ČESKÁ REPUBLIKA – MINISTERSTVO KULTURY

STRATEGIE ICT MK
(obecná a projektová část)

Ing. Josef Praks, ředitel odboru informačních technologií

Aktuální verze	1.0
Název souboru	Projektova a obecna cast ICT strategie MKCR v 1.0 - FINAL 20150601
Zpracovatel	Ing. Josef Praks, ředitel odboru informačních technologií
Datum vytvoření	1. 6. 2015
Datum poslední revize	
Počet stran	126
Počet příloh	
Důvěrnost	Pro potřebu orgánů státní správy

Obsah

1 Identifikace strategie ICT

1.1 Základní údaje strategie ICT

Název organizace	Ministerstvo kultury
IČO	00023671
Typ organizace	Ústřední orgán veřejné správy
Adresa	Maltézské náměstí 1/471 118 01 Praha 1
Doba platnosti	5 let
Konec platnosti	31. 12. 2020
Aktuální verze	1.0

Tabulka 1: Základní údaje o strategii ICT

Role	Osoba	Datum	Podpis
Autor:	Ing. Josef Praks	1. 6. 2015	
Schválil:	Ing. René Schreier		

Tabulka 2:Autorizace a schválení strategie ICT

1.2 Verze strategie ICT

V dílčích článcích této kapitoly jsou popsány všechny verze strategie ICT chronologicky od aktuálně platné až po nejstarší.

Veškeré verze strategie ICT jsou umístěny na intranetovém portálu Ministerstva kultury a jsou dostupné všem zaměstnancům Ministerstva kultury. Odkaz je: http://in/odbor/informatika/strategie.

1.2.1 Verze 1.0 – aktuální verze strategie ICT

značení verze	1.0
Datum vzniku	1. 6. 2015
Datum schválení	XX.5.2015
Počátek platnosti	Po schválení - XX.5.2015
Autor verze	Ing. Josef Praks
Útvar	Odbor informačních technologií
Funkce	Ředitel odboru
Verzi schválil	Ing. René Schreier
Funkce	Ekonomický náměstek ministra kultury
Název souboru	Projektova a obecna cast ICT strategie MKCR v 1.0 - FINAL 20150601
Verze souboru	1.0
Umístění souboru	http://in/odbor/informatika/ictstrategie
Počet stran	126
Počet příloh	0
Atestovaná verze	
Odkaz na interanetový portál	http://in/odbor/informatika/

Tabulka 3: Údaje o verzi 1.0 strategie ICT

Změny provedené v aktuální verzi

Číslo	Popis změny	Důvod změny	Místo změny
1.0	Původní verze strategie	---	---

Tabulka 4: Změny provedené ve verzi

2 Manažerské shrnutí

Dokument popisuje strategii rezortu Ministerstva kultury pro rozvoj ICT v období 2015-2020.

Předkládaný dokument je určen vrcholovému vedení rezortu Ministerstva kultury. Jeho cílem je seznámit čtenáře s vizí a strategií jejího naplnění v oblasti řízení a rozvoje informačních a komunikačních technologií (dále též jen ICT) MK v dlouhodobém časovém horizontu počínaje rokem 2015.

Vize řízení a rozvoje komunikačních technologií Ministerstva kultury jsou charakterizovány následovně:

1) koncepce stabilizace stávající infrastruktury a aktuálně poskytovaných služeb

2) rozšíření stávající infrastruktury k poskytování služeb spojených s moderními trendy v ICT (digitalizační platforma a nástroje eCulture)

3) poskytování služeb spojených s moderními trendy v ICT (mobilní přístroje, velká data, internet věcí, sociální sítě, etc.)

4) podpora výzkumu a vývoje v oblastech využívající ICT

5) zajištění vícezdrojového financování a stanovení priorit řešení jednotlivých oblastí ICT.

Vlastní strategie dosažení prezentovaných vizi je formulována do programů, u nichž jsou uváděny expertní odhady termínů jejich časové realizace. Související finanční náklady budou pokrývány z rozpočtů následujících období s vazbou na využití evropských zdrojů. Dokument tak slouží i jako výchozí, rámcový podklad pro vytváření budoucích rozpočtů rezortu MK v oblasti ICT.

Popsané vize a strategie představují konceptuální záměr, který je z pohledu řízení a poskytování služeb ICT závazný a musí být v jednotlivých diskutovaných oblastech dále rozpracováván. Dokument je tak zastřešujícím dokumentem pro další rozvoj ICT MK s tím, že je možno předběžně rozlišit dvě fáze:

a) fázi stabilizační - v jejímž rámci dojde k zajištění provozu ICT MK na požadované úrovni efektivity a bezpečnosti,

b) fázi rozvojovou - která bude zaměřena na využití nástrojů eCulture pro využití digitalizace kulturního obsahu a veřejných kulturních služeb pro podporu posilování institucionální kapacity účinné veřejné správy v oblasti kultury, kreativity, inovací a znalostní ekonomiky a zároveň pro zatraktivnění českého kulturního dědictví jako celku prostřednictvím informačních a komunikačních technologií tak, aby toto zaujalo mladou generaci a zahraniční návštěvníky. Jako příklad můžeme uvést využití mobilních přístrojů a rozšířené reality k vzdělávání návštěvníků muzeí hravou formou či využití kontinuálního datového toku k vyhodnocování atraktivity exponátů pro případná jednání se sponzory.

V předkládané strategii je akcentována především fáze stabilizační, fáze rozvojová je zachycena především v kapitole 5.1.2 - Aktuální trendy a digitální transformace. Předkladatel předpokládá zpracování dílčích "vizionářských" dokumentů v průběhu počáteční etapy stabilizační fáze tak, aby mohl být zmapován a formulován možný kulturně politický dopad využití aktuálních ICT trendů a aby

následně mohlo dojít k aktualizaci předkládaného dokumentu s cílem modernizace nejen ICT infrastruktury, nýbrž i poskytovaných služeb kulturního fondu tak, aby tyto byly adekvátní 21. století a přispěly k vnímání MK jako progresivní instituce.

Standardně se počítá s tím, že plnění tohoto dokumentu bude cca v polovině období, na které je zpracován, vyhodnocen a bude zpracována aktualizace na další období jako střednědobý výhled. Dokument je koncipován takovým způsobem, aby byl srozumitelný i čtenářům, kteří nejsou odborníky v oblasti informačních technologií. Na druhou stranu je snaha uváděné informace prezentovat jasně, jednoznačně a stručně, i když v některých případech se nelze zcela vyhnout použití některých odborných, zpravidla však všeobecně známých, pojmů.

Rozsah dokumentu vychází ze snahy předat čtenáři ucelenou informaci v čase umožňujícím souvislé, nepřerušované přečtení dokumentu. Zvolená míra abstrakce a konkretizace je dána požadovanou dlouhodobou platností dokumentu v období střednědobého výhledu řádově pěti let.

V dokumentu je zapracováno propojení vizí řízení a rozvoje ICT MK se strategickými přístupy řízení jednotlivých oblastí, které všechny musí být řešeny, aby došlo k pokrytí problematiky jako komplexu a nesmí být opomenuty vazby mezi nimi a jejich návaznost.

Rozvojové hledisko je ve strategii zachyceno především prostřednictvím krátkého zmapování aktuálních trendů (mobilita, cloud, sociální sítě, velká dat, internet věcí) a následným cílem implementace digitální platformy pro komunikaci a spolupráci, která by umožnila všechny současné trendové prvky propojit do jednoho smysluplného celku - digitálního prostředí české kultury. V rámci tohoto prostředí bude možný přístup ke všem digitálním (zprostředkovaně i fyzickým obsahům) odkudkoliv v kterémkoliv okamžiku. Na základě profilu uživatele a přístupových práv pak budou poskytované specifické digitální služby - jiné pro badatele či správce sbírek, jiné pro návštěvníky či sponzory.

Neopomenutelnou podmínkou, kterou Strategie splňuje je zasazení do rámce tvořeného Legislativou České republiky (vztahující se k ICT, kybernetické bezpečnosti , státní správě), vnitřními předpisy a dokumenty MK a strategickými dokumenty MK. Základem pro navrhovaný budoucí stav je analýza současného stavu v jednotlivých oblastech. Ta je zpracovaná v základních oblastech, kterých se realizace Strategie bezprostředně týká. Jedná se zejména o řízení ICT, koncová zařízení, systémové služby, síťové a hlasových služby, datová centra, bezpečnosti aplikační služby. Strategie ICT MK uvádí vize rezortu MK, jejichž naplnění zajistí úkoly dané legislativou. Půjde zejména o informační podporu elektronizace a zefektivnění výkonu agend a služeb, které rezort vykonává v rámci veřejné správy, dlouhodobé řízení informačních systémů a poskytování jejich služeb v souladu s legislativou i s technickými a architektonickými principy eGovernmentu v ČR, a v rámci mezinárodní interoperability. Stejně tak o podporu v oblasti tvorby prostředků pro ochranu a zabezpečení rezortem zpracovávaných údajů, informací a poskytovaných služeb, poskytovaných v rezortu i zbytku veřejné správy. V dlouhodobém měřítku pak poskytovaní moderní služby informační společnosti plynoucí z agend, jež rezort vykonává.

Návazně na uvedené vize vytyčuje Strategie sledované cíle, jejich plnění vytvoří podmínky pro IT podporu, naplňování podstaty funkce spravované organizace – zajištění provozní stability všech systémů, efektivní plánování a řízení služeb, standardizace řízení služeb (ITIL, TOGAF), snížení celkových nákladů, zajištění kybernetické a informační bezpečnosti. Dále pak pro konsolidované řízení IT projektů, zajištění kontinuity služeb, soulad s požadavky eGovernmentu a eCulture, zkvalitnění manažerského rozhodování, zvýšení provozní efektivity, digitalizaci národního kulturního

dědictví atd. Závěrečná část strategie je věnována výčtu a definovaní projektů, kterými, bude možné naplňovat vize a cíle Strategie.

3 Slovník pojmů

Zkratka	Význam
AD	Active Directory – systém umožňující administrátorům nastavovat politiky instalovat programy nebo aplikovat aktualizace na počítače.
AIS	Agendový informační systém – ISVS, který slouží k výkonu agendy orgánu veřejné moci.
CDS	Centrální datový sklad
CDÚ	Centralizace dat, decentralizace přístupu, unifikace procesů
CMS 2.0	Modernizované Centrální místo služeb - slouží jako hlavní propojovací místo eGovernmentu
DC	Datové centrum
DDÚ	Dlouhodobé datové úložiště
DHCP	Dynamic Host Configuration Protocol (DHCP) – standartní síťový protokol pro dynamické přidělování síťových parametrů, např. IP adres.
DLP	Data loss prevention - systémy na ochranu dat
DMS	Document management system – řešení pro ukládání a zpřístupňování dokumentů
DNS	Domain Name System je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
EIS JASU	Ekonomický informační systém používaný využívaný MK
ESB	Enterprise Service Bus
G2B	Government to business - používání informačních a komunikačních technologií pro poskytování vládních služeb, výměnu informačních a komunikačních transakcí, integraci různých samostatných systémů a služeb mezi vládou a obchodním sektorem
G2C	Government to citizen - používání informačních a komunikačních technologií pro poskytování vládních služeb, výměnu informačních a komunikačních transakcí, integraci různých samostatných systémů a služeb mezi vládou a zákazníkem (občanem)
G2G	Government to government - používání informačních a komunikačních technologií pro poskytování vládních služeb, výměnu informačních a komunikačních transakcí, integraci různých samostatných systémů a služeb mezi vládami navzájem
GINIS	GINIS SSL MKCR – IS pro spisovou službu využívaný MK
HA	High availability – vysoká dostupnost
HW	Hardware
ICT/IT	Informační a komunikační technologie/Informační technologie
IK	Informační koncepce
IPAM	Internet Protocol Address Management
IPF	Integrační platforma – sjednocující prvek pro integraci datové základny a procesů včetně rozhraní mezi systémy
ISVS	Informační systémy veřejné zprávy
ISZR-	Informační systém základních registrů – ISVS, jehož prostřednictvím je zajišťováno sdílení dat mezi jednotlivými ZR navzájem a ZR a AIS, správa oprávnění přístupu k datům a další činnosti podle zákona o základních registrech.
ITIL	Information Technology Infrastructure Library je soubor praxí prověřených konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních

Zkratka	Význam
	technologií (IT), a to jak ze strany dodavatelů IT služeb, tak i z pohledu zákazníků
JDBC	Java Database Connectivity – Java programátorské rozhraní pro přístup k databázi
MIS	Manažerský informační systém – systém pro analýzu a reporting dat
MITB	Man-in-the-browser – typ útoku na softwarovou aplikaci.
MITM	Man-in-the-middle – typ útoku na softwarovou aplikaci.
MK	Ministerstvo kultury ČR
MS	Obecné označení produktů společnosti Microsoft, v dalším používáno případně ve spojení s úpřesňujícím označením např. MS Windows, MS SQL apod.
NPÚ	Národní památkový ústav
NTP	Network time protocol – síťový protokol pro synchronizaci času.
OAIS	Open Archival Information System je referenční model archivačního systému, který definuje terminologii, procesy, komponenty a datové struktury systému pro uchovávání dat. OAIS vyvinula organizace CCSDS (Consultative Committee for Space Data Systems). OAIS je ISO standardem (ISO 14721: 2003).
OAI-PMH	Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH) – protokol pro sběr popisných metadat záznamů v dlouhodobých archivech.
ODBC	Open Database Connectivity – programátorské rozhraní pro připojení k databázi.
OIT	Odbor informačních technologií
OKbase	Personální informační systém OKbase využívaný MK
PFI	Paměťové a fondové instituce
RIS	Rezortní informační systém
ROB	Registr obyvatel – základní registr, v němž jsou vedeny aktuální referenční údaje o občanech Česka, cizincích s povolením k pobytu nebo cizincích, kterým byla na území České republiky udělena mezinárodní ochrana formou azylu. Gestorem je Ministerstvo vnitra.
ROS	Registr osob – základní registr, v němž jsou vedeny údaje o právnických osobách, podnikajících fyzických osobách nebo orgánech veřejné moci. Gestorem je Český statický úřad.
RPP	Registr práv a povinností – základní registr, v němž jsou vedeny údaje o působnosti orgánů státní moci, právech a povinnostech osob. Gestorem je Ministerstvo vnitra.
RÚIAN	Registr územní identifikace, adres a nemovitostí – základní registr, v němž jsou vedeny údaje o základních územních prvcích, např. území států, krajů, obcí nebo částí obcí, parcel, ulic. Gestorem je Český úřad zeměměřičský a katastrální.
SDDA/SDDO	Smart Data Driven Architecture/Smart Data Driven Organisation – Inteligentní řízení organizace na základě dat
SLA	Service Level Agreement – termín označuje smlouvu sjednanou mezi poskytovatelem služby a jejím konzumentem definující parametry, resp. požadovanou úroveň (či kvalitu) odebírané služby.
SOA	Service Oriented Architecture – architektura orientovaná na služby. Sada principů a metodologií, která doporučuje skládat složité aplikace a jiné systémy ze skupiny na sobě nezávislých komponent poskytujících služby.
SSO	Single-Sign-On: Jednotné přihlašování do aplikací
SW	Software
TOGAF	The Open Group Architecture Framework - Globální standard pro návrh, plánování, implementaci a řízení IT enterprise architektury

Zkratka	Význam
WF	Workflow. Sled dílčích aktivit a rozhodnutí.
ZoKB	Zákon o kybernetické bezpečnosti č. 181/2014 Sb.
ZR	Základní registry – základní registry veřejné správy ČR.

Tabulka 5 Slovník pojmů

4 Rozsah a účel dokumentu

Dokument má za úkol popsat základní strategické cíle a pro útvary spravované ICT MK specifikovat i plán kroků k dosažení těchto cílů. Organizace s vlastním IT oddělením definují postup k dosažení cílů vlastními strategiemi, které však musí být vypracovány v souladu se strategií rezortní. Obsah dokumentu zohledňuje již existující strategické cíle obsažené v jednotlivých strategiích.

Strategie jFe vypracována za účelem strategického plánování rozvoje informatiky MK, resp. celého rezortu MK včetně všech podřízených útvarů. Do budoucna se předpokládá pravidelná aktualizace tak, aby byla platná v delším časovém horizontu. Obsahem strategie je analýza stávajícího stavu, návrh cílového (budoucího chtěného) stavu a plán postupného přechodu do tohoto cílového stavu.

ICT Strategie rezortu MK vychází z role odboru IT jako útvaru, který:

- řídí provoz a rozvoj aplikací a systémů, za jejichž fungování odpovídá, nezávisle na tom, zda je přímo provozuje nebo jeho dostupnost uživatelům zajišťuje formou služby. Věcné požadavky na aplikace a systémy definují věcní garanti,
- konzultuje provoz a rozvoj aplikací a systémů, které spadají do správy podřízených organizačních jednotek (Národní památkový ústav, Národní knihovna, Národní muzeum, Národní divadlo, Národní filmový archiv, Národní galerie v Praze,… atd.), formou strategie a definici standardů v jednotlivých IT oblastech,
- zajišťuje kybernetickou a informační bezpečnost všech provozovaných systémů po technologické a procesní stránce.

Do kompetencí ICT útvaru spadá:

- systémová integrace (řízení vzájemné provázanosti produktů a poskytovaných služeb, které zprostředkovávají uživatelům jednotlivé komponenty),
- datová integrace (řízení vzájemné provázanosti datových zdrojů, resp. zajištění toho, aby data byla ukládána pouze jednou),
- definice řízení k dosažení strategických cílů,
- efektivní nastavení a provádění procesů provozu, rozvoje a péče o uživatele (interní zákazníky),
- vyhodnocování kvality a kvantity plnění smluvních závazků ze strany dodavatelů,
- přijímání reaktivních a proaktivních opatření v případě kybernetických událostí a incidentů v technologické a procesní rovině.

Strategie jsou rozděleny do následujících oblastí a jsou rozpracovány v odpovídajících kapitolách tohoto dokumentu:

- Strategie řízení ICT MK
- Strategie v oblasti koncových zařízení
- Strategie v oblasti systémových služeb
- Strategie v oblasti síťových a hlasových služeb
- Strategie v oblasti datových center/HW infrastruktury

- Strategie v oblasti bezpečnosti ICT
- Strategie v oblasti aplikačních služeb
- Strategie v oblasti digitalizace

4.1.1 Aktuální trendy a digitální transformace

V současné hyperkonkurenční globální ekonomice je klíčovým faktorem úspěchu efektivní schopnost shromažďování relevantních informací pro rozhodování a následná implementace tržně validních rozhodnutí v adekvátním čase a na adekvátním místě. Díky masivnímu využívání informačních technologií dochází k snižování nákladů a zrychlování vývoje, výroby, distribuce výrobků a služeb. Exponenciální růst výkonnosti informačních technologií (Moorův zákon) ve spojitosti s globalizací mění pravidla podnikání. Na jedné straně vysoká efektivita a dostupnost jakýchkoliv vstupů v reálném čase, na straně druhé pak nejistota, zvýšená míra rizika a dříve nevídané turbulence ekonomického prostředí.

Díky IT se začíná vynořovat nový typ skutečnosti – takzvaná virtuální realita. Tato se reálně skládá pouze z „nul a jedniček“ uložených v počítačích, nicméně hraje stále větší roli v tvorbě hodnoty pro zákazníka. Paralelní zpracování dat a Internet jako univerzální médium komunikace a spolupráce mění způsob produkce dříve nevídaným způsobem. Na rozdíl od reálného světa, kde z důvodu fyzického omezení probíhají interakce především prostřednictví kanálů (telefonní rozhovor, obchodní návštěva, porada), je v digitálním světě možná komunikace prostřednictvím platforem, tj. nástrojů, umožňujících komunikaci mnohých osob s mnohými. Platformy jsou soubory digitálních obsahů, ke kterým mohou čtenáři a přispěvatelé přistupovat odkudkoliv a v kterémkoliv okamžiku a v kterých jsou data uchovávána trvale tak, aby mohla být konzultována, prohledávána a vyhodnocována. Přístup k platformě může být omezen přístupovými právy, nicméně cílem nasazení platformy je umožnit nový typ komunikace a spolupráce prostřednictvím digitálně sdílených obsahů (dokumenty, zvukové záznamy, videa, školící obsahy, etc.) přístupných všem členům hodnototvorné komunity.

Příkladem tu může být práce s dokumenty: díky využití počítačových textových procesorů (např. MS Word) jsou dnešní dokumenty jednodušší, méně formální a málokdy se přenášejí v papírové podobě; pořád počítač používáme jako prostou náhradu psacího stroje. Dokument sepíšeme a uložíme, následně jej odesíláme e-mailem. Zde ručně vytvoříme zprávu, ke které dokument následně připojíme. Pokud po adresátovi požadujeme práci s dokumentem, musí tento dokument otevřít a prostřednictvím svého textového procesoru provést korektury, následně dokument uložit (ideálně pod pozměněným názvem) a opět poslat elektronickou poštou zpět, tj. ručně připojit ke svému e-mailu. Jinými slovy, naše činnost v digitálním světě přesně kopíruje postup, který bychom použili, pokud bychom měli k dispozici psací stroj a „normální“ poštu. Výsledkem je, že se ten samý dokument vyskytuje v několika kopiích roztroušený na lokálních harddiscích a v centralizovaných adresářích s nepřehlednou strukturou, nárůst emailové komunikace a narůstající digitální chaos. S tím pak souvisí zbytečné reálně vyčíslitelné ztráty:

- Je složité získat relevantní a aktuální informace. Organizace neví, co o sobě ví a zaměstnancům chybí znalost o tom, co mohou a mají vědět – existují různá úložiště, podklady jsou díky digitálnímu chaosu reálně nedostupné

- Dokumenty v různých verzích – často neaktuální, chybějící kontrola plnění úkolů. Procesy jsou roztříštěné a neprovázané na informační zdroje, dochází k zbytečným prodlevám a opominutím
- Zahlcování zaměstnanců nepotřebnými informacemi a nepotřebnými daty – vznik duplicit a „multiplicit“, špatná orientace v potřebných informacích a datech, ztráta znalostí vázaných na nedostupné informace.

Souhrnně můžeme hovořit o datové potopě. V tradičním chápání může být organizace řízena dobře, nicméně ze systémového hlediska nezvládnutím datové potopy dojde k vytvoření a případnému prohlubování vnitřního deficitu, což může být při socioekonomických turbulencích velmi nákladné.

Aktuálně dochází v ICT světě ke konvergenci pěti směrodatných trendů:

- Mobilní přístroje – chytré telefony a tablety umožňují personalizovaný přístup k datům, informacím, procesům a službám prostřednictvím multidotykového uživatelského rozhraní
- Cloud computing – digitální služby, informace a data dodávaná z „oblaků“ prostřednictvím datových center odkudkoli, kamkoliv, kdykoliv
- Sociální sítě – software, umožňující propojování velkých skupin lidí, prostřednictvím jimi generovaných obsahů a příslušných digitálních služeb
- Velká data (Big Data) – velké objemy dat, které nejdou zpracovávat tradičními přístupy založenými na lineárním chápání procesů
- Internet věcí - reprezentace fyzických věcí v digitálním prostoru prostřednictvím jednoznačné URL adresace a případné softwarové a datové extenze. Internet věcí propojuje fyzický a virtuální prostor do jednoho vyššího celku poskytujícího efektivitu a prožitky kvalitativně nového druhu

Úspěšné organizace 21. století budou ty, kterým se podaří co nejlépe využít výše uvedené trendy a propojit jednotlivé ostrovy znalostí do integrovaného celku provázaného s aktuálními datovými toky a se schopnostmi a kompetencemi zaměstnanců.

Tvorba hodnoty se přesune prvotně do virtuálního světa, principy dělby práce industriálního věku založené na myšlence hierarchicky kontrolovaných lineárních procesů budou překonány kooperačními modely, založenými na otevřených digitalizačních platformách a integraci tržně orientovaných datových toků v reálném čase. Můžeme tu hovořit o novém typu procesů, které souhrnně nazveme **masivně kooperativní**. Patří k nim především rozhodovací procesy nad datovými agregáty v reálném čase, komunikační procesy a procesy spolupráce mnohých s mnohými z různých lokalit též v reálném čase. Díky masivně kooperativním procesům dojde k extrakci znalostí (nyní „uloženo“ v hlavách zaměstnanců) a jejich rozprostření do virtuálního pracovního prostoru organizace. Můžeme začít hovořit o **organizační inteligenci**, neboť dojde k:

- permanentnímu přenosu znalostí mezi jednotlivými odbory – zaměstnanci mohou díky digitalizační platformě lépe a rychleji koordinovat vzájemnou spolupráci a řešení problémů
- permanentnímu přenosu znalostí ve vertikále – management bude mít k dispozici strukturovaná data o vývoji v organizaci a v jejím okolí v reálném čase; zaměstnanci budou mít vhled do strategie organizace a budou chápat smysl svých činností

- přenosu znalostí v čase – každá data, každá informace bude zachycena v systému, což umožní organizační vzdělávání. Bude možno poučit se z minulých aktivit o tom, co bylo úspěšné a efektivní a co naopak zbytečné a ztrátové. Díky extrakci znalostí do digitálního pracovního prostoru organizace nebude ztrácet znalost s odchodem klíčových zaměstnanců.

K budování **organizační inteligence** je třeba naplnit tři základní podmínky:

- Kvalitní systémová architektura – Na organizaci je třeba nahlížet jako na systém propojující osoby a hodnototvorné činnosti reálného světa s modely, informacemi a daty světa virtuálního. Systémová architektura propojuje efektivně oba světy a tím se stává klíčovým faktorem tvorby hodnoty v 21. století
- Adekvátní informační infrastruktura – Integrované uchopení možností virtuálního světa není možné bez kvalitní informační infrastruktury. Tato by měla především umožňovat komunikaci a spolupráci ve virtuálním prostředí, integraci procesně strukturovaných a nestrukturovaných dat v rámci kontinuálního datového toku a srozumitelnou navigaci v informačním prostředí
- Kulturní změna v tvorbě hodnoty – odbor IT zajišťuje služby a rozvoj informační infrastruktury, nicméně nasazení nových technologií a budování virtuálního pracovního prostoru se týká každého zaměstnance organizace. Zaměstnanec je aktivním tvůrcem a správcem obsahu, na jeho orientaci a schopnostech práce ve virtuálním prostředí často závisí úspěch organizace. Proto můžeme hovořit o „malé“ (odbor IT) a „velké“ (všichni zaměstnanci) informatice. Klíčovou kompetencí se pro zaměstnance stává informační gramotnost, kulturní změna je pak především spojena s úpravou stávajících procesů a vyžadováním digitální disciplíny.

Po naplnění základních podmínek se organizace vydává na cestu „chytré organizace“ disponující digitalizovanou organizační inteligencí. Jedná se o organizaci, která prostřednictvím technologie (investice) umožňuje dělat více práce s nižšími náklady, a to nikoliv jednou, nýbrž s využitím exponenciální síly informatiky neustále. Otázka zvládnutí přechodu od fyzické k virtuální produkci je jednou z nejdůležitějších otázek úspěšného řízení organizace, implementace digitální integrační **platformy pro komunikaci a spolupráci** je prvním krokem k vyřešení této otázky.

Transformaci do podoby digitální organizace můžeme nazvat **digitální transformací -** organizace se mění v takzvaný kybersociální systém, v kterém virtální realita neoddeltitelně prorůstá nám známou fyzickou realitou. Můžeme hovořit o hluboké kulturní změně srovnatelné minimálně s nástupem knihtisku. Domníváme se, že přijetí této změny bude mít na společnost velmi pozitivní ekonomicko sociální dopady, nepřijetí této změny pak může vést k ekonomickému zaostávání se všemi průvodními jevy jako je např. vysoká zadluženost státu, nezaměstanost a technologická stagnace. Dále se domníváme, že vhodně nastavená digitální transformace kulturních statků může být vhodným katalyzátorem této pozitivní kulturní změny.

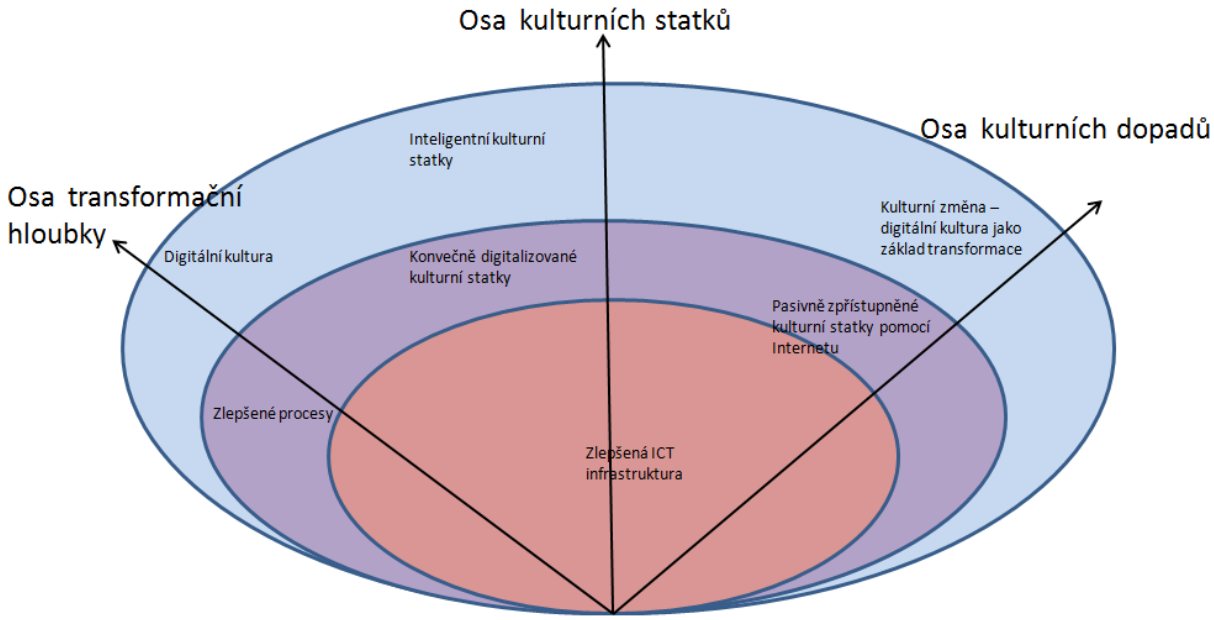
Níže uvedený obrázek nám ukazuje tři osy digitální transformace:

- První osa je osou transformační hloubky - od zlepšené ICT infrastruktury se dostáváme přes zlpešení a zefektivnění kulturního procesu až k inovativní digitální kultuře - kde je digitalizované kulturní dědictví zdrojem a inspirací pro kreativní činnost občanů.

- Druhá osa je osou kulturních statků - zde by mělo dojít k překročení konvenční digitalizace kulturních statků v podobě jejich evidence a pasivní prezentace na Webu k vytvoření

skutečně digitálního kulturního prostředí, ve kterém jsou kulturní statky za pomoci přístupů "Internetu věcí " (senzory, jednoznačná identifikace, umělá inteligence) nadány určitou svébytnou inteligencí a jsou tak například schopny vstupovat aktivně do interakcí s diváky a dalšími participanty v kulturním dění.

- Třetí osa je osou kulturních dopadů - na této ose jsou pasivně zpřístupněné kulturní statky prostřednictvím digitální transformace zapojovány do kulturní transformace společnosti. V digitální ekonomice a kultuře budoucnosti budou algoritmizované činnosti nahrazené strojovou prací, poptávka na trhu práce bude po kreativních činnostech, a proto se může digitalizované kulturní dědictví stát akceleráterem rozsáhlé kulturní změny směrem k digitální transformaci české společnosti.



Obrázek 1 Dopad digitální transformace na kulturu jako celek

5 Zdroje a východiska

5.1 Legislativní rámec

- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů** ve znění pozdějších předpisů, který definuje informační systémy veřejné správy (dále též jen zkráceně „ISVS“) a provozní informační systémy (v dalším může být zkráceně použito pro informační systémy obecně užívané označení „IS“), ukládá orgánům veřejné správy povinnosti týkající se dlouhodobého řízení ISVS a atestační povinnosti ve vztahu k ISVS a dlouhodobému řízení ISVS.
    - **Prováděcí vyhlášky k zákonu č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů**, zejména:
        - **Vyhláška č. 64/2008 Sb.**, o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (**vyhláška o přístupnosti**)
        - **Vyhláška č. 53/2007 Sb**., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (**vyhláška o referenčním rozhraní**)
    - **Vyhláška č. 529/2006 Sb.,** o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (**vyhláška o dlouhodobém řízení informačních systémů veřejné správy**), která definuje strukturu, obsah a řízení informační koncepce a požadavky na provozní dokumentaci.
- **Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů**
- **Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů**
- **Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů**
- **Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů**
- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisůZákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů**
- **Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů**
- **Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů**

- **Zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy a o změně některých dalších zákonů, ve znění pozdějších předpisů**

    - **Vyhláška Ministerstva kultury č. 275/2000 Sb., kterou se provádí zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy a o změně některých dalších zákonů, ve znění vyhlášky č. 96/2013 Sb.**

- **Zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů**

- Zákon č. 496/2012 o audiovizuálních dílech a podpoře kinematografie a o změně dalších zákonů (zákon o audiovizi)**, ve znění pozdějších předpisů**

- **Zákon č. 20/1987 Sb., o státní památkové péči, ve znění pozdějších předpisů**

    - **Vyhláška č. 66/1988 Sb., kterou se provádí zákon č. 20/1987 Sb., o státní památkové péči**

- **Zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon), ve znění pozdějších předpisů**

    - **Vyhláška 88/2002 Sb., k provedení zákona č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon)**

- **Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů**

- **Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů**

- **Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů**

- **Zákon č. 234/2014 Sb., (o státní službě), ve znění pozdějších předpisů**

- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů,** který s účinností od 1. 1. 2015 upravuje práva a povinnosti osob a působnost a pravomoc orgánů veřejné moci v oblasti kybernetické bezpečnosti

a prováděcí vyhlášky k tomuto zákonu, tj.

- **Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti** (vyhláška o kybernetické bezpečnosti), která stanovuje požadavky na systém řízení informační bezpečnosti,

- **Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,** která definuje významný informační systém, a

- **Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.**

- **Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů**
- **Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů**
- **Zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů**
    - **Usnesení vlády č. 689 ze dne 11. září 2013 č. 689 o Plánování, vyhodnocování a koordinaci kontrol výkonu přenesené a samostatné působnosti územních samosprávných celků prováděných ústředními správními úřady, krajskými úřady, Magistrátem hlavního města Prahy a magistráty územně členěných statutárních měst.**

Další právní předpisy, vyhlášky a usnesení vlády, taxativně neuvedeny výše, mohou ovlivňovat tuto strategii ICT, resp. související bezpečnostní politiku zprostředkovaně a nejsou tudíž ve výčtu uvedeny.

