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. (dále jen „zákon“), národní standard pro elektronické systémy spisové služby (dále jen „národní standard“).

Předkládané znění národního standardu bylo zásadně upraveno s ohledem na nový proces atestace elektronických systémů spisových služeb. Celková revize národního standardu byla provedena s vědomím potřeby zajištění testovatelnosti jednotlivých obsažených požadavků a dále na základě dosavadních zkušeností veřejnoprávních původců a výrobců informačních systémů i poznatků kontrolních orgánů na úseku archivnictví.

Národní standard reaguje na úpravy pojmů ve vyhlášce č. 259/2012 Sb., o podrobnostech výkonu spisové služby (dále jen „vyhláška o spisové službě“); nově je redefinována komponenta (nyní platný pojem pouze pro digitální dokumenty) a v souvislosti s ní i kontejnerové datové formáty. Terminologie byla dále upravena i vypuštěním řady překonaných či zbytných pojmů.

Za zásadní změny lze považovat ty, které souvisí se změnami koncepce zpracování dokumentů, mezi něž patří především povinné vyřizování dokumentů ve spisu a převod datových formátů komponent dokumentu do výstupních formátů, a to co nejdříve je to možné a účelné, většinou již v procesu příjmu. Dále pak změny související s konstrukcí čísla jednacího, dříve tzv. tvorbou spisu. Nově je požadováno, aby elektronický systém spisové služby dokázal konfigurovat tvorbu čísla jednacího dle jednoho ze dvou způsobů na úrovni věcné skupiny či součásti typového spisu. Spisům jsou přiřazovány spisové znaky a další metadata ve chvíli jejich založení, nikoliv až uzavření, a iniciační či vložené dokumenty je následně dědí. Další koncepční změnou s dopadem na požadavky národního standardu je opuštění pojmu rozpracovaného dokumentu (konceptu) a jeho nahrazení povinnou tvorbou a ukládáním verzí všech komponent dokumentu po celou dobu jeho životního cyklu v rámci elektronického systému spisové služby.

Zcela nově jsou v samostatných částech popsány požadavky na jmenný rejstřík a dále požadavky na funkčnost samostatných evidencí dokumentů, pokud nezajišťují dané části výkonu péče o dokumenty pomocí propojení s elektronickým systémem spisové služby. Upravena byla i oblast typových spisů, jejichž součásti je možné navzájem hierarchicky prohlubovat, přičemž zásadní roli hrají ty na nejnižší úrovni hierarchie, ve kterých je možné zakládat či do nich vkládat spisy. Současně tak bylo omezeno využití pevných křížových vazeb pouze na spojování dvou spisů. Pro typové spisy jsou určeny zvláštní věcné skupiny obsahující konfigurovatelné šablony typového spisu, podle kterých je možné následně jednotlivé typové spisy zakládat.

Změny se týkají i oblasti vyřazování dokumentů a spisů, jejich změn a zničení. Označení „druh dokumentu“ bylo doplněno o skartační režim, a může tak při aplikaci na dokument sloužit k vyvolání konfliktu se skartačním režimem, který dokument zdědil ze spisu. Konflikt lze vyřešit většinou automatizovaně, a daný proces tak ochrání zájmy původce v případě potřeby ochrany vybraných druhů dokumentů. Ze spisových znaků byl vzhledem k požadavkům vyhlášky o spisové službě vypuštěn spisový znak „V“ (výběr), samozřejmě bez zpětné platnosti. Požadavky národního standardu též

zohledňují rostoucí důraz na používání institutu trvalého skartačního režimu. Poprvé jsou formulovány požadavky upravující možnost znepřístupnění (storna) dokumentu či spisu.

V souvislosti s potřebou tvorby testovacích scénářů a postupů i dosavadními zkušenostmi s využíváním národního standardu byla řada z požadavků zpřesněna a jednoznačněji formulována, nebo vypuštěna. Odstraněny byly například ty, které upravovaly proces zálohy a obnovy či spolupráci s antivirovými programy. Celkově byl počet požadavků národního standardu snížen o čtvrtinu oproti předchozímu stavu. Současně tak doznala změn i struktura kapitol, která se ale významněji nezměnila a stále odpovídá posloupnosti činností při výkonu spisové služby.

Přílohy národního standardu byly upraveny v souladu s upravenou podobou textu. Nově přibyla příloha obsahující výčet a popis všech povinných metadat entit, se kterými musí elektronický systém spisové služby pracovat. Dále pak přílohy týkající se migrace dat mezi elektronickými systémy spisové služby a migrace dat při spisové rozluce, a to v reakci na podstatnou úpravu kapitol týkajících se přenosu, exportu a importu entit. Přibyl též popis struktury popisných a evidenčních metadat podporující automatizované zpracování přijímaných entit do elektronického systému spisové služby. Naopak struktura SIP balíčku se téměř nezměnila a nebude vyžadovat bezprostřední přechod na další verzi.

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 1. července 2023, týmž dnem se zrušuje národní standard pro elektronické systémy spisové služby zveřejněný ve Věstníku Ministerstva vnitra čá. 57/2017.

Veřejnoprávní původci uvedou výkon spisové služby do souladu s požadavky národního standardu, ve znění účinném ode dne nabytí účinnosti tohoto národního standardu, do 31. prosince 2025.

Pro účely atestací se posuzuje soulad elektronického systému spisové služby s požadavky národního standardu ve znění účinném ode dne nabytí účinnosti tohoto národního standardu.

Č. j. MV-109932-1/AS-2023

Ředitel odboru archivní správy a spisové služby

PhDr. Daniel DOLEŽAL, Ph.D., v. r.

Národní standard pro elektronické systémy spisové služby

OBSAH

1 ZÁKLADNÍ POJMY

1.1 Analogový dokument

Analogový dokument je dokument, jehož alespoň jedna část je analogová. Tato část může být v listinné podobě nebo se jedná o technický nosič dat, který neobsahuje dokumenty v digitální podobě (například obrazový a zvukový nosič s analogovým záznamem signálu, trojrozměrné předměty). Dokument tvořený z částí a komponent se pro účely národního standardu pokládá za analogový.

1.2 Část dokumentu

Dokument v analogové podobě je tvořen částmi dokumentu (například průvodní dopis, přílohy, případně obálka doručeného dokumentu).

1.3 Číslo jednací

Číslo jednací je evidenční znak dokumentu v rámci evidence dokumentů, jehož tvar vychází z požadavků právního předpisu upravujícího podrobnosti výkonu spisové služby upřesněných ve spisovém řádu původce.

1.4 Datový balíček SIP

Informační balíček (Submission Information Package) určený k exportu, importu nebo přenosu replik entit z eSSL nebo do eSSL. Je tvořen podle přílohy č. 2 a obsahuje metadata a komponenty

a) spisu,

b) dokumentu zatříděného přímo do věcné skupiny (podle předchozí právní úpravy), nebo

c) dílu typového spisu.

1.5 Datový formát komponenty

Datový formát je způsob kódování komponenty - pro účely zpracování výpočetní technikou. Pojem „datový formát komponenty“ 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 kancelářskými aplikacemi.

1.6 Dědičnost

Dědičnost vyjadřuje vlastnost, na jejímž základě mateřská entita předává určitá metadata dceřiné entitě.

1.7 Digitální (elektronický)

Pojem „digitální“ vyjadřuje entitu představovanou numerickým řetězcem tvořeným hodnotami „1“ a „0“ (proud bitů) a interpretovatelným pouze pomocí výpočetní techniky. Pojem „elektronický“ se pro účely národního standardu užívá obdobně. Za elektronickou nebo digitální se pro účely národního standardu považuje taková entita, kterou lze spravovat prostředky výpočetní techniky; z tohoto důvodu je obvyklé analogové entity převést (konvertovat) do digitální podoby.

1.8 Díl typového spisu

Pomocí dílu typového spisu jsou členěny součásti typového spisu. Díl typového spisu slouží k zajištění manipulace s jeho obsahem jako s celkem. Je vytvářen na základě konfigurovatelného časového období, nikoli obsahově. V dílu typového spisu se vytvářejí spisy nebo se do něj vkládají. Díl typového spisu je zařazován do výběru archiválií jako celek.

1.9 Druh dokumentu

Druhem dokumentu je tematické označení přiřazené dokumentu bez ohledu na jeho zatřídění v hierarchii entit spisové služby. Druhem dokumentu jsou například „faktury“, „smlouvy“ nebo „dokumenty operačního programu XY“. Pokud je druhu dokumentu přiřazen skartační režim, může dojít k vyvolání a řešení konfliktu skartačního režimu dokumentu a spisu.

1.10 Elektronický

Pojem „elektronický“ se pro účely národního standardu používá obdobně jako pojem „digitální“.

1.11 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.

1.12 Entita

Entitou se rozumí objekt spravovaný eSSL. Mezi entity patří zejména věcná skupina, spisový a skartační plán, skartační režim, typový spis, součást typového spisu, díl typového spisu, spis, dokument, komponenta. Replika entity je jiná instance téže entity.

1.13 Export

Export je proces vytvoření repliky vybraných entit spojený s vytvořením repliky metadat těchto entit nebo proces vytvoření repliky transakčního protokolu, a to za účelem převedení vzniklé repliky do jiného systému. Exportované entity a transakční protokol zůstávají zachovány v původním informačním systému spravujícím dokumenty, nejsou tedy na rozdíl od přenosu po jeho ukončení znepřístupněny.

1.14 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.

1.15 Import

Import je proces vložení entit a jejich metadat, které byly vytvořeny v jiném informačním systému spravujícím dokumenty, do eSSL, například při spisové rozluce nebo migraci na jiný systém eSSL.

1.16 Informační systém spravující dokumenty

Informační systém spravující dokumenty je jakýkoli informační systém obsahující komponenty nebo evidující dokumenty. Tento pojem zahrnuje zejména eSSL a samostatné evidence dokumentů vedené v elektronické podobě.

1.17 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 nebo součást typového spisu. Doplněním jednoduchého spisového znaku o jednoduché spisové znaky všech nadřazených věcných skupin vzniká spisový znak.

1.18 Jednoznačný identifikátor entity

Jednoznačný identifikátor entity je znak pevně spojený s entitou zajišťující její nezaměnitelnost a jedinečnost v rámci informačního systému spravujícího dokumenty. Každá entita je v eSSL označena jednoznačným identifikátorem, kterým je údaj v metadatech. Jednoznačný identifikátor entity může být v případě dokumentu nazýván jako „jednoznačný identifikátor dokumentu“ a rozumí se jím jednoznačný identifikátor podle zákona o archivnictví a spisové službě, nebo v případě spisu jako „jednoznačný identifikátor spisu“ a rozumí se jím identifikátor spisu podle právního předpisu upravujícího podrobnosti výkonu spisové služby apod.

1.19 Komponenta

Komponentou se rozumí jednoznačně vymezený proud bitů tvořící datový soubor charakterizovaný zpravidla formátem datového souboru, běžně zpracovávaným programovými aplikacemi, které umožňují provádět správu souborů, složek a disků tak, aby k nim bylo možné uživatelsky srozumitelně přistupovat a s nimi samostatně manipulovat (správce souborů). Komponentou může být i metasoubor zahrnující společné uložení dat a metadat (datový kontejner, například PDF/A-3, ZFO, ZIP), z kterého lze - s pomocí k tomu určených programových aplikací - vyčlenit v něm zapouzdřené datové soubory, se kterými lze pracovat jako se samostatnými komponentami podle věty první.

1.20 Kontejnerové datové formáty

Kontejnerové datové formáty jsou formáty komponent obsahující alespoň jednu další komponentu.

1.21 Křížový odkaz

Křížový odkaz je vazba mezi entitami. Pevný křížový odkaz zajišťuje spojení spisů, které nelze bez uvedení důvodu odstranit, a přihlíží se k němu při exportu a přenosu. Historicky bylo možné realizovat pevný křížový odkaz i mezi dokumenty, dokumenty a spisy a použít ke vkládání spisů do dílu typového spisu. V případě volného křížového odkazu se jedná o informační vazbu mezi entitami, která nemá vliv na entity spojené tímto odkazem a práci s nimi.

1.22 Otevření (činnost)

Otevřením se rozumí:

a) iniciační okamžik uvedení konkrétní instance entity, který umožňuje, aby do dané entity byly vkládány další entity, pokud je to podle národního standardu možné. Otevírá se součást typového spisu, která je definována šablonou typového spisu pro věcnou skupinu umožňující vytvářet typové spisy, díl typového spisu a věcná skupina,

b) proces navrácení uzavřené instance entity do aktivního stavu. Znovuotevřít lze věcnou skupinu, součást typového spisu, spis. Vzhledem k povaze dílu typového spisu jej není možné opětovně otevřít.

1.23 Otevřený (stav)

Otevřený je stav vzniklý otevřením nebo založením entit spisové služby. Ve stavu „otevřený“ je po svém otevření věcná skupina, součást typového spisu a díl typového spisu a po svém založení typový spis, spis.

1.24 Posuzovatel skartační operace

Posuzovatel skartační operace je specifická správcovská role, jejíž nositel (konkrétní fyzická osoba pověřená původcem) zejména spravuje spisovnu. Posuzovatel skartační operace dále rozhoduje o znepřístupněných dokumentech, přetřiďuje chybně zatříděné uzavřené spisy, edituje metadata spisů, připravuje výběr archiválií a realizuje rozhodnutí o výběru archiválií.

1.25 Pozastavení skartační operace

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

1.26 Přenos

Přenos je proces přemístění repliky entity spolu s jejími metadaty do jiného informačního systému spravujícího dokumenty. Účelem přenosu je zejména převést vybrané entity do externí elektronické spisovny**,** digitálního archivu, externího eSSL (spisová rozluka) nebo jiného informačního systému spravujícího dokumenty.

1.27 Příjem

Příjem je úkon odborné správy dokumentů, jímž se přijímá dokument do informačního systému spravujícího dokumenty. Příjem zahrnuje také procesy spojené se záznamem do evidenční pomůcky (označení, doplnění metadat) a vložení do spisu.

1.28 Role

Role je souhrn oprávnění, jejichž prostřednictvím jsou přidělována práva uživateli informačního systému spravujícího dokumenty. Pro účely národního standardu se rozlišují dva druhy rolí: uživatelská role, správcovská role. Jeden uživatel může mít v informačním systému spravujícím dokumenty přidělenu jednu nebo více rolí (například uživatelskou roli a správcovskou roli).

1.29 Rozhraní (informačního systému spravujícího dokumenty)

Rozhraní informačního systému spravujícího dokumenty je soubor webových služeb a XML, s jejichž pomocí komunikuje informační systém spravující dokumenty s eSSL, popřípadě s jiným informačním systémem spravujícím dokumenty. Rozhraní informačního systému spravujícího dokumenty je realizováno prostřednictvím webových služeb a schémat uvedených v příloze č. 1.

1.30 Samostatná evidence dokumentů v elektronické podobě

Samostatná evidence dokumentů je informační systém spravující dokumenty, který musí být v souladu s požadavky stanovenými národním standardem a v případě, že sám nezajišťuje v požadovaném rozsahu některé činnosti výkonu spisové služby, musí být integrován se základní evidenční pomůckou pomocí rozhraní informačního systému spravujícího dokumenty. Stanoví-li tak jiný právní předpis nebo spisový řád původce, mohou být dokumenty evidované v samostatných evidencích dokumentů, kterými jsou informační systémy spravující dokumenty, s výjimkou eSSL.

1.31 Schvalování (činnost)

Schvalování je proces ve spisové službě, kdy k tomu oprávněná role (schvalovatel) v souladu s vnitřním předpisem původce označuje dokumenty, včetně jejich komponent, jako schválené. Schvalovatel může, ale nemusí být zároveň osobou, která dokument v rámci této činnosti podepisuje. Obsah komponenty schváleného dokumentu nelze měnit bez opakovaného procesu schválení.

1.32 Skartační operace

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

1.33 Skartační režim

Skartační režim zahrnuje údaje stanovené původcem, které určují okamžik, kdy musí být dokument, spis nebo díl typového spisu navržen ke skartačnímu řízení (skartační lhůta a spouštěcí událost); původce jím navrhuje, jak má být s dokumentem, spisem nebo dílem typového spisu ve skartačním řízení naloženo (skartační znak). Skartační režim stanovuje původce ve svém spisovém a skartačním plánu pro věcnou skupinu nebo součást typového spisu na nejnižší úrovni hierarchie a u typu dokumentu, pokud jej původce využívá.

1.34 Skartační lhůta

Doba, po kterou musí být dokument, spis nebo díl typového spisu uložen u původce. Vyjadřuje se počtem let (nejméně 0) počítaným od roku následujícího po roce, kdy nastala spouštěcí událost. Spolu se skartačním znakem a spouštěcí událostí tvoří skartační režim.

1.35 Skartační znak

Návrh původce, jak má být s dokumentem, spisem nebo dílem typového spisu naloženo ve skartačním řízení. Vyjadřuje se písmeny A – k trvalému uložení do archivu, S – ke zničení, V – podle předchozí právní úpravy se rozhodne při skartačním řízení. Skartační znak spolu se skartační lhůtou a spouštěcí událostí tvoří skartační režim.

1.36 Součást typového spisu

Součást typového spisu člení typový spis podle obsahu. Každá součást typového spisu je pojmenována a její název je uveden ve spisovém a skartačním plánu. Každý typový spis obsahuje alespoň jednu součást typového spisu.

1.37 Spis

Spis je entita, v níž jsou organizovány dokumenty vztahující se ke stejnému předmětu (věci).

1.38 Spisová značka

Spisová značka je označení spisu; její podobu stanovuje spisový řád původce.

1.39 Spisový a skartační plán

Spisovým a skartačním plánem se rozumí souhrn věcných skupin a součástí typového spisu platných v časovém období (časový řez), doplněný o skartační režimy. Spisový a skartační plán je součástí spisového řádu původce.

1.40 Spisový znak

Spisový znak je označení věcné skupiny nebo součásti typového spisu, které stanovuje místo entity v hierarchii spisového plánu prostřednictvím dědění spisových znaků mateřských věcných skupin nebo mateřských součástí typového spisu. Je tvořen jednoduchým spisovým znakem věcné skupiny postavené v hierarchii nejvýše a jednoduchými spisovými znaky věcných skupin, popřípadě součástí typového spisu, ležících v hierarchii spisového plánu níže, a to až do dosažení nejbližší mateřské věcné skupiny, popřípadě součásti typového spisu. Spisové znaky jsou jednoznačné v rámci hierarchického spisového plánu, zatímco jednoduché spisové znaky jako takové jsou jednoznačné jen v rámci konkrétní mateřské věcné skupiny.

1.41 Spouštěcí událost

Spouštěcí událostí je skutečnost rozhodná pro počátek plynutí skartační lhůty, a pokud to není uzavření spisu, je stanovena ve spisovém a skartačním plánu původce. Spouštěcí událost spolu se skartačním znakem a skartační lhůtou tvoří skartační režim.

1.42 Správcovská role

Správcovská role je role vybavená specifickými oprávněními (určit, stanovit, konfigurovat, udržovat, spravovat, vytvářet atp.), která jsou určena národním standardem nebo původcem. Správcovskou rolí je například „Posuzovatel skartační operace“.

1.43 Stručný obsah

Stručný obsah dokumentu nebo spisu je několikaslovná charakteristika oblasti, které se dokument nebo spis týkají. Stručný obsah v praxi obvykle odpovídá zažité kolonce „věc“.

1.44 Šablona typového spisu

Šablonou typového spisu se rozumí struktura typového spisu definovaná v rámci konfigurace příslušné mateřské věcné skupiny. Šablona typového spisu definuje součásti typového spisu, jejich hierarchii a metadata včetně spisových znaků a skartačních režimů a nastavení časového úseku pro díly typového spisu otevírané v součástech typového spisu. Pro každou mateřskou věcnou skupinu umožňující vytváření typových spisů, je vytvořena právě jedna šablona.

1.45 Transakční protokol

Transakční protokol je úplný soubor informací o operacích provedených v informačním systému spravujícím dokumenty, které ovlivnily nebo změnily informační systém spravující dokumenty, entity a jejich metadata. Tyto informace umožňují dohledání, identifikaci, rekonstrukci a kontrolu těchto operací, stavu entit v minulosti a činnosti uživatelů. Transakční protokol je základní prvek důvěryhodnosti informačního systému spravujícího dokumenty. Obsah transakčního protokolu za časové období je ztvárněn do samostatného dokumentu.

1.46 Třídění

Tříděním se rozumí systematická klasifikace dokumentů do věcné skupiny a spisu, v souladu se spisovým řádem a spisovým a skartačním plánem, prováděná při výkonu spisové služby. Pojem třídění zahrnuje operace zatřídění a přetřídění.

1.47 Typový spis

Typový spis je vnitřně strukturovaná entita vytvořená z předem definované šablony typového spisu. Strukturu tvoří věcné, podle obsahu stanovené součásti typového spisu (jedna nebo více), které mohou být hierarchicky členěné na další součásti. Součást typového spisu na nejnižší úrovni obsahuje alespoň jeden díl typového spisu mechanicky vytvářený pro časové období stanovené pro věcnou skupinu, v níž se typové spisy otevírají. V dílu typového spisu se vytvářejí spisy nebo se do nich vkládají spisy. Základní vlastností typových spisů je, že

a) mají předvídanou strukturu svého obsahu stanovenou ve spisovém a skartačním plánu původce,

b) jsou dlouhodobě spravovány v rámci konkrétní agendy původce,

c) spisovou značku tvoří název, jehož způsob tvorby je stanoven ve spisovém řádu původce (například katastrální území, číslo popisné, identifikace konkrétní právnické nebo fyzické osoby), a

d) nevyřazují se jednotlivé spisy z dílu typového spisu, ale díl typového spisu se vyřazuje jako celek.

1.48 Uzavření

Uzavřením se rozumí změna atributů věcné skupiny, typového spisu**,** součásti typového spisu, dílu typového spisu nebo spisu, v jejímž důsledku je zejména znemožněno vkládání dalších dokumentů nebo spisů.

1.49 Uživatel

Uživatelem je fyzická osoba používající na základě přidělené role informační systém spravující dokumenty. Různí uživatelé mohou mít rozdílná oprávnění.

1.50 Uživatelská role

Uživatelská role je souhrn funkčních oprávnění udělených uživatelům, kteří mohou v informačním systému spravujícím dokumenty vykonávat činnost týkající se odborné správy dokumentů. Jeden uživatel může mít několik uživatelských rolí.

1.51 Věcná skupina

Věcná skupina je na věcném (obsahovém) základě vytvořená položka spisového a skartačního plánu, která označuje část jeho hierarchie a je identifikována spisovým znakem. Věcná skupina odpovídá položce spisového a skartačního plánu a může obsahovat jiné věcné skupiny, spisy (historicky i dokumenty) nebo typové spisy. Věcná skupina obsahující typové spisy nebo jinou věcnou skupinu nemůže obsahovat jinou entitu.

1.52 Vyřízení

Vyřízením se rozumí změna atributů spisu nebo dokumentu, v jejímž důsledku je zejména znemožněna editace vybraných metadat. Vyřízení je možné zrušit. Vyřízení spisu může být jednou ze spouštěcích událostí.

1.53 Zajišťovací prvky

Zajišťovacími prvky dokumentu v digitální podobě, včetně datové zprávy, v níž je obsažen, se rozumí

a) uznávaný elektronický podpis podle § 6 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,

b) uznávaná elektronická pečeť podle § 9 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,

c) uznávaná elektronická značka podle § 19 odst. 9 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,

d) kvalifikované elektronické časové razítko podle čl. 3 odst. 34 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.

1.54 Založení

Založením vzniká na základě jednání uživatele nebo systému v konkrétní věcné skupině nový spis nebo typový spis. Současně je spis nebo typový spis otevřen pro vkládání.

1.55 Znázornění

Znázornění je uživatelsky vnímatelná interpretace komponenty nebo metadat, zpravidla v podobě zobrazení na obrazovce.

1.56 Znepřístupnění (storno)

Znepřístupnění je vyloučení entity z dalšího zpracování v eSSL. Znepřístupněné entity jsou dále uchovány v eSSL v nezměněné podobě s doprovodným zápisem v metadatech, ale uživatelské roli je nelze znázornit ani ztvárnit (stejně jako by byly z eSSL vyjmuty nebo zničeny).

Znepřístupněné entity je možné znovu zpřístupnit, nebo je možné je zničit. V předchozí právní úpravě byl používán ve shodném významu pojem „smazání“.

1.57 Zničení

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

1.58 Zpracovatel

Zpracovatel je uživatelská role, zejména s následujícími oprávněními

a) editovat stanovená metadata spisu a dokumentu, do spisu vkládat nebo v něm vytvářet dokumenty a vytvářet stanovená metadata, nahlížet do komponent a v případě neschválených komponent tyto měnit, měnit datový formát komponent na výstupní datový formát a opatřovat komponenty zajišťovacími prvky, předat spis nebo součást typového spisu jinému zpracovateli nebo jinému zpracovateli postoupit svá vybraná uživatelská oprávnění („držitel spisu“ nebo „držitel součásti typového spisu“),

b) na základě uživatelských oprávnění postoupených držitelem spisu nebo držitelem součásti typového spisu nahlížet na metadata a entity, vkládat entity (dokumenty do spisu, spisy do dílu typového spisu), vkládat stanovená metadata, v případě vlastních dokumentů původce měnit datový formát komponent na výstupní datový formát a opatřovat komponenty zajišťovacími prvky.

1.59 Ztvárnění

Znázorněné komponenty nebo metadata mohou být ztvárněny tiskem (do listinné podoby), nebo uložením do nové komponenty. Ztvárněním se také rozumí výsledek

a) změny datového formátu,

b) převedení dokumentu,

c) autorizované konverze dokumentu.

2 PŘÍJEM A EVIDENCE DOKUMENTŮ

2.1 Příjem

Číslo	Požadavek
2.1.1	ESSL automaticky čísluje všechny verze komponent dokumentu.
2.1.2	Pokud je přijímaný dokument složen z několika komponent, eSSL přijme všechny jeho komponenty a dále spravuje dokument jako jedinou entitu tak, aby byly zachovány vztahy mezi komponentami a aby byla uchována struktura dokumentu. ESSL současně automaticky zaznamená počet komponent do metadat dokumentu.
2.1.3	ESSL při příjmu komponenty dokumentu automaticky identifikuje její datový formát, včetně verze formátu podle vnitřní struktury komponenty. ESSL tyto informace ukládá do metadat komponenty. *Informace pro automatickou identifikaci datových formátů poskytuje například registr PRONOM (www.nationalarchives.gov.uk/PRONOM/).*
2.1.4	ESSL přijímá entity a metadata v souladu s XML schématy uvedenými v přílohách č. 1, 3, 5, 6 a 8.
2.1.5	ESSL od příjmu do vyřazení entity průběžně zaznamenává metadata v rozsahu podle přílohy č. 8.
2.1.6	ESSL umožní předat doručený dokument příslušné fyzické osobě, pokud byl určen k rukám nebo do vlastních rukou.
2.1.7	ESSL na pokyn uživatelské role při příjmu dokumentu neuloží komponentu dokumentu v případě, že se jedná o komponentu v nepřijímaném datovém formátu, nepřijímané velikosti nebo s jinou vadou, na jejímž základě je odesílatel vyzván k opravě vad dokumentu. ESSL nahradí neuloženou komponentu ztvárněním informací o důvodu jejího neuložení do nové komponenty. *ESSL vždy zaznamená údaje o odesílateli a datu doručení dokumentu bez ohledu na uložení, nebo neuložení jeho komponent.*
2.1.8	ESSL při příjmu zaznamená do metadat velikost jednotlivých komponent obsažených v datové zprávě doručené datovou schránkou.

2.2 E-mailové schránky

Číslo	Požadavek
2.2.1	ESSL zajišťuje a) automatizované stahování a uložení e-mailových zpráv doručených na elektronické adresy podatelny, b) odesílání e-mailových zpráv prostřednictvím elektronické adresy podatelny.
2.2.2	ESSL prostřednictvím funkčního rozšíření poštovního klienta nebo prostředky eSSL umožňuje uživatelské roli přijetí touto rolí vybrané e-mailové zprávy, která byla doručena na jinou e-mailovou adresu, než je elektronická adresa podatelny.
2.2.3	Pokud je e-mailová zpráva přijata, eSSL uchová jako samostatné komponenty dokumentu a) e-mailovou zprávu v původním formátu postupem podle požadavku 2.4.2,

Číslo	Požadavek
	b) obsah (tělo) e-mailové zprávy a c) jednotlivé připojené přílohy.
2.2.4	ESSL z přijaté e-mailové zprávy automaticky vyjímá následující metadata (pokud jsou obsažena v hlavičce e-mailové zprávy): a) datum a čas odeslání e-mailové zprávy, b) předmět (věc), c) odesílatel e-mailové zprávy ve vazbě na jmenný rejstřík.
2.2.5	ESSL umožňuje uživatelské roli při příjmu e-mailové zprávy upravit metadata automaticky vyjmutá z e-mailové zprávy podle požadavku 2.2.4.
2.2.6	ESSL automatizovaně zašle potvrzení a) o přijetí zprávy, b) o nepřijetí/vadě zprávy.

2.3 Datové schránky

Číslo	Požadavek
2.3.1	ESSL zajišťuje a) automatizované stahování a uložení datových zpráv doručených prostřednictvím informačního systému datových schránek, b) odesílání datových zpráv prostřednictvím informačního systému datových schránek, c) stahování a uložení informace o dodání datové zprávy do datové schránky adresáta a o doručení datové zprávy (zásilky).
2.3.2	ESSL zajišťuje využití následujících služeb informačního systému datových schránek: a) doručení datové zprávy, b) odeslání datové zprávy, c) ověření datové zprávy, d) získání informace o dodání a doručení datové zprávy, e) získání informace o odesílateli datové zprávy, f) vyhledání datové schránky a údajů o majiteli, g) kontrola přístupnosti datové schránky. *Pravidla pro realizaci rozhraní eSSL vůči informačnímu systému datových schránek pro využívání jednotlivých služeb se řídí Provozním řádem informačního systému datových schránek a jeho přílohami s definicí jednotlivých webových služeb informačního systému datových schránek.*
2.3.3	ESSL umožňuje uživatelské roli vyhledání datové schránky v informačním systému datových schránek.
2.3.4	ESSL zajišťuje stahování údajů z obálek doručených datových zpráv a jejich uložení do metadat eSSL v rozsahu: a) datum a čas dodání,

Číslo	Požadavek
	b) datum a čas doručení, c) odesílatel.
2.3.5	Pokud je datová zpráva přijata, eSSL uchová jako samostatné komponenty dokumentu a) datovou zprávu v původním formátu postupem podle požadavku 2.4.2, b) hlavičku datové zprávy ztvárněnou do samostatné komponenty a c) jednotlivé připojené komponenty.

2.4 Kontejnerové datové formáty

Číslo	Požadavek
2.4.1	ESSL zajistí při příjmu automatizované zpracování komponenty dokumentu v datovém formátu, který má charakter kontejneru, podle požadavků 2.4.3 a 2.4.4, a to alespoň pro formáty ASiC, FO/ZFO, EML, ISDOCX, ZIP, PDF/A. Povinnost automatického zpracování se nevztahuje na šifrované komponenty v datovém formátu, který má charakter kontejneru, a na již zpracované datové zprávy.
2.4.2	ESSL uchová došlý kontejner v nezměněné podobě jako samostatnou komponentu alespoň do okamžiku uzavření spisu.
2.4.3	ESSL při automatizovaném zpracování kontejneru zajistí vyjmutí všech komponent vnořených v první úrovni kontejneru a jejich uložení jako samostatných komponent. Pokud je vyjmutá komponenta v datovém formátu uvedeném v požadavku 2.4.1, proces automatického zpracování se opakuje. ESSL v případě selhání automatického zpracování kontejneru poskytne zpracovateli informaci o selhání.
2.4.4	ESSL při automatizovaném zpracování kontejneru, který obsahuje komponentu ve formátu XML v souladu s XML schématem v příloze č. 3, zapíše popisná metadata z XML v komponentě do metadat příslušného dokumentu.
2.4.5	ESSL zajistí, že vyhotovovaná textová komponenta nebo statická kombinovaná textová a obrazová komponenta určená k odeslání obsahuje metadata ve formátu XML, a to v souladu se schématem XML v příloze č. 3.

2.5 Změna datového formátu komponenty a převod dokumentu

Číslo	Požadavek
2.5.1	ESSL po provedení požadavků kapitoly 2.6 v případě statických textových dokumentů, statických kombinovaných textových a obrazových dokumentů a statických obrazových dokumentů (alespoň DOC, DOCX, XLS, XLSX, PPT, PPTX, ODT, ODS, ODP, RTF, TXT, PDF, HTM, HTML, BMP) automatizovaně zajistí změnu datového formátu komponenty na výstupní a výstup změny datového formátu uloží jako novou verzi téže komponenty. *Převod datových formátů lze řešit i jako asynchronní operaci tak, aby nebylo blokováno další zpracování dokumentu*.
2.5.2	ESSL při změně datového formátu podle požadavku 2.5.1 připojí doložku obsahující informace uvedené v právním předpisu upravujícím podrobnosti výkonu spisové služby

Číslo	Požadavek
	a) do stejné komponenty za obsah vstupu změny datového formátu, umožňuje-li to formát výstupu změny datového formátu, nebo b) do nové komponenty ve výstupním formátu statických textových dokumentů; v takovém případě bude součástí doložky hash výstupní komponenty ze změny datového formátu a název použité hashovací funkce.
2.5.3	ESSL v případě vlastních dokumentů původce postupuje obdobně jako v požadavku 2.5.1 a) před podepsáním komponenty, a b) při uzavření spisu, pokud nebyla komponenta podepsána. Připojení doložky podle požadavku 2.5.2 a časového razítka se nevyžaduje.
2.5.4	ESSL v případě převodu dokumentu z analogové do digitální podoby připojí doložku obsahující informace uvedené v právním předpisu upravujícím podrobnosti výkonu spisové služby obdobně jako v požadavku 2.5.2.
2.5.5	ESSL opatří výstup převodu dokumentu podle požadavku 2.5.2 nebo změny datového formátu dokumentu podle požadavku 2.5.4 příslušnými zajišťovacími prvky.

2.6 Ověřování zajišťovacích prvků

Číslo	Požadavek
2.6.1	ESSL při příjmu nebo vložení komponenty automatizovaně zajistí ověření platnosti zajišťovacích prvků, které jsou ke komponentám připojeny. *Ověření platnosti zajišťovacích prvků lze řešit i jako asynchronní operaci tak, aby nebylo blokováno další zpracování dokumentu*.
2.6.2	ESSL při ověření zajišťovacích prvků v době příjmu nebo vložení zaznamená do metadat údaje stanovené právním předpisem upravujícím podrobnosti výkonu spisové služby nebo k dokumentu připojí samostatnou komponentu, která údaje o ověření obsahuje.

2.7 Evidence dokumentů

Číslo	Požadavek
2.7.1	ESSL automatizovaně přidělí každé entitě jednoznačný identifikátor. Jednoznačné identifikátory se přiřazují alespoň k a) spisovému a skartačnímu plánu jako celku, b) věcné skupině, c) spisu, d) typovému spisu, e) součásti typového spisu, f) dílu typového spisu, g) dokumentu (jednoznačný identifikátor dokumentu), h) komponentě, i) skartačnímu režimu.

Číslo	Požadavek
2.7.2	ESSL přiřadí dokumentu pořadové číslo v rámci předem určeného časového období, zpravidla konkrétního kalendářního roku. Správcovská role stanoví před začátkem určeného časového období jeho počátek a konec.
2.7.3	ESSL vede číselník organizačních součástí původce nebo jiných údajů stanovených původcem. Číselník udržuje správcovská role a obsahuje alespoň a) údaj, b) datum počátku používání údaje, c) datum konce používání údaje. ESSL umožňuje znázornění a export/import číselníku prostřednictvím přílohy č. 7.
2.7.4	ESSL umožňuje správcovské roli konfigurovat strukturu čísla jednacího (míněno pořadí metadat a oddělovače) podle právního předpisu upravujícího podrobnosti výkonu spisové služby: a) vycházející z pořadového čísla dokumentu v rámci předem určeného časového období (viz požadavek 2.7.2), b) vycházející ze spisové značky doplněním pořadového čísla dokumentu ve spisu. *Například URAD-EPR/2008-525, kde „525“ je pořadové číslo v rámci určeného časového období, „2008“ určené časové období a „EPR“ označení organizační součásti (požadavek 2.7.3). Obdobně URAD-EPR/2008-222-11, kde „URAD-EPR/2008-222“ je spisová značka a „11“ pořadové číslo dokumentu ve spisu. Použití variant podle písm. a) nebo b) se řídí v příslušné věcné skupině nebo součásti typového spisu příznakem podle požadavku 3.1.2 písm. h), respektive požadavku 3.3.6 písm. c).*
2.7.5	ESSL podporuje sledování oběhu dokumentů a spisů v analogové podobě prostřednictvím funkce předání a převzetí, s cílem zaznamenat jejich umístění, zpracovatele a datum předání, popřípadě převzetí.
2.7.6	ESSL umožní uživateli zaznamenat do metadat pokyny pro schvalování a oběh dokumentu nebo spisu.

2.8 Jmenný rejstřík

Číslo	Požadavek
2.8.1	ESSL neumožní uživatelské roli ukončit příjem doručeného dokumentu bez vytvoření vazby mezi záznamem o osobě odesílatele ve jmenném rejstříku a dokumentem.
2.8.2	ESSL umožní v rámci odeslání dokumentu výběr adresáta ze jmenného rejstříku a automaticky zaznamená vazbu mezi záznamem o osobě adresáta ve jmenném rejstříku a dokumentem.
2.8.3	ESSL do okamžiku vyřazení dokumentu umožní uživatelské roli zaznamenání vazby mezi záznamem o jiné osobě ve jmenném rejstříku a dokumentem.
2.8.4	ESSL při příjmu dokumentu automatizovaně z jeho komponent obsahujících XML v souladu se schématem v příloze č. 3 vytěží metadata o osobách a vytvoří vazbu dokumentu na záznam o vytěžených osobách ve jmenném rejstříku, případně vytvoří nový záznam o osobách, které se ve jmenném rejstříku nenacházejí.

Číslo	Požadavek
2.8.5	ESSL do okamžiku vyřazení spisu umožní uživatelské roli zaznamenání vazby mezi záznamem ve jmenném rejstříku a spisem.
2.8.6	ESSL umožňuje uživatelské roli vyhledávat ve jmenném rejstříku záznamy o právnických osobách.
2.8.7	ESSL umožňuje uživatelské roli vyhledávat ve jmenném rejstříku záznamy o fyzických osobách a výsledky vyhledávání omezí na záznamy, se kterými má uživatelská role oprávnění disponovat a) na základě nastavených oprávnění nebo b) existujících vazeb na dokumenty nebo spisy.
2.8.8	ESSL umožňuje uživatelské roli ztotožnit záznam ve jmenném rejstříku prostřednictvím zadání údajů potřebných pro jeho ztotožnění. Za údaje potřebné pro ztotožnění osoby se považují alespoň: a) jméno, příjmení, datum narození a adresa trvalého pobytu u fyzické osoby, b) jméno, příjmení, datum narození, adresa sídla a právní forma u fyzické osoby podnikající, c) obchodní firma nebo název nebo označení a právní forma u právnické osoby, d) identifikační číslo osoby u právnické osoby nebo fyzické osoby podnikající, e) identifikátor datové schránky, f) jiná elektronická identifikace (například adresa elektronické pošty).
2.8.9	V případě, že na základě údajů o osobě nelze k dokumentu nebo spisu přiřadit záznam ve jmenném rejstříku: a) jsou-li k dispozici údaje podle požadavku 2.8.8, eSSL umožní ztotožnění ve zdrojích dat o fyzických osobách podle požadavku 2.8.10 nebo o právnických osobách podle požadavku 2.8.11 a zaznamená údaje z použitého zdroje dat do záznamu jmenného rejstříku, b) nejsou-li k dispozici údaje podle požadavku 2.8.8 nebo se nepodaří osobu ztotožnit podle písm. a), eSSL umožní vytvoření nového záznamu ve jmenném rejstříku bez ztotožnění osoby a záznam označí jako neztotožněný.
2.8.10	ESSL umožňuje ověřování údajů o fyzických osobách alespoň v těchto zdrojích: a) registr obyvatel informačního systému základních registrů, b) informační systém datových schránek.
2.8.11	ESSL umožňuje ověřování údajů o právnických osobách a fyzických osobách podnikajících alespoň v těchto zdrojích: a) registr osob informačního systému základních registrů, b) informační systém datových schránek.
2.8.12	ESSL je možné konfigurovat tak, že využívá notifikační služby informačního systému základních registrů pro automatickou aktualizaci údajů u záznamů jmenného rejstříku ztotožněných v informačním systému základních registrů.
2.8.13	ESSL při příjmu a odeslání dokumentu spojeného se záznamem ve jmenném rejstříku zajišťuje automatickou aktualizaci údajů u záznamů osob ztotožněných podle

Číslo	Požadavek
	požadavků 2.8.10 a 2.8.11; s výjimkou případů, kdy eSSL využívá notifikační službu podle požadavku 2.8.12.
2.8.14	ESSL automaticky identifikuje vícečetné záznamy ve jmenném rejstříku a o nalezeném stavu informuje uživatelskou roli oprávněnou ke správě jmenného rejstříku. ESSL umožní této uživatelské roli manuálně identifikovat vícečetné záznamy ve jmenném rejstříku. ESSL provede na základě potvrzení této uživatelské role sloučení touto rolí označených vícečetných záznamů.
2.8.15	ESSL umožní správcovské roli nastavit lhůtu pro automatické vymazání údajů a) o fyzické osobě vedené ve jmenném rejstříku, která nemá vazbu na dokument nebo spis, a b) o právnické osobě vedené ve jmenném rejstříku, která nemá vazbu na dokument nebo spis.
2.8.16	ESSL umožní správcovské roli manuální zničení údajů o osobě vedené ve jmenném rejstříku, která nemá vazbu na dokument nebo spis.
2.8.17	ESSL provádí identifikaci záznamů ve jmenném rejstříku, které nemají vazbu na dokument nebo spis, a u těchto záznamů sleduje lhůtu pro jejich zničení podle požadavku 2.8.15. Pokud je k záznamu ve jmenném rejstříku nově připojena vazba na dokument nebo spis a u tohoto záznamu již plyne lhůta pro zničení, je plynutí této lhůty zrušeno.
2.8.18	ESSL provádí automaticky zničení záznamů ve jmenném rejstříku, kterým uplynula lhůta pro zničení podle požadavku 2.8.15 a které nemají vazbu na dokument nebo spis.
2.8.19	ESSL umožňuje správcovské roli nastavit specifické podmínky ochrany osobních údajů v podobě určení uživatelské role oprávněné ke čtení, zápisu, úpravě a správě jmenného rejstříku a rozsahu oprávnění této uživatelské role ve vztahu k vedení jmenného rejstříku.
2.8.20	ESSL umožňuje uživatelské roli vyhledávat, filtrovat a setřídit záznamy ve jmenném rejstříku.

2.9 Samostatná evidence dokumentů

Číslo	Požadavek
2.9.1	Je-li samostatná evidence dokumentů napojena na eSSL, musí tak být realizováno rozhraním podle kapitoly 8.1, jehož prostřednictvím samostatná evidence dokumentů zajišťuje správu entit v eSSL, není-li jiný způsob napojení efektivnější.
2.9.2	Samostatná evidence dokumentů, která je napojena na eSSL, nemusí splňovat požadavky 2.9.3 až 2.9.16, pokud je zajišťuje prostřednictvím eSSL. Pokud samostatná evidence dokumentů využívá integraci na eSSL, musí taková samostatná evidence podporovat tvorbu spisů v souladu s požadavkem 2.9.9.
2.9.3	Jestliže samostatná evidence dokumentů zajišťuje příjem dokumentů, musí splňovat alespoň požadavky 2.1.1 až 2.1.3 a požadavky kapitoly 2.6.
2.9.4	Jestliže samostatná evidence dokumentů zajišťuje příjem e-mailů, musí zajišťovat alespoň

Číslo	Požadavek
	a) automatizované stahování a uložení e-mailových zpráv doručených na určené elektronické adresy, b) označení stažených e-mailových zpráv z určené elektronické adresy příznakem, že byly staženy, c) odesílání e-mailových zpráv prostřednictvím určené elektronické adresy, d) uchování e-mailové zprávy v původním formátu postupem podle požadavku 2.4.2 jako samostatné komponenty, e) uchování obsahu (těla) e-mailové zprávy jako samostatné komponenty a f) uchování jednotlivých připojených příloh jako samostatných komponent.
2.9.5	Jestliže samostatná evidence dokumentů zajišťuje příjem a odesílání dokumentů prostřednictvím informačního systému datových schránek, musí splňovat požadavky kapitoly 2.3.
2.9.6	Samostatná evidence dokumentů musí splňovat požadavky 2.4.1, 2.4.3, 2.4.4 a 2.5.1 až 2.5.5 týkající se datových formátů komponent.
2.9.7	Samostatná evidence dokumentů musí splňovat při evidenci dokumentu alespoň požadavky 2.7.1 a 2.7.5.
2.9.8	Samostatná evidence dokumentů zajišťuje, že dokumenty nebo spisy jsou vkládány do věcných skupin splňujících alespoň požadavky 3.1.1, 3.1.2, 3.1.8 až 3.1.12.
2.9.9	V případě, že samostatná evidence dokumentů spravuje spisy, musí splňovat alespoň požadavky 3.2.1, 3.2.2, 3.2.4 až 3.2.7.
2.9.10	Pokud samostatná evidence dokumentů spravuje typové spisy, musí splňovat požadavky kapitoly 3.3.
2.9.11	Samostatná evidence dokumentů musí splňovat alespoň požadavky 3.4.1, 3.4.4 a 3.4.5 týkající se vazeb mezi entitami.
2.9.12	Samostatná evidence dokumentů zajišťuje vedení a ztvárnění transakčního protokolu podle požadavku 5.2.12 a kapitoly 7.4.
2.9.13	Samostatná evidence dokumentů musí splňovat požadavky 6.1.4, 6.1.6 písm. a) až d), 6.1.7, 6.1.10, 6.1.11 a 6.1.12 týkající se skartačního režimu.
2.9.14	Samostatná evidence dokumentů při skartačním řízení musí splňovat alespoň požadavky kapitoly 6.2 a požadavky 7.2.1 až 7.2.10. V případě požadavku 7.2.10 se pro samostatnou evidenci jedná o doporučený seznam metadat.
2.9.15	Samostatná evidence dokumentů v případě exportu, importu nebo přenosu dat musí splňovat alespoň požadavek 6.3.1.
2.9.16	Samostatná evidence dokumentů musí splňovat požadavky kapitoly 2.8 týkající se jmenného rejstříku.

3 SPISOVÝ A SKARTAČNÍ PLÁN A ORGANIZACE SPISŮ

3.1 Věcné skupiny

Číslo	Požadavek
3.1.1	ESSL spravuje věcné skupiny v souladu se spisovým a skartačním plánem původce. ESSL zajišťuje, že věcné skupiny jsou uspořádány hierarchicky, přičemž spisy a typové spisy smí být zatříděny pouze do věcných skupin na nejnižší úrovni hierarchie (neobsahují jiné věcné skupiny).
3.1.2	ESSL vede o věcné skupině alespoň tato metadata: a) jednoznačný identifikátor, b) spisový znak, c) obsah – slovní popis, d) datum otevření, e) datum uzavření. O věcné skupině na nejnižší úrovni hierarchie eSSL dále vede alespoň tato metadata: f) odkaz na skartační režim, g) příznak, že věcná skupina je určena pro typové spisy, h) příznak, který stanoví způsob přidělování čísla jednacího dokumentům v zakládaných spisech dané věcné skupiny (požadavek 2.7.4), i) příznak, že na obsah věcné skupiny je uplatněn trvalý skartační souhlas vydaný příslušným archivem a s vyznačením, zda má být realizován požadavek 3.2.9 písm. a).
3.1.3	ESSL umožňuje správcovské roli stanovit datum otevření věcné skupiny a) pro jednotlivé věcné skupiny samostatně, b) stanovením data otevření spisového plánu. *Primární entitou je věcná skupina, spisový a skartační plán je časový řez aktuálně platných věcných skupin.*
3.1.4	ESSL umožňuje správcovské roli a) přidat nové věcné skupiny, b) uzavřít stávající věcné skupiny pro vkládání.
3.1.5	ESSL umožňuje správcovské roli upravit v metadatech obsah – slovní popis stávající věcné skupiny, aniž by vznikla nová věcná skupina.
3.1.6	ESSL umožňuje správcovské roli v každé konkrétní věcné skupině spisového plánu nastavit možnost vytvářet typové spisy. ESSL zajistí, že v této věcné skupině nesmí být vložena jiná věcná skupina nebo spis.
3.1.7	ESSL spravuje spisové a skartační plány, které jsou souhrnem věcných skupin používaných v danou dobu. ESSL vede o spisovém a skartačním plánu alespoň tato metadata: a) jednoznačný identifikátor, b) název spisového a skartačního plánu, c) popis spisového a skartačního plánu,

Číslo	Požadavek
	d) platnost od, e) platnost do, f) odkaz na věcné skupiny, které tvoří spisový a skartační plán.
3.1.8	ESSL umožňuje uživatelské roli vkládat spisy a typové spisy pouze do otevřených věcných skupin, tj. do aktuálně platného spisového a skartačního plánu.
3.1.9	ESSL umožňuje posuzovateli skartační operace přetřídění uzavřených spisů z věcné skupiny do jiné věcné skupiny; tyto věcné skupiny mohou být uzavřené nebo otevřené.
3.1.10	ESSL umožňuje správcovské roli stanovit, k jakým věcným skupinám má uživatelská role nebo uživatel přístup.
3.1.11	ESSL zajišťuje, aby všechny spisové znaky byly jednoznačné v rámci konkrétního spisového a skartačního plánu.
3.1.12	ESSL zajistí, že spisové znaky jsou tvořeny zřetězením jednoduchých spisových znaků, oddělených znakem oddělovače: a) „ “ (mezera), b) „–“ (pomlčka), c) „/“ (lomítko), d) „.“ (tečka).

3.2 Spisy

Číslo	Požadavek
3.2.1	ESSL zajistí, že podle volby uživatelské role se nový spis otevře a) ve věcné skupině, nebo b) v dílu typového spisu zvolené součásti typového spisu.
3.2.2	ESSL při založení spisu automaticky přiřadí spisu jednoznačný identifikátor, spisovou značku, spisový znak a způsob přidělování čísla jednacího podle věcné skupiny nebo součásti typového spisu, ve které byl spis založen. ESSL automaticky zaznamená datum založení spisu.
3.2.3	ESSL při vložení dokumentu do spisu automaticky přiřadí dokumentu pořadové číslo ve spisu a číslo jednací podle požadavku 2.7.4.
3.2.4	ESSL zajistí založení spisu a) na základě dokumentu; v tom případě automaticky vyplní stručný obsah spisu podle stručného obsahu dokumentu a umožní jeho bezprostřední editaci, nebo b) bez dokumentu; v tom případě stručný obsah spisu vyplní uživatelská role.
3.2.5	ESSL na základě volby uživatelské role zajistí vložení dokumentu do založeného spisu podle přístupových práv uživatelské role.
3.2.6	ESSL na základě volby uživatelské role vyřídí spis a datum vyřízení zaznamená do metadat. Vyřízením spisu jsou současně vyřízeny všechny dokumenty v něm, které již dříve nebyly vyřízeny samostatně podle požadavku 3.2.7.

Číslo	Požadavek
3.2.7	ESSL umožní uživatelské roli označit jednotlivé dokumenty ve spisu jako vyřízené. Tím není dotčen požadavek 3.2.6.
3.2.8	ESSL na základě konfigurace umožní vyznačení vyřízení spisu jeho uzavřením.
3.2.9	ESSL na základě volby uživatelské role uzavře spis. Přitom provede kontrolu a) datových formátů komponent, které popřípadě převede do výstupních datových formátů, b) metadat zapisovaných uživatelskou rolí, která jsou nezbytná pro vytvoření SIP balíčku podle přílohy č. 2, přičemž uživatelskou roli případně vyzve k jejich doplnění.
3.2.10	ESSL zajistí, že pokud je věcná skupina nebo součást typového spisu, ve kterém se spis v okamžiku svého uzavření nachází, označena příznakem podle požadavku 3.1.2 písm. i), resp. 3.3.6 písm. d), pak neprovede kontrolu a související činnosti a) podle požadavku 3.2.9, nebo b) podle požadavku 3.2.9 písm. b). *V případě delších skartačních lhůt je vhodné i v případě uděleného skartačního souhlasu provést kontrolu a případně převod všech komponent do výstupního formátu, aby původce byl schopen po dobu trvání lhůty realizovat potřeby spojené s ukládaným dokumentem podle požadavku 3.2.10 písm. a).*
3.2.11	ESSL na základě volby uživatelské role uzavřený spis otevře. Uzavřený spis vytvořený nebo vložený do dílu typového spisu, který je již uzavřen, se při otevření automaticky přetřídí do otevřeného dílu typového spisu v příslušné součásti.
3.2.12	Jestliže je znovuotevíraný spis v uzavřené věcné skupině, uzavřeném typovém spisu nebo v uzavřené součásti typového spisu, eSSL vyzve uživatelskou roli, aby spis přetřídila do otevřené věcné skupiny nebo otevřeného dílu typového spisu, a přetřídění umožní.
3.2.13	Při změně spisového a skartačního plánu, v jejímž rámci dojde k uzavření věcné skupiny, ve které jsou zatříděny spisy, eSSL vyzve správcovskou roli k přetřídění otevřených spisů z uzavírané do otevřené věcné skupiny. Na základě volby správcovské role eSSL hromadně přetřídí označené spisy.

3.3 Typové spisy, součásti typového spisu a díly typového spisu

Číslo	Požadavek
3.3.1	ESSL umožňuje uživatelské roli zakládat typové spisy. ESSL umožňuje zakládat typové spisy pouze v otevřené věcné skupině k tomu určené.
3.3.2	ESSL při založení nového typového spisu v dané věcné skupině automaticky otevře součásti a díly typového spisu podle šablony typového spisu definované pro tuto věcnou skupinu.
3.3.3	ESSL zajišťuje, že a) šablona typového spisu obsahuje alespoň jednu součást typového spisu,

	b) součást typového spisu obsahuje alespoň jednu součást typového spisu nebo alespoň jeden díl typového spisu; žádná součást typového spisu nemůže obsahovat jinou součást typového spisu a současně díl typového spisu, c) pokud otevřená součást typového spisu neobsahuje jinou součást typového spisu, pak obsahuje právě jeden otevřený díl typového spisu, d) díly typového spisu v různých součástech typového spisu jsou na sobě nezávislé.
3.3.4	ESSL při uzavření věcné skupiny s otevřenými typovými spisy zajistí, že správcovská role a) stanoví věcnou skupinu, do které mají být typové spisy přetříděny, b) namapuje šablonu původní věcné skupiny a nové věcné skupiny tak, aby všechny součásti typového spisu v šabloně původní věcné skupiny měly odpovídající součást v šabloně nové věcné skupiny. ESSL zajistí hromadné přetřídění otevřených typových spisů do nové věcné skupiny podle namapování šablon k datu platnosti nového spisového řádu. *Pro každou součást typového spisu v šabloně původní věcné skupiny musí být přiřazena součást typového spisu v šabloně nové věcné skupiny. To nebrání, aby více součástí typového spisu v šabloně původní věcné skupiny bylo přiřazeno jedné součásti typového spisu v šabloně nové věcné skupiny.*
3.3.5	ESSL zajistí, že v rámci vytváření věcné skupiny obsahující typové spisy správcovská role definuje pro tuto věcnou skupinu šablonu typového spisu.
3.3.6	ESSL musí pro určitou věcnou skupinu umožnit správcovské roli vytvoření šablony typového spisu. Každá součást typového spisu v šabloně typového spisu: a) je označena spisovým znakem, který vzniká doplněním zděděného spisového znaku věcné skupiny typového spisu, ve které jsou typové spisy vytvářeny, nebo doplněním zděděného spisového znaku součásti typového spisu, do které je daná součást typového spisu vložena, o jednoduchý spisový znak součásti typového spisu, b) má přidělený skartační režim, pokud do ní není vložena jiná součást typového spisu, c) má nastavený způsob přidělování čísla jednacího v zakládaných spisech dané součásti typového spisu (požadavek 2.7.4), d) příznak, že je na obsah součásti typového spisu uplatněn trvalý skartační souhlas vydaný příslušným archivem a s vyznačením, zda má být realizován požadavek 3.2.9 písm. a). *Například požadavky na typové spisy týkající se organizací zřizovaných původcem mohou zahrnovat následující součásti: Statutární dokumenty a jejich příprava, Podklady statutárních orgánů a jejich vedení, Vnitřní předpisy, Zápisy vedení zasílané na vědomí, Zprávy a hlášení, Výroční zprávy, Rozbory hospodaření, Audity, Příprava rozpočtu, Zaměstnanecