – tedy kumulativní, každá další INCREMENTAL záloha je větší než předešlá
- INCREMENTAL DELTA – záloha jen změn od poslední zálohy DELTA nebo FULL – tedy rozdílová – pouze změny mezi 2 posledními zálohami

Online se také zálohují transakční žurnály (logical logs) – log, který se zaplní se automaticky archivuje buď do filesystému nebo přímo do centrálního systému zálohování (Storage manager) pomocí API knihovny.
Transakční log se dá také zálohovat přímým příkazem před jeho zaplněním a tím dodržovat stanovenou metriku RPO (repait point objective)
Obnova ze záloh databáze je vždy offline a provádí se ve 2 krocích:

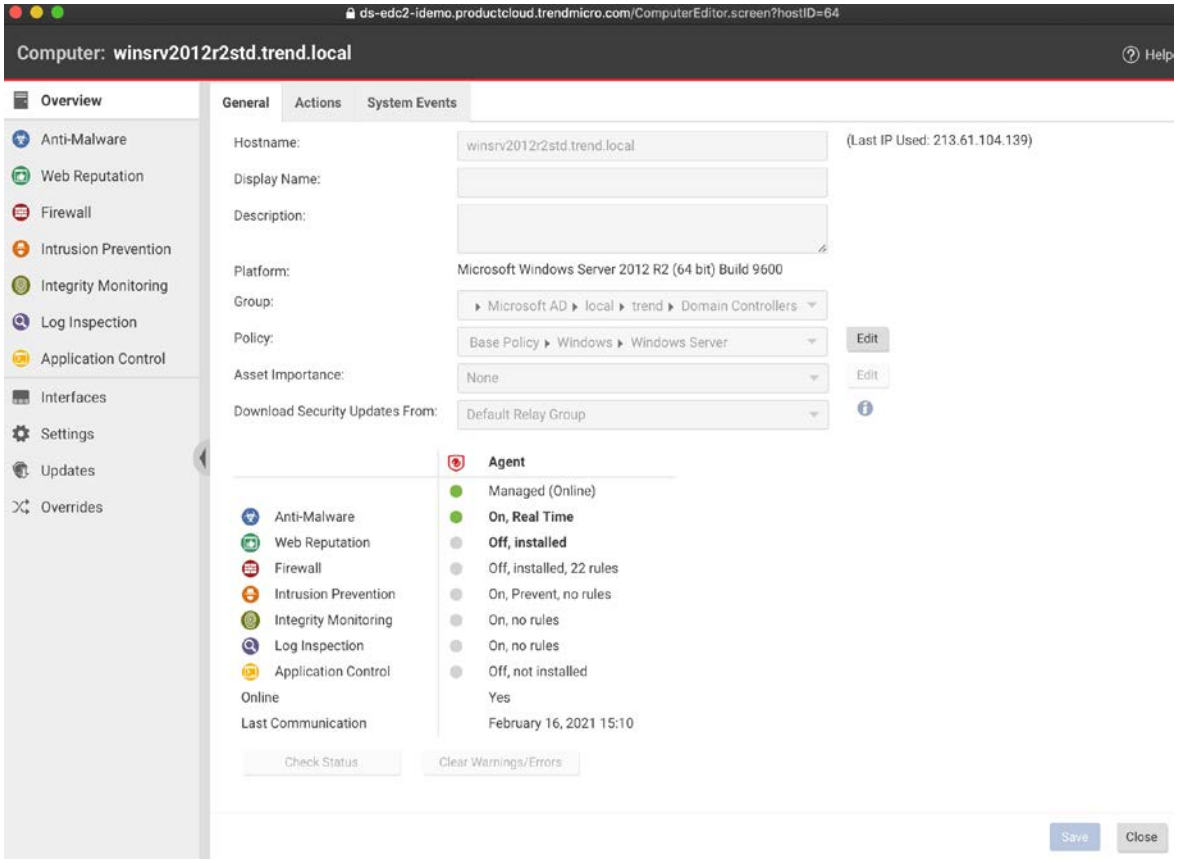
- obnovat databáze (restore from db) – pokud se používalo pro zálohy inkrementů, obnoví se napřed z FULL zálohy a potom z následných inkrementů
- obnova z archivnich logů (rollforward database – logické zotavení) – zopakují se transakce z logických žurnálů, provedené od poslední použité zálohy pro obnovu

Logické zotavení je možné provést k poslední transakci posledního archivovaného logu, k určitému číslu logu nebo k určitému okamžiku v čase.
Zálohovat DB2 je možné také nástroji diskového pole (snapshot) nebo nástroji virtualizace, pokud je takové pole (nebo virtuální prostředí) k dispozici
Vysokou dostupnost nebo odolnost proti haváriím (HA/DR – high availability/disaster recovery) je umožněna komponentou DB2 HADR.
DB2 HADR pracuje na principu 2 instancí DB2 (primary a standby) na různých lokalitách a synchronizace dat probíhá replikací informací z logických logů po síti do standby instance. V režimu HADR se buffer logického žurnálu v okamžiku, kdy se posílá do logického logu současně posílá po síti do standby instance, která je v režimu kontinuálního logického zotavení – transakce se automaticky aplikují na standby instanci z informací v logických žurnálech poslaných z primární instance.
Mezi primární a standby instancí se pravidelně kontroluje heartbeat, pomocí něhož je případně notifikováno, pokud se spojení přeruší.
Součástí řešení jsou pak příkazy pro převzetí primární role standby instanci nebo naopak vrácení primární role primární instanci. Využití DB2 HADR umožňuje výrazní zkrácení doby obnovy databáze po havárii, protože se nemusí obnovovat ze záloh.
Standardní součásti DB2 jsou i nástroje pro monitoring, správu DB2 – řádkové i grafické (např. db2pd, db2mtrk, db2 studio), které umožňují databáze upravovat, ladit, pomáhat

s identifikací problémů apod. Pro Portál Badatelny je navržena technologie MySQL, jejíž data budou replikována do prostředí DR prostřednictvím virtualizačních prostředků. Princip obnovy vyplývá z principu obnov DB technologie. Dojde k obnově hlavní DB, která se bude zálohovat a následně se na tuto budou aplikovat zálohované binární logy. Tím dojde k obnově, tak aby byla minimalizována ztráta dat. Zálohování probíhá standardními prostředky MySQL (tzv. build-in) a její detailní popis součástí analýzy.

Agenti

Pro zajištění ochrany vlastních VM bude nasazen DeepSecurity agent od společnosti TrendMicro v kombinaci s agentem Integrity and Control od společnosti McAfee. Produkt Deep Security zajistí svojí funkcionalitou komplexní ochranu i na síťové komunikaci. Agent tohoto produktu dokáže nastavovat host-firewall a zároveň i host-IPS na každém serveru. Zároveň má anti-malware, web reputaci a další moduly. Je schopen kontrolovat i TLS přenos, jestliže bude možné poskytnout privátní klíč a provádět nastavení prostřednictvím centrální konsole, která poběží na mgmt serveru Níže jsou uvedeny obrázky z nasazení v nejmenovaném prostředí (příklad). Základní funkcionalitou je i logování a napojení na SIEM, pro další vyhodnocování chování a změn stavu jednotlivých serverů.



Obrázek: Příklad prostředí nastavení Deep Security

Pro kontrolu a Integrity serverů je v rámci DA MO použito již ověřeného modulů Integrity and Control od společnosti TrendMicro, případně produktu McAfee. V kombinaci s Deep Security agentem, je toto nasazení schopno naplnit všechna bezpečnostní očekávání pro virtuální servery, které jsou na taková prostředí kladena v rámci ZD.

Připojení a management klienta (nastavení politik) v rámci centrálního managementu poskytuje logy a doplňující informace pro SIEM, který tyto logy vyhodnocuje.

Ochrana DB je zajištěna agentem řešení, které bylo povoleno Zadavatelem použít, systém Guardium. Nastavení politik pro kontrolu dat, případně blokování aktivit bude v analýze vycházet z nastavení ESA, nicméně dle potřeb Zadavatele bude modifikováno.

Operační systémy
Všechny části core systémů budou provozovány operačních systémech RedHat (Brána/Prod, Archiv/Prod).a CentOS(pro systémy Badatelna Prod+Test). Systém Windows Server 2019 bude použit pro Digitalizaci Prod+Test (DMS), a proxy server.

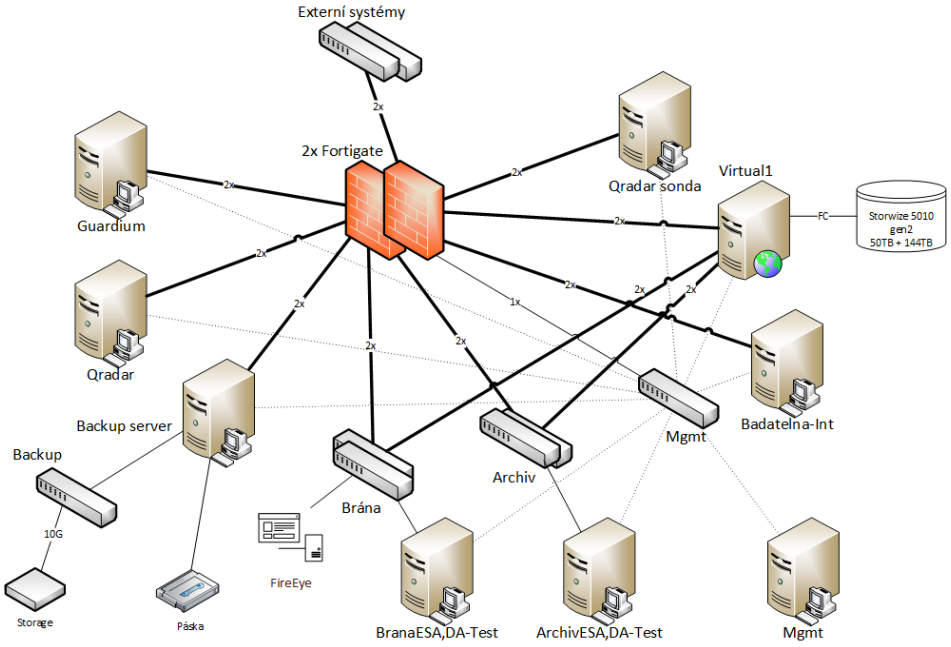
Digitalizační linka (DMS) bude zajišťovat prostřednictvím komponenty Datacap (modul Digitalizační linka) potřebné napojení zpracovávaných (skenovaných) dokumentů na interface Brány pro následné uložení do prostředí Archivu. Proto, aby mohl být dokument zpracován, bude muset projít kontrolou v rámci karantény. Aby byla zajištěna vyšší ochrana prostředí DA, bude použita dvoufázová kontrola dokumentů. Jednak v prostředí FireEye, tak i v prostředí v FortiSandbox, které je integrální součástí ochrany dat s technologií Fortigate. V rámci spojení těchto technologií, dostává Zadavatel k dispozici nástroj pro široké využití (více v odkazu níže na konci upřesnění pro tuto otázku). FortiSandbox je provozován jako virtual appliance, která nepotřebuje licencovat vlastní OS. Její napojení a zvýšení ochrany a bezpečnosti prostředí DA je popsáno níže. (viz upřesnění Dotaz č.4 bod 92)
Pro navýšení konektivity a kapacity propustnosti (16xGb RJ45 + 8xSFP) bude nasazen nový pár firewallů Fortigate v lokalitě Praha. Tento pár firewallů umožní rozšíření a důsledné oddělení jednotlivých segmentů sítě. Propustnost těchto firewallů je více než 2x vyšší a v některých parametrech dokonce až 3x vyšší než u stávajících.

Níže Účastník uvádí očekávané kroky při nasazení (seznam aktivit ani posloupnost není vyčerpávající a pouze dokresluje navrhovaný postup prací, který bude upřesněn během případného kick-off-u):

a. Analýza stavu prostředků v obou lokalitách
b. Práce na Analýze nasazení DA MO
c. Rozšíření diskových storages
d. Implementace a nasazeni firewall a sandboxů v lokalitě Praha a Olomouci
e. Nasazení virtuálního prostředí
f. Migrace do virtuálního prostředí a integrace s bezpečnostními technologiemi
g. Ověření nastavení jednotlivých komponent a jejich komunikace
h. Akceptace analýzy
i. Nasazení systému DA MO, včetně DR lokality
j. Kontrola nastavení jednotlivých funkcionalit
k. Nastavení replikací
l. Nastavení recovery
m. Migrace dat
n. Nasazení ELZA
o. Testování

Lokalita Praha

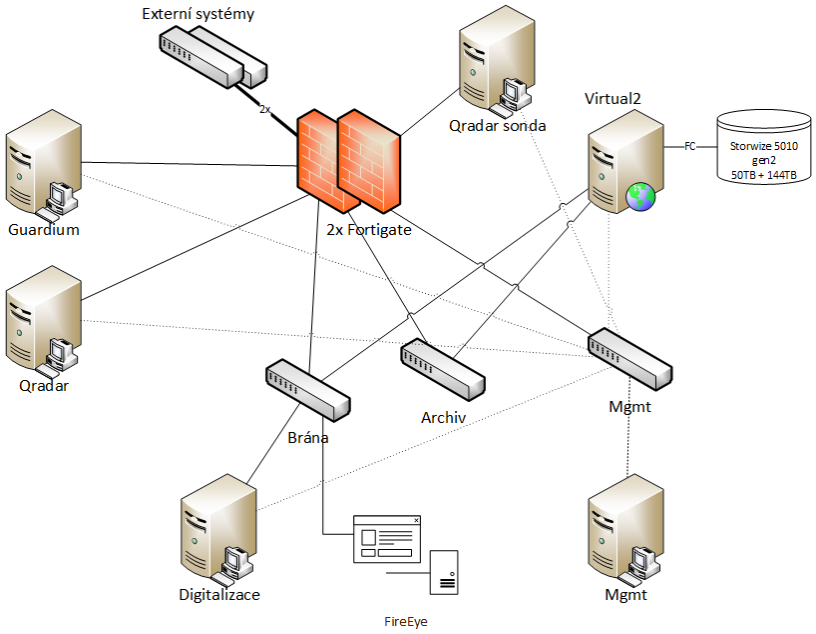
Přepokládané zapojení základních infrastrukturních komponent, je uvedeno níže v HLD (High Level Design). Návrh této topologie by měl být dodržen pro zajištění segmentace a ochrany jednotlivých částí systému ESA a DA. (případně může být komunikace Test prostředí oddělena od prostředí Produkce, tak aby byla komunikace řízena firewallem).