5.2 Zdroje informací

Legislativa České republiky

- zákony, vyhlášky a nařízení vlády uvedené v kap. 5.1.1

Vnitřní předpisy a dokumenty MK

- Informace o odboru veřejných zakázek, informatiky a vnitřní správy (25. 4. 2014)
- Digitalizace kulturního dědictví – infrastrukturní část (verze 1.0, 19. 3. 2015)
- Analýza stavu a návrh bezpečnostních opatření pro dosažení souladu se zákonem o kybernetické bezpečnosti (verze 15. 01. 2015)

Strategické dokumenty

- Strategie rozvoje ICT v rezortu MK pro období 2011 – 2014 (verze 1.00, 16. 12. 2011)
- Návrh Státní kulturní politiky na léta 2015-2020 (s výhledem do roku 2025)
- Informační koncepce Ministerstva kultury (verze 1.0, 2. 10. 2014)

Rozhovory s vedoucími a odbornými pracovníky OIT MK

6 Popis současného stavu

6.1 Oblast řízení ICT

6.1.1 Strategické plánování

V oblasti strategického plánování rezortu docházelo k nepravidelné aktualizaci strategie a vize ICT, koncepce ICT atestovaná dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů vznikla až na podzim 2014. Ucelená strategie rezortu neexistuje, ale existují strategie některých podřízených organizací rezortu.

Neexistují formálně definované procesy práce se strategickým plánem, nejsou definovány pravidelné termíny jeho revize a kontroly souladu skutečného vývoje s plánem. Uvedená situace vede ke změnám strategie v souvislosti s organizačními změnami v oblasti ICT rezortu bez příčinné souvislosti se změnou vnějšího prostředí (například v oblasti legislativy) na které musí strategie reagovat.

6.1.2 Řízení architektury

V oblasti řízení architektury panuje roztříštěnost zpracování dílčích oblastí, kdy architektura je navrhována převážně dodavateli a řešiteli dílčích oblastí. Koordinace architektur je řešena parciálním způsobem ze strany ICT odboru a projektové řízení používáno spíše na úrovni mediační.

Neexistuje tak organizační subjekt, kterému by byla svěřena potřebná pravomoc a který by činnost dílčích řešitelů řídil a byl skutečně schopen si vynucovat dodržování celkové architektury, jejich principů a standardů.

Situace dále komplikují nastavené smluvní vztahy s řešiteli, které potřebu řízení architektury opomíjejí, stejně jako nejasné nastavení kompetencí v odpovědnosti za definování uživatelských požadavků mezi zástupci MK, pracovníky podřízených organizací a řešiteli aplikací.

6.1.3 Bezpečnost

V oblasti řízení bezpečnosti aktuálně probíhá příprava pro vytvoření bezpečnostní politiky v souladu s požadavky zákona o kybernetické bezpečnosti. Vzhledem k současnému trendu poskytování klíčových aplikací formou služeb třetích stran v oblasti řešení informatiky velkých organizací je tedy nezbytné ve výše uvedeném kontextu bezpečnostní strategii a politiku aktualizovat a důsledně vyžadovat plnění povinností z nich plynoucí.

V oblasti implementace bezpečnosti nyní nejsou základní bezpečnostní cíle zahrnující ochranu spravovaných informací a řízení přístupu k informacím uspokojivě řešeny.

6.1.4 Projektové řízení a řízení kvality

Projektové řízení v oblasti řízení ICT je na spíše základní úrovni. V současné době vzniká v rámci MK projektová kancelář, která definuje metodiku projektového řízení resortu v obecné rovině, je

plánována její verze pro potřeby ICT. Není definováno organizační ani personální obsazení projektových týmů, role a zodpovědnosti v jednotlivých fázích životního cyklu projektu.

V oblasti řízení kvality není vybudována metodická a předpisová základna. Řízení kvality (SLA) tak probíhá částečně v rámci dílčích projektů bez společného jednotícího faktoru.

6.1.5 Řízení rozvoje

V oblasti rozvoje převažuje nákup služeb od třetích stran před aktivitami vlastních pracovníků ICT MK, což odpovídá stávajícímu personálního zajištění. Nákup služeb probíhá na základě ad-hoc navrhovaných výběrových řízení a smluv normalizovaných pouze v obecné právní rovině.

6.1.6 Zajištění provozu

Provoz aplikací a podpůrných systémů je typicky zajišťován dodavateli řešení a je případně koordinován ze strany pracovníků ICT MK. Poskytované služby nejsou kvalitativně měřeny ani odpovídajícím způsobem kategorizovány. Na úrovni existujících smluv pak SLA v řadě případů nejsou dostatečným způsobem definována.

Provoz je tak zajišťován odborně (na základě odbornosti řešitelů) s úrovní, která vznikla koncensem mezi řešitelem a úřadem a neohrožuje standardní provoz aplikací a systémů. Problémy pak vznikají zejména v okamžiku identifikace problému při snížené kvalitě služby a následného určení zodpovědnosti.

6.1.7 Smluvní zajištění

V oblasti stávajícího smluvní zajištění panuje značná diverzifikace ve smlouvách s jednotlivými řešiteli zejména v oblasti popisu kvality poskytovaných služeb, požadavků na dodržování standardů rezortu v oblasti ICT a řízení architektury.

6.1.8 Legislativní soulad

Soulad s legislativou v oblasti ICT je v současné době realizován na základě odbornosti ICT pracovníků rezortu, účasti na seminářích a školeních. Není definován žádný proces definující zajištění legislativního souladu ani mechanismy kontroly kvality souladu.

6.2 Oblast koncových zařízení

6.2.1 Výběr hardware a nákup zařízení

Nákup nového hardware a výběr použitých zařízení vychází z aktuálních potřeb definovaných aplikačním programovým vybavením a vlastním procesem zpracování dat na pracovišti organizace. Zavedený systém centrálního nákupu zařízení přispívá k jednotnosti použitého hardware, především v oblasti pracovních stanic a připojených periferních zařízeních. Do tohoto procesu nejsou v současné době zahrnuty nově se rozvíjející oblasti mobilních zařízení.

6.2.2 Evidence hardware

Evidence hardware je plně podřízena majetkové evidenci, včetně procesu zavedení nového zařízení do evidence. Vlastní proces je zcela mimo působnost oddělení informačních a komunikačních technologií a nejsou do něj zahrnuty potřeby ICT.

6.2.3 Instalace základního operačního systému

Operační systém je na zařízení instalován s využitím předpřipravených image a systémů pro jeho distribuci. Pro 64 bit systémy je využit nástroj clonezilla, 32 bit systémy využívají wim soubory s následnou doinstalací programů skriptem. V rámci sjednocení operačních systému na 64 bit, bude využíván jen jeden systém distribuce v prostředí MK (ne rezortu). V rámci rezortu ani jednotlivých organizačních složek není zajištěna jednotnost používaných prostředků. Současné řešení do systému vnáší chybu rozdílné konfigurace.

V rámci rezortu není zavedeno před-produkční testování ani jednotnost verzí operačního systému.

6.2.4 Instalace aplikačního programového vybavení

Obdobně, jako v případě instalace základního operačního systému, není zaveden jednotný systém ani při instalaci aplikačního programového vybavení. V systému jsou pro distribuci software použity nativní prostředky operačního systému, aplikace třetích stran i ruční metoda.

6.2.5 Evidence software

Evidence software je prováděna jen nárazově, a to z důvodu majetkové evidence. Výstupy této evidence nejsou zapracovány do procesů ICT.

6.2.6 Správa zařízení a software v průběhu provozu

Správa zařízení není jednotná. Každý typ zařízení je spravován samostatně. Jednotná správa neexistuje ani u stejných zařízení v rámci jedné organizační složky.

Pro správu zařízení a instalovaného software jsou používány aplikace třetích stran i speciální nástroje dodané výrobci.

6.2.7 Vyřazení z provozu, likvidace

Po ukončení životnosti jsou zařízení vyřazována dle zákonných povinností státní organizace. V první řadě jsou zařízení nabídnuta k jinému využití a teprve poté je zařízení doporučeno k ekologické likvidaci.

6.2.8 Bezpečnost zařízení a dat na nich uložených

Otázky bezpečnosti dat se týkají především mobilních zařízení, která nejsou chráněna fyzickou bezpečností pracoviště organizace. V současném systému neexistují standardy, které by tuto problematiku řešily.

6.3 Oblast systémových služeb

6.3.1 Adresářové služby (Active Directory)

Organizace MK v současnosti provozuje jednu Active Directory 2003 doménu mkcr.local:

- Tato doména slouží primárně serverům, obsahuje např. také MS Exchange. Dva doménové řadiče jsou v lokalitě MH, jeden v lokalitě NP. Tato doména obsahuje všechny uživatelské účty a uživatelské politiky a MS Exchange se schránkami uživatelů.

Správa domény je zajištěna informatiky MKČR.

6.3.2 Elektronická pošta (MS Exchange)

MK provozuje systém elektronické pošty založený na technologii MS Exchange 2003.

Servery Exchange organizace jsou umístěny v datovém centru MK a spravovány pracovníky ICT MK. V datovém centru MK jsou vzájemně zálohované brány Symantec Brightmail Gateway pro příjem a odesílání elektronické pošty napojené na MS Exchange.

Na poštovních branách jsou implementovány antivirové a antispamové filtry.

Podřízené organizace MK provozují vlastní mailový systém.

6.3.3 Identity management (IDM)

Organizace MK v současnosti neprovozuje žádné řešení pro Identity Management. V první polovině roku 2015 probíhá analýza procesů a postupů životního cyklu uživatelských účtů v organizaci MK a bude připraven projektový záměr možných variant nasazení IDM systému – předpokládáná realizace ve druhé polovině roku 2015.

6.3.4 Antivirový a antispamový systém

Pro antivirovou ochranu serverů a stanic MK se využívá software společnosti Symantec SEP 12.1.4. Připravuje se veřejná zakázka na vysoutěžení nové podpory včetně sofistikované DLP a správy mobilních zařízení.

6.3.5 Systém pro evidenci IT majetku (HW, SW)

V současné době v oblasti správy SW licencí probíhá nasazení nástroje Alvao asset management. Evidence není aktivně propojena s evidencí majetku v účetním systému.

6.3.6 Správa stanic a SW

V současné době se nevyužívá pro distribuci SW balíčků na pracovní stanice žádný systém.

6.3.7 Service Desk

V současné době se využívá HelpDesk systém společnosti Alvao, verze 8.0.

6.3.8 Zálohování

Centrální zálohování je řízeno systémem Legato Networker 7.4.4 instalovaném na dedikovaném fyzickém serveru.

Zálohování je nastaveno jednotně pro všechny systémy. V rámci zálohovacích politik je nastaveno o víkendech plné zálohování (týdenní záloha). V týdnu pak každý den u filesystemu zálohování nárůstové, u databází a Exchange pak zálohování plné (denní záloha). Denní zálohy jsou uchovávány po dobu 14 dní, týdenní po dobu 1 – 2 měsíců v závislosti na množství dat. Zálohy jsou ukládány na vyčleněný diskový prostor zálohovacího serveru a následně přesouvány na pásky prostřednictvím SAN.

Aktuálně neexistuje kontrolní mechanizmus ověřování obnovy zálohovaných systémů. Současně není zajištěna kontrola, zda a jakým způsobem jsou data zálohována.

6.3.9 Archivace dat

Aktuálně není nastaven proces archivace a neexistuje pro něj podpora u jednotlivých informačních systémů.

Žádný z provozovaných systémů nemá archivační režim definován.

6.4 Oblast síťových a hlasových služeb

Komunikační infrastruktura – popis topologie WAN/LAN, směrovače, přepínače, firewally.

Připojení lokalit

Datová centra

MK provozuje dvě neredundantní datová centra – DC Milada Horáková (DC MH) a DC Nostický palác (DC NP). V datových centrech jsou provozovány centrální aplikace a služby, jsou zde terminovány agregační přípojky poskytovatelů datových služeb a také centrální přípojky do Internetu. V datových centrech je umístěna centrální firewallová soustava zajišťující filtrování provozu mezi jednotlivými logickými částmi datové sítě a bezpečné připojení k Internetu.

Externí konektivita

Připojení do Internetu je realizováno nezávisle v obou datových centrech. Přípojky jsou připojeny k firewallové soustavě. Je zajištěna dostupnost služeb jak na IPv4, tak i na IPv6.

Připojení do Centrálního místa služeb (CMS) je realizováno přes privátní okruh GTS sítě přímo do KIVS (Kritická Infrastruktura Veřejných Služeb). Připojení je fyzicky realizováno přes jedinou linku z lokality Nostický palác.

Vzdálený přístup

V současnosti je zařízení Cisco ASA 5510 využíváno jako VPN koncentrátor pro vzdálený přístup uživatelů MK. Fyzicky je toto samostatné zařízení (tedy bez režimu vysoké dostupnosti) umístěno v DC Milady Horákové.

Uživatelé se připojují do sítě MK pomocí vzdáleného VPN přístupu pomocí uživatelského jména a hesla.

Po úspěšné autentizaci klienta následuje jeho autorizace. V rámci sítě MK mají úspěšně autentizovaní uživatelé přístup pouze ke konkrétním vyjmenovaným službám.

Po připojení je veškerý provoz z koncového zařízení odesílán do šifrovaného tunelu, žádná komunikace přímo do internetu zde není možná.

V současnosti se využívá Cisco VPN Klient ver.5.0.07, který již není podporován.

Bezpečnostní prvky (FW)

FW soustava je tvořena hlavní branou CheckPoint v DC MH (redundantně v HA clusteru) a singl CheckPoint branami na pobočkách. Soustava využívá nejen filtrování provozu na základě pravidel, ale i další pokročilé technologie pro sledování provozu (DLP – ztráta dat, IPS – ochrana před napadením), které aktivně brání škodlivému provozu (DDoS, ICMP útoky, scan portů a jiné).

Služby sítě

DNS, DHCP, NTP

Monitoring komunikační infrastruktury

V současnosti není využíván žádný proaktivní systém monitoringu, je pouze nasazeno sledování dostupnosti jednotlivých prvků v síti, a to prostřednictvím aplikace NAGIOS. V pravidelných intervalech je ověřována dostupnost serverů a aktivních prvků a v případě chyby je zaslána e-mailová notifikace na správce systému.

Hlasové služby

Hlasové služby zajišťuje telefonní ústředna, která je přes 10 telefonních linek připojena do veřejné telefonní sítě. Umožňuje přímou provolbu na konkrétního zaměstnance ministerstva, odpadají tedy služby spojovatelky. Ústředna je vybavena rovněž GSM bránou, která umožňuje volání z a do mobilních sítí za nižší režiji. Komunikační systém byl rozšířen o hlasovou a obrazovou techniku, která umožňuje videokonferenční jednání s libovolným účastníkem kdekoliv na světě. Veškerá komunikace je zabezpečená šifrováním a lze využít i mobilní klienty v chytrých telefonech či přenosných PC.

6.5 Oblast datových center / HW infrastruktury

6.5.1 Datová centra MK

Datová centra rezortu jsou umístěna na adrese:

- Milady Horákové 139, Praha 6
- Nostický Palác, Maltézské nám. 471/1, Praha 1
- DC dalších rozpočtových a jiných organizací rezortu.

Jádro sítě tvoří lokalita Milady Horákové, kde je zakončeno připojení do Internetu. Konektivita lokality do Internetu je 34 Mbit. Připojení do Internetu je zajištěno hraničním firewallem v lokalitě

Milady Horákové. Hraniční firewall je pro případ výpadku zálohován druhým se stejnou konfigurací, který je poskytnut společností ANECT a.s..

Ostatní lokality jsou připojeny zabezpečeným tunelem k lokalitě Milady Horákové a dále přes hraniční firewall do Internetu prostřednictvím připojení Milady Horákové. Lokality Milady Horákové a Nostický palác jsou propojeny pronajatým optickým vláknem a paralelním záložním bezdrátovým spojem. Lokalita Nostický palác disponuje přímým připojením do Internetu o konektivitě 6Mbit/s. Toto přímé připojení je v současnosti využíváno pouze pro připojení uživatelů k Internetu v konferenční místnosti „Konírna“ prostřednictvím lokální wifi. Uvedené 6Mbit/s připojení v Nostickém paláci je možné využít jako záložní připojení MK do Internetu, ale není nastavena automatická rekonfigurace v případě výpadku připojení lokality Milady Horákové. V případě výpadku by se musela rekonfigurace provést manuálně.

Počet připojených stanic v jednotlivých lokalitách:
Milady Horákové 139 – cca 160
Nostický Palác – cca 100
Vila Bubeneč – 8
Národní Galerie – 12

Celková topologie sítě je vzhledem k potřebám MK vyhovující a konektivita k Internetu dostatečná. Bylo by však z bezpečnostního hlediska vhodné přemístit jeden z hraničních firewallů z lokality Milady Horákové do Nostického paláce, aby v případě výpadku připojení do Internetu bylo možné provést automatické přesměrování provozu na záložní konektivitu z Nostického paláce.

Příspěvkové organizace:
Každá příspěvková organizace zajišťuje nákup a správu prostředků infrastruktury ve vlastní gesci.
V současnosti neexistuje plán na centrální pořízení služeb konektivity do Internetu pro všechny příspěvkové organizace.

6.5.2 Infrastruktura DC

V rámci datových center je umístěna technologie, která je z větší části zastaralá, rozvoj infrastruktury datových center v posledních letech stagnoval.

6.5.3 Databázová vrstva

Databázová vrstva je dnes řešena pomocí dvou MS SQL serverů ve verzích 2005 a 2008.

6.5.4 Disková vrstva

Disková kapacita je poskytována centrálně jako služba, ale prostředky jsou již zastaralé. Disková kapacita je poskytována prostřednictvím zařízení:

- Dell EMC CX3-20
- IBM DS3524
- NetApp FAS2240-2

Z výčtu vyplývá, že je nutné provést sjednocení diskových polí na jednu technologii, jelikož provoz těchto technologií není nadále finančně a administrativně únosný.

Disková kapacita je cca 25 TB.

Disková kapacita je k serverům připojena pomocí SAN Infrastruktury pomocí tří prvků Brocade o rychlostech 4, 8, 8/16 Gb.

6.5.5 Aplikační a prezentační vrstva

Stav březen/2015

Aplikační vrstva není konsolidovaná do serverů s vysokou hustotou výkonu, „blade serverů“. Většina infrastruktury používá standalone servery. Další část serverů je z pohledu životnosti již na hranici efektivity provozu a oprav. Celkem je v datových centrech instalováno 30 serverů, z toho 17 je starších než 4 roky.

Součástí aplikační vrstvy je virtualizace za použití virtualizačního SW VMware vSphere 4.1 Essential Plus.

Stav květen/2015

Aplikační vrstva je konsolidovaná do serverů s vysokou hustotou výkonu, „blade serverů“. Většina infrastruktury používá virtuální servery. Celkem je v datových centrech instalováno 30 serverů.

Součástí aplikační vrstvy je virtualizace za použití virtualizačního SW VMware vSOM Enterprise Plus (verze 5.5).

6.5.6 Centrální zálohování

Stav březen/2015

Centrální zálohování je postaveno na páskové knihovně Dell ML6000 a na SW Legato Networker.7.4.4.

Stav *květen/2015*

Virtuální infrastruktura je zálohována SW Veeam Backup & Replication Enterprise (verze 8).

6.5.7 Klasifikace dostupnosti služeb DC

- **Dostupnost systémů**

Provozované systémy nejsou rozděleny do skupin dle charakteru provozu z hlediska požadované dostupnosti systémů.

- **Využití systémových zdrojů DC jako služby**

Systémové zdroje - servery, disková úložiště jsou koncipována jako univerzální zdroj pro potřeby aplikací. Platí následující pravidla:

Diskový prostor je přidělován primárně z centrálních diskových polí. Je tak zajištěna potřebná úroveň zabezpečení a výkonu. Jde také o opatření zabezpečující efektivitu provozu - po uvolnění prostoru jedním systémem jej lze přidělit pro systém jiný, potřebná provozní rezerva může být sdílena pro více účelů.

Servery databázové vrstvy jsou rovněž budovány jako univerzální prostředek, jejich užití pro informační systémy lze sdílet, popřípadě se může v průběhu času měnit.

Aplikační servery jsou spravovány převážně jako souhrn zdrojů, které jsou přidělovány podle potřeby jednotlivým informačním systémům ,resp. aplikacím. V případě snížení náročnosti aplikace, nebo při ukončení jejího provozu lze uvolněné zdroje (výkon serverů) použít pro aplikaci jinou.

6.6 Oblast bezpečnosti

V závěru roku 2014 si vedení ICT MK nechalo zpracovat analýzu současného stavu bezpečnostního prostředí v rezortu MK zejména s ohledem na míru naplnění shody procesních bezpečnostních opatření, komunikační infrastruktury, bezpečnostních technologií a informačních systémů MK s požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. (dále ZKB) kladených na významné informační systémy.

Analýza a hodnocení aktuálního stavu bylo realizováno s ohledem na opatření specifikovaná v ZKB a pokrývá následující oblasti:

- **Organizační**

a) systém řízení bezpečnosti informací b) řízení rizik c) bezpečnostní politika d) organizační bezpečnost e) stanovení bezpečnostních požadavků pro dodavatele f) řízení aktiv g) bezpečnost lidských zdrojů h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému	i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů l) řízení kontinuity činností m) kontrola a audit kritické informační infrastruktury a významných informačních systémů

- **Technická**

a) fyzická bezpečnost b) nástroj pro ochranu integrity komunikačních sítí c) nástroj pro ověřování identity uživatelů d) nástroj pro řízení přístupových oprávnění e) nástroj pro ochranu před škodlivým kódem f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů	g) nástroj pro detekci kybernetických bezpečnostních událostí h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí i) aplikační bezpečnost j) kryptografické prostředky k) nástroj pro zajišťování úrovně dostupnosti informací l) bezpečnost průmyslových a řídicích systémů

Z výsledků analýzy všech analyzovaných oblastí vyplynulo, že drtivá většina opatření není s požadavky ZKB ve shodě vůbec či pouze částečně a je nutné realizovat množství opatření, aby byly naplněny legislativní požadavky. Tyto jsou dále uvedeny v kap. 8 – Plán strategických projektů.

6.7 Oblast aplikačních služeb

6.7.1 Oblast IT potřeb věcných agend

Potřeby jednotlivých agend IT MK plní pomocí zajištění služeb svých dodavatelů. IT MK má zaveden proces sběru požadavků věcných agend pro již existující systémy. Nicméně nemá zaveden proces proaktivního sběru požadavků na agendy, které má odbor IT nově podporovat.

IT MK také neřeší rozšíření nakupovaných služeb mezi své uživatele, kteří tak v některých případech nemají zajištěnou informační podporu ani v případech, že dodavatel dodal plnění.

Mezi věcné agendy, které je třeba aplikačně podporovat na MK, patří:

- Evidence českých audiovizuálních děl
- Evidence jiných než českých audiovizuálních děl
- Evidence knihoven
- Evidence periodického tisku
- Evidence podnikatelů v oblasti audiovize
- Seznam kulturních památek
- Informační systém církví a náboženských společností
- Seznam osob s povolením k restaurování
- Registr oznámení o činnostech, oznámení o majetku a oznámení o příjmech, darech a závazcích
- Seznam osob, kterým bylo uděleno povolení k provádění archeologických výzkumů

Z výše uvedených ISVS ve správě MK byly, na základě zákona č. 496/2012 Sb., o audiovizuálních dílech a podpoře kinematografie a o změně některých zákonů (zákon o audiovizi), Evidence českých audiovizuálních děl, Evidence jiných než českých audiovizuálních děl a Evidence podnikatelů v oblasti audiovize převedeny na příspěvkové organizace MK (Národní filmový archiv a Státní fond kinematografie).

Seznam kulturních památek je, na základě zmocnění v zákoně, veden Národním památkovým ústavem. Stejně tak Seznam osob s povolením k restaurování je, na základě pověření, provozován Národním památkovým ústavem, nicméně za kvalitu dat v tomto seznamu a komunikaci se základními registry odpovídá MK.

Tyto agendy jsou podporovány, ale není v dostatečném rozsahu zajištěno řešení změnových požadavků daných legislativou nebo uživatelských požadavků, popř. je problém se školením uživatelů.

6.7.1.1 Informační systém církví a náboženských společností (IS CNS)

Název IS	Informační systém církví a náboženských společností
Zkratka názvu	IS CNS

Typ IS	Informační systém veřejné správy
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor církví
Právní předpisy zakotvující IS	zákon č. 3/2002 Sb., vyhláška č. 232/2002 Sb.
Registrační číslo v IS o ISVS	168

Tabulka 6: Základní údaje informačního systému

6.7.1.1.1 Charakteristika informačního systému

IS byl vytvořen na základě úkolu zajistit vedení rejstříku registrovaných církví a náboženských společností a rejstříku evidovaných právnických osob evidovaných dle zákona č. 3/2002 Sb., o svobodě náboženského vyznání a postavení církví a náboženských společností a o změně některých zákonů (zákon o církvích a náboženských společnostech).

Zpracovávaná data

IS CNS zpracovává následující data:

- Údaje o registrovaných církvích a náboženských společnostech a jejich svazech
- Údaje o evidovaných právnických osobách dle zákona č. 3/2002Sb.

Zajišťované služby a vazby na ostatní systémy

IS CNS zajišťuje následující služby:

- Webové služby spojené se zveřejňováním povinných informací
- Vedení rejstříku registrovaných církví a náboženských společností
- Vedení rejstříku svazů církví a náboženských společnostíVedení rejstříku evidovaných právnických osob dle zákona č. 3/2002 Sb.
- Vazba na základní registr osob
- Vazba na základní registr územní identifikace a adres

Technické a programové prostředky

HW prostředí sdíleno s ostatními aplikace MK. SW budován dodavatelsky.

6.7.1.1.2 Současný stav

Aplikace pro IS CNS je řešena jako Klient/Server aplikace s grafickým uživatelským rozhraním. Jedná se o prostředí MS Windows a databázový server SQL Server firmy Microsoft. Serverová část aplikace je provozována pod operačním systémem MS Windows Server a databázovým systémem MS SQL Server. Klientská část aplikace je provozována v prostředí MS Windows. Informace poskytované prostřednictvím Web technologií jsou optimalizovány pro prohlížeč Internet Explorer verze 6.0 a vyšší.

6.7.1.1.3 Předpokládané změny

Vzhledem zastaralosti systému, nákladné podpoře a vysokým nákladům na rozvoj systému a udržování rozhraní vůči systémům základních registrů bylo rozhodnuto současný systém nahradit novým, uživatelsky přívětivějším systémem

V rámci nasazení nového systému se očekává vybudování vazby na spisovou službu GINIS.

6.7.1.2 Evidence knihoven

Název IS	Evidence knihoven
Zkratka názvu	---
Typ IS	Informační systém veřejné správy
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor umění, literatury a knihoven
Právní předpisy zakotvující IS	zákon č. 257/2001 Sb.
Registrační číslo v IS o ISVS	823

Tabulka 7: Základní údaje informačního systému

6.7.1.2.1 Charakteristika informačního systému

Systém určen pro podporu evidence knihoven.

Zpracovávaná data

Systém zpracovává následující data:

- Údaje o evidovaných knihovnách

Zajišťované služby a vazby na ostatní systémy

- Vedení seznamu evidovaných knihoven

Technické a programové prostředky

Systém nemá žádné přímé nároky na HW a SW (viz následující kapitola).

6.7.1.2.2 Současný stav

Primárně je evidence knihoven vedena v xls souboru pracovníky MK. Soubor je po pravidelně po aktualizaci vystavován na webové prezentaci MK.

6.7.1.2.3 Předpokládané změny

Vzhledem k stávajícímu stavu je nutné toto řešení nahradit sofistikovanějším, včetně vybudování odpovídajících vazeb na základní registry.

Evidence knihoven, Evidence periodického tisku a Evidence restaurátorů budou v budoucnu sloučeny v jeden komplexního evidenční systém MK.

6.7.1.3 Centrální evidence sbírek (CES)

Název IS	Centrální evidence sbírek
Zkratka názvu	CES
Typ IS	Informační systém veřejné správy
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor ochrany movitého kulturního dědictví, muzeí a galerií
Právní předpisy zakotvující IS	zákon č. 122/2000 Sb.
Registrační číslo v IS o ISVS	Zatím není evidován v IS o ISVS

Tabulka 8: Základní údaje informačního systému

6.7.1.3.1 Charakteristika informačního systému

Jedná se o první databázový systém zaměřený na správu muzejních sbírek. Od roku 2006 jsou do systému vkládány obrazové informace tak, aby byla maximalizována výpovědní hodnota systému.

Zpracovávaná data

- Údaje o muzejních sbírkách

Zajišťované služby a vazby na ostatní systémy

- Webová prezentace sbírek muzejní povahy
- Evidence sbírek muzejní povahy

Technické a programové prostředky

HW prostředí sdíleno s ostatními aplikacemi MK. SW bude budován dodavatelsky.

6.7.1.3.2 Současný stav

Stávající CES není interoperabilní s jinými systémy (např. policejní databáze). Není uživatelsky přívětivý pro správce sbírek při provádění ze zákona povinných hlášení změn stavu sbírek – stále funguje na bázi potvrzování změn prostřednictvím poštou zasílaných listinných formulářů. Systém správy evidenčních čísel sbírek není dosažitelný pro správce sbírek prostřednictvím Internetu, ke komunikaci je nezbytný meziprvek – program CESik (na platformě MS Access), který s sebou přináší řadu problémů daných technologickými možnostmi (nesoulad čísel, omyly, ztráty dat…).

Technická dokumentace je k dispozici (odbor OMG).

6.7.1.3.3 Předpokládané změny

Umožnit online přístupnost pro správce sbírek – změny v systému, namísto listinné žádosti by vkládání dat prováděli přímo správcové sbírek. Pracovník MK by poté pouze jednotlivé provedené změny autorizoval.

Doplnění o provázání sbírkového evidenčního čísla na stručný popis sbírkového předmětu, případně na obrazový náhled předmětu.

6.7.1.4 Seznam osob s povolením k restaurování (Seznam restaurátorů)

Název IS	Seznam osob s povolením k restaurování
Zkratka názvu	Seznam restaurátorů
Typ IS	Informační systém veřejné správy
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor památkové péče
Právní předpisy zakotvující IS	zákon č. 20/1987 Sb.
Registrační číslo v IS o ISVS	875

Tabulka 9: Základní údaje informačního systému

6.7.1.4.1 Charakteristika informačního systému

Evidence vede, v souladu s příslušným zákonem, seznam osob s oprávněním k restaurováním. V případě, že se jedná o občana ČR nebo cizince s trvalým pobytem na území ČR a požádá o povolení k restaurování je zapsán do seznamu osob s povolením k restaurování.

V případě, že se na území ČR provádí restaurátorské práce restaurátor, který není občanem ČR a ani nemá trvalý pobyt na území ČR a je zapsán do obdobného seznamu v členském státě EU, plní pouze ohlašovací povinnost, která se provádí v papírové formě a není vedena v elektronické podobě.

Zpracovávaná data

- Údaje o osobách s povolením k restaurování

Zajišťované služby a vazby na ostatní systémy

- Vyhledávání osob s povolením k restaurování

Technické a programové prostředky

Evidence je provozována na platformě vytvářené NPÚ a její veřejná část je přes webové rozhraní.

6.7.1.4.2 Současný stav

Dosavadní právní úprava na úseku památkové péče předpokládá vedení tří samostatných rejstříků. Údaje o restaurátorech, kterým bylo uděleno povolení k restaurování podle dosavadních právních předpisů, jsou obsažené v Seznamu osob s povolením k restaurování. Údaje o osobách oprávněných k restaurování (tedy o osobách, které oznámily svůj záměr provést restaurování v rámci svobody poskytování služeb, přiložily stanovené doklady a zároveň doložily stanovené náležitosti oznámení) jsou obsaženy v evidenci osob oprávněných k restaurování. Údaje o uchazečích, kterým bylo uděleno povolení k provádění archeologických výzkumů v souvislosti se systémem uznávání odborné kvalifikace a jiné způsobilosti získané v jiných členských státech Evropské unie, jsou obsažené v evidenci uchazečů, kterým bylo uděleno povolení k provádění archeologických výzkumů a osob

oprávněných k výzkumům. V evidenci uchazečů, kterým bylo uděleno povolení k provádění archeologických výzkumů, a osob oprávněných k výzkumům jsou současně obsaženy údaje o osobách oprávněných k výzkumům (tedy o osobách, které oznámily svůj záměr provést archeologický výzkum v rámci svobody poskytování služeb, přiložily stanovené doklady a zároveň doložily stanovené náležitosti oznámení). Údaje o tuzemských oprávněných organizacích tedy o osobách oprávněných k provádění archeologických výzkumů se v žádném specifickém rejstříku podle dosavadní právní úpravy nevedou, jejich informativní seznam v podobě excelové tabulky je však na webu MK umístěn.

Seznam osob s povolením k restaurování není online napojen na základní registry a neumožňuje evidovat IČO restaurátora. Vazba mezi základními registry (ROS a ROB) je prováděna manuálně pracovníkem MK, který ověřené údaje předává NPÚ.

6.7.1.4.3 Předpokládané změny

Vzhledem k nutnosti napojení IS na základní rejstříky bude třeba současný systém upravit nebo nahradit novým.

Evidence knihoven, Evidence periodického tisku a Evidence restaurátorů budou v budoucnu sloučeny v jeden komplexní evidenční systém MK.

6.7.1.5 Evidence periodického tisku (MKEPT)

Název IS	Evidence periodického tisku
Zkratka názvu	MKEPT
Typ IS	Informační systém veřejné správy
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor médií a audiovize
Právní předpisy zakotvující IS	zákon č. 46/2000 Sb.
Registrační číslo v IS o ISVS	824

Tabulka 10: Základní údaje informačního systému

6.7.1.5.1 Charakteristika informačního systému

Systém byl vyvinut k evidenci periodického tisku.

Zpracovávaná data

- Údaje o periodickém tisku

Zajišťované služby a vazby na ostatní systémy

- Vedení evidence periodického tisku

Technické a programové prostředky

HW prostředí sdíleno s ostatními aplikacemi MK. SW bude budován dodavatelsky.

6.7.1.5.2 Současný stav

Systém byl vyvinut na základě specifikace pracovníků odboru médií a audiovize. Nadále však systém není žádným způsobem rozvíjen a neexistuje k němu žádná dokumentace.

Systém je prostou evidencí splňující požadavky zákona. Konečným uživatelům však neposkytuje žádné informace nad rámec zákonných povinností. Prezentační modul je pro veřejnost dostupný přes web MK.

Velkým nedostatkem je Case-sensitive vyhledávání v rámci prezentační vrstvy.

6.7.1.5.3 Předpokládané změny

Evidence knihoven, Evidence periodického tisku a Evidence restaurátorů budou v budoucnu sloučeny v jeden komplexní evidenční systém MK.

6.7.1.6 Informační systém Legislativní mapa

6.7.1.6.1 Současný stav

K 1. 7. 2015 se předpokládá spuštění informačního systému „Legislativní mapa“, který by měl od sloužit k efektivnější administraci vývozů sbírkových předmětů do zahraničí. Systém je navržen pro potřeby správců sbírek v příspěvkových organizacích Ministerstva kultury. Je realizován ve spolupráci s Moravským zemským muzeem.

6.7.1.6.2 Charakteristika informačního systému

Legislativní mapa vývozů je internetová aplikace, jejímž hlavním cílem je podstatné zefektivnění a zjednodušení administrativních činností Ministerstva kultury České republiky a jeho příspěvkových organizací při vývozu sbírkových předmětů do zahraničí. V tomto elektronickém systému se pověřený pracovník libovolné příspěvkové organizace MK dozví vše podstatné k získání právně závazných dokumentů proti zabavitelnosti sbírkových předmětů v zahraničí (vychází z důsledků sporu ČR a firmy Diag Human). Kromě toho se dozví i další důležité a aktuální informace pro uskutečnění bezproblémového vývozu.

6.7.2 Oblast IT potřeb průřezových procesů agend a sdílených komponent

Mezi průřezové procesy agend a sdílené komponenty, které je nutné řešit na strategické úrovni, patří např. externí portál (dnes provozovaný na adrese http://www.mkcr.cz/). Ostatní aplikace (např. spisová služba GINIS), které spadají do této kategorie, budou v případě potřeby řešeny standardními prostředky řízení IT MK. Těmito prostředky je míněno především identifikace potřeby na novou aplikaci ,resp. modernizaci stávající zastaralé verze, vypsání otevřeného výběrového řízení, realizace projektu, příjem služeb a vyhodnocování kvality služby atd.

Dále např. poskytování statistik a dat minimálně z agendových systémů je pro práci manažerů MK ,resp. podřízených organizací klíčovou složkou, protože jinak nemají relevantní informace pro svou práci a agendy jsou řízeny bez správných informací, tedy spíše metodou pokus omyl a není možné hovořit o systematické činnosti a řešení klíčových problémů.

Pro řádnou práci v rámci celého rezortu je pak nutné propojit data z MK a alespoň vybraných klíčových podřízených organizací. Bez tohoto propojení bude vždy možné provádět manažerské rozhodování pouze lokálních problémů jednotlivých organizačních složek rezortu, ale nikdy nepůjde o systémové řízení problémů rezortu jako celku, které je tolik potřebné a dlouhodobě neřešené.

Co nejdříve je třeba závést integrovanou digitální platformu národního kulturního dědictví, prostřednictvím které budou sjednocena důležitá data tak, aby tato mohl sloužit k tvorbě inovativních datových produktů.

6.7.3 Oblast konsolidovaného řízení datových zdrojů

Klíčový potenciál zlepšení situace digitalizace národního kulturního dědictví představuje především zachycení aktuálních trendů: internetu v chytrých telefonech, cloud computingu, velkých dat, sociálních sítí a internetu věcí. Prostřednictvím národní digitální platformy bude možno vytvořit sjednocený datový prostor, v jehož rámci bude možno kombinovat datovou správu, využití dat, datovou analytiku a reporting. Sjednocená datová základna pak povede na jedné straně k radikálnímu zvýšení efektivity, zrychlení a zpřesnění manažerského rozhodování na straně jedné a k možnosti poskytování nových vysoce inovativních datových produktů pro využití aktuálními technologiemi a tím i ke zvýšení marketingového potenciálu národního kulturního dědictví.

6.7.4 Oblast doplňkových aplikací

IT MK provozuje aplikace pro podporu běžných nebo naopak specifických věcných potřeb uživatelů. Tyto aplikace nejsou důsledně řízené, není jasné, které aplikace se ještě používají a které nikoli a není ani zřejmé, jak moc jsou uživatelé spokojeni s jednotlivými aplikacemi. Lze očekávat, že spokojenost s řadou z nich je velmi nízká.

6.7.5 Oblast IT podpůrných systémů

Mezi podpůrné systémy řešené na úrovni strategie patří aplikace pro podporu ekonomiky (účetnictví) a personalistiky, dále groupware (intranet a e-mail). Ostatní organizace rezortu si řeší intranet a e-mail svými silami. Provoz ekonomiky a personalistiky řeší MK a podřízené organizace rezortu zcela samostatně.

Typ	Název	Zkratka
Provozní IS s vazbami na ISVS	Personální informační systém	OKbase
Provozní IS bez vazby na ISVS	Ekonomický informační systém	EIS JASU
	Docházkový a přístupový informační systém	AKTION
	Systém pro centrální řízení tiskových služeb	SafeQ

Tabulka 11: Přehled podpůrných IS MK

6.7.6 Oblast integrací aplikačních služeb

Na současný svět, ve kterém vzniká obrovský objem dat o každé osobě, ve kterém existují možnosti zpracování těchto dat a existuje možnost využití výsledků pro manažerské řízení je IT MK naprosto nepřipraveno. IT MK je v oblasti integrací aplikačních služeb na základní úrovni a má problém se zajištěním dat pro základní statistiky v rámci MK popř. podřízených organizací. Propojení dat mezi podřízenými organizacemi je řešeno ad-hoc a občas vůbec. Propojení dat mezi systémy, které vlastní nebo provozuje IT MK je v podobné situaci. IT MK není prakticky schopno plnit uživatelské požadavky na integraci systémů a dat, tak jak přicházejí a uživatelé je potřebují.

Mezi prakticky nefungující integrace patří i zajištění integrací s externími organizacemi jako jsou např. základní registry.

6.7.7 Oblasti správy licencí

IT MK má velké množství licencí, u některých je jasné, jak a kdo je používá, u některých to zřejmé není. IT MK nemá nastavený proces pro správu licencí včetně jejich nákupu. Není tak jasné, jak moc efektivně jsou vynakládané prostředky na nákup licencí. V současné chvíli probíhá na MK příprava SAM auditu licencí Microsoft, mimo jiné pomocí nástroje společnosti Alvao. Cílem je mít zmapovaný počet užitých licencí, počet případně nutných licencí k nákupu a nastavení procesu s cílem provádět pravidelný softwarový audit dle vládní vyhlášky.

7 Návrh budoucího stavu

7.1 Poslání a vize ICT

Informatika a informační technologie jsou disciplíny, bez kterých již není možno plnit úkoly dané legislativou rezortu. Přes svoji nezbytnost je však informatika disciplínou servisní, umožňující plnit primární úkoly vyplývající z poslání MK jakožto rezortu veřejné správy.

Uváděné vize a strategie jejich naplnění jsou plně v souladu s informační strategií státu a rozvojem eGovernmentu, a to nejen v oblastech legislativy, koncepce, architektury a standardů, ale též v oblastech mezirezortní kooperace a financování chodu státu.

V rezortu MK je tak poslání informatiky následující:

- Zajistit informační podporu elektronizace a zefektivnění výkonu agend a služeb, které rezort vykonává v rámci veřejné správy a služeb pro svoje klienty, ať už plně elektronických, či poskytovaných s podporou elektronizace.
- Zajistit dlouhodobé řízení informačních systémů a poskytování jejich služeb v souladu s legislativou i s technickými a architektonickými principy eGovernmentu jak v ČR, tak v rámci mezinárodní interoperability.
- Poskytovat nástroje pro řízení rezortu na základě možností včasného, hromadného zpracování informací a údajů.
- Poskytovat prostředky pro ochranu a zabezpečení rezortem zpracovávaných údajů, informací a poskytovaných služeb.
- Vyhledávat a případně realizovat nové způsoby zpracování informací vyplývajících z rozvoje informatizace.
- Poskytovat rezortu i zbytku veřejné správy služby informační společnosti plynoucí z agend, jež rezort vykonává, a to se zachováním významné bezpečnosti a také kvality poskytovaných služeb.
- Řídit v dlouhodobém měřítku kvalitu informačních služeb a informačních systémů provozovaných rezortem a jeho orgány veřejné moci.
- Rozvíjet moderní elektronické služby pro klienty.

Uvedené poslání informatiky rezortu MK musí být naplňováno efektivně, bez zbytečných nákladů avšak umožňující poskytování služeb občanům v kvalitě srovnatelné s kvalitou běžnou v komerční sféře a oblasti veřejných služeb států Evropské unie.

Oblast informačních a komunikačních technologií rezortu MK (dále jen ICT MK) je bezesporu klíčovou oblastí činnosti rezortu. Řízení ICT je tak samostatnou oblastí, která musí být připravena na stále častější změny v oblasti legislativy, podřízených organizací a trendů v oblasti technologií a služeb ve světě informatiky.

V následujícím období musí být oblast ICT řízena způsobem, který je procesně orientovaný, zvládá stále rostoucí komplexitu poskytovaných IT služeb, zohledňuje rozpočtové možnosti rezortu a zajišťuje poskytování svých služeb a efektivně a požadované kvalitě.

Vzhledem k rozsáhlosti některých záměrů lze předpokládat vznik požadavků na rozšíření stávajícího personálního krytí a navýšení mzdových prostředků buď na OIT MK nebo u dotčených podřízených organizací. Veškeré požadavky podřízených organizací odůvodněné „Strategií ICT“ budou vypořádávány výhradně po projednání mezi odborem informačních technologií a oddělením PO.

V předchozí kapitole je uvedeno zhodnocení stávající situace ICT MK. Zde popisujeme cíle a oblasti, které jsou součástí řízení ICT a musí být dlouhodobě pokrývány. V následující kapitole jsou pak představeny strategické projekty vedoucí k dosažení plánovaných cílů a orientační časohový plán jejich realizace.

7.2 Cíle

7.2.1 Obecné cíle

Níže definované cíle jsou společné pro všechny organizace rezortu MK. K dosažení těchto cílů může být využito synergií jednotlivých organizací rezortu v oblasti informačních technologií. Naplnění jednotlivých cílů je do jisté míry závislé na specifících jednotlivých organizací a legislativních požadavcích, a to zejména v oblasti zákona na ochranu osobních údajů. Z těchto důvodů závisí na každé organizaci, jakým způsobem bude obecné cíle plnit a současně jaké vlastní konkrétní dílčí cíle si v oblasti IT definuje.

- Obecný cíl 1. IT podpora naplňování podstaty funkce spravované organizace – zajištění provozní stability všech systémů.
- Obecný cíl 2. Efektivní řízení služeb, standardizace řízení služeb (ITIL, TOGAF).
- Obecný cíl 3. Snížení celkových nákladů.
- Obecný cíl 4. Zajištění kybernetické a informační bezpečnosti.
- Obecný cíl 5. Konsolidované řízení IT projektů.
- Obecný cíl 6. Zajištění kontinuity služeb.
- Obecný cíl 7. Soulad s požadavky E-Governmentu.
- Obecný cíl 8. Konsolidovaná práce s daty prostřednictvím integrované platformy tak, aby bylo významně zkvalitněno manažerské rozhodování, zvýšena provozní efektivita a umožněn vznik nových datových produktů
- Obecný cíl 9. Digitalizace národního kulturního dědictví
- Obecný cíl 10. Přístup k integrované platformě a veškerým interním informacím pomocí mobilního zařízení v „terénu“. Propojení a provázání veškerých informací tak, aby bylo možné zdokumentování a následná implementace podkladů online přímo do systému.
- Obecný cíl 11. Podpora výzkumu a vývoje
- Obecný cíl 12. Efektivní rozhodování a plánování

7.2.2 Dílčí cíle

Tyto cíle definují jednotlivé dílčí strategie, které však musí být v souladu jak s obecnými cíli, tak základními principy.

7.2.2.1 Cíle řízení ICT

7.2.2.1.1 Soulad s legislativou

Rezort MK se musí při výkonu svého úřadu řídit řadou legislativních norem, které určují co je předmětem jeho činnosti a co musí zajišťovat. Tyto normy jsou doplněny řadou dalších obecně platných norem například z oblasti ekonomické evidence, správního řádu a též oblasti informačních technologií.

Jedním z nejdůležitějších cílů řízení ICT je tak zachovávat v každém okamžiku soulad s platnou legislativou. Kromě důsledného dodržování a zavádění opatření, které zákony vyžadují, je nezbytné kontrolovat a zajišťovat aby nedocházelo k zavádění opatření, která zákon nevyžaduje a nejsou ani důsledkem dalších (například interních) požadavků rezortu a tak v konečném důsledku jsou plýtváním prostředky daňového poplatníka či dokonce mohou být v kontradikci s některými právními normami.

Soulad s legislativou je tak nezbytným předpokladem dosažení obecného cíle „Zajištění provozní stability všech systémů“ vyplývajícím s koncepčního cílového a včasného plánování změn v reakci na změny legislativní a předpisové základny. V oblasti legislativy týkající se ochrany zpracovávaných informací je dosažení souladu výchozím krokem pro dosažení cíle „Zajištění kybernetické a informační bezpečnosti“.

7.2.2.1.2 Podpora činnosti MK a řízených organizací

Základním cílem řízení ICT je zajistit poskytování služeb z oblasti informačních technologií pracovníkům věcně odborných útvarů MK a tam, kde je to vhodné a možné též pracovníkům podřízených organizací. Služby musí být poskytovány tak, aby uspokojovaly požadavky uživatelů plně avšak efektivně.

Poskytování služeb ICT v rozsahu a kvalitě odpovídající relevantním požadavkům uživatelů je základem efektivního řízení, součástí obecného strategického cíle „Efektivní řízení služeb, standardizace řízení služeb“. Navíc poskytování relevantních, tj. též ne nadbytečných služeb je nutnou podmínkou naplnění obecného cíle „Snížení celkových nákladů“.

7.2.2.1.3 Optimalizace nákladů

Vlastní řízení ICT musí kromě cíle uspokojení požadavků uživatelů též reflektovat náklady spojené s vybudováním a provozem odpovídajících IT služeb.

Řízení ICT tak musí neustále vyvíjet snahu optimalizovat náklady a vytvářet rovnováhu mezi požadavky na služby IT a spotřebu zdrojů na jejich realizaci.

Optimalizace nákladů na úrovní řízení ICT, následována optimalizací nákladů v rámci dílčích realizačních a provozních projektů, je stěžejním nástrojem pro dlouhodobé snižování nákladů. Je tak pilířem dosažení obecného cíle „Snížení celkových nákladů“.

7.2.2.1.4 Optimalizace architektury

Služby ICT jsou poskytovány v prostředí neustále se vyvíjejících požadavků uživatelů a v dynamickém prostředí možností nových technologií pro jejich realizaci. Aby služby vždy efektivně plnily na ně kladené požadavky, je nezbytné zajistit průběžnou a dlouhodobou optimalizaci architektury služeb.

Optimalizace architektury služeb ICT je také jedním z důležitých nástrojů optimalizace nákladů a nástrojem napomáhajícím jasnému vymezení kompetencí mezi uživateli a poskytování služeb. V konečném důsledku tak má dopad na naplnění řady obecných cílů, zejména na „Zajištění provozní stability všech systémů“ a „Konsolidovaného Řízení IT projektů“.

7.2.2.1.5 Standardizace

Standardizace ve smyslu využívání oborových standardů a vydávání vlastních vyžadovaných standardů je klíčovým nástrojem normalizace poskytovaných služeb ICT. Dodržování standardů vede ke snadnějšímu řízení služeb, zlepšení kvality jejich realizace a provozu a v konečném důsledku ke snížení spojených nákladů.

Cílem standardizace je dlouhodobá údržba a rozvoj standardů v oblasti ICT a jejich důsledného vyžadování v rámci rezortu a od spolupracujících třetích stran.

Standardizace je základním kamenem dosažení cíle „Efektivního řízení služeb, standardizace řízení služeb“ a předpokladem dosažení cílů provozní stability a konsolidovaného řízení IT projektů. Navíc je standardizace klíčovou položkou kvality požadavků v rámci výběrových řízení.

7.2.2.1.6 Controling

Řízení procesů ICT MK musí být doplněno o efektivní mechanismy controllingu, které pro každou činnost stanoví role a harmonogramy realizace, kontroly a evaluace.

7.2.2.2 Cíle v oblasti koncových zařízení

Cílem strategie koncových zařízení je optimalizovat celý životní cyklus koncových zařízení a zajistit, že proces zajištění koncových zařízení bude i nadále hladce fungovat. Z obecných cílů tato strategie naplňuje cíle snížení celkových nákladů a zajištění kybernetické a informační bezpečnosti.

Strategie koncových zařízení se zabývá technikou, kterou k výkonu své činnosti používá uživatel informačního systému a kterou je výhodné centrálně řídit. Mezi koncová zařízení, na která se vztahuje strategie, budou zahrnuty:

- osobní počítače nebo terminály včetně periferií (zobrazovač, klávesnice, myš),
- přenosné počítače (notebooky),
- výstupní zařízení – tiskárny (osobní i síťové),
- vstupní zařízení – scannery (osobní i síťové),
- mobilní zařízení (tablety, chytré telefony).

Mezi koncová zařízení uživatele nejsou zahrnuty pro potřeby této strategie pevné stolní telefony.

Koncová zařízení jsou strategií řízena v rámci celého životního cyklu. Životním cyklem zařízení se rozumí:

- výběr hardware a nákup zařízení,

- evidence hardware,
- instalace základního operačního systému,
- instalace aplikačního programového vybavení,
- evidence software,
- správa zařízení a software v průběhu provozu,
- údržba a opravy
- vyřazení z provozu, likvidace.

7.2.2.3 Cíle v oblasti systémových služeb

Cílem v této oblasti je efektivní řízení a provozování systémových služeb rezortu MK tak, aby bylo možné těmito službami podporovat provoz aplikací MK, případně i vybraných podřízených organizací.

Strategie v oblasti systémových služeb pokrývá následující částí:

- Adresářové služby (Active Directory)
- Certifikační autorita
- Elektronická pošta (MS Exchange)
- Identity management
- Antivirový a antispamový systém
- Systém pro evidenci IT majetku (HW, SW)
- Správa stanic a SW
- ServiceDesk

7.2.2.4 Cíle v oblasti sítových a hlasových služeb

Cílem v této oblasti je vybudování jednotné komunikační infrastruktury rezortu MK tak, aby bylo možné po této infrastruktuře efektivně provozovat jednotlivé aplikace organizací rezortu MK. Pro naplnění tohoto cíle je potřebná infrastruktura rozdělena do následujících oblastí:

- Komunikační infrastruktura
- Síťové služby
- Monitoring
- Bezpečnost síťových a hlasových služeb

7.2.2.5 Cíle v oblasti HW infrastruktury a datových center

Hlavním cílem strategie v oblasti datových center je revitalizace technologie 2 datových center rezortu MK ideálně budovaných v modelu private cloud nebo využití sdílených datových center státní správy.

Pro tyto účely je strategie rozdělena do následujících části:

- Datová centra – zabývá se datovými centry z hlediska technické připravenosti lokality a sálů

- Infrastruktura datových center – zabývá se IT infrastrukturou, tedy vybavením datových center

Popis cílového stavu je popsán v jednotlivých bodech samostatně.

- Datová centra
- Infrastruktura DC
- Databázová vrstva
- Disková vrstva
- Aplikační a prezentační vrstva
- Virtualizace
- Centrální zálohování
- Klasifikace dostupnosti služeb DC
- Monitoring

7.2.2.6 Cíle v oblasti integrované platformy řízení dat

- Zavedení platformy
- Katalogizace dat
- Pilotní datový produkt
- Architektonický model SDDO
- Provozní model SDDO
- Portfolio inovativních datových produktů na bázi prediktivních analýz

7.2.2.7 Cíle v oblasti aplikačních služeb

Cíle strategie v oblasti aplikačních služeb vychází z obecných cílů IT MK, které jsou určující pro další konání v oblasti IT. Pro strategii v oblasti aplikačních služeb jsou určující především cíle:

- zajištění provozní stability všech systémů,
- snížení celkových nákladů,
- zajištění informační bezpečnosti,
- příprava prostředí a služeb pro OVŘ na modernizaci agendových IS a dalších ICT služeb MK a podřízených organizací.

Hlavním cílem strategie v oblasti aplikačních služeb je zajištění aplikační podpory specifických věcných potřeb jednotlivých organizačních celků MK a celého rezortu. Cíle v oblasti aplikačních služeb jsou dělené do základních kategorií, které tvoří kompletní oblast aplikačních služeb:

- **Cíle v oblasti naplnění IT potřeb věcných agend** – IT jednotlivých organizací bude schopné plánovat a dostatečně rychle plnit potřeby věcných agend MK včetně agend podřízených organizací.

- **Cíle v oblasti naplnění IT potřeb průřezových procesů agend a sdílených komponent** – organizační jednotky napříč MK budou mít informační podporu pro společné/průřezové procesy a budou využívat pro své aktivity sdílené komponenty (např. portál otevřená kultura, platforma pro sdílení dat). Aplikace, které patří do této kategorie, plní požadavky uživatelů na více odborech stejně a aplikace je proto možné sdílet napříč širokou skupinou uživatelů.
- **Cíle v oblasti doplňkových aplikací** – IT oddělení jednotlivých organizací bude schopné plánovat a dostatečně kvalitně (rychle a správně) plnit potřeby jednotlivých sekcí, odborů a oddělení na informační systémy pro jejich specifické potřeby. Doplňkovými aplikacemi se rozumí takové, které plní pouze specifický požadavek pro určitou skupinu uživatelů a které nepatří do jiné, zde jmenované, skupiny aplikací.
- **Cíle v oblasti IT podpůrných systémů** – jednotlivé organizace rezortu budou mít zajištěné podpůrné systémy: ekonomiku, personalistiku, intranet a e-mail (groupware).
- **Cíle v oblasti integrací aplikačních služeb** – zajistit, že rezort bude schopen integrovat své aplikační služby tak, jak si to vyžádá věcná potřeba.
- **Cíle v oblasti správy licencí** – každá organizace rezortu bude nakupovat a spravovat licence podle standardního procesu a bude průběžně optimalizovat počet svých licencí a hospodárně s nimi nakládat.

Obecným cílem v oblasti aplikačních služeb je pak dodržování standardů a architektury, které jsou řešeny v části strategie řízení IKT a průběžné posuzování, zda není ekonomicky výhodné jednotlivé aplikace přesoutěžit v otevřeném výběrovém řízení.

Cíle strategie jsou popsány primárně pro MK, které využívá služby IT MK. Strategie pro ostatní organizační složky rezortu jsou platné v obecných bodech, přičemž každá podřízená organizační jednotka musí mít svou IT strategii, která je v souladu s IT strategií MK.

7.2.2.8 Cíle v oblasti digitalizace

V oblasti digitalizace MK považuje za strategické následující cíle:

- defragmentovat rozdílný institucionální přístup prosazováním národní strategie za účasti všech zainteresovaných subjektů, usilovat o konzistentní národní politiku digitalizace kulturního obsahu;
- získat nejvyspělejší technologie digitalizace a orientovat se na perspektivní standardy digitalizace, tvorbu metadat, on-line přístupu a dlouhodobého archivování;
- integrovat digitalizační aktivity v rámci informační společnosti a znalostní ekonomiky s potřebami vzdělávání (studijní osnovy a programy vysokých škol), s potřebami vědy, techniky, inovací, podnikání, cestovního ruchu, kulturních a kreativních průmyslů ad.;
- řešit problémy interoperability informačních systémů paměťových a fondových institucí (dále též „PFI“), a dále mezi sektorem PFI a sektory vědy a vzdělávání a dalšími, kde digitální obsah může proniknout;
- určit úkoly, které je třeba na národní úrovni řešit ve spojitosti s digitalizací (např. migraci digitálního obsahu, jeho uchovávání, ochrana, nástroje vyhledávání, využívání digitálního obsahu ve školách, řízené slovníky, tezaury, klasifikace, mnohojazyčná prezentace a

dostupnost digitálního obsahu, využití digitálního obsahu pro vědu, výzkum, inovace, pro rozvoj služeb, pro cestovní ruch, právní aspekty zpřístupňování digitálního obsahu, technologické aspekty ochrany digitálního obsahu apod.)

- z pozice MK uchopit funkci kompetenčního centra pro infrastrukturu jakožto národního agregátoru a určit mezi PFI kompteneční centra a digitalizační pracoviště coby sektorových agregátorů pro digitalizaci;
- nastavit procesy a výstupy digitalizace v souladu s principy a nástroji eCulture.

7.3 Základní principy

7.3.1 Princip centralizace

Snížení nákladů na pořízení a provoz informačních technologií, neustálé zvyšování výkonu serverů a diskových polí a současně rozsáhlý seznam požadavků na konsolidace dat a funkcionalit nutně vedou k zavedení principu centralizace. Obecně lze definovat, že k centralizaci dochází doposud pouze v rámci jednotlivých organizací. Prostředky nejsou tedy sdíleny jednotlivými organizacemi rezortu. V rámci rezortu MK je nutné odlišovat mezi jednotlivými typy a rozsahem centralizací, a to hlavně z legislativních a procesních důvodů:

- **Centralizace technologií v rámci celého rezortu**

  Využití dostupných kapacit informačních technologií: sjednocení a optimalizace počtu datových center, sjednocení síťového prostředí a dalších systémových služeb, může vést k celkovému snížení nákladů na provoz IT služeb rezortu.

- **Centralizace dat v rámci celého rezortu v rozsahu.**

  Legislativa, a to zejména v oblasti ochrany osobních údajů a sdružováním informací doposud nemusí umožňovat cílenou centralizaci dat celého rezortu nicméně z hlediska využití dat k tvorbě datových produktů je přiměřená míra centralizace dat potřebná.

- **Centralizace technologií v rámci organizace.**

  Tento princip je dostatečně známý a je dle něho postupováno. Jedná se zejména o virtualizace existujících systémů a aplikací a další rozšiřování této technologie, sjednocení datových úložišť, sjednocení administrace a správy systémů.

- **Centralizace aplikací v rámci organizace.**

  K tomuto principu je nutné přistoupit z důvodu tlaku na úsporu nákladů, zjednodušení správy aplikací a v neposlední řadě také eliminaci lokální aplikačních uzlů.

- **Centralizace dat v rámci organizace v rozsahu, který legislativa umožňuje.**

  Princip si vynucují např. požadavky na statistiky (rozsah a požadovaná rychlost jejich zpracování) a nákladovost provozu necentralizovaných nebo oddělených kooperujících systémů.

7.3.2 Princip unifikace

Tento princip navazuje na princip centralizace. Zásadní ideou je sjednocení procesů, používaných technologií a definice odpovídajících standardů. Nejedná se pouze o standardy technologické a procesní, ale také o normalizaci vstupů a výstupů aplikací a systémů. Tento princip má za úkol stabilizovat a zpřehlednit IT prostředí a současně snížit náklady na jeho provoz pří zvýšení bezpečnosti.

7.4 Společné teze

Způsob řízení má vést k naplnění následujících tezí odvozených z jednotlivých strategických a dílčích cílů:

- Jsou definovány metriky pro hodnocení kvality, spolehlivosti a bezpečnosti souboru ICT.
- Služby souboru ICT pokrývají 100 % nároků, které jsou na ně kladeny.
- Služby souboru ICT jsou nasazovány synchronně se změnami příslušné legislativy.
- Maximálně jsou sdíleny informace tak, aby se plně využilo služeb a možností ICT. Minimalizuje se sběr již pořízených informací (zejména od klientů).
- Jsou definovány role odpovídající funkčnímu zařazení uživatelů.
- Každý uživatel má disponibilní takové služby ICT, které odpovídají jeho roli
- Je zavedena a podporována bezpečnostní kultura rezortu.
- Jsou zavedeny bezpečnostní politiky včetně dalších odpovídajících standardů a jejich dodržování je důsledně vyžadováno.
- Integrační platforma sjednocuje potřebná data s ohledem na potřeby aplikací a datových produktů
- Aplikace jsou optimalizovány z hlediska uživatelské přívětivosti (jednoduchost ovládání, grafické rozhraní).
- Soubor ICT je budován jako otevřený a transparentní.
- Informační systémy jsou maximálně zabezpečeny proti ztrátě důvěrnosti, integrity, dostupnosti a nepopíratelnosti použitím technických, systémových, procesních, personálních a administrativních opatření.
- Cena za pořizování a provozování ICT je přiměřená s ohledem na rozsah a kvalitu poskytovaných služeb. Využívání a provozování ICT je hospodárné a šetrné ke státnímu rozpočtu.
- Provoz a rozvoj informačních systémů je moderně řízen a je budován nebyrokraticky pomocí ICT expertů.
- Informační systémy odpovídají v čase a prostoru aktuálním trendům technologickým, architektonickým a bezpečnostním.
- Je perfektně vyřešena legislativa upravující nakládání s informacemi.
- Informační systémy fungují s maximální spolehlivostí, dostupností a bezpečností, nemají datové duplicity (nebo jiné podstatné nedostatky), optimálně sdílí data uvnitř i vně rezortu.
- V plném rozsahu je zavedena funkční a moderní elektronická komunikace a plně se využívá legislativní prostor pro elektronický oběh dokumentů.
- Celý životní cyklus všech prostředků ICT od pořízení přes provoz, údržbu, obnovu, aktualizaci až po likvidaci je definován a efektivně řízen. Číselníky a registry jsou kompatibilní s číselníky ISVS. Data v nich nejsou duplicitní ani nICTerak nekonzistentní a vyjadřují informace o reálném stavu.
- Uživatelé rezortu MK jsou průběžně školeni a je udržována odpovídající úroveň znalostí potřebných pro efektivní využívání veškerých funkcí/služeb, které jim soubor ICT nabízí.
- Smluvní vztahy mezi dodavateli a organizacemi rezortu MK jsou jednoznačně definované a řeší veškeré předvídatelné konflICTní stavy.

- Čerpané IT služby jsou dostatečně detailně popsány v rámci katalogu služeb (viz předcházející bod) jehož cílem je udržet informace o poskytovaných službách a jejich parametrech.
- Je vytvořen systém pro trvalé sledování kvality čerpaných IT služeb.

7.5 Nástroje k dosažení cílů

7.5.1 Řízení služeb

Služby je třeba řídit po celou dobu jejich životního cyklu. Služby mohou mít různé podoby a formy, základní principy jejich řízení jsou společné pro všechny typy služeb. Podmínkou pro řízení služeb je sestavení a udržování katalogu služeb a který bude obsahovat informace o všech provozovaných a připravovaných službách. Informace ke každé službě bude obsahovat aktuální informace, parametry, status, rozhraní a závislosti všech dalších služeb. V katalogu budou uvedeny jak služby nakupované od dodavatelů, tak služby poskytované ICT útvarem. K zajištění kontroly každé služby bude jmenován IT garant odpovědný za IT oblast a věcný garant odpovědný za věcnou náplň dané služby. V praxi se jedná nejčastěji o vlastníka procesu.

Aktuální stav a postup naplnění strategických cílů v oblasti řízení ICT je definován kapitolách 5 a 6.

Obecným cílem v oblasti řízení služeb je pak kontrola dodržování požadovaných parametrů jednotlivých služeb a průběžné posuzování, zda není výhodné jednotlivé služby revidovat nebo přesoutěžit v otevřeném výběrovém řízení z důvodů ekonomických nebo funkčních.

7.5.2 Standardy

Jedním z dalších nástrojů jsou interní směrnice, normy, standardy a předpisy, které definují jak způsob realizovaných změn v informačním systému, tak ovlivňují konkrétní řešení. Tyto směrnice a standardy je nutno díky neustálým změnám pravidelně aktualizovat a z pohledu celého rezortu i postupně sjednocovat. Současně je nutné do nich promítat změny ve strategii a zohledňovat velmi rychlý vývoj informačních technologií.

Jedná se zejména o standardy pokrývající následující oblasti

- Bezpečnostní standard,
- Aplikační standard,
- Dokumentační standard,
- Technologický standard,
- Standard pro provozní prostředí.

Součástí problematiky uplatnění standardů budou odpovídající metodiky, které definují procesy aplikace konkrétních standardů.

7.5.3 Projekty

Jednotlivé projekty v rámci rezortu budou řízeny metodikou řízení projektů MK, případně některou z běžně užívaných projektových metodik tak, aby průběh procesu byl jasně popsán ve všech svých fázích. Tímto bude docíleno transparentnosti celého procesu projektu, bude ochráněna investice a

zvýší se rovněž výkonnost realizace každého projektu. Zavedení projektové metodiky je nutné pro zajištění koordinace souběžných projektů v rámci rezortu, ale i u projektů realizovaných různými organizacemi rezortu. Způsob a kvalita řízení projektů odpovídá i stanovené strategii na řízení ICT a IT služeb. Zejména pak na transparentnost a udržitelnost daného projektu.

Aktuálně probíhá projekt zavedení jednotného způsobu projektového řízení v rámci Ministerstva kultury.

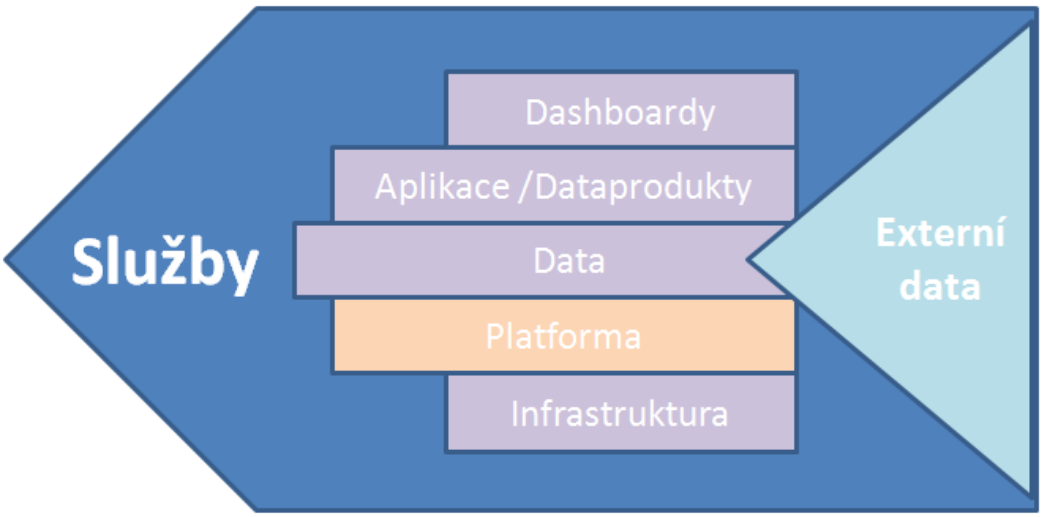
7.5.4 Globální architektura

Globální aplikační architektura definuje celkový pohled na uspořádání hrubé podoby IS. Jde o vizi budoucího stavu, která zachycuje jednotlivé komponenty a jejich vzájemné vazby, obsahuje základní stavební bloky, kde blok představuje množinu informačních služeb, které slouží pro podporu jednoho nebo více procesů. Je koncipována tak, aby jednotlivé organizace rezortu byly připraveny na společné projekty s dopadem do IS.

Jednotlivé organizace ve stávajícím stavu nemají architekturu obdobnou a tento stav je potřeba narovnat. V první vlně na globální úrovni. Jednotlivé dílčí oblasti architektury by pak měly být typologicky obdobné s cílem je postupně sjednocovat a normalizovat tak, aby bylo dosaženo strategických cílů nejen v rámci jednotlivých organizací, ale rovněž v rámci celého rezortu.

Koncept architektury vychází z již výše uvedených principů centralizace datové základny a SOA architektury. Tato architektura předpokládá:

- Integrovanou digitální platformu pro správu důležitých datových zdrojů
- Centralizovanou aplikační vrstvu nad integrovanou digitální platformou s nezbytnou výpočetní kapacitou
- Robustní datovou sběrnici pro výměnu informací,
- Dostatečně výkonnou infrastrukturu pro všechny uvedené vrstvy,
- Prezentační uživatelskou vrstvu.



Obrázek 2 Model SDDO založený na práci s velkým objemem dynamických dat

Cílová architektura je postavena nad dostatečně zajištěnými backend službami, které zprostředkovávají své funkcionality ostatním komponentám a systémů prostřednictvím výkonné ESB sběrnice. Ta současně řídí provoz poskytovaných služeb a tok všech informací mezi jednotlivými systémy.

Aktuální nedostatky nutné k nasazení globální architektury:

- Není zajištěno jednotné centrum řízení ICT v rámci rezortu.
- Neexistuje sdílení komponent v rámci rezortu.
- Každý ICT útvar odpovídá za spravované služby vlastní organizace.
- Výše uvedená architektura není nasazena ve všech archaizacích rezortu.

I přes výše uvedená fakta je uvedená architektura závazná pro jednotlivé organizace. Případné další sdílení služeb a dat lze následně realizovat propojením jednotlivých ESB rozhraní nebo sdílením funkčních komponent.

Detailní popis fungování je uveden v kapitole Strategie v oblasti aplikačních služeb.

7.6 Oblasti řešení

7.6.1 Strategie řízení ICT Ministerstva kultury

Oblasti řešení řízení ICT jsou v dnešní době oblasti činností, které musí zabezpečit, jakákoliv organizace, jejíž činnost se zásadně opírá o využívání informačních a komunikačních technologií.

Organizace se však mohou lišit v intenzitě, efektivnosti a kvalitě pokrytí dílčích oblastí s ohledem na potřeby a schopnosti, často určené vnějšími okolnostmi jako jsou například nedostatek zdrojů finančních či odborných.

7.6.1.1 Strategické plánování

Strategické plánování představuje soubor činností, které jsou potřebné ke stanovení základního rámce zvládnutí oblasti ICT v různých časových horizontech.

S ohledem na servisní povahu využívání ICT v rámci úřadu, jej není možno provádět bez znalosti strategických plánů rezortu jako celku. Na druhou stranu, některé ze strategických konceptů v oblasti ICT mohou inspirovat či přerůst ve strategické koncepty rezortu.

Strategické plánování je průběžnou činností, která cyklicky ústí ve zpracování strategie v oblasti ICT, a to s mírou detailu v závislosti na její časové charakteristice jinými slovy krátkodobé strategie musí být konkrétnější než dlouhodobé.

Plánování je činností, která je pracovní náplní nejvyššího vedení ICT na úrovni náměstků a ředitelů. Je to však činnost nemyslitelná bez odpovídajících informací od pracovníků pověřených pokrytím dílčích oblastí řízení ICT a širšího vedení organizace reprezentujícího uživatele poskytovaných služeb ICT.

7.6.1.2 Řízení architektury

Řízení architektury je poměrně moderní oblastí činností, které jsou součástí řízení ICT moderní organizace. Novost nespočívá přímo v tom, že problémy z oblasti architektury nebyly řešeny, ale spočívá ve vymezení architektury jako samostatné disciplíny svým způsobem přesahující hranice ICT směrem k procesům a činnostem, které jsou hlavní náplní práce rezortu.

Dnešní, již značně propracované rámce, řízení architektury se shodují na trojici architektur, které musí organizace znát a udržovat. Jedná se o

- architekturu technologické infrastruktury,
- architekturu informačních systémů (zahrnující architekturu aplikací a architekturu datové základny),
- datová architektura jako separátní přístup - důležitější než vlastní aplikace - je dynamickým akcelerátorem organizační efektivity
- architekturu předmětné činnosti organizace založené na datech a službách, jež je základem pro návrh výše uvedených architektur.

Zejména poslední ze jmenovaných architektur pak přesahuje rámec typicky řešený v oblasti ICK. Na druhou stranu, je nejčastěji tato oblast nejhůře řízena a formálně popisována.

7.6.1.3 Bezpečnost

Oblast bezpečnosti v řízení ICT je oblastí, jejíž specifikum je dáno tím, že problematika bezpečnosti se prolíná všemi oblastmi ICT a podléhá řízení bezpečnosti celé organizace.

V oblasti bezpečnosti vznikla v průběhu minulých let nepřeberná řada standardů, doporučení a metodik jejího řízení. Oblast je tak v důsledku pokrývána pracovníky se specifickou znalostí problematiky.

Základními koncepty řízení bezpečnosti jsou „Bezpečnostní strategie“ a „Bezpečnostní politika“. Prvně jmenovaný koncept určuje přístup k zajištění bezpečnosti, druhý koncept pak zavádí soubor pravidel k naplnění strategických bezpečnostních cílů. Strategie a politika je doplněna analýzou

bezpečnostních rizik a návrhu zmírňování jejich dopadu. Všechny tři koncepty se vzájemně ovlivňují, musí být v souladu s obdobnými koncepty bezpečnosti organizace a jejich stanovení je jedním z hlavních úkolů řízení ICT.

7.6.1.4 Projektové řízení a řízení kvality

V kontextu moderního řízení ICT jsou prováděné činnosti v důsledku pokrytí oblasti ICT strukturovány do logicky konzistentních jasně vydělitelných celků – projektů. Projekt je soubor činností, který má definovaný cíl a předmět, kterého se má dosáhnout (rozsah). Má definovaný rozpočet, přidělené zdroje a časová omezení (harmonogram). Každý projekt má také odpovědnou osobu za jeho realizaci.

Struktura projektů je pak nástrojem pro řízení ICT s jasnými ekonomickými, časovými a obsahovými metrikami.

Nad rámec realizace jednotlivých projektů je nezbytné zajistit jejich vzájemnou koordinaci a řešení nesouladů. Pokrytí této problematiky je pak řešeno specializovaným projektem zpravidla označovaným jako systémová integrace.

Nedílnou součástí projektového řízení je řízení kvality, jejímž cílem je kvantifikovat aspekty dodávaného projektu, tak, aby mohl být sledován soulad realizace projektu s jeho záměrem, a to měřitelným způsobem.

7.6.1.5 Řízení rozvoje

Řízení rozvoje je řízení skupiny činností vedoucích k rozvoji (obecně změnám) ICT v důsledku nových požadavků. Je úzce svázáno s průběžnou evidencí a správou požadavků a tím s řízením architektury a (strategickým) plánováním.

Rozvojové činnosti jsou téměř výhradně realizovány jako projekty a většinou jsou realizovány smluvními stranami z důvodu potřeby dodatečné expertízy a doplnění organizačních a lidských zdrojů. Přesto však na straně organizace musí mít i rozvojové projekty svého odpovědného vlastníka a nemůže tato role být předána třetí straně.

Výstupy rozvojových činností musí být před jejich začleněním v rámci provozu akceptovány jednoznačně převzaty a nasazeny. Tím vyplývá potřeba řízení akceptace a testování, řízení transferu znalostí a řízení migrace. Uvedené činnosti jsou pak zpravidla prováděny v kontextu daného rozvojového projektu.

7.6.1.6 Zajištění provozu

Řízení provozu je řízením skupiny činností zajišťujících chod nasazených informačních a komunikačních technologií. I provozní činnosti mají povahu projektů z hlediska jejich vymezení, odpovědnosti, řízení zdrojů a financí. S ohledem na jejich opakovatelnost, je smysluplné je formálněji vymezit a nazývat je provozními procesy.

Provozní procesy ICT napříč různými organizacemi mají velmi podobnou povahu a jsou vytvořeny standarty metodik pro realizaci těchto procesů.

S ohledem na potřebu sledování kvality provozních procesů je nezbytné vytvářet odpovídající nástroje řízení kvality, typicky označovaných jako SLA (z anglického Service Level Agreement).

Provozní procesy mohou být zajišťovány jak samotnou organizací, tak i dalšími stranami nebo kombinací obou přístupů.

7.6.1.7 Smluvní zajištění

Oblast smluvního zajištění pokrývá činnosti pro řízení projektů zajišťovaných právními subjekty mimo organizaci. Z hlediska ICT se jedná zejména o

- Příprava věcných podkladů pro výběrová řízení v souladu s legislativou.
- Hodnocení věcné a ekonomické relevance předložených nabídek.
- Účast na přípravě věcných částí smluv s dodavateli.
- Účast na případných vyjednáváních s dodavateli.
- Příprava a vymezení smluvně požadovaných SLA.
- Příprava a vymezení vyžadovaných standardů.
- Účast při rušení či ukončování smluvních vztahů.

7.6.1.8 Legislativní soulad

Oblast legislativního souladu v rámci řízení ICT znamená sledování a zajištění požadavků kladených zákonem na využívání informačních technologií. Nejedná se o legislativní požadavky na předmětnou činnost ale obecně na informatiku či informační technologie. Příkladem může být povinnost využívání registrů veřejné správy.

7.6.2 Strategie v oblasti koncových zařízení

7.6.2.1 Výběr hardware a nákup zařízení

Zavedený centrální výběr a nákup zařízení bude i nadále rozvíjen. Do tohoto procesu budou zahrnuta i mobilní zařízení tak, aby byla umožněna jejich centrální správa a jednotnost.

Před zahájením výběru zařízení bude vypracována studie, která shrne požadavky aplikačního programového vybavení a nové technologické trendy. Výsledkem této studie bude určující směr pro výběr typů zařízení s výhledem na čtyři roky.

Například v oblasti pracovních stanic budou posuzovány varianty nákupu osobních počítačů, virtuálních desktopů nebo terminálových pracovišť. Součástí posouzení nejvhodnějšího řešení bude vždy pilotní ověření vybrané varianty.

7.6.2.2 Evidence hardware

Cílem rozvoje evidence hardware je spojit potřeby majetkové evidence a potřeby ICT. Současné nedostatky jsou především v oblastech

- zanesení nových zařízení do evidence majetku až po jejich fyzické instalaci,
- nevyužívání jednotných číselníků pro označení zařízení (například PC, počítač, pracovní stanice),

- chybějící výrobní čísla zařízení v majetkové evidenci,
- informace o délce podpory zařízení (záruční pozáruční servis).

Doplněním majetkové evidence o výše uvedené informace vznikne propojený jednotný systém, který dokáže v plné míře zajistit správu zařízení. V budoucnu bude možné provázat evidenci majetku se systémy fyzické správy zařízení.

Evidence a doplňování musí být ideálně zajištěno přímo na daném místě s přímým přístupem do systému pomocí naskenování nebo zadání kódu z daného zařízení. Stejným způsobem musí být zajištěno zadávání údržby, oprav, přesunu (stěhování) a správy poruch.

7.6.2.3 Instalace základního operačního systému, aplikačního vybavení a správa zařízení

Stávající prostředky použité pro instalaci základních operačních systémů, následnou instalaci aplikačního programového vybavení a správu zařízení budou shrnuty v systémovém projektu, který formou hodnotících kritérií posoudí jejich vlastnosti a doporučí jednotné řešení. Cílem systémového projektu bude vybrat takové řešení, které jedním prostředkem pokryje kompletní softwarovou správu zařízení, tedy instalaci operačního systému, instalaci aplikačního programového vybavení a instalaci následných oprav systému nebo aplikace a umožní vlastní správu zařízení, včetně poskytnutí vzdálené odborné pomoci uživateli. Systémový projekt musí posoudit také možnosti automatické instalace, bez nutnosti zásahu pracovníka ICT, a to již od začátku životního cyklu zařízení (instalace operačního systému).

Systémový projekt může pro různé typy zařízení doporučit různé prostředky správy. Například jeden systém pro osobní počítače, jeden pro terminálová pracoviště, jeden pro mobilní zařízení.

Součástí systémového návrhu bude také vytvoření procesu testování a návrh vlastního testovacího prostředí, které bude sloužit k ověření standardizovaných konfigurací dále použitých pro instalace.

Na základě výstupu systémového projektu bude zpracován projekt implementační, který doporučené řešení zavede do prostředí.

7.6.2.4 Evidence software

Stávající evidence software bude rozšířena o proces pro řízení licenčních aktiv. Tento proces bude pokrývat oblast správy, evidence a řízení nákupu softwarových licencí. Zavedením procesu budou podchycena rizika:

- nákupu softwarových licencí, které nejsou zapotřebí (vzhledem k počtu, verzi, funkcionalitě, nebo edici),
- stavu, kdyby byly využívané licence, ke kterým nejsou zakoupené licenční oprávnění,
- nejasné dokumentace softwarových licencí,
- nákupu softwarových licencí dle nevhodných metrik.

Tento proces bude mít svého vlastníka zodpovědného za jeho správu. Jedná se o osobu, která musí disponovat znalostí v oblasti řízení licenčních aktiv (znalost licenčních metrik, potřebné dokumentace licencí apod.).

Proces současné majetkové evidence software bude rozšířen o informace o verzi, edici, době ukončení platnosti a údržby a o vazbu mezi software a fyzickým zařízením.

Nový proces bude podpořen systémem pro řízení licencí, jehož hlavním úkolem bude

- řádně evidovat všechny zakoupené licence,
- evidovat jednotlivá zařízení,
- on-line sledovat stav instalovaných licencí na zařízení a porovnávat ho s počty zakoupených licencí,
- spravovat číselníky zařízení a software,
- sledovat využívání software,
- zabránit instalaci neautorizovaného software.

Před zavedením nového systému pro řízení licencí zvážit možnosti využít stejného nástroje, který lze použit rovněž pro správu software zařízení (instalaci operačního systému, instalaci aplikačního programového vybavení a instalaci následných oprav).

7.6.2.5 Bezpečnostní opatření vztahující se ke koncovým zařízením

Do kapitoly bezpečnostních opatření je zahrnuta problematiky vyřazení zařízení z provozu a likvidace a problematika bezpečnosti zařízení a dat na nich uložených.

Bezpečnost má vazbu na bezpečnostní politiku úřadu a na ochranná opatření, plynoucí z analýzy rizik organizace. Z pohledu koncových zařízení jde především o informační aktiva na těchto zařízeních uložená. Požadavky bezpečnostních opatření budou shrnuta v systémovém projektu, který posoudí různé scénáře plnění opatření a doporučí změny procesů, případně zavedení procesů nových, popisujících nakládání s koncovými zařízeními a daty na nich uložených. Pokud to bude nutné, bude proces podpořen technickými prostředky, jejichž doporučení bude taktéž výstupem systémového projektu.

Samostatnou kapitolou bezpečnostní politiky je i nakládání s přenosnými nosiči informací (CD-ROM, USB disk), které však sami o sobě nejsou zařízením. V případě potřeby budou do procesů vztahujících se ke koncovým zařízením zaneseny také požadavky na tato přenosná zařízení. Vlastní proces může i zde být podpořen technickým prostředkem.

7.6.3 Strategie v oblasti systémových služeb

7.6.3.1 Adresářové služby (Active Directory)

Strategie v oblasti adresářových služeb povede k takové konfiguraci AD, kdy bude každá organizace rezortu MK pokryta vlastním AD adresářem s jedinou AD doménou (s výjimkou vybraných podřízených organizací, kde je efektivnější zařazení do domény MKČR. Mezi těmito adresáři bude navázán adresářový vztah důvěry (obousměrný, transitivní).

Služby AD budou zcela centralizovány do datových center na dostatečném počtu kontrolérů zajišťujících služby AD. Služby AD budou rozprostřeny mezi datovými centry tak, aby umožnily plnou geografickou vysokou dostupnost.

Datová struktura služby AD bude členěna do organizačních jednotek tak, aby v maximální míře umožnila delegaci správy datového obsahu služby.

V dlouhodobém horizontu (po roce 2015):

- Zvážit vybudování nového nebo použít některý ze stávajících adresářů MK jako centrální adresář, do kterého budou postupně migrovány veškeré identity, servery, počítače, další objekty AD a integrované služby (např. MS Exchange a další) organizací MK.

7.6.3.2 Elektronická pošta (MS Exchange)

Strategie v oblasti elektronické pošty je taková, že každá organizace rezortu MK bude pokryta vlastní Exchange Organizací. Exchange bude integrován v AD adresáři příslušné organizace.

Služby MS Exchange budou zcela centralizovány v datových centrech a budovány s ohledem na možnost rozšiřitelnosti (velikost schránky, počet uživatelů apod.). Služby MS Exchange budou rozprostřeny mezi datová centra tak, aby umožnily plnou geografickou vysokou dostupnost.

Pro příjem pošty z internetu a odeslání do internetu budou organizace rezortu využívat systém poštovních bran, který poskytne zároveň první úroveň virové, spamové a malware kontroly (viz strategie v oblasti síťových a hlasových služeb). Bude zváženo sjednocení (centralizace) této funkcionality pro celý rezort.

V dlouhodobém horizontu (po roce 2015):

- Společně s budováním nového AD adresářů organizací MK bude vybudován i nový MS Exchange integrovaný v tomto AD a následně v rámci migrace objektů budou přeneseny též všechny uživatelské schránky a další objekty MS Exchange.

7.6.3.3 Identity management

Strategie v oblasti identity managementu je taková, že o životní cyklus uživatelských účtů organizací rezortu se bude starat IDM systém, přímo napojený na systémy oddělení správy lidských zdrojů (personálních oddělení). Každá organizace bude používat vlastní systém, napojený na její AD adresář. IDM systém bude plnit především následující funkce (dle potřeb další):

- Založení uživatelského účtu a vyplnění mandatorních atributů (na základě pracovního zařazení, lokality apod.)
- Zařazení účtu do skupin pro získání přístupů do aplikací příslušející danému pracovnímu zařazení (roli) metodou single sign on (SSO)
- Spuštění schvalovacího procesu pro získání přístupů do aplikací
- Zařazení účtu do skupin pro získání oprávnění k nakládání s klasifikovanými informacemi způsobem odpovídajícím přiřazené roli
- Vytvoření Emailové schránky s požadovanými parametry (limity apod.)

- Změny v atributech účtu během fáze jeho existence (např. změna jména, lokace, pracovní pozice a členství ve skupinách apod.)
- Zneplatnění účtu při přerušení nebo ukončení pracovněprávního vztahu
- Smazání účtu

Služby IDM nemusí být bezpodmínečně rozprostřeno mezi datovými centry pro umožnění plnou geografickou vysokou dostupnost, ale musí být zajištěno zálohování dat.

V krátkodobém horizontu (do poloviny roku 2015):

- Proběhne analýza procesů a postupů životního cyklu uživatelských účtů organizací MK a bude připraven projektový záměr možných variant nasazení IDM systému.

V dlouhodobém horizontu (konec roku 2015 a dále):

Začne postupná implementace IDM v organizacích MK.

V souladu s rozvojem eGovernmentu a Jednotného identitního prostoru úředníků lze do budoucna uvažovat také o rozšíření IDM o:

- Napojení IDM na JIP/KAAS

7.6.3.4 Antivirový a antispamový systém

Strategie v oblasti antivirových a antispamových systémů bude směřovat k ochraně jednotlivých vrstev sítě:

- ochrana všech serverů a pracovních stanic
- ochrana mobilních zařízení
- ochrana poštovních systémů
- ochrana poštovních bran (komunikace s internetem) – popsáno v jiné části strategie - viz strategie v oblasti síťových a hlasových služeb
- přístup do internetu – popsáno v jiné části strategie - viz strategie v oblasti síťových a hlasových služeb

7.6.3.4.1 Ochrana serverů a pracovních stanic

Strategie v oblasti této ochrany bude zaměřena na zvýšení zabezpečení serverů, stanic a dat pomocí detekčních a ochranných technologií.

7.6.3.4.2 Ochrana poštovních systémů

Strategie v této oblasti je zaměřena na zabezpečení interní pošty proti rozesílání a přijímání nebezpečných (škodlivých) kódů a spamů.

7.6.3.5 Systém pro evidenci IT majetku (HW, SW)

Pro evidenci IT majetku (HW i SW) bude provozován systém, který bude plnit následující funkční požadavky:

- Evidence vlastnictví majetku a možnosti propojení na modul majetku systému EKIS
    - Řízení životního cyklu hardware a software
    - Evidence smluv a smluvních podmínek
    - Evidence dodavatelů
    - Strukturované sledování jednorázových a opakovaných nákladů
    - Okamžitý přístup k informacím na místě, kde se nachází daný HW pro zadávání, kontrolu a zpětné získávání potřebných informací.
    - Přímý přístup na Service Desk po naskenování nebo zadání kódu ze zařízení. Zajištění možnosti přímého zadání požadavku na údržbu, opravu nebo přesun HW včetně správy poruch daného zařízení
- Evidence vlastnictví software a podpora licenční čistoty (SW Asset Management)
    - Evidence SW včetně parametrů
    - Evidence nákupů SW licencí
    - Evidence vazby na hardware, kde je software instalován
    - Evidence práva užívání k softwarovým produktům
    - Evidence licencí – oprávnění užívat software pro uživatele, lokality, organizace, počítače, atd.
    - Evidence smluv o softwarové podpoře nebo pronájmu licencí.
    - Evidence, kontrola a řízení SLA, Reminder (Připomínkovač), dokumentace smluvních povinností, automatizace přípravy návrhu smluvních pokut za chybné smluvní plnění.
    -

7.6.3.6 Správa stanic a SW

Z ICT koncepce vyplývá nutnost mít do budoucna zajištěnu službu distribuce nových vydání aplikací využívajících technologii „tlustého“ klienta. Pro zajištění distribuce nových vydání těchto aplikací je s ohledem na šetrné hospodaření s dostupnou kapacitu linek WAN nutné zajistit decentralizovanou distribuci nových verzí klientů na koncové stanice.

7.6.3.7 ServiceDesk

Pro řešení řízení procesů podpory uživatelů informačních systémů rezortu bude provozován ServiceDesk systém, který bude plnit následující funkční požadavky:

- Podpora procesů podle ITIL
    - Request/Ticket Management
    - Incident Management
    - Problem Management
    - Change Management

    - Knowledge Management
    - Configuration Management
    - Service Management
- Konfigurační databáze CMDB – tato CMDB bude provázána se systémem pro evidencí IT majetku i se systémem pro správu stanic a SW
- Znalostní báze
- Reporting
- Portál pro podporované uživatele
- Integrace na systémy podpory dodavatelů (pomocí Web Services).
- Zajištění informačního procesu v návaznosti na propojení konkrétního HW a SW, kterého se proces týká tak, aby bylo odstraněno dlouhodobé vyhledávání a chyby v implementaci a správě dat.

V rámci této oblasti je nutno zajistit také procesní zajištění výše zmíněných ITIL procesů. Detailní informace ke způsobu řízení jsou uvedeny v části Strategie řízení ICT MK.

7.6.3.8 Zastřešující monitoring

Vzhledem ke vzrůstajícím požadavkům na efektivní a spolehlivé fungování ICT MK je nezbytné vybudovat robustní zastřešující systém monitoringu aplikací, infrastruktury a komunikační infrastruktury tak, aby odpovídal požadavkům kladeným na něj ze strany provozovatelů jednotlivých částí ICT a pracovníků dohledového centra.

V dnešní době odběratelé IT služeb očekávají:

- službu v provozním stavu (tj. použitelná) ve chvíli, kdy ji potřebují
- při výpadku služby zajištění co nejrychlejšího navrácení do provozu

Tyto skutečnosti bývají zpravidla formalizovány v podobě smluv na dodávku služeb s vyjasněním obsahu a hlavně úrovně poskytovaných služeb (Service Level Objective - SLO a Service Level Agreement - SLA). V souvislosti s těmito trendy je zapotřebí rozvíjet správu a dohled IT infrastruktury směrem ke správě služeb. Již není dostačující zajistit provoz sítě popř. provoz počítačů, ale je nutné zajistit provoz sítě a počítačů současně, a to z pohledu dodávané služby, která běží na počítači a využívá síť. Dohled a správa IT infrastruktury hraje velmi důležitou roli. Na jedné straně umožňuje koncovým uživatelům bezproblémový odběr očekávaných služeb a na druhé straně dovoluje vedení společnosti využívat IT pro zabezpečení podnikatelských záměrů. Podle společnosti Gartner Group však míra naplnění těchto skutečností závisí na fázi, v jakém se dohled a správa IT infrastruktury nachází. Následující odstavec popisuje různé typy nástrojů pro správu a dohled:

- Element management – nástroje pro správu elementů v IT infrastruktuře, většinou neintegrovatelné, pracující bez návazností na ostatní nástroje, sloužící k detailní správě určitého typu technologie, schopné identifikovat chybu pouze v dané technologii, většinou dodávané výrobcem dané technologie

• Operations management – nástroje vzájemně integrované do jednoho kompozitního celku, schopné identifikovat problém napříč různými technologiemi, často pracují v proaktivním režimu, tedy mají určitou schopnost předvídat problematické situace

• Service management – nástroje schopné držet informaci o provázanosti jednotlivých technologií, umožňující definovat službu a její elementy, popsat vlivy výpadků jednotlivých elementů na chod celé služby, kontrolovat dodávku služeb podle SLA

• Business management – nástroje service managementu obohacené o možnosti modelování různých situací a s podpůrnými nástroji na analýzu vlivu IT na chod firmy, umožňující provázat služby s finančními toky.

Cíl: V prostředí MK bude vybudován konsolidovaný systém zastřešující a sjednocující informace od monitorovacích nástrojů jednotlivých vrstev a celků. Zdrojem informací bude tedy zejména:

- monitoring infrastruktury
- monitoring komunikační infrastruktury
- bezpečnostní monitoring
- aplikační monitoring
- monitoring dodávk a služeb dodavatelů (SLA)
- maintenance monitoring

7.6.3.9 Archivace dat

Instituce státní správy musí řešit požadavky na dlouhodobé ukládání elektronických dokumentů nebo dokumentů, které byly do elektronické podoby převedeny z podoby listinné, jak jim ukládá platná legislativa České republiky a Evropské unie a také interní předpisy organizace.

V rámci revize služeb a provozovaných systémů bude definován požadavek na minimální rozsah této služby.

7.6.3.9.1 Legislativní rámec a shoda se standardy

Dlouhodobé ukládání elektronických dokumentů musí být ve shodě s následující legislativou ČR a EU:

- zákon č.499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění vyhlášky č. 283/2014 Sb.
- věstník MV částka 76/2009 část II, Národní standard pro elektronické systémy spisové služby
- zákon č.300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů ve znění pozdějších předpisů.
- zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.
- Spolu se spisovou službou bude DDÚ odpovídat požadavkům uvedeným v „Metodickém návodu pro kontrolu výkonu spisové služby vedené prostřednictvím elektronického systému spisové služby u veřejnoprávních původců“ vydaným

Ministerstvem vnitra. Metodický návod je pojat jako seznam a obsahuje vybrané požadavky především zákona č. 499/2004 Sb. o archivnictví a spisové službě ve znění zákona č. 190/2009 Sb. včetně Novely zákona o archivnictví a spisové službě, vyhlášky č. 259/2012 Sb. o podrobnostech výkonu spisové služby a Národního standardu pro elektronické systémy spisové služby (dále jen NSESSS)

Podle legislativy musí Dlouhodobé úložiště (DDÚ) zajistit

- Formáty uložených dat podle archivační politiky
- Elektronické podpisy a časová razítka, která jsou součástí dat vstupujících do dlouhodobého úložiště a uložit výsledek tohoto ověření
- Integritu a autenticitu uložených dat
- Archivaci po archivační dobu a řízenou skartaci poté
- Pokud je to požadováno předat vybraná data po uplynutí doby uložení do Národního archivu

Dlouhodobé úložiště musí umět ověřovat kvalifikované certifikáty dle zákona č. 227/2000 Sb., o elektronickém podpisu, a kvalifikované certifikáty zemí Evropské unie (viz rozhodnutí Evropské komise č. 2009/767/ES)

Dále musí být Dlouhodobé ukládání elektronických dokumentů ve shodě s platnými archivačními standardy.

7.6.3.9.2 Dlouhodobé uložiště

MK vybuduje řešení důvěryhodného datového úložiště. MK bude provozovatelem DDÚ. V úvahu nepřipadají řešení DDÚ formou služby, cloudové řešení u poskytovatele cloudu apod.

- DDÚ bude archivovat výhradně nestrukturovaná data.
- DDÚ musí splňovat Open archival information system (OAIS) (ISO 14721) standard (viz: http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284).
- DDÚ bude obsahovat výhradně elektronické dokumenty ve vlastnictví MK.
- Elektronické dokumenty uložené v DDÚ musí být uloženy tak, aby nevyžadovaly uložení papírového originálu (pokud existuje) nebo vytváření papírové kopie.
- DDÚ bude nakládat s elektronickými dokumenty ve shodě s archivačním a skartačním řádem MK. Archivační a skartační znaky budou součástí povinných metadat každého uloženého archivačního balíčku.
- DDÚ bude uchovávat originály elektronických dokumentů nebo kopie nascanovaných dokumentů.
- DDÚ bude provádět migrace formátů.
- DDÚ musí umět zobrazit nezkresleně archivovaný dokument (nebo jeho formátově migrované kopie) v celém průběhu doby archivace.
- Podpora standardu OAI-PMH
- DDÚ bude navrženo tak, aby nebylo v rozporu s požadavky ISO16363.
- Navrhované řešení musí být připraveno na případné kontroly prováděné například

    - Státním oblastním archivem na základě § 71 odst. 1 písm. c) zákona č. 499/2004 Sb.
    - Národním archivem na základě § 71 odst. 1 písm. b) zákona č. 499/2004 Sb.
    - Ministerstvem vnitra na základě § 71 odst. 1 písm. a) zákona č. 499/2004 Sb.
    - Nejvyšším kontrolním úřadem na základě § 3 odst. 1 písm. a) zákona č. 166/1993 Sb.
- DDÚ bude navrženo tak, aby mohlo poskytovat obecné informace neautentizovaným uživatelům (např. veřejnosti).
- DDÚ bude navrženo tak, aby umožnilo registrovaným a autentizovaným uživatelům (např. vybraným zaměstnancům státní správy) prohledávat DDÚ.
- DDÚ bude navrženo tak, aby mohlo přijímat žádosti na vybrané výstupní archivační balíčky (DIP balíčky) autentizovaným uživatelům (např. vybraným zaměstnancům státní správy).
- DDÚ bude navrženo tak, aby mohlo na základě přijaté a akceptované žádosti generovat výstupní archivační balíčky (DIP balíčky) autentizovaným uživatelům (např. vybraným zaměstnancům státní správy)
- DDÚ by mělo pracovat se spisovou službou MK (spisová služba GINIS od firmy Gordic), která bude používána jako místo prostřednictvím, kterého budou dokumenty do DDÚ ukládány a také prostřednictvím spisové služby vyzvedávány.
- Také výměna informací s Národním archivem a výstupy archivačních balíčků do Národního archivu jako součást skartačního procesu musí být DDÚ podporovány.
- DDÚ musí plně podporovat Národní standard pro elektronické systémy spisové služby (dále též jen „NSESSS“).
- Do DDÚ se budou ukládat elektronické dokumenty spolu se souvisejícími metadaty ve formě archivačních balíčků. Na předpřípravě archivačních balíčků pro DDÚ se může spolupodílet spisová služba, DDÚ si však podrží vstupní kontrolu před vstupem do DDÚ – Předarchivační modul.
- V rámci vstupu do DDÚ (Předarchivační modul) jsou požadovány následující funkce:
    - Antivirová kontrola
    - Kontrola integrity vstupních dat
    - Kontrola formátů vstupních dat a jejich shody s archivační politikou
    - Kontrola platnosti elektronických podpisů a časových razítek vstupních dat, pokud budou k archivovanému objektu připojeny.
    - Kontrola metadat a jejich doplnění do povinné struktury. Doplnění metadat může být jak automatické na základě konfigurovatelného nastavení na vstupu, tak ruční oprávněným uživatelem přes webové rozhraní.
    - Případné opatření vstupních dat elektronickým podpisem a časovým razítkem ve shodě s archivační politikou
    - Kompletace vstupních balíčků ve shodě s archivační politikou
- Zabezpečení archivovaných elektronických dokumentů
    - Proti neoprávněnému přístupu
    - Proti neoprávněné modifikaci
    - Proti neoprávněnému smazání
    - Zabezpečení elektronické dokumenty elektronickým otiskem

- Umožní šifrování elektronických dokumentů. Uchazeč popíše manipulaci se šifrovacími klíči tak, aby se vyloučila možnost nepřečtení archivovaných dat v budoucnosti.
- Zkontroluje platnost případných časových razítek a elektronických podpisů
- Opatří elektronické dokumenty průvodní košilkou (metadaty) včetně těch, které zajišťují integritu archivovaného dokumentu.
- DDÚ umožní výměnu metadat se schválenými autorizovanými subjekty protokolem OAI-PMH
- DDÚ bude podporovat následující metadatové standardy:

METS	verze 1.9.1	http://www.loc.gov/standards/mets/	strukturální metadata
MODS	verze 3.5	http://www.loc.gov/standards/mods/	popisná metadata
Dublin Core	verze 1.1	http://dublincore.org/documents/dces/	popisná metadata
PREMIS	verze 2.2	http://www.loc.gov/standards/premis/	administrativní a technická metadata
copyrightMD	verze 0.91	http://www.cdlib.org/groups/rmg/	autorsko-právní metadata

7.6.4 Strategie v oblasti síťových a hlasových služeb

7.6.4.1 Komunikační infrastruktura

Spolehlivá, vysoce dostupná, bezpečná a dostatečně výkonná komunikační infrastruktura je nezbytným základem pro spolehlivý provoz jednotlivých aplikací v rámci informačního systému (IS) Ministerstva kultury. Komunikační infrastruktura tak představuje z pohledu spolehlivého a efektivního poskytování služeb strategickou platformu MK. Kvalitní komunikační infrastruktura je předpokladem nejen pro rozvoj tradičních datových komunikací, ale rovněž je i nezbytným předpokladem pro další rozvoj hlasových komunikací a videokomunikací v rámci celého rezortu MK. Praktické zkušenosti ukazují, že pouze architekturní přístup k budování komunikační infrastruktury je zárukou investičně i provozně vyváženého, předvídatelného a tudíž i úsporného vynakládání finančních prostředků na zajištění komunikačních potřeb dané organizace (oproti skládání komunikačních zařízení více méně ad hoc dle aktuálně vnímané potřeby).

Pro všechny nově implementované aktivní prvky je platný požadavek plynoucí z usnesení Vlády ČR z 8. 6. 2009 č. 727, které mimo jiné požaduje u síťových prvků jejich kompatibilitu s IPv6.

Komunikační infrastruktura musí splňovat podmínky zákona o kybernetické bezpečnosti a souvisejících zákonů.

Z těchto důvodů je komunikační infrastruktura dekomponována do následujících celků:

- Externí konektivita (slouží pro připojení externích subjektů)
- Datová centra (jsou komunikační centra, která slouží pro propojení externí konektivity s konektivitou k lokalitám)
- Přenosová síť (přenosová síť je realizována pronájmem služeb od operátorů)
- Připojení lokalit (kategorizované přípojky do jednotlivých lokalit)

Pro spolehlivou elektronickou výměnu dat v rámci jednotlivých aplikací rezortu MK musí komunikační infrastruktura zajistit především vysoce dostupnou a spolehlivou IP konektivitu s garantovanými parametry dle potřeb jednotlivých provozovaných aplikací.

Pro zajištění bezpečnosti, provozuschopnosti a rozvoje komunikační infrastruktury je požadováno zajištění dostupnosti softwarových oprav a podpory výrobce pro všechny aktivní prvky. Aktivní prvky, na které již výrobce neposkytuje podporu, budou řízeně nahrazeny vhodnou alternativou.

Pro zajištění řádného stavu KI bude nutné, aby byla prováděna pravidelná analýza dostupnosti podpory na prvky v komunikační infrastruktuře rezortu MK. Tato kontrola bude probíhat pravidelně minimálně 1x za rok. Analýza umožní proaktivně identifikovat taková zařízení, u nichž bude ukončena podpora v následujících dvou až třech letech.

Nejdůležitějším úkolem komunikační infrastruktury rezortu MK je zajistit požadovanou kvalitu transportní služby pro různé typy aplikačního provozu rezortu MK a současně musí být připravena na implementaci takových technologií, jejichž implementace se vzhledem k vývoji a dostupnosti na trhu dá očekávat.

Z technologií, které mohou zásadním způsobem ovlivňovat požadavky na přenosovou infrastrukturu, se jedná především o tyto aplikace:

- Tenký klient. Centralizované aplikace založené na použití tenkého klienta jsou preferovaným způsobem implementace agendových systémů a aplikací.
- DMS. Způsob práce s dokumenty (místo vzniku, cílové umístění, množství a velikost dokumentů, četnost přístupu uživatelů) určuje požadavky na přenosovou infrastrukturu především s ohledem na dostupnou šířku pásma.
- Virtualizace koncových stanic, pokud by byla plánována.
- Sdílené share prostory. Předpokládá se využití sdílených prostor s řízením přístupu jednotlivých uživatelů i v budoucnu.
- Administrace a dohled. Pro řízení a dohled komunikační infrastruktury bude preferováno využití dedikovaných přenosových cest, které budou logicky odděleny od produkčních dat (logické oddělení lze realizovat na úrovni VLAN, VRF, MPLS VPN). Přístup do administračního prostředí bude zajištěn paketovými filtry a bude omezen jen na oprávněné uživatele/prostředky.

KI MK by měla být připravena zajistit transportní služby také pro provoz široké škály multimediálních aplikací (přenos hlasu, videokonferenční služby) se zcela různorodými požadavky na síťové přenosové vlastnosti a síťovou topologii vlastních multimediálních toků.

Cíle v dané oblasti:

- Zavedení procesu řízení životního cyklu komunikační infrastruktury napříč rezortem MK a sladění postupné náhrady komunikačních prvků s plánem nasazení nových technologií. Implementace inteligentní, tzv. application-aware komunikační infrastruktury schopné spolehlivě detekovat a řídit jednotlivé aplikační toky včetně měření jejich výkonnostních metrik.

- Modernizace a zvýšení dostupnosti a spolehlivosti LAN a WAN infrastruktury.

- Konsolidace WAN infrastruktury rezortu MK.

7.6.4.1.1 Datová centra

Datová centra budou sloužit jako hlavní centra pro propojení komunikační infrastruktury jednotlivých lokalit s externími subjekty pomocí externí konektivity. V datových centrech budou umístěna komunikační centra, která tuto komunikaci realizují. V komunikačních centrech budou implementovány základní komunikační služby a bezpečnostní prvky. Komunikační infrastruktura datových center bude umožňovat virtualizaci na síťové úrovni pro oddělení jednotlivých provozních prostředí a organizací. Obě centra budou propojena dostatečně silným redundantním propojením, tak, aby zde mohly být realizovány služby na bázi Ethernet, Fibre Channel pro zajištění veškeré potřebné komunikace.

Řešení infrastruktury datových center MK bude založeno na následujících stěžejních principech:

- hierarchická a modulární struktura s podporou virtualizace pro bezpečné oddělení a segmentaci jednotlivých aplikačních infrastruktur,
- podpora virtualizace na síťové infrastruktuře
- vysoká dostupnost, spolehlivost, propustnost a nízká latence,
- rychlá L2 i L3 konvergence v případě poruchy,
- vysoká škálovatelnost a snadná rozšiřitelnost,
- konvergence LAN a SAN infrastruktury,
- těsná integrace síťové a virtualizované serverové infrastruktury,
- široká podpora QoS a bezpečnostních mechanismů,
- jednoduchá a efektivní správa včetně využití pokročilých nástrojů pro automatizaci konfigurace výpočetních a síťových zdrojů,
- jednoduchý a efektivní autorizovaný způsob konfigurace a přístupu k provozním a správcovským datům na určeném místě přes naskenování nebo zadání kódu z daného zařízení.

Cíl v dané oblasti:

Cílem v dané oblasti je návrh architektury datových center, konsolidace stávajících komunikačních center do 2 a jejich optimalizace. Dále je předmětem povýšení propustnosti mezi datovými centry na minimálně 10GB, přičemž součástí architektury datových center bude i optimalizace komunikace mezi DC.

Dalším cílem je vybudování konektivitní části pro připojení farem serverů, umístěných v datových centrech. Je kladen důraz na podporu virtualizace serverů, virtualizace na síťové úrovni, konvergence LAN a SAN infrastruktury a začlenění KI datových center do systému automatizace DC infrastruktury. Optimalizace komunikační infrastruktury datových center MK, snížení počtu prvků, obnova páteřních prvků pro budování konektivity pro připojení farem serverů, napojení na

serverové farmy s respektováním virtualizace a protažením do druhého datového centra, zajištění dostupnosti serverů/aplikací.

7.6.4.1.2 Přenosová síť

Přenosová síť bude realizována formou služby od jednotlivých telekomunikačních operátorů. Budou použity privátní sítě, které garantují základní bezpečnostní požadavky, které budou vyplývat z bezpečnostní politiky. Tyto sítě musí minimálně garantovat, že nedojde ke smíšením daného provozu MK s provozem jiného zákazníka.

7.6.4.1.3 Externí konektivita

Externí konektivita bude tvořena hlavně konektivitou do Internetu, do sítě GovNet a CMS Dále sem patří veškeré další propojky k externím subjektům (například připojení bankovních domů, zdravotních pojišťoven, atd.).

7.6.4.1.4 Vzdálený přístup

Pro zajištění vzdáleného přístupu do komunikační infrastruktury bude zajištěno takové řešení, které umožní sdílení hardwarového vybavení všemi organizacemi v rámci rezortu včetně zajištění bezpečné autentizace uživatelů. Bude zajištěna integrace s relevantními Active Directory foresty, případně jinými systémy pro správu uživatelů. Technické řešení musí podporovat protokol IPv4 i IPv6.

7.6.4.1.5 Bezpečnostní prvky (FW)

Strategie v oblasti bezpečnostních prvků musí umožňovat oddělení jednotlivých částí či organizačních složek rezortu na základě definované jednotné bezpečnostní politiky. Bezpečnostní prvky budou podporovat kategorizaci provozu na základě použité aplikace a identifikace koncového uživatele.

V rámci rezortu budou provozovány tyto bezpečnostní soustavy:

- vnitřní bezpečnostní soustava
- vnější FW soustava

Sjednocení infrastruktury bezpečnostních prvků, soustav a jejich unifikace je prostředek k budování efektivní a bezpečné komunikační infrastruktury. Konsolidace v oblasti bezpečnosti na komunikační infrastruktuře musí být v souladu se sjednocením vnitřních procesů vedoucích k dosažením jednotné bezpečností politiky.

Bezpečnostní soustava musí kromě samotného řízení provozu disponovat systémem IPS a dalšími nástroji na detekci a eliminaci škodlivých kódů a aktivit, jako je detekce botů, řízení přístupů na úrovni aplikací, atd.

Řešení bude odolné proti výpadku a musí umožnit vzájemné zálohování lokalit obou datových center pro internetové spojení. Součástí ochrany perimetru bude i ochrana proti útokům typu DoS a DDoS.

Vnitřní bezpečnostní soustava

Dojde ke konsolidaci infrastruktury vnitřní bezpečnostní soustavy s ohledem na požadavky jednotlivých organizací a vzhledem k zefektivnění fungování komunikační infrastruktury jako celku. Cílová architektura vnitřních oddělených zón či VPN bude v souladu s jednotnou bezpečnostní politikou.

Vnější FW soustava

Vnější FW soustava bude chránit rezort před hrozbami z internetu, publikovat aplikace a služby do internetu.

Brány pro směrování elektronické pošty

V obou datových centrech budou vzájemně zálohované brány pro příjem a odesílání elektronické pošty. Ty budou napojeny na interní poštovní systémy každé organizace v rámci rezortu.

Na poštovních branách budou implementovány antivirové a antispamové filtry.

Antispamová ochrana bude využívat technologie pro sledování důvěryhodnosti, které přímo komunikují se zdrojovými IP adresami v Internetu a budou podporovat i tradiční technologie (antispamové signatury, atd.) v detekci a blokování spamů.

Komunikace elektronickou poštou musí podléhat kontrole z hlediska možného úniku citlivých dat, tedy poštovní systémy budou napojeny na systémy prevence ztráty dat (Data Loss Prevention), případně dále systémy prevence ztráty dat budou integrovány se šifrováním komunikace.

Administrace musí být oddělitelná pro jednotlivé správce daných organizací.

Řízení přístupu uživatelů do internetu (Webfiltering)

V rámci bezpečného přístupu do internetu bude řízen WWW provoz. Tento provoz bude na úrovni proxy serverů filtrován dle kategorií WWW stránek pro jednotlivé skupiny uživatelů. Kategorie musí být pravidelně doplňovány. Autentizace uživatelů musí být napojena na centrální správu identit.

Všechny stahované WWW stránky a soubory budou kontrolovány antivirovým systémem.

Proxy servery musí být odolné proti výpadku a zajistit spolehlivými mechanismy vzájemnou zálohu mezi internetovými přípojkami.

Komunikace uživatelů musí být kontrolována z hlediska možného úniku citlivých dat, tedy systémy proxy budou napojeny na systémy prevence ztráty dat (Data Loss Prevention), případně dále systémy prevence ztráty dat budou integrovány se systémy na šifrování komunikace.

Administrace musí být oddělitelná pro jednotlivé správce daných organizací.

Cíl v dané oblasti:

Cílem této oblasti je standardizace těchto prvků v rámci rezortu MK, konsolidace oddělených infrastruktur a optimalizace souvisejících procesů.

7.6.4.2 Síťové služby

S rozrůstáním komunikační infrastruktury a spojováním s dalšími celky dochází k nárůstu složitosti služeb podpůrných síťových protokolů DNS/DHCP/NTP. Správa, údržba a případné změny těchto systémů v sobě často skrývají nepředpokládané problémy a zvýšenou možnost výpadků, či jiných provozních systémů. Z těchto důvodu strategie v oblasti síťových služeb míří ke zjednodušení a centralizaci správy těchto služeb s možností delegování správy celků na konkrétní správce/subjekty (k této centralizaci se využije současný systém IPAM) a také podporu nových vlastností, které budou po těchto službách požadovány (např. IPv6, unikódové DNS záznamy,…).

Cíl v dané oblasti:

Cílem v této oblasti je sjednocení nástrojů používaných pro administraci v rámci rezortu MK CŘ

7.6.4.2.1 DNS

Služba DNS s centralizovanou správou bude složená z následujících komponent - systém pro centrální správu DNS (například systém IPAM – IP Address Management) – interní DNS – externí DNS.

Interní DNS

Interní DNS musí zajišťovat:

- DNS pro WAN
- DNS pro datová centra

Počet jednotlivých DNS serverů pro WAN i pro datová centra se bude řídit aktuálními požadavky. Všechny interní DNS servery ale budou spravovány z centrálního systému (např. IPAM).

Zabezpečení dynamické aktualizace DNS záznamů (DDNS) – bude se to týkat primárně klientů a serverů ve vnitřní síti.

Dotazy na záznamy DNS zóny patřící jiné organizaci v rámci rezortu MK budou přeposílány autoritativním serverům (conditional forwarding).

Interní DNS budou plně podporovat IPv6 záznamy.

Řešení interního DNS bude vysoce dostupné.

Externí DNS

Externí DNS musí zajišťovat

- internetové DNS umístěné v DMZ
- externí DNS pro ostatní externí sítě (Govbone, CMS,…)

Počet jednotlivých externích DNS serverů se bude řídit aktuálními požadavky. Všechny externí DNS servery ale budou spravovány z centrálního systému (IPAM).

Externí DNS budou podporovat unikódové DNS záznamy i plně IPv6 záznamy.

Řešení externího DNS bude vysoce dostupné.

Centrální systém pro správu DNS

Systém pro centrální správu umožní:

- centrálně řídit všechny DNS servery v síti MK
- delegaci práv pro jednotlivé správce/subjekty – např. delegace práv pro DNS datových center správci datových center

7.6.4.2.2 DHCP

Službu DHCP s centralizovanou správou bude složená z následujících komponent:

- systém pro centrální správu DHCP (například stejný systém pro správu DNS – IPAM)
- samotné DHCP servery pro WAN MK, řízené pomocí centrálního systému pro správu (IPAM)

DHCP systém musí být připraven na IPv6.

Řešení DHCP bude vysoce dostupné, protože centralizovaná forma této služby bude kritickou aplikací pro funkčnost pracovišť a dostupnost centrálních aplikací.

7.6.4.2.3 NTP

Pro službu NTP bude jednotný (nejlépe smluvně zajištěný) časový zdroj pro MK včetně ostatních organizací rezortu. Služba NTP bude provozována na stejném systému, jako služby DNS a DHCP.

7.6.4.3 Monitoring

7.6.4.3.1 Provozní monitoring komunikační infrastruktury

Těmito systémy se rozumí nástroje monitorující prvky komunikační infrastruktury jednotlivých složek rezortu MK, či její jednotlivé technologické celky. Jednotlivé systémy mohou být provozovány u dodavatele služby (např. u dodavatele IP telefonie) nebo jako vlastní.

Z provozního monitoringu se do zastřešujícího dohledového systému budou propagovat informace o stavu a výkonu.

Stavový monitoring

Stavový monitoring bude sledovat aktuální stav prvků komunikační. Systémy stavového monitoringu musí umožnit zasílání dat do zastřešujícího dohledového systému.

Výkonnostní (Performance) monitoring

Sběr výkonnostních parametrů bude zaměřen na sledování výkonnosti aktivních prvků sítě, využití přenosového pásma linek, sběr a analýzu přenášených dat. Tento výkonnostní monitoring musí umožnit zasílání dat o překročení nastavených prahových hodnot do zastřešujícího dohledového systému.

Úlohou výkonnostního monitoringu bude také měření doby odezvy systémů síťových služeb pomocí IP SLA testů. Výsledky testů, stejně jako všechna měření výkonnosti, budou zapracovány do měření kvality služeb (SLA) v zastřešujícím dohledovém systému.

Kapacitní plánování

Plánování kapacit bude využívat nástrojů performance monitoringu (zejména reporty trendů nad historickými daty) pro potřeby navýšení nebo snížení přenosové kapacity linek, kontrolu využívání systémových zdrojů serverů nebo podporu migračních scénářů.

7.6.4.3.2 Bezpečnostní monitoring komunikační infrastruktury

Strategie v oblasti bezpečnostního monitoringu je postavena na potřebě včasné a rychlé reakce na aktuální bezpečnostní hrozby v komunikační infrastruktuře rezortu MK vybudováním bezpečnostního dohledového centra. Cílem bezpečnostního monitoringu KI je redukce rizik vyplývajících z aktuálních bezpečnostních hrozeb a regulatorních požadavků následujícími aktivitami:

- Včasnou identifikací a následnou eliminací aktuálních rizik
- Snížením dopadů bezpečnostních událostí zkrácením času mezi detekcí a reakcí
- Automatizací manuálně vytvářených reportů
- Mapováním schopností bezpečnostního monitoringu na vyhovění požadavkům regulativ
- Vyhodnocováním a měřením efektivnosti bezpečnostních procesů pro další zlepšování

- Plným zaintegrováním lidí, procesů a technologií do životního cyklu informační bezpečnosti – plánování, provedení, kontrola a aktualizace bezpečnosti

Primárními klíčovými prvky, které budou tvořit bezpečnostní monitoring, jsou:

- sběr bezpečnostních událostí
- automatická analýza bezpečnostních událostí v reálném čase
- bezpečnostní procesy a bezpečnostní odborníci pro rychlou reakci na vzniklé bezpečnostní incidenty
- detekční mechanismy pro zachycení pokusů o porušení bezpečnostních pravidel

Sběr bezpečnostních událostí bude zajišťovat jednotný, konsolidovaný, plně kontrolovaný sběr událostí ze všech informačních systémů v prostředí rezortu MK. Sběr událostí dále zajistí normalizaci, klasifikaci a agregaci bezpečnostních událostí včetně podpory při investigaci/vyšetřování probíhajících bezpečnostních incidentů.

Nástroj pro sběr bezpečnostních událostí, postavený na řešení HP ArcSight Logger, bude sbírat události, a to nejen bezpečnostní, z různých datových zdrojů:

- Prvky bezpečnostní infrastruktury (např. IPS/IDS, FW, AAA)
- Systémové a aplikační logy
- Flow data
- Sledování aktivit uživatelů na serverech a stanicích

Automatická analýza bezpečnostních událostí v reálném čase bude řešena tzv. SIEM (Security Information and Event Management) nástrojem, který sbírá a zpracovává bezpečnostní události a data z prvků IT infrastruktury rezortu MK a jehož výstupem bude identifikace bezpečnostních incidentů pro včasnou detekci hrozeb, normalizované pohledy nad korelovanými událostmi a reporty. Tento nástroj bude sloužit pro zajištění přesnějšího odhadu dopadů identifikovaných bezpečnostních hrozeb a incidentů.

Pro realizaci procesů bezpečnostního monitoringu (detekce hrozeb, analýza, pochopení a stanovení protiopatření, aplikace protiopatření, kontrola účinnosti protiopatření) v praxi bude nutné etablovat bezpečnostní tým (vlastní popř. dodavatelsky).

Nedílnou součástí bezpečnostního monitoringu budou detekční mechanismy pro zachycení pokusů o porušení bezpečnostních pravidel a ověřování citlivosti detekčních mechanismů realizovaných pomocí IPS/IDS nástrojů, reputačních databází, nástrojů na identifikaci zranitelností systémů a aplikací a provádění penetračního testování včetně propojení s bezpečnostními procesy a SIEM nástrojem. Testy zranitelnosti budou prováděny pravidelně několikrát ročně. Výsledkem bude seznam a ohodnocení zranitelností dle jejich závažnosti s doporučením, jak tyto zranitelnosti eliminovat.

7.6.4.4 Bezpečnost síťových a hlasových služeb

Nezbytným krokem k zajištění bezpečnosti síťových a hlasových služeb je vytvoření kompletní bezpečnostní dokumentace. A to takové, která bude plně v souladu nejen s legislativními požadavky, ale i odborných norem zejména ISO/IEC 27000.

Klíčovým atributem řešení komunikační infrastruktury MK je její bezpečnost. S ohledem na zajištění kybernetické bezpečnosti IT infrastruktury MK ve smyslu zákona o kybernetické bezpečnosti a v souladu se stávající legislativou musí být vypracována bezpečnostní politika.

Komunikační infrastruktura rezortu MK musí být tedy nejen odolná proti útokům typu Denial of Service, útokům cíleným na její jednotlivé uzly, přenosové trasy, kritické služby, útokům vedeným na síť jako celek, ale rovněž musí být schopna poskytovat relevantní informace o bezpečnostních incidentech a směrovat je do centrálních dohledových systémů včetně možnosti spolupráce s národním pracovištěm CERT (Computer Emergency Response Team).

Cíl v dané oblasti:

Cílem v dané oblasti je vytvoření bezpečnostní dokumentace pro celý rezort MK a prosazení bezpečnostní politiky do IT.

7.6.5 Strategie v oblasti datových center/HW infrastruktury

Revitalizace stávajících datových center MK či jejich náhrada v lokalitách vlastněných či pronajímaných MK je činnost nákladná a z pohledu kompetenční činnosti rezortu podpůrná. Budování privátních datových center jednotlivých rezortů státní správy je také v rozporu s vládní koncepcí využívání služeb v oblasti informatiky napříč rezorty.

V dlouhodobém horizontu tak MK hodlá přesunout vybranou technologickou infrastrukturu ze svých datových center do datových center státem centrálně poskytovaných rezortům (například datové centrum Státní tiskárny cenin) využívaných formou služby se smluvně zajištěnou kvalitou (SLA) a vybrané aplikace a informační systémy dále provozovat ve svých zrevitalizovaných datových centrech.

V konkrétní rovině tak MK v budoucnu plánuje využívání dvojice - primárního a záložního - datových center, geograficky vzdálených v rámci Prahy. Datová centra pak budou doplněna o lokalitu, v rámci které budou ukládána archivační a záložní média.

S ohledem na ochranu investic a z důvodu bezpečnosti přístupu k aplikacím a datům budou ve stávajících datových centrech umístěné technologie ve vlastnictví MK využívány minimálně do konce jejich životnosti.

7.6.5.1 Infrastruktura datových center

Infrastruktura datových center je budována jako multitenant, tedy tak, aby umožňovala logické i fyzické oddělení prostředků dle bezpečnostních a právních požadavků aplikací a aplikačních vrstev.

Infrastruktura jednotlivých prostředí je rozdělena do několika bezpečnostně a funkčně oddělených bloků:

- Prezentační vrstva
- Aplikační vrstva

- Databázová vrstva
- Služební vrstva (Dohled, správa, zálohování, automatizace,…)

Dále je infrastruktura v duchu multitenant architektury rozdělena podle způsobu práce s daty na následující logicky a komunikačně oddělená prostředí:

- Produkční prostředí
- Testovací prostředí
- Integrační prostředí
- Školicí prostředí

Pro aplikace u kterých je vyžadována vysoká dostupnost se předpokládá dosažení vysoké dostupnosti v jednotlivých vrstvách formou failover clusteru nebo aplikačního clusteru. Není nutné, aby všechny aplikace implementovaly všechny navržené vrstvy a prostředí. Implementace se řídí požadavky konkrétní aplikace.

Všechna prostředí a aplikační vrstvy sdílí jednu centrální infrastrukturu datových center, která je na technické vybavení mapována následujícím způsobem:

- Servery umístěné v blade chassis připojené do LAN a SAN komunikační infrastruktury
- Data, aplikace i operační systémy serverů jsou po SAN ukládána na centrální disková pole
- Zálohování dat je prováděno na deduplikační knihovny (zálohování na disk)
- Dlouhodobá záloha je prováděna na páskové knihovny s médii typu LTO, které umožňují následný odnos

Při budování je základní premisou stavba z unifikovaných komoditních stavebních bloků (blade servery, bloková rozšiřitelnost diskových polí a zálohovacích zařízení, …) tak, aby bylo možné infrastrukturu v případě potřeby rozšiřovat.

7.6.5.1.1 Operační systémy

Všechny systémy budou provozovány na jednom z následujících operačních systémů:

- MS Windows 2008 nebo novější
- Red Hat Enterprise Linux
- SuSe Enterprise Linux

7.6.5.1.2 Serverová infrastruktura

Z hlediska možnosti efektivního připojení do komunikační infrastruktury, snadné rozšiřitelnosti, spravovatelnosti a úspory prostoru, bude veškerý výpočetní výkon realizován na platformě blade.

Všechny blade chassis budou vybaveny konektivitou do SAN a LAN.

Blade chassis budou osazeny servery s CPU platforem Intel x64.

Součástí řešení bude služební vrstva, která umožní snadný provisioning, administraci, zálohování a dohled fyzických i virtuálních serverů.

7.6.5.1.3 Virtualizace x86/x64

V rámci datových center bude na x64 serverové infrastruktuře vybudována centrální virtualizační vrstva na platformě VMware ESXi. Tato virtualizační vrstva bude jednotná pro všechna prostředí. Jednotlivá prostředí budou logicky oddělena až na úrovni této virtualizační infrastruktury.

Na této virtualizační infrastruktuře budou provozovány všechny systémy, u kterých to bude z hlediska kompatibility a licenčních podmínek možné a výhodné.

Virtualizační infrastruktura bude vybudována jako vysoce dostupná v rámci jednoho datového centra i mezi datovými centry s podporou replikace mezi diskovými poli.

Poznámka: pokud bude vhodné, resp. nutné využít fyzické servery, použijí se rovněž unifikované technologie popsané v tomto dokumentu.

7.6.5.1.4 Prezentační vrstva

Servery prezentační vrstvy budou připojeny do oddělené části společné komunikační infrastruktury. V rámci komunikační infrastruktury bude zajištěn jak případný load balancing požadavků, tak i bezpečnostní oddělení serverů, jednotlivých vrstev a prostředí.

Servery prezentační vrstvy budou typu x86/x64. Tam, kde to bude vhodné, bude prezentační vrstva provozována na VMware ESX virtualizované infrastruktuře na platformě x86. V ostatních případech je možno provozovat prezentační vrstvu na fyzických serverech.

Vysoká dostupnost prezentační vrstvy bude zajištěna s ohledem na možnosti aplikace buď samotnou aplikací a load balancingem nebo virtualizační vrstvou.

Cíl v dané oblasti:

Cílem je vytvoření prezentační vrstvy a přesun současných serverů do nově vybudovaného prostředí.

7.6.5.1.5 Aplikační vrstva

Servery aplikační vrstvy budou připojeny do oddělené části společné komunikační infrastruktury. V rámci komunikační infrastruktury bude zajištěn jak load balancing požadavků, tak i bezpečnostní oddělení serverů, jednotlivých vrstev a prostředí.

Servery prezentační vrstvy budou typu x86/x64. Tam, kde to bude především z licenčního hlediska vhodné, bude aplikační vrstva provozována na VMware ESX virtualizované infrastruktuře na platformě x86. V ostatních případech je možno provozovat prezentační vrstvu na fyzických serverech.

Vysoká dostupnost aplikační vrstvy bude zajištěna s ohledem na možnosti aplikace buď samotnou aplikací a load balancingem nebo virtualizační vrstvou.

Cíl v dané oblasti:

Cílem je vytvoření aplikační vrstvy a přesun současných serverů do nově vybudovaného prostředí.

7.6.5.1.6 Databázová vrstva

Databázový výpočetní výkon bude realizován na platformě Microsoft SQL a MySQL. Data i operační systémy databázové vrstvy budou umístěny na diskových polích připojených přes SAN.

Lokální vysoká dostupnost databázové vrstvy v rámci datového centra bude zajištěna virtualizační vrstvou. Vysoká dostupnost databázové vrstvy mezi datovými centry bude zajištěna technologií Metro clusterů za pomocí replikace dat mezi diskovými poli.

Cíl v dané oblasti:

Cílem je vytvoření jednotné databázové vrstvy se 2 typy databází MySQL a Microsoft SQL, jejich dostatečné dimenzování a umožnění snadné a ekonomické rozšiřitelnosti.

7.6.5.2 Disková úložiště

Data aplikací a případně i operační systémy a aplikace budou uložena na dvou centrálních diskových polích. V každé lokalitě bude jedno diskové pole. U diskových polí je kladen důraz především na výkona rozšiřitelnost.

Mezi primárním a záložním datovým centrem bude vytvořena transparentní komunikační infrastruktura SAN, do které budou připojena všechna zařízení s přístupem k diskovým polím nebo zálohovacím zařízením připojeným do SAN.

Diskový prostor bude realizován jako virtualizované diskové úložiště s možnosti Tier.

a. Tier 0 rychlá disková kapacita typu SSD
b. Tier 1 rychlá disková kapacita například disky typu SAS
c. Tier 2 pomalá disková kapacita například disky typu SATA

Cíl v dané oblasti:

Cílem v dané oblasti je vytvoření multi-tier diskové kapacity, která je připojitelná k jednotlivým výpočetním prostředkům pomoci technologie SAN.

7.6.5.3 Služební vrstva

Služební vrstva zajišťuje společně a povinně využívané služby poskytované datovým centrem na systémové úrovni, tj. systémy a aplikace implementované v DC využívají těchto služeb povinně, nenahrazují jejich roli vlastní implementací (např. zálohování, dohled a pod.)

Služební vrstva zahrnuje:

- Přidělování HW prostředků všech instalovaných fyzických i virtuálních serverů a diskových polí
- Provisioning – automatizace administrativních zásahů prováděných na infrastruktuře datového centra včetně souvisejících zásahů na komunikační infrastruktuře DC.
- Možnost automatické konfigurace související infrastruktury
- Monitoring infrastruktury
- Zálohování dat, aplikací a operačních systémů
- Monitoring konfigurace a maintenance HW odděleně od HW (podpora rychlé výměny “WakeUp” a jednoduchého rozšíření “scaling")

Cíl v dané oblasti:

Vytvoření servisní vrstvy.

7.6.5.4 Monitoring infrastruktury

Infrastrukturní monitoring je určen pro správu a dohled systémů pomocí inteligentních agentů, kteří jsou distribuováni na jednotlivé sledované stroje rozdílných platforem. Primárním úkolem agentů je sběr dat, jejich vyhodnocování, vytváření vazeb mezi informacemi z jednotlivých částí v rámci monitorovaného systému, vzájemnou korelaci informací a o provádění nápravných akcí v případě potřeby. Jako primární datové zdroje musí být agent schopen využívat:

- SNMP (Simple Network Management Protocol),
- Perflib (NT/Win2K),
- WMI Store (Windows Management Instrumentation),
- Windows Event Logfiles (NT/Win2K),
- systémové logy,
- aplikační logy,
- ODBC/JDBC
- informace zajištěné prostřednictvím vlastního API,
- informace zpřístupňované pomocí skriptů či externích programů,
- informace z integrovaných aplikací,
- vlastní veličiny vytvářené a zpřístupňované pomocí skriptů nebo externích programů

Vyhodnocování nasbíraných údajů bude zajištěno prostřednictvím předpisů (policies), které se spolu s agentem distribuují na dohlížené stoje. Předpisy popisují, co se má sledovat a jak reagovat na identifikovanou událost (buď automaticky, nebo se nabízí akce ke spuštění operátorovi). Logika rozhodování bude tedy distribuována na agenty, čímž se výrazně šetří komunikační pásmo. Agenti budou i při výpadku komunikace s dohledovým serverem schopni nadále autonomně monitorovat všechny předepsané atributy v jednotlivých šablonách.

Cíl v dané oblasti:

Cílem je vybudovat centrální dohledové pracoviště pro monitoring a správu infrastruktury z hlediska dostupnosti a výkonnosti všech kritických komponent.

7.6.5.5 Centrální zálohování

Zálohováním se v následujícím textu rozumí ukládání dat a operačních systémů pro jejich obnovu do posledního funkčního stavu v případě poruchy či neštěstí, které způsobí ztrátu těchto dat. Vzhledem k povaze zálohy se předpokládá držení dat v maximální periodě 4 týdny.

Dlouhodobou zálohou se rozumí dlouhodobé ukládání dat, které je vyžadováno právními předpisy nebo interními nařízeními. Předpokládá se uchování vybrané množiny záloh (například měsíční záloha vybraných systémů) a její držení až po dobu 10 let. Držení záloh se předpokládá v chráněné lokalitě oddělené od datových center.

Zálohování a dlouhodobé zálohování bude řešeno jako vrstva společná pro všechny části infrastruktury datových center. Zálohování všech aplikací a operačních systémů využívaných v rámci datových center bude v rámci úspory místa a přenosové kapacity prováděno způsobem D2D2T. Tedy:

- Pravidelná (denní/týdenní) záloha dat z disků na diskové zálohovací zařízení (s deduplikací)
- Pravidelná (měsíční) kopie vybraných dat na fyzické páskové zařízení typu LTO včetně odnosu páskových médií mimo datové centrum

Vzhledem k maximálnímu možnému zabezpečení dat bude použita funkcionalita kopie dat mezi primární a záložní deduplikační knihovnou.

Cíl v dané oblasti:

Vytvoření technologie centrálního zálohování a prosazení technologie jednotného zálohování napříč aplikacemi.

7.6.5.6 Klasifikace dostupnosti služeb

Pro jednotné poskytování služeb datových center je nutné vytvořit jednotnou klasifikaci kvality poskytovaných služeb (služeb virtuálního výkonu). Z tohoto důvodu je nutné vytvořit standard pro jednotnou klasifikaci kvality služeb poskytovaných službami DC.

Cíl v dané oblasti:

Vytvoření standardu dostupnosti služeb v rámci datových center

7.6.6 Strategie v oblasti bezpečnosti ICT

IT bezpečnost, jejíž součástí jsou kybernetická a informační bezpečnost, je nedílnou součástí jednotného systému řízení bezpečnosti rezortu MK.

Základním cílem strategie je vytvoření bezpečného IT prostředí, kde veškerá informační aktiva budou odpovídajícím způsobem chráněna proti vnějším i vnitřním hrozbám napříč celým rezortem MK ve všech jeho složkách. Bude zajištěn soulad s existující i připravovanou legislativou. Budou průběžně vyhodnocovány bezpečnostní trendy a bezpečnostní opatření budou v těchto souvislostech aktualizována. Bude zajištěno odpovídající finanční a personální zázemí, potřebné pro zajištění schopnosti plnit úkoly z toho vyplývající. V souladu s navrženým systémem jednotného řízení bezpečnosti rezortu MK bude vytvořena odpovídající bezpečnostní dokumentace.

Cíl strategie bude naplňován současně s naplňováním ostatních cílů dílčích strategií celkové strategie ICT MK. To znamená, že realizace opatření, vyplývajících z ostatních dílčích strategií bude v souladu s nároky na bezpečnost.

K naplnění celkové strategie bezpečnosti IT je nutno zajistit minimálně úkoly popsané v kapitole 8 Plán strategických projektů.

7.6.7 Strategie v oblasti aplikačních služeb

7.6.7.1 Oblast IT potřeb věcných agend

7.6.7.1.1 Zajištění provozu a rozvoje existujících agendových informačních systémů

Mezi stěžejní úkoly v této oblasti patří vývoj a implementace systému pro OCNS a JEGIS – viz související text s popisem.

7.6.7.1.2 Zajištění informační podpory doposud nepodporovaných agend

MK musí podporovat informačním systémem i další agendy, které je potřeba teprve realizovat. Pro jeho realizaci bude nutné připravit výběrové řízení, a proto musí proběhnout následující kroky (všechny kroky musí respektovat Příkaz ministra pro závazný postup při zadávání veřejných zakázek

Ministerstvem kultury ve smyslu zákona č. 137/2006 sb., o veřejných zakázkách, ve znění pozdějších předpisů):

- Připravit harmonogram otevřeného zadávacího řízení (dle § 27 ZVZ),
- Provést analýzu věcné potřeby:
  - provést analýzu procesů, které mají být podporovány novou agendou (včetně zohlednění připravované legislativy),
  - analyzovat požadavky na uživatelské rozhraní,
  - analyzovat potřeby z hlediska architektury systému,
- Stanovit předpokládanou hodnodu veřejné zakázky na základě již realizovaných veřejných zakázek na podobné služby,
- Zpracování zadávací dokumentace a zpracování její technické části na základě provedené analýzy (součástí zadávací dokumentace musí být požadavek na dodavatele na zpracování detailní funkční specifikace na základě legislativy, metodik a dodané analýzy procesů),
- Vymezení požadavků na kvalifikaci,
- Stanovení hodnotících kritérií,
- Zpracování návrhu na realizaci zadávacího řízení,
- Zveřejnění předběžného oznámení o zadávacím řízení dle zákon č. 137/2006 Sb.,
- Finalizace kompletních zadávacích podmínek.

Pro úplnost uveďme, že po přípravě výběrového řízení budou následovat kroky směřující k uzavření smlouvy s dodavatelem:

- Zahájení otevřeného zadávacího řízení,
- Jmenování hodnotící komise,
- Příjem nabídek, otevření obálek a posouzení nabídek,
- Rozhodnutí o výběru nejvhodnější nabídky,
- Uzavření smlouvy a realizace.

7.6.7.2 Oblast IT potřeb průřezových procesů agend a sdílených komponent

7.6.7.2.1 Integrovaný analytický systém kultury a archivů (IASKA)

Základním strategickým cílem je vybudování integrovaného analytického systému v oblasti kultury a archivů za účelem poskytnutí výsledků analytických dotazů nad dostupnými daty veřejnosti, školství a vědeckým institucím. Data jsou již dnes často k dispozici v digitalizované formě ovšem ve značně roztříštěné podobě a často složitě dostupné koncovým uživatelům (tj. občanům, zaměstnancům dotčených organizací, badatelům, atd.) v archivech NDK, informačních systémech MK, externích zdrojích (např. jiné knihovny, galerie, burzy, muzea, …) a také otevřeného Internetu.

Mezi zcela zjevné přínosy patří možnost získání podstatných informací pro zvýšení kulturní informovanosti veřejnosti, nacházení nových zdrojů kulturního dědictví, získání informací o českém kulturním dědictví z externích zdrojů a nacházení vztahů mezi informacemi z kultury, historie, ale také společenských vztahů. Takovýto systém pokryje svým rozsahem extrémně velký objem dat, ale poskytne uživatelům nové informace, které dnes se dohledávají buď složitě nebo intuitivně, nebo dohledat vůbec nejde.

Realizace tohoto cíle obnáší vytvoření jednak ICT infrastruktury úložného systému

typu „Big Data“, systému získávání dat („crawlery“), ale hlavním systémem bude samotný analytický software s moderními nástroji vizualizací. Tento analytický software musí mít kromě přirozených analytických vlastností určených pro předem neznámé formy dat jak strukturované, tak i nestrukturované, musí mít expertní charakter systému, využívající např. prvky umělé inteligence („AI“) a být schopen „se učit“ a přizpůsobovat svůj vnitřní systém dynamickému vývoje a aktuálním výsledkům. Problematika dat, jejich pořizování a zejména hodnocení je klíčová pro resort z pohledu jeho efektivního řízení a plánování. Výstupy a výsledky systému budou jistou formou podpory rozhodování. Proto je nutné implementovat nejen samotné technologie, ale zohlednit i problematiku z oblastí teorie informace a systémů řízení. Hlavní cíl bude tedy získat ze systému a výsledků maximální množství efektivních dat a ty dát k dispozici manažerům pro budoucí plánování, ale i zpětné vyhodnocení předešlých rozhodnutí.usí také mít vlastnosti umělé inteligence („AI“), kde systém je schopen „učit se“ a tak přizpůsobovat další jeho vnitřní program dle předchozích výsledků. Na dodané produkty bude navazovat přiz přizpůsobení produktů potřebám MK, což bude obsahovat i programování a služby.

7.6.7.3 Oblast doplňkových aplikací

7.6.7.3.1 Zajištění stavu existujících aplikací a provedení nápravných opatření

Pro zajištění informační podpory dalších ať již specifických nebo běžných informačních potřeb jednotlivých organizačních složek MK a podřízených organizací jsou provozovány další aplikace. Pro narovnání aktuálního neutěšeného stavu a dosažení cíle, že IT bude schopné kvalitně plnit informační potřeby odborů a oddělení jsou třeba následující kroky:

- Zpracovat katalog aplikací se všemi náležitostmi
- Zjistit využití aplikací a které aplikace nejsou vůbec používané,
    - Zjistit důvody, proč nejsou používané (nejsou potřeba / jsou nepoužitelné / jiné důvody),
- Vyřadit nepotřebné aplikace a přestat je provozovat,
- Zjistit spokojenost uživatelů s používanými aplikacemi,
- Realizovat nápravná opatření ke zvýšení spokojenosti uživatelů s potřebnými aplikacemi formou jejich opravy nebo vybrání nového řešení (otevřené výběrové řízení) v případě, že není ekonomické provést opravu. Pro provozované a nepodporované aplikace bude nutné zajistit pomocí otevřeného výběrového řízení podporu aplikací.

7.6.7.3.2 Systém evidence vyhrazených technických zařízení (VTZ) MK

Účelem je získat evidenci VTZ, zaregistrovat kategorizaci v souvislosti na zákonné úpravy. Vyhláška č. 73/2010 Sb. o stanovení vyhrazených elektrických technických zařízení, jejich zařazení do tříd a skupin a o bližších podmínkách jejich bezpečnosti (vyhláška o vyhrazených elektrických technických zařízeních)

Systém je možné využívat jako kontrolní prostředek a důkazový server na vyhrazené technické zařízení. K zařízením je postupně připojená dokumentace, jako jsou například: manuály, atesty, schémata, kontakty na servis, HelpDesk apod. V systému budou evidovány revizní zprávy, atesty, opravy, termíny, legislativní podmínky a záznamy prací a poruch.

- Protipožární systémy, zdvihací zařízení, Elektro, tlak, plyn, chemie, atd.

7.6.7.3.3 Systém evidencí a správy vztahů k BOZP zákon 09/2006 Sb. § 1-14, kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci

Systém bude umožňovat centrální evidenci nařízení, opatření, formulářů, vykonávacích předpisů ve struktuře potřeb

- Registrace a hlídání zákonných termínů
- Pracovní pokyny
- Posouzení rizika
- Kvalifikační požadavky a oprávnění
- Formuláře a záznamy
- Ticket management
- První Pomoc
- Registrace pracovních úrazů
- Registrace externích zaměstnanců
- Provázaný katalog formulářů

7.6.7.4 Oblast IT podpůrných systémů

Personální systém (OKbase)

Provoz a rozvoj personálního systému (OKbase) je nyní po věcné, technické i smluvní stránce zajištěn. Pro zajištění bezproblémového provozu a rozvoje systému v dalším období bude vypsáno otevřené výběrové řízení nejpozději 1 rok před ukončením platnosti stávající smlouvy.

Ekonomický systém (EIS JASU)

Provoz a rozvoj ekonomického systému (EIS JASU) je nyní po věcné, technické i smluvní stránce zajištěn.. Běžný provoz a správa je zajišťována zaměstnanci IT odboru MK.

7.6.7.5 Oblast integrací aplikačních služeb

7.6.7.5.1 Zajištění integrace agendových IS s externími systémy

Pro budoucí integrace agendových systémů MK a ostatních systémů rezortu, státní správy a internetu je nutné zajistit integrační vrstvu, která umožní tyto integrace provádět. Integrační služby budou řešeny jednotnou integrační sběrnicí, která aktuálně na MK neexistuje.

Oblast integrace agendových informačních systémů s externími systémy je klíčovou oblastí pro výměnu informací mezi rezortem a ostatními ISVS. V souladu s definovaným cílem 7. této Strategie „Soulad s požadavky eGovernmentu“ je nutné zajistit funkční a spolehlivé napojení rezortních informačních systémů na stávající i plánované centrální služby eGovernmentu ČR.

Mez stávající centrální služby eGovernmentu patří:

- **Základní registry** - ve smyslu zákona č.111/2009 Sb., o základních registrech (ZZR);
- **Datové schránky** – ve smyslu zákona č.300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů;
- **Centrální Místo Služeb –** napojení na CMS;
- **JIP/KAAS** – propojení identiního prostoru úřadu s JIP/KAAS;
- **CzechPOINT** – poskytování asistovaných služeb klientům rezortu prostřednictvím poboček CzechPOINT, poskytování online služeb pomocí samoobsluženého portálu CzechPOINT@home, poskytování služeb úředníkům prostřednictvím CzechPOINT@office;

V rámci tohoto projektu je potřeba reagovat i na plánovaný rozvoj eGovernmentu ČR zejména v těchto oblastech:

- **Úplné elektronické podání** – připravit aplikační prostředí pro příjem strukturovaného elektronického podání a pro poskytování informací o stavu vyřízení elektronického podání.
- **eIDAS** – implementovat změny související se zavedením eIDAS. Nařízení EU se týká zavedení jednotného digitálního trhu a má za cíl zvýšit důvěryhodnost elektronických transakcí mezi státy EU. Nařízení se dotýká zejména těchto oblastí:
    - důvěryhodná elektronická identita fyzické osoby;
    - důvěryhodný podpis zaručující integritu a vazbu na identitu fyzické osoby;
    - důvěryhodná značka zajišťující integritu a vazbu na právnickou osobu;
    - důvěryhodné časové razítko zajišťující integritu a vazbu na čas;
    - důvěryhodná služba registrovaného elektronického doručování zajišťující integritu a vazbu na odesílatele, adresáta a čas odeslání a doručení;
    - důvěryhodný dokument se zaručenou integritou;
    - důvěryhodnost webových stránek s vazbou na provozovatele
- **eGON Service Bus –** připravit prostředí pro sdílení nereferenčních údajů subjektů práva. eGON Service Bus bude sloužit OVM pro výměnu informací, které se vztahují na subjekty práva vedené v Základních registrech (ROB, ROS) a objekty vedené v Základních registrech (RUIAN).

Postup

- V souladu s referenčním modelem ústředního správního úřadu, které definovalo Ministerstvo vnitra, vytvořit jednotné komunikační rozhraní úřadu, které by řešilo bezpečné napojení na stávající služby eGovernmentu ČR, zejména na Základní registry, ISDS, CMS, JIP/KAAS.
- Implementovat změny v souvislosti se zavedením eIDAS.
- Implementovat rozhraní na eGON Service Bus.
- Implementovat rozhraní pro poskytování služeb prostřednictvím CzechPOINT.
- Implementovat rozhraní pro příjem a poskytování informací o úplném elektronickém podání.

Přínosy

Vytvoření jednotného komunikačního rozhraní bude mít tyto přínosy:

- Zavedení jednotné elektronické komunikace s klienty úřadu
- Zavedení jednotné elektronické komunikace s OVM
- Zavedení spolehlivého a bezpečného propojení se stávajícími centrálními službami eGovernmentu ČR
- Snížení nákladů na implementaci změn v souvislosti s eIDAS

Snížení nákladů na implementaci změn v souvislosti s rozvojem eGovernmentu ve stávajícím programovém období

7.6.7.6 Oblasti správy licencí

7.6.7.6.1 Optimalizace licencí aplikací provozovaných v rezortu MK

Pro naplnění cíle v oblasti správy licencí je třeba nastavit proces a podpořit ho vhodnými nástroji a personálně zajistit. Kroky k narovnání stavu v oblasti licencí jsou následující:

- IT MK nastaví proces nákupu licencí pro MK a podřízené organizace,
- IT MK zajistí, že tento proces bude mít dostatečné personální pokrytí,
- Vyhodnocení stavu využívání licencí a cílem zjistit, zda neprobíhají platby za nevyužívané licence,
- Přestat platit nevyužívané licence, pokud to smluvní vztahy dovolí,
- Nakupovat všechny licence nadále přes jeden centrální proces.

Nákup licencí je jedním z typických procesů, kde lze s výhodou využít synergického efektu centralizace pro celý rezort.

7.6.8 Strategie v oblasti digitalizace

7.6.8.1 Východiska

Digitalizace kulturního dědictví představuje jedinečné procesy, kterými se v oblasti kultury může MK připojit k eGovernmentu implementací nástrojů a principů eCulture, čímž přispěje k rozvoji informační společnosti a znalostní ekonomiky zaváděním elektronických služeb v oblasti přístupu k obsahu kulturního dědictví, jeho konverzí na digitální objekty, zajištěním dlouhodobého uchovávání, jeho ochrany a zpřístupňování veřejnosti prostřednictvím informačních systémů. Prioritním úkolem těchto aktivit je záchrana kulturního dědictví (formou vytvoření digitálních kopií s nejvyšší efektivní dosažitelnou kvalitou), u kterého existuje – kvůli věku, poškození, konečné trvanlivosti apod. - nebezpečí nevratné ztráty. Dále pak online zpřístupnění reprezentativního výběru kulturního dědictví České republiky, dokumentujícího historii, kulturní rozmanitost a jeho příspěvek k rozvoji lidské společnosti, podpora národní identity a zviditelnění v zahraničí a zvýšení míry zapojení do mezinárodních aktivit, např. směřujících k vytvoření evropské digitální knihovny - Europeany. Tento záměr je promítnut i v 3. Prioritní ose a specifických cílech Integrovaného regionálního operačního programu (IROP), jehož prostřednictvím garantuje Evropská unie pro Českou republiku finanční zdroje pro projekty digitalizace českého kulturního dědictví a rozvoj eCulture.

Digitalizace kulturního dědictví jako technologické téma se nyní nevyhnutelně stává součástí strategie ICT. Systém digitalizace projektově představuje široké spektrum technologických aktivit, které je nezbytné řídit centrálně, v rámci úkolů Státní kulturní politiky, mj. z důvodu následujících strategických nedostatků:

- fragmentace přístupů k digitalizaci kulturního dědictví na úrovni paměťových a fondových institucí;

- nedostatečná institucionální definice digitalizace coby prioritní oblasti v rámci chodu a strategického plánování jednotlivých PFI;
- neschopnost mnohých PFI odpovědět v oblasti kulturního a vědeckého dědictví na potřeby uživatelů, rozpoznat a implementovat perspektivy možností informační společnosti;
- nedostatečná integrace digitalizačních akcí ve znalostní ekonomice a slabé uplatnění digitálních kulturních zdrojů ve znalostní společnosti;
- slabé propojení současné legislativy v oblasti kulturního dědictví s požadavky uživatelů, zejména při prosazování využití kulturního obsahu ve vzdělávání, výzkumu, v obsahovém průmyslu a v službách s přidanou hodnotou (meziodvětvové zájmy s cílem podpory růstu znalostní ekonomiky);
- fragmentované mechanismy definice výběru objektů, financování a cílů digitalizace kulturního obsahu;
- stagnující a neefektivní národní technická vybavenost a odbornost;
- absence logiského rozdělení digitalizační práce a produkce mezi kompetentní paměťové a fondové instituce;
- neadekvátní přispívání ČR do mezinárodního kulturního dialogu a k propojení evropského dědictví ve smyslu doporučení a programů Evropské komise v oblasti digitalizace.

Potřebu centrálního strategického řešení odůvodňují technologické důvody:

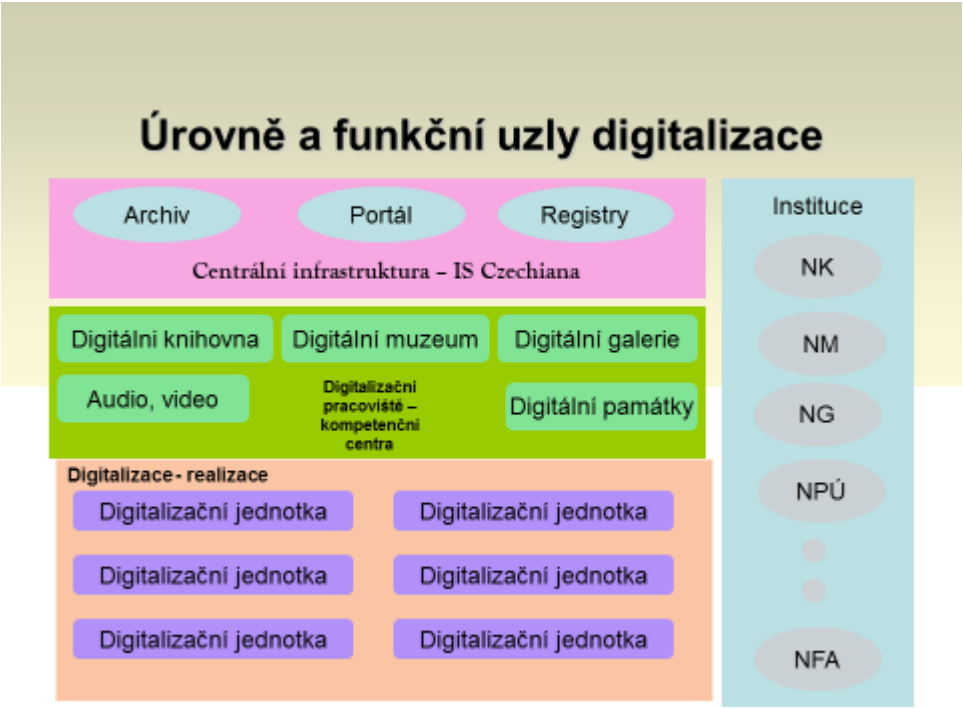
- neschopnost klíčových informačních technologií na decentralizované úrovni vypořádat se s technologickou změnou a informační bezpečností;
- nedostatečná interoperabilita informačních systémů, nedostatek vhodných softwarových nástrojů pro integraci;
- nutnost překonat roztříštěnost a duplikaci v dosavadních digitalizačních aktivitách a zajištění kompetencí pro národní a věcně příslušné paměťové a fondové instituce;
- roztříštěná digitalizační praxe v oblasti jedinečných kulturních objektů, vyžadujících zvláštní přístup;
- nutnost zajištění udržitelnosti procesu digitalizace;
- nutnost efektivního propojení digitálního obsahu kulturního dědictví na evropskou digitální knihovnu - Europeana prostřednictvím národního informačního systému.

7.6.8.2 Základní linie procesu digitalizace

Digitalizace jako soubor činností je z technologického hlediska struktúrovaná na dvě základní linie projektů:

- **infrastrukturní projekty** - centrální systémová infrastruktura pro zajištění dlouhodobé archivace, ochrany, správy, zpracování a zpřístupnění digitálního obsahu zahrnuje centrální datové úložiště (sklady) a centrální aplikační a prezentační infrastrukturu - informační systém Czechiana, nositelem které bude Ministerstvo kultury jako národní agregátor;
- **digitalizační projekty** - Digitální knihovna a archiv, Digitální muzeum, Digitálním galerie, Digitální film, video, audio, Digitální památky - nositeli budou národní a věcně příslušné paměťové a fondové instituce jako sektoroví agregátoři.

Schéma komplexního systému digitalizace naznačuje základní vazby mezi subsystémy na obr. č. 1



Obrázek 3 Základní schéma úrovní digitalizace

7.6.8.3 Infrastrukturní projekty

Projekty centrální systémové infrastruktury pro zajištění dlouhodobé archivace, ochrany, správy, zpracování a zpřístupnění digitálního obsahu sledují vytvoření hardwarové infrastruktury, platformy pro centrální aplikační systém Czechiana a poskytování hardwarové platformy digitalizačních projektů.

V praxi to znamená vytvoření robustní infrastruktury dvou hlavních datových center (primární a záložní, které fungují online) a záložního tzv. dark archive (offline), které vzniknou centralizací vybraných služeb v rezortu na jedno místo (tam, kde je to z hlediska realizace a nákladů efektivnější) a jejich propojení se systémy paměťových a fondových institucí i digitalizačních pracovišť.

Z funkčního hlediska budou datová centra plnit specifické cíle:

- podpora dlouhodobé archivace a ochrany dat velkého objemu;
- realizace velkokapacitního sdíleného on-line úložiště pro zpracování digitálního obsahu a jeho prezentaci;
- poskytování hostování IS a kapacit pro data i aplikace vybraných PFI;
- platforma pro poskytování nadstavbových elektronických služeb souvisejících s podporou digitalizace a eCulture.

Z technického hlediska jsou tyto cíle realizovány dodávkou portálových, aplikačních a databázových serverů, serverů pro zálohování a archivování - HSM, páskových knihoven, diskových polí a síťové infrastruktury. Podmínkou dodržení požadavků a standardů pro poskytování dlouhodobé archivace a ochrany obsahu je vybudování nejméně dvou online úložišť digitálního obsahu a jednoho dark

archive (offline)včetně úpravy vybraných fyzických lokalit pro vybudování datových center. V těchto lokalitách bude vzhledem k požadovaným cílům pořízena dostatečná výpočetní a datová kapacita (sítě, servery, disková pole, pásky ad.) pro nepřetržitý chod podpory digitalizace.

Datové centrum jako takové přispívá ke zvýšení schopnosti různých institucí efektivně spolupracovat s PFI v ČR, EU a v zahraničí, prostřednictvím transferu poznatků a technologií. Projekt řeší vybudování ICT infrastruktury tak, aby byla schopna uchovávat a poskytovat data dlouhodobě a plnit tak požadavek udržitelnosti. Součástí řešení je i zajištění rychlého přístupu prostřednictvím datových sítí a implementace řešení umožňujících efektivní využívání a zpracování uskladněných dat a informačních zdrojů. Vybudování takové infrastruktury vyžaduje nejen propojení s dalšími datovými centry (konsolidace), ale musí respektovat i požadavek na homogenní infrastrukturu, definované standardy a platné legislativní i technické normy.

7.6.8.3.1 Základní výstupy po vybudování centrální hardwarové infrastruktury:

- realizace velkokapacitního sdíleného online úložiště pro zpracovaný digitální obsah určený pro prezentační účely;
- zřízení datových center (jednoho primárního, jednoho záložního a tzv. dark archive) pro provoz centrálního digitálního archivu s dodávkou potřebných technologických a hardwarových celků.

7.6.8.3.2 Dopady projektu

- podpora digitálních archivů pro dlouhodobé uchovávání a ochranu kulturního a vědeckého obsahu, vybudování centrálního úložiště dat s centrálním poskytováním archivních služeb (krátkodobé ale hlavně dlouhodobé archivace a ochrany dat velkého objemu);
- podpora systémové digitalizace;
- podpora agregace, zpracování a zpřístupňování digitálního obsahu a poznatků.

7.6.8.3.3 Předpokládané úrovně elektronické správy

Centrální datové sklady (CDS) budou poskytovat standardní hardwarovou platformu pokrývající potřeby pro naplnění cílů eCulture definovaných v IROP. Dalším důležitým úkolem CDS je poskytnutí infrastrukturní báze pro komplexní prezentaci kulturního dědictví formou portálů (v užším slova smyslu mluvíme o technologických celcích), přičemž údaje budou adresovány do více segmentů jako státní správa, organizace, školy, občan, další rezorty aj. Elektronická zpráva nebo e-governance predstavuje používání informačních a komunikačních technologií pro poskytování vládních služeb, výměnu informačních a komunikačních transakcí, integraci různých samostatných systémů a služeb mezi vládou a zákazníkem (občanem) (G2C), vládou a obchodním sektorem (G2B), vládami navzájem (G2G), stejně jako back-office procesů a interakcí v rámci veřejných rozpočtů, prostřednictvím e-správy. Veřejné služby budou k dispozici občanům pohodlným, efektivním a transparentním způsobem, proto mluvíme v rámci budování CDS a jeho aplikační nástavby (IS Czechiana) o G2C, G2G a G2B funkcionalitách. Interoperabilita a zajištění vazby mezi současným heterogenním prostředím je podmínkou úspěšné realizace projektu CDS. Uvedené řešení vzniká na základě standardů, technických a bezpečnostních norem jakož i doporučení a programů EU a zahraničních zkušeností. Cílový stav bude umožňovat, aby organizace nadále provozovaly vlastní IT infrastrukturu potřebnou pro běh vnitřních agend rezortu.

7.6.8.4 Požadavky na informační technologie CDS

7.6.8.4.1 Primární zohledňovaná kritéria pro IT technologie datových skladů

- Kapacita
- Datové připojení a šířka přenosového pásma
- Identifikace klíčových technologií
- Maximální geografická vzdálenost a topologické uspořádání
- Informační bezpečnost

Kromě plánované kapacity je z hlediska digitalizace, budování datových skladů a provozu podstatná možnost rozšiřování kapacity v čase.

7.6.8.4.2 Kvalitativní a kvantitatívní kriteria na klíčové technologie

Kritérium	***Opis kritéria***
Správa datové infrastruktury (Data Infrastructure Management)	Systém poskytuje nástroje pro správu infrastruktury. Úroveň nástrojů se posuzuje podle dokumentované funkcionality.
Dostupnost dat a kontinuita provozu (Business Continuity)	Požadovaná dostupnost je 7 x 24. Připouštějí se plánované servisní odstávky.
Optimalizace vzdáleného přístupu	Je možný přístup z jiné lokality. Systém dosahuje požadované parametry přenosového pásma a zpoždění.
Datová bezpečnost	Systém zajišťuje ochranu před ztrátou dat.
Migrace dat	Systém poskytuje nástroje pro migraci dat.

7.6.8.4.3 Oblasti poskytované funkcionality a služeb ze strany technologií:

Přepojitelnost	Je zabezpečené připojení k jiným systémům pomocí definovaných komunikačních štandardů a technologii.
Škálovatelnost	Kapacita je rozšiřitelná přidáváním dalších modulů ,resp. zařízení.
Kompatibilita	Systém spolupracuje s jinými systémy (zařízeními) - na bázi technologických standardů.
Výkonnost	Definována počtem vstupně-výstupních operací za jednotku času, případně jinými odvozenými ukazateli.
Funkcionalita (možnosti řešení)	Poskytuje funkcionalitu dle požadavků.
Spolehlivost	Je charakterizována střední dobou mezi poruchami nebo procentuálním vyjádřením podílu bezporuchového provozu.
Měřitelnost (provozních ukazatelů)	Poskytuje pravidelné výkazy o provozních parametrech.
Propustnost	Je charakterizována objemem přenesených nebo zpracovaných dat za jednotku času.
Vykazování (reporting)	Poskytuje pravidelné výkazy o provozních parametrech.
Kapacita	Celková efektívní kapacita.
Deduplikace	Zajišťuje efektivní ukládání dat technologiemi, které brání opakovanému ukládání.
Dostupnost	Požadovaná uživatelská dostupnost např. 7 x 24.
Převzetí činnosti v případě poruchy (zálohovaní provozu)	Schopnost obnovení ,resp. pokračování provozu v plném funkčním rozsahu při výpadku zařízení.
Redundantnost	Dvou- a více násobnost funkčních celků.
Vytěžení	Procentuální vytížení.
Zotavení	Čas potřebný k obnovení provozní schopnosti na určené

	úrovni.
Údržba a udržitelnost	Existence služeb a materiálů na zajištění provozu
Environmentální parametry	Obvykle stanovené technickými a environmentálními normami. Také přímá a nepřímá spotřeba energie.
Prevence	Nástroje na včasné odhalování hrozících poruch.
Replikovatelnost	Rozšiřitelnost opakovaným nasazováním modulů a míra nezávislosti od externích podmínek.
Instalace	Technická kritéria instalace.
Dodržování standardů	Doporučené standardy.
Správa systémů a zařízení	Technické a programové nástroje pro správu systému.

7.6.8.5 Standardy a certifikace

Při realizaci projektu je důležitým aspektem certifikace zařízení a technologií, prohlášení o parametrech (shodě) jednotlivých produkčních komponentů (HW, technologických, kvality aj.), podle mezinárodních standardů. Případná odchylka může mít za následek ohrožení funkcionality řešení, interoperability a úspěšné realizace dalších projektů digitalizace. Při selhání jakékoli části tohoto projektu může být výstupem nehomologizované a necertifikované prostředí nevhodné k nasazení aplikační, systémové vrstvy, což může mít negativní vliv na další digitalizační projekty a procesy (finanční, personální, časové technické aj.). Kritéria pro vybudování CDS budou, vzhledem ke specifickým požadavkům na CDS určena dle norem a standardů The Uptime Institute a certifikace TIERkteré souvisejí s ochranou kulturního dědictví, jako jedinečného a nesrovnatelného obsahu a nepřetržitým provozem CDS i při katastrofě nebo deaktivace vnějšími vlivy - vyšší mocí (požár, záplava, sesuv půdy atd.). Samozřejmostí je i důvěryhodnost takového úložiště pro PFI a instituce, které budou plnit a ukládat do těchto CDS své konvertované (digitalizované) kulturní objekty v elektronické podobě. V případě špatného navržení CDS nebo zničení může dojít k nezvratné ztrátě celého kulturního digitalizovaného a popisného obsahu, který bude vytvářen během příštích let. Minimální životnost CDS je předpokládana na 15 let bez dalších potřebných úprav ve stavebně-technologických částech.

8 Plán strategických projektů

8.1 Zavedení řízení architektury

8.1.1 Cíl projektu

Cílem projektu je zavést v rámci řízení ICT MK řízení architektury jako rozeznatelné, samostatné, systematické a odpovědné činnosti. Řízení architektury bude zavedeno na základě metodického rámce TOGAF 9.1 (nebo novějšího) a postupně implementováno s rozvojem změn v architektuře MK včetně zpětného popisu již realizovaných částí.

Zavedení řízení architektury je rozhodujícím krokem k transparentnímu naplnění cíle „Optimalizace architektury“. Navíc bez jeho realizace lze pouze problematicky zajišťovat efektivní sběr požadavků ze stran uživatelů a promítat je do řešení, které je dlouhodobě udržitelné a účinné a ohrozit tak naplnění cíle „Podpora činnosti MK a řízených organizací“.

8.1.2 Postup

Postup zavedení architektury je činnost procesně metodického charakteru, která má dopad nejenom na řízení ICT ale i celého rezortu. Jeho součástí jsou následující kroky.

- Zpracování výchozí studie možnosti zavedení řízení architektury na základě rámce TOGAF a SDDA.
- Zajištění organizačních změn a nastavení personálních kompetencí pro řízení architektury.
- Výběr, pořízení a nasazení nástrojů pro zpracování architektonických výstupů.
- Vytvoření nezbytné dokumentové základny, standardů, šablon a referenčních architektur.
- Vytipování klíčových dílčích architektur, zahájení jejich řízení v nově zavedeném rámci a postupný přechod k řízení architektury celého rezortu.

Souběžně s výše uvedenými kroky bude probíhat seznamování s novým řízením architektury MK všech subjektů, kterých se dotýká. Pracovníci ICT, garanti věcných útvarů, vedení rezortu, subdodavatelé a řešitelé.

8.1.3 Předpoklady

Zavedení řízení architektury nevyžaduje žádné zvláštní předpoklady s výjimkou souhlasu vedení rezortu z důvodu dopadu změny vytváření architektury předmětné činnosti v součinnosti s odbornými útvary.

Projekt zavedení řízení architektury, tak může být realizován bezodkladně.

8.2 Zavedení integrované digitální platformy k řízení datových zdrojů

8.2.1 Platforma pro ukládání a analýzu velkých objemů dat - Hadoop

8.2.1.1 Cíl projektu

Vybudování velkokapacitních datových úložišť, které následně poskytnou rychlou diskovou platformu s paralelním přístupem umožňující následný aktivní analytický přístup k datům. Jako možné využití této platformy lze uvést aktivní archiv nestrukturovaných dat, projekt webarchivu, ukládání a následná analýza IT a bezpečnostních logů.

8.2.1.2 Přínosy

Hadoop jako nový technologický trend se ukazuje jako velice finančně výhodný a z pohledu následného aktivního přístupu k datům také velmi perspektivní. Inovativním a pro prostředí MK také velmi přínosným může být poskytnutí následné paralelizace úloh pracující s daty.

8.2.2 Softwarově definované úložiště

8.2.2.1 Cíl projektu

Jedná se o využití technologie, která je základním technologickým kamenem pro budování velkoobjemových úložišť, popř. cloudových úložišť a analytických řešení. Softwarově definovaná úložiště mohou také sloužit jako součást řešení v kombinaci s výše uvedenou Hadoop platformou.

Úložiště budovaná na softwarově definovaných technologiích poskytnou potřebné funkcionality, jako jsou diskové a páskové Tiery, kopírovací služby (replikace, klony, snapshoty) a protokoly pro sdílení a zprostředkování dat známé z běžných diskových polí a úložišť.

8.2.2.2 Přínosy

Technologie softwarově definovaného úložiště umožní budování úložišť moderním způsobem a paralelní přístup k uloženým datům. Podstatnou výhodou těchto úložišť je nezávislost na výrobci hardwaru využitého pro samotné uložení dat.

Jako jednu z možných výhod pro MK lze vidět i využití pro garantované ukládání dat a řešení garantovaných důvěryhodných archivů.

8.2.3 Analýza obsahu, umožnění badatelského přístupu

8.2.3.1 Cíl projektu

Toto řešení předpokládá provedení jazykové analýzy obsahu dat ukládaných v datových úložištích a dlouhodobých archivech. Následný uživatelský přístup k takto zanalyzovaným datům poskytne plnohodnotný „badatelský“ přístup a poskytne hlubší možnosti práce s daty kulturních bohatství.

Jako zdroj pro analýzu obsahu lze považovat -jakákoli data v textové podobě, například OCR výstupy skenů knih nebo obsahy kulturních a vědeckých studií. Primárně se tedy bude jednat o analýzu nestrukturovaných dat textů a k nim poskytnutých metadat.

8.2.3.2 Přínosy

Řešení analýzy obsahu umožní hluboké pochopení obsahu uložených dat. Z pohledu badatelského přístupu toto řešení nabízí široké uplatnění a lze jej využít jako vstup do mnoha aplikací a systému primárně zaměřených na poskytnutí dat a poskytnutí analytického prostředí.

8.2.4 Vyhledávání, zpřístupnění a vizualizace dat

8.2.4.1 Cíl projektu

Cílem této oblasti je zpřístupnění dat uložených v archivech a jiných datových úložištích pomocí rychlého vyhledávače a následné prezentace výstupů uživateli formou grafického vizualizační prostředí.

Primárně se bude jednat o vizualizaci proindexovaných strukturovaných a nestrukturovaných dat ve spojení s náhledy na originály objektů (dokumenty, skeny, atd …).

Toto řešení lze kombinovat ve spojení s výše uvedenou Hadoop platformou a také s prostředím pro analýzu obsahu. Řešení vyhledávání a zpřístupnění dat si bere za cíl primárně data zpřístupnit uživatelům v rychlé a přehledné podobě. Vedle toho analýza obsahu uvedena výše primárně poskytuje analytické a badatelské prostředí pro hlubší práce s obsaženými daty.

8.2.4.2 Přínosy

Tento přístup k indexování a zpřístupnění dat, lze považovat za základ budování aktivního archivu. Z uživatelského pohledu je možné velice intuitivně prohledávat obsah a řešení poskytne vizualizační sady pro následné procházení obsahem.

8.3 Zavedení Jednotného systému řízení bezpečnosti

8.3.1 Cíl projektu

Primárním cílem projektu je vytvoření aktualizované bezpečnostní strategie a bezpečnostní politiky, zejména v souladu s moderními způsoby poskytování služeb ICT a nasazováním moderních technologií (například mobilní služby).

Následným cílem je zavedení procesu revize bezpečnosti jako systematického procesu prováděného opakovaně za účelem aktualizace bezpečnostní předpisové základy v důsledku změn okolí a nových požadavků.

Pravidelná revize bezpečnostní předpisové základny je klíčovou činností vyžadovanou legislativou ČR v oblasti bezpečnosti a je tak nutnou podmínkou naplnění cíle „Soulad s legislativou“. Navíc je zásadním vstupem pro „Vymezení kompetencí“ z pohledu vyjasnění odpovědnosti za správu a tím i ochranu zpracovávaných informací.

8.3.2 Postup

Kroky, které je nutné realizovat pro revizi bezpečnostní předpisové základní, jsou následující.

- Provést revizi aktuální bezpečnostní strategie s ohledem na současné požadavky a zapracovat případné modifikace.
- Sestavit revidovaný seznam informací a dat, která mají být chráněna (tzv. aktiva).
- Sestavit revidovaný seznam aktuálních rizik, která ohrožují informace a data podléhající ochraně.
- Provést kontrolu jak je dodržována aktuální bezpečnostní politika a zkontrolovat, že aktuální bezpečnostní politika reaguje na všechna aktuální rizika. Kontrolu provést pomocí simulovaných útoků.
- Vyhodnotit, zda existují rizika, na která bezpečnostní politika nereaguje a je tak ohrožena důvěrnost, integrita a dostupnost dat.
- Doplnit aktuální bezpečnostní politiku o chybějící hrozby a reakci na ně,
- Provést implementaci doplněné části bezpečnostní politiky do organizace.
- Provést test implementované bezpečnostní politiky pomocí simulovaných útoků.
- Provést případná nápravná opatření plynoucí z výsledků simulovaných útoků.

8.3.3 Předpoklady

Revize bezpečnostní předpisové základny nevyžaduje žádné zvláštní předpoklady. Může tak být zahájena bezodkladně.

8.4 Formalizace řízení kvality

8.4.1 Cíl projektu

Cílem projektu formalizace řízení kvality je zavedení formalizovaného procesu řízení kvality jako související aktivity k projektovému řízení včetně revitalizace procesu oponentního řízení.

Formalizace řízení kvality je nezbytným krokem k dlouhodobě efektivnímu poskytování služeb ICT a nelze tak bez ní naplňovat cíle „Optimalizace nákladů“, neboť není možno sledovat, zdali samotná optimalizace nemá dopad na kvalitu poskytovaných služeb. V konečném důsledku mohou být vzniklé úspory v oblasti ICT přenášeny do nákladů jiných částí rezortu, například zvýšením pracnosti na straně uživatelů.

8.4.2 Postup

Zavedení formalizovaného řízení kvality bude probíhat v následujících krocích.

- Zpracování hodnotící studie způsobu řízení kvality činností prováděných útvary ICT.
- Stanovení organizačního a personálního zajištění řízení kvality.

- Zavedení metodické základny, zejména klasifikace projektů, procesů a služeb, stanovení měřitelných parametrů (metrik), stanovení způsobu hodnocení.
- Zavedení opakovaného procesu hodnocení kvality a jeho začlenění do řízení změn a požadavků v důsledků sjednání přípravné nápravy při nevyhovujícím hodnocení.
- Revitalizace procesu oponentního řízení vycházející z dosavadní implementace.

8.4.3 Předpoklady

Zahájení zavedení formalizovaného řízení kvality nevyžaduje žádné zvláštní předpoklady. Může tak být zahájeno bezodkladně.

8.5 Revize rezortních standardů

8.5.1 Cíl projektu

Cílem revize rezortních standardů je provést konsolidaci a revizi všech standardů v oblasti ICT přes všechny rezortní organizace. Konsolidované standardy revidovat a kategorizovat do následujících skupin standardů

- Společných – standardy, které budou využívány napříč všemi organizacemi (například standardy na dokumentaci softwarového díla).
- Specifických – standardy specifické pro danou organizaci, které nemusí být dodržovány ostatními organizacemi (například standardy v oblasti koncových stanic).

Následně zajistit vyžadování těchto standardů od všech řešitelů a dodavatelů.

Posledním cílem je zavedení procesu pravidelné revize standardů a řízení jejich změn.

Projekt revize rezortních standardů je úvodním krokem k naplnění cíle „Standardizace“ na úrovni rezortu MK.

8.5.2 Postup

Postup revize rezortních standardů bude probíhat v posloupnosti následujících kroků.

- Konsolidace (sběr) standardů od všech rezortních organizací.
- Kategorizace standardů do skupin společných a specifických standardů.
- Revize společných standardů za účelem jejich aplikovatelnosti pro všechny organizace.
- Zavedení standardů a poskytnutí zainteresovaným stranám (útvary ICT, řešitelé, dodavatelé, popřípadě veřejnost).
- Vymezení a zahájení procesu aktualizace (revize) standardů na pravidelné bázi.

8.5.3 Předpoklady

Pro úspěšnou realizaci revize rezortních standardů je nezbytné zajistit součinnost všech rezortních organizací, zejména poskytnutí aktuálně existujících a využívaných standardů.

8.6 Implementace metodického rámce řízení služeb

8.6.1 Cíl projektu

Cílem projektu je procesně formalizovat řízení služeb ICT (ITSM – IT Service Management) v souladu s rámce řízení služeb ITIL. Následně zajistit poskytování služeb výhradně v implementovaném rámci řízení.

8.6.2 Postup

Zavedení metodického rámce řízení služeb je kritická činnost zejména z pohledu provozních služeb. Rámec bude zaváděn v následujících krocích.

- Zpracování výchozí studie zavedení řízení služeb v rámci ITIL zaměřené na výběr a vhodnost implementovaných procesů v prostředí MK.
- Zajištění případných organizačních změn, nastavení personálních kompetencí a proškolení odpovědných osob.
- Výběr, pořízení a nasazení nástrojů pro podporu řízení služeb.
- Vytvoření nezbytné dokumentové základny, procesů, postupů a standardů.
- Vytipování konkrétních oblastí služeb, zahájení jejich řízení v nově zavedeném rámci a postupný přechod k řízení služeb celého úřadu v rámci ITIL.

Souběžně s výše uvedenými kroky bude probíhat seznamování s novým řízením služeb všech subjektů, kterých se dotýká.

Implementace metodického rámce řízení služeb je nezbytná s ohledem na efektivní výkon služeb ICT a je tak nutným předpokladem naplnění cílů „Podpora činností MK a řízených organizací“ a „Optimalizace nákladů“.

8.6.3 Předpoklady

Implementace metodického rámce řízení služeb nevyžaduje žádné zvláštní předpoklady. Může tak být zahájena bezodkladně.

8.7 Centralizované zadávání v oblasti infrastruktury a technologií

8.7.1 Cíl projektu

Cílem projektu je zjištění možností a přínosů centralizovaného zadávání v oblasti infrastruktury a technologií za účelem dosažení stejných obchodních podmínek pro všechny rezortní organizace.

Centralizovanén zadávání vychází z faktu, že mnoho prvků a technologií pořizovaných v rámci naplnění služeb v oblasti ICT má stejný či podobný charakter. Takové prvky a technologie mohou být pořizovány společně zajišťujícím dosažení stejných, nebo výhodnějších podmínek než při pořizování odděleném.

8.7.2 Postup

V rámci zajištění centralizovaného zadávání je nutné mimo jiné provedení dále uvedených kroků a činností.

- Identifikovat jednotlivé služby poskytované v oblasti ICT celého rezortu.
- Identifikovat parametry kvality jednotlivých služeb (SLA) a typy služeb.
- Porovnat úroveň SLA srovnatelných služeb a typů služeb a jejich ceny.
- Pro každou službu nastavit požadované parametry dle kritičnosti služby.
- Identifikovat smlouvy, kde existuje potřeba pro vyjednání vyšší kvality služeb nebo prostor pro snížení ceny za poskytované služby.
- Ve všech nových výběrových řízeních na zajištění ICT služeb standardně zahrnovat parametry SLA jednotné pro celý rezort.

Centralizované zadávání je klíčovým předpokladem dlouhodobé optimalizace nákladů na rozvoj a provoz služeb ICT a je tak nezbytné pro dlouhodobé naplňování cíle „Optimalizace nákladů“.

8.7.3 Předpoklady

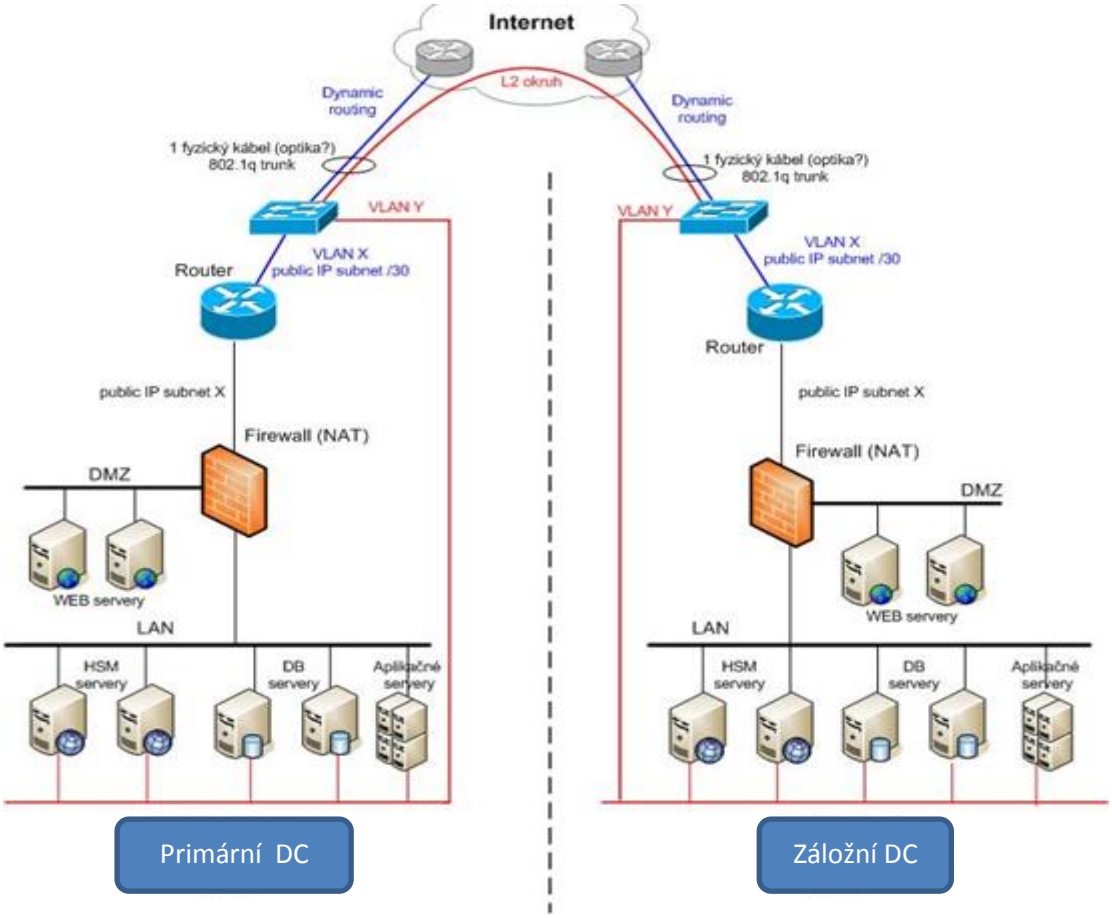
Pro realizaci centralizovaného zadávání služeb je nezbytné zajistiti koordinaci ICT rezortních organizací, zejména pak popisy čerpaných služeb, jejich kvalitativní parametry a finanční náklady.

8.8 Modernizace datových center

8.8.1 Cíle

Základní podmínkou a cílem realizace/revitalizace datového centra je jeho technologická a aplikační neutralita. Z hardwarového hlediska bude řešení postavené na takových zařízeních, které jsou vzájemně propojitelné, rychle servisovatelné, obnovitelné a škálovatelné. Hardwarová architektura je vytvořena na základě potřeb rezortu MK, přihlíží se však na to, aby byla navržena tak, aby

poskytovala služby v požadované kvalitě v heterogenním prostředí, nezávisle od fyzického hardware s vysokou mírou virtualizace, přičemž konkrétní rámcová vysoko-úrovňová architektura bude do detailů specifikována v projektové dokumentaci podle funkčních komponentů, na které se budou upravovat požadavky podle vývoje aplikace, která bude nasazena na poskytnutém prostředí. Komponenty (moduly) budou konkretizovány také na úrovni projektů. Každý navrhovaný komponent je technologickým celkem systému, který se skládá z požadované technologie a základní rámcová funkční specifikace a rámcová technická specifikace bude popsána na úrovni projektů.



Obrázek 4 Základní logická architektura zapojení ICT v DC

8.9 Privátní Cloud

8.9.1 Cíl projektu

V závislosti na rozhodnutí o modernizaci/revitalizaci vlastních datových center je vhodné pořízení potřebné výpočetní kapacity ve formě vybudování řešení "Privátního Cloudu". Z uživatelského pohledu se bude jednat o jednotnou platformu poskytující služby „infrastruktury" (Infrastructure as a Service) a „Platformy" (Platform as a Service). Privátní cloudové řešení poskytne virtualizované prostředky IT s plně automatizovaným procesem vytváření a konfigurace těchto virtualizovaných zdrojů. Jako diskové úložiště pro interní cloud lze technologicky efektivně využít výše uvedené softwarově definované úložiště.

Cloud bude budován jak pro interní potřeby MK, tak pro potřeby vnějších a podřízených složek.

8.9.2 Přínosy

Privátní cloudová řešení umožňují zjednodušit a zlevnit interní procesy v IT prostředí a poskytují příjemnější a zákaznicky orientované služby zákazníkům IT. Z technologického hlediska jsou nezávislá na výrobci využitých hardwarových prostředků.

Hlavním přínosem je podstatné zlepšení dynamiky v poskytování ICT služeb pro své uživatele, což můžou být jak interní potřeby rezortu, tak i podřízených nebo vnějších složek. Podstatně se tím zvýší rychlost zavádění nových služeb v oboru ICT a zlepší přehled a efektivita. Ve finálním důsledku se sníží celkové náklady na ICT infrastrukturu a zvýší možnosti a kvalita prostředí.

8.10 Modernizace ekosystému nástrojů pro řízení kvality služeb

8.10.1 Cíl projektu

Cílem projektu je zajistit modernizaci a případné doplnění nástrojů používaných pro poskytování informací sloužících pro řízení kvality. Jedná se zejména o aplikace poskytující charakteristiky a metriky chování služeb ICT a chování informačních systémů a technologií, které služby využívají.

Bez efektivních nástrojů pro řízení kvality služeb nelze v konečném důsledku úspěšně realizovat projekt „Formalizace řízení kvality“, neboť je nezbytné zajistit důvěryhodné měření údajů, na základě kterých je kvalita hodnocena.

8.10.2 Postup

Vlastní modernizace nástrojů pro řízení kvality služeb bude probíhat v následujících krocích.

- Zpracování studie charakterizující současný stav – popis používaných nástrojů, sledované ukazatele a jejich zhodnocení pro využití v rámci řízení kvality.
- Zpracování návrhu modernizace a doplnění nástrojů s ohledem na výstupy a požadavky projektu formalizace řízení kvality.
- Zajištění dílčích projektů modernizace včetně případných výběrových řízení.
- Metodické a procesní zavedení využívání nástrojů v kontextu řízení kvality a rámce řízení služeb.

8.10.3 Předpoklady

Vlastní zahájení projektu je nutno realizovat v koordinaci s projektem „Formalizace řízení kvality,“ a to zejména v oblasti vymezení a stanovení způsobu měření ukazatelů, které budou v rámci řízení kvality využívány.

8.11 Projekty v oblasti bezpečnosti

8.11.1 Vytvoření bezpečnostní dokumentace rezortu MK

Na základě zákonných požadavků (zejména se jedná o zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, ZoKB), výsledků analýzy uvedené v kapitole 6.5 a dalších vstupů, je nutné zpracovat komplexní bezpečnostní dokumentaci:

- Rezortní bezpečnostní politika a navazující dokumenty.
- Bezpečnostní politiky složek rezortu MK s navazujícími dokumenty. V těch složkách, kde dokumentace existuje a vyhovuje současným požadavkům, bude, pokud se takováto potřeba vyskytne, s minimálním zásahem přizpůsobena rezortní bezpečnostní politice.
- Dokument popisující informační aktiva a jejich hodnotu.
- Katalog aplikací s definování jejich vlastníků a správců.
- Registr rizik a hrozeb jako podklad pro jejich efektivní řízení včetně analýzy jejich vzájemných vazeb a vazeb na ostatní rizika.

8.11.2 Zavedení systému řízení informační bezpečnosti

bude zaveden systém řízení informační bezpečnosti jako nedílná součást jednotného systému řízení bezpečnosti rezortu.

- Budou zavedeny bezpečnostní politiky a bude zajištěna jejich pravidelná aktualizace.
- Budou definovány a průběžně aktualizovány role a zodpovědnosti.
- Budou definovány procesy a průběžně kontrolována jejich funkčnost.
- Bude zaveden systém pro efektivní řízení a zvládání rizik.

8.11.3 Řízení dodavatelů

Bude zaveden účinný systém pro kontrolu kvality poskytovaných služeb ze strany externích dodavatelů. Kontrolováno bude nejen formální plnění smluvních závazků ale i ostatní parametry poskytovaných služeb.

- Smlouvy s budoucími dodavateli budou nastaveny s důrazem na řiditelnou a kontrolovatelnou kvalitu poskytovaných služeb.
- Bude zaveden systém pro efektivní monitoring technické kvality služeb včetně splnění požadavků na monitorující personál.
- Bude zaveden systém na vkládání důkazů o vykonaných službách ověřovaným způsobem pomocí zabezpečené aplikace.

8.11.4 Řízení životního cyklu prvků systému ICT

Bude zavedeno řízení životního cyklu všech prvků ICT MK od pořízení až po jejich bezpečnou likvidaci bez nebezpečí úniku informací v nich uložených. To vyžaduje:

- Definování požadavků na bezpečnost prvků a jejich ICT.
- Zavedení a údržba efektivní evidence prvků systému s vysokou vypovídací schopností.
- Zavedení a údržba systému pro řízení bezpečné konfigurace prvků.
- Zavedení a údržba systému pro efektivní údržbu prvků z hlediska jejich funkčnosti včetně přehledu o poruchách a opravách a jejich ekonomičnosti.
- Zavedení a údržba systému pro řízení update software/firmware prvků.
- Zavedení a údržba systému pro prokazatelně bezpečnou likvidaci prvků systémů.
- Testování prvků systému z hlediska bezpečnosti.

8.11.5 Řízení personální bezpečnosti

Vybudování systému pro řízení personální bezpečnosti vytvoří z hlediska personálního bezpečné prostředí, pro to je důležité:

- Provést personální audit zaměstnanců MK i zaměstnanců externích dodavatelů s ohledem na bezpečnostní požadavky na jejich funkce, s ohledem na aktiva, ke kterým přistupují a s ohledem na jejich zodpovědnosti.
- Zavedení a údržba systému pro zajištění bezpečných personálních změn.
- Zavedení a údržba systému pro vzdělávání a personálu zodpovědného za funkčnost všech částí bezpečnosti.
- Zvyšování bezpečnostního povědomí laického personálu.

8.11.6 Zvládání incidentů, sdílení informací, znalostní management

Pro zajištění IT bezpečnosti rezortu je nezbytné mít schopnost detekovat a zvládat bezpečnostní incidenty a také mít schopnost o nich informovat. Proto je nutné:

- Vybudovat a udržovat schopnost řešit incidenty kybernetické a informační bezpečnosti zřízením rezortního dohledového centra stavu kybernetické a informační bezpečnosti – tzv. rezortní CSIRT (Computer Security Incident Response Team) .
- Zavést a udržovat systém pro průběžné hodnocení a řízení zranitelností a jejich evidenci v systému pro řízení znalostí.
- Zavést a udržovat systém pro zvládání bezpečnostních incidentů.
- Zavést a udržovat systém pro spolupráci s autoritami v oblasti kybernetické bezpečnost (NBÚ- Národní Bezpečnostní Úřad, NCKB - Národní Centrum Kybernetické Bezpečnosti).
- Zavést a udržovat systém pro řízení a sdílení znalostí o zranitelnostech a hrozbách v rezortu MK i na národní úrovni.

8.11.7 Audity funkčnosti

Bezpečnostní parametry systému ICT musí být pod stálou a v některých aspektech pravidelnou kontrolou. Proto je nutné:

- Zavedení systému pro pravidelný audit bezpečnosti systému a jeho prvků, a to včetně hloubkových vnitřních i vnějších penetračních testů.
- Vybudování systému pro monitorování bezpečnosti systému ICT.
- Vybudování systému pro ochranu a vyhodnocování auditních informací .

8.11.8 Zajištění kontinuity

Zajištění kontinuity provozu respektive jeho obnovení po havárii je životně důležité pro plnění úkolů, které jsou na rezort MK plní. Je nezbytné:

- Vybudování a údržba systému pro zajištění kontinuity funkčnosti po havárii.

8.11.9 Fyzická bezpečnost prvků systému

Důraz bude kladen na fyzickou bezpečnost prvků zajišťujících bezpečnost systému ICT MK.

- Vybudování a údržba systému pro fyzickou bezpečnost prvků systému – budovy, komponenty, systémy, úložiště apod.
- Zavedení a údržba systému pro kontrolu zajištění fyzické bezpečnosti prvků umístěných mimo objekty rezortu.
- Zavedení a údržba systému pro kontrolu přístupu k prvkům systému ze strany vlastních zaměstnanců i personálu externích dodavatelů služeb.

8.11.10 Bezpečnost informačních systémů – aplikační bezpečnost, klasifikace informací, DLP systémy atd.

Bezpečnost informačních systému, informací do nich vkládaných, v nich zpracovávaných a v nich ukládaných, je stěžejním parametrem pro věrohodnost informací využívaných při tvorbě stěžejních rozhodnutí v rezortu MK. Informace je nutno chránit proti úniku, kompromitaci, znevěrohodnění a je nutno zajistit jejich kontrolovanou dostupnost. Proto je nutné:

- Zavedení a údržba systému pro řízení přístupu k informacím na všech úrovních.
- Zavedení a údržba systému pro klasifikaci informací.
- Zavedení a údržba systému pro kontrolu nad pohybem informací.
- Zavedení procesů bezpečného používání a výměny všech médií.

8.11.11 Bezpečnost infrastruktury

Bezpečná infrastruktura je jedním z pilířů celkové kybernetické a informační bezpečnosti. I s ohledem na výše uvedené je nutno:

- Klást důraz na bezpečnou architekturu budovaných počítačových sítí v plné šíři od datových center až po koncové stanice nebo mobilní zařízení firemní i soukromá (BYOD – Bring Your Own Device).
- Trvale hodnotit trendy a aplikovat nové poznatky do systému pro zajištění bezpečnosti infrastruktury.
- Zajistit bezpečné propojení mezi jednotlivými sítěmi v systému ICT MK.

8.11.12 Postup realizace

Výše uvedené činnosti, které vedou k naplnění hlavního cíle strategie IT bezpečnosti, budou realizovány ve dvou paralelních větvích.

V první větvi budou aplikována opatření, která lze aplikovat v krátkodobém horizontu, protože jsou v rezortu MK k dispozici technické, systémové i personální zdroje k zavedení bezpečnostních opatření cestou změn přístupu. Realizaci úkolů z toho plynoucích lze zahájit prakticky okamžitě ve spolupráci s externími dodavateli služeb v oblasti bezpečnosti.

V druhé paralelní větvi bude zahájen a realizován projekt zavedení jednotného systému řízení bezpečnosti rezortu MK, který se skládá z analýzy a návrhu opatření, jejich implementace a závěrečné testování funkčnosti implementovaných opatření.

8.12 Pořízení informačního systému RCNS

Název IS	Rejstřík církví a náboženských společností
Zkratka názvu	IS RCNS
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor církví
Způsob pořízení	Dodavatelsky
Právní předpis zakotvující IS	zákon č. 3/2002 Sb., vyhláška č. 232/2002 Sb.
Důvod vzniku IS	Náhrada nevyhovujícího IS
Předpokládaný začátek realizace	Květen 2015 (start analýzy)
Předpokládaný konec realizace	Prosinec 2016
Plánované náklady pořízení	10 mil. Kč, z toho 6 mil. na část DDÚ (navýšení odpovídá upravené analýze a zohlednění kurzového posunu)
Plánované náklady na roční provoz	1 mil. Kč (v předpokládaném poměru 60:40 ve prospěch DDÚ)

Tabulka 12: Základní údaje informačního systému

8.12.1 Cíl projektu

Jedná se o náhradu informačního systému církví a náboženských společností (IS CNS).

Důvodem náhrady je celková zastaralost architektury řešení IS CNS, která se projevuje zejména v oblasti udržování a vytváření vazeb na základní registry a vyvolává na straně MK nepřiměřeně vysoké finanční náklady.

Dalším důvodem k pořízení nového systému je zajištění požadavku na archivaci podkladů vedených v systému po dobu 50 let. Stávající systém toto neumožňuje a podklady jsou archivovány pouze v papírové podobě. Dlouhodobé datové úložiště bude určeno pro potřeby využití všech útvarů ministerstva.

Vlastní funkční charakteristika nově budovaného IS je definována v legislativě.

Zpracovávaná data

IS RCNS bude zpracovávat následující data:

- Údaje o registrovaných církvích a náboženských společnostech a jejich svazech.
- Údaje o evidovaných právnických osobách dle zákona č. 3/2002Sb.

Zajišťované služby

IS RCNS zajišťuje následující služby:

- Webové služby spojené se zveřejňováním povinných informací.
- Vedení rejstříku registrovaných církví a náboženských společností.
- Vedení rejstříku svazů církví a náboženských společností.
- Vedení rejstříku evidovaných právnických osob dle zákona č. 3/2002 Sb.
- Vazba na základní registr osob.
- Vazba na základní registr územní identifikace a adres.
- Vydávání výpisů z IS RCNS.
- Zajištění odpovídající dlouhodobé archivace.
- Propojení na spisovou službu GINIS.

Technické a programové prostředky

HW prostředky budou použity standardní v rámci provozního prostředí MK, kterým je sdílené serverové prostředí na bázi virtuálních serverů.

Systémové SW prostředí (operační systémy a databázové systémy) je k dispozici standardní na bázi platformy společnosti Microsoft, v případě, že dodavatel bude požadovat jinou platformu, musí být tato součástí nabídky dodavatele.

8.12.2 Stávající stav

Zajištění agendy vedení rejstříku církví a náboženských společností je realizováno prostřednictvím systému IS CNS, který po stránce souladu s legislativou a funkčních požadavků odboru církví v době přípravy této koncepce vyhovuje.

Hlavní nedostatky stávajícího řešení (a důvody k vytvoření nového IS) jsou:

- Architektura systému odpovídá době vzniku, systém od svého nasazení nebyl optimalizován v rámci aktuálních trendů ve vývoji IS.
- Není řešena archivaci elektronických dokumentů v požadované délce (50 let).
- Problematické (nákladné) udržování rozhraní na základní registry.
- Problematické (nákladné) provádění úprav v šablonách vydávaných výpisů.
- Nejednoznačně definované služby podpory a rozvoje systému ve smluvních vztazích.

8.12.3 Postup

Způsob realizace

Předpokládá se vypsání otevřené soutěže na dodavatele IS RCNS v souladu s příslušným zákonem.

Finanční specifikace

Uvedené finanční specifikace vychází z kvalifikovaného odhadu pracovníků OIT a orientačního průzkumu na trhu ICT pro přípravu podobného řešení.

Předpokládá se financování ze státního rozpočtu.

Časové specifikace

Uvedené časové specifikace vycházejí ze lhůt výběrového řízení daných zákonem o veřejných zakázkách a kvalifikovaného odhadu pracovníků OIT pro nasazení/vytvoření obdobného řešení.

Další okolnosti

Byla zvažována též možnost úpravy stávajícího IS CNS tak, aby vyhovoval kladeným požadavkům, nicméně finanční náročnost těchto úprav, včetně vyřešení dlouhodobé archivace, odpovídala ceně nového SW řešení.

Na základě výše uvedeného bylo rozhodnuto o vytvoření nového řešení.

8.13 Pořízení systému JEGIS

Název IS	Jednotný evidenční a grantový informační systém MK
Zkratka názvu	JEGIS
Útvar zajišťující správu IS	Odbor informačních technologií
Gesčně odpovědný útvar	Odbor médií a audiovize Odbor památkové péče Odbor umění, literatury a knihoven Odbor mezinárodních vztahů Odbor ochrany movitého kulturního dědictví, muzeí a galerií Odbor regionální a národnostní kultury Odbor církví (z časových důvodů bude implementace provedena samostatně a zde bude řešena integrace agend)
Způsob pořízení	Dodavatelsky
Právní předpis zakotvující IS	zákon č. 218/2000 Sb a prováděcí vyhlášky 52/2008 Sb. zákon č. 20/1987 Sb. zákon č. 46/2000 Sb.
Důvod vzniku IS	Náhrada nevyhovujícího řešení při zajišťování zákonné povinnosti
Předpokládaný začátek realizace	Červen 2015 (start analýzy)
Předpokládaný konec realizace	Červen 2016 až červen 2017 (dle charakteru a rozsahu projektu)
Plánované náklady pořízení	až 35 mil. Kč (dle charakteru a rozsahu projektu)
Plánované náklady na roční provoz	Cca 500 tis. Kč

Tabulka 13: Základní údaje informačního systému

8.13.1 Cíl projektu

Jednotný evidenční a grantový informační systém MK pro elektronickou správu žádostí o evidenci, registraci a granty/dotace.

Zpracovávaná data:

- Údaje o evidovaných knihovnách.
- Údaje o osobách s povolením k restaurování.
- Údaje o periodickém tisku.

- Údaje o projektech u výběrových dotačních řízeních (dále též nazyváno jako „grantových řízení“) v celé agendě MK.

Zajišťované služby

- Jednotný systém legislativou dané evidence kulturních subjektů napříč odbory MK.
- Přehledná evidenci, reportování, analýzy a evaluace podpořených projektů u grantových řízení v rámci celé agendy MK.
- Jednotné, přístupné a neduplicitní výstupy pro strategické plánování, auditing, zpřístupňování a statistické údaje.
- Úspora finančních prostředků MK.
- Přesné zmapování velké části procesních agend MK.

Při specifikaci funkcionality IS JEGIS bude zohledněna funkcionalita IS VaVaI (informační systém výzkumu, experimentálního vývoje a inovací), aby nedošlo k duplikaci údajů a zvýšení administrativní zátěže zejména na straně odboru OVV.

Technické a programové prostředky

HW prostředky budou použity standardní v rámci provozního prostředí MK, kterým je sdílené serverové prostředí na bázi virtuálních serverů.

Systémové SW prostředí (operační systémy a databázové systémy) je k dispozici standardní na bázi platformy společnosti Microsoft, v případě, že dodavatel bude požadovat jinou platformu, musí být tato součástí nabídky dodavatele.

Bude zajištěna integrace s informačním systémem DOTINFO, který je ve správě Ministerstva financí.

8.13.2 Stávající stav

Legislativou je MK uloženo vedení několika různých evidencí, které mají charakter ISVS. V těchto systémech je často veden velice omezený počet záznamů (řádově tisíce), případně dochází ke změně v datech sporadicky. Tato zákonná povinnost je v současné době řešena buď samostatnými agendovými informačními systémy (např. u odboru církví), nebo je prováděna pomocí emailu popř. manuálně v papírové podobě a s následným převodem inform-ací do elektronické podoby (většinou excelové tabulky).

Stávající stav byl ovlivněn:

- neexistencí systému základních registrů v době vzniku evidencí;
- nedostatkem finančních prostředků na vytvoření evidencí;
- neznalost praxe v ICT při vytváření evidencí;
- použití aktuálně dostupných technických možností MK.

Důsledkem výše uvedeného je, že:

- neexistující dokumentace k evidencím;
- neexistence smluvně garantované podpory od dodavatele evidence;
- evidence často nahrazeny tabulkou ve formátu MS Excel, která je po aktualizaci nahrávána na web MK;
- neexistence propojení na základní registry a kontroly kvality dat v evidencích;
- pokud jsou již data v evidencích kontrolována (verifikována) proti údajům v základních registrech, děje se tak prostřednictvím přístupu zaměstnance MK do těchto registrů a změna v registrech se nepromítne do evidencí.

S ohledem na výše uvedené není možné stávající řešení evidencí, byť naplňují znaky ISVS a jsou evidovány v IS o ISVS, považovat za informační systémy veřejné správy, v některých případech dokonce není možné užívané řešení považovat ani za informační systém.

Totéž platí pro grantové/dotační tituly jednotlivých odborů MK.

Mimo jiné chybí:

- jednoduše dohledatelný celkový přehled o evidovaných subjektech napříč odbory MK;
- přehledné reportování, analýzy a evaluace podpořených projektů u grantových řízení v rámci celé agendy MK;
- možnost žadatele podat žádost pomocí webového portálu;
- propojení se spisovou službou a ekonomickým systémem MK;
- propojení se základními registry;
- propojení s Centrálním registrem dotací MF;
- propojení se statistickými a jinými požadovanými daty PO a kulturních organizací ve vztahu k MK, NIPOS, ČSÚ ad.

8.13.3 Postup

Způsob realizace

Předpokládá se vypsání otevřené soutěže na dodavatele řešení v souladu s příslušným zákonem. Předpokládaná doba realizace 18 – 30 měsíců dle charakteru a rozsahu projektu.

Finanční specifikace

Uvedené finanční specifikace vychází z kvalifikovaného odhadu pracovníků OIT a orientačního průzkumu na trhu ICT pro přípravu podobného řešení.

Rozpočet výše JEGIS závisí na jeho šíři a charakteru agend, které bude řešit. Přesná částka tedy závisí na definovaných požadavcích MK.

Předpokládá se financování ze státního rozpočtu.

Časové specifikace

Uvedené časové specifikace vycházejí ze lhůt výběrového řízení daných zákonem o veřejných zakázkách, kvalifikovaného odhadu pracovníků OIT pro nasazení/vytvoření obdobného řešení a celkové rozsahu a šíři pokrývané agendy.

Další okolnosti

Základem pro snížení administrativní zátěže je elektronizace systému – převedení dosud manuálně prováděných činností do prostředí JEGIS.

Takové řešení zjednoduší implementaci všech požadavků odborných útvarů ministerstva kultury na jednotný modulární informační systém, sníží celkové finanční dopady na vývoj a implementaci parciálních evidenčních či dotačních informačních systémů a výrazně zefektivní chod MK.

Výhody:

- větší efektivita správy evidencí a dotačních titulů;
- jednotná správa systému;
- jednotné, přístupné a neduplicitní výstupy pro strategické plánování, auditing, zpřístupňování a statistické údaje;
- transparentnost poskytování grantů/dotací;
- výrazná úspora finančních prostředků MK;
- přesné zmapování velké části procesních agend MK;
- možnost finanční úspory při pořízení systému, a to díky využití a úpravě stávajících systémů v rezortu či veřejné sféry obecně (Státní fond kinematografie, Česká knihovna, TAČR, MMR, CEDR ad.);
- nezanedbatelný pozitivní dopad na mediální obraz MK.

8.14 Pořízení informačního systému právních informací pro organizace rezortu

8.14.1 Cíl

Vybudovat systém distribuce právních informací relevantních problematice Ministerstva kultury, kde právními informacemi jsou myšleny

- externí zdroje
    - právní předpisy z vybraných oblastí vyhlášené ve Sbírce zákonů ,resp. Sbírce mezinárodních smluv ve všech zněních za celou jejich historii společně se všemi souvisejícími informacemi (např. novelizující předpisy)
    - informace o průběhu legislativního procesu změn těchto předpisů ze zdrojů
    - soudní rozhodnutí vyšších soudů relevantní k výše uvedeným předpisům
- interní zdroje MK
    - dokumenty rezortních předpisů (nevyhlášené v Sb.)
    - ostatní právní dokumenty podle uvážení zadavatele

8.14.2 Požadavky

8.14.2.1 Základní funkce

- vyhledání podle názvu a čísla dokumentu
- vyhledávání v plných textech dokumentů
    - je-li výraz nelezen v názvu dokumentu, názvu jeho částí, nebo klíčových slovech dokumentu, bude v seznamu výsledků zařazen s vyšší váhou
- možnost vyhledávat informace ke zvolenému datu (v minulosti nebo budoucnosti)
- fazetové filtrování seznamu výsledků podle předem určených kritérií
- zobrazení detailů dokumentů včetně vazeb a metadat
- nástroje pro tvorbu dokumentů interních zdrojů, případně vložení dokumentů připravených jinak do PIK, popis metadaty a vzájemné provázání (týmový Content Management System)

8.14.2.2 Osobní účet uživatele a personalizace

- uživatelé s příslušným oprávněním budou mít IS k dispozici prostřednictvím uživatelsky přátelské aplikace v prostředí webového prohlížeče
- IS bude svébytným a samostatným systémem, jeho rozhraní bude vytvořeno na míru zobrazení a používání výše uvedených zdrojů
- IS bude součástí intranetu zadavatele
- každý uživatel bude mít svůj osobní účet
    - podmínkou nutnou je „jediné přihlášení“
    - uživatel, který bude přihlášen k intranetu v konkrétní roli, bude mít oprávnění relevantní k této roli i v IS
- na osobní účet budou navázány následující základní možnosti personalizace
    - tvorba rešerší, tedy pojmenovaných skupin odkazů do IS
        - odkazy budou mířit na jednotlivé dokumenty, resp. u strukturovaných právních předpisů na jednotlivá ustanovení (možno jen u předpisů Sbírky zákonů)
        - rešerši si může každý uživatel doplnit vlastními komentáři
    - sdílení rešerší s ostatními uživateli – dle výběru uživatele, který rešerši vytvořil
    - uložená mapa procházení IS, tedy seznamu navštívených dokumentů nebo ustanovení jednotlivých dokumentů (vytváří se automaticky, uživatel má základní možnosti modifikace této mapy
- e-mailové notifikace změn dokumentů
    - předdefinované notifikace stejné pro všechny uživatele, např. nová znění právních předpisů nebo změn v legislativním procesu

- notifikace změn uživatelem nastavených dokumentů

8.14.3 Podrobnější specifikace právních informací

8.14.3.1 Právní předpisy

- právní předpisy se budou předběžně týkat těchto oblastí práva
  - cestovní ruch
  - kultura
  - umění
  - zájmová činnost
  - autorská práva a práva související s právem autorským
  - mezinárodněprávní právní ochrana duševního vlastnictví
- předběžně se jedná o cca 600-700 předpisů
- seznam předpisů může být ze strany MK libovolně upraven (rozšířen, zúžen) i mimo rozsah výše uvedených oblastí např. Občanský zákoník, Správní řád apod.

8.14.3.2 Monitoring legislativních změn

- informace budou čerpány z těchto zdrojů
  - knihovny připravované legislativy (https://apps.odok.cz/kpl)
  - ze sněmovních tisků Poslanecké sněmovny (http://www.psp.cz/sqw/sntisk.sqw)
  - senátních tisků (http://senat.cz/xqw/xervlet/pssenat/historie)
- budou navázány k dotčeným právním předpisům

8.14.3.3 Soudní rozhodnutí

- zdroje
  - Nejvyšší soud
  - Nejvyšší správní soud
  - Ústavní soud
- výběr soudních rozhodnutí bude řízen jejich vazbou na právní předpisy, tj. budou vybrána taková soudní rozhodnutí, která obsahují odkazy (tedy citace) na vybrané právní předpisy

8.15 Manažerský informační systém

Jednou z priorit je vytvoření projekt P704 – MIS pro zpřístupnění a vizualizaci manažerských dat. Předpokladem pro tento projekt je vznik adekvátní datové infrastruktury, která bude svým datovým modelem lépe přizpůsobena potřebám reportingu (OLAP) a maximálně odizoluje od další možné nežádoucí zátěže zdrojové transakčních systémy. Proto vznikl návrh na vybudování datového skladu DWH (data warehouse), který se stane základnou pro data, která jsou pravidelných intervalech importována (ETL procesy) z primárních pořizovacích - transakčních systémů rezortu a případně i podřízených organizací. Nad DWH pak bude možné vybudovat řešení umožňující efektivní reporting nebo další složitější analýzy a šetření typu BI (Business Intelligence) pro potřeby širšího vedení rezortu, ale i případně všech podřízených organizací.

8.15.1 Postup

- Definice cílů.
- Analýza datových zdrojů a požadavků (specifikace potřeby tržišť, výběr dimenzí a faktů.
- Návrh modelu DWH (specifikace granularity a návrh logického a fyzické datového modelu).
- Specifikace technických požadavků a výběr platformy.
- Implementace a vývoj (nastavení ETL a OLAP).
- Testování a migrace dat.
- Provoz, údržba a rozvoj.

8.15.2 Přínosy

Realizace řešení přinese kvalitativní zlepšení procesů analýzy informací a zrychlení rozhodovacích procesů rezortu. Dojde i ke sjednocení přístupu k informacím a ke zjednodušení přípravy výstupů pro interní i externí subjekty a jejich prezentace. Je předpokladem pro efektivní manažerské výkaznictví a rozšíření možností v oblasti pokročilých datových analýz (BI)

8.16 Otevřená data

Otevřená data jsou vybraná data státní správy, které je možné poskytovat veřejnosti.

Na rozdíl od Zákona 106/1999 Sb., o svobodném přístupu k informacím, jsou Otevřená data publikována veřejně a poskytována pro kohokoliv, nikoliv pouze tomu kdo o ně žádá. Užívat je tedy může každý a jejich využívání se nijak neomezuje, nekontroluje a nesleduje. Taková data mohou být využívána nejen pro potřeby veřejných služeb, ale i pro potřeby občanů a komerčního i neziskového využití. Očekává se, že nad takovými daty začnou vznikat další komerční služby a produkty, které mohou být přínosné nejen pro veřejnost ale zpětně i pro zkvalitnění služeb, který rezort MK poskytuje. Publikace otevřených dat a otevřených služeb je jednou ze základních součástí aktivit Partnerství pro otevřené vládnutí, ke kterým ČR přistoupila.

Základní požadavky na Otevřená data jsou, že data musí být:

- úplná,
- snadno dostupná,
- strojově čitelná,
- používající standardy s volně dostupnou specifikací,
- zpřístupněna za jasně definovaných podmínek užití dat s minimem omezení,
- dostupná uživatelům při vynaložení minima možných nákladů.

Požadavky na podmínky užití otevřených dat:

- neomezují jejich uživatele ve způsobu použití dat,
- opravňují uživatele k jejich dalšímu šíření,
- musí být uveden autor dat (i při dalším šíření),
- při dalším šíření musí i ostatní uživatelé mít stejná oprávnění s daty nakládat - během šíření dat nesmí dojít např. k omezení jejich využití pouze pro nekomerční účely.

8.16.1 Cíle

Projekt má za cíl implementovat principy otevřených dat do prostředí rezortu MK v souladu se strategickými dokumenty ČR a evropskou legislativou. V důsledku tedy vytvořit legislativní vymezení v rámci rezortu v souladu s implementace EU směrnice 2003/98/ES a její novelizace směrnicí 2013/37/EU a zpřístupnit vybrané datové sady a vybudovat rezortní katalog otevřených dat, včetně procedur zajištění kvality. Dále navrhnout v praxi aplikovatelné postupy pro kontinuální přípravu, publikaci a katalogizaci otevřených dat rezortu a poskytnutí metodické a technické pomoci jednotlivým podřízeným organizacím při publikaci otevřených dat

Otevřená data by měla být zveřejněna v maximálním možném rozsahu a v podobě, vjaké byla původcem jako primární (původní) vytvořena.

- Je třeba určit podmínky užití dat/zvolit licenci dat. Licence by měla klást na využití otevřených dat minimum omezení
- Pro zveřejněná data je třeba jmenovat odpovědnou osobu, tzv. kurátora dat.
- Je vhodné vytvořit samostatnou stránku na rezortním portálu určenou pro zveřejňování otevřených dat.
- Na stránku s otevřenými daty je vhodné umístit odkaz z hlavní nabídky/domovské stránky.

8.16.2 Postup

Projekt otevírání dat rezortu MK by měl mát následující fáze:

1. Analýza a výběr dat k uveřejnění – cílem tohoto kroku je analyzovat dostupná data, popsat jejich strukturu a zvolit data, která je možné a vhodné zveřejnit jako otevřená data.
2. Výběr vhodného formátu dat – krok je věnován výběru vhodného formátu dat.
3. Preferovány jsou otevřené standardizované (nebo alespoň široce využívané) formáty.
4. Návrh způsobu přístupu k datům – rozhodnutí, zda mají být data zpřístupněna v podobě stažitelných souborů nebo pomocí webových služeb.
5. Export dat do navrženého formátu – technické zajištěním převodu dat do zvoleného formátu.
6. Publikace dat – určení vhodné webové prezentace dat a volba URL, na které budou data dostupná uživatelům.
7. Katalogizace dat – tvorba záznamu o zveřejněných otevřených datech v Datovém katalogu, případně vytvoření – technická implementace rezortního datového katalogu.

8.16.3 Přínosy otevřených dat

- Zvýšení efektivity: uvolnění dat znamená možnost je sdílet a analyzovat;
- Podpora ekonomiky: data jsou zdrojem inovací, podnikatelských příležitostí a pracovních nabídek – lze je využít třeba v dopravě, logistice, zdravotnictví či bankovnictví. Firmy pracují s daty jako se surovinou, vytváří nad nimi aplikace, které generují přidanou hodnotu a zisk;
- Transparentnost, zefektivnění a kontrola veřejné správy: zveřejněná data umožňují kontrolu, jak se hospodaří s daněmi nebo jaké jsou náklady organizací, které podporujeme;
- Zapojení občanů do rozhodování: občané se mohou díky datům a analýzám kvalifikovaněji podílet na fungování státu;

- Datová žurnalistika: otevřená data jsou nezastupitelným zdrojem informací pro novináře.

8.17 Projekty v oblasti digitalizace

Níže navržená základní struktura prioritních projektů digitalizace vychází ze struktury a definice kulturních objektů podle NUMERIC:

Název projektu	Obsah	Gestor
Digitální knihovna	Predevším textové dokumenty: tištěné vázané knihy, noviny, časopisy od nejstarších dob po současnost, staré a vzácné tisky ad.	Národní knihovna
Digitální muzeum a galerie	Především 2 D objekty a 3 D malé objekty	Národní muzeum
Digitální památky	Především 3D velké objekty	Národní památkový ústav
Digitální audiovizuální archiv	Film, audio, audiovize	Národní filmový archiv (film, audiovize; ČT jako partner), Moravská zemská knihovna (zvuk, ČRo jako partner)
Digitální knihovna	Predevším textové dokumenty: tištěné vázané knihy, noviny, časopisy od nejstarších dob po současnost, staré a vzácné tisky ad.	Národní knihovna

Tabulka 14: Přehled prioritních projektů v oblasti digitalizace

Jednotlivé digitalizované objekty, které je možné aktuálně v rámci Europeany různými cílovými skupinami využívat, představují reprezentativní výběr evropského kulturního a vědeckého dědictví z více než 1 000 kulturních institucí členských států EU. Europeana se primárně orientuje na kontextuální informace o předmětu, včetně zachycení jeho vizuální podoby; druhá rovina umožňuje prostřednictvím jednoduchého prokliku přístup k detailnějšímu relevantnímu obsahu (text, obrázek, video, audiovizuální záznam), uloženému na serverech individuálních paměťových institucí (partnerů Europeany). Systém Europeany tak prostřednictvím tzv. národních agregátorů a sektorových agregátorů respektuje plnou kontrolu vlastníků a správců kulturního obsahu nad výběrem předmětů, realizací prioritních projektů digitalizace a dlouhodobým uchováváním digitálního obsahu po digitalizaci. Přes tzv. evropské agregátory zároveň eliminuje redundantnost digitalizovaných dat v evropském kontextu a izolaci jednotlivých paměťových institucí. Při této agregaci a následném harvestingu metadat vznikají nové digitální objekty (surogáty), které jsou obohaceny o nové typy metadat. Surogáty je následně možné dále spojovat do sémantických sítí a vytvářet sémantické uzly, pomocí kterých mohou koncoví uživatelé rychle vyhledávat vazby mezi kulturními objekty z různých

sbírek. Europeana umožňuje zejména rychlé vyhledávání typu "kdo", "co", "jak", "kdy". Identifikace, analýza, vyhodnocení a praktická aplikace výsledků v oblasti uživatelských potřeb při tvorbě prototypu Europeany vycházela zejména ze studie statistiky digitalizace Evropské komise NUMERIC (Numeric, STATISTICS ON DIGITISATION OF CULTURAL MATERIALS IN Evropě, Desk-Research Findings, IPF ltd. Listopad, 2007, http://www.numeric.ws).

Europeana vychází z následujících požadavků, které jsou zároveň oblastmi dalšího systémového rozvoje:

- zajistit dlouhodobou ochranu digitálních hodnot
- poskytnout agregované informační služby odborné i laické veřejnosti
- umožnit kvalitní a lákavou prezentaci informací, která přitáhne zájem veřejnosti
- vytvořit koncept, který lze konzistentně rozvíjet kvalitativně, funkčně i kapacitně.

Systémové řešení digitalizace kulturního dědictví v České republice navazuje na koncepci Europeany a dále pak na principy best practises a lessons learned z procesů digitalizace kulturního obsahu v zahraničí. Dále pak navazuje na navrhované principy a nástroje eCulture dle Integrované strategie podpory kultury do roku 2020.

Ve smyslu struktury a základních vymezení a definic kulturních objektů dle národní legislativy a v kontextu studie NUMERIC je potřeba na projektové úrovni v našich národních podmínkách ve spolupráci Ministerstva kultury s národními paměťovými a fondových institucemi vymezit a definovat kulturní objekty a zajistit agregaci, dále též implementovat jednotnou metodiku pro řešení digitalizace (touto problematikou se aktuálně zabývá pracovní skupina vytvořená ve smyslu příkazu ministra kultury). Vyžaduje se, aby jednotlivé agregační úrovně odpovídaly budované struktuře kompetenčních center, digitalizačních pracovišť a sektorových agregátorů.

Předmětem samostatného dokumentu „Strategie digitalizace kulturního obsahu na léta 2013 – 2020“ je soubor aktivit v oblasti samotného procesu digitalizace (konverze), výběru a kategorizace objektů, předpřípravy, postprocessingu, tvorby metadat a vytvoření metodik (průřezové metodiky, postprocessingové metodiky, konverzní metodiky a doplňkové metodiky, pro všechny hlavní a související digitalizační aktivity, určení kompetenčního systému, projektových týmů, logistiky řešení). Aktuální prioritní a iniciální etapou digitalizace je kategorizace a výběr objektů vstupujících do digitalizace a systémové členění kompetenčních center digitalizace a digitalizačních pracovišť.

V rámci strategie ICT MK se, ve vztahu k budování infrastruktury pro digitalizaci, identifikuje park digitalizační techniky jako součást technologické platformy, technické předpřípravy konverze i postprocessingu. Jednotlivá pracoviště z hlediska technologických a logistických vazeb a struktury budou navržena v návaznosti na iniciální fázi digitalizace.

V uplynulém pětiletém období se digitalizace v České republice rozvinula jak kvantitativně (řada institucí zapojených do digitalizačních projektů, vznik digitalizačních jednotek i úložišť na úrovni krajů, zdigitalizování desítek milionů stran beletristické i vědecké literatury, denních zpráv atp.), tak kvalitativně (byla posílena výbava některých PFI, dosluhující technika je nahrazována novou, tržní segment obsadila řada firem se špičkovými technologiemi, studenti prestižních českých univerzit

získávají znalosti v oblasti digitalizace a dlouhodobého uchovávání dat v rámci akreditovaných studijních programů). V tomto přelomovém období (2010-2014) bylo dosaženo významných výsledků v oblasti digitalizace na všech úrovních pracovního i osobního života a v důsledku hluboké technologické penetrace trhu se potvrzuje potřeba koordinace činností nejen po stránce organizační, ale i odborné, a též potřeba záštity z vládní úrovně napříč ministerstvy kultury, školství, práce a soc. věcí, průmyslu, místního rozvoje, životního prostředí (akcentovány kategorie, nikoli věcně správné názvy jednotlivých ministerstev).

8.18 Rozvoj informačního systému Czechiana[1]

8.18.1 Cíle

- uchovávání a prezentace kulturního dědictví - sem patří záznam, sbírání, dlouhodobé archivování a ochrana digitálního obsahu, webharvesting, webarchiving; jakož i správa, zpracování a zpřístupňování digitálního obsahu paměťových a fondových institucí včetně systému uplatnění autorských práv pro digitální objekty

- podpora procesu digitalizace - sem spadá systematická podpora fyzické digitalizace kulturního, vědeckého a intelektuálního dědictví včetně digitalizace záznamů audiovizuálního fondu (textové dokumenty, 2D objekty, 3D malé objekty, 3D velké objekty, filmy, zvukové záznamy, videozáznamy, televizní vysílání, hmotné a nehmotné projevy kultury).

8.18.2 Komponenty a registry aplikační vrstvy Czechiana

Informační systém Czechiana představuje národní agregátor a přímou vazbu na portál Europeana. Komplexní systém je tvořen komponentami, které jsou vzájemně propojeny sémantickými i technologickými vazbami. Koncept je především v prezentační části inspirován základní myšlenkou portálu Europeana - zpřístupnění kulturního obsahu co nejširší veřejnosti jednoduchým a dostupným způsobem.

Komplexním infrastrukturním projektem se budou naplňovat mezinárodní závazky v oblasti budování Evropské digitální knihovny - Europeany a zpřístupňování digitálního evropského kulturního dědictví budoucím generacím.

Řešení obsahuje nasledujíci komponenty:

- Portál kultury - realizuje centrální přístupový bod ke kulturnímu dědictví, pro laickou veřejnost synonymum pro Czechianu.

- Národní agregátor – průřezový, národní agregátor popisných údajů realizující přidané služby, které jsou umožněny právě mezisektorovou agregací, tj. slučováním obsahu z různých zdrojů. Národní agregátor je zapojen do sítě regionálních, sektorových, národních a evropských agregátorů.

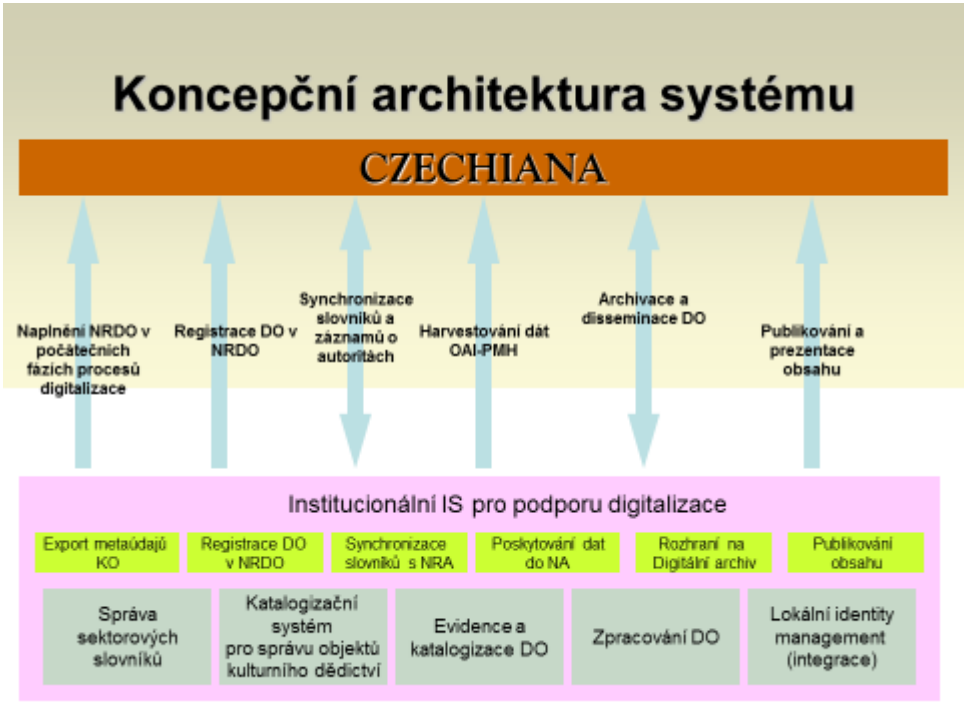
[1] Název „Czechiana“ je prozatimní identifikací tohoto IS a bude revidován.

- Systém pro zpracování obsahu - automatizovaný ,resp. částečně automatizovaný systém pro zpracování primárních příp. postprocessovaných digitalizovaných objektů do prezentovatelné podoby tam, kde je to možné. Nezbytná komponenta pro naplnění cílů digitalizace - prezentaci kulturních objektů veřejnosti.
- DRM - Digital rights managment je subsystém nezbytný pro zajištění zpřístupňování a prodeje obsahu, který je předpokladem udržitelnosti celého systému
- Centrální služby - centrální hostingové služby, rozhraní na komponenty na úrovni G2C.
- Digitální knihovna - Digitální knihovna pro instituce, které nechtějí ,resp. nemohou udržovat vlastní systém.

Řešení obsahuje nasledujíci registry:

Součástí cíle je podpora národních registrů nezbytných pro poskytování elektronických služeb v krossektorovém a distribuovaném prostředí informačních systémů kulturních institucí a digitalizačních pracovišť i pro koordinovaný a efektivní průběh masové průřezové digitalizace. Tento cíl se realizuje následujícími registry:

- Národní registr kulturních objektů
- Národní registr autorit
- Národní registr digitalizace
- Národní registr autorských prav



Obrázek 5 Koncepční architektura IS Czechiana

9 Postup realizace

Dále uvedené tabulky uvádí předpokládaný časový rámec realizace projektů představených v kapitole 8 „Plán strategických projektů“ v členění dle jednotlivých oblastí.

9.1 Oblast řízení ICT MK

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P101	Zavedení řízení architektury	T	T+13M	Projekt je koordinován s projektem P104.
P102	Zavedení Jednotného systému řízení bezpečnosti	T	T+12M	
P103	Formalizace řízení kvality	T	T+6M	
P104	Revize rezortních standardů	T	T+10M	Projekt je koordinován s projektem P102.
P105	Implementace metodického rámce řízení služeb	T	T+12M	Projekt je koordinován s projektem P101.
P106	Centrální zadávání v oblasti infrastruktury a technologií	T	T+8M	
P107	Modernizace ekosystému nástrojů pro řízení kvality služeb	T	T+6M	Projekt je řešen v koordinaci s projektem P103.

9.2 Oblast koncových zařízení

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P201	Standardizace koncových zařízení použitých na pracovišti úřadu.	T	T + 12M	
P202	Analytický projekt standardizace mobilních zařízení a zařízení vlastních (BYOD)	T	T + 4M	
P203	Analytický projekt rozšíření majetkové evidence zařízení o potřeby ICT.	T	T + 4M	

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P204	Analytický projekt řízení licenčních aktiv.	T	T + 4M	
P205	Analytický projekt jednotné správy operačních systémů a aplikací, návrh procesu testování a testovacího prostředí.	T	T + 4M	
P206	Analytický projekt plnění bezpečnostních opatření vztahujících se na koncová zařízení.	T	T + 4M	
P207	Implementace systému pro řízení licencí, propojení majetkové evidence s evidencí zařízení a software.	T	T + 24 M	
P208	Implementace správy operačních systémů a aplikací, výstavba testovacího prostředí.	T	T + 24 M	
P209	Implementace bezpečnostních opatření vztahujících se na koncová zařízení.	T	T + 24 M	

9.3 Oblast systémových služeb

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P301	Vytvoření identity managementu	T	T+7M	Analýza procesů a procedur životního cyklu uživatelských účtů (IDM). Pilotní ověření nasazení IDM. Implementace řízení plného životního cyklu uživatelských účtů IDM systémem.
P302	Konsolidace AD adresářů MK	T	T+7M	Konsolidace současných AD adresářů MK do jednoho (nově vybudovaného/stávajícího). Migrace všech identit, serverů, uživatelů, politika a dalších AD objektů do cílového adresáře

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P303	Migrace Exchange do sjednoceného AD adresáře	T	T+7M	Implementace Exchange v sjednoceném AD adresáře a migrace všech schránek ze stávajících Exchange organizací.
P303	Rozvoj systému pro správu koncových stanic MK	T	T+12M	
P304	Výběr a nasazení systému pro evidenci IT majetku	T	T+6M	Implementace vybraného produktu pro evidenci IT majetku
P305	Rozvoj servicedesku	T	T+6M	Rozvoj či reimplementace řešení pro pokrytí vybraných ITIL procesů a integrace s bezpečnostním monitoringem.
P306	Rozvoj v oblasti antivirové ochrany	T	T+6M	Implementace řešení na servery a pracovní stanice, které kromě standardních detekčních technologií bude k detekci nebezpečných kódů využívat nové detekční technologie založené na pokročilé heuristice a reputaci souborů.
P307	Antivirová ochrana vnitřních poštovních serverů	T	T+6M	Implementace řešení, které bude chránit vnitřní poštovní servery před rozesíláním nebezpečných kódů a spamu.
P308	Antivirová ochrana mobilních zařízení	T	T+6M	Implementace řešení, které bude chránit mobilní zařízení před nebezpečnými kódy.
P309	Aktuálnost verzí systémových služeb	průběžně		V pravidelných intervalech řešit povýšení (upgrade) verzí všech systémových služeb na aktuální verze
P310	Analýza zálohování a požadavků na archivaci	T	T+3M	Výstupem projektu je návrh na řešení požadavků ve stávajících nebo nových systémech v závislosti na provedených zjištěních.
P311	Implementace dlouhodobého úložiště	T	T+12M	Výstupem projektu je implementace řešení dlouhodobého úložiště.
P312	Zastřešující monitoring	T	T+4M	Vyhodnocení nástroje a jeho nasazení za účelem zastřešení monitorovacích nástrojů rezortu.

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P313	Implementace autentizačního serveru	T	T+6M	Implementace řešení pro dvoufaktorovou autentizaci pro zabezpečení přístupu všech oprávněných uživatelů k dotčeným aplikacím.

9.4 Oblast síťových a hlasových služeb

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P401	Centralizace správy síťových služeb DNS a DHCP pomocí IPAM nástroje. Konsolidace a centralizace správy	T	T + 12M	Centralizace správy síťových služeb DNS a DHCP pomocí IPAM nástroje.
P402	Nasazení Ipv6	T	T + 12M	Nasazení protokolu Ipv6 v interní síti MK
P403	Implementace ochrany proti DDOS útokům	T	T + 6M	
P404	Doplnění poštovních bran o technologie pro sledování důvěryhodnosti	T	T + 6M	Implementace řešení, které bude podporovat technologii sledování důvěryhodnosti odesílatelů v internetu a tak významně pomáhat tradičním antispamovým technologiím v detekci spamu
P405	Implementace DLP na poštovních branách	T	T + 6M	Implementace řešení prevence ztráty dat a jeho integrace s poštovními bránami
P406	Implementace DLP na proxy serverech	T	T + 6M	Implementace řešení prevence ztráty dat a jeho integrace s proxy soustavou
P407	Obnova zastaralých prvků	T	T + 3M	Obnova aktivních prvků, které jsou technologicky zastaralé.
P408	Vytvoření bezpečnostní politiky	T	T + 5M	Vytvoření zastřešující bezpečnostní politiky rezortu MK
P409	Rozvoj provozního monitoringu	T	T + 12M	Rozvoj stávajícího provozního monitoringu a napojení do zastřešujícího systému

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P410	Výstavba bezpečnostního monitoringu	T	T + 24M	Nasazení systému bezpečnostního monitoringu a napojení do zastřešujícího systému

9.5 Oblast datových center / HW infrastruktury

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P501	Modernizace a revitalizace ICT infrastruktury v datových centrech	T	T+12	
P502	Vybudován řešení Private Cloud	T	T+9	
P503	Datový sklad	T	T+6	Vytvoření infrastruktury pro P704 – MIS

9.6 Oblast bezpečnosti

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P601	Vytvoření bezpečnostní dokumentace rezortu MK	T	T +	
P602	Zavedení systému řízení informační bezpečnosti	T	T +	
P603	Řízení dodavatelů	T	T +	
P604	Řízení životního cyklu prvků systému ICT	T	T +	
P605	Řízení personální bezpečnosti	T	T +	
P606	Zvládání incidentů, sdílení informací, znalostní management	T	T +	
P607	Audity funkčnosti	T	T +	
P608	Zajištění kontinuity	T	T +	
P609	Fyzická bezpečnost prvků systému	T	T +	

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P610	Bezpečnost informačních systémů – aplikační bezpečnost, klasifikace informací, DLP systémy	T	T +	
P611	Bezpečnost infrastruktury	T	T +	

9.7 Oblast aplikačních služeb

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P701	Pořízení systému IS RCNS	T	T+10M	Oblast IT potřeb věcných agend
P702	Pořízení systému JEGIS	T	T+24M	Oblast IT potřeb věcných agend
P703	Zajištění provozu a rozvoje portálu MK a stanovení pravidel využití	T	T+6M	Oblast IT potřeb průřezových procesů agend a sdílených komponent
P704	Pořízení MIS pro získání celorezortních statistik pro manažerské řízení rezortu a zajištění provozu a rozvoje systému	T	T+24M	Oblast IT potřeb průřezových procesů agend a sdílených komponent
P705	Zajištění stavu existujících aplikací a provedení nápravných opatření	T	T+6M	Oblast doplňkových aplikací
P706	Zajištění provozu a rozvoje ekonomického systému MK	T		Oblast IT podpůrných systémů
P707	Zajištění provozu a rozvoje personálního systému MK	T		Oblast IT podpůrných systémů
P708	Zajištění provozu groupware	T		Oblast IT podpůrných systémů
P709	Zajištění integrace agendových IS s externími systémy	T		Oblast integrací aplikačních služeb
P710	Optimalizace licencí aplikací provozovaných na MK a v podřízených organizacích	T	T+9M	Oblast správy licencí
P711	Zajištění provozu spisové služby	T		Oblast IT podpůrných systémů
P712	Integrovaný analytický systém kultury a archivů (IASKA)	T	T + 24M	Oblast IT potřeb průřezových procesů agend a sdílených komponent

Kód	Název projektu	Termín zahájení	Termín dokončení	Poznámka
P713	Pořízení informačního systému právních informací pro organizace rezortu	T	T+6M	Oblast doplňkových aplikací
P714	Rozvoj informačního systému Czechiana	T	T+12M	Oblast IT potřeb průřezových procesů agend a sdílených komponent
P715	Otevřená data	T	T+9M	Zpřístupnění vybraných dat v gesci MK veřejnosti

10 Přílohy

Žádné.