

Systém pro dlouhodobou ochranu digitálních dat vznikající v rámci projektu NDK

Základní popis systému

Jeho úkolem je zajistit trvalé (po dobu, dokud budou mít uchovávané digitální objekty význam pro uživatele) uchování digitálních nebo digitalizovaných dokumentů v takovém stavu, ve kterém je budou moci uživatelé použít. Uchovávané zdroje musí být vyhledatelné, uživatel je musí mít možnost v pro něj běžném technickém prostředí zobrazit tak, jak zamýšlel jejich tvůrce, a uživatel musí být schopen jim porozumět, pochopit jejich obsah a smysl. Dosažení těchto cílů předpokládá uchování nejen bit streamu reprezentujícího daný digitální objekt, ale také uchování dalších informací, které umožní objekt vyhledat, adekvátně technicky zobrazit a uživateli objektu i porozumět. V kontextu modelu OAIS to znamená, že spolu s jednotlivými digitálními objekty musí být uchován nejen informační obsah uchovávaných objektů, ale také další informace o původu a historii změn dokumentu, o jeho kontextu a zdrojích potřebných k porozumění (identifikační informace, informace o provenienci, kontextuální informace, informace o úplnosti).

Přijetí materiálu (Ingest I.) – první fáze:

Příprava dokumentů pro vstup do repozitáře bude začínat již na pracovišti masové digitalizace nebo při harvestingu ve WebArchivu. Odtud, přes aplikaci, která případně zajistí převod metadat do formátu podporovaného LTP systémem, budou data přicházet již se základními metadaty (popisnými, strukturálními, administrativními, po kontrole kvality obrazu, zpracování OCR a vytvoření uživatelské kopie). Pro pracoviště masové digitalizace a WebArchivu musí na straně LTP systému existovat nezávislé aplikace pro zpracování příjmu (Ingest), které budou v podstatě automatizované a budou se lišit od ručního vkládání do systému.

V budoucnu může vzniknout potřeba archivovat i další typy dat (například audiovizuální data), což může vyžadovat zapojení dalších aplikací pro vstup dat nebo minimálně flexibilitu deposit modulu systému, který by si měl umět poradit s jakýmkoliv typem souboru. Systém bude v této fázi provádět: kontroly úplnosti dat, antivirové kontroly, validaci struktury balíčků, vytvoření intelektuálních entit, přidělení URN:NBN:CZ nebo i dalších vnitřních identifikátorů, validaci metadat, kontrolu záznamu v registru digitalizace, doplnění metadat, vytvoření balíčku pro další fázi, odeslání do další fáze zpracování aj. V každém okamžiku v případě problému bude dokument vrácen buď producentovi, nebo zaměstnanci, který rozhodne o jeho dalším osudu.

Přijetí materiálu (Ingest II.) – druhá fáze:

Druhá fáze vstupu do repozitáře by měla být společná pro všechny typy vkládaných materiálů a pro všechny dodavatele. Zde půjde především o provedení automatické identifikace a validace formátů souborů, tzv. enrichment (obohacení metadat automatickou cestou), případnou migraci do preferovaných formátů (normalizace), opětovou antivirovou kontrolu. Toto bude probíhat zapojením služeb jako je JHOVE, PRONOM/DROID případně s využitím NZME (New Zealand Metadata Extactor). Průběh pohybu vstupního balíčku by měl být vidět v online monitorovacím modulu systému, kde bude informace dostupná správci repozitáře i dodavateli dat a tato data se budou dále archivovat. V druhé fázi Ingestu stále ještě jsou uživatelské kopie v LTP systému (na pracovním prostoru), po uložení archivních dat do

Archivu (AIP) se budou předávat do aplikací zpřístupnění a v LTP systému nezůstávají.

Správa archivního modulu

Jedná se o jádro systému dlouhodobé ochrany. Základem je systém archivace (archival storage) – vlastní technologie uchovávání digitálních dokumentů na fyzických úložištích. Současné metody archivace mají řadu funkcionalit, které dlouhodobou archivaci podporují. Ačkoli využívají ultra levná úložná média, díky pokročilému clustrování, inteligentnímu nakládání s daty, monitoringu a dalším funkcím jsou z hlediska dlouhodobé ochrany velmi vhodné. Nad archivací musí mít systém komplexní data, metadata management a administrativní rozhraní. To vše bezpodmínečně s odpovídajícím GUI rozhraním.

Plánování ochrany

Systém by měl monitorovat základní vlastnosti (za pomoci externích služeb jako je např. PRONOM) a metadata vkládaného materiálu a inteligentně pomáhat správcům repozitáře s plánováním dlouhodobé ochrany (musí uchovat informace o vložených formátech a platformách, na kterých fungují; o použitých metodách komprese a dalších souvisejících technologiích, které mohou mít potenciálně dopad na použitelnost archivovaného materiálu). Systém musí umožňovat, aby oprávněný správce repozitáře mohl vyexportovat z archivu různě definované množiny objektů pro účely například migrace nebo jiné ochranné akce mimo repozitář (ve fázi testování migračních nástrojů atp.), případně obsahovat základní nástroje pro migraci dat. Jinou možností je, že systém umožní provádět hromadné ochranné akce použitím externích nástrojů. Další vývoj v oblasti dlouhodobé ochrany zcela jistě přinese nové praktické nástroje, jež provádění ochranných akcí podpoří nebo usnadní (viz evropské projekty jak např. PLANETS a jejich nástroj PLATO). Proto musí být systém dostatečně otevřený, aby tyto nástroje bylo možné v budoucnu využívat.

Přístup

Systém repozitáře bude muset umožňovat vyhledávání a dodání archivovaných dokumentů a jejich metadat v různě – volitelně – strukturovaných balíčcích DIP při dodržení přístupových práv.

Administrace, Monitoring

Systém musí mít propracovaný modul pro monitoring. Měl by podporovat sledování pohybu dokumentů v jednotlivých fázích životního cyklu balíčků SIP>AIP>DIP a tyto informace uchovávat. Měl by také monitorovat a zaznamenávat všechny prováděné akce; použité formáty a software. Musí podporovat monitoring distribuce dokumentů z repozitáře. Bylo by vhodné, aby monitoring bylo možné použít v obchodním modelu repozitáře, tj. sledovat náklady na skladování dokumentů, vykazovat náklady jednotlivým skupinám uživatelů a dodavatelů dat.

Administrace musí být flexibilní, umožnit nastavení přístupů do systémů, práv k určitým akcím a nastavení systému samotného, to vše za použití GUI rozhraní.

Integrace s okolními systémy

- knihovní katalogy
- vazba na katalogizační modul ILS – kontrola záznamu v katalogu, případně spuštění procesu jeho vytvoření při ingestu (pro data, která nepřicházejí z masové digitalizace, ale z jiných zdrojů)
- vazba na producenta, dodavatele dat (především automatizované přijímání dat z masové digitalizace v rámci projektu, kromě toho otevřenost dalším potenciálním

dodavatelům dat)

- vazba resolver URN:NBN – výměna metadat s revolverem/generátorem URN:NBN, (data z masové digitalizace budou mít URN:NBN vytvořená v procesu digitalizace, LTP systém je musí zkontrolovat v revolveru, případně se musí vzájemně obohatit. Pro data z jiných zdrojů – měl by být schopen URN:NBN přidělit, nebo proces vyvolat)
- autentizace (pro admin users, pro end users přístup nebude)
- (m)oaipmh propojení (Europeana)
- access aplikace (např. Kramerius)
- JHOVE, DROID
- registry formátů (UDFR, PRONOM)
- preservation planning tool (PLATO)
- audit a certifikace
- nástroje na migraci (SW pro migraci)
- RegistrDigitalizace.cz
- konverzní aplikace pro transformace metadat a uživatelských kopií

Přehled požadavků na systém pro dlouhodobou ochranu digitálních dat v projektu NDK

Systém dlouhodobé ochrany dat vznikající v rámci projektu NDK musí být založen na referenčním rámci OAIS, musí obsahovat plánování ochranných akcí, jejich provedení a hlavně musí zajišťovat práci s metadaty, která jsou klíčová při jakémkoliv pokusu o dlouhodobé uchování.

Dalšími standardy, které musí nový systém podporovat, jsou (mimo OAIS):

- metadatové formáty PREMIS, METS, MODS, MIX aj., které jsou celosvětovými standardy
- musí spolupracovat se službami třetích stran (PRONOM, UDFR, Jhove2 apod.)
- musí být jednoduché k systému napojit jakékoliv nové služby třetích stran
- měl by být schopen projít certifikací (TRAC, DRAMBORA)

Základní požadavky:

- Informace a dokumenty uložené v systému musí být uloženy na velmi dlouhou dobu (permanentně) a po celou dobu musí být zachována jejich použitelnost, čitelnost a srozumitelnost
- Systém musí odpovídat konceptuálnímu modelu OAIS
- Systém musí být připraven pro certifikaci „důvěryhodného digitálního repozitáře“ (TRAC)
- Systém musí odpovídat aktuálním standardům v oboru dlouhodobé ochrany digitálních dat a používat aktuální nástroje pro validaci a charakterizaci formátů
- HW a SW systému musí odpovídat existujícím standardům v oblasti
- LTP systém musí obsahovat dostatečné informace o uchovávaných objektech tak, aby byly vyhledatelné, aby bylo možné prokázat jejich původ a dokumentovat změny na nich provedené
- Integrace s existujícími systémy NK ČR a MZK
- Kontrola přístupu
- Řízení vztahů s producenty dat, i mimo rámec IOP projektu
- Vkládání digitálního materiálu (z různých zdrojů)
- LTP systém musí být schopen přijmout data – dokumenty v jakémkoli formátu. Je věcí smlouvy s producentem, jak se s daty bude pak nakládat. V některých těchto případech budou

data normalizována do přijatelnějších formátů. V jiných případech, pokud to producent, dodavatel nebo formát dat neumožní, bude garantována pouze bit stream preservation.

- Možnost rozšiřovat specifikaci metadatových formátů
- Připravenosti pro vstup nepublikovaného materiálu (e-deposit) a potřebné napojení na katalogizaci
- Monitorování digitálního materiálu
- Implementace strategií dlouhodobé ochrany
- Archivní modul musí udržovat minimálně dvě kopie dat na dvou geograficky oddělených lokalitách (v Praze a Brně)
- Monitorování a podpora technologické infrastruktury
- Zpřístupnění obsahu archivu
- Role based autorizace
- Protokoly FTP, OAI-PMH, sFTP, FTPS, SWORD, SRU/SRW
- Scheduler na ingest
- Nutná funkcionality vložení z fyzického přenosného nosiče (CD, DVD, externí HDD)
- Musí být možné přeskočit některé fáze ingestu
- Roll back scenario musí být dostupné pro různé moduly (hlavně ovšem pro ingest)
- Nutné zvládnout na vstupu až desítky tisíc dokumentů za den
- Graphical user interface (GUI) na všechny moduly

Obecné vlastnosti systému na dlouhodobou ochranu digitálních dat (LTP systému) – Nefunkční požadavky

- systém musí být otevřený a vysoce interoperabilní, tj. musí umožňovat odpojení a připojení různých částí systému bez omezení funkcionality jiných, musí umožňovat jednoduchou a otevřenou integraci externích nástrojů (přes API a SDK) a jejich využití v pracovních postupech systému pro případnou migraci, emulaci, validaci formátů, ale i pro spolupráci s katalogem, deposit, zpřístupňovací aplikace, vyhledávací nástroje apod.;
 - systém musí být kvalitně a kompletně zdokumentován;
 - systém musí být rozšířitelný, tj. musí být možné pružně měnit parametry systému, jak z hlediska celkové ukládací datové kapacity, tak z hlediska počtu a typů uložených objektů, jejich velikosti a z hlediska datové prostupnosti kritických míst systému;
 - systém musí být v mnoha ohledech nastavitelný (NDK například bude i přes relativní homogenitu materiálů přicházejícího z masové digitalizace potřebovat různé definice informačních balíčků SIP, AIP a DIP, systém musí být schopen je zpracovávat paralelně, musí umožňovat snadnou integraci nových formátů a nových projektů);
- 102
- systém musí mít pravidly řízené pracovní postupy (rule based workflow);
 - řešení musí být zcela nezávislé na použitých typech HW ani na SW platformě (architektura řešení nesmí být svázána s jedním určitým typem archivního úložiště (archival storage), jedním výrobcem ...);
 - zajištění trvalého rozvoje systému, migrace na nová média, využívání nových formátů, nového softwaru pro hodnocení a sledování obsahu archivu atd.;
 - řešení musí být pokud možno maximálně automatizované (ve smyslu zpracování hromadných dodávek dokumentů, automatická musí být i distribuce, konverze), ovšem při maximálním zachování možnosti manuálního zpracování nastavení;
 - systém musí umožňovat provádět ochranné akce hromadně na administrátorem definovaných skupinách objektů; řešení musí podporovat řízení práv dostupnosti, podporovat systémy typu Onelog, Shibboleth, udržovat databázi uživatelů i dodavatelů dat, zaznamenávat jejich aktivity;

- systém musí mít maximálně propracovaný modul pro monitorování a sledování akcí probíhajících na vstupu do repozitáře, dále při archivaci, distribuci, správě a administraci;
- systém musí podporovat zapojení nástrojů třetích stran pro plánování dlouhodobé ochrany, realizaci hromadných ochranných aktivit a hodnocení jejich úspěšnosti;
- systém musí mít naplánován vývoj (roadmap), který nebude závislý na zákazníkovi – tj. samostatný vývoj produktu;
- producent systému musí být aktivní na poli DP – skutečně aktivní – mít vlastní vývoj apod., přítomnost na konferencích apod.;
- dostupnost zdrojového kódu v případě potřeby;
- nutnou podmínkou je reference na běžící systém s digitalizovanými daty v něm kdekoliv na světě.

Základní funkční požadavky na systém dlouhodobé ochrany digitálních dat

Název		Popis
<i>1. Vložení materiálu - Ingest</i>		
1	Řízený tok vstupujících dat (podle různých typů sbírek)	Systém poskytuje služby pro kontrolu toku vstupujících dat, s možností nastavení paralelních datových toků pro různé sbírky: např. pro data z digitalizace, z webharvestingu, z povinného výtisku, pro zvukový materiál atd.
2	Vytvoření vstupního balíčku SIP	Systém umožňuje producentům dat vytvořit vstupní balíček z jakýchkoli digitálních dat s metadaty.
3	Mechanismus pro předání vstupního balíčku	Systém umožňuje vkládání digitálního materiálu pomocí standardních komunikačních protokolů (např. FTP, HTTP, sdílená síť, atp.) nebo z fyzických elektronických médií (např. CD-R, externí HDD aj.)
4	Dávkové nebo manuální vkládání	Systém je schopen přijímat vstupující materiál jednotlivě nebo dávkově.
5	Metadata vstupujícího balíčku	Systém je schopen získat data o vstupujícím materiálu od producenta/depozitora, např. popisná metadata, data specifikující práva k zpřístupnění. Systém používá hash ke kontrole integrity dat.
6	Oznámení o výsledku vstupu	Systém automaticky generuje oznámení o tom, zda vstup materiálu do úložiště proběhl úspěšně nebo ne, toto oznámení zaznamená a pošle producentovi a administrátorovi.
7	Identifikace producenta	Systém je schopen v okamžiku vkládání dat identifikovat producenta/vkladatele, a využít nastavení, které je pro daného producenta v systému uloženo pro řízení vstupních operací.
8	Identifikace a sledování PSP ¹ /SIP	Systém zajistí, že každý PSP a konečný SIP dostane při vstupu jedinečný identifikátor.
9	Zajištění integrity PSP	Pro každý soubor v PSP musí systém sledovat hash.
10	Předvyplnění vstupních metadat	Producent/dodavatel si může na vstupu vybrat z přednastavených šablon s předem vyplněnými metadaty.
<i>2. Administrace</i>		
11	Management producentských účtů a nastavení vstupního procesu.	V systému je možné vytvářet, udržovat a rušit účty producentů. Účty musí obsahovat kontaktní informace a ujednání o způsobech vkládání materiálů do systému, o zpřístupnění, případně další informace a nastavení.

¹ PSP – Producent Submission Package – to co se do LTP systému zasílá a až v LTP systému se z toho stane SIP (Submission Information Package)

12	Zaznamenávání aktivity producentů	Systém monitoruje a zaznamenává aktivity producentů, kontroluje, zda jsou v souladu s příslušnými ujednáními, umožňuje prohlížet seznamy vloženého materiálu od jednotlivých producentů atd.
13	Workflow systému je pružně nastavitelné, automatizované, založené na pravidlech	Systém používá pravidla pro řízení automatického workflow. Workflow je možné měnit (např. přeskokovat některé kroky) a mělo by být možné vrátit se ve workflow o krok zpět (roll back).
14	Lokální knihovna formátů	Systém udržuje knihovnu formátů, které do něj byly vloženy, a podporuje jejich identifikaci, charakterizaci a validaci.
3. Management intelektuálních entit		
15	Jedinečný identifikátor pro každou intelektuální entitu	Systém zajistí, že každá skladovaná logická entita a digitální objekt mají jedinečný trvalý vnitřní identifikátor od okamžiku vstupu do Ingestu (LTP systému).
16	Automatická kontrola kvality souborů a metadat.	V systému lze nastavit pravidelné a automatizované kontroly kvality dat v archivu. Tyto kontroly mohou obsahovat antivirovou kontrolu (prováděnou v oddělené zabezpečené lokalitě) validaci formátů a kontroly integrity souborů (check-sum).
17	Rozpoznání formátů souborů a jejich charakterizace	Systém je schopen identifikovat, charakterizovat a validovat formáty souborů a kontroluje, zda je vstupující formát v souladu s nastavenými pravidly workflow.
18	Bezpečný karanténní úložný prostor	Systém obsahuje oddělenou a zabezpečenou oblast pro skladování digitálního materiálu, který neprojde automatickými kontrolami a poskytuje automatické oznámení správci systému pro další zpracování.
19	Automatická extrakce metadat z vložených souborů	Systém automaticky získává metadata ze souborů podle nastavených pravidel a spolupracuje s externími službami (pokud je třeba).
20	Systém umožňuje manuální výběr vložených digitálních objektů	Systém umožňuje lidský zásah za účelem selekce a kontroly obsahu digitálního materiálu. Manuální selekce nebo kontrola digitálních dat je podporována systémem založeným na pravidlech, např. v případech, kdy je digitální materiál na vstupu do úložiště z nestandardního zdroje.
21	Systém umožňuje uspořádání a popis digitálních objektů	Systém poskytuje možnost manuálně třídit a popisovat vkládaný materiál před tím, než je vložen do archivu.
22	Mazání souborů, které nebudou součástí SIPu	Systém umožňuje mazání souborů z balíčku PSP, které byly na základě manuálního výběru ze SIPu identifikovány jako odmítnuté. Systém uchovává metadata spojená se soubory vymazanými ze SIPu.
23	Vyhledávání v repozitáři	Systém poskytuje mechanismy podporující několik metod použití metadat spojených s entitami a jejich reprezentacemi. Umožňuje vyhledávat reprezentace uložené v archivu a poskytuje výsledky vyhledávání ke stažení apod. Archivovaná data by měla být dostupná i bez systému pro dlouhodobou ochranu.
24	Uchovávání derivátů vložených souborů	Systém umožňuje vložení jiných verzí uchovávaných digitálních objektů v jiných přijatelných formátech a poskytuje nástroje jak spojit tyto deriváty se SIP nebo archivními reprezentacemi, a tato spojení zobrazit, tj. udržuje více verzí jednoho dokumentu vzniklých např. v průběhu let.
25	Extrakce reprezentace pro manuální údržbu	Systém je schopen komunikovat s nástroji pro autentikaci a poskytuje pravidly řízené workflow pro manuální vytváření nových verzí archivovaných objektů nebo pro mazání reprezentací souborů a/nebo jejich metadat.
26	Vytvoření dodatečné reprezentace	Systém poskytuje mechanismus pro vytvoření nových reprezentací z vybraných souborů (jako součásti existující intelektuální entity v archivu).
27	Příprava a vložení metadat (pro jednotlivé soubory nebo pro	Systém podporuje manuální i automatické vytváření metadat pro jak individuální tak dávkové zpracování.

	balíky)	
28	Aplikace softwarových nástrojů a postupů pro dlouhodobou ochranu	Systém má otevřená API a podporuje integraci externích ochranných nástrojů jako součásti reservačních workflow. Systém umožňuje definovat ochranné workflow a postupy, jejich autorizaci a provedení na nějak vybraných/definovaných souborech reprezentací/digitálních objektů. Nástroje na ochranné akce jsou ideálně součástí LTP systému, za předpokladu zachování možnosti připojit nástroje externí. LTP systém obsahuje modul na plánování a testování ochranných operací.
<i>4. Plánování dlouhodobé ochrany</i>		
29	Výběr a vytvoření identických kopií pro účely testování ochranných aktivit	Systém poskytuje mechanismus pro výběr a kopírování reprezentací ven z archivu do odděleného prostředí, ve kterém budou testovány nástroje a procedury pro testování akcí dlouhodobé ochrany. Systém udržuje logy o provedení těchto kopií a jejich exportu.
30	Identifikace a oznámení ohrožených reprezentací	Systém má mechanismus pro hledání v metadatech objektů a generování reportů o identifikovaných ohrožených datech/formátech.
31	Výběr souboru reprezentací pro dlouhodobou ochranu	Systém využívá selekční kritéria, která definuje autorizovaný uživatel, a využívá informace z metadat pro vytvoření seznamu úkolů, který definuje různé skupiny reprezentací určených pro konkrétní ochrannou akci.
32	Hodnocení výsledku ochranných akcí	Systém vybírá a vypíše na parametrech založený soubor aktualizovaných reprezentací, na kterých byla provedena nějaká konkrétní reservační akce, pro hodnocení konkrétním člověkem.
<i>5. Management archivu</i>		
33	Management metadat objektů v archivu, která jsou v jiných knihovních systémech	Systém specifikuje, které systémy jsou odpovědné za skladování částí metadat uložených reprezentací.
34	Management lokací souborů v archivu	Systém určuje lokaci reprezentací a jednotlivých souborů v archivu pro účely uložení a přemístění (pokud je to nutné).
35	Management procesů archivního skladu	Systém poskytuje mechanismus pro management reprezentací v archivním skladu. To znamená, že je schopen uložit, aktualizovat, vyložit data nebo metadata spojená s konkrétní reprezentací (bez nutnosti exportovat celý archivní balíček ven z archivního systému a opětný re-ingest)
36	Automatické zajišťování kvality souborů a metadat skladovaných objektů.	Systém umožňuje pravidelnou a automatickou kontrolu pro zajištění integrity a kvality archivovaného digitálního materiálu, podle nastavených pravidel, která je schopen interpretovat a použít.
37	Komplexní metadata pro kontrolu přístupu ke skladovaným digitálním objektům	Systém drží, aktualizuje a aplikuje pravidla pro řízení práv a podmínek dostupnosti k jednotlivým reprezentacím jako součást metadat.
<i>6. Access</i>		
38	Využití existujících nástrojů pro vyhledávání zdrojů	Systém musí spolupracovat s existujícími nástroji NK ČR a MZK pro vyhledávání, musí být schopen zpracovat jejich požadavky na vyhledání digitálního materiálu a metadat. Komplexní vyhledávací mechanismus by měl mít i vlastní samostatný archivní modul LTP systému.
39	Data pro kontrolu dostupnosti a podmínky použití	Systém drží data o kontrole dostupnosti a podmínkách použití digitálního materiálu pro podporu interpretace práv dostupnosti systémy pro vyhledávání. Systém musí být otevřený jiným systémům pro kontrolu dostupnosti.

40	Poskytnutí DIPu	<p>Systém generuje a odesílá DIP (nebo uživatelskou kopii) pro existující vyhledávací systémy v NK ČR a MZK na základě dotazu. Odpověď na žádost o přístup k digitálnímu obsahu může obsahovat:</p> <ul style="list-style-type: none"> - výsledný balík obsahující metadata spojená s příslušnými entitami, nebo - jeden nebo více digitálních objektů a jejich metadata, nebo - jeden nebo více balíčků metadat, nebo - odpověď, že objekt není dostupný, uživatel nemá autorizaci atp.
7. <i>Sdílené služby</i>		
41	Audit	Systém poskytuje mechanismus pro provádění a deaktivaci událostí pro audit, vlastnosti těchto událostí jsou zaznamenávány do systému.
42	Generování reportů	Systém poskytuje mechanismy pro zpracování reportů na požádání, umí generovat reporty o vloženém materiálu. Uživatel může nastavit profil reportů. Systém umožňuje nastavit, vytvořit nebo zrušit šablony pro reporty.
43	Monitorování událostí	<p>Systém disponuje mechanismy pro identifikaci a interpretaci událostí v archivu jakožto podmínek pro:</p> <ul style="list-style-type: none"> • Stanovení automatických systémových procesů a standardních akcí/postupů • Informuje zaměstnance a externí účastníky (např. vydavatele, dárce) o postupech, které je na základě interpretace podmínek nutné aplikovat • Notifikace nebo automatické procesy mohou být spuštěny za různých systémových nebo environmentálních podmínek, např. identifikací virusu či selhání sítě
44	Konfigurace výkonu	<p>NDK využívá operačních a výkonnostních limitů, které jsou:</p> <ul style="list-style-type: none"> • konfigurovatelné (systémovým administrátorem) dle SW a HW • využívány NDK aplikací pro zjištění podmínek, které spadají nad rámec limitů, od notifikace přes běžnou správu událostí, odezvu/akce systémového administrátora až po výmaz.
45	Správa systému a konfigurace	NDK LTP aplikační software využívá pro interakci s externími systémy pro správu a konfigurace otevřených programovacích rozhraní (API) nebo messaging protokolů.
46	Bezpečnostní management	NDK LTP aplikační software využívá pro interakci se zabezpečenými externími službami otevřených programovacích rozhraní (API) nebo messaging protokolů.
47	Management identifikace a přístupu	NDK LTP aplikační software využívá jako primární mechanismus pro interakci s externími identifikačními a přístupovými službami otevřených programovacích rozhraní (API) nebo messaging protokolů.
48	Administrace databáze a úložiště	NDK LTP aplikace interaguje se systémy úložišť pro získání strojově čitelných politik a pravidel o umístění metadat a archivních objektů.
49	Archivní zálohování (objektů a metadat)	<p>Systém umožňuje „on-line“ zálohování archivu způsobem, který neovlivňuje negativním způsobem ostatní systémové funkce. Zálohy mohou být:</p> <ul style="list-style-type: none"> • konfigurovatelné tak, aby zahrnovaly popisná metadata ze systémů pro správu sbírek v NK/MZK

		<ul style="list-style-type: none">• nastaveny pro automatický chod/spuštění
50	Audit a analýza	System poskytuje mechanismus k zachycení jakékoliv události v auditu pro všechny transakce vzešlé z jakéhokoliv použití funkcionality NDK LTP systému. System umožní tyto jednotlivé položky auditu vyhledávat, filtrovat a vyhodnocovat na základě kritérií, která mohou být nastavena a autorizována systémovým uživatelem (administrátorem).