Obrázek základního návrhu topologie sítě nasazení systému DA MO s využitím komponent ESA MO v lokalitě Praha

Lokalita Olomouc

V lokalitě Olomouc budou do virtuálního prostředí zmigrovány servery Brána (ESA)/DR a server Archiv (ESA)/DR. Zapojením virtuálního serveru (Virtual2) a po migraci serverů, bude možné zajistit konektivitu ze storage a tím poskytnout serverům dodatečnou diskovou kapacitu a dokončit tak nastavení záložní lokality pro systém DA včetně replikací z primární lokality. Zároveň bude možné lépe řešit přidělování zdrojů (specificky pro Portál Badatelny). Firewally zůstanou v lokalitě Olomouc identické, pouze se ze stávajících FW (v Praze) použijí moduly, aby se doplnili Gbic a bylo tak možné rozšířit možnosti připojení jednotlivých komponent v Olomouci. Opět platí, pravidlo, že při přesunu majetku budeme vyžadovat potvrzení a instrukce Zadavatele (součást analýzy).



Obrázek základního návrhu topologie sítě nasazení systému DA MO s využitím komponent ESA MO v lokalitě Olomouc

3. Dotaz č. 3 (Legislativní a normativní požadavky)

3.1 Dotaz či požadavek zadavatele na objasnění

Legislativní a normativní požadavky – nabídce účastníka chybí uvedení dalších platných zákonů, které musí řešení splnit. Jedná se minimálně o zákon č. 250/2017 Sb., o elektronické identifikaci a zákon č. 12/2020 Sb., o právu na digitální služby. Zadavatel žádá o potvrzení, že nabízený návrh řešení plní i tyto aktuálně platné zákony.

3.2 Objasnění účastníka IBM

Účastník potvrzuje, že řešení splní požadavky zákonů 250/2017 Sb., o elektronické identifikaci a zákon č. 12/2020 Sb., o právu na digitální služby.

Nad rámec výše uvedeného si Účastník dovoluje upozornit na následující skutečnosti::

- splnění požadavků zákona 250/2017 Sb. je nabídce již obsaženo, a to v kapitole 2.1 „Legislativní a normativní požadavky“ a znovu (bez citace čísla zákona) v kapitole 2.3 „Migrace“. Citace: „Do veřejné části je umožněn přístup laické i odborné veřejnosti, a to buď anonymní nebo autorizované (na základě registrace, případně ověření přes MojeID nebo NIA).“
- požadavek na splnění zákona 12/2020 Sb., o právu na digitální služby nebyl dle názoru uchazeče v zadávací dokumentaci ani v tabulce pro posouzení nabídek Zadavatelem explicitně zmíněn.

4. Dotaz č. 4 (Tabulka pro posouzení nabídek – 8 bodů)

4.1 Dotaz či požadavek zadavatele na objasnění

V tabulce pro posouzení nabídek účastníka (příloha č. 3 nabídky) je deklarováno splnění všech požadavků s odkazem na příslušné kapitoly návrhu. V uvedených kapitolách ale není zadavatel schopen ověřit způsob řešení minimálně následujících požadavků:

- č. 6 „Řešení umožňuje příjem vstupních dat včetně archivních balíčků, jejich prověření v rámci karantény, dlouhodobé uložení a opětovné poskytnutí archiválií oprávněným žadatelům."

- č. 20 „Řešení umožňuje poskytnutí archiválie ve formě výstupního DIP balíčku jako důkazního materiálu."

- č. 37 „Vyhledané archiválie je možné zpřístupnit prostřednictvím Portálu DA MO, který slouží pro dočasné zpřístupnění kopie archivovaného dokumentu oprávněným (ztotožněným) osobám v režimu pouze pro čtení."

- č. 39 „V rámci Badatelského portálu je zaznamenávána činnost ztotožněného uživatele s vyžádanou poskytnutou kopií archiválie. Údaje jsou zapisovány do badatelského listu."

- č. 74 „Zabezpečení dat před změnou – úložiště garantuje, že uložená data nemohou být uživatelským zásahem smazána ani nijak pozměněna (retence). Výjimkou je archivářem naplánovaná a provedená výběrová skartace."

- č. 92 „Řešení provádí dynamickou analýzu souborů ve virtuálním prostředí (sandbox) jako součást přizpůsobeného hypervisorového frameworku, který je speciálně vytvořen pro účely bezpečnostní analýzy a který není založen na standardním / komerčním hypervisoru, aby se zabránilo detekci sandboxu."

- č. 108 „Řešení umožňuje zamezení stažení definovaných souborů koncovým uživatelem na jeho pracovní stanici, takový soubor musí být možné pouze prohlížet v integrovaném prohlížeči dokumentů v rámci internetového prohlížeče."

- č. 110 „V případě výpadku jakékoliv bezpečnostní komponenty v systému není narušena dostupnost služeb."

Zadavatel žádá účastníka o konkretizaci a detailní popis návrhu řešení v jednotlivých výše uvedených bodech takovým způsobem, aby byl zadavatel schopen ověřit, že návrh řešení dodavatele tyto požadavky skutečně splní.

4.2 Objasnění účastníka IBM

K bodu č. 6 Účastník upřesňuje:

Příjem vstupních dat včetně archivních balíčků je možný několika způsoby.

- Ruční vložení pracovníkem archivu. Na bráně bude dostupný webový klient, který umožní ruční vložení dokumentu ve formě SIP balíčku nebo vložením obsahu a doplněním metadat ve formuláři.
- Integrační API pro vstup dokumentů ze skenovací linky a dalších externích systémů. API bude založeno na WS SOAP a REST.

Každý vložený dokument projde automaticky:

- Ověřením metadat, tedy kontrolou, že obsahuje povinná metadata.
- Kontrolou a elektronických podpisů a razítek.
- Předáním dokumentu ke kontrole v karanténě. Toto je asynchronní proces. Karanténa je samostatná služba.

Pokud dokument úspěšně projde všemi kontrolami, bude předán z Brány do Archivu, kde bude trvale uložen. Archiv obsahuje služby, které zajistí přerazítkování a další úkony potřebné pro dlouhodobé uložení dokumentu.

Pokud dokument neprojde kontrolami, Brána odešle chybovou odpověď pomocí API a dokument zařadí do chybové fronty. Přístup k seznamu dokumentů bude v klientské aplikaci pro archiváře.

Opětovné poskytnutí archiválií oprávněným žadatelům probíhá přes Badatelský portál.

Z Archivu přes API Brány pomocí služby pro komunikaci s Badatelským portálem bude pravidelně aktualizovaný seznam archiválií, sadu metadat a náhledem. Uživatelé Badatelského portálu mohou pomocí těchto metadat vyhledat dokument a požádat o jeho zpřístupnění. Požadavek předá Badatelský portál na Bránu, která spustí proces zpřístupnění archiválie. V rámci tohoto procesu proběhne v Archivu automatické vytvoření náhledu dokumentu. Pokud bude potřeba, proběhne jeho anonymizace a následně je dokument předán prostřednictvím Brány Badatelskému Portálu. Badatelský Portál zpřístupní daný dokument pouze oprávněnému žadateli. Badatelský Portál bude pomocí API předávat na Bránu aktualizace badatelského listu pro daný dokument. Služba Brány předá aktualizovaný badatelský list Archivu, který jej uloží k příslušnému dokumentu.

Archiváři mohou k dokumentům přistupovat klientskou aplikací na Bráně. Klientská aplikace Brány zobrazí dokumenty z Archivu podle přístupových práv, vždy pouze ke čtení. Změny v dokumentech budou možné pouze v rámci změnových procesů.

Třetí způsob přístupu k archiváliím bude pomocí klienta Archivu. Uživatel musí být zaveden v interním LDAP Archivu, aby měl do této aplikace přístup. Zde může nahlížet na dokumenty uložené v Archivu. Vlastnosti dokumentu, jejichž změna by zneplatnila elektronické podpisy a časová razítka budou pouze ke čtení. Ostatní vlastnosti a propojené objekty, jako například anonymizované náhledy budou přístupné podle přístupových práv.

K bodu č. 20 Účastník upřesňuje:

Pro vygenerování DIP balíčku jako důkazního materiálu má DA MO samostatnou službu. Přístup k této službě je pro archiváře pomocí klientské aplikace na bráně.

Služba zajistí, aby DIP balíček obsahoval veškerá data potřebná k ověření dokumentu. Kromě podpisů a razítek zajistí služba i uložení všech certifikátů včetně historických.

Službu je možné volat i z workflow, může být začleněna i do automatických procesů. Aplikace umožní podat žádost o vydání a po schválení archivářem, bude-li potřeba, vygeneruje DIP balíček.

K bodu č. 37 Účastník upřesňuje:

V kapitole 2.2.4.1 Interní část je popsaná práce administrátorů, je zde uvedena možnost zobrazení seznamu dávek k zpřístupnění a také zobrazení detailu dávky. Pomocí tohoto mechanismu dochází ke zpřístupnění archiválie, a to procesem řízeným administrátorem a prostřednictvím Portálu DA MO. Upřesňujeme, že veškerá data prezentovaná badatelům (anonymním, registrovaným i ztotožněným) jsou vždy v režimu jen pro čtení (tento fakt vychází z vlastností architektury systému, proto jsme ho explicitně neuváděli). Řešení, mimo aktualizaci badatelských listů, nedovoluje tok dat z komponenty Portálu do ostatních částí systému (tímto je zabráněno neoprávněnému pozměňování dokumentů).

Dále je uvedeno v kapitole 2.2.4.2., že je v Portálu Badatelny, je poskytnuta kopie archiválie

Ke zpřístupnění dokumentů pro Portál DA MO složí samostatná služba na Bráně. Ta pomocí API zprostředkuje předání náhledu dokumentu z Archivu na Portál. Portál si dokument vyžádá voláním API funkce. Služba dokument vyhledá v archivu, vytvoří náhled dokumentu, a pokud je potřeba, vyžádá si anonymizaci obsahu u archiváře. Anonymizaci provede Archivář v klientské aplikaci na Bráně.

Portál dostane vybraná metadata k dokumentům v archivu spolu s náhledem. Pomocí těchto metadat bude možné dokumenty vyhledat v rámci Portálu a požádat o zpřístupnění.

K bodu č. 39 Účastník upřesňuje:

Zde poukazujeme zejména na formulaci "Badatelský portál pro jednotlivá bádání (a badatele) předává informace do Badatelského listu, který je veden v Archivu" v závěru kapitoly 2.2.4.2

Zároveň uvádíme, že na Bráně běží služba pro komunikaci s Portálem. Ta pomocí API volání bude přijímat aktualizace badatelského listu. Tyto informace uloží do Badatelského listu v Archivu a propojí s příslušnou archiválií.

K bodu č. 74 Účastník upřesňuje:

FileNet je vhodný nástroj pro vývoj, implementace, udržování a podporu důvěryhodných úložišť v souladu s požadavky normy ISO 16363:12, zákonem č.499/2004 Sb., vyhláškou č.259/2012 Sb., zákonem č. 227/2000 Sb. a normou ISO/IES 9126-1. Řešení DAMO rozšiřuje stávající systém ESA, využitý dle zadávací dokumentace – příloha č.1, kapitola 16 a u systému ESA byla garance deklarována.

Jako systém pro důvěryhodné úložiště podporuje definované intervaly, po které je garantováno, že uložený dokument nemůže být uživatelským zásahem smazán ani nijak pozměněn. Tato doba není ovlivnitelná vnějším zásahem, např. zásahem do systémového času.

V Archivu jsou dokumenty uloženy společně s časovým razítkem. Časové razítko má časově omezenou platnost, proto na straně Archivu běží služba, která automaticky vyhledá dokumenty, kterým se blíží vypršení platnosti časového razítka a tyto dokumenty přerazítkuje. Přerazítkování znamená vytvoření nového časového razítka, které zajistí důvěryhodnost dokumentu i po vypršení platnosti předchozího časového razítka.

Díky tomu je kdykoli možné ověřit, že obsah dokumentu nebyl změněn.

Aby se zabránilo neoprávněné manipulaci se systémovými hodinami, jsou místní systémové hodiny pravidelně porovnávány s hodinami RDBMS.

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcb010.htm

Při vytváření DIP balíčku jsou veškerá data, podpisy, časová razítka a certifikáty připojeny, aby bylo možné ověřit platnost všech podpisů, certifikátů i časových razítek.

Detailní popis nastavení rolí a oprávnění je uveden v upřesnění na dotaz č.105.

K bodu č. 92 Účastník upřesňuje:

Účastník v kap. 2.5.1. Vlastnosti karantény uvedl – „Navrhované řešení je velice flexibilní v rámci konfigurace virtuálního stroje, kde je možné instalovat a konfigurovat různé aplikace, včetně specifických aplikací Nabyvatele případně aplikací třetích stran.“, dále pak "Vlastní testovací prostředí běží ve specifickém framework, v kterém je provozován vlastní sandbox. Tím je zajištěna vlastní bezpečnost a nemožnost kompromitace vlastního prostředí karantény, neboť pro odeslání do takto připraveného prostředí jsou připravené činnosti, které nemohou vlastní firmware zařízení kompromitovat ani detekovat, čímž se eliminuje možnost odhalení běhu ve vnitřním prostředí karantény."

Dále pak Účastník v rámci stejné kapitoly uvedl, že „Pro prostředí VHA však budou použity již vestavěné a customizované images, které používá i ESA MO nad technologií, která naplňuje požadavky pro takové využití.“

Pro upřesnění Účastník dále uvádí, že systém karantény bude složen ze dvou nezávislých zařízení. Pro zvýšení ochrany prostředí DA bude společně s novými firewally nasazena i technologie sandboxingu, která umožňuje lépe chránit obsah a být zároveň integrální součástí firewallu. (v případě lokality Olomouc musí dojít k upgrade firmware). Systém FireEye poskytuje dostatečný výkon, a patentovaný engine, patří stále mezi špičku v oboru, nicméně jiný přístup od jiného dodavatele přináší systému DA významnou přidanou hodnotu. Proto je pro testování souborů navrženo vícestupňové řešení, s použitím stávající karantény založené na technologii FireEye FX (s již vestavěnými images), které je provozováno aktuálně v prostředí ESA MO a zároveň jako další kontrola, nad technologií FortiSandbox, která zajistí co nejvěrnější testování a nastavení, odpovídající prostředí koncové stanice u Zadavatele (customizované images). Tato běží ve virtuálním prostředí. Díky možnostem instalovat a konfigurovat vlastní image, je zajištěna široká konfigurovatelnost prostředí. (podpora operačních systémů od WinXP až po Win10, Mac OS, různé aplikace, nastavení prostředí). Pro předání dokumentu do Archivu, budou muset obě zařízení poskytnout kladný výsledek testování.

Kombinací těchto zařízení je zajištěna vyšší míra ochrany, neboť testování bude probíhat na různých prostředích s různými nastaveními a každá technologie přináší jiný pohled a použití jiných patentovaných technologií (engines), prostřednictvím, kterých budou archiválie testovány. FireEye MVX (MultiVector Virtual Execution) – patentované prostředí, které je provozováno nad hypervisor frameworku, který je pro účelu sandboxingu vyvinut.

Obě technologie disponují integračními možnostmi použití sdílených složek, detailním reportingem a dalšími funkcemi pro vyhodnocování malware. Zároveň se nabízí i možnost, jak nově nasazenou technologii snadno, a rychle integrovat se systémem ESA.

Detailní popis integrace bude součástí analýzy (např. paralelní zpracování nebo zpracování v rámci zřetězení, uvedení verzí operačních systémů a aplikací pro úpravu testovací image).

Proces testování:

Karanténa si převezme k testování ze sdílené složky dokumenty v části Brány a podrobuje je jednotlivě behaviorální analýze. Vlastní testování dokumentů v rámci behaviorální analýzy probíhá kompletně v prostředí zařízení (karanténa = FireEye + Fortisandbox), které je umístěno v prostředí Zadavatele, tj. neprovádí se zasílání testovaných dokumentů do cloudu pro účely tohoto testování. Po skončení analýzy je dokument uložen do jedné z výstupních složek na základě výsledku analýzy.:

Výstupní složky jsou dále zpracovávány v rámci procesu **Chyba! Nenalezen zdroj odkazů.**. Dokumenty, u kterých je detekována potenciální hrozba, jsou vyřazeny ze standardního zpracování a za jejich zpracování je zodpovědný určený pracovník, který proces vstupu a zpracování dokumentů řídí. Z výstupních složek si přebírá dokumenty FileNet k dalšímu zpracování.

Vyřazení dokumentů:

Dokumenty, u nichž je detekována potenciální hrozba (kontrola na malware), jsou ze strany karantény umístěny do výstupní složky, která je pro tyto účely určena a vlastní dokumenty tím jsou vyřazeny ze standardního zpracování. Proces dalšího zpracování těchto dokumentů je na pracovníkovi, který je zodpovědný za tento proces a práci s archiválií.

Proces Automatický vstup dokumentu:

Jedná se o proces, který přijme dokument z libovolného podporovaného vstupu, tedy dle požadavku ze skeneru souborového systému nebo webových služeb SOAP a REST. Skener souborového systému vybírá postupně z definované složky soubory a metadata (soubor s koncovkou XML se shodným názvem jako má vlastní soubor).

Po přijetí dokumentu se provedou požadované kontroly (jejich definice bude součástí analýzy).

Dokument, který vyhoví všem požadavkům a všem kontrolám, je automaticky předán do archivu a zde je zařazen do archivního balíčku.

Dokumenty, které nevyhoví, jsou uloženy do dočasného prostoru a jejich další zpracování provádí Archivář.

Podrobné výsledky testů behaviorální analýzy testovaných dokumentů jsou dostupné v prostředí administrační konzole karantény, která je dostupná přes webové zabezpečené rozhraní v prohlížeči uživatele.

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/fireeye-fx-series.pdf

K bodu č. 108 Účastník upřesňuje:

Pro prohlížení dokumentů v požadovaných formátech obsahuje FileNet klient prohlížeč DaejaView. Prohlížeč DaejaView běží v rámci internetového prohlížeče a umožňuje prohlížet dokumenty bez stažení souboru na disk počítače a bez nutnosti mít na klientském počítači nainstalované další aplikace (např Word, Excel, pdf prohlížeč…). Prohlížeč je možné nastavit pro konkrétní potřeby, aby nabízel různé funkce. Např. pro různé situace lze povolit prohlížení dokumentů, tvorbu anotací a podobně.

https://www.ibm.com/support/pages/ibm-daeja-viewone-507-release-notes

K bodu č. 110 Účastník upřesňuje:

Účastník uvádí, že bezpečnostní komponenty, které jsou použity v rámci systému DA MO, jsou provozovány buď v režimu vysoké dostupnosti nebo jejich výpadek nemá dopad na celkovou dostupnost služeb. Firewall je na obou lokalitách provozován ve vysoké dostupnosti. Výpadky ostatních komponent jako je karanténa, integrity-control, ips agenti, QRadar SIEM, QRadar Qflow sonda nebo Guardium, nemají vliv na dostupnost služeb poskytovaných systémem DA MO. V rámci výpadu karantény (obou boxů nebo jednoho) dojde k dočasnému ukládání dokumentů na Bráně, nicméně služby jsou dostupné a jak Archivář, tak i ostatní pracovníci mohou pracovat a dokumenty dočasně zůstávají uloženy na komponentě Bráně, dokud nebude karanténa opět v provozu.

5. Dotaz č. 5 (Tabulka pro posouzení nabídek – 10 bodů)

5.1 Dotaz či požadavek zadavatele na objasnění

U následujících požadavků tabulky pro posouzení nabídek žádá zadavatel o doplnění detailního popisu návrhu řešení, protože text nabídky je v těchto částech nedostatečný a neodpovídá požadavku bodu B. 7. zadávací dokumentace:

- č. 46 – v kap. 2.2.1.4. je sice popsáno výchozí znění požadavku, ale příklad politik ukládání již uveden není.

- č. 70 – v kap. 2.2 je sice naplnění požadavku na RTO potvrzeno, nicméně žádné požadované časy garantovány nejsou, navíc je uvedeno, že pro replikace budou použity technologie poskytované nabyvatelem, případně rsync a nativní replikace DB2, což podle zkušenosti zadavatele z projektu ESA MO nefunguje tak, jak by mělo a bylo záměrem tohoto projektu. Zadavatel žádá o doplnění detailního popisu návrhu řešení a garanci funkčnosti a požadovaných časů přechodu a obnovy dat s podrobným popisem, jak budou současné problémy z ESA napraveny novým způsobem řešení pro DA MO.

- č. 73 – v kap. 2.2 ani v 2.2.1.4 není popsán způsob řešení požadavku, aby k vyloučení možnosti ztráty dat nebylo potřeba provádět zálohy uložených dat.

- č. 76 – v kap. 2.2.1.4 je sice popsána možnost rozšíření pole, ale pole se již nevyrábí a je tedy do budoucna diskutabilní, jak dlouho bude možné rozšíření/upgrade provádět.

- č. 78 – v kap. 2.2 je požadavek replikace popsán nedostatečně, platí stejná připomínka jako k požadavku č. 70 – splnění tohoto požadavku je z ohledem na zkušenosti z projektu ESA MO nejisté a zadavatel tak požaduje detailní popis nového řešení, aby si ověřil, že splnění požadavku je možné důvěřovat.

- č. 82 – v kap. 2.2.1.4 je splnění tohoto požadavku popsáno jen velmi obecně. S ohledem na fakt, že se úložiště již nevyrábí, bude cena na jeho provoz do budoucna naopak stoupat.

- č. 84, 85, 86 – řešení popsané v kapitolách 2.2.2.2, 2.5.1 a 2.2.1.4 se odvolává na stávající řešení v ESA MO. Nedá se dovodit, zda bude navržené řešení plně funkční dle hodnotících požadavků.

- č. 103 – v kap. 2.2 ani 2.5 není způsob řešení požadavku pomocí samostatné HW sondy popsán.

- č. 104 – v kap. 2.6.2 není způsob řešení požadavku podrobně popsán, detailní řešení je odkázáno na předimplementační analýzu.

- č. 105 – v kap. 2.2.1.2 je ověření identity uživatele potvrzeno, nicméně způsob řešení souvisejících podbodů požadavku již není v kap. 2.2.1.1. popsán.

5.2 Objasnění účastníka IBM

K bodu č. 46 Účastník upřesňuje:

FileNet nabízí pro ukládání obsahu dokumentů více možností:

- Database and file storage - ukládá data na diskové úložiště a do databáze.
- Fixed storage areas - externí ne FileNetové úložiště, které zodpovídá za ukládání a retenci.
- Advanced Area Storage - kombinuje několik typů ukládání.
- Replication - s využitím Advanced Area Storage je možné replikovat data na několik cílových úložišť. Detailní popis funkcionality je uveden v upřesnění na dotaz č.70, resp. č.71 (viz níže)

Ve FileNetu lze určit na úrovni jednotlivých dokumentů, na které úložiště bude uložen jeho obsah. Přesun může být spuštěn Sweep jobem, Workflow nebo Administrátorem.

V rámci nasazení s využitím replikací se používá kombinace Fixed storage areas a Advanced Storage areas. Nastavení ukládání obsahu lze přesunout i na běžícím systému. Přesunutí obsahu neovlivní dostupnost dokumentů z pohledu uživatele. Detailní popis bude uveden v rámci analýzy.

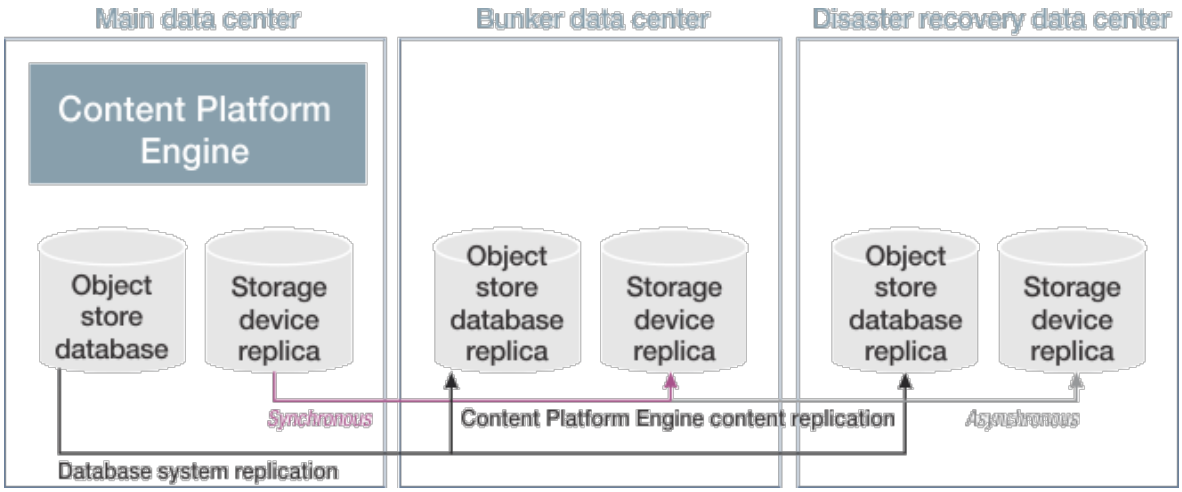
FileNet je komponenta modulu Brána a modulu Archiv nabízí široké možnosti pro práci s obsahem a místem jeho uložení:

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcb000.htm

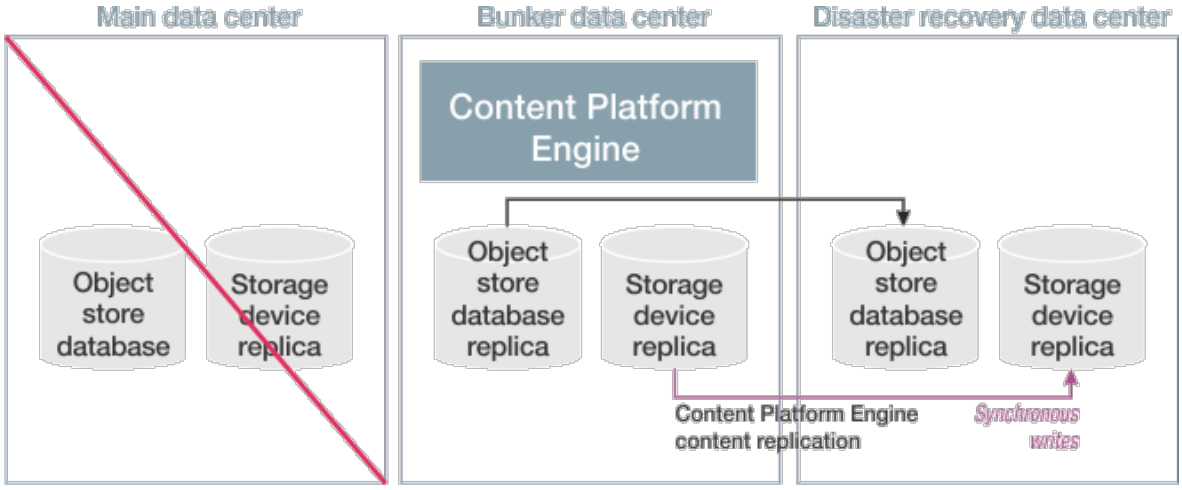
K bodu č. 70 Účastník upřesňuje:

Účastník předpokládá, že dotaz se týkal bodu 71. Proto uvádí, že v otázce replikace dat na jednotlivé storages je Účastník připraven použít vestavěnou technologii přímo určenou pro práci s daty napříč lokalitami, kterou software FileNet disponuje. Jedná se o komponentu a funkcionalitu Advanced Storage Area. Tato funkcionalita je schopna na pozadí replikovat data napříč téměř jakýmkoliv úložišti.

Tyto pokročilé funkce pro práci s úložišti jsou navrženy tak, aby byly dostatečně flexibilní pro podporu široké škály replikačních modelů, včetně následujících běžných režimů: tradiční vysoká dostupnost/zotavení po havárii, vzdálená lokalita a úložiště v síti. Pomocí konzoly pro správu pro Content Platform Engine může správce konfigurovat modely replikace. Nicméně pomocí konzoly pro správu pro Content Platform Engine může správce konfigurovat běžné i vlastní modely replikace. Níže je uveden příklad standardního nasazení, který by mělo být možné nasadit i v prostředí Zadavatele. Jedna primární lokalitě a následná replika v lokalitě vzdálené. Účastník předpokládá, že detail nasazení bude popsán v Analýze.

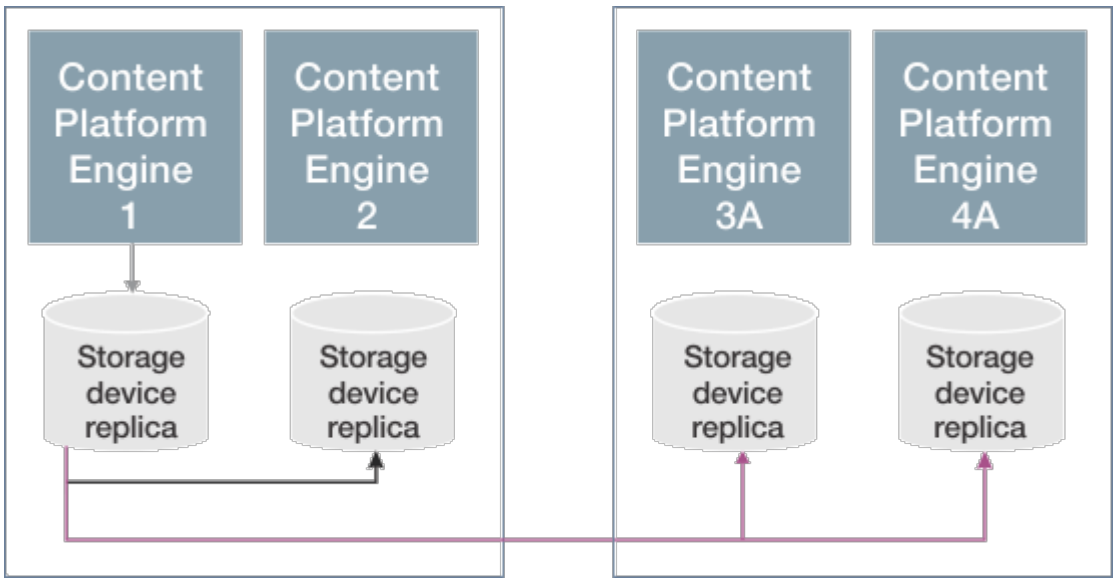


Příklad nastavení repliky v rámci nasazení HA a zároveň lokality DR.



Příklad jak zafunguje replikace v případě výpadku

Jedním z dalších modelových příkladů je model replikace do vzdálené sítě pouze pro obsah (content). Rozšiřuje tím model s vysokou dostupností nebo zotavením po havárii, přidáním podpory replikace z a do vzdálené lokality z primární repliky. Obsah je nejdříve synchronně zapsán v lokální síti jako replika2 (Content Platform Engine 1 a 2) a asynchronně zapsán na vzdálenou lokalitu (Content Platform Engine 3A a 4A).



Příklad repliky v lokální síti a zároveň ve vzdálené lokalitě

Nastavení konfigurace replikace lokality se provádí v prostředí Filenet Content Manager, v části, Object Storage, kde lze nastavení provézt. Pro ilustraci zde uvádíme postup.

Otevřete oblast úložiště (Object storage), kterou chcete nakonfigurovat (prostředí Filenet Content Manager):

- *Ve stromovém zobrazení klikněte na Úložiště objektů (Object Store) > zvolte název úložiště objektů (object store name) a otevřete úložiště objektů, které zařízení používá.*
- *Ve stromové struktuře zobrazení klikněte pravým tlačítkem myši na položku Správce (Administrative) > úložiště (Storage) > rozšířeného úložiště (Advanced Storage) > rozšířené oblasti úložiště (Advanced Storage Area) > zvolte název oblasti úložiště a klikněte na otevřít. (storage area name – open)*

Na kartě Zařízení (Device tab) nastavte výchozí hodnotu typu synchronizace (Default sync type) pro každou lokalitu, která přistupuje k rozšířené oblasti úložiště. (Advanced Storage Area).

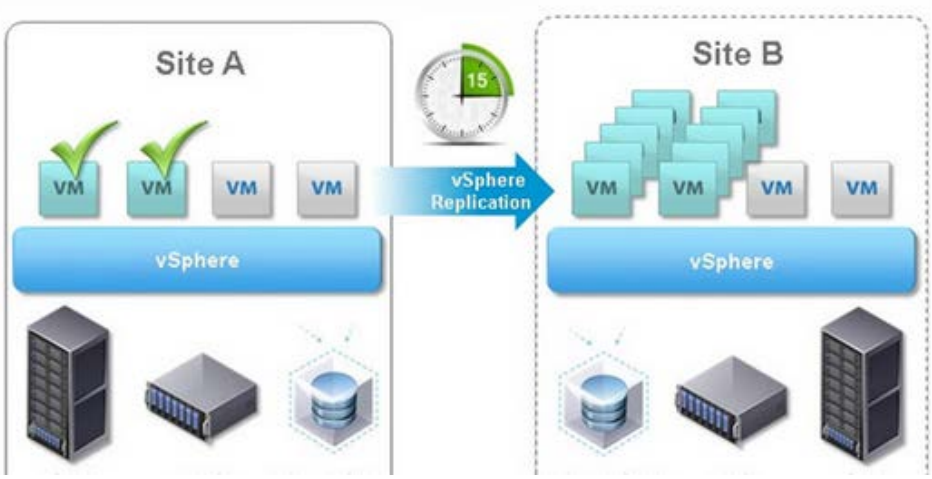
Podle potřeby nastavte hodnotu názvu lokality typu Synchronizace replik pro každou lokalitu. (Default Synch type site name)

Ve výchozím nastavení používá každá lokalita typ, který jste nastavili pro výchozí typ synchronizace.

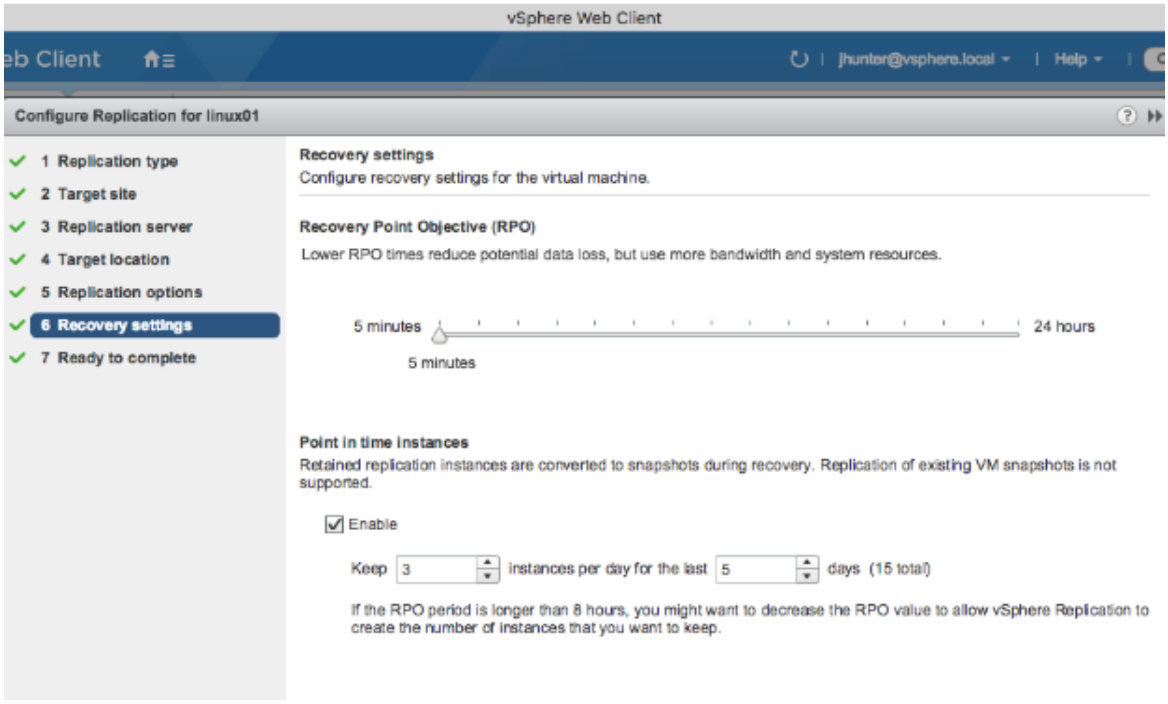
- *Chcete-li přepsat typ synchronizace pro konkrétní lokalitu, nastavte hodnotu pro konkrétní lokalitu, dle Vaší volby.*
- *Chcete-li odebrat přepsání pro konkrétní lokalitu, nastavte hodnotu pro konkrétní lokalitu na Výchozí použití. (Use default),*

Další technologií, která bude použita pro replikaci do vzdálené lokality bude použito funkcionality prostředků VMWARE, jež umožňuje vytvoření repliky daného VM do vzdálené lokality i přes nekvalitní nebo pomalé linky. Funkce vReplication je hluboce integrovaná součást technologií VMware. Jedná se o robustní replikační nástroj virtuálního prostředí založený na VMWARE hypervizoru. Změněná data na discích virtuálních strojů

pro běžící virtuální stroj na primární lokalitě se odesílají na sekundární server na vzdálené lokalitě. Tam se změny zapisují na disky virtuálního počítače jako offline kopie (repliky) virtuálního počítače.



Po dokončení počáteční (první) úplné synchronizace prostřednictvím vReplication se již přenášejí pouze změněná data. Jádro této technologie sleduje jedinečné zápisy do chráněných virtuálních počítačů a identifikuje a replikuje pouze ty bloky, které se mezi cykly replikace změnily. To udržuje síťový provoz na minimu a umožňuje nastavení velmi nízkého času RPO až v řádu jednotek minut. Tzn, že i přes nekvalitní linku je technologie schopna do jedné hodiny přenést změny, tak, aby byly zajištěny požadované časy na RTO a RPO Zadavatelem.



Tímto Účastník garantuje, že budou dodrženy časy RTO a RPO, tak jak Zadavatel požaduje v rámci ZD. S použití technologií Filenet Advanced Storage Area a VMWARE (vReplication) zajistí dodržení požadovaných parametrů (RTO-12hod, RPO-1h).

Detailní popis je uveden na stránkách výrobce:

Vytvoření Advanced Storage Area

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc254.htm

Popis replikačních mechanismů a existence funkcionality přímo ve FileNet technologii

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc223.htm

Popis funkcionality vReplication

https://www.vmware.com/cz/products/vsphere/replication.html

(V rámci replikace DB2 nemá Účastník žádné informace, které by naznačovaly, že replikace není funkční. Naopak při pravidelných profylaxích bylo ověřeno, že replikace je funkční a zcela validní.)

K bodu č. 73 Účastník upřesňuje:

Základním předpokladem proto, aby nebylo nutné provádět zálohy uložené na vlastní Storage, což může být náročné, jak časově, tak i výkonnostně, je provádění replikací. Jakým způsobem bude Účastník řešení schopen dosáhnout replikací je popsáno v odpovědi na bod číslo 70, resp. 71. Variabilita a nastavení replikací je nativní funkcionalitou technologie FileNet a tato bude pro tyto účely použita. Detailní popis, jak funguje Advanced Storage Area, jaké jsou možnosti nastavení a jak se replikace nastavuje je uvedeno v upřesnění, viz bod výše. Zároveň bude Účastník nasazovat nové technologie v rámci virtuální infrastruktury (vReplication, vData Protection), které jsou schopné pomoci s replikací prostřednictvím nekvalitních nebo pomalých linek.

K bodu č. 76 Účastník upřesňuje:

Řadič diskového pole (Storwize V5010) sice již není v prodeji, nicméně tento řadič je kompatibilní pro rozšíření o nový typ expanzních jednotek (IBM FlashSystem 5100 LFF Expanzion, M/T 2078-12G) s aktuálními typy disků, což je také předmětem nabízeného rozšíření. Diskové pole s instalovaným řadičem tedy bude možné i v budoucnu rozšiřovat ve stejném časovém horizontu jako aktuální řadiče diskových polí IBM, tj. minimálně po dobu smluvního vztahu dle zadávací dokumentace na DA MO.

K bodu č. 78 Účastník upřesňuje:

Účastník předpokládá, že dotaz se týkal bodu 71.

Informace týkající se replikace jsou uvedeny v upřesnění k bodu č.70 výše.

K bodu č. 82 Účastník upřesňuje:

V odpovědi na dotaz k bodu č. 76 výše Účastník uvádí informace o možnosti rozšíření stávajících diskových polí a potvrzuje, že tato rozšíření bude možné realizovat po celou dobu smluvního vztahu dle zadávací dokumentace na DA MO.

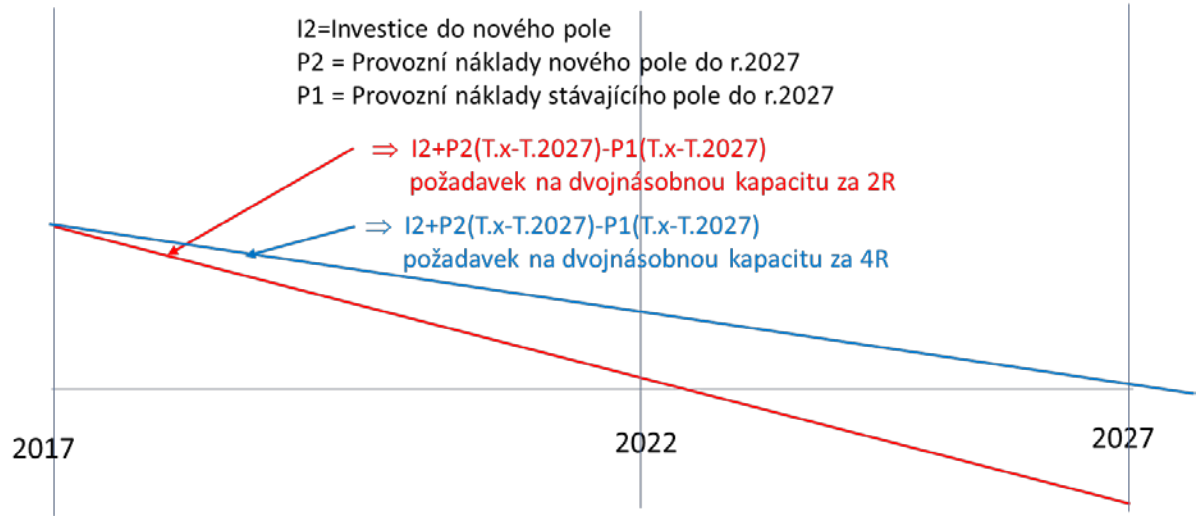
V rámci využití investic do předmětného diskového pole (které je v současnosti v provozu), spolu s uvažovanými náklady na jeho provoz, je ekonomicky optimální doba obměny

diskového pole závislá na míře zvyšování požadavků ne jejich kapacitu – viz níže uvedený graf.

Optimální doba výměny závisí především na:

- Požadavcích na zvyšování kapacit datového úložiště
- Požadavcích na zvyšování výkonnosti I/O operací
- Požadavcích na virtualzaci
- Nových požadavcích na řízení a podporu DR u diskového pole

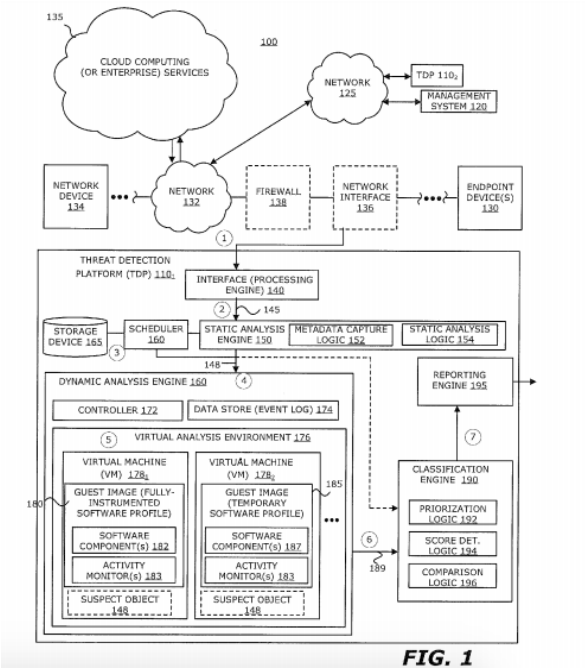
Na níže uvedeném grafu je znázorněna obvyklá ekonomická rozvaha optimální doby výměny technologie diskových polí v závislosti na požadavcích zvyšování kapacity. Pro dvojnásobné zvýšení kapacity během každých 2 let je to cca rok 2023; pro zvýšení kapacity během každých 4 let je to cca rok 2028.



K bodům č. 84,85,86 Účastník upřesňuje:

Účastník v rámci kapitoly 2.5., resp. 2.5.1 uvedl popis a v rámci doplnění dotazu č.92 upřesnil postup jak bude testování prováděno. Zároveň v rámci upřesnění uvedl, jak jsou naplněny požadavky výše uvedených bodů. Níže Účastník upřesňuje, že testování chování dokumentů probíhá v rámci statické i tzv. dynamické analýzy (viz obrázek níže). Právě technologie Fortisandbox od společnosti Fortinet má tyto analýzy (jejich postupy) patentované. Testování v zařízení od společnosti FireEye probíhá také v patentované technologii MVX (MultiVector-Virtual Execution), tak aby provedená behaviorální analýza, byla co nejefektivnější. Pro každý testovaný dokument je spuštěna nová instance „čistého“ virtuálního stroje, aby bylo zamezeno ovlivnění případné detekce malware předchozími testováními, a následně probíhá a sledování jeho chování. Jedná se zejména o sledování zápisu na diskový systém, manipulace s registry, pokusy o infiltrace do již běžících procesů, pokusy o komunikaci do Internetu (stahování dalších částí malware, stahování řídících instrukcí od řídících C&C server; zasílání získaných dat) a komunikaci v rámci vnitřní sítě (infiltrace do dalších systémů a zdrojů na síti, pokusy o stahování dat apod.). Dynamickou analýzou, kterou obě technologie disponují, podporuje i analýzu chování v rámci další fáze případného útoku, tj. analýza případných dalších součástí malware. Možnost zachytit APT hrozby je dána typem technologie, která je pro daný účel vyrobena. A právě sandbox technologie (FireEye FX, FortiSandbox a jiné) jsou pro tyto účely zachytávání vyrobeny.

S využitím upraveného jádra pro testování je tak možné souběžně testovat na několika různých platformách běžících v prostředích x64 nebo x86 a detekovat běžně rozšířený malware, který se pokouší o zneužití zranitelností různých verzí prohlížečů nebo jiného software nebo jiných APT.



Obrázek: Nákres workflow malware detekce

Technologie provádí rekurzivní, plánované testování a na vyžádání skenuje přístupné nebo poskytnuté síťové složky, soubory a úložiště obsahu, za účelem identifikace a karantény rezidentního malwaru.

https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/fireeye-fx-series.pdf

https://www.greschitz.net/wp-content/uploads/2015/12/fireeye-fx-series.pdf

https://www.fortinet.com/products/sandbox/fortisandbox

K bodu č. 103 Účastník upřesňuje:

V rámci implementace bude použitá možnost využití více VDOM (2x) pro jednotlivé pokročilé funkce v rámci zařízení Firewall next-gen od společnosti Fortigate, stejně tak jak je to použito u stáajících zařízení. V rámci nasazení bude v jedné VDOM použita a nastavena IPS sonda, která umožňuje kontrolovat a zajistit ochranu před uvedenými hrozbami. Druhá VDOM bude použita jako Firewall. V rámci kap. 2.6. Účastník uvedl: "Celé řešení systému DA MO, je dle požadavku postaveno na logicky oddělených komponentách Brána, Archiv, Badatelna, které běží v různých bezpečnostních zónách a jsou oddělené prostřednictvím firewallu. Na serverech jsou agenti pro zajištění integrity a ochrany dat, stejně tak jsou příslušné operace monitorovány v reálném čase a to i privilegovaných uživatelů. Toto sledování může být založeno na mnoha atributech a hodnotách „ Proto bude na virtuáních serverech nasazen Deep Security agent. Společně s využitím firewallu, bude možné bránit vlastní paměťový prostor, a zároveň i monitorovat procesy a komunikační rozhraní na základě signatur, politik a potencionálně škodlivého chování. Technologie jsou schopné vyhodnocovat komunikaci a blokovat neoprávněné přístupy nebo nepovolené aktvity. Některé další vlastnosti a funkcionalita vlastního agenta je uvedena níže:

- Antimalware sken v reálném čase (RealTime scan)
- Smart Scan pro optimalizaci vytížení CPU při detekci signatur
- Detekce škodlivého chování (Behavior monitoring)
- Ochrana proti ransomware včetně automatické zálohy souborů před jejich zašifrováním
- Ochrana před spyware a grayware
    - Blokace všech nových aplikací, pokud nejsou schváleny
    - Povolení všech aplikací, pokud nejsou zakázány
- Mód údržby (Maintenance mode) pro dočasné povolení spouštění aplikací při plánovaných změnách na serveru
- Notifikace v případě spuštění zakázané aplikace
- Možnost povolení aplikace z administračního rozhraní na základě vygenerované notifikace
- automatická aktualizace politiky dle aktuálního stavu operačního systému a nainstalovaných aplikací - automatický virtuální patching
- Možnost fungování v detekčním módu nebo preventivním módu
- Podpora SSL/TLS inspekce (nahráním certifikátu s privátním klíčem, který slouží pro dešifrování obsahu)

- Virtuální záplatování (Virtual Patching) – instalace ochran na síťové úrovni na zranitelnosti vyskytující se v operačním systému a nainstalovaných aplikacích
- Pro modul Aplication control jsou k dispozici dva módy:
  - Blokace všech nových aplikací, pokud nejsou schváleny
  - Povolení všech aplikací, pokud nejsou zakázány
- Sken procesů běžících v operační paměti, detekce škodlivé aktivity
- Automatický sken, který prohledá operační systém a doporučí pravidla a nastavení pro sledování systému přímo na míru systému, na kterém je nainstalovaný agent
- Možnost automatického přebírání pravidel z automatických naplánovaných skenů, které aktualizují doporučenou politiku pro sledování integrity
- Podpora pro definici vlastních pravidel pro sledování změn v systému:
  - Změna v registrech
  - Obsah souboru
  - Atributy souboru
  - Definice také pomocí XML
  - Nastavení závažnosti
- Podpora nastavení pro „fail close/fail open“
- Podpora restriktivního (co není povoleno je zakázáno) i permisivního módu

Zároveň bude pro každý virtuální stroj definována VLAN, která může znemožnit interní komunikaci mezi virtuálními stroji, bez komunikace přes vlastní IPS sondu..

Možnosti logování a ukládání na dedikované prostředí může Zadavateli přinést další pohled na celkovou bezpečnost. Vytvářením korelačních pravidel pro specifické prostředí se zvyšují detekční schopnosti celého systému.

Detailní popis IPS sondy je uveden níže v odkazu. Zároveň Účastník uvádí, že je připraven text přeložit a doplnit tak Zadavateli informace v českém jazyce.

Zároveň Účastník uvádí, že dle informací v ZD (kapitoly 16 přílohy 1) technologie Fortigate již byla použita pro implementaci ESA MO, kde tyto požadavky již byly splněny.

https://www.trendmicro.com/en_us/business/products/hybrid-cloud/deep-security.html
https://www.fortinet.com/products/ips

K bodu č. 104 Účastník upřesňuje

V rámci kap.2.6.2. Účastník uvedl následující: “Modul ochrany souborů dokáže monitorovat a kontrolovat přístup k souborům v celém prostředí firmy, díky tomu získají Nabyvatel přehled o tom kdo, kam, kdy a jak přistupoval k souborům. Systém dokáže tyto informace využít a dát je do vzájemných souvislostí a upozorňovat na případné podezřelé aktivity uživatelů.” Dále Účastník upřesňuje, že řešení bude realizováno instalací agenta na příslušný OS, který zajistí tuto kontrolu, logování, blokování a další pokročilé funkce ochrany a kontroly stavu operačního systému pro zachování integrity daného prostředí. Daný agent poběží na vlastním koncovém zařízení, ale bude spojen a bude komunikovat s centrálním managementem, přes který bude dostávat pokyny a výjimky pro kontrolu vlastního běžícího prostředí.

V centrálním managementu bude možné veškeré výjimky spravovat, stejně jako nastavovat politiky pro jednotlivé položky v rámci operačních systémů, registrů, povolení spouštění nebo blokování spouštění daného software. Veškeré operace jsou logovány a přístup na centrální management je povolen pouze oprávněné obsluze. Je pravda, že v nabídce je zároveň uvedeno, že: „Detailní popis nasazení řešení, bude součásti analýzy, kde Účastník vyspecifikuje seznam vlastních politik. V kombinaci s nasazení next-gen firewall, poskytuje toto řešení možnou blokaci portů, ochranu před kybernetickými hrozbami, monitoring a ochranu před exploity."

Účastník tím myslel především vlastní nastavení politik, které se mohou v závislosti na vnitřních předpisech Zadavatele měnit. (např. Badatelna může mít nastavenu jinou politiku ochrany serveru než servery digitalizace, neboť ty nekomunikují do internetu). Jakmile se v rámci analýzy ověří tyto informace a Během analýzy si proto Účastník se Zadavatelem potvrdí (jaké jsou vstupní informace pro nastavení), a na základě těchto informací provede nastavení těchto politik na centrálním managementu.

K bodu č. 105 Účastník upřesňuje:

Pro systém DA MO navrhujeme 3 zdroje pro identifikaci uživatelů:

- ActiveDirectory nebo LDAP - zde budou interní uživatelé. Heslové politiky jsou řešeny nastavením na ActiveDirectory nebo LDAP serveru. Zde budou uživatelé přistupující na Bránu.
- Interní LDAP - slouží pro přístup do Archivu. Jedná se o interní server, na kterém je možné nastavit heslové politiky.
- Samostatná správa uživatelů Badatelského Portálu.

V rámci software FileNet je možné nastavovat přístupy, oprávnění, přístupová práva na jednotlivé dokumenty, dědit práva v rámci složek, složených dokumentů, marking setů a nebo používat kombinací těchto přístupů na jednotlivé dokumenty nebo složky prostřednictvím vlastností komponenty Object Store.

Při iniciálním nastavení Object Store je nezbytné definovat typ autorizace a autentizace.

V DA MO jsou navrženy 2 základní Object store. Jeden pro Bránu a jeden pro Archiv. Brána ukládá dočasně vstupní dokumenty pro zpracování. Zkontroluje, zda jsou vložená data validní, ověří dokumenty v karanténě a předá je do Archivu. Přístup k těmto dokumentům bude uzpůsoben pro role uživatelů v rámci procesu zpracování.

Object store Archivu bude navázán na interní LDAP a umožní přímý přístup pouze pro uživatele Archivu. Přístup k dokumentům bude řízen dědičností složek a podle stavu dokumentu. Retence dokumentů bude řízena pomocí workflow, které po splnění kritérií výběrové skartace umožní odstranění dokumentů a zároveň zaznamená, že ke smazání došlo.

6. Dotaz č. 6 (Implementace a podpora systému ELZA)

6.1 Dotaz či požadavek zadavatele na objasnění

Implementace systému ELZA – v bodu 6.4 Přílohy č. 1 zadávací dokumentace jsou vyžadovány v rámci vytvoření technických předpokladů také služby implementace systému v rozsahu do 140 člověkodní a roční podpora 25 člověkodní, tj. celkem 265 člověkodní za 5 let. Zadavatel neidentifikoval v nabídce deklaraci, že tyto služby jsou součástí návrhu řešení. Současně tyto služby nejsou uvedeny v cenovém rozkladu. Zadavatel žádá účastníka o objasnění, proč účastník splnění tohoto požadavku zadávací dokumentace ve své nabídce a cenovém rozkladu pominul.

6.2 Objasnění účastníka IBM

Účastník deklaruje, že zde popsané plnění v uvedeném rozsahu je součástí nabídky a cenové kalkulace.

7. Dotaz č. 7 (PC pro Badatelnu a pracoviště Digitalizace)

7.1 Dotaz či požadavek zadavatele na objasnění

PC pro Badatelnu a pracoviště Digitalizace – v Příloze č. 1 zadávací dokumentace zadavatel požaduje:

6 PC pro Badatelnu pro připojení k internetu

4 + 2 PC pro digitalizační pracoviště

1 PC pro fotoarchiv

V nabídce v kapitole 3.5 Digitalizace je uvedeno 1 PC pro fotoarchiv. V kapitole 3.4 Badatelna je uvedeno „6ks PC v konfiguraci standardního PC“ a dále v odstavci „Níže je uvedena specifikace“ jsou podrobně specifikovány 4 + 2 PC pro pracoviště Digitalizace. Chápe zadavatel správně, že se v tomto odstavci jedná celkem o 6 + 4 + 2 PC a jsou jen uvedeny ve špatné kapitole nebo rozepsaná specifikace 4 + 2 PC popisuje těchto 6ks PC Badatelny? Z cenového rozkladu ani nabídky opět není zadavateli zřejmé, kolik kusů PC a v jaké konfiguraci nabídka obsahuje. Zadavatel dále žádá o doložení podrobné specifikace těchto HW a SW komponent, které musí být položkově uvedeny i v cenovém rozkladu.

7.2 Objasnění účastníka IBM

V rámci dodávky pracovních stanic dojde k dodání všech pracovních stanic, které Zadavatel vyjmenoval v rámci ZD. Ano uvedená PC byla uvedena ve špatných kapitolách. Účastník tento seznam upřesňuje, tak aby jednotlivá zařízení byla odkazována na příslušnou kapitolu v rámci dodávky. Detailní cenový rozpis a kalkulace je uvedena v příloze, viz upřesnění na dotaz č.1.

Kap. 5.2.1. ZD - HW Badatelny:

- 6ks PC v konfiguraci pro standardní kancelářskou práci vč. klávesnice a myši, monitor 27“, rozlišení alespoň 2560x1440, OS Windows 10 OEM.

Kap.6.4 ZD - Hardware a implementace

rozšíření digitalizačního **pracoviště listinných archiválií**

- 4ks PC určených k digitalizaci v optimální konfiguraci vzhledem k výše uvedenému určení, v konfiguraci minimálně: CPU Intel i7, 16GB RAM, SSD disk 128GB, HDD 1TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440
- 2ks PC určených k verifikaci digitalizovaných dat v optimální konfiguraci k této činnosti, v konfiguraci minimálně: CPU Intel i7, 16GB RAM, SSD disk 128GB, HDD 1TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440

rozšíření specializovaného **digitalizačního pracoviště fotoarchivu**

- 1ks PC v konfiguraci CPU Intel i7, 16GB RAM, SSD disk 512GB, HDD 2TB, Windows 10 64bit OEM verze, monitor 27“ rozlišení alespoň 2560x1440

8. Dotaz č. 8 (Migrace)

8.1 Dotaz či požadavek zadavatele na objasnění

Zadavatel konstatuje, že návrh migrace v kapitole 2.3 nabídky je sice v souladu se zadávací dokumentací, ale je doplněn o další nové předpoklady nad rámec ZD (omezení kontroly dat na 5 jednotlivých položek metadat, konverze má probíhat na infrastruktuře nabyvatele). Zadavatel žádá o garanci, že součástí návrhu řešení účastníka je plnohodnotné provedení migrace dle požadavků ZD bez jakýchkoliv dalších podmínek, které by záměr migrace omezily nebo vyvolaly případné další vícenáklady na straně zadavatele. V ZD není uvedeno, že zadavatel poskytne pro migraci dat svoji infrastrukturu a zadavatel s tím nepočítá. Migrace musí proběhnout na infrastruktuře účastníka, která je součástí smluvního plnění zadávacího řízení DA MO.

8.2 Objasnění účastníka IBM

Účastník potvrzuje, že

- kontrola metadat v průběhu konverze nebude omezena jejich počtem.
- součástí návrhu řešení účastníka je plnohodnotné provedení migrace dle požadavků ZD bez jakýchkoliv dalších podmínek, které by záměr migrace omezily nebo vyvolaly případné další vícenáklady na straně zadavatele.
- migrace proběhne na infrastruktuře, která bude součástí smluvního plnění dle zadávacího řízení DA MO.

9. Dotaz č. 9 (Testovací prostředí)

9.1 Dotaz či požadavek zadavatele na objasnění

Testovací prostředí je pouze krátce zmíněno v kapitole 3.1 nabídky účastníka bez jakéhokoliv dalšího popisu řešení. Zadavatel žádá o upřesnění a podrobný popis návrhu řešení testovacího prostředí, včetně topologie a specifikace HW a SW komponent, které musí být položkově uvedeny i v cenovém rozkladu.

9.2 Objasnění účastníka IBM

Účastník upřesňuje informace takto: Testovací prostředí bude vybudováno identicky jako prostředí Produkční. Tzn, že na serveru TEST Brána, bude v komponentě Filenet vytvořena další instance (profil), která bude dedikována výhradně pro systém DA MO. Stejně tak bude tvořena nová databáze, která bude dedikována pro běh a ukládání dat systému DA MO na prostředí TEST Brána. Identicky bude vytvořeno prostředí TEST DAMO i na serveru TEST ARCHIV. Vytvoření nové instance (profilu) zajistí oddělení funkčních částí a znemožní jakoukoliv výměnu dat mezi ESA MO a DA MO jinak, než přes rozhraní, které pro tyto účely bude vytvořeno (různé síťové subnety).

Hardware pro souběh obou aplikací a jejich současného testování bude navýšen z migrovaných zvirtualizovaných produkčních serverů (Brána, Archiv). Testovací prostředí je umístěno v lokalitě Praha, za respektování stejných politik a architektury jako produkční prostředí.

Pro TEST prostředí Badatelny a Digitalizace, tak tyto prostředí budou vytvořena nově, neboť aktuálně neexistují a budou na dedikovaných virtuálních serverech. Detailní návrh a popis nasazení deploymentu je uveden v upřesnění na dotaz č.2. Pro karanténu bude využita DR lokalita (obě zařízení).

Z pohledu stávajících serverů aktuální stav:

Server ESA Brána TEST – provozované prostředí ESA MO Brána

Server ESA Archiv TEST – provozované prostředí ESA MO Archiv

Nový stav:

Server ESA Brána TEST (stávající server) – provozované prostředí ESA MO Brána + prostředí DA MO

Server ESA Archiv TEST (stávající server) – provozované prostředí ESA MO Archiv + prostředí DA MO

Server Digitalizace TEST (virtuální server) – provozované prostředí DA MO Digitalizace

Server Badatelna TEST (virtuální server) – provozované prostředí DA MO Badatelna

Účastník dále uvádí, že architektura testovacího prostředí je závislá na architektuře produkčního prostředí. Pro naplnění požadavku dodržení stejných politik, je nutné, aby testovací architektura „kopírovala“ architekturu prostředí produkčního. Účastník je schopen s prostředky, které má k dispozici (po migraci do virtuální infrastruktury) změnit architekturu TEST prostředí, ale tato by neodpovídala nasazení v produkci.

10. Dotaz č. 10 (Technologie, architektura, topologie)

10.1 Dotaz či požadavek zadavatele na objasnění

U serverů a datových úložišť návrh řešení předpokládá vybudování DA MO na stávajících, zastaralých technologiích, s jejichž podporou jsou problémy již v současné době v rámci ESA MO. Také stávající SW komponenty mají technologické problémy např. při zajištění důsledného zálohování a zrcadlení dat ve 2 lokalitách, a některé SW verze jsou již zastaralé a vyžadují upgrade na aktuální podporované verze. Požadavkem ZD bylo postavit systém DA MO, který bude sice technologicky navazovat na ESA MO, ale bude na nových, modernějších technologiích a aplikacích, a nebude pouhým doplňkem ESA MO.

Zadavatel žádá účastníka o podrobné vysvětlení včetně popisu architektury a topologie řešení, jak budou řešeny replikace dat, když stávající systém GPFS řádně nefunguje ani v ESA MO, a v nabídce je zřejmě předpokládáno jeho použití i dále pro systém DA MO. Garantuje návrh řešení účastníka plnohodnotné replikace lokalit na stávajících linkách? Garantuje také návrh řešení účastníka, že veškeré SW komponenty navrženého řešení DA MO budou nasazeny v posledních aktuálních platných verzích a součástí nabídky je v souladu s požadavky ZD také zajištění jejich SW podpory po celou dobu trvání smluvního plnění (veškeré SW komponenty včetně podpory musí být uvedeny také v cenovém rozkladu)?

10.2 Objasnění účastníka IBM

Návrh řešení Účastníka na vytvoření systému DA MO je postaven dle požadavků Zadavatele, které byly uvedeny v rámci ZD. Zároveň Účastník uvádí, že systém DA MO, je sice tvořen na technologické základně ESA MO, což Zadavatel umožňuje, ale jedná se o samostatný systém, který je schopen běžet v případě, že se komponenty systému ESA MO odstaví nebo vypnou. Ze ZD jednoznačně nevyplynulo a dle odpovědí do Zadavatel potvrdil, že nepožaduje jednoznačně nový systém. Na základě těchto informací, které Zadavatel uvedl, Účastník připravil návrh řešení.

Architektura, zapojení komponent a topologie a doplnění popisu je uvedena v upřesnění č.2. Tato topologie byla navržena s ohledem na poskytnuté informace a navržena s využitím nových a moderních technologií (Virtualizace, Bezpečnost). Účastník postupoval tak, aby dodržel všechny požadavky Zadavatele na bezpečné nasazení a s ekonomickou udržitelností

Účastník může potvrdit, že jestliže budou poskytnuty linky (a její kapacita), tak jak je uvedena v ZD (interní síť 1Gbit), je schopen garantovat plnou funkčnost replikací. Asynchronní přenos dat, který je pro replikace používán, je doporučený pro nededikované linky. Pro nativní replikace diskových polí se používají dedikované linky s garantovanou kvalitou linek, prostřednictvím kterých je možné využívat pokročilých replikačních mechanismů přímo mezi diskovými poli. Tyto funkce u méně kvalitních linek použít nelze, neboť by hrozila ztráta dat nebo v lepším případě jejich nekonzistence.

Zároveň tímto potvrzujeme, že navrhované replikační mechanismy jsou provozovány i u jiných zákazníků a jsou funkční. Účastník garantuje, že navržené replikační mechanismy v kombinaci se zálohováním zajišťují minimalizaci ztráty dat a zároveň Účastník ručí za to, že po dobu podpory systému, nedojde ke ztrátě dat.

Popis a návrh řešení replikačních mechanismů, které používá technologie FileNet je doplněn výše v bodě 5, upřesnění pro bod č.73. Zároveň Účastník potvrzuje, že v rámci implementace budou nasazeny podporované verze DB a poslední aktuální verze software, které jsou určeny pro systém DA MO. Rozpad komponent je uveden v přiloženém a doplněném cenovém rozkladu.

11. Dotaz č. 11 (Firewally)

11.1 Dotaz či požadavek zadavatele na objasnění

Z nabídky účastníka není zřejmé, zda návrh řešení předpokládá dodání nových firewallů (z cenového rozkladu to není patrné), v jakém počtu a pro obě nebo pouze pro jednu z lokalit? Zadavatel konstatuje, že stávající FW v rámci ESA MO již nemají volné porty, přes které by bylo možné připojit jednotlivé nové VLAN segmenty DA MO. Firewally v DA MO musí dle názoru zadavatele dále zajišťovat segmentaci a pomocí pravidel řízení také komunikace jednotlivých systémů mezi sebou, řešit přístupy z externího prostředí, provádět základní inspekci provozu a hlavně zajišťovat důsledné oddělení ESA MO a DA MO.

Dále není zadavateli z návrhu řešení zřejmé, zda účastník ve své nabídce garantuje, že stávající firewally zvládnou provoz obou prostředí. Zadavatel žádá o objasnění, jakým způsobem návrh řešení řeší vrstvu firewallů včetně popisu architektury a topologie řešení v obou lokalitách a uvedení specifikace HW komponent, které musí být položkově uvedeny i v cenovém rozkladu.

11.2 Objasnění účastníka IBM

V lokalitě Praha, jak již bylo uvedeno, budou oba stávající firewally vyměněny za 2 nové kusy stejné značky (Fortigate s 5letou podporou, jak je požadováno), zapojené opět v clusteru, aby Zadavateli nevznikly náklady s dodatečným školením na nové technologie. Součástí nabídky je dodávka, nasazení a integrace těchto firewallů do prostředí ESA a DA v Praze. Navýšení propustnosti firewallů na více jak dvoj až troj-násobek zajistí bezproblémový chod obou systémů. Tyto budou spojeny do clusteru a se svými 16ks GE RJ 45 porty (s další možností rozšíření prostřednictvím SFP portů) bude možné doplnit další nové části infrastuktury DA MO (Badatelna, Digitalizace) a zároveň tím i umožnit, zkonsolidovat a lépe segmentovat stávající technologie v této lokalitě. (zapojení Qflow sondy a QRadar). Zároveň bude možné použít stávající Gbic moduly z firewallů běžících v Praze, v lokalitě Olomouc, a to tak, aby byl zapojen další server s hypervisorem (Virtual2) v lokalitě Olomouc, na kterém poběží záložní instance Badatelny a Backup Proxy server.(podpora pro WAN Akceleraci)

Jak již bylo uvedeno výše, systémy ESA MO a DA MO jsou komunikačně odděleny a využívají pouze rozhraní jednotlivých Bran (jejich služeb a volání, včetně komunikace prostřednictvím SIP). Informace týkající se topologie upřesnil Účastník v rámci upřesnění na dotaz č.2.

Z pohledu Účastníka jsou některé výše uvedené požadavky zcela nové a nebyly v rámci ZD uvedeny "Zajištovat důsledné oddělení ESA MO a DA MO." Návrh Účastníka byl připraven na základě požadavků, které jsou uvedeny ve výzvě ZD, doplňujících přílohách a upřesněních Zadavatele. Požadavek na zajištění důsledného oddělení ESA MO a DA MO tam Účastník nenalezl. (Vyplývá rovněž z odpovědi Zadavatele na dotaz č. 1 v rámci Vysvětlení zadávací dokumentace č. 4.)

V rámci návrhu infrastruktury Účastník uvádí, že Firewally umístěné v lokalitě Olomouc jsou schopné zvládnout nasazení (doplnění) záložních pracovišť DA MO (Brána, Archiv, Badatelna) a po doplnění o GBic z lokality Praha, toto bude zajištěno. Stejně tak Účastník garantuje, že výkonnost dodávaných serverů je na dostatečné úrovni pro běh plánovaných virtuálních serverů.

V případě požadavku na navýšení nebo rozšíření kapacit (výpočetních, diskových) je Účastník připraven a ochoten na základě analýzy rozšířit stávající navrhované řešení. (Architektura návrhu řešení umožňuje plynulé rozšíření).

S ohledem na svůj expertní odhad Účastník dodává, že v případě, kdy by z pohledu výkonu docházelo k jakýmkoliv problémům, Účastník tímto garantuje, že dodá místo stávajícího hardware takový, jenž bude odpovídat provozním požadavkům (především výkonnostním nárokům), s příslušnou podporou a naplňující všechny další požadavky DA MO dle zadávací dokumentace bez jakéhokoliv navýšení ceny nebo dodatečných nároků na Zadavatele.

V Praze dne : dle elektronického podpisu

IBM Česká republika, spol. s r.o.

……..
Ing. Petr Havlík,
jednatel společnosti

Přílohy

~~**Příloha 1 – Priloha 1_Cenovy_rozklad_detail_IBM.xlsx**~~

Příloha 2 – Priloha 2_Cenovy_rozklad_detail_IBM.pdf

Příloha 3 – Priloha 3_Zakladni_model_deploymentu_IBM.pdf

Příloha 2 smlouvy č. 195310197
Počet listů: 1

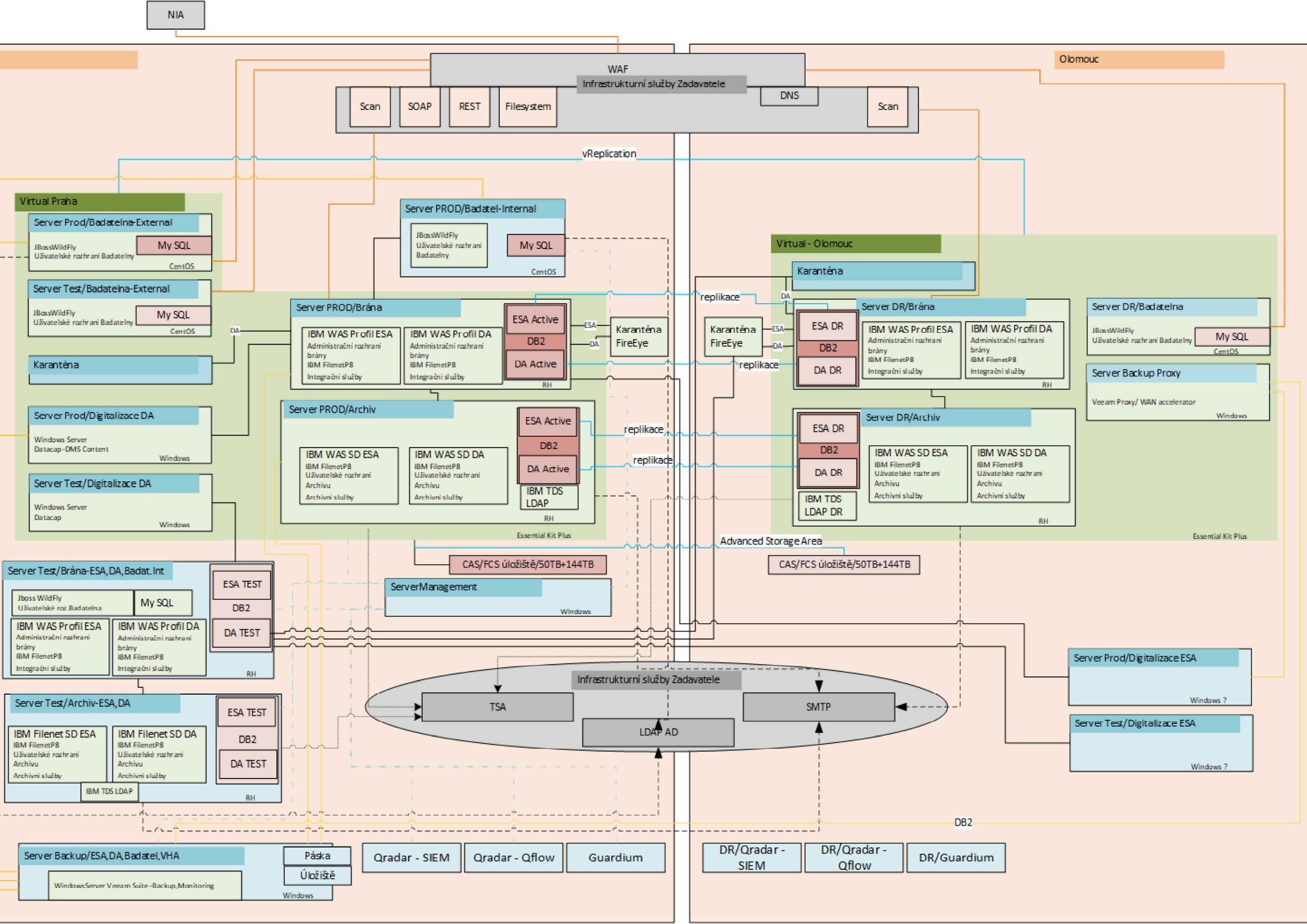
CENOVÝ ROZKLAD

Položka		L = licence, V = vývoj	cena/jednotku bez DPH	cena/jednotku včetně DPH	**cena celkem bez DPH**	cena celkem včetně DPH	**cena instalace/konfigurace bez DPH**	cena instalace/konfigurace včetně DPH	servisní podpora/rok bez DPH	servisní podpora/rok včetně DPH	**servisní podpora/5 let bez DPH**	servisní podpora/5 let včetně DPH	pozn
Služby													
	~~Podrobná analýza a tvorba cílového konceptu řešení~~	~~*~~					~~*~~	~~*~~	~~*~~	~~*~~	~~*~~	~~*~~	
	Podrobná analýza a tvorba cílového konceptu řešení (v rozsahu kap. 5.2)	x	1,272,812	1,540,102	1,272,812	1,540,102	x	x	x	x	x	x	
	Zaškolení a proškolování obsluh (v rozsahu kap 4.6)	x	66,885	80,931	66,885	80,931	x	x	x	x	x	x	
Hardware	Rozpis položek a konfigurace												
	~~Servery oblast Brána, Archiv, Badatelsky portál~~	~~*~~											
	Rozšíření stávajících serverů a zalohování (v rozsahu kap. 3.1 a 4.1)	x	975,723	1,180,625	975,723	1,180,625	59,147	71,568	0	0	0	0	
	2ks Firewall včetně Fortisandbox a další síťová infrastruktura (v rozsahu kap. 3.2)	x	775,313	938,128	1,550,625	1,876,256	289,072	349,777	80,000	96,800	400,000	484,000	
	2ks Rozšíření stávajícího diskového úložiště (v rozsahu kap. 3.3)	x	416,031	503,397	832,062	1,006,795	140,000	169,400	30,995	37,503	154,973	187,517	
	6ks PC v konfiguraci standardního PC pro Badatelnu pro připojení k internetu (v rozsahu uvedeném v ka	x	32,677	39,539	196,063	237,236	20,706	25,054	0	0	0	0	
	4ks PC určených k digitalizaci (v rozsahu uvedeném v kap. 3.4)	x	41,570	50,300	166,280	201,199	13,804	16,703	0	0	0	0	
	2ks PC určených k verifikaci digitalizovaných dat (v rozsahu uvedeném v kap. 3.4)	x	41,570	50,300	83,140	100,600	6,902	8,351	0	0	0	0	
	Barevná laserová tiskárna A4 (v rozsahu uvedeném v kap. 3.4)	x	18,343	22,195	18,343	22,195	0	0	0	0	0	0	
	Barevná laserová tiskárna A3 (v rozsahu uvedeném v kap. 3.4)	x	51,693	62,548	51,693	62,548	0	0	0	0	0	0	
	24-portový switch v provedení Rack-mount 19" a optický převodník (v rozsahu uvedeném v kap. 3.4)	x	18,215	22,040	18,215	22,040	6,500	7,865	0	0	0	0	
	PC pro digitalizaci (v rozsahu uvedeném v kap. 3.5)	x	44,724	54,116	44,724	54,116	13,804	16,703	0	0	0	0	
	Skener fotografií (včetně skenovacího SW) – formát A3 (v rozsahu uvedeném v kap. 3.5)	x	175,088	211,856	175,088	211,856	13,804	16,703	0	0	0	0	
	Skener negativů/pozitivů (včetně skenovacího SW) – formát A3 (v rozsahu uvedeném v kap. 3.5)	x	215,108	260,280	215,108	260,280	13,804	16,703	0	0	0	0	
	Aplikační server ELZA (v rozsahu uvedeném v kap. 3.5)	x	203,345	246,048	203,345	246,048	7,500	9,075	0	0	0	0	
	Databázový server ELZA (v rozsahu uvedeném v kap. 3.5)	x	117,003	141,574	117,003	141,574	7,500	9,075	0	0	0	0	
	Ostatní komponenty systému ELZA (v rozsahu uvedeném v kap. 3.5)												
	1ks APC Symmetra LX 12kVA Scalable to 16kVA	x	428,548	518,542	428,548	518,542	0	0	0	0	0	0	
	1ks APC Symmetra LX Battery Module	x	19,677	23,809	19,677	23,809	0	0	0	0	0	0	
	8ks Rack PDU, 1U, 16A, 8x230V	x	7,504	9,080	60,030	72,636	0	0	0	0	0	0	
	1ks Jistič 3x20A	x	1,167	1,412	1,167	1,412	0	0	0	0	0	0	
	15ks Kabel 1-CXHK-R-J 5 x 4/O/-/B2 CAS 1dO	x	250	303	3,752	4,540	0	0	0	0	0	0	
	2ks Pomocný a montážní materiál (pro rack, pro UPS)	x	5,836	7,062	11,673	14,124	0	0	0	0	0	0	
	1ks APC Symmetra LX 8kVA Scalable to 16kVA	x	346,840	419,676	346,840	419,676	0	0	0	0	0	0	
	1ks APC Symmetra LX Battery Module	x	19,677	23,809	19,677	23,809	0	0	0	0	0	0	
	8ks Rack PDU, 1U, 16A, 8x230V	x	7,504	9,080	60,030	72,636	0	0	0	0	0	0	
	1ks Jistič 3x20A	x	1,167	1,412	1,167	1,412	0	0	0	0	0	0	
	15ks Kabel 1-CXHK-R-J 5 x 4/O/-/B2 CAS 1dO	x	250	303	3,752	4,540	0	0	0	0	0	0	
	2ks Pomocný a montážní materiál (pro rack, pro UPS)	x	5,836	7,062	11,673	14,124	0	0	0	0	0	0	
	2ks RACK TRITON 32U 600x900, nosnost 400kg	x	14,007	16,948	28,014	33,897	0	0	0	0	0	0	
	2ks Podstavec pod RACK 600x900	x	2,418	2,926	4,836	5,851	0	0	0	0	0	0	
	2ks Ventilační jednotka 600x900	x	5,836	7,062	11,673	14,124	0	0	0	0	0	0	
	HW Virtualizace1 - Praha (v rozsahu uvedeném v kap. 3.4)	x	369,322	446,880	369,322	446,880	27,400	33,154	0	0	0	0	
	HW Virtualizace2 - Olomouc (v rozsahu uvedeném v kap. 3.4)	x	337,121	407,916	337,121	407,916	27,400	33,154	0	0	0	0	
	Tel. a emailový helpdesk pro pracovníky centrálního dohledu objednatele (v rozsahu uvedeném v kap. 4	x	x	x	x	x	x	x	40,020	48,425	200,102	242,124	
	5let - Technická podpora HW, SLA (v rozsahu uvedeném v kap. 4.3 a 4.4)	x	x	x	x	x	x	x	270,321	327,088	1,351,605	1,635,442	
Software	Rozpis položek												
	~~Modul Brána&Archiv~~												
	20ks Modul Brána (v rozsahu kap. 2.2.2 a dle licenčních podmínek v kap. 6.1)	L*	62,500	75,625	1,250,000	1,512,500	854,145	1,033,515	75,113	90,887	375,565	454,434	
	20ks Modul Archiv (v rozsahu kap. 2.2.3 a dle licenčních podmínek v kap 6.1)	L*	62,500	75,625	1,250,000	1,512,500	1,418,243	1,716,074	75,113	90,887	375,565	454,434	
	Služby implementace systému ELZA v rozsahu do 140 člověkodní a roční podpora 25 člověkodní	x	x	x	x	x	548,100	663,201	82,998	100,427	414,990	502,137	
	~~Modul MS Office View, Redakce & Digitalizační linka~~	~~L*~~											
	20ks Modul MS Office View (v rozsahu uvedeném v kap. 2.2.3 a dle licenčních podmínek v kap. 6.1)	L*	1,756	2,125	35,120	42,495	1,480,000	1,790,800	307,025	371,500	1,535,125	1,857,501	
	20ks Modul Redakce (v rozsahu uvedeném v kap. 2.2.3 a dle licenčních podmínek v kap. 6.1)	L*	1,756	2,125	35,120	42,495	1,465,587	1,773,360	287,025	347,300	1,435,125	1,736,501	
	15ks Modul Digitalizační linka (v rozsahu kap. 2.4 a dle licenčních podmínek v kap. 6.1) včetně IBM Dat	L*	69,970	84,664	1,049,555	1,269,961	1,723,000	2,084,830	327,502	396,277	1,637,510	1,981,387	
	5ks Windows Server 2019	L	23,851	28,859	119,254	144,297	41,296	49,968	0	0	0	0	
	4ks Red Hat Enterprise Linux	L	26,871	32,514	107,483	130,055	41,296	49,968	0	0	0	0	
	VMWARE Essential Kit Plus - max 3hosts (v rozsahu uvedeném v kap. 3.4)	L	262,411	317,517	262,411	317,517	182,592	220,936	0	0	0	0	
	Veeam Availability Suite (v rozsahu uvedeném v kap. 4.1.)	L	183,462	221,989	183,462	221,989	427,000	516,670	0	0	0	0	
	5let - Technická podpora OS a Virtualizace, SLA (v rozsahu uvedeném v kap. 4.3 a 4.4)	x	x	x	x	x	x	x	167,279	202,408	836,395	1,012,038	
	10ks Trend Micro Deep Security	L	10,000	12,100	100,000	121,000	427,000	516,670	20,000	24,200	100,000	121,000	
	5ks McAfee Change Control for Servers	L	12,435	15,046	62,173	75,229	130,000	157,300	40,435	48,927	202,177	244,634	
	5ks McAfee Application Control for Servers	L	9,085	10,992	45,423	54,961	130,000	157,300	34,580	41,841	172,898	209,207	
	Modul Badatelský portál (v rozsahu kap. 2.2.4)	L	589,766	713,617	589,766	713,617	806,049	975,319	198,099	239,700	990,497	1,198,502	
			x	x	12,795,823	15,482,945	10,321,650	12,489,197	x	x	10,182,527	12,320,858	

Celková cena bez DPH: 33,300,000.00
Celková cena s DPH: 40,293,000.00

Poznámky k cenám:
Ceny uváděny v Kč, sazba DPH v % k datu podání nabídky,
Rozpis položek u serverového operačního systému zahrnuje náklady na licence veškerých virtuálních nebo fyzických strojů pro potřeby systému DA MO,
U SW komponent je uvedeno, zda se jedná o licenci hotového SW nebo vlastní vývoj (L nebo V v příslušném sloupci), dále způsob licencování a doba platnosti licence - zvlášť cena pořízení licence a cena maintenance/technické podpory včetně legislativního upgrade (podrobné licenční podmínky jsou součástí dokumentace předávané v rámci dodávky),
Cena SW komponent zahrnuje veškeré licence nutné pro jejich funkční provoz,
Cenu instalace a servisní podpory je uvedena za celkový počet položek (pokud to nelze dle vzoru, dodavatel upraví tabulku),
Servisní podpora je plánovaná na 5 let, v příslušných sloupcích jsou uvedeny ceny na jeden rok a na 5 let. V případě plánované obnovy zařízení nebo SW v pětiletém cyklu může položka servisní podpora/5 let nabývat jiné hodnoty než prosté násobení servisní podpora/rok x 5,
V položce HW uvedena také cena za skenovací pracoviště vč. SW, HW a servisu,
Celková cena je součtem veškerých dodávek a služeb včetně servisu a technické podpory na 5 let a legislativního upgrade na 5 let (tato celková cena je stejná jako cena uvedená v nabídce.

***informace o licenčních podmínkách pro produkty naleznete v dokumentu Příloha 1 - Specifikace předmětu plnění ke smlouvě č.195310197**


NIA
WAF
Infrastrukturní služby Zadavatele
Scan
SOAP
REST
Filesystem
DNS
Scan
Olomouc
vReplication
Virtual Praha
Server Prod/Badatelna-External
JBossWildFly
Uživatelské rozhraní Badatelny
My SQL
CentOS
Server Test/Badatelna-External
JBossWildFly
Uživatelské rozhraní Badatelny
My SQL
CentOS
Karanténa
Server Prod/Digitalizace DA
Windows Server
Datacap-DMS Content
Windows
Server Test/Digitalizace DA
Windows Server
Datacap
Windows
Server PROD/Badatel-Internal
JBossWildFly
Uživatelské rozhraní Badatelny
My SQL
CentOS
Server PROD/Brána
IBM WAS Profil ESA
Administrační rozhraní brány
IBM FilenetP8
Integrační služby
IBM WAS Profil DA
Administrační rozhraní brány
IBM FilenetP8
Integrační služby
ESA Active
DB2
DA Active
RH
Karanténa FireEye
Server PROD/Archiv
IBM WAS SD ESA
IBM FilenetP8
Uživatelské rozhraní Archivu
Archivní služby
IBM WAS SD DA
IBM FilenetP8
Uživatelské rozhraní Archivu
Archivní služby
ESA Active
DB2
DA Active
IBM TDS LDAP
RH
Essential Kit Plus
replikace
replikace
Virtual - Olomouc
Karanténa
Karanténa FireEye
Server DR/Brána
ESA DR
DB2
DA DR
IBM WAS Profil ESA
Administrační rozhraní brány
IBM FilenetP8
Integrační služby
IBM WAS Profil DA
Administrační rozhraní brány
IBM FilenetP8
Integrační služby
RH
Server DR/Archiv
ESA DR
DB2
DA DR
IBM TDS LDAP DR
IBM WAS SD ESA
IBM FilenetP8
Uživatelské rozhraní Archivu
Archivní služby
IBM WAS SD DA
IBM FilenetP8
Uživatelské rozhraní Archivu
Archivní služby
RH
Server DR/Badatelna
JBossWildFly
Uživatelské rozhraní Badatelny
My SQL
CentOS
Server Backup Proxy
Veeam Proxy/ WAN accelerator
Windows
Essential Kit Plus
replikace
Advanced Storage Area
CAS/FCS úložiště/50TB+144TB
CAS/FCS úložiště/50TB+144TB
ServerManagement
Windows
Server Test/Brána-ESA,DA,Badat.Int
Jboss WildFly
Uživatelské roz.Badatelna
My SQL
IBM WAS Profil ESA
Administrační rozhraní brány
IBM FilenetP8
Integrační služby
IBM WAS Profil DA
Administrační rozhraní brány
IBM FilenetP8
Integrační služby
ESA TEST
DB2
DA TEST
RH
Server Test/Archiv-ESA,DA
IBM Filenet SD ESA
IBM FilenetP8
Uživatelské rozhraní Archivu
Archivní služby
IBM Filenet SD DA
IBM FilenetP8
Uživatelské rozhraní Archivu
Archivní služby
IBM TDS LDAP
ESA TEST
DB2
DA TEST
RH
Infrastrukturní služby Zadavatele
TSA
SMTP
LDAP AD
Server Prod/Digitalizace ESA
Windows ?
Server Test/Digitalizace ESA
Windows ?
DB2
Server Backup/ESA,DA,Badatel,VHA
WindowsServer Veeam Suite -Backup,Monitoring
Windows
Páska
Úložiště
Qradar - SIEM
Qradar - Qflow
Guardium
DR/Qradar - SIEM
DR/Qradar - Qflow
DR/Guardium

Příloha 4 smlouvy č. 195310197

Počet listů: 1

CENOVÝ ROZKLAD

Položka		L = licence, V = vývoj	cena/jednotku bez DPH	cena/jednotku včetně DPH	cena celkem bez DPH	cena celkem včetně DPH	cena instalace/konfigurace bez DPH	cena instalace/konfigurace včetně DPH	servisní podpora/rok bez DPH	servisní podpora/rok včetně DPH	servisní podpora/5 let bez DPH	servisní podpora/5 let včetně DPH	pozn
Podrobná analýza a tvorba cílového konceptu řešení		x	1 339 697	1 621 033	1 339 697	1 621 033	x	x	x	x	x	x	
Hardware	Rozpis položek a konfigurace												
	- Hardwarové řešení a komponenty - rozšíření												
	Servery oblast Brána, Archiv, Badatelsky portál	x	5 534 298	6 696 500	5 534 298	6 696 500	507 343	613 885	390 341	472 313	1 951 707	2 361 566	
	- Diskové úložiště												
	Rozšíření stávajícího diskového úložiště	x	832 062	1 006 795	832 062	1 006 795	140 000	169 400	30 995	37 503	154 973	187 517	
Software	Rozpis položek												
	- Modul Brána&Archiv	L*	2 500 000	3 025 000	2 500 000	3 025 000	2 820 488	3 412 790	233 224	282 201	1 166 120	1 411 005	
	- Modul MS Office View, Redakce & Digitalizační linka	L*	2 000 000	2 420 000	2 000 000	2 420 000	6 047 771	7 317 803	1 183 846	1 432 454	5 919 230	7 162 269	
	- Modul badateklský portal	L	589 766	713 617	589 766	713 617	806 049	975 319	198 099	239 700	990 497	1 198 502	
			x	x	12 795 823	15 482 945	10 321 650	12 489 197	x	x	10 182 527	12 320 858	

Celková cena bez DPH: 33 300 000,00 Kč
Celková cena s DPH: 40 293 000,00 Kč

Poznámky k cenám:

Ceny uváděny v Kč, sazba DPH v % k datu podání nabídky,
Rozpis položek u serverového operačního systému zahrnuje náklady na licence veškerých virtuálních nebo fyzických strojů pro potřeby systému DA MO,
U SW komponent je uvedeno, zda se jedná o licenci hotového SW nebo vlastní vývoj (L nebo V v příslušném sloupci), dále způsob licencování a doba platnosti licence - zvlášť cena pořízení licence a cena maintenance/technické podpory včetně legislativního upgrade (podrobné licenční podmínky jsou součástí dokumentace předávané v rámci dodávky),
Cena SW komponent zahrnuje veškeré licence nutné pro jejich funkční provoz,
Cenu instalace a servisní podpory je uvedena za celkový počet položek (pokud to nelze dle vzoru, dodavatel upraví tabulku),
Servisní podpora je plánovaná na 5 let, v příslušných sloupcích jsou uvedeny ceny na jeden rok a na 5 let. V případě plánované obnovy zařízení nebo SW v pětiletém cyklu může položka servisní podpora/5 let nabývat jiné hodnoty než prosté násobení servisní podpora/rok x 5,
V položce HW uvedena také cena za skenovací pracoviště vč. SW, HW a servisu,
Celková cena je součtem veškerých dodávek a služeb včetně servisu a technické podpory na 5 let a legislativního upgrade na 5 let (tato celková cena je stejná jako cena uvedená v nabídce.

***informace o licenčních podmínkách pro produkty naleznete v dokumentu Příloha 2 - Specifikace předmětu plnění IBM ke smlouvě č.195310197**

Příloha 5 smlouvy č. 195310197
Počet stran: 1

Specifikace utajovaných informací stanovených nařízením vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů

příloha č. 14

P. č.	Informace	Stupeň utajení
1	Způsob zajištění fyzické bezpečnosti objektů, zabezpečených oblastí a jednacích oblastí, ve kterých jsou ukládány, zpracovávány nebo pravidelně projednávány utajované informace.	VYHRAZENÉ

KATALOGIZAČNÍ DOLOŽKA[1]

K zabezpečení procesu katalogizace položek majetku (výrobků), které jsou předmětem smlouvy a které podléhají katalogizaci podle zásad Kodifikačního systému NATO (dále jen „NCS") a Jednotného systému katalogizace majetku v ČR (dále jen „JSK") se **prodávající zavazuje**:

1. Neprodleně po uzavření smlouvy, nejpozději do 5 pracovních dní, oznámit e-mailem Oddělení katalogizace majetku Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti (dále jen „OdKM") na e-mailovou adresu katalogizace@army.cz číslo smlouvy, kontaktní osobu a kontaktní údaje osoby zodpovědné ze strany prodávajícího za provedení katalogizace položek dané smlouvy.[2]
2. Na vlastní náklady zpracovat nebo zabezpečit zpracování Souboru povinných údajů pro katalogizaci (dále jen „SPÚK") majetku definovaného smlouvou vždy prostřednictvím aplikace umístěné na www.cz-katalog.cz.
3. Povinnou součástí zpracování SPÚK každé dosud nekatalogizované položky majetku je:
   a) fotografie reálně zobrazující dodávanou položku majetku ve formě elektronického souboru ve formátu JPG, rozlišení do 1024x768 bodů[3];
   b) hypertextový odkaz na webovou stránku nebo elektronický soubor, které obsahují technické údaje o výrobku. Elektronický soubor musí být ve formátu JPG, rozlišení do 1024x768 bodů, nebo ve formátu PDF, v rozměrech strany A4. V případě, že nelze poskytnout hypertextový odkaz nebo elektronický soubor, doložit správnost údajů nezbytných k provedení popisné identifikace jiným způsobem.
4. Zabezpečit doručení SPÚK OdKM v termínu **15. 8. 2021** před fyzickým dodáním předmětu smlouvy.
5. Dodat bez prodlení písemně nebo elektronicky v průběhu realizace smlouvy informace o všech změnách, týkajících se předmětu smlouvy, které mají vliv na identifikaci katalogizovaných položek majetku, včetně změn u položek majetku nakupovaných prodávajícím od subdodavatelů.

Katalogizační doložka je naplněna dodáním úplných a bezchybných dat, které je potvrzeno po kontrole a zpracování dodaných dat vydáním kladného „Stanoviska Úř OSK SOJ k naplnění katalogizační doložky".

Přidělené identifikátory (KČM, NSN) a zpracovaná katalogizační data jsou dostupná na www.cz-katalog.cz po ukončení procesu katalogizace majetku.

Kontaktní adresa:

Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti
ODDĚLENÍ KATALOGIZACE MAJETKU
nám. Svobody 471
160 01 PRAHA 6

TEL.: 973 229 274
E-MAIL: katalogizace@army.cz
INTERNET: www.okm.army.cz

[1] Platná pro kupní smlouvy uzavírané po 1. únoru 2020.
[2] Zákon 309/2000 Sb., §14, bod 2
[3] Prodávající tímto souhlasí s použitím dodané fotografie pro účely JSK a NCS.