Oznámení Ministerstva vnitra,

kterým se zveřejňuje

národní standard pro elektronické systémy spisové služby

Ministerstvo vnitra zveřejňuje na základě § 70 odst. 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění zákona č. 190/2009 Sb. a zákona č. 167/2012 Sb., národní standard pro elektronické systémy spisové služby (dále jen „národní standard“).

Nové znění národního standardu bylo upraveno na základě praktických zkušeností původců i dodavatelů elektronických systémů spisové služby. Současně byla provedena celková revize národního standardu, která spočívala v posouzení textu a v odstranění tzv. doporučených (nepovinných) požadavků a duplicitních ustanovení. Současně byl text přestrukturován podle posloupnosti činností při výkonu spisové služby.

Za zcela zásadní je třeba považovat začlenění popisu rozhraní na propojení systémů spravujících dokumenty. S tím souvisí i nové schéma XML v příloze č. 1. S ohledem na problémy se ztvárňováním transakčního protokolu do PDF/A bylo pro něj vytvořeno nové schéma XML (příloha č. 6). V oblasti skartačního řízení byla zohledněna také činnost Národního archivu na úseku péče o archiválie v digitální podobě a existence jeho portálu pro zpřístupňování archiválií v digitální podobě a zejména výkladem (kapitola 11) zpřesněna schémata XML pro předávání metadat a digitálních dokumentů k trvalému uložení v podobě datového balíčku SIP (přílohy č. 2 a 3). V neposlední řadě byly křížové odkazy rozděleny na pevné (bez možnosti odstranění) a volné.

Mezi další významné změny patří odstranění pojmu záznam a zavedení pojmu koncept (rozpracovaný dokument), který je spravován v elektronickém systému spisové služby shodně jako dokument, avšak může existovat ve více verzích a nemusí být evidován v evidenci dokumentů. S tím souvisí i nahrazení zkratky ERMS (anglicky elektronický systém pro správu dokumentů) obecnější zkratkou eSSL (elektronický systém spisové služby) – systém spravuje i koncepty. V podmínkách výkonu spisové služby v České republice neužívané řízené slovníky byly nahrazeny číselníky. Zcela zrušena a rozpuštěna byla původní kapitola 10 (účelové moduly), vypuštěny byly požadavky na výtah, redakci a nezbytné dokumenty; naopak zaveden byl pojem zásilka. Místo pojmu agendový informační systém je nově použit obecnější výraz informační systém spravující dokumenty. V souvislosti s platností nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES a s ním souvisejícím zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, byla upravena terminologie a postupy elektronického podepisování. Nově byl spisový plán omezen pouze na věcné skupiny a termín organizace nahrazen termínem původce.

Současně byly požadavky národního standardu nově očíslovány. Aby bylo možné kontrolovat znění s předcházející úpravou, jsou u jednotlivých požadavků uvedena jejich původní čísla s případnou poznámkou, zda došlo k významnější úpravě.

Znění národního standardu je zpřístupněno způsobem umožňujícím dálkový přístup na internetových stránkách Ministerstva vnitra v sekci „O nás“, ve složce „Archivnictví a spisová služba“.

Národní standard nabývá účinnosti dnem 4. července 2017 s výjimkou požadavků kapitoly 2.1, pokud se jedná o rozpracované dokumenty (koncepty), 2.1.33, 2.3.6, 2.3.10, 2.7.19, 3.1.19, 3.2.22 kapitoly 3.3, pokud se jedná o rozlišování pevných a volných křížových odkazů (všechny nerozlišené křížové odkazy se považují za pevné), 5.3.4 až 5.3.8, 6.2.4, 6.2.6, 6.3.5, 6.3.19, 7.1.21, 7.1.22, 7.2.3, 7.2.8, 8.1.4, 8.2.4, 8.2.5, 8.2.10, kapitoly 9.1, 11.2, které nabývají účinnosti 1. května 2018.

Národní standard pro elektronické systémy spisové služby zveřejněný ve Věstníku Ministerstva vnitra čá. 64/2012 se dnem 4. července 2017 zrušuje.

Po dobu jednoho roku ode dne nabytí účinnosti tohoto národního standardu lze k importu, exportu nebo přenosu metadat entit a jejich komponent použít rovněž přílohu č. 1 národního standardu pro elektronické systémy spisové služby, ve znění účinném před nabytím účinnosti tohoto národního standardu. V takovém případě se neuplatní požadavky kapitoly 9.1.

Po dobu jednoho roku ode dne nabytí účinnosti tohoto národního standardu lze k vytvoření datového balíčku SIP použít rovněž přílohy č. 2 a 3 národního standardu pro elektronické systémy spisové služby, ve znění účinném před nabytím účinnosti tohoto národního standardu. V takovém případě se neuplatní požadavky kapitoly 11.2.

Č. j. MV-33371-16/AS-2017

Ředitel odboru archivní správy

PhDr. Jiří ÚLOVEC v. r.

Národní standard
pro elektronické systémy spisové služby

Obsah

1 ZÁKLADNÍ POJMY

Bezpečnostní kategorie
Bezpečnostní kategorie je jedno nebo více opatření spojené s dokumentem nebo seskupením, která podmiňují nebo definují pravidla určující podmínky přístupu k němu, a to zejména v souvislosti s klasifikací dokumentu, který obsahuje chráněnou informaci. Tyto informace jsou označovány v souvislosti s rozhodnutím původce omezit přístup k jím stanoveným kategoriím dokumentů nebo seskupení (například personální dokumenty, obchodní tajemství). Pokud nevyplývá omezení přístupu k dokumentu nebo seskupení z jiných právních předpisů, lze bezpečnostní kategorii specificky stanovit na organizační úrovni.

Číslo jednací
Číslo jednací je evidenční znak dokumentu v rámci evidence dokumentů, jehož tvar vychází z požadavků jiných právních předpisů a potřeb původce.

Datový balíček SIP
Informační balíček („Submission Information Package“) určený k exportu nebo přenosu entit z eSSL do digitálního archivu. Je tvořen podle příloh č. 2 a 3 a obsahuje metadata a digitální komponenty

a) spisu,
b) dokumentu zatříděného přímo do věcné skupiny, nebo
c) dílu typového spisu.

Datový formát
Datový formát je způsob kódování komponenty, který zajišťuje uložení dokumentu nebo jeho části (částí) pro účely zpracování výpočetní technikou a jeho znázornění. Pojem „datový formát“ se pro účely národního standardu užívá v obdobném významu jako „formát“. Datovými formáty jsou například

a) formát Portable Document Format/Archive (PDF/A, ISO 19005),
b) formát Portable Network Graphics (PNG, ISO/IEC 15948),
c) formát Tagged Image File Format (TIFF, revize 6 – nekomprimovaný),
d) formát JPEG File Interchange Format (JPEG/JFIF, ISO/IEC 10918),
e) formát Graphics Interchange Format (GIF),
f) formát Waveform audio format (WAV), modulace Pulse-code modulation (PCM),
g) formát XML,
h) proprietární formáty dokumentů vytvářené například kancelářskými aplikacemi.

Dědičnost
Dědičnost vyjadřuje schopnost entity umožnit předání určitých vlastností z mateřské entity na entitu dceřinou.

Deklarování dokumentu
Deklarování dokumentu je zaevidování verze rozpracovaného dokumentu (konceptu) do evidence dokumentů.

Digitální
Pojem „digitální“ vyjadřuje způsob zpracování entity představovaný numerickým řetězcem tvořeným čísly „1“ a „0“ (proud bitů) interpretovatelný pomocí výpočetní techniky. Pojem „elektronický“ se pro účely národního standardu užívá obdobně.

Díl
Pomocí dílu jsou členěny součásti v typových spisech. Díly slouží k zajištění účelné správy rozsáhlých spisů pomocí zpracovatelsky přehledných manipulačních jednotek a jsou vytvářeny mechanicky dle časového rozpětí, nikoli obsahově logicky. Díl lze uzavřít i v případě, že typový spis nebo jeho součást, do kterých patří, zůstává dlouhodobě otevřen. K dokumentům v dílu lze přistupovat bez ohledu na to, zda je díl otevřený nebo uzavřený. Každá součást musí obsahovat alespoň jeden díl. Spisy je možné zařadit do dílu (a tedy do typového spisu) prostřednictvím pevných křížových odkazů. Díl je zařazován do výběru archiválií jako celek.

Doba konfigurace
Doba konfigurace je časový úsek v životním cyklu elektronického systému spisové služby, ve kterém je tento systém instalován a ve kterém jsou stanoveny jeho parametry.

Dokument
Dokumentem je každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové nebo digitální, která byla vytvořena původcem nebo byla původci doručena [§ 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, (dále jen „zákon“)].
Dokument tvoří jedna nebo více komponent (například průvodní dopis má připojeny přílohy). Dokument vytvořený původcem vzniká jako koncept a do okamžiku přidělení evidenčního čísla existuje v eSSL jako rozpracovaný dokument.
Dokument lze zaznamenat na jakémkoliv médiu a v jakémkoli datovém formátu.

Elektronická spisovna
Elektronickou spisovnou je funkční složka elektronického systému spisové služby určená k ukládání, vyhledávání a předkládání dokumentů pro potřebu původce a k provádění skartačního řízení.

Elektronický
Pojem „elektronický“ se pro účely národního standardu používá obdobně jako pojem „digitální“. Analogové nahrávky, i když je lze považovat za elektronické, však nejsou pro účely národního standardu považovány za „elektronické“, neboť je nelze jako takové spravovat prostředky výpočetní techniky; za tímto účelem je nutné je převést (konvertovat) do digitální podoby. Podle zásad užití požadavků stanovených národním standardem lze analogové nahrávky ukládat pouze jako dokumenty v analogové podobě (fyzické dokumenty).

Elektronický dokument
Elektronický dokument je jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka [čl. 3 bod 35 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014

o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES].

Elektronický systém spisové služby
Elektronický systém spisové služby (dále jen „eSSL“) je informační systém určený ke správě dokumentů ve smyslu ustanovení § 2 písm. l) zákona, s využitím § 63 odst. 3 a 4 téhož zákona. Může se jednat o funkční součást informačního systému spravujícího dokumenty, která plní úkoly stanovené zákonem.

Entita
Entitou se rozumí objekt spravovaný eSSL, mezi entity patří věcné skupiny, spisy, typové spisy, součásti, díly, rozpracované dokumenty a dokumenty.

Evidence dokumentů
Evidence dokumentů (dále jen „ED“) je nezbytný nástroj umožňující přehledné odborné vedení spisové služby. ED je vedena v eSSL přírůstkovým způsobem v souladu s právním předpisem upravujícím podrobnosti výkonu spisové služby.

Export
Export je proces vytvoření repliky elektronických seskupení a dokumentů spojený s vytvořením metadat těchto seskupení a dokumentů nebo proces vytvoření repliky transakčního protokolu, a to za účelem převedení vzniklé repliky do jiného systému. Exportovaná seskupení, dokumenty a transakční protokol zůstávají zachovány v původním eSSL, nejsou tedy na rozdíl od přenosu bezprostředně po jeho realizaci smazány. Úspěšný export do digitálního archivu je doplněn záznamem příslušného jednoznačného identifikátoru digitálního archivu do metadat.

Fyzická složka
Fyzická složka je jednotka pro ukládání fyzických rozpracovaných dokumentů a fyzických dokumentů.

Historie entity
Historie je záznam o životním cyklu entity, která je vyjádřena údaji zaznamenávanými v metadatech entity. Tyto údaje deklarují kontinuálním způsobem nakládání s entitou při výkonu spisové služby.

Hlavička metadat
Hlavička metadat je podmnožina metadat pro entitu, která zůstane zachována po zničení nebo přenosu entity. Hlavička metadat je dokladem, že předmětná entita existovala a byla spravována eSSL.

Identifikace spisu a typového spisu
Identifikace spisu je evidenčním znakem spisu nebo typového spisu v rámci ED. Je jím spisová značka nebo, v případě, že tato není použita, je jím znak, který je konstruován na základě čísla jednacího dokumentu (například z jednacího čísla iniciačního dokumentu, prvního dokumentu). U typových spisů je tímto evidenčním znakem název typového spisu. V jedné věcné skupině určené pro typové spisy se název typového spisu tvoří jednotným způsobem.

Informační systém spravující dokumenty
Informační systém spravující dokumenty (dále jen „ISSD“) je jakýkoli elektronický systém obsahující komponenty. V případě ED v samostatných evidencích podle právního předpisu upravujícího podrobnosti výkonu spisové služby musí splňovat požadavky na eSSL podle tohoto standardu nebo dokumenty a jejich metadata ukládat v eSSL, který je splňuje. V případě vedení ED v samostatných ED se jedná o ISSD.

Jediná (jedna) operace
Posloupnost činností aplikace vyvolaná jedním iniciačním úkonem uživatele.

Jednoduchý spisový znak
Jednoduchý spisový znak je označení věcné skupiny nebo součásti typového spisu, které ji odlišuje od jiné věcné skupiny zařazené pod stejnou mateřskou věcnou skupinu. Doplněním jednoduchého spisového znaku o jednoduché spisové znaky všech nadřazených věcných skupin vzniká spisový znak.

Jednoznačný identifikátor
Jednoznačný identifikátor je znak pevně spojený s entitou zajišťující jeho nezaměnitelnost a jedinečnost. Každá entita v eSSL je označena jednoznačným identifikátorem, kterým je údaj v metadatech. V případě dokumentu tento identifikátor plní funkci jednoznačného identifikátoru ve smyslu § 64 odst. 2, nebo odst. 3 zákona. Jednoznačný identifikátor obsahuje vždy označení původce, popřípadě zkratku označení původce, a to ve formě alfanumerického kódu.

Klíčové slovo
Klíčové slovo je identifikátor specifického významu, který v podmínkách výkonu spisové služby v elektronické podobě představuje volitelná metadata určená k popisu obsahu věcných skupin, spisů, typových spisů**,** součástí nebo dokumentů, nikoli však dílů. Klíčová slova se zpravidla vybírají nebo ověřují podle číselníku nebo jsou automaticky přiřazována eSSL.

Komponenta
Komponentou v digitální podobě se rozumí jednoznačně vymezený proud bitů tvořící počítačový soubor. V analogové podobě je komponentou dále nedělitelná část dokumentu (průvodní dopis, příloha). Komponenta, popřípadě skupina komponent, vytváří rozpracovaný dokument nebo dokument.

Koncept
Koncept je rozpracovaný dokument přijatý do eSSL, který se využívá pro prvotní zaznamenání informace při tvorbě dokumentu (je vytvořen původcem). Je opatřen jednoznačným identifikátorem a může existovat ve verzích.

Konverze
Konverze je proces transformace jedné nebo více komponent do jiného formátu. Výsledkem konverze je ztvárnění.

Křížový odkaz
Křížový odkaz je vazba mezi spisy, mezi spisy a díly typových spisů, mezi dokumenty a mezi spisy a dokumenty. Pevný křížový odkaz zajišťuje spojení entit, které nelze bez uvedení důvodu odstranit, a přihlíží se k němu při exportu a přenosu. V případě

volného křížového odkazu se jedná o informační vazbu, která nemá vliv na tímto odkazem spojené entity a práci s nimi.

Metadata
Metadaty se rozumí data popisující souvislosti, obsah a strukturu dokumentů a jejich správu v průběhu času [§ 2 písm. o) zákona].

Objekt
Objektem se rozumí informace nebo skupina informací tvořících jednotný celek bez ohledu na typ nebo datový formát. Každá entita je objektem, ale ne každý objekt je entitou.

Odborná prohlídka
Odbornou prohlídkou se rozumí souhrn odborných činností, jejichž cílem je posoudit, zda dokumenty mají nebo nemají trvalou hodnotu, tedy zda mají být předány k trvalému uložení do příslušného archivu nebo určeny ke zničení. Odbornou prohlídku provádí zaměstnanec příslušného archivu na základě předloženého skartačního návrhu.

Oprávněný uživatel
Oprávněným uživatelem je uživatel eSSL, který je pověřen k provedení operace náležející k výkonu spisové služby na základě pravidel původce, popisovaných v kontextu spisové služby. Různí uživatelé mohou mít rozdílná oprávnění.

Otevření
Otevřením se rozumí proces umožňující vkládání entit do jiných entit. Nejčastěji jde o vkládání dokumentů do seskupení. Tento proces se netýká komponent.

Označování
Označování je jedním z úkonů výkonu spisové služby, kterým se rozumí přiřazování jednoznačného identifikátoru k dokumentu při zahájení jeho příjmu.

Posuzovatel skartační operace
Posuzovatel skartační operace je správcovská role, jejíž nositel je zodpovědný za provedení procesu výběru archiválií vůči vedení původce. Posuzovatel skartační operace je určen ve vnitřním předpisu původce.

Poštovní klient
Poštovní klient je počítačový program umožňující zpracovávat zprávy elektronické pošty.

Pozastavení skartační operace
Pozastavení skartační operace je úkon, kterým je entita dočasně vyřazena ze skartačního řízení, čímž je zabráněno jejímu zničení nebo přenosu.

Profil
Pojmem profil se rozumí souhrn oprávnění přidělených v eSSL uživateli, správci nebo skupině uživatelů.

Přenos
Přenos je proces přemístění entit spolu s jejich metadaty do jiného systému. Účelem přenosu je zejména převést vybrané dokumenty do externí elektronické spisovny**,** digitálního archivu nebo externího eSSL (spisová rozluka). Přenos probíhá ve čtyřech etapách

a) export repliky entit se všemi příslušnými metadaty,
b) export transakčních protokolů,
c) následné zničení komponent exportovaných dokumentů (pokud nemají křížové odkazy na entity, které nepodléhají přenosu),
d) následné zničení metadat přenesených entit s výjimkou hlavičky metadat.

Příjem
Příjem je úkonem odborné správy dokumentů, jímž se přijímá rozpracovaný dokument nebo dokument do eSSL nebo se rozpracovaný dokument deklaruje jako dokument. Obsahem příjmu jsou také procesy spojené s uložením a zatříděním dokumentu v eSSL, zejména jeho označení, evidence, přidání metadat a zatřídění v rámci spisového plánu.

Role
Role je souhrn funkčních oprávnění udělených předem stanovenému uživateli nebo skupině uživatelů eSSL.

Redakce
Redakce je úprava dokumentů obsahující proces skrytí určitých informací v dokumentu (například na základě právní povinnosti), zpravidla zahrnující zakrytí osobních údajů, utajovaných informací, informací označených jako důvěrné, nebo zakrytí části dokumentu, která není potřebná pro další využití repliky dokumentu apod. Ve všech případech není ovlivněn původní dokument v digitální podobě jako celek. Úprava redakcí se provádí v replice dokumentu v digitální podobě, která se označuje jako „výtah“.

Seskupení
Seskupení je společným názvem pro entity věcná skupina, spis, typový spis, součást a díl. Vkládání dokumentů je možné do seskupení věcná skupina, spis a díl.

Schvalovatel
Schvalovatel je osoba nebo role v eSSL odpovědná v rámci svých oprávnění udělených původcem za obsah dokumentu nebo seskupení. Jedná se o osobu, která dokument podepisuje zpravidla podle vnitřního předpisu původce.

Skartační operace
Skartační operace je úkon odborné správy dokumentů, při kterém je ve skartačním řízení uplatněn skartační režim.

Skartační režim
Skartační režim je původcem stanovený systém vyřazování entit, který vymezuje dobu jejich ukládání (skartační lhůta) a určuje typ skartační operace (skartační znak: A – návrh na trvalé uložení, V – předložení k přezkumu, S – zničení), popřípadě z roku zařazení dokumentu do skartačního řízení a jiné skutečnosti, kterou veřejnoprávní

původce stanoví jako spouštěcí událost. Při posouzení se v rámci odborné prohlídky vyhodnocují

a) metadata,
b) obsah dokumentu, nebo
c) metadata a obsah dokumentu.

V případě, že skartační režim uplatňuje veřejnoprávní původce zřizující správní archiv podle § 69 odst. 1 zákona, nepovažuje se předání dokumentů ze spisovny do správního archivu podle § 69 odst. 4 zákona za skartační operaci a lhůta stanovená pro uložení dokumentů ve spisovně ve spisových řádech není skartační lhůtou; pro převod dokumentu mezi spisovnami (například po odtajnění spisu) platí část věty před středníkem obdobně.

Skupina uživatelů
Skupinou uživatelů se rozumí souhrn fyzických osob užívajících eSSL, kterým byly přiděleny stejné role.

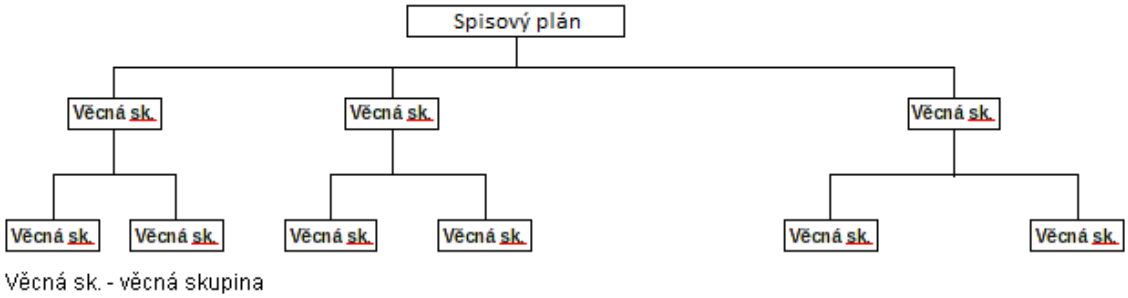
Smazání
Smazáním se rozumí proces vyloučení entit z dalšího zpracování v eSSL. V případě vyloučení entit z dalšího zpracování jsou entity dále uchovány v eSSL v nezměněné podobě s doprovodným zápisem v metadatech, ale pro uživatelské role jsou tyto entity nepřístupné, jako by byly z eSSL přeneseny nebo zničeny.

Součást
Součást je logická část typového spisu. Každá součást je pojmenována a použita prostřednictvím jejího dílu k uložení stanoveného druhu nebo stanovených okruhů dokumentů, jako jsou například „pracovní skupina WP1“ nebo „daňová přiznání“. Každý typový spis obsahuje alespoň jednu součást.

Spis
Spis je entita, v níž jsou organizovány dokumenty vztahující se ke stejnému předmětu (věci). Spisy se vyskytují pouze ve věcných skupinách, které neobsahují jiné věcné skupiny nebo typové spisy.

Spisová značka
Spisová značka je evidenčním znakem spisu (identifikací spisu), pokud tak stanoví jiný právní předpis nebo interní předpis původce. Příkladem je spisová značka podle správního řádu nebo spisová značka soudního spisu (podle kancelářského řádu soudů). Spisovou značkou je zejména číslo jednací sběrného archu, iniciačního nebo jiného původcem určeného dokumentu vloženého ve spisu, popřípadě jiné označení, které původce pro své účely obvykle užívá nebo je z jiných důvodů považuje za účelné. Funkci spisové značky u typového spisu plní jeho název**.**

Spisový plán
Spisovým plánem se rozumí hierarchické uspořádání věcných skupin.



Obrázek č. 1 – schéma spisového plánu

Spisový a skartační plán
Spisovým a skartačním plánem se rozumí spisový plán doplněný o skartační režimy.

Spisový znak
Spisový znak je označení věcné skupiny nebo součásti typového spisu. Spisový znak je označení věcné skupiny, které určuje její jednoznačné místo v hierarchii spisového plánu prostřednictvím dědění spisových znaků mateřských věcných skupin. Je tvořen jednoduchým spisovým znakem v hierarchii nejvýše postavené věcné skupiny a jednoduchými spisovými znaky věcných skupin níže ležících v hierarchii spisového plánu až do dosažení nejbližší mateřské věcné skupiny. Spisové znaky jsou jednoznačné v rámci hierarchického spisového plánu, zatímco jednoduché spisové znaky jako takové jsou jednoznačné jen v rámci konkrétní mateřské věcné skupiny.
Spisový znak má také součást typového spisu, její spisový znak tvoří označení příslušné věcné skupiny určené pro vkládání typových spisů a jednoduchý spisový znak součásti.

Spouštěcí událost
Spouštěcí událostí se rozumí kritéria, kterými je stanoven začátek plynutí skartační lhůty. Spouštěcí událost je – pokud jí není vyřízení dokumentu nebo uzavření spisu – vyjádřena ve spisových a skartačních plánech, a to obvykle poznámkou.

Správce
Správce je fyzická osoba, která je uživatelem eSSL a byla jí přidělena zvláštní oprávnění. Správce je odpovědný za chod spisové služby u původce. U velkých původců mohou být úkoly a oprávnění přidělované k zajištění spisové služby správcům rozděleny mezi několik fyzických osob (pracovní zařazení „administrátor eSSL“, „vedoucí spisové služby“, „referent spisové služby“ apod.).

Správcovská role
Správcovskou rolí se rozumí souhrn funkčních oprávnění přidělených fyzickým osobám, které mohou vykonávat jeden nebo více úkonů náležejících správci eSSL.

Transakční protokol
Transakční protokol je důvěryhodný zápis informací o operacích provedených v eSSL, které ovlivnily nebo změnily entity nebo eSSL. Tyto informace umožňují dohledání, identifikaci, rekonstrukci a kontrolu těchto operací, stavu entit v minulosti a činnosti uživatelů.

Třídění
Tříděním se rozumí systematická klasifikace dokumentů do seskupení v souladu se spisovým řádem a spisovým a skartačním plánem, prováděná při výkonu spisové služby.

Typ dokumentu
Typem dokumentu se rozumí věcná charakteristika popisující dokument. Konkrétní charakteristika umožňuje eSSL, aby spravoval dokumenty stejného typu (konkrétní charakteristiky) shodně a stanoveným, určitým způsobem bez ohledu na jejich zařazení do seskupení. Typem dokumentu jsou například „faktury“, „smlouvy“ nebo „webové stránky“.

Typový spis
Typový spis je soubor dokumentů s předem stanovenou strukturou, členěný na věcné, podle obsahu stanovené součásti, které jsou dále členěny na díly, do kterých se zatřiďují dokumenty nebo vkládají křížové odkazy na spisy. Typový spis se týká jedné nebo více agend. Základním odlišujícím znakem typových spisů je skutečnost, že příslušný typový spis je vždy výsledkem stejnorodých opakujících se procesů (například stavební spisy budov, zdravotnická dokumentace, personální spisy), má obdobný obsah nebo strukturu. K dalším znakům typových spisů patří skutečnost, že

a) mají předvídatelnou strukturu svého obsahu,
b) jsou početné,
c) používají se a jsou spravovány v rámci známého a předem stanoveného procesu**,**
d) jejich označení názvem nemá vazbu na ED.

Uzavření
Uzavřením se rozumí proces změny atributů spisu, typového spisu**,** součásti nebo dílu, který se projeví v metadatech, v jehož důsledku je znemožněno vkládání dalších dokumentů nebo vyjímání dokumentů stávajících. Pro vkládání spisů pomocí pevných křížových odkazů platí omezení na uzavřené spisy obdobně. Současně se dokumenty zatříděné do spisu nebo dílu převedou do výstupního datového formátu.

Uživatel
Uživatelem je každá fyzická osoba používající eSSL. Uživatel má v rámci svého uživatelského profilu přiděleny role a může být členem skupin uživatelů se stejnou uživatelskou rolí.

Uživatelská role
Uživatelská role je souhrn funkčních oprávnění udělených uživatelům, kteří mohou vykonávat činnost týkající se odborné správy dokumentů. Uživatel může mít několik uživatelských rolí, ale jenom jeden uživatelský profil.

Věcná skupina
Věcná skupina je entita spisového plánu označující část jeho hierarchie a je identifikována spisovým znakem. Věcná skupina odpovídá položce spisového plánu (obrázek č. 1) a obsahuje jiné věcné skupiny, dokumenty, spisy nebo typové spisy. Věcná skupina obsahující typové spisy nebo jinou věcnou skupinu nemůže obsahovat odlišnou entitu.

Verze
Verzí je číselné nebo slovní označení vývoje stavu rozpracovaného dokumentu (stadia konceptu) v určité fázi jeho životního cyklu. Verzí je zpravidla jeden z rozpracovaných dokumentů. V některých případech dokončené rozpracované dokumenty existují v několika verzích (například připomínky k textu více uživateli). Národní standard používá pojem verze výlučně ve vztahu k rozpracovanému dokumentu, tj. konceptu.

Vlastník (držitel)
Vlastníkem (držitelem) dokumentů nebo seskupení je osoba nebo organizační součást původce, v jejichž držení se dokumenty nebo seskupení nacházejí. Pojem „vlastník (držitel)“ používaný v národním standardu nelze užívat obdobně jako pojem „vlastník“ ve smyslu občanského práva.

Vyhledávání
Vyhledávání je proces identifikace dokumentů nebo spisů pomocí uživatelsky definovaných parametrů za účelem lokalizace, zpřístupnění a výběru dokumentů, věcných skupin, spisů, součástí, dílů nebo jejich metadat.

Výtah
Výtahem dokumentu se rozumí replika dokumentu, ve které byla provedena redakce.

Vytištění
Vytištěním se rozumí operace spojené s vyhotovením listinné podoby dokumentu v digitální podobě.

Webová služba
Webová služba je nástroj umožňující komunikaci a výměnu informací prostřednictvím sítě Internet.

Zásilka
Zásilka je prostředek pro doručování dokumentů v analogové nebo digitální podobě. Zásilkou je nejčastěji listinná obálka, datová zpráva z informačního systému datových schránek, e-mail, optický disk nebo flash disk.

Znázornění
Znázorněním je uživatelsky srozumitelná interpretace dokumentu nebo rozpracovaného dokumentu v digitální podobě. Znázornění má zpravidla podobu zobrazení na obrazovce, tiskového výstupu, zvukové nebo multimediální prezentace.

Zničení
Zničením se rozumí proces likvidace entit, který znemožňuje jejich rekonstrukci a identifikaci jejich obsahu.

Ztvárnění
Ztvárněním se rozumí výsledek konverze nebo převedení dokumentu, kterým je vyjádřena transformace dokumentu nebo komponenty při použití jednoho nebo více formátů odlišných od původních formátů. Ztvárnění se zpravidla vytvářejí pro uchování dokumentů v digitální podobě za účelem minimalizace rizika ztráty přístupu k jejich obsahu v čase. Například dokumenty vyhotovené v proprietárním datovém formátu musí být uloženy jako ztvárnění ve výstupním datovém formátu stanoveném

prováděcím právním předpisem upravujícím podrobnosti výkonu spisové služby (například PDF/A). Výsledkem konverze dokumentu je ztvárnění některých nebo všech jeho komponent. Po konverzi může mít dokument stejný nebo rozdílný počet komponent jako před jejím provedením. Ztvárněna jako dokument mohou být také metadata nebo transakční protokol.

2 PŘÍJEM A EVIDENCE DOKUMENTŮ

2.1 Příjem

Dokumenty vytvořené původcem vznikají (jsou do eSSL přijaty) jako rozpracované dokumenty (koncepty). Jedná se o jednu nebo více komponent opatřených metadaty. Jedna nebo více verzí rozpracovaného dokumentu jsou deklarovány jako dokument.

Příjem dokumentů je zahajován po doručení prostřednictvím různých komunikačních kanálů: elektronické pošty, datové schránky, prostřednictvím elektronického formuláře z portálu, faxu, provozovatele poštovních služeb, doručených osobně. Příjem zahrnuje vedle správy rozpracovaných dokumentů i jejich deklaraci dokumenty zaevidováním v ED a zatřídění v rámci spisového plánu.

Číslo	Požadavek	Původně
2.1.1	eSSL spravuje rozpracované dokumenty a dokumenty v rámci stejného spisového plánu a s použitím stejných mechanismů kontroly přístupu. *Účelem tohoto požadavku je umožnit uživatelům ukládat a spravovat rozpracované dokumenty v eSSL stejným způsobem jako dokumenty.*	10.3.1 D upraveno
2.1.2	eSSL umožňuje uživatelům spravovat rozpracovaný dokument a deklarovat jej jako dokument v rámci jedné operace. Každý rozpracovaný dokument musí být deklarován jako dokument nejpozději v okamžiku jeho vyřízení, a to i v případě vyřízení rozpracovaného dokumentu zamítnutím.	10.3.6 upraveno
2.1.3	eSSL umožňuje kopírovat obsah dokumentu v digitální podobě za účelem vytvoření nového samostatného rozpracovaného dokumentu bez potřeby automaticky vytvořit nový dokument a se zárukou zachování nezměněného původního dokumentu.	10.3.7
2.1.4	eSSL umožňuje uživatelským rolím předat jakýkoli rozpracovaný dokument, ke kterému mají přidělena přístupová práva.	10.3.8
2.1.5	eSSL umožňuje uživatelským rolím převzít jakýkoli rozpracovaný dokument, který jim byl předán, a umožnit uživateli volbu převzít nebo nepřevzít rozpracovaný dokument jako jeho novou verzi (požadavek 2.1.7).	10.3.9 D
2.1.6	eSSL umožňuje správcovské roli nebo uživateli, který rozpracovaný dokument předal, aby jeho předání zrušil, pokud nebyl již převzat.	10.3.13 D
2.1.7	eSSL automaticky čísluje verze. Pokud je rozpracovaný dokument přihlášen jako nová verze, číslo verze se zvýší o jednu oproti verzi předchozí.	10.3.20 D
2.1.8	eSSL umožňuje uživateli zapsat hodnoty metadat pro dokument již v době příjmu rozpracovaného dokumentu.	10.3.24 upraveno
2.1.9	eSSL zajišťuje, aby každý přijatý prvek metadat byl spravován v souladu s požadavky národního standardu a prováděcího právního předpisu upravujícího podrobnosti výkonu spisové služby.	10.3.25
2.1.10	eSSL spravuje různé verze rozpracovaného dokumentu jako	10.3.29

	jedinou entitu.	
2.1.11	Proces příjmu v eSSL zahrnuje jeho kontrolu a umožňuje uživatelům a) přijímat beze změny obsahu dokumenty a rozpracované dokumenty v digitální podobě bez ohledu na jejich datový formát, metodu kódování nebo jiné technické charakteristiky, b) zajistit spojení dokumentů a rozpracovaných dokumentů se spisovým plánem, c) zajistit vložení dokumentů a rozpracovaných dokumentů do jednoho spisu, jednoho dílu nebo do jedné věcné skupiny. *Proces příjmu neznamená, že eSSL vždy umožňuje znázornění dokumentů všech možných formátů.*	6.1.1
2.1.12	eSSL nezavádí jakákoli omezení počtu dokumentů nebo rozpracovaných dokumentů, které lze přijmout do věcné skupiny, spisu nebo dílu, ani počtu dokumentů nebo rozpracovaných dokumentů, které je možné uložit v eSSL.	6.1.2
2.1.13	Pokud je přijat dokument složený z několika komponent, eSSL přijme všechny jeho komponenty.	6.1.3
2.1.14	Pokud je přijat dokument složený z několika komponent, eSSL dokument spravuje jako jedinou entitu tak, aby byly zachovány vztahy mezi komponentami a aby byla uchována struktura dokumentu. *Příkladem takových dokumentů je e-mailová zpráva s přílohami různých formátů nebo do textu odkazem napojený obrázek umístěný v jiném souboru.*	6.1.4 upraveno
2.1.15	eSSL při příjmu komponenty dokumentu automaticky identifikuje její datový formát a příslušnou verzi formátu; tyto informace ukládá do metadat komponenty. eSSL a) vede seznam datových formátů, které mohou být identifikovány, b) vychází z odkazů na existující registr datových formátů (zpravidla na ten, který byl navržen pro podporu dlouhodobého uchovávání dokumentů). *Takovým registrem je například PRONOM (www.nationalarchives.gov.uk/PRONOM/).*	6.1.7
2.1.16	eSSL umožňuje uživatelům přijmout dokument v digitální podobě i v případě, že aplikace použitá k jeho vytvoření se v prostředí eSSL nevyužívá. *Například jako přílohu e-mailu eSSL přijme komponentu tvořenou formátem vektorové grafiky, aniž by uživatel měl přístup k aplikaci pro její znázornění*.	6.1.10
2.1.17	eSSL přijímá metadata popisující dokumenty, pokud tato odpovídají metadatům stanoveným schématy XML v příloze.	6.1.11
2.1.18	eSSL přijímá všechny metadatové prvky specifikované ve svém	6.1.13

	nastavení a zajistí jejich uchovávání ve spojení s dokumentem v digitální podobě.	
2.1.19	eSSL zajišťuje, aby hodnoty některých prvků metadat dokumentu v digitální podobě mohly být aktualizovány oprávněnými uživateli nebo správcovskou rolí v souladu s požadavky uvedenými v kapitole 11.	6.1.15
2.1.20	eSSL zajišťuje, aby všechny dokumenty byly přiřazeny alespoň k jedné věcné skupině, spisu, popřípadě dílu typového spisu.	6.1.16
2.1.21	eSSL zaznamenává datum a čas příjmu rozpracovaného dokumentu nebo příjmu dokumentu jak ve formě metadat, tak zápisem do transakčního protokolu.	6.1.19
2.1.22	eSSL umožňuje zobrazit na obrazovce u každého přijatého rozpracovaného dokumentu nebo dokumentu metadata, včetně těch, která byla stanovena v době konfigurace eSSL. Metadata stanovená v době konfigurace mohou obsahovat všechny nebo pouze některé prvky stanovené požadavky uvedenými v kapitole 11.	6.1.20
2.1.23	eSSL zajišťuje, aby u každého přijatého dokumentu byla přítomna veškerá metadata, která národní standard stanoví jako povinná.	6.1.21
2.1.24	eSSL při příjmu každého dokumentu automaticky vyzve uživatele, aby doplnil veškerá požadovaná metadata, která nebyla přijata automaticky.	6.1.22
2.1.25	eSSL podporuje přiřazení více klíčových slov ke každému spisu, typovému spisu**,** součásti a dokumentu.	6.1.23
2.1.26	eSSL umožňuje vytvoření více než jedné entity s použitím stejné kombinace klíčových slov.	6.1.25
2.1.27	eSSL umožňuje výběr nebo ověřování klíčových slov a hodnoty jiných prvků metadat podle číselníků.	6.1.28
2.1.28	eSSL umožňuje zápis dalších popisných a jiných metadat v době příjmu, nebo také kdykoliv později (v pozdějším stadiu zpracování).	6.1.29
2.1.29	Pokud má uživatel v eSSL rozpracovaný dokument, který je ve více než jedné verzi, eSSL mu umožní výběr alespoň jedné z následujících možností: a) určit všechny verze jako jeden dokument, b) určit jednu stanovenou verzi jako dokument, c) určit každou verzi jako samostatný dokument. Verze, které nejsou deklarovány jako dokument, nejsou dále předmětem výkonu spisové služby. Dokument musí být zaevidován v ED (kapitola 2.7).	6.1.32 upraveno
2.1.30	eSSL umožňuje ukončení procesu příjmu rozpracovaného dokumentu nebo dokumentu více než jedním uživatelem, tedy rozdělení příjmu mezi více uživatelů. *Realizace požadavku znamená, že jeden uživatel zavede některá metadata a předá dokument nebo* rozpracovaný dokument *jinému uživateli, který zavede zbývající metadata a dokument nebo* rozpracovaný dokument *zatřídí*.	6.1.34 D
2.1.31	Při příjmu rozpracovaného dokumentu nebo dokumentu eSSL umožňuje uživateli před dokončením příjmu v jeho rámci a) procházet spisový plán s cílem najít příslušnou věcnou	6.1.44 D

	skupinu, b) znázornit metadata (oprávnění, klíčová slova, popisy apod.) zvolených věcných skupin, spisů, typových spisů a součástí.	
2.1.32	eSSL zaznamená do metadat komponenty dokumentu a do transakčního protokolu a) hash komponenty, b) označení použitého hashovacího algoritmu.	6.1.45
2.1.33	eSSL lze konfigurovat tak, že při zahájení příjmu automaticky předá dokument nebo jeho stanovenou část stanovenému ISSD postupem popsaným v příloze 9.	

2.2 Správa e-mailů

Číslo	Požadavek	Původně
2.2.1	Pokud je e-mailová zpráva přijata, eSSL uchová její hlavičku.	6.3.1
2.2.2	eSSL podporuje příjem e-mailových zpráv takovým způsobem, aby příjem mohl provést uživatel v rámci jedné operace bez toho, že by musel samostatně obsluhovat poštovního klienta, a samostatně eSSL.	6.3.2
2.2.3	eSSL podporuje příjem e-mailových zpráv do eSSL včetně jejich příloh jako dokumentů a automaticky vyjímá následující metadata, pokud jsou tyto údaje obsaženy v hlavičce e-mailové zprávy: a) datum a čas odeslání e-mailové zprávy, b) adresát (adresáti), c) adresát (adresáti) případné kopie, d) předmět (věc), e) odesílatel e-mailové zprávy, f) připojený elektronický podpis nebo elektronická pečeť a kvalifikované elektronické časové razítko, g) jméno kvalifikovaného poskytovatele služeb vytvářejících důvěru.	6.3.5
2.2.4	eSSL automaticky zapíše do metadat e-mailovou adresu (například „xy@seznam.cz“) i přiřazené jméno a příjmení, pokud jsou přítomny (například „Jan Novák“).	6.3.18
2.2.5	eSSL umožňuje uživateli, který přijímá e-mailovou zprávu, upravit položku předmět (věc) dokumentu automaticky vyjmutou z hlavičky e-mailové zprávy podle požadavku 2.2.3.	6.3.11
2.2.6	eSSL umožňuje ruční zavedení metadat s informační hodnotou „datum odeslání“ a „datum přijetí“ uživatelem. V konfiguraci eSSL lze tuto funkci vyřadit.	6.3.14
2.2.7	Uživateli je umožněno přijmout do eSSL jedinou operací několik manuálně vybraných e-mailových zpráv jako a) jeden dokument, nebo b) několik dokumentů – jednotlivé došlé e-mailové zprávy samostatně, a to na základě volby uživatele.	6.3.15
2.2.8	eSSL umožňuje uživateli, který přijímá e-mailovou zprávu v proprietárním formátu, uložit ji ve více datových formátech, včetně	6.3.17 upra-ve-

	otevřeného a výstupního.	no

2.3 Skenování a konverze

Při implementaci eSSL musí být přihlíženo k povinnosti uložené zákonem, a sice k povinnosti vykonávat spisovou službu v elektronické podobě v elektronických systémech spisové služby podle § 63 odst. 3 zákona. Prováděcí právní předpis upravující podrobnosti výkonu spisové služby stanoví, že zpravidla (tedy ne vždy) musí být realizován převod dokumentů v analogové podobě do podoby digitální. To se děje třemi způsoby:

a) autorizovanou konverzí dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů; výstup této konverze má stejné právní účinky jako dokument, jehož převedením výstup vznikl,
b) převodem dokumentu dle § 69a zákona; výstup převodu dokumentu má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl,
c) prostým skenováním; výstup prostého skenování nemá žádné právní účinky.

Skenovací funkce eSSL je zpravidla realizována externím zařízením; požadavky na skenovací funkci eSSL jsou v tomto případě požadavky na toto zařízení.

Číslo	Požadavek	Původně
2.3.1	Skenovací funkce eSSL podporuje oba způsoby snímání, tedy černobílý i barevný.	6.5.2
2.3.2	Skenovací funkce eSSL ukládá snímky ve výstupních datových formátech uvedených v právním předpisu upravujícím podrobnosti výkonu spisové služby.	6.5.3
2.3.3	Skenovací funkce eSSL ukládá snímky s použitím různých rozlišení.	6.5.4
2.3.4	Skenovací funkce eSSL pracuje se standardními velikostmi papíru, zejména velikostí A4 nebo A3 (podle ČSN EN ISO 216).	6.5.6
2.3.5	Skenovací funkce eSSL po nasnímání dokumentů pro účely jejich dalšího zpracování všechny snímky automaticky odešle do dočasného úložiště naskenovaných dokumentů v řazení podle pořadí jejich zpracování.	6.5.11
2.3.6	eSSL umožňuje provést hromadný import sady naskenovaných snímků a jejich metadat.	6.5.21 D
2.3.7	eSSL umožňuje uživatelům přijímat naskenované snímky jako komponenty dokumentu.	6.5.23
2.3.8	eSSL zajistí provedení převodu dokumentu podle zákona.	
2.3.9	eSSL identifikuje datový formát komponenty a v případě, že se nejedná o výstupní datový formát podle prováděcího právního předpisu upravujícího podrobnosti výkonu spisové služby a) změní datový formát na výstupní v případě statických textových dokumentů, statických kombinovaných textových a obrazových dokumentů, statických obrazových dokumentů, dynamických obrazových dokumentů, zvukových dokumentů a databází,	

	b) nezmění datový formát v případě dokumentů neuvedených v písm. a).	
2.3.10	Jestliže eSSL využívá pro převod dokumentu nebo pro změnu datového formátu externí systém, musí s ním být funkčně propojen.	
2.3.11	eSSL připojí k výstupu převodu dokumentu nebo změny datového formátu ke každé komponentě ověřovací doložku obsahující informace uvedené v prováděcím právním předpisu upravujícím podrobnosti výkonu spisové služby.	
2.3.12	eSSL doložku výstupu podle požadavku 2.3.11 umožní podepsat osobě odpovědné za převedení nebo změnu datového formátu kvalifikovaným elektronickým podpisem nebo eSSL zapečetí doložku výstupu kvalifikovanou elektronickou pečetí a dále doložku eSSL opatří kvalifikovaným elektronickým časovým razítkem.	

2.4 Datové schránky

Podle ustanovení § 17 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, jsou orgány veřejné moci povinny doručovat dokumenty, jejichž povaha to umožňuje, prostřednictvím datových schránek, pokud není doručováno na místě.

V této kapitole stanovené požadavky se vztahují výlučně na vazbu informačního systému datových schránek (dále jen „ISDS“) ke zpracování datových zpráv v eSSL, tedy nikoliv na požadavky pro provozování datové schránky.

Číslo	Požadavek	Původně
2.4.1	eSSL přijímá a odesílá dokumenty prostřednictvím ISDS.	6.6.1
2.4.2	eSSL umožňuje správcovské roli konfigurovat systém tak, aby využíval webových služeb ISDS podle požadavků uvedených v této kapitole.	6.6.2
2.4.3	eSSL zajišťuje přihlášení k ISDS při každé iniciaci webové služby ISDS včetně zachování přístupových oprávnění k datovým schránkám ve smyslu § 8 zákona č. 300/2008 Sb.	6.6.3
2.4.4	eSSL umožňuje uživatelské roli zprostředkování nalezení jiné datové schránky, než je datová schránka původce, a získání informace, že příslušná datová schránka není znepřístupněna.	6.6.4
2.4.5	eSSL zajistí při odesílání datové zprávy a) vytvoření datové zprávy podle pravidel stanovených pro tyto účely správcem ISDS; datová zpráva obsahuje dokumenty, ke kterým eSSL doplní stanovená metadata, b) zadání identifikátoru datové schránky adresáta; pokud není identifikátor datové schránky adresáta znám, pak jeho vyhledání v systému ISDS.	6.6.5
2.4.6	eSSL uloží identifikátor odeslané datové zprávy vytvořený ISDS do metadat dokumentu v eSSL.	6.6.6
2.4.7	eSSL zajišťuje stahování údajů z obálek datových zpráv a jejich uložení do metadat dokumentů zaslaných datovou zprávou v eSSL.	6.6.7 upraveno
2.4.8	eSSL zajišťuje a) stahování doručených datových zpráv,	6.6.8

	b) uložení stažených datových zpráv, c) označení stažených datových zpráv v ISDS příznakem, že byly staženy, d) ověření, zda obálka datové zprávy obsahuje údaj, že obsah datové zprávy je určen do vlastních rukou adresáta.	
2.4.9	eSSL zajišťuje, pokud obálka datové zprávy (zásilky) neobsahuje údaj, že obsah datové zprávy je určen do vlastních rukou adresáta, zahájení příjmu na základě metadat obsažených v datové zprávě.	6.6.9
2.4.10	eSSL umožní předat datovou zprávu (zásilku) příslušné fyzické osobě, pro kterou je v obálce datové zprávy vyznačeno určení do vlastních rukou.	6.6.10
2.4.11	eSSL umožňuje uživatelské roli zadat ISDS požadavek na vyhledání přehledu doručených a odeslaných datových zpráv (zásilek) za určené časové období, v rámci organizační součásti původce nebo v zadaném rozmezí pořadových čísel záznamů v ISDS.	6.6.11
2.4.12	eSSL automaticky zajistí stažení a uložení informace o dodání datové zprávy do datové schránky a o doručení datové zprávy (zásilky).	6.6.12

2.5 Elektronický podpis, elektronická pečeť a elektronické časové razítko

Národní standard v jednotlivých požadavcích důsledně pracuje s pojmy definovanými v zákonu č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Po dobu přechodného období je dle tohoto zákona možné užívat místo elektronické pečetě elektronickou značku.

Číslo	Požadavek	Původně
2.5.1	eSSL přijme a ověří platnost elektronického podpisu, elektronické pečeti a elektronického časového razítka, které jsou k doručenému dokumentu připojeny.	10.7.1
2.5.2	eSSL při ověření elektronického podpisu, elektronické pečeti a elektronického časového razítka v době příjmu zaznamená do metadat údaje stanovené prováděcím právním předpisem upravujícím podrobnosti výkonu spisové služby. *Informace o ověření je nutné uložit, protože později je nemusí být možné již získat (nebude možné provést ověření).*	10.7.2, 10.7.5 upraveno
2.5.3	eSSL ověřuje platnost elektronického podpisu a elektronické pečeti současně se zahájením příjmu dokumentu a umožňuje ověřit platnost po zahájení příjmu. Výsledek ověření eSSL uloží do metadat dokumentu.	10.7.4 D upraveno

2.6 Šifrování

Šifrování je postup použití komplexní transformace digitální komponenty tak, aby jej aplikace nemohla znázornit ve srozumitelné podobě bez použití odpovídajícího dešifrovacího algoritmu.

Číslo	Požadavek	Původně
2.6.1	eSSL v době příjmu dokumentu přijme a uloží informace o šifrování.	10.8.2
2.6.2	eSSL umožňuje konfigurovat funkci dešifrování, jestliže je nějaký dokument určen pro přenos, export, import nebo příjem. Tuto vlastnost konfiguruje správcovská role.	10.8.5
2.6.3	eSSL vždy odstraní šifrování při exportu entity do digitálního archivu.	10.8.7

2.7 Evidence dokumentů

ED slouží k zajištění evidenčních metadat ve spisové službě a navazuje na tradici evidenčních pomůcek v analogové podobě (zejména podací deník).

ED zajišťuje evidenci dokumentů, evidenci spisů a typových spisů, dále zaznamenává proces vyřízení spisů nebo dokumentů. Zaevidováním v ED je rozpracovaný dokument deklarován dokumentem.

ED stanoví požadavky na evidenční znaky (číslo jednací, identifikace spisu), které slouží k evidenci dokumentů, spisů a typových spisů, ale nenahrazují použití jednoznačného identifikátoru. ED ISSD stanoví požadavky na evidenční číslo ze samostatné ED.

Požadavky na ED ISSD jsou užší. V případě, že ED ISSD zajišťuje v evidenci z rozhodnutí původce větší rozsah údajů, použijí se požadavky na ED obdobně.
Dokumenty v analogové podobě společně existují s dokumenty v digitální podobě, pokud

a) spis nebo díl obsahuje pouze dokumenty v analogové podobě; v tomto případě je entita reprezentovaná fyzickou složkou na dokumenty (například spisová obálka) a v eSSL je evidována jejími identifikačními znaky; nebo
b) spis nebo díl obsahuje jak dokumenty v digitální podobě, tak dokumenty v analogové podobě; dokumenty v analogové podobě jsou uloženy odděleně od dokumentů v digitální podobě a nemusí být uloženy v žádné fyzické složce vhodné pro spisovou správu (například technické výkresy jako přílohy spisů mohou být uloženy přímo ve fyzickém depozitu).

Pro zajištění správy dokumentů v analogové podobě eSSL spravuje jejich metadata. Tato metadata umožňují správcovským a uživatelským rolím za podmínky platnosti kontroly přístupu vyhledávat, sledovat, vybrat, posuzovat, přenášet nebo zničit dokumenty v analogové podobě a přidělovat jim přístupová práva k dokumentům v analogové podobě stejným způsobem jako k dokumentům v digitální podobě.

Číslo	Požadavek	Původně
2.7.1	Každý dokument je evidován pod jedinečným pořadovým číslem v rámci určeného časového období. Každý dokument vytvoří spis, nebo je vložen do spisu, nebo do dílu v rámci součásti typového spisu, anebo přímo do věcné skupiny.	6.7.1
2.7.2	Dokumenty vložené přímo do věcné skupiny jsou evidovány pod číslem jednacím, které zahrnuje jedinečné pořadové číslo. Pokud je nutné, aby byl daný dokument vložen do spisu nebo do typového spisu, dokument je přetříděn.	6.7.2

2.7.3	V místě a čase doručení dokumentu se v podatelně do ED zaznamenají základní údaje zaručující jeho označení, tedy jednoznačný identifikátor vytvořený eSSL, datum doručení a zpravidla adresa odesílatele. Dále je a) dokument ihned zaevidován, a to tak, že je obsluhou podatelny vložen do spisu tvořeného sběrným archem, nebo je evidován s unikátním pořadovým číslem (požadavek 2.7.6), nebo b) dokument po označení předán přímo zpracovateli, který v rámci zpracování dokumentu zajistí i jeho evidenci. V případě, že pořadovým číslem byl omylem opatřen dokument, který měl být vložen do již existujícího spisu tvořeného formou sběrného archu, je společně s přetříděním opatřen číslem jednacím; jeho dosavadní číslo jednací zůstane uchováno v metadatech dokumentu a eSSL umožňuje v rámci ED jeho znázornění a vyhledávání podle tohoto čísla jednacího. *Zejména je nutné dbát na to, aby dokumenty patřící do spisu tvořeného formou sběrného archu nebyly opatřovány novým jedinečným pořadovým číslem. Vložení do místa hierarchie znamená, že je vytvořen nový spis (formou sběrného archu), nebo že je dokument vložen do stávajícího spisu, dílu, nebo do věcné skupiny.*	6.7.5 upraveno
2.7.4	eSSL umožňuje v ED evidovat údaje o dokumentech, spisech a typových spisech.	6.7.6
2.7.5	V ED se o dokumentu vedou podle právního předpisu upravujícího podrobnosti výkonu spisové služby tyto údaje: a) pořadové číslo dokumentu (požadavek 2.7.6), b) datum doručení dokumentu původci, c) údaje o odesílateli, d) doručené množství, e) stručný obsah dokumentu (předmět, věc), f) identifikace dokumentu provedená odesílatelem, g) označení organizační součásti, které je dokument přidělen k vyřízení, h) způsob vyřízení, i) identifikace adresáta vyřízení, j) datum odeslání, k) odesílané množství, l) identifikace vlastníka v případě dokumentů vložených přímo ve věcné skupině (požadavek 2.7.2), m) spisový znak, n) skartační režim, o) jednoznačný identifikátor dokumentu, p) informace o tom, zda jde o dokument v digitální podobě nebo dokument v analogové podobě, q) informace o zařazení dokumentu do výběru archiválií, r) informace o tom, zda byl dokument vybrán za archiválii a v případě, že se jedná o dokument v digitální podobě,	6.7.7 upraveno

	identifikátor digitálního archivu.	
2.7.6	Pořadové číslo je dokumentu přiřazováno v rámci předem určeného časového období, zpravidla kalendářního roku. Správcovská role v době konfigurace stanoví podobu pořadového čísla s přihlédnutím k a) určení časového období (určeného časové období ve smyslu právního předpisu upravujícího podrobnosti výkonu spisové služby), b) přítomnosti nebo nepřítomnosti bezvýznamových (počátečních) nul, c) minimálnímu počtu znaků (v případě použití bezvýznamových nul), d) výchozí hodnotě, e) přírůstku (inkrementace).	6.7.8
2.7.7	V případě, že je dokument vložen do spisu vzniklého formou sběrného archu, pořadové číslo podle požadavku 2.7.6 se nepřiřazuje.	6.7.9
2.7.8	Jestliže původce stanoví, že do čísla jednacího nebo do položky „přidělení k vyřízení“ je zaznamenána konkrétní organizační součást původce, správcovská role v době konfigurace vytvoří a dále udržuje číselník organizačních součástí původce.	6.7.10 upraveno
2.7.9	V ED se o spisu vedou následující údaje: a) jednoznačný identifikátor spisu, b) stručný obsah spisu (předmět, věc, název), c) spisová značka spisu, d) datum založení spisu, e) datum uzavření spisu, f) spisový znak, g) skartační režim spisu, h) počet uložených listů dokumentů v listinné podobě, popřípadě svazků příloh v listinné podobě, i) údaje o existenci dokumentů v analogové podobě ve spisu a jejich fyzické umístění, j) informace o zařazení spisu do výběru archiválií, k) informace o tom, zda byl spis vybrán za archiválii a v případě, že se jedná o dokument v digitální podobě, identifikátor digitálního archivu, l) označení organizační součásti původce, který spis vyřizuje, identifikace vlastníka, schvalovatele a zpracovatele spisu, m) odkazy na dokumenty do něho vložené, n) zpravidla počet dokumentů obsažených ve spisu.	6.7.11
2.7.10	V ED se o typovém spisu vedou následující údaje: a) jednoznačný identifikátor typového spisu, b) název spisu, který tvoří spisovou značku spisu, c) datum založení typového spisu, d) datum uzavření typového spisu, e) spisový znak, f) odkazy na součásti typového spisu.	
2.7.11	V ED se o součásti typového spisu vedou následující údaje:	

	a) jednoznačný identifikátor mateřského typového spisu, b) jednoznačný identifikátor součásti, c) stručný obsah součásti dle spisového a skartačního plánu, d) datum založení součásti, e) datum uzavření součásti, f) spisový znak, g) skartační režim součásti, h) údaje o existenci dokumentů v analogové podobě v dílech součásti a fyzické umístění těchto dílů nebo částí dílů, i) odkazy na díly do něho vložené.	
2.7.12	V ED se o dílu typového spisu vede jednoznačný identifikátor dílu, datum jeho otevření a datum jeho uzavření.	
2.7.13	eSSL umožňuje zaznamenat do metadat dokumentu nebo seskupení zařazení do bezpečnostní kategorie.	10.13.33
2.7.14	V ED ISSD se evidují údaje o dokumentech; pokud jsou v této evidenci z rozhodnutí původce evidovány údaje o spisech (typových spisech), použijí se požadavky 2.7.5 až 2.7.11 obdobně.	6.7.12 upraveno
2.7.15	V ED ISSD se vedou povinně pouze údaje dle písmen b), c), e) a m) až r) požadavku 2.7.5.	6.7.13 upraveno
2.7.16	Pořadové číslo v rámci ED ISSD je dokumentu přiřazováno v rámci předem určeného časového období, zpravidla kalendářního roku, kdy správcovská role v době konfigurace stanoví podobu pořadového čísla s možností následujících nastavení pro jeho tvorbu: a) určení časového období, b) přítomnost nebo nepřítomnost bezvýznamových (počátečních) nul, c) minimální počet znaků (v případě použití bezvýznamových nul), d) výchozí hodnota, e) přírůstek (inkrementace).	6.7.14
2.7.17	Číslo jednací dokumentu je vždy tvořeno pořadovým číslem dokumentu v rámci určeného časového období a rokem vzniku společně se zaznamenáním označení původce nebo jeho útvaru v předponě (v prefixu). V případě, že dokument náleží do spisu vytvořeného formou sběrného archu, číslo jednací dokumentu je tvořeno z identifikace spisu (čísla jednacího iniciačního dokumentu) společně se zaznamenáním pořadí dokumentu ve spisu v příponě (v sufixu).	6.7.17
2.7.18	Evidenční číslo samostatné ED vždy obsahuje nejméně označení, popřípadě zkratku původce.	6.7.24
2.7.19	Pokud původce zajišťuje správu dokumentů ve více ISSD (eSSL a informační systémy, které nejsou primárně určeny pro výkon spisové služby), dokumenty, které mají být spravovány v ISSD a byly označeny v ED, jsou do těchto systémů přeneseny, přičemž je v ED zdrojového systému zaznamenáno číslo ze samostatné ED cílového systému. Kromě transakčního protokolu se o těchto	6.7.27 upraveno

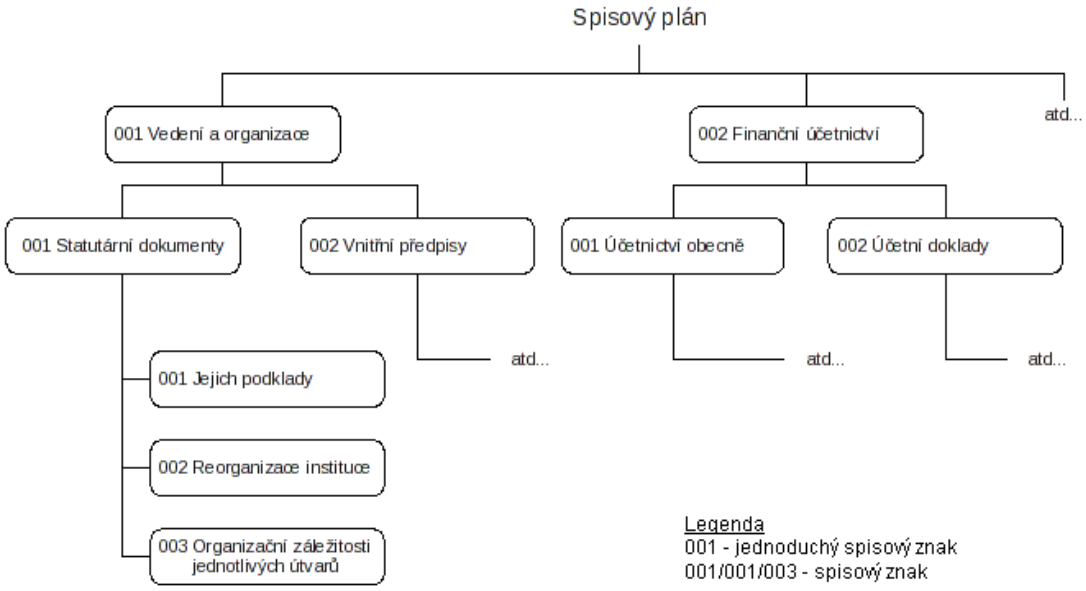
	dokumentech uchovává zejména hlavička metadat (požadavek 6.3.14).	
2.7.20	eSSL zajišťuje, aby byla metadata dokumentů v analogové podobě spravována stejným způsobem jako metadata dokumentů v digitální podobě, včetně jakékoli jejich dědičnosti.	10.1.5
2.7.21	eSSL zajišťuje, aby při výběru věcné skupiny, spisu, typového spisu, součásti nebo dílu byla zároveň jedinou operací vybrána metadata jak pro entity v digitální podobě, tak pro s nimi spojené analogové entity.	10.1.8
2.7.22	eSSL podporuje sledování fyzických složek a dokumentů v analogové podobě prostřednictvím funkce předání a převzetí, s cílem zaznamenat jejich umístění, vlastníka a datum předání, popřípadě převzetí.	10.1.9 D
2.7.23	eSSL znázorní uživatelské roli s přihlédnutím k jejím přístupovým právům informaci o aktuálním umístění předané analogové entity, jejím vlastníkovi a datu, kdy došlo k předání entity.	10.1.18
2.7.24	eSSL zaznamenává všechny operace předání a převzetí a jejich čas do transakčního protokolu.	10.1.19

3 SPISOVÝ PLÁN A ORGANIZACE SPISŮ

eSSL umožňuje zatřídění dokumentu přímo do věcné skupiny, spisu nebo dílu typového spisu. Zajištění souladu s národním standardem vyžaduje podporu hierarchického třídění věcných skupin.

3.1 Věcné skupiny, spisy a typové spisy

Pro zatřídění dokumentů, spisů a typových spisů slouží spisový plán sestávající z hierarchicky členěných věcných skupin. Obrázek č. 2 popisuje příklad několika věcných skupin; každá věcná skupina je pojmenována v souladu se spisovým a skartačním plánem původce a je jí přidělen spisový znak.



Obrázek č. 2 – spisové znaky

Na obrázku č. 2 jsou pro ilustraci znázorněny jednoduché spisové znaky, které jsou samy o sobě nejednoznačné. Jedinečné jsou až spisové znaky zohledňující hierarchii spisového plánu prostřednictvím dědění jednoduchých spisových znaků z mateřských věcných skupin. Například spisový znak věcné skupiny „001-001-002“ se sestavuje takto:

a) začne se u spisového znaku v hierarchii nejvýše postavené věcné skupiny (001 „Vedení a organizace“),
b) přidá se jednoduchý spisový znak následující věcné skupiny směrem dolů v hierarchii (001 „Statutární dokumenty“), vzniká tak spisový znak „001-001“,
c) předchozí krok se opakuje až do dosažení nejbližší mateřské věcné skupiny,
d) přidá se jednoduchý spisový znak věcné skupiny (002 „Reorganizace instituce“), a tím je vytvořen v tomto příkladě spisový znak „001-001-002“.

V případě součástí typových spisů tvoří jejich spisový znak zděděný spisový znak věcné skupiny, v níž se typové spisy vytvářejí, a jednoduchý spisový znak součásti typového spisu.

Číslo	Požadavek	Původně
3.1.1	eSSL podporuje spisový plán, který je kompatibilní se spisovým a skartačním plánem odpovídajícím potřebám původce, jež spisový a skartační plán udržuje.	3.1.1
3.1.2	eSSL kontinuálně udržuje svou vnitřní celistvost (relační a datovou integritu), a to bez ohledu na a) běžné udržovací činnosti, b) operace uživatelů, c) případné zhroucení částí systému.	3.1.2
3.1.3	eSSL umožňuje správcovské roli označit každý spisový plán jednoznačným identifikátorem, názvem a jeho popisem.	3.1.3
3.1.4	eSSL podporuje spisový plán, ve kterém jsou věcné skupiny členěny hierarchicky. Použití hierarchického spisového plánu umožňuje dědičnost spisových znaků a dalších metadat a usnadňuje přehlednost.	3.1.4
3.1.5	eSSL umožňuje správu spisového plánu výlučně správcovské roli. Správa spisového plánu se týká operací stanovených v kapitole 3.1.	3.1.5 upraveno
3.1.6	eSSL neomezuje počet úrovní v hierarchii spisového plánu.	3.1.7
3.1.7	eSSL umožňuje zavedení textových vysvětlivek do všech věcných skupin, do všech spisů, součástí a do typových spisů. Textové vysvětlivky objasňují zamýšlený obsah dokumentů nebo určitých věcných skupin, spisů, součástí a typových spisů.	3.1.10
3.1.8	eSSL podporuje import celého spisového plánu nebo jeho části ve formě odpovídající schématu XML dle přílohy č. 5.	3.1.12
3.1.9	eSSL při provádění požadavku 3.1.8 přiřadí každé importované věcné skupině spisový znak, a to a) podle stejných pravidel, jaká by byla použita při ručním sestavování spisového plánu, b) zachováním původního spisového znaku v jeho úplnosti (což je umožněno pouze, když jsou struktury kompatibilní), nebo c) připojením původního spisového znaku ke spisovému znaku v přijímaném spisovém plánu. Výběr konkrétní možnosti provede správcovská role. Pokud při importu nelze použít dosavadní spisový znak, lze jej například uložit do jiného prvku metadat („starý spisový znak“).	3.1.15
3.1.10	Jestliže eSSL importuje spisový plán a skartační režimy, postupuje podle stejných pravidel, která by byla použita při ručním sestavení spisového plánu. Pokud jsou při ověřování zjištěny chyby, eSSL označí předmětná metadata a upozorní na tyto chyby správcovskou roli, která import provádí.	3.1.16
3.1.11	eSSL podporuje export celého spisového plánu nebo jeho části ve formě odpovídající schématu XML dle přílohy č. 5.	3.1.17 upraveno
3.1.12	eSSL umožňuje správcovské roli přidat v kterékoli části spisového plánu věcné skupiny. Věcné skupiny se neumisťují do věcných skupin, ve kterých jsou zatříděny spisy, dokumenty nebo typové spisy. Do věcných skupin, ve kterých jsou umístěny jiné věcné	3.1.25

	skupiny, nelze zatřídit spisy, dokumenty nebo typové spisy.	
3.1.13	eSSL podporuje vytvoření a současné využívání více spisových plánů.	3.1.26
3.1.14	eSSL umožňuje správcovské roli v každé konkrétní věcné skupině spisového plánu nastavit možnost vytvářet typové spisy. V této věcné skupině nesmí být vložena jiná věcná skupina, dokument nebo spis.	3.3.1
3.1.15	eSSL umožní vložit do věcné skupiny, která je konfigurována pro vkládání typových spisů, pouze typové spisy.	
3.1.16	eSSL umožňuje uživateli pracujícímu s věcnou skupinou, spisem, typovým spisem nebo dokumentem zjistit kontextové informace o příslušné věcné skupině, spisu, typovém spisu nebo dokumentu, tedy o metadatech a mateřském spisu nebo věcné skupině. eSSL umožňuje uživateli identifikovat mateřskou entitu přímo z věcné skupiny, spisu, typového spisu nebo dokumentu.	3.4.27
3.1.17	eSSL umožňuje správci konfigurovat systém tak, aby určil, k jakému rozsahu spisového plánu má každá uživatelská role nebo skupina uživatelů přístup.	3.4.30
3.1.18	eSSL znázorňuje spisový plán a samostatně i jeho jednotlivé části.	3.4.31
3.1.19	eSSL umožňuje uživateli definovat nejčastěji používané věcné skupiny.	
3.1.20	eSSL podporuje příjem, udržování a znázornění metadat pro spisy, typové spisy a věcné skupiny.	3.2.1
3.1.21	eSSL neomezuje možnost přidávat do spisu, typového spisu a věcné skupiny metadata nad rámec metadat stanovených ve schématech XML v příloze.	3.2.2
3.1.22	eSSL poskytuje v rámci spisového plánu funkci pro automatické přidělování jednoduchého spisového znaku každé věcné skupině. Pokud spisový znak existuje, uplatní se požadavek 3.1.9.	3.2.3
3.1.23	eSSL zaznamená datum otevření a datum uzavření věcné skupiny, spisu nebo typového spisu do jejich metadat. Otevřením nebo uzavřením věcné skupiny nedochází ke změně spisového plánu.	3.2.8 upraveno
3.1.24	eSSL zaznamenává datum vytvoření nové věcné skupiny, spisu, typového spisu, součásti nebo dílu do jejich metadat.	3.2.9
3.1.25	eSSL nezavádí žádná praktická omezení pro počet věcných skupin, spisů nebo typových spisů.	3.2.15
3.1.26	eSSL přiřadí spisový znak věcné skupině a součásti typového spisu.	7.1.1 upraveno
3.1.27	eSSL zajišťuje, aby všechny spisové znaky byly jednoznačné v rámci spisového plánu.	7.1.2
3.1.28	eSSL zajišťuje, aby všechny spisové znaky zachovaly jednoznačnost bez ohledu na jakékoli operace přetřídění.	7.1.3 upraveno
3.1.29	eSSL ukládá spisové znaky do metadatových prvků entit, ke kterým se vztahují.	7.1.4
3.1.30	Spisové znaky jsou tvořeny zřetězením jednoduchých spisových znaků, oddělených znakem oddělovače. *Příklad oddělovače:*	7.1.6, 7.1.7 D

	a) „ „(mezera), *b) „-“(pomlčka),* *c) „/“ (lomítko),* d) *„ .“ (tečka).*	
3.1.31	eSSL umožňuje správcovské roli při vytvoření nové věcné skupiny stanovit, zda pro její entity – dceřiné věcné skupiny – se jednoduché spisové znaky generují automaticky prostřednictvím eSSL, nebo zda jsou přiděleny uživatelem, anebo externí aplikací. eSSL a) generuje každý jednoduchý spisový znak automaticky a brání uživatelům jej ručně vložit nebo upravovat, nebo b) umožňuje oprávněnému uživateli nebo externí aplikaci přidělit jednoduchý spisový znak, ale brání jim provést jeho případné následné změny. V případě součásti typového spisu se její jednoduchý spisový znak, zpravidla vyjádřený ve spisovém a skartačním plánu původce, tvoří obdobně.	7.1.8
3.1.32	Pokud eSSL automaticky generuje nový jednoduchý spisový znak [písmeno a) požadavku 3.1.31], generuje následující pořadové číslo s přihlédnutím a) k naposledy použitému jednoduchému spisovému znaku v daném místě spisového plánu, nebo výchozí hodnotě (například v obrázku č. 5 přidání věcné skupiny 003 – „Organizační záležitosti jednotlivých útvarů“ po 002 – „Reorganizace instituce“), b) ke stanovenému přírůstku.	7.1.9
3.1.33	Při vkládání jednoduchého spisového znaku uživatelem nebo externí aplikací eSSL ověřuje jednoznačnost jednoduchého spisového znaku v rámci jeho mateřské entity.	7.1.10
3.1.34	eSSL nejpozději při uzavření spisu nebo dílu typového spisu a) označí spisovým znakem dokumenty shodně se spisovým znakem spisu nebo součásti, ve které je vložen díl typového spisu, b) označí spisovým znakem spisy a dokumenty připojené pevným křížovým odkazem do dílu typového spisu shodně se spisovým znakem součásti, ve které je vložen díl typového spisu, c) podle konfigurace eSSL označí spisovým znakem nejstaršího nebo nejmladšího spisu všechny spisy spojené pevným křížovým odkazem.	

3.2 Typové spisy, součásti a díly

V řadě případů může být spis veden dlouhodobě (i desítky let), slouží pro shromáždění dokumentů „ve věci“ a často je vnitřně strukturován. Přitom přírůstková ED (čísla jednací) je pro něj zcela podružná a postupně ztrácí i svůj význam pro odkazování. Takovýto spis se nazývá typový spisem. Je to soubor

dokumentů a spisů v rámci konkrétní věcné skupiny s předem stanovenou strukturou, členěný na věcné, podle obsahu stanovené části nazývané součásti, které jsou dále členěny na díly (na základě rozsahu – fakticky manipulační jednotky). Dokumenty jsou vkládány do dílů v rámci jednotlivých součástí typového spisu. Stejným způsobem jsou do typového spisu vkládány i pevné křížové odkazy na spisy.

Dokumenty a spisy vložené přímo do věcné skupiny nelze dělit podle dalšího (a pro ukládání podstatného) kritéria – tím je věc, z níž vychází i označení typového spisu, např. konkrétní fyzická nebo právnická osoba. Bez použití typového spisu by všechny dokumenty a spisy všech zmíněných osob byly bez vzájemných vazeb v dané věcné skupině pohromadě. Spis, který není typovým spisem, navíc nelze vnitřně členit a jeho označení zpravidla vychází z přírůstkové ED, takže přiřazení ke zmíněné osobě nemusí být vždy jednoznačné. Vzhledem k početnosti subjektů (např. uvedených osob) není vždy ani možné pro každý předem vytvořit vlastní věcnou skupinu (spisový a skartační plán by byl pro svoji rozsáhlost a nutnost časté aktualizace nepoužitelný).

Základními vlastnostmi typového spisu jsou:

- Typový spis se vztahuje k jedné agendě vyjádřené konkrétní věcnou skupinou v rámci spisového plánu; tato agenda je výsledkem předem stanoveného procesu vyřizování nebo ukládání (např. spisy živnostníků u živnostenského úřadu, spisy týkající se jednotlivých mezinárodních organizací v agendě ministerstva, daňový spis dle daňového řádu apod.).
- Označení typového spisu není vázáno na ED, která zde nehraje roli identifikace – tu přebírá název.
- Název se vytváří u všech typových spisů v rámci stejné věcné skupiny jednotným způsobem a je reprezentován jménem, číselným nebo alfanumerickým označením (např. název organizace; jméno, příjmení a datum narození fyzické osoby; identifikační číslo organizace; číslo popisné stavby, číslo projektu).
- Předem se předpokládá členění na součásti a toto členění je žádoucí z hlediska četnosti do nich (resp. do jejich dílů) vkládaných dokumentů nebo křížových odkazů (např. v agendě mezinárodních organizací se jedná o součásti „zasedání řídícího orgánu“, „pracovní komise“, „výroční zprávy“, „vysílání zástupců“, „placení příspěvků“; u spisu stavby např. „územní řízení“, „stavební dokumentace“, „stavební řízení“, „kolaudace“); členění však není nutnou podmínkou existence typového spisu (může existovat jen jedna součást).
- Součásti jsou pojmenovány shodně ve všech typových spisech příslušné věcné skupiny.
- Vnitřní strukturu typového spisu (rozdělení na součásti) lze předem stanovit (určit, že v dané agendě reprezentované věcnou skupinou budou vytvářeny typové spisy) a součásti pojmenovat, což se projeví i ve spisovém a skartačním plánu.

Číslo	Požadavek	Původně
3.2.1	eSSL umožňuje vytvářet typové spisy pouze ve věcné skupině, pro kterou je to nastaveno (požadavek 3.1.14).	
3.2.2	eSSL umožňuje vytvářet typové spisy uživateli s rolí pracovníka s typovými spisy.	10.5.5
3.2.3	eSSL umožňuje roli pracovníka s typovými spisy v konkrétní věcné skupině nastavit a) názvy součástí typového spisu, b) rozsah dílu.	3.3.1 upraveno
3.2.4	eSSL umožňuje roli pracovníka s typovými spisy vytvořit šablonu součástí pro určitou věcnou skupinu, jež mají být automaticky	3.3.17 upra-

	vytvořeny pro každý nový typový spis následně vytvořený v dané věcné skupině. Každá šablona součásti je označena spisovým znakem, který vzniká doplněním zděděného spisového znaku věcné skupiny, ve které jsou typové spisy vytvářeny, o jednoduchý spisový znak součásti. *Například šablona v komerční pojišťovně může specifikovat pro věcnou skupinu týkající se pojistek klientů následující součásti: pojistné smlouvy a jejich změny, interní korespondence, korespondence s odborníky ve zdravotnictví, účetní doklady, ostatní korespondence s klienty. Každý nový typový spis vytvořený v této věcné skupině je poté automaticky vytvořen s těmito součástmi. Spisový znak je přidělován následovně:* *2.1 Věcná skupina XZ pro typové spisy* *2.1. Typový spis A* *2.1.1 Součást I* *2.1.2 Součást II*	no
3.2.5	eSSL umožňuje vkládat dokumenty a pevné křížové odkazy na spisy (požadavek 4.2.2) uživateli s příslušným oprávněním.	
3.2.6	eSSL zajišťuje, že a) každý typový spis obsahuje jednu nebo více součástí, b) každá součást obsahuje jeden nebo více dílů, c) díly různých součástí jsou vytvářeny nezávisle.	
3.2.7	eSSL umožňuje nastavit rozsah dílu typového spisu v konkrétní věcné skupině stanovením a) doby, po kterou má být díl otevřen (počet let), b) maximálního množství dokumentů, které mají být do dílu vloženy a při jehož dosažení se díl uzavře, nebo c) souhrnnou velikostí komponent vložených dokumentů, po jejímž překročení se díl automaticky uzavře (v MB). *Nejobvyklejším způsobem je stanovení doby, po kterou mají být dokumenty a spisy do dílu vkládány. Po jejím uplynutí se díl uzavře a začne plynout jeho skartační lhůta zděděná od mateřské součásti; díl se po jejím uplynutí vyřazuje jako celek.*	
3.2.8	eSSL zajistí v příslušné součásti po automatickém uzavření dílu na základě rozsahu (požadavek 3.2.7) automatické otevření nového dílu.	
3.2.9	eSSL zajišťuje, že a) pouze posledně vytvořený díl v součásti může být otevřený a b) všechny ostatní díly v součásti musí být uzavřené.	3.3.4
3.2.10	eSSL zabraňuje uživateli vkládat dokumenty nebo pevné křížové odkazy na spisy do uzavřeného dílu.	3.3.5
3.2.11	eSSL umožňuje přidat díl do kterékoli součásti, která není uzavřená na základě nastaveného rozsahu dílu (požadavek 3.2.7). Proces přidávání nového dílu se skládá z uzavření dílu, který byl aktuálně otevřený, a vytvoření nového otevřeného dílu.	3.3.6
3.2.12	eSSL kontroluje, zda jsou v případě uzavření dílu uzavřeny i všechny spisy připojené do dílu pevnými křížovými odkazy.	

	Jestliže tyto spisy uzavřeny nejsou: a) eSSL automaticky vyjme pevný křížový odkaz z uzavíraného dílu a vloží ho do nově otevřeného dílu v příslušné (otevřené) součásti, b) v případě uzavírání typového spisu nebo jeho součásti vyzve uživatele k uzavření spisů vložených pevným křížovým odkazem, přitom nepovolí pevné křížové odkazy odstranit.	
3.2.13	eSSL umožňuje roli pracovníka s typovými spisy přidat součásti do kteréhokoli typového spisu, který není uzavřen.	3.3.7
3.2.14	eSSL umožňuje roli pracovníka s typovými spisy u součásti, která není uzavřena, změnit název.	
3.2.15	eSSL umožňuje kdykoli roli pracovníka s typovými spisy uzavřít součást.	3.3.8
3.2.16	eSSL zaznamená datum otevření nového dílu nebo součásti v jejich metadatech.	3.3.9
3.2.17	eSSL automaticky ukládá do metadat dílu nebo součásti vždy, když jsou nově otevřeny, ty hodnoty metadat jejich mateřského typového spisu, jež jsou nezbytné.	3.3.10
3.2.18	Součásti jednoho typového spisu mohou mít odchylné skartační režimy. Typový spis skartační režim nemá.	
3.2.19	eSSL automaticky ukládá do metadat dílu skartační režim součásti.	
3.2.20	eSSL automaticky při otevření nového dílu přiřazuje identifikátor, jednoznačný v rámci jeho mateřské součásti.	3.3.11
3.2.21	eSSL uloží datum uzavření dílu nebo součásti v jejich metadatech.	3.3.12
3.2.22	Jestliže uživatel zatřiďuje dokument nebo vytváří pevné křížové odkazy na spisy v rámci typového spisu, eSSL mu znázorní příslušnou součást. Uživatel nesmí být nucen vyhledávat v rámci součásti díl.	3.3.13 upraveno
3.2.23	eSSL umožňuje vytváření více souběžně otevřených součástí v kterémkoli typovém spisu.	3.3.14
3.2.24	eSSL automaticky uzavře všechny díly, kdykoli je uzavřena jejich mateřská součást.	
3.2.25	eSSL smaže prázdný díl, jestliže je uzavřena jeho mateřská součást nebo typový spis.	3.3.15 upraveno
3.2.26	eSSL umožňuje roli pracovníka s typovými spisy smazat prázdný díl a znovu otevřít v součásti díl předchozí, a to v rámci jedné operace, která je zaznamenána do transakčního protokolu.	3.3.16
3.2.27	eSSL automaticky uzavře všechny součásti, kdykoli je uzavřen jejich mateřský typový spis.	3.3.18
3.2.28	eSSL umožňuje ve výjimečných případech a výlučně správcovské roli vložit dokument do uzavřeného dílu, a to pouze za předpokladu, že datum vzniku dokumentu není pozdější než datum uzavření dílu. Datum uzavření dílu se touto operací, která se zaznamená do transakčního protokolu, nemění. Tento požadavek nesmí být použit u entit, u kterých uplynula skartační lhůta.	6.1.41 upraveno

3.3 Udržování vazeb mezi entitami

Číslo	Požadavek	Původně
3.3.1	eSSL umožňuje správcovské roli přetřídit (přemístit) celý obsah celé věcné skupiny nebo jeho vyznačenou část do jiné věcné skupiny v rámci spisového plánu jedinou operací.	3.4.1 upraveno
3.3.2	eSSL zajišťuje označení dokumentů, spisů nebo typových spisů přetříděných do jiných věcných skupin novými spisovými znaky odpovídajícími novému umístění ve spisovém plánu. Pro označení součástí spisovými znaky platí první věta obdobně.	3.4.5 upraveno
3.3.3	eSSL zajišťuje správné vložení všech dokumentů při přemístění do věcných skupin, spisů a dílů, do kterých byly vloženy. eSSL zaručuje, že vazby součástí, dílů a spisů zůstanou zachovány.	3.4.8
3.3.4	eSSL uplatní po přetřídění dědičnost skartačního režimu z nové mateřské věcné skupiny do přetříděných dokumentů a spisů, pokud nejsou označeny jako vyřízené (uzavřené). Dědičnost se neuplatní při vložení dokumentu do nevyřízeného spisu.	3.4.13 upraveno
3.3.5	eSSL zapíše do transakčního protokolu před přetříděním dokumentu, spisu nebo typového spisu jejich původní spisový znak a s výjimkou typového spisu původní skartační režim tak, aby bylo možné rekonstruovat libovolný stav v rámci jejich životního cyklu.	3.4.15 upraveno
3.3.6	eSSL umožňuje oprávněným uživatelským rolím uzavření věcné skupiny, spisu, typového spisu a součásti. Do uzavřené entity není možné vkládat dokumenty ani pevné křížové odkazy.	3.4.20

4 ODKAZOVÁNÍ MEZI ENTITAMI

Tato část popisuje požadavky na odkazy mezi věcnými skupinami, spisy, typovými spisy, součástmi, díly a dokumenty (entitami).

4.1 Jednoznačné identifikátory

Všem entitám uloženým v eSSL jsou přiřazovány jednoznačné identifikátory, a to za účelem

a) umožnit eSSL entity zpracovávat a
b) umožnit uživatelům entity vyhledávat, odkazovat na ně a využívat je.

Číslo	Požadavek	Původně
4.1.1	eSSL přiřadí jednoznačný identifikátor každé položce dále uvedené v písmenech a) až g), která je vytvořena v eSSL, při každém jejím novém výskytu. Jednoznačné identifikátory se přiřazují k a) spisovému plánu jako celku, b) věcné skupině, c) spisu, d) typovému spisu, e) součásti, f) dílu, g) dokumentu.	7.2.1
4.1.2	eSSL zajišťuje, aby byly všechny jednoznačné identifikátory v rámci spisového plánu a v rámci jednoho eSSL provozovaného na geograficky oddělených místech jednoznačné. *Tento požadavek platí, pokud je spisový plán rozdělen na samostatné části, z nichž některé se uplatňují na oddělená pracoviště. Požadavek se vztahuje také na případy, kdy je současně používáno více spisových plánů.*	7.2.2
4.1.3	eSSL ukládá jednoznačné identifikátory do metadatových prvků entit, ke kterým se vztahují.	7.2.3
4.1.4	eSSL nepožaduje po uživateli, aby ručně vkládal jednoznačné identifikátory a využíval je pro funkce v eSSL, pokud se pro provedení těchto operací sám nerozhodne.	7.2.6

4.2 Křížové odkazy

Číslo	Požadavek	Původně
4.2.1	eSSL umožňuje vytváření křížových odkazů mezi a) spisy, b) spisy a díly typových spisů, c) dokumenty, d) spisy a dokumenty.	3.4.23 upraveno
4.2.2	eSSL vytváří automaticky pevné křížové odkazy v případě: a) trvalého spojení spisů uživatelem,	

	b) vložení spisu do dílu typového spisu, c) spojování dokumentů při tvorbě spisu.	
4.2.3	eSSL zajistí v okamžiku uzavření příslušného dílu typového spisu dědičnost spisového znaku a skartačního režimu součásti na spis vložený do dílu pomocí pevného křížového odkazu dle požadavku 4.2.2 písmene a).	
4.2.4	eSSL umožní odstranění pevného křížového odkazu pouze oprávněnému uživateli, který v eSSL zapíše důvod odstranění.	
4.2.5	eSSL umožňuje uživateli vytvářet volné křížové odkazy mezi a) spisy, b) dokumenty, c) spisy a dokumenty.	
4.2.6	eSSL umožní volné křížové odkazy oprávněnému uživateli odstranit.	
4.2.7	eSSL umožňuje uživateli pracujícímu s věcnou skupinou, spisem, typovým spisem, součástí nebo dokumentem zjistit jedinou operací kontextové informace o metadatech entit připojených křížovým odkazem. Tyto entity umožní eSSL na základě uživatelských práv znázornit.	

4.3 Typy dokumentů

Typy dokumentů se vyznačují zejména následujícími vlastnostmi:
a) atributy metadat,
b) požadavky na uchovávání,
c) kontrola přístupu, nebo
d) druh (například smlouva, životopis).

Číslo	Požadavek	Původně
4.3.1	eSSL podporuje definování a udržování typů dokumentů.	6.4.1
4.3.2	Všechny dokumenty v eSSL nemají žádný nebo mají nejvýše jeden typ dokumentu.	6.4.2
4.3.3	eSSL omezuje definování a udržování typů dokumentů výlučně na správcovskou roli.	6.4.3
4.3.4	eSSL umožňuje správcovské roli omezit vytváření dokumentů stanoveného typu dokumentů výlučně specifikovaným skupinám uživatelů podle jejich pracovních potřeb.	6.4.4
4.3.5	eSSL umožňuje správcovské roli definovat jeden typ dokumentu jako výchozí, používaný zpravidla všemi uživateli, kteří jsou oprávněni přijímat dokumenty.	6.4.5

5 VYHLEDÁNÍ, VÝBĚR, ZNÁZORNĚNÍ A ZTVÁRNĚNÍ

Nedílnou součástí eSSL je funkce umožňující uživatelům vyhledávat a znázorňovat seskupení a dokumenty. Funkce vyhledávání a znázorňování je v konkrétních eSSL koncipována v odlišném rozsahu uživatelské nabídky, a to s přihlédnutím k požadavkům různých typů uživatelů. V této části národního standardu jsou proto stanoveny současně požadavky na obvyklé vyhledávací funkce. Veškeré požadavky, které jsou dále uvedeny v této části, je nutné aplikovat společně s požadavky na kontrolu přístupu, včetně kontroly bezpečnosti (uživatelská oprávnění).

S přihlédnutím k tomu, že dokumenty v digitální podobě nejsou bez prostředků výpočetní techniky čitelné, musí eSSL zajistit nebo zprostředkovat funkce sloužící k znázornění dokumentů zejména zobrazením a vytištěním.

5.1 Vyhledání a výběr

Číslo	Požadavek	Původně
5.1.1	eSSL neposkytne uživateli informace (metadata nebo obsah dokumentu), ke kterým tento uživatel nemá oprávněný přístup.	8.1.1
5.1.2	eSSL umožňuje uživatelům vyhledávat a vybírat a) dokumenty, b) jakoukoli úroveň seskupení a jejich příslušná metadata.	8.1.2
5.1.3	eSSL umožňuje uživatelům stanovit, zda mají být prostřednictvím funkce vyhledávání nalezeny dokumenty nebo seskupení.	8.1.4
5.1.4	eSSL umožňuje uživatelům vyhledávat v metadatech a zpravidla i v textovém obsahu dokumentů.	8.1.6
5.1.5	eSSL pomocí funkce vyhledávání lokalizuje seskupení pro účely zatřídění dokumentu do spisového plánu při evidenci dokumentů. eSSL nesmí vyzvat uživatele, aby zastavil proces příjmu a zahájil vyhledávání. *Účelem tohoto požadavku je usnadnění použití eSSL při příjmu dokumentů.*	8.1.7
5.1.6	eSSL zobrazuje celkový počet nalezených položek jako výsledek vyhledávání (seznam úspěšných výsledků) a zobrazuje nebo umožňuje uživateli, aby si vyžádal zobrazení počtu položek v seznamu úspěšných výsledků vyhledávání.	8.1.10
5.1.7	eSSL umožňuje správcovským rolím volitelně konfigurovat a následně změnit specifikaci standardního vyhledávání v prvcích metadat dokumentu, dílu, součásti, spisu**,** typového spisu a věcné skupiny nebo v textu.	8.1.12
5.1.8	eSSL poskytuje vyhledávací funkci, která umožňuje v jakékoli kombinaci, s cílem spojit neomezený počet vyhledávacích podmínek, použití booleovských operátorů, a to a) A („AND“), b) NEBO („OR“), c) PRÁVĚ JEDEN („EXCLUSIVE OR“), d) NE („NOT“).	8.1.13
5.1.9	eSSL umožňuje uživatelům vyhledávat entity podle jejich klíčových slov, pokud se v systému používají.	8.1.14

5.1.10	eSSL umožňuje uživatelům vybrat klíčová slova z číselníků v průběhu jakéhokoli vyhledávání založeného na využití klíčových slov.	8.1.15
5.1.11	Pokud eSSL zahrnuje využití číselníku, umožňuje správcovské roli tento číselník udržovat.	8.1.19
5.1.12	eSSL umožňuje uživatelům omezit rozsah vyhledávání na jimi určená seskupení.	8.1.23
5.1.13	eSSL vyhledává a vybírá spis, typový spis**,** součást nebo díl, celý jejich obsah – pokud je v digitální podobě – a kontextová metadata a poskytuje seznam všech položek i jednotlivé položky samostatně v kontextu konkrétního seskupení v jediném procesu vyhledávání.	8.1.24
5.1.14	eSSL umožňuje uživatelům stanovit časové intervaly pro vyhledávání, například formou kalendářních dat nebo počtem dnů.	8.1.28 D
5.1.15	eSSL zajišťuje vyhledávání a řazení v ED zejména podle a) identifikace spisu, typového spisu a součásti typového spisu, b) čísla jednacího dokumentu, c) jednoznačného identifikátoru, d) vlastníka, schvalovatele, nebo zpracovatele, e) data odeslání, f) data přijetí, g) označení a identifikace dokumentu provedených odesílatelem, h) názvu (věci) věcné skupiny, dokumentu, spisu, typového spisu nebo součásti, i) spisového znaku, j) skartačního režimu, k) způsobu odeslání, l) způsobu doručení.	6.7.25
5.1.16	ISSD zajišťuje vyhledávání a řazení v samostatné ED ISSD, zejména podle a) evidenčního čísla dokumentu, b) jednoznačného identifikátoru dokumentu, c) data přijetí dokumentu, d) označení a identifikace dokumentu provedených odesílatelem, e) spisového znaku, f) názvu (věci) věcné skupiny, dokumentu, spisu, typového spisu nebo součásti, g) skartačního režimu dokumentu.	6.7.26
5.1.17	eSSL zajišťuje dostupnost dat transakčního protokolu tak, aby byly na výzvu znázorněny uskutečněné operace a všechna související data.	4.2.12
5.1.18	eSSL obsahuje uživatelsky jednoduché funkce umožňující oprávněným uživatelům vyhledávat informace v transakčním protokolu.	4.2.13
5.1.19	eSSL umožňuje oprávněným uživatelům vyhledávat v transakčních protokolech specifické operace, entity, uživatele,	4.2.14

	skupiny uživatelů, role, časové údaje nebo časové intervaly.	
5.1.20	Když je vyhledán smazaný dokument, eSSL informuje uživatele na základě kontroly jeho přístupu a bezpečnostní kategorie o existenci původního dokumentu a zpřístupní jej uživateli.	9.3.18

5.2 Znázornění dokumentů a metadat

Číslo	Požadavek	Původně
5.2.1	eSSL zpřístupňuje obsah věcných skupin, spisů, typových spisů, součástí nebo dílů k prohlížení bez rozlišování mezi uzavřenými a otevřenými věcnými skupinami, spisy, typovými spisy, součástmi nebo díly.	3.4.22
5.2.2	eSSL znázorní v jediné operaci obsah nebo metadata věcné skupiny, spisu, typového spisu, součásti, dílu nebo dokumentu vždy, když jsou identifikovány. Pokud eSSL ukládá dokumenty ve formátu proprietární aplikace, znázornění může být provedeno aplikací mimo eSSL. Tento požadavek zahrnuje následující situace: a) uživatel provede vyhledání a získá seznam výsledků udávající několik dokumentů; eSSL umožňuje uživateli znázornit obsah v digitální podobě nebo metadata každého nalezeného dokumentu, b) uživatel prochází spisový plán na úroveň věcné skupiny, která obsahuje spisy nebo typové spisy. eSSL umožňuje uživateli v jediné operaci znázornit seznam všech spisů nebo typových spisů přiřazených do této věcné skupiny a umožňuje uživateli obdobně znázornit metadata věcné skupiny.	8.2.1
5.2.3	Kdykoli je vytvořen nový spis nebo díl a existuje pro ně fyzická složka, eSSL umožňuje uživateli vytištění obalu těchto entit se základními metadaty, kterými jsou zejména a) spisová značka spisu nebo název typového spisu, b) stručný obsah (předmět, věc) spisu nebo součásti, c) datum založení/uzavření spisu nebo dílu, d) jednoznačný identifikátor, e) spisový znak, f) bezpečnostní kategorie (pokud se používá), g) počet listů dokumentu v listinné podobě, počet listinných příloh dokumentu a počet listů těchto příloh, popřípadě počet svazků listinných příloh dokumentu; u příloh v nelistinné podobě jejich počet a druh, h) skartační režim.	10.1.25 upraveno
5.2.4	eSSL znázorní údaje vedené v ED o dokumentech, spisech, typových spisech a jejich součástech.	6.7.15 upraveno
5.2.5	eSSL znázorní u dokumentu z ED zejména a) položky stanovené v požadavku 2.7.5, b) číslo jednací (požadavek 2.7.17),	6.7.16 upraveno

	c) spisový znak, d) zděděný nebo přidělený skartační režim, pokud je odlišný od skartačního režimu seskupení, ve kterém je dokument uložen, e) historii dokumentu (zejména oběh, zpravidla i nahlížení do dokumentu), f) identifikace spisu, v němž je případně vložen (například na spisovou značku**,** název typového spisu). V ED se dále znázorňují u dokumentu, a) který je umístěn ve věcné skupině název mateřské věcné skupiny a její spisový znak, b) který je umístěn pevným křížovým odkazem nebo vložen do dílu typového spisu, název typového spisu a název a spisový znak součásti typového spisu, c) který byl určen pro export do ISSD podle požadavku 5.1.16, evidenční číslo daného dokumentu, pod nímž je zaevidován do cílového ISSD.	
5.2.6	eSSL znázorní u spisu z ED zejména a) všechny položky podle požadavku 2.7.9, b) historii spisu (zejména oběh a schvalování), c) datum vytvoření a uzavření spisu.	6.7.18 upraveno
5.2.7	eSSL znázorní z ED dále a) u spisu, který byl priorován, pevný křížový odkaz na identifikaci spisu, do kterého byl priorován, b) u spisu, do kterého byly priorovány jiné spisy, seznam pevných křížových odkazů na identifikaci těchto spisů, c) u typového spisu seznam všech dokumentů zařazených do dílů jednotlivých součástí v členění po dílech pro jednotlivé určené časové období, d) u typového spisu, do kterého byly zařazeny pevné křížové odkazy na jiné spisy, seznam všech odkazů do jednotlivých součástí, e) seznam všech dokumentů ve spisu a jejich čísla jednací, f) pro zobrazení spisů propojených volnými křížovými odkazy platí písm. a) a b) obdobně.	6.7.19 upraveno
5.2.8	eSSL umožňuje takové znázornění údajů stanovených v požadavcích 5.2.5 až 5.2.7 o jednotlivém dokumentu, spisu, součásti, dílu nebo typovém spisu, které zajistí jejich vytištění jedinou operací.	6.7.20
5.2.9	eSSL umožňuje přehledné znázornění údajů popisujících dokumenty podle požadavku 5.2.5, a to podle pořadového čísla v rámci určeného časového období. eSSL zpravidla umožňuje jejich vytištění jedinou operací.	6.7.21
5.2.10	eSSL umožňuje znázornit seznam všech spisů nebo typových spisů včetně zatřídění do věcné skupiny ve formátu uživatelsky srozumitelném.	3.2.16 upraveno
5.2.11	ISSD znázorní údaje o dokumentech vedené v samostatné ED. Pokud se v této evidenci z rozhodnutí původce znázorňují i údaje o seskupeních, použijí se požadavky 5.2.6 a 5.2.7 obdobně.	6.7.22
5.2.12	ISSD znázorňuje u dokumentu zejména položky stanovené v	6.7.23

	požadavku 2.7.15.	upraveno
5.2.13	U dokumentu, který byl eSSL exportován nebo přenesen z jiného eSSL nebo ISSD stejného původce, se znázorní evidenční číslo dokumentu, pod kterým byl zaevidován v ED původního eSSL, resp. v samostatné ED původního ISSD.	
5.2.14	eSSL podporuje znázornění spisů, typových spisů, součástí, dílů a dokumentů přímo zatříděných do věcné skupiny, které jsou určeny k provedení skartační operace, a to včetně jejich metadat a informací o skartačním režimu.	5.2.2 upraveno
5.2.15	eSSL umožňuje vytisknout všechny tisknutelné komponenty dokumentu jedinou operací.	8.3.1 upraveno
5.2.16	eSSL umožňuje správcovské roli vytištění nebo export všech stanovených správcovských parametrů nebo jejich výběr (například seznam všech uživatelů s bezpečnostním oprávněním).	8.3.8
5.2.17	eSSL umožňuje oprávněným rolím vytištění celého nebo části spisového plánu.	8.3.14
5.2.18	eSSL umožňuje vytisknout seznam klíčových slov.	8.3.11

5.3 Ztvárnění komponent, dokumentů, spisů a metadat

Vzhledem k tomu, že eSSL musí být auditovatelným a důvěryhodným systémem, je stanovena povinnost exportu transakčního protokolu a jeho opatření autentizačními prvky (elektronický podpis nebo elektronická pečeť a elektronické časové razítko). Obdobně musí eSSL umožnit ztvárnění podstatných údajů z ED.

Pro účely předání zejména spisu k dalšímu jednání (postoupení spisu dle příslušných právních předpisů) nelze předpokládat využití exportu nebo přenosu (kapitola 5.3), neboť v takovém případě by exportované nebo přenášené entity musely být do eSSL adresáta importovány a staly by se tak jeho entitami. V případě uváděného postoupení je spis odeslán jako dokument a jako jeden dokument u adresáta také evidován (zpravidla je odeslán jako příloha k průvodnímu dopisu). Ztvárnění spisu a typového spisu tak umožňuje předávat v jakémkoli stupni vyřizování kompletní informaci a ne pouze komponenty.

Číslo	Požadavek	Původně
5.3.1	eSSL zajistí, aby komponenty, které nejsou ve výstupních datových formátech podle prováděcího právního předpisu upravujícího podrobnosti výkonu spisové služby, byly do těchto formátů ztvárněny postupem podle zákona a) při příjmu po provedení požadavku 2.1.15, b) při uzavření spisu, c) při uzavření typového spisu, součásti nebo dílu, d) při vyřízení dokumentu vloženého přímo do věcné skupiny. *Ztvárnění do výstupních datových formátů se předpokládá pouze v případech, jestliže takové formáty pro komponentu existují.*	
5.3.2	eSSL zajistí možnost opakovaného ztvárnění údajů vedených v ED do samostatného dokumentu, který opatří elektronickým	6.7.28 upra-

	podpisem nebo elektronickou pečetí a následně kvalifikovaným elektronickým časovým razítkem. Údaje z ED v rozsahu stanoveném právním předpisem upravujícím podrobnosti výkonu spisové služby eSSL ztvární za časové období zvolené uživatelem.	no
5.3.3	eSSL obsah transakčního protokolu za stanovený časový úsek, nejdéle však 1 den, automaticky na konci tohoto časového úseku uloží jako ztvárnění dokumentu v datovém formátu PDF/A nebo XML dle přílohy č. 6, který opatří elektronickým podpisem nebo elektronickou pečetí a elektronickým časovým razítkem. Tento dokument eSSL zatřídí do příslušné věcné skupiny nebo do spisu.	4.2.17 upraveno
5.3.4	eSSL zajistí možnost ztvárnění informací vyhledaných dle kapitoly 5.1 nebo znázorněných dle kapitoly 5.2 do různých datových formátů dle jejich povahy a účelu (PDF/A, datový formát tabulkového procesoru, textového editoru).	
5.3.5	eSSL zajistí ztvárnění jednoho nebo více dokumentů v jedné operaci. Ztvárněný dokument obsahuje komponenty v pořadí stanoveném uspořádáním dokumentu.	
5.3.6	eSSL zajistí ztvárnění jednoho nebo více spisů v jedné operaci. Ztvárněný spis obsahuje a) název původce, b) spisový znak, c) skartační režim spisu, d) spisovou značku, číslo jednací nebo evidenční číslo ze samostatné ED, e) předmět (věc), f) zpracovatele, g) schvalovatele, h) soupis spisů a dokumentů připojených pevným křížovým odkazem, i) soupis spisů a dokumentů připojených volným křížovým odkazem, j) uživatelské poznámky spisu se jménem uživatele a datem, k) transakční protokol spisu, l) soupis dokumentů ve spisu, m) jednotlivé dokumenty a jejich komponenty. Samostatné datové soubory se řadí následujícím způsobem 1) údaje dle písmen a) až j), 2) transakční protokol [písmeno k)], 3) soupis dokumentů ve spisu ([písmeno l)], 4) jednotlivé dokumenty a jejich komponenty [písmeno m)]. *Například dokumenty se označí třímístným pořadovým číslem počínaje „001“ a každá jejich komponenta se (ve správním pořadí) označí dvoumístným pořadovým číslem komponenty za pomlčkou (např. „001-02“).*	
5.3.7	eSSL zajistí ztvárnění jedné nebo více součástí typového spisu v jedné operaci. Ztvárněná součást obsahuje a) název původce,	

	b) spisový znak, c) skartační režim součásti, d) název typového spisu, e) název součásti, f) soupis dokumentů a spisů připojených pevným křížovým odkazem, g) transakční protokol, h) soupis dokumentů ve spisu, i) jednotlivé spisy, dokumenty a jejich komponenty. Spisy, dokumenty a jejich komponenty se ztvární podle požadavku 5.3.6.	
5.3.8	eSSL umožní uživateli zvolit, zda komponenty dokumentů ztvárňovaného spisu budou a) ponechány ve stávajícím datovém formátu, nebo b) ztvárněny do výstupního datového formátu podle prováděcího právního předpisu upravujícího podrobnosti výkonu spisové služby.	
5.3.9	Soupis dokumentů nebo spisů připojených křížovým odkazem obsahuje zejména jejich číslo jednací nebo číslo spisu a jejich předmět (věc).	
5.3.10	eSSL při ztvárnění do výstupního datového formátu PDF/A použije verzi PDF/A-2 nebo vyšší v případě podepisování ztvárnění kvalifikovaným elektronickým podpisem. *K zjištění souladu s normou ISO 19005 pro jednotlivé verze PDF/A lze využít např. validátor Národního archivu na adrese http://digi.nacr.cz/validatorPDF/.*	
5.3.11	Jestliže je pro ztvárnění do výstupního datového formátu použita verze PDF/A-3, eSSL neumožní do PDF vložit komponentu v datovém formátu, který není výstupním datovým formátem, pokud není současně vloženo ztvárnění těchto komponent ve výstupním datovém formátu.	
5.3.12	eSSL u datového formátu, který nemá definován prováděcím právním předpisem upravujícím podrobnosti výkonu spisové služby výstupní datový formát, datový formát nepřevádí.	

6 UKLÁDÁNÍ A VYŘAZOVÁNÍ DOKUMENTŮ

6.1 Skartační režimy

Číslo	Požadavek	Původně
6.1.1	eSSL umožňuje výlučně správcovským rolím vytvářet a upravovat skartační režim.	5.1.1
6.1.2	eSSL neomezuje počet skartačních režimů.	5.1.2
6.1.3	eSSL vyžaduje od správcovské role provádějící úpravu nebo smazání skartačního režimu, aby zapsala důvod úpravy nebo smazání; tyto informace zaznamená eSSL do transakčního protokolu. *Úpravy skartačního režimu jsou důsledně kontrolovány tak, aby bylo minimalizováno riziko zničení dokumentu jiným způsobem, než který stanoví pravidla skartačního řízení.*	5.1.8
6.1.4	eSSL importuje a exportuje skartační režimy v rámci exportu spisového plánu ve struktuře dle přílohy č. 5.	5.1.9
6.1.5	eSSL zajišťuje, aby každá věcná skupina na nejnižší úrovni hierarchie, spis, součást, díl nebo dokument byl zařazen do skartačního režimu.	5.1.10 upraveno
6.1.6	Ve výchozí konfiguraci je skartační režim uplatňovaný na nově vytvořený dokument, spis, nebo díl děděn a) z mateřské věcné skupiny v případě spisu a dokumentu zatříděného přímo do věcné skupiny, b) ze spisu v případě dokumentu vloženého do spisu, c) z příslušné součásti v případě jejího dílu, d) z dílu typového spisu v případě dokumentu do dílu vloženého.	5.1.11 upraveno
6.1.7	eSSL umožňuje správcovské roli vždy přidělit skartační režim každé věcné skupině na nejnižší úrovni hierarchie, součásti nebo typu dokumentu. *Tento požadavek se uplatňuje v případě nahrazení skartačního režimu uplatněného ve výchozí konfiguraci jakýmkoli jiným.*	5.1.14 upraveno
6.1.8	Ukládání a vyřazování každého dokumentu se řídí skartačním režimem, přiřazeným k věcné skupině, spisu, dílu nebo typu dokumentu, do kterých dokument patří, popřípadě platným pozastavením skartační operace.	5.1.17
6.1.9	Každý skartační režim obsahuje a) skartační lhůtu a spouštěcí událost, nebo rok vyřazení seskupení nebo dokumentu, b) typ skartační operace (skartační znak „A“, „V“ nebo „S“).	5.1.19 upraveno
6.1.10	eSSL umožňuje v rámci každého skartačního režimu tyto typy skartačních operací a) návrh na trvalé uložení pro dokumenty trvalé hodnoty (dokumenty označené skartačním znakem „A“), b) návrh na předložení k přezkumu (dokumenty označené skartačním znakem „V“), c) návrh na zničení (dokumenty označené skartačním znakem „S“).	5.1.24 upraveno

6.1.11	eSSL umožňuje stanovit zejména následující spouštěcí události a) vyřízení dokumentu, vyřízení nebo uzavření spisu, uzavření typového spisu, součásti nebo dílu, b) vznik externí události, která je popsána ve skartačním režimu, a do eSSL ji zaznamená zpravidla správcovská role (například formou užití slov „po podpisu smlouvy“, „od likvidace skládky“ nebo „po zahájení insolvenčního řízení“).	5.1.25 upraveno
6.1.12	Pokud u dokumentu nebo seskupení současně platí další skartační režim s jinou skartační lhůtou nebo s jiným skartačním znakem, vzniká konflikt skartačních režimů. Konflikty vznikají v následujících případech a) dokument byl přetříděn z jiného spisu, dílu nebo věcné skupiny obsahující dokumenty, kde měl přidělen skartační režim, b) skartační režim se vztahuje k seskupení a k některým dokumentům v něm, které současně mají skartační režim přidělen na základě typu dokumentu, c) pokud jsou spisy spojovány pomocí pevných křížových odkazů [požadavek 4.2.2 písmeno a)], nebo d) jestliže jsou spisy pevnými křížovými odkazy vloženy do dílu typového spisu [požadavek 4.2.2 písmeno b)]. eSSL zajišťuje automaticky vyřešení konfliktů dle písmen a) a b) před uložením uzavřeného seskupení nebo vyřízeného dokumentu. Když eSSL iniciuje návrh na vyřazení spisu, u kterého vznikl konflikt popsaný v písmenu c) nebo d), automaticky o něm informuje posuzovatele skartační operace, který rozhodne, který ze skartačních režimů má mít přednost. Posuzovatel skartační operace při řešení konfliktu rozhodne o a) odstranění jednoho nebo více konfliktních skartačních režimů z příslušného seskupení nebo dotčených dokumentů, b) změně jednoho nebo více konfliktních skartačních režimů za účelem odstranění konfliktu, c) odstranění všech konfliktních skartačních režimů a aplikaci nového skartačního režimu.	5.1.23 upraveno
6.1.13	eSSL zajistí automatické vyřešení konfliktů skartačních režimů dle požadavku 6.1.12 písm. a) a b) následujícím způsobem: a) pokud spis nebo díl obsahuje dokument se skartačním znakem „V“ a „S“, označí spis skartačním znakem „V“, b) skartační lhůtu spisu nebo dílu stanoví podle dokumentu v tomto spisu nebo dílu, který má být zařazen do skartačního řízení nejpozději. Obdobně c) pokud spis nebo díl obsahuje dokument se	

	skartačním znakem „A“, označí spis skartačním znakem „A“, d) pokud spis nebo díl obsahuje pouze dokumenty se skartačním znakem „S“, označí spis skartačním znakem „S“.	
6.1.14	Pokud uplyne skartační lhůta stanovená určitému dokumentu, spisu nebo dílu skartačním režimem, eSSL vytvoří po vyřešení konfliktů skartačních režimů (požadavek 6.1.12) návrh na jejich vyřazení.	5.1.22 upraveno
6.1.15	eSSL umožňuje řízení výběru dokumentů výlučně posuzovateli skartační operace.	5.1.28
6.1.16	Pro přetřídění spisu nebo dokumentu mezi věcnými skupinami správcovskou rolí eSSL zajistí a) nahrazení existujícího skartačního režimu skartačním režimem nové mateřské věcné skupiny, b) výběr jiného skartačního režimu, nebo c) ponechání stávajícího skartačního režimu.	5.1.33
6.1.17	eSSL umožňuje, aby oprávněný uživatel nastavil u věcné skupiny, spisu, typového spisu, součásti, dílu nebo dokumentu přímo zatříděného do věcné skupiny příkaz k pozastavení skartační operace. Toto pozastavení se vztahuje na všechny dceřiné entity seskupení, na kterém bylo pozastavení skartační operace provedeno, i na dokumenty a seskupení připojené pevnými křížovými odkazy k entitám, kde k pozastavení došlo.	5.1.34 upraveno
6.1.18	Pozastavení skartační operace nepřerušuje plynutí skartační lhůty.	5.1.35
6.1.19	eSSL zabraňuje u entity (včetně jejích dceřiných entit), na kterou je uplatněno pozastavení skartační operace, a) smazání, b) zařazení do návrhu na vyřazení dokumentů.	5.1.36
6.1.20	eSSL umožňuje oprávněnému uživateli odstranění pozastavení skartační operace.	5.1.37
6.1.21	Pokud oprávněný uživatel zavede nebo odstraní pozastavení skartační operace, eSSL identifikuje a uloží do transakčního protokolu a) datum, kdy bylo pozastavení zavedeno nebo odstraněno, b) identifikaci oprávněného uživatele, c) důvod pozastavení.	5.1.38

6.2 Skartační řízení

Číslo	Požadavek	Původně
6.2.1	eSSL na základě pokynu posuzovatele skartační operace vytvoří návrh na vyřazení dokumentů, který je tvořen datovými balíčky SIP dle příloh č. 2 a 3; datový balíček SIP obsahuje a) spis, b) dokument zatříděný přímo do věcné skupiny, c) díl typového spisu, nebo d) všechny pevnými křížovými odkazy propojené entity	

	vztahující se k jednomu spisu nebo dílu. Tento návrh zpravidla neobsahuje komponenty dokumentů v digitální podobě. *Nezáleží přitom, zda uvedený dokument nebo seskupení obsahuje komponenty dokumentů v digitální podobě, podstatná jsou metadata.*	
6.2.2	Příloha k návrhu na vyřazení dokumentů obsahující datové balíčky SIP dle požadavku 6.2.1 se a) předá příslušnému archivu na technických nosičích dat, b) vloží na portál pro zpřístupnění archiválií v digitální podobě na základě uživatelského oprávnění posuzovatele skartační operace. *Nezbytnou součástí návrhu na vyřazení dokumentů je průvodní dopis, jehož přílohu tvoří technický nosič dat s balíčky SIP nebo přehled vytvořený portálem pro zpřístupnění archiválií v digitální podobě po uložení datových balíčků SIP.*	
6.2.3	eSSL vždy zaznamená v datovém balíčku SIP vazbu na uložení analogových komponent, pokud existují. *V případě dokumentů v analogové podobě je nezbytné spolu s evidencí udržovat jednoznačnou vazbu na fyzické dokumenty, které musí být v souladu s rozhodnutím o výběru archiválií přeneseny nebo zničeny.*	10.2.2 upraveno
6.2.4	eSSL exportuje datový balíček SIP obsahující komponenty digitálních dokumentů v průběhu archivní prohlídky, jestliže o to příslušný archiv požádá předáním seznamu datových balíčků SIP v podobě přílohy č. 4. V seznamu jsou požadované datové balíčky SIP uvedeny s operací „předložit k výběru“.	
6.2.5	eSSL zajistí vyznačení rozhodnutí o výběru archiválií na základě seznamu vytvořeného podle přílohy č. 4, který je zaslán příslušným archivem jako příloha protokolu o výběru archiválií: a) u entit s vyznačenou operací „vybrat za archiválii“ vytvoří datové balíčky SIP obsahující i komponenty dokumentů v digitální podobě a entity označí jako určené k přenosu nebo exportu do digitálního archivu (kapitola 6.3.) a v případě analogových entit nebo jejich částí k přenosu do příslušného archivu, b) u entit s vyznačenou operací „zničit“ tyto entity označí ke zničení (kapitola 6.3); přitom podporuje například prostřednictvím seznamů zničení odpovídajících entit v analogové podobě, c) u entit s vyznačenou operací „vyřadit z výběru“ vyzve posuzovatele skartační operace k úpravě skartačního režimu, d) u dotčených entit vyznačí identifikátor skartačního řízení (číslo jednací příslušného archivu).	
6.2.6	eSSL umožní posuzovateli skartační operace stanovit, které entity s vyznačenou operací „vybrat za archiválii“ budou určeny k přenosu a které k exportu. Toto rozhodnutí lze uskutečnit	

	a) jednotlivě pro konkrétní entity, nebo b) jedinou operací pro všechny entity označené „vybrat za archiválii“.	
6.2.7	eSSL vyznačí identifikátory digitálního archivu zaslané příslušným archivem v podobě seznamu dle přílohy č. 4 k příslušným entitám (příloha úředního záznamu o předání). Tím je export nebo přenos těchto entit úspěšně ukončen. *Současně musí být do příslušného archivu přeneseny entity v analogové podobě.*	
6.2.8	eSSL zabraňuje zničení dokumentu, spisu, typového spisu nebo dílu nebo jejich metadat, s výjimkou zničení po provedeném skartačním řízení.	3.4.19 upraveno

6.3 Přenos, export a zničení

Číslo	Požadavek	Původně
6.3.1	eSSL přenáší nebo exportuje dokumenty a jejich metadata stanovená příslušným schématem XML v příloze.	5.3.4
6.3.2	Vždy, když eSSL přenáší nebo exportuje dokumenty, přenáší nebo exportuje současně všechny jejich komponenty a zachovává vazby mezi těmito entitami.	5.3.2
6.3.3	eSSL zajišťuje přesně definovaný proces přenosu dokumentů a jejich metadat a informací transakčního protokolu do jiného systému nebo do jiné organizace.	5.3.3
6.3.4	Když eSSL přenáší nebo exportuje věcnou skupinu, spis, typový spis, součást nebo díl, zahrnuje tyto operace: a) přenos nebo export stanovené věcné skupiny, spisu, dokumentu, typového spisu, součásti nebo dílu, b) export všech entit hierarchicky nadřazených v případě, že je to požadováno, c) export spisů napojených k exportované nebo přenášené entitě pevným křížovým odkazem, d) přenos spisů napojených k exportované nebo přenášené entitě pevným křížovým odkazem, pokud jsou napojené spisy určeny k přenosu, e) export nebo přenos všech nebo vybraných metadat spojených s entitami uvedenými v písmenech a) až d), f) export nebo přenos transakčního protokolu pro všechny nebo vybrané entity uvedené v písmenech a) až d). eSSL exportuje veškerá metadata nebo transakční protokol, i když cílovým systémem, do kterého jsou data importována, nejsou požadována.	5.3.5 upraveno
6.3.5	Metadata, která nelze vložit do prvků příslušného schématu XML podle přílohy, eSSL a) ztvární jako dokument zpravidla ve formátu PDF/A, b) připojí k prvkům, které jsou v příslušném schématu XML přítomny.	

	Obdobně eSSL postupuje při exportu transakčního protokolu.	
6.3.6	eSSL exportuje nebo provádí přenos spisu, dílu, dokumentu nebo obsahu věcné skupiny v jedné posloupnosti operací tak, aby a) zůstaly nezměněny obsah a struktura je tvořících dokumentů v digitální podobě, b) byly jako celek exportovány všechny komponenty dokumentu v digitální podobě, který je tvořen více než jednou komponentou se zachováním jejich posloupnosti v dokumentu, c) byly zachovány všechny vazby mezi dokumentem a jeho metadaty a transakčním protokolem, d) byly zachovány všechny vazby mezi věcnými skupinami, spisy, typovými spisy, součástmi, díly, dokumenty, a to za účelem jejich možné rekonstrukce v systému, do něhož mají být dokumenty importovány.	5.3.9 upraveno
6.3.7	Když eSSL přenáší nebo exportuje spisy nebo díly, které obsahují pevné křížové odkazy na jiné entity, exportuje nebo přenáší i tyto odkazované entity, nikoli pouze odkazy na ně.	5.3.10 upraveno
6.3.8	eSSL exportuje a přenáší dokumenty v jakémkoli formátu (formátech), do kterého byly dokumenty ztvárněny nebo v němž byly přijaty.	5.3.12 upraveno
6.3.9	eSSL uchovává všechna seskupení, dokumenty, metadata a transakční protokoly, které jsou přenášeny, a to nejméně do doby potvrzení úspěšnosti ukončeného přenosu. Do této doby eSSL umožní kdykoli opakování přenosu. *Tento požadavek představuje záruku uchování dokumentů do doby, než je potvrzeno ukončení úspěšného přenosu dokumentů.*	5.3.14 upraveno
6.3.10	eSSL zničí seskupení, dokumenty, metadata a transakční protokoly, které jsou přenášeny, jestliže obdrží potvrzení o úspěšném ukončení přenosu, a to s výjimkou metadat, která jsou uchovávána v hlavičkách metadat (požadavek 6.3.14).	5.3.15
6.3.11	eSSL zničí seskupení, dokumenty, metadata a transakční protokoly, které byly určeny ke zničení při skartačním řízení (požadavek 6.2.5), a to s výjimkou metadat, která jsou uchovávána v hlavičkách metadat (požadavek 6.3.14).	
6.3.12	Pokud je v eSSL realizována konfigurační možnost podle požadavku 8.3.3, eSSL postupuje tak, že dokument zničí spolu s příslušnými metadaty, kromě metadat specifikovaných jako hlavička metadat (požadavek 6.3.14); eSSL tuto skutečnost zaznamená do transakčního protokolu (fyzické vymazání dokumentu).	9.3.4
6.3.13	eSSL zajišťuje, aby v něm byla zničena všechna ztvárnění dokumentu určeného ke zničení i tento dokument. Pokud je však na dokument určený ke zničení odkazováno pevným křížovým odkazem z jiného spisu, který zničení nepodléhá, dokument a jeho ztvárnění se nezničí, ale jsou přetříděny včetně údajů transakčního protokolu ničeného dokumentu. Pro seskupení platí toto ustanovení obdobně.	5.3.18 upraveno

	Dokument a jeho ztvárnění nebo seskupení nesmí být definitivně zničeny, dokud nebudou odstraněny všechny pevné křížové odkazy na ně nebo na jejich obsah.	
6.3.14	eSSL uchovává hlavičku metadat popisujících a) spisy, b) součásti, c) díly, nebo d) dokumenty uložené přímo ve věcné skupině, které byly zničeny nebo přeneseny.	5.3.19
6.3.15	Hlavička metadat obsahuje nejméně tyto údaje: a) jednoznačný identifikátor, b) datum vzniku, c) číslo jednací nebo evidenční číslo ze samostatné ED, d) datum zničení nebo přenosu, e) datum exportu nebo přenosu do digitálního archivu k trvalému uložení, f) spisový znak, g) název entity, h) popis, i) označení uživatele odpovědného za zničení nebo přenos, j) důvod zničení nebo přenosu (například uvedený posuzovatelem skartační operace nebo odkazem na skartační režim), k) odkaz, do kterého byly dokumenty přeneseny, s cílem usnadnit vyhledávání přenesených dokumentů, l) identifikátor digitálního archivu v případě, že byly dokumenty exportovány nebo přeneseny k trvalému uložení, m) číslo ze samostatné ED ISSD, jestliže byl do tohoto systému dokument přenesen.	5.3.20 upraveno
6.3.16	eSSL umožňuje správcovské roli stanovit podmnožinu dalších prvků metadat, která bude uchována jako hlavičky metadat.	5.3.21
6.3.17	eSSL umožňuje, aby byla tatáž metadata, transakční protokol a komponenty exportovány více než jednou.	5.3.23 upraveno
6.3.18	eSSL umožňuje provádět hromadný import dokumentů, seskupení a metadat podle přílohy č. 1.	6.2.1
6.3.19	eSSL umožňuje provádět hromadný export nebo přenos dokumentů, seskupení a metadat podle příloh č. 1, 2 a 3.	
6.3.20	eSSL exportuje, importuje nebo přenáší metadata entit v analogové podobě obdobně jako v případě metadat entit v digitální podobě.	10.2.3

7 KONTROLA A BEZPEČNOST

Původce musí zajistit takové programové vybavení (funkce) eSSL, které

a) umožní kontrolu povolení přístupu k dokumentům, protože dokumenty mohou obsahovat například osobní údaje, obchodní nebo jiné tajemství, na které se vztahuje ochrana podle jiných právních předpisů, popřípadě na jejichž ochraně má zájem původce sám,
b) umožní omezení přístupu pro externí uživatele, pokud tak stanoví jiný právní předpis nebo původce,
c) umožní sdílení částí úložiště eSSL.

Pro zajištění přístupu v eSSL a jako podporu obnovy dat lze ve správcem stanovených případech ukládat v transakčním protokolu informace o každém nahlédnutí do dokumentů a rozpracovaných dokumentů a o jiných činnostech týkajících se dokumentů i rozpracovaných dokumentů.

7.1 Přístup

Původce musí vytvořit organizační a technická opatření, která mu umožní kontrolovat přístup k jím spravovaným dokumentům. Tato organizační a technická opatření obsahují zejména specifikaci bezpečnostních opatření a pravidla jejich provádění tak, že přístup k dokumentům je poskytován v souvislosti s pracovní pozicí, kterou fyzická osoba (zaměstnanec) u původce plní. Bezpečnostní politika eSSL je určována centrálně, i když uživatelům jsou přístupová práva udělována k řadě informačních systémů původce, tedy včetně (nikoliv však výlučně) k systému eSSL.

Číslo	Požadavek	Původně
7.1.1	eSSL neumožňuje žádné osobě provést v něm jakoukoli operaci, není-li tato osoba oprávněným uživatelem, kterého eSSL úspěšně identifikoval a ověřil.	4.1.1
7.1.2	eSSL umožňuje správcovským rolím přidělovat na stanovenou dobu přístup k dokumentům, součástem, spisům, typovým spisům, věcným skupinám a metadatům konkrétním uživatelům, uživatelským rolím nebo skupinám uživatelů.	4.1.2
7.1.3	eSSL neomezuje počet uživatelských rolí nebo skupin uživatelů, které mohou být konfigurovány.	4.1.3
7.1.4	eSSL umožňuje správcovským rolím správu oprávnění pro všechny uživatelské role a skupiny uživatelů. Tato oprávnění určují funkce eSSL, prvky metadat, dokumenty, typové spisy nebo spisy, ke kterým mají uživatelské role a skupiny uživatelů přístup, a kategorie povoleného přístupu.	4.1.4
7.1.5	eSSL umožňuje správcovským rolím využít konfiguraci oprávnění tak, aby byl a) omezen přístup ke konkrétním typovým spisům, součástem, spisům nebo dokumentům, b) omezen přístup ke konkrétním věcným skupinám, c) omezen přístup v souvislosti s oprávněním uživatele, d) omezen přístup k určitým vlastnostem a funkcím eSSL (například ke čtení, k aktualizaci nebo k mazání určitých	4.1.5

	prvků metadat), e) odmítnut přístup po stanoveném datu, f) umožněn přístup po stanoveném datu.	
7.1.6	eSSL umožňuje správcovským rolím kdykoli přidělovat nebo odebírat uživatelům role a u skupin uživatelů přidávat nebo odebírat uživatele.	4.1.7
7.1.7	eSSL umožňuje přidělovat různým správcovským rolím správcovská práva k různým částem spisového plánu.	4.1.8
7.1.8	eSSL umožňuje správcovským rolím označit konkrétního uživatele jako neaktivního, aniž by tohoto uživatele vyřadil ze systému.	4.1.9
7.1.9	eSSL umožňuje správcovským rolím definovat pro uživatelské role stejná přístupová práva jako pro jednotlivé uživatele. *Tento požadavek umožňuje správcovským rolím spravovat a udržovat soubor přístupových práv spíše pro limitovaný počet rolí, než je udržovat pro velký počet jednotlivých uživatelů. Rolemi jsou například „obsluha podatelny“, „zpracovatel“, „vedoucí spisovny“, „správce databáze“*.	4.1.10
7.1.10	eSSL uplatňuje u jednotlivých rolí výběr přístupových práv.	4.1.11
7.1.11	eSSL umožňuje správcovským rolím zřizovat a udržovat skupiny uživatelů. *Skupinami uživatelů jsou například „vedení organizace“, „projektový tým“.*	4.1.12
7.1.12	eSSL umožňuje uživateli, aby byl členem jedné skupiny uživatelů, více skupin uživatelů, nebo aby nebyl členem žádné skupiny uživatelů.	4.1.13
7.1.13	eSSL umožňuje správcovským rolím vytvářet jednorázové účelové seznamy jednotlivých uživatelů pro kontrolu jejich přístupu ke konkrétním entitám.	4.1.14
7.1.14	eSSL omezuje použití systémových funkcí a s nimi souvisejících událostí jen na správcovské role.	4.1.15
7.1.15	eSSL umožňuje pouze správcovským rolím vytvářet uživatelské profily a přidávat uživatele do skupin uživatelů a přidělovat jim role.	4.1.16
7.1.16	eSSL umožňuje rolím schvalovatelů stanovit, kteří další uživatelé nebo skupiny uživatelů mají k příslušným dokumentům přístup.	4.1.17
7.1.17	eSSL omezuje jen na správcovské role provádění změn (například přidávání, úprava a mazání profilů u skupin uživatelů, rolí nebo uživatelů). *Tento požadavek se realizuje zejména prostřednictvím přístupových práv a jejich správy.*	4.1.18
7.1.18	eSSL umožňuje správcovským rolím vytvářet a spravovat pravidla s cílem určovat práva uživatelů k funkcím eSSL, a to tak, že různé role mají přístup k různým kombinacím funkcí.	4.1.19 upraveno
7.1.19	Pokud uživatel provádí vyhledávání zahrnující vyhledávání podle obsahu (například prostřednictvím plnotextového vyhledávání), eSSL nezahrne do výsledku hledání dokumenty, ke kterým nemá	4.1.22

	uživatel přístup.	
7.1.20	Pokud uživatel požaduje přístup k entitám, ke kterým nemá přístupová práva, a jejich vyhledávání nebo přístup požaduje provést jiným způsobem, než je uvedeno v požadavku 7.1.19, eSSL a) neposkytne žádné informace o entitě (uživateli není poskytnuta informace, zda entita existuje nebo nikoliv), b) potvrdí existenci entity (znázorní identifikaci spisu**,** typového spisu**,** součásti nebo dokumentu), popřípadě uvede schvalovatele entity, neznázorní však název ani jiná metadata, c) znázorní pouze název, typ entity (například u věcné skupiny a dokumentu), datum vytvoření a schvalovatele, nebo d) znázorní název a další metadata entity.	4.1.23
7.1.21	Správcovská role s výjimkou posuzovatele skartační operace nemá přístup ke komponentám.	
7.1.22	eSSL umožňuje, aby komponenty byly v úložišti šifrovány nebo zabezpečeny jinými prostředky k zamezení čtení nebo manipulace s nimi jinou osobou než oprávněným uživatelem a mimo eSSL.	

7.2 Transakční protokol

Transakční protokol je zápis provedených operací uskutečněných eSSL a v něm. Zahrnuje operace provedené uživateli nebo správci, anebo operace automaticky iniciované eSSL na základě parametrů systému. Transakční protokol umožňuje dohledat, identifikovat, popřípadě rekonstruovat činnost eSSL, jednotlivých uživatelů v systému a stav entit v minulosti.

Číslo	Požadavek	Původně
7.2.1	eSSL udržuje transakční protokol, ve kterém nemůže správce nebo uživatel provádět změny a který je schopný automaticky uložit údaje o a) operacích provedených s dokumenty, seskupeními nebo spisovými plány, b) uživateli, který operaci provádí, c) datu a času operace. Operace zaznamenané do transakčního protokolu zahrnují zejména a) příjem dokumentů v digitální podobě, b) přetřídění spisu nebo typového spisu v rámci spisového plánu, c) změny skartačních režimů, d) úkony spojené s přenosem nebo zničením entit, e) úkony spojené s pozastavením skartační operace, f) změny provedené v metadatech věcných skupin, spisů**,** typových spisů**,** součástí dokumentů nebo rozpracovaných dokumentů,	4.2.1

	g) pozměnění nebo smazání metadat uživatelem, h) změny provedené v přístupových oprávněních, i) vytvoření, změny nebo odebrání uživatelů nebo skupiny uživatelů, j) export nebo přenos, k) vytvoření znázornění, l) zničení dokumentů.	
7.2.2	eSSL zajišťuje, aby veškeré operace provedené s věcnou skupinou, spisem, typovým spisem, součástí, dílem, dokumentem nebo rozpracovaným dokumentem, které byly provedeny oprávněným uživatelem nebo jinou aplikací, byly zaznamenány do transakčního protokolu.	10.5.17
7.2.3	eSSL v transakčním protokolu zaznamenává zejména údaje stanovené přílohou č. 6.	
7.2.4	eSSL v prostředí vysokého zabezpečení systému (např. dokumenty obsahují osobní nebo jiné chráněné údaje) automaticky zaznamenává do transakčního protokolu každý přístup ke komponentám, dokumentům nebo seskupením.	4.2.3 D
7.2.5	Parametry transakčního protokolu eSSL jsou konfigurovatelné tak, aby správcovské role mohly určit, které operace nad rámec požadavku 7.2.1 budou automaticky zaznamenávané.	4.2.4
7.2.6	Po nastavení parametrů transakčního protokolu eSSL automaticky sleduje prováděné operace a informace o nich ukládá do transakčního protokolu.	4.2.6
7.2.7	eSSL zaznamenává do transakčního protokolu všechny operace prováděné s rozpracovanými dokumenty, dokumenty, díly, součástmi, spisy, typovými spisy**,** věcnými skupinami a skartačními režimy bez ohledu na to, zda předmětná operace ovlivňuje jednu nebo více z těchto entit.	4.2.8
7.2.8	eSSL exportuje data transakčního protokolu pro konkrétní dokumenty, díly, součásti, spisy**,** typové spisy a věcné skupiny bez ovlivnění transakčního protokolu samotného v podobě XML dle přílohy č. 6.	4.2.15 upraveno
7.2.9	eSSL zaznamená do transakčního protokolu informace o všech pokusech o narušení systému neoprávněným přístupem (pokus uživatele zpřístupnit si dokument, díl, součást**,** typový spis nebo spis, ke kterým má odepřen přístup).	4.2.16
7.2.10	eSSL zaznamenává do transakčního protokolu změny a údaje o nakládání s analogovými entitami obdobně jako v případě entit digitálních.	10.1.20

7.3 Záloha a obnova

eSSL pravidelně zálohuje dokumenty a metadata tak, aby byly neprodleně obnovitelné v případě jejich ztráty, při poruše systému, nepředvídatelné události nebo narušené bezpečnosti systému. Tato funkcionalita může být zajištěna jiným systémem.

Číslo	Požadavek	Původně
7.3.1	eSSL zajišťuje automatické zálohování a obnovu všech vybraných	4.3.1

	věcných skupin, spisů, typových spisů**,** dokumentů, metadat, správcovských parametrů a transakčního protokolu eSSL ve všech případech, které správce označí jako účelné.	
7.3.2	eSSL umožňuje správcovským rolím naplánovat zálohování a) stanovením četnosti zálohování v časovém intervalu, b) stanovením místa ukládání (ukládání na externí média, do jiného systému nebo do vzdáleného úložiště).	4.3.2
7.3.3	eSSL umožňuje obnovu ze záloh tohoto systému jen oprávněným správcovským rolím.	4.3.3
7.3.4	eSSL zajišťuje, že při obnově informací ze zálohy je zachována plná integrita dat, včetně transakčního protokolu. *Dokumenty, které byly smazány (označeny ke zničení) a uloženy v záloze, se zpravidla neobnovují.*	4.3.4
7.3.5	Pokud eSSL umožňuje zálohu a obnovu databáze pomocí funkcionality „body obnovení“, k použití této funkcionality jsou oprávněny pouze příslušné správcovské role.	4.3.5

7.4 Škodlivý kód

Číslo	Požadavek	Původně
7.4.1	eSSL obsahuje nebo je konfigurován ke spolupráci s počítačovými programy zajišťujícími bezpečnost informačních systémů a jejich komunikace.	4.5.1

8 SPRÁVCOVSKÉ FUNKCE

Tato část popisuje funkce údržby a systémové podpory. S funkcemi údržby a systémové podpory souvisejí funkce oprávnění k přístupu (kapitola 7.1) a zálohy a obnovy (kapitola 7.3).

8.1 Všeobecná správa

Tato kapitola stanoví požadavky na správu parametrů eSSL, zálohu a obnovu, správu a konfiguraci systému a správu uživatelů.

Číslo	Požadavek	Původně
8.1.1	eSSL umožňuje správcovským rolím vyhledávání, zobrazení a změnu parametrů a nastavení provedených v době konfigurace eSSL.	9.1.1
8.1.2	eSSL umožňuje správcovským rolím, aby a) přidělovaly oprávnění uživatelům a rolím a b) přiřadily jednoho nebo více uživatelů k jakékoli roli.	9.1.2
8.1.3	eSSL sleduje dostupný ukládací prostor, který je k dispozici, a uvědomí správcovské role o zaplnění ukládacího prostoru na úroveň nastavenou v době konfigurace jako limitní, nebo o tom, že došlo k chybě. Je přijatelné, aby byly správcovské role uvědomovány prostřednictvím samostatného softwaru pro správu systému.	9.1.3
8.1.4	eSSL umožňuje správcovským rolím snadným způsobem měnit postavení uživatele v rámci skupin uživatelů a rolí. eSSL umožňuje přesunout roli nebo změnit stav uživatele bez nutnosti smazání role nebo stavu z eSSL a opakovaného zavedení údajů o uživateli.	9.1.5 D
8.1.5	eSSL umožňuje správcovské roli konfigurovat nabídkové seznamy, z nichž uživatel vybírá hodnoty metadat pro jejich zápis.	10.14.2

8.2 Hlášení o stavu eSSL

Stavová hlášení jsou důležitou funkcí eSSL. Jejich účelem je umožnit správcovským rolím systém spravovat a vedení původce umožnit sledování práce v eSSL.

eSSL poskytuje stavová hlášení o své správě, stejně jako statistické a jednorázové zprávy, jejichž prostřednictvím správcovské role sledují činnost a stav systému. To je požadováno v celém eSSL a vztahuje se k

a) věcným skupinám,
b) spisům, typovým spisům a dokumentům,
c) aktivitě uživatelů,
d) přístupovým a bezpečnostním oprávněním a
e) výběru archiválií (skartačnímu řízení).

Číslo	Požadavek	Původně
8.2.1	eSSL zahrnuje funkce pro vytištění zpráv, jejich prohlížení na obrazovce a uložení v digitální podobě (například	9.2.2

	pro zpracování tabulkovým procesorem).	
8.2.2	eSSL ukládá nastavení žádostí o zpracování zpráv pro opětovné použití v budoucnu.	9.2.8
8.2.3	eSSL poskytuje zprávy o celkovém počtu a umístění a) spisů, typových spisů, součástí a dílů, b) komponent tříděných podle datového formátu a podle jejich verze, c) spisů, typových spisů, součástí a dílů tříděných podle kontroly přístupu a bezpečnostní kategorie, d) spisů, typových spisů, součástí a dílů obsahujících dokumenty v digitální podobě tříděných podle velikosti, e) spisů, typových spisů, součástí a dílů tříděných podle místa uložení.	9.2.10
8.2.4	eSSL poskytuje zprávy o a) množství přijatých dokumentů, b) množství vyhledaných dokumentů, c) množství nově vytvořených věcných skupin a spisů, d) četnosti použití spisových znaků u dokumentů a spisů.	9.2.11 upraveno
8.2.5	eSSL umožňuje správcovským rolím sestavit zprávy s přehledem nebo s počty dokumentů, spisů, typových spisů, součástí a dílů strukturované podle celého nebo části spisového plánu a za stanovené časové období.	9.2.16 upraveno
8.2.6	eSSL umožňuje správcovským rolím sestavovat zprávy z údajů transakčního protokolu. Tyto zprávy obsahují zejména informace o nejméně jedné entitě vybrané z následujících: a) věcná skupina, b) spis, c) typový spis, d) součást, e) díl, f) dokument, g) uživatel, h) časové období.	9.2.18
8.2.7	eSSL podává zprávu o výsledku procesu výběru archiválií s uvedením věcných skupin, spisů, typových spisů, součástí, dílů a dokumentů, které byly úspěšně zničeny, přeneseny nebo exportovány, s uvedením případných chyb, které v průběhu procesu nastaly.	9.2.20
8.2.8	eSSL poskytuje zprávy o výsledcích procesu exportu s uvedením věcných skupin, spisů, typových spisů, součástí, dílů a dokumentů, které byly úspěšně přeneseny nebo exportovány, s uvedením případných chyb, které v průběhu procesu nastaly.	9.2.21
8.2.9	eSSL poskytuje správcovským rolím zprávu o pokusu narušit kontrolu přístupu a další bezpečnostní zásady systému.	9.2.24
8.2.10	eSSL poskytuje zprávy o množství dokumentů za stanovené období, které mají být předmětem posouzení při provedení výběru archiválií.	9.2.26 D
8.2.11	eSSL poskytuje zprávu popisující každou chybu v průběhu procesu přenosu, exportu, zničení nebo smazání. Zpráva identifikuje dokumenty, seskupení a s nimi spojená metadata,	9.2.30

	při jejichž přenosu se vyskytly chyby, a entity, které nebyly úspěšně přeneseny, exportovány, zničeny nebo smazány.	
8.2.12	eSSL vytvoří zprávu popisující všechny chyby, které nastaly v průběhu importu. Zpráva identifikuje dokumenty, seskupení a s nimi spojená metadata, při jejichž importu se vyskytly chyby, a entity, které nebyly úspěšně importovány.	9.2.31
8.2.13	eSSL poskytuje správcovské roli nástroje pro vedení údajů nutných ke statistickým zpracováním informací o činnosti v rámci spisového plánu (včetně údajů o počtu a velikosti věcných skupin, spisů, typových spisů, součástí, dílů nebo dokumentů vytvořených, uzavřených, smazaných nebo zničených v průběhu daného období).	3.4.25

8.3 Změny a smazání dokumentů a rozpracovaných dokumentů

Základní zásadou výkonu spisové služby je, že spisy, typové spisy, součásti, díly i dokumenty a rozpracované dokumenty (s výjimkou provedení výběru archiválií) nemohou být zničeny.

Tato kapitola stanoví požadavky pro výjimečné situace, kdy může být nezbytné obsah dokumentu změnit nebo dokument smazat a nahradit. V určitých situacích je nutné, aby správcovské role „smazaly“ dokumenty, aby opravily chyby nebo například splnily povinnosti vyplývající z jiných právních předpisů.

Operace smazání představuje

a) fyzické vymazání, nebo
b) vyloučení z dalšího zpracování (uchování doprovázené zápisem v metadatech dokumentu, že se dokument považuje za přenesený nebo zničený).

Smazání je vždy výjimečnou operací, a tedy možnost smazání musí být přísně kontrolována, aby byla chráněna celková integrita dokumentů. Informace o smazání musí být zaznamenána do transakčního protokolu.

Číslo	Požadavek	Původně
8.3.1	eSSL ve výchozí konfiguraci zabraňuje zničení jednou přijatého dokumentu nebo rozpracovaného dokumentu s výjimkou skartačního řízení (kapitola 6.1).	
8.3.2	eSSL nabízí konfigurační možnost dokument nebo rozpracovaný dokument smazat – vyloučit z užívání.	9.3.1
8.3.3	eSSL nabízí konfigurační možnost, která ve výjimečných případech po souhlasu posuzovatele skartační operace umožňuje zničení jednou přijatého dokumentu nebo rozpracovaného dokumentu. *Tato možnost se užije v případě dokumentů, na které byl vydán příslušným archivem trvalý skartační souhlas.*	9.3.2
8.3.4	Pokud je v eSSL realizována konfigurační možnost podle požadavku 8.3.2, eSSL postupuje tak, že požadovaným způsobem jsou označena metadata dokumentu nebo rozpracovaného dokumentu a eSSL utají obsah a metadata tohoto dokumentu nebo rozpracovaného dokumentu před všemi uživateli, jakoby byl dokument nebo rozpracovaný	9.3.3

	dokument zničen, s tím, že umožní výjimku k přístupu k tomuto dokumentu nebo rozpracovanému dokumentu výlučně pro oprávněnou správcovskou roli; eSSL současně tyto skutečnosti zaznamená do transakčního protokolu (vyloučení dokumentu).	
8.3.5	Správcovským rolím je umožněno změnit jakýkoli uživatelem zapsaný prvek metadat. *Tato funkce umožňuje správcovským rolím provádět případné opravy chyb uživatelů (například chyby při vkládání dat, chybné zařazení ve spisovém plánu).*	9.3.8

9 ROZHRANÍ K PROPOJENÍ INFORMAČNÍCH SYSTÉMŮ SPRAVUJÍCÍCH DOKUMENTY

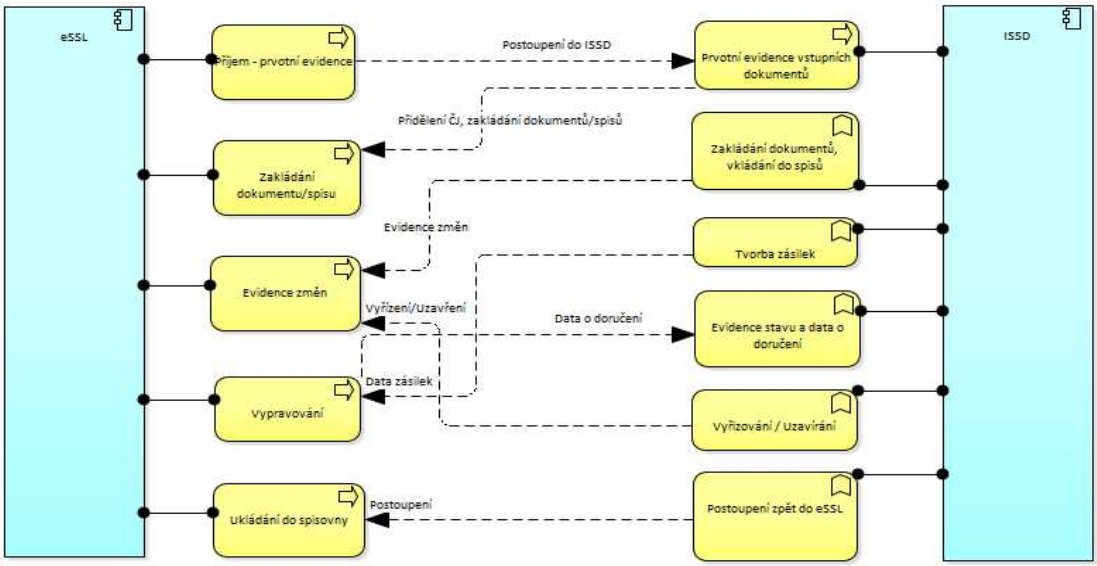
9.1 Vazby mezi systémy pro správu dokumentů

Všechny systémy pro správu dokumentů (ISSD) provozované původcem musí plnit požadavky tohoto standardu, avšak mohou je plnit i tak, že jsou integrovány s centrálním (z hlediska původce) provozovaným eSSL. V tom případě musí vzájemné integrační rozhraní plně podporovat požadavky a funkce podle této kapitoly.

Rozhraní je řešeno na bázi webových služeb, přičemž má dvě části, synchronní i asynchronní. Obě části jsou implementovány současně a pracuji nad společnými daty. Synchronní funkce se využívají pouze v nezbytně nutné míře, neboť jsou vždy závislé na on-line dostupnosti obou provázaných ISSD, resp. eSSL. Vše ostatní je řešeno asynchronními funkcemi.

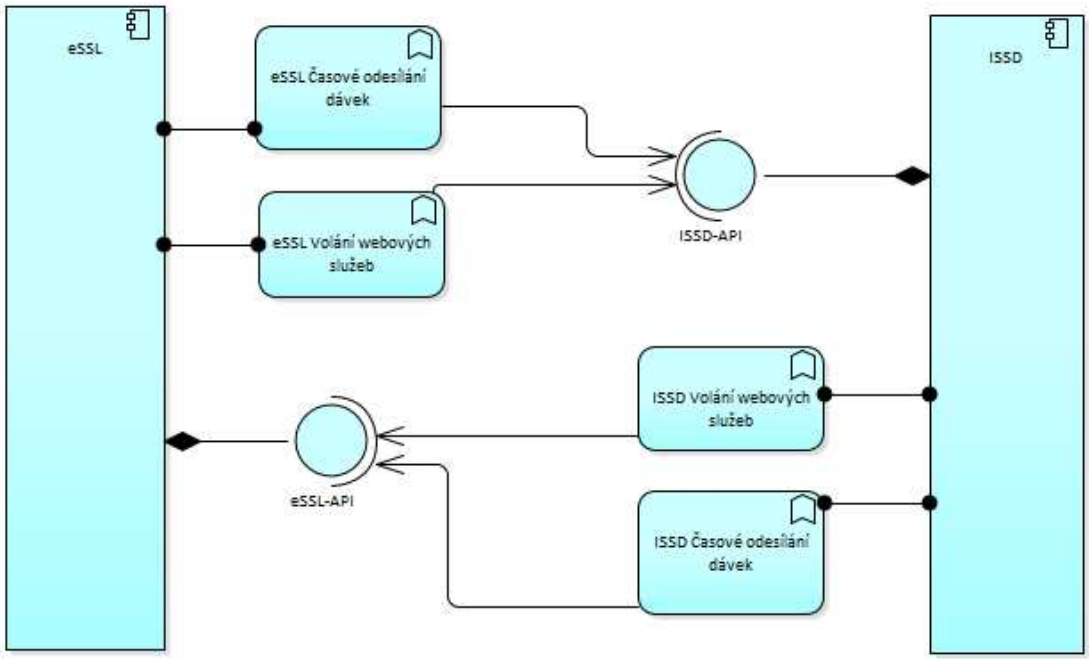
Synchronní rozhraní je založeno na okamžitém zpracování jednoho atomárního (dále nedělitelného) požadavku předaného voláním webové služby. Tento požadavek je jako celek volanou stranou okamžitě zpracován, a to úspěšně nebo neúspěšně. V obou případech je volající okamžitě informován o výsledku zpracování a získá tak potřebná data pro další svou práci nebo se v případě neúspěšného zpracování dozví důvod neúspěšného zpracování a může na zjištěné skutečnosti adekvátně reagovat.

Asynchronní rozhraní je založeno na dávkách, které se v určitých časových periodách na straně odesilatele připravují. Poté se prostřednictvím komunikačního kanálu odešlou protistraně. Příjemce v rámci příjmu dávky nezahájí okamžité zpracování dávky, pouze překontroluje její formální správnost a dávku uloží pro následné zpracování. Ke zpracování přijatých dávek dojde odloženě, a to většinou v předem zvolených časových periodách. Obsah dávek se zpracuje a výsledky zpracování se odešlou jako dávka zpět. Protistrana, opět odloženě, zpracuje dávku obsahující výsledky zpracování dříve odeslaných dávek a teprve po potvrzení úspěšného zpracování tyto dávky může považovat za převzaté a zpracované protistranou. Schematicky je vazba znázorněna na následujícím obrázku.



Obrázek č. 3 – procesní schéma komunikace eSSL a ISSD.

Rozhraní je založeno na přenosu dat popisujících události a dat spojených se vzniklými událostmi. Událostí se pro účely tohoto rozhraní rozumí popis jednoho nedělitelného procesu, který je vyobrazen na níže uvedeném diagramu.



Obrázek č. 4 – schéma rozhraní pro komunikaci eSSL a ISSD.

Manipulace s entitami na obou stranách spolu s oboustrannou komunikací a asynchronním přenosem dat jednoznačně vede k potřebě stanovit pravidlo, kdo smí s entitou aktuálně manipulovat. Toto pravidlo stanoví, že entity, které jsou předmětem komunikace v rámci tohoto rozhraní, budou vždy ve výhradní správě pouze jednoho z obou systémů ISSD, resp. eSSL. Systém, který bude mít entitu ve výhradní správě, smí realizovat všechny manipulace s ní, které jsou v rámci metodiky práce systému korektní. Všechny realizované manipulace s entitou musí systém s výhradní správou entity prostřednictvím dávek oznámit druhému nebo dalším systémům, které k entitě v té době výhradní správu nemají.

Číslo	Požadavek	Původně
9.1.1	eSSL umožňuje synchronní i asynchronní komunikaci s dalšími ISSD, přičemž toto rozhraní je realizováno prostřednictvím webových služeb a schémat XSD uvedených v příloze č. 1.	
9.1.2	eSSL umožňuje nastavit rozhraní pro více různých ISSD. Počet těchto spojení není omezován. Každé spojení je identifikováno unikátním (v rámci původce) identifikátorem, který je používán v kořenovém elementu komunikačních dávek jako zdroj a cíl komunikace. Též eSSL má pro tyto účely komunikace přiřazen svůj unikátní (v rámci původce) identifikátor.	
9.1.3	eSSL umožňuje, aby identifikace dle požadavku 9.1.2 mohla být rozšířena o certifikát elektronického podpisu, který může být volitelně použit při zabezpečení dávek XML elektronickou pečetí.	
9.1.4	Rozhraní mezi eSSL a ISSD je založeno na nedělitelných událostech dle požadavků 9.1.8 a 9.1.11 a pracuje	

Číslo	Požadavek	Původně
	s komponentami, dokumenty, spisy, zásilkami a jejich metadaty.	
9.1.5	Při synchronní komunikaci dle 9.1.1 volaná strana okamžitě vykoná požadovanou událost. Výsledek události je vrácen volající straně jako výsledek volání webové služby.	
9.1.6	V rámci jednoho volání synchronní webové služby podle 9.1.8 musí být událost buď zcela a bezezbytku zpracována, nebo v případě vzniku chyby nebo stavu, kdy příjemce aktivně odmítne událost zpracovat, nesmí být zpracována vůbec. Částečné zpracování události je nepřípustné.	
9.1.7	Při příjmu opakované identické události, která již byla jednou úspěšně provedena, musí volaná strana vrátit vždy stejný výsledek. Takové opakování se nesmí považovat za chybu. Volaná strana událost podruhé nezpracuje, ale pouze volajícímu vrátí stejnou výslednou informaci, jako při prvním úspěšném zpracování události.	
9.1.8	Synchronní rozhraní eSSL poskytuje pro ISSD nejméně následující funkce: • SpisZalozeni – založení spisu nad dokumentem. Je možné založit celý spis i s dokumenty v něm, nebo je spis založen nad existujícím dokumentem. • DokumentZalozeni – zaevidování nového dokumentu přijatého nebo vzniklého v ISSD. • DokumentPostoupeniZadost – žádost o postoupení dokumentu (převzetí dokumentu do výhradní správy volajícím systémem). • ProfilDokumentuZadost – žádost o poskytnutí detailních informací o dokumentu. • ProfilSpisuZadost – žádost o poskytnutí detailních informací o spisu. • SouborZadost – žádost o poskytnutí obsahu zadané komponenty. • CiselnikZadost – žádost o poskytnutí číselníku. Kód (název) číselníku zpravidla odpovídá názvu elementu, k němuž se číselník vztahuje. • DavkySeznam – služba umožní ISSD získat seznam dávek, které jsou v eSSS pro daný ISSD připraveny. • DavkaZadost – služba umožní ISSD získat z eSSL dávku. Služba je určena pro ISSD, které neposkytují službu (webový server) pro příjem dávek. • FunkcniMista – služba umožní získat ISSD seznam organizačních součástí původce na základě osobního čísla uživatele. • Udalosti – žádost o okamžité vykonání předaného pole událostí a to v jediné uzavřené operaci. • WsTestSyn – funkce pro otestování komunikace. Pouze informuje o aktuální dostupnosti eSSL nebo ISSD. • PrideleneSeznam – funkce pro zaslání seznamu všech entit konkrétního uživatele v eSSL.	

Číslo	Požadavek	Původně
9.1.9	eSSL i ISSD v rámci asynchronního rozhraní sdružují události do dávek. Součástí dávek jsou též zprávy o zpracování přijatých událostí. Dávka může obsahovat a) události, b) zprávy, nebo c) události a zprávy.	
9.1.10	Asynchronní rozhraní eSSL i ISSD poskytuje minimálně následující funkce: • ESSLAsyn – přenos dávek obsahujících události a zprávy podle 9.1.9. • WsTest – funkce pro otestování komunikace. Pouze informuje o aktuální dostupnosti eSSL nebo ISSD.	
9.1.11	eSSL podporuje příjem nejméně následujících událostí: • DokumentUprava – úprava metadat existujícího dokumentu. • DokumentZruseni – stornování existujícího dokumentu. • SpisZalozeni – založení spisu nad dokumentem. Iniciační dokument je vložen do spisu. • SpisUprava – úprava metadat existujícího spisu. • DokumentVlozeniDoSpisu – vložení dokumentu do spisu. Spis nesmí být uzavřen. Pokud je spis veden sběrným archem a dokument měl již přiděleno číslo jednací, dostává dokument nové na základě sběrného archu. Pokud je spis veden sběrným archem a dosud neměl přiděleno číslo jednací, je mu přiděleno podle pořadí na sběrném archu. • DokumentVyjmutiZeSpisu – vyjmutí dokumentu ze spisu. Dokument a spis musí existovat, spis nesmí být uzavřen. • SpisVyrizeni – vyřízení spisu včetně všech vložených dokumentů. Podle konfigurace eSSL může být vyřízení spisu spojeno také s jeho uzavřením. • SpisOtevreni – otevření dříve uzavřeného spisu. • SpisZruseni – stornování spisu včetně všech vložených dokumentů. • DoruceniUprava – změna metadat dokumentu týkajících se informací o přijetí původcem. • VypraveniZalozeni – založení zásilky pro dokument. Stav nové zásilky je „nevypraveno“. • VypraveniUprava – úprava metadat zásilky. • VypraveniVypraveno – předání informace, že zásilka byla vypravena. • VypraveniDoruceno – zápis informací o doručení k zásilce. • VypraveniZruseni – stornování zásilky. • VypraveniPredatVypravne – pokyn k předání zásilky do výpravny k vypravení. • SouborZalozeni – založení komponenty. V události může být předán elektronický obsah přímo nebo pouze	

Číslo	Požadavek	Původně
	odkaz (identifikátor) na soubor a v takovém případě eSSL poskytuje ISSD REST službu (adresu URL), která na základě identifikátoru vrátí elektronický obsah komponenty včetně mimeType. REST služba musí podporovat metodu GET, názvy parametrů jsou „HodnotaID“ a „ZdrojID“. • SouborNovaVerze – nahrazení stávající komponenty novou. • SouborZruseni – odstranění komponenty. • SouborVlozitKDokumentu – přiložení existující komponenty k dokumentu. • SouborVyjmoutZDokumentu – odstranění komponenty z dokumentu. Komponenta nesmí být u tohoto dokumentu součástí zásilky, která je předána k vypravení. • SouborVlozitKVypraveni – určení komponenty, že bude součástí zásilky. • SouborVyjmoutZVypraveni – určení komponenty, že nebude dále součástí zásilky. • DokumentZmenaZpracovatele – předání dokumentu jinému zpracovateli. Při předání mezi uživateli je v elementu „Autorizace“ původní držitel, element „Prebirajici“ obsahuje údaje o novém držiteli. Při administrativním přidělení je administrátor v elementu „Autorizace“ a v elementu „Prebirajici“ je nový držitel dokumentu. Pokud k události došlo jindy než v okamžiku zaevidování, je možno do elementu „predanoKdy“ uvést skutečné datum události. • SpisZmenaZpracovatele – předání spisu a všech vložených dokumentů jinému zpracovateli. Při předání mezi uživateli je v elementu „Autorizace“ původní držitel, element „Prebirajici“ obsahuje údaje o novém držiteli. Při administrativním přidělení je administrátor v elementu „Autorizace“ a v elementu „Prebirajici“ je nový držitel spisu. Pokud k události došlo jindy než v okamžiku zaevidování, je možno do elementu „predanoKdy“ uvést skutečné datum události. • DokumentVraceni – předání výhradní správy dokumentu z ISSD do eSSL. • SpisVraceni – předání výhradní správy spisu a všech v něm vložených dokumentů dokumentu z ISSD do eSSL. • DokumentVyrizeni – označení dokumentu za vyřízený. Podle konfigurace jiného ISSD, resp. eSSL může být vyřízení dokumentu spojeno také s jeho uzavřením. • SpisUzavreni – uzavření vyřízeného spisu. • DokumentUzavreni – uzavření vyřízeného dokumentu. • DokumentOtevreni – znovuotevření dříve uzavřeného dokumentu.	

Číslo	Požadavek	Původně
	• DokumentExterniSpousteciUdalost, SpisExterniSpousteciUdalost – předání informace, že nastala událost, kterou je podmíněn začátek běhu skartační lhůty. • SouborOdemkniFinal – událost zruší příznak konečného tvaru komponenty.	
9.1.12	ISSD podporuje příjem nejméně následujících událostí: • DokumentPostoupeni – předání dokumentu do výhradní správy jiného ISSD, resp. eSSL. • SpisPostoupeni – předání spisu do výhradní správy jiného ISSD, resp. eSSL. • VypraveniVypraveno – předání informace, že zásilka byla vypravena. • VypraveniDoruceno – předání informace, zda zásilka byla nebo nebyla doručena. • SouborZalozeni – předání komponenty jinému ISSD, resp. eSSL. Událost je potřeba použít před použitím komponenty v dalších událostech, např. DokumentPostoupeni. V události může být předán elektronický obsah komponenty přímo anebo pouze odkaz (identifikátor) na komponentu; v takovém případě poskytuje ISSD jinému ISSD nebo eSSL REST službu (adresu URL), která na základě identifikátoru vrátí elektronický obsah včetně mimeType. REST služba musí podporovat metodu GET, názvy parametrů jsou „HodnotaID“ a „ZdrojID“. • SpisSkartovano, DokumentSkartovano – předání informace, že nad spisem, resp. dokumentem proběhlo skartační řízení.	
9.1.13	V případě zpracování událostí v dávkách při asynchronní komunikaci jsou transakce realizovány na úrovni událostí, nikoliv dávek. *Jedná se o rozdíl oproti synchronní komunikaci dle požadavku 9.1.6.*	
9.1.14	Po odeslání jedné dávky nemusí odesílatel čekat s odesláním dalších dávek až do příjmu potvrzení o zpracování předchozí odeslané dávky příjemcem. Lze odesílat i několik po sobě jdoucích dávek bez čekání na jejich zpracování a potvrzení protistranou.	
9.1.15	Číslování dávek je unikátní jen pro každou vazbu, tj. komunikaci mezi eSSL a jiným ISSD. Dávky jsou číslovány vzestupnou řadou s přírůstkem 1. Pořadová čísla dávek na sebe musí navazovat v nepřerušené, spojité řadě.	
9.1.16	Pořadí dávek musí odpovídat pořadí dávek podle položky DatumVzniku uvedené v hlavičce každé dávky.	
9.1.17	Události jsou číslovány vzestupnou řadou v rámci každé dávky. Pořadová čísla událostí nesmí svým pořadím odporovat pořadí zápisu událostí v XML souboru dávky. Číslo události nemusí	

Číslo	Požadavek	Původně
	být unikátní pro různé dávky. Počáteční hodnota, přírůstek ani spojitost číselné řady pro číslování událostí nejsou vyžadovány.	
9.1.18	Dávky musí být vždy zpracovávány sekvenčně. Následující dávku lze zpracovat jen, pokud byla úspěšně zpracována dávka předchozí. Pokud nastane při zpracování dávky chyba, potom se zpracování všech dávek zastaví a musí se realizovat opravné zaslání a zpracování dávky, ve které byla detekována chyba, poté musí následovat sekvenční odeslání všech následujících dávek, a to i v případě, že již byly dříve zaslány. Tedy od chybně zpracované dávky se musí znovu poslat postupně všechny dávky znovu, přičemž první musí být poslána opravená dávka, ve které byla detekována chyba.	
9.1.19	Každá dávka musí ve své hlavičce obsahovat identifikaci zdroje a cíle dávky.	
9.1.20	Události jsou zpracovávány důsledně v pořadí, ve kterém jsou zapsány v dávce. Toto pořadí (umístění v dávce) musí odpovídat pořadí číselného označení událostí podle 9.1.17.	
9.1.21	Událost musí být zpracována zcela, nebo nesmí být zpracována vůbec. Není přípustné částečné, neúplné zpracování jedné události. *Jedná se o obdobu požadavku 9.1.6 pro asynchronní komunikaci.*	
9.1.22	Událost lze považovat za úspěšně odeslanou a zpracovanou příjemcem pouze v případě, že je zpracování potvrzeno v některé z následujících přijatých dávek.	
9.1.23	Dávku lze považovat za zpracovanou pouze v případě, že všechny v ní obsažené události byly protistranou potvrzeny jako úspěšně zpracované.	
9.1.24	Je povoleno použít při potvrzení událostí následující zjednodušení: Pokud je potvrzeno úspěšné zpracování poslední události v dávce, potom jsou tímto potvrzena úspěšná zpracování všech událostí této dávky.	
9.1.25	Komunikace dle 9.1.1 probíhá prostřednictvím protokolů http nebo https. Pokud probíhá komunikace výhradně v rámci počítačové sítě původce, postačí protokol http. Pokud probíhá prostřednictvím veřejné sítě (Internetu), musí být použit zabezpečený protokol https. Jako vyšší stupeň zabezpečení může https server vyžadovat při komunikaci autentizaci klienta klientským certifikátem. *Použití zabezpečeného protokolu https není primárně určeno pro ověření autentičnosti dat – jeho účelem je filtrování neoprávněných pokusů o průnik do počítačové sítě apod.*	
9.1.26	Integrita dat může být zabezpečena elektronickou pečetí přenášených XML dávek ve standardu dle platných právních předpisů. Použití nebo nepoužití tohoto zabezpečení závisí na konkrétní vazbě a eSSL musí umožňovat toto nastavení samostatně pro každou vazbu na jiný ISSD. Vztah mezi	

Číslo	Požadavek	Původně
	označením zdroje komunikace a konkrétním certifikátem elektronického podpisu nebo elektronické pečeti se nastaví při zavádění rozhraní, a to jako součást výchozí konfigurace komunikujících eSSL a ISSD.	
9.1.27	Přístup k entitám je vždy výhradní, tedy události týkající se dané entity smí vytvářet pouze systém, který má aktuálně entitu ve své výhradní správě. Změna výhradní správy z jednoho systému na druhý je možná pouze prostřednictvím příslušných událostí. Výjimka je přípustná pouze jedna a je popsána požadavkem 9.1.29.	
9.1.28	Systém s aktuálně nevýhradní správou může požádat voláním synchronní metody rozhraní o postoupení dokumentu z výhradní správy druhého systému do své výhradní správy. Této žádosti o postoupení výhradní správy dokumentu druhý systém může a nemusí vyhovět. V případě zamítnuté žádosti o převzetí do výhradní správy musí volaný systém navrátit chybový kód, který bude popisovat zdůvodnění takového odmítnutí.	
9.1.29	eSSL musí obsahovat správcovskou funkci, která zruší příznak výhradní správy entity ISSD zejména v případě nefunkčnosti tohoto systému. U každé této servisní operace je třeba evidovat důvod a zaznamenat ji do transakčního protokolu.	
9.1.30	V době konfigurace vazby mezi eSSL a ISSD musí být: a) sjednoceny všechny hodnoty ve všech propojených systémech, nebo b) vytvořeny a implementovány převodní můstky mezi hodnotami použitými v jednotlivých systémech. Jedná se zejména o následující metadata: • Uživatel („provedlKdo“, „novyZpracovatel“, „VlastniKdo“) • Spisový plán („SpisovyPlan“) • Spisových znak („SpisovyZnak“) • Typ dokumentu („TypDokumentu“) • Podací deník („PodaciDenik“) • Způsob vyřízení spisu nebo dokumentu („ZpusobVyrizeni“)	
9.1.31	eSSL umožní postoupit entitu ke zpracování ISSD na žádost uživatele podanou prostřednictvím ISSD. Uživatel ISSD si může vyžádat seznam přidělených dokumentů, spisů a dílů typových spisů prostřednictvím ISSD bez toho, že by musel pracovat s eSSL.	
9.1.32	Identifikátor entity přiděluje vždy ten ze systémů (eSSL nebo ISSD), který objekt zaeviduje jako první. Ostatní systémy musí identifikátor převzít.	
9.1.33	Označení zdroje identifikátoru podle 9.1.32 je shodné s identifikací podle 9.1.2 a musí být v rámci původce unikátní.	
9.1.34	V případech, kdy je nutné mezi systémy eSSL a ISSD vyměňovat, popř. modifikovat metadata nad rámec specifikace jednotlivých funkcí (požadavek 9.1.8) nebo událostí	

Číslo	Požadavek	Původně
	(požadavky 9.1.11 a 9.1.12), jsou funkce a události vybaveny obecným elementem „DoplnujiciData“, který slouží pro specifikaci takovýchto metadat. Výčet a rozsah následného užití těchto metadat závisí na implementaci rozhraní mezi eSSL a ISSD.	

10 DOKUMENTACE ŽIVOTNÍHO CYKLU eSSL

10.1 Dokumentace eSSL

Tato kapitola specifikuje požadavky na dokumentaci, kterou vede původce vykonávající spisovou službu v eSSL nebo ISSD, a to pro každý eSSL nebo ISSD, který provozuje. Účelem požadavků je dokumentovat základní skutečnosti provozu eSSL nebo ISSD, a to jak pro potřebu původce, tak pro plnění povinností vyplývajících z působnosti kontroly (například příslušného archivu).

Dokumenty s údaji vyžadovanými touto kapitolou jsou během životního cyklu ukládány do typového spisu eSSL nebo ISSD vedeného v analogové podobě. Pokud některé z dokumentů uvedených v této kapitole s výjimkou evidenčního listu eSSL nebo ISSD neexistovaly, není to důvod k jejich dodatečnému vytváření.

Číslo	Požadavek	Původně
10.1.1	O eSSL nebo ISSD se vedou, doplňují a aktualizují údaje v typovém spisu, a to po celou dobu životního cyklu eSSL nebo ISSD.	11.1.1
10.1.2	Typový spis eSSL nebo ISSD obsahuje evidenční list eSSL nebo ISSD, ve kterém jsou uvedeny: a) název eSSL nebo ISSD jako obchodního produktu, b) obchodní firma dodavatele eSSL nebo ISSD, c) datum uvedení eSSL nebo ISSD do zkušebního provozu, d) datum uvedení eSSL nebo ISSD do řádného provozu, e) informace o významných změnách eSSL nebo ISSD (například informace o změnách datové struktury a migracích eSSL nebo ISSD na jeho nové verze), f) datum ukončení provozu eSSL nebo ISSD, g) technická charakteristika eSSL nebo ISSD, zejména použité technologie a databáze, h) věcná charakteristika eSSL nebo ISSD, zejména určení části agendy původce, na niž se vztahuje (rozsah zpracovávaných dat), i) přehled právních předpisů vztahujících se k obsahu eSSL nebo ISSD, j) údaje o přístupu veřejnosti k eSSL nebo ISSD (například internetová adresa stránky s přístupem k eSSL nebo ISSD), k) přehled správcovských rolí a správců eSSL nebo ISSD a jejich zařazení v organizační struktuře původce, l) přehled uživatelských rolí a jejich charakteristika.	11.1.2
10.1.3	Typový spis eSSL nebo ISSD obsahuje doklady o nabytí, právním titulu a podmínkách jeho užívání (licence) a dokumentaci o zavedení eSSL nebo ISSD u původce, a to včetně předávacích protokolů.	11.1.3
10.1.4	Typový spis eSSL nebo ISSD obsahuje analytickou a projektovou dokumentaci a dokumentaci o zavádění eSSL nebo ISSD u původce, a to včetně předávacích protokolů.	11.1.4

10.1.5	Typový spis eSSL nebo ISSD obsahuje systémovou příručku, jejímiž náležitostmi jsou a) minimální softwarové požadavky, b) minimální hardwarové požadavky, c) údaje rozhodné pro konfiguraci eSSL nebo ISSD, zejména popis uživatelských a správcovských rolí, d) údaje o způsobech a použití šifrování, e) popis vazeb na jiné eSSL nebo ISSD a externí software.	11.1.5
10.1.6	Typový spis eSSL nebo ISSD obsahuje uživatelské příručky pro všechny uživatelské a správcovské role, popřípadě školicí texty.	11.1.6
10.1.7	Typový spis eSSL nebo ISSD obsahuje vnitřní předpisy, jimiž jsou stanovena pravidla pro provoz eSSL nebo ISSD, například spisový řád, spisový a skartační plán, vnitřní předpisy původce pro oběh účetních údajů.	11.1.7
10.1.8	Typový spis eSSL nebo ISSD obsahuje bezpečnostní dokumentaci popisující zejména způsoby zálohování, obnovy ze zálohy a uložení záložních dat.	11.1.9

11 METADATA

Tato kapitola stanoví základní funkční požadavky na metadata a způsob jejich zpracování.

11.1 Obecné požadavky na metadata

Číslo	Požadavek	Původně
11.1.1	eSSL neomezuje počet prvků metadat povolených pro každou entitu.	12.1.1
11.1.2	eSSL je nakonfigurován tak, aby metadata byla zpracovávána zpravidla automaticky. *Například pokud eSSL ukládá metadata týkající se data otevření spisu, tato data se zaznamenávají automaticky, kdykoli je spis otevřen, tedy aniž by byl k tomu uživatel vyzván*.	12.1.2
11.1.3	eSSL umožňuje v době konfigurace definovat různé sady prvků metadat pro specifické typy dokumentů v digitální podobě. Například faktury se odlišují použitím metadat čísel účtů.	12.1.3
11.1.4	eSSL umožňuje správcovské roli v době konfigurace definovat, který prvek metadat je povinný a který volitelný.	12.1.4
11.1.5	eSSL podporuje zejména následující formáty prvků metadat: a) alfabetické, b) alfanumerické, c) numerické, d) časové, e) logické („ANO/NE“).	12.1.5
11.1.6	eSSL podporuje pro všechny jím zpracované časové údaje časové formáty stanovené v ČSN ISO 8601.	12.1.7
11.1.7	eSSL umožňuje správcovské roli stanovit, které hodnoty prvků metadat mají být zapsány a udržovány ručně nebo výběrem z číselníku.	12.1.9
11.1.8	eSSL podporuje kontrolu platnosti metadat, pokud jsou metadata zapsána uživateli nebo jsou importována. Kontrola platnosti metadat postihuje zejména a) formát obsahu prvku, b) rozmezí hodnot, c) ověření podle řízeného slovníku hodnot udržovaného správcovskou rolí.	12.1.14
11.1.9	eSSL umožňuje ověřovat metadata prostřednictvím jiných softwarových aplikací nebo podle interního číselníku.	12.1.15 upraveno
11.1.10	eSSL umožňuje správcovské roli konfigurovat ověřování metadat v souladu s požadavky 11.1.8 a 11.1.9 tak, aby se vztahovalo na každý metadatový prvek.	12.1.16
11.1.11	eSSL umožňuje správcovské roli omezit provádění změn v hodnotách metadat pro jednotlivé správcovské nebo uživatelské role nebo pro konkrétního uživatele.	12.1.21
11.1.12	eSSL umožňuje správcovské roli změnu konfigurace	12.1.22

	metadat, která jsou zaznamenávána do transakčního protokolu.	
11.1.13	eSSL umožňuje konfiguraci prvků metadat v době konfigurace tak, aby hodnoty generované eSSL nebo jinými softwarovými aplikacemi (například data o odeslání e-mailové zprávy) nemohli uživatelé změnit.	12.1.23

11.2 Požadavky na metadata datových balíčků SIP dle příloh č. 2 a 3

Číslo	Požadavek	Původně
11.2.1	Datový balíček SIP se skládá z adresáře (složky) s jednoznačným názvem v rámci jednoho skartačního řízení.	
11.2.2	Adresář (složka) obsahuje soubor XML vytvořený ve formátu značkovacího jazyka XML verze 1.0 nebo 1.1 a případně dalších souborů reprezentujících příslušné komponenty.	
11.2.3	Soubor XML je pojmenován „mets.xml“. Příklad: jednoznacny_nazev_sip [dir] |-mets.xml	
11.2.4	Každý soubor XML popisuje právě jeden datový balíček SIP. Není možné v jednom souboru XML popisovat více datových balíčků SIP.	
11.2.5	Základní logická struktura souboru XML je předepsána schématem XML METS 1.11 podle přílohy č. 3.	
11.2.6	Obsah souboru XML je dále specifikován podmínkami použití prvků schématu XML METS podle přílohy č. 3 části 2. Tyto podmínky jsou závazné pro určení správnosti datového balíčku SIP.	
11.2.7	Znakovou sadou souboru XML je Unicode/UCS v kódování UTF 8 bez BOM (Byte order mark).	
11.2.8	Soubory reprezentující komponenty se ukládají do adresáře (složky) s názvem „komponenty“. Příklad: jednoznacny_nazev_sip [dir] |-komponenty [dir] |-nazev_souboru_pdfA.pdf |-mets.xml	

11.2.9	Datový balíček SIP může být komprimován do souboru v datovém formátu ZIP, přičemž soubor ZIP bude pojmenován stejným způsobem jako adresář (složka) datového balíčku SIP.
	
	Příklad:
	jednoznacny_nazev_sip [dir]
	|-jednoznacny_nazev_sip [dir]
	  |-komponenty [dir]
	  |-nazev_souboru_pdfA.pdf
	  |-mets.xml	

11.3 Autentizační prvky v transakčním protokolu dle přílohy č. 6

Číslo	Požadavek	Původně
11.3.1	XML soubor transakčního protokolu (požadavek 5.3.3) musí být podepsán podle standardu XAdES-T.	
11.3.2	Podepisovanou oblastí XML bude vždy kořenový element, kterým je TransakcniLogSystemu. Tato podepisovaná data budou zapouzdřena v elementu Signature/Object. Syntaxe podpisu bude Enveloping.	

11.4 Schémata XML

Schémata XML, která tvoří přílohy č. 1 až 6, zajišťují export, import a přenos entit a jejich metadat a naplňují příslušné požadavky národního standardu.

Příloha č.	Název schématu XML	Poznámka
1	Schéma XML pro výměnu dokumentů a jejich metadat	Schéma je určeno pro výměnu dokumentů a jejich metadat mezi ISSD a eSSL, přičemž se použije také pro export, import a přenos dokumentů. V tom případě se využijí pouze ve schématu definované datové prvky.
2	Schéma XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP	
3	Schéma XML pro vytvoření datového balíčku SIP	Schéma vychází ze standardu METS.
4	Schéma XML pro zasílání údajů o rozhodnutí ve skartačním řízení a potvrzení přejímky s identifikátory digitálního archivu původci	Schéma je určeno pro zasílání seznamu entit vybraných za archiválie nebo entit určených ke zničení. Poskytuje tak informace pro doplnění metadat příslušných entit v eSSL. Druhou funkcí schématu je zaslání identifikátoru digitálního archivu po provedení přenosu nebo exportu k zaznamenání do eSSL.
5	Schéma XML pro export a import spisového a skartačního plánu	Schéma je určeno pro export spisového plánu, metadat věcných skupin a jejich skartačních režimů.
6	Schéma XML pro export a import transakčního protokolu	Schéma je určeno pro export a import transakčního protokolu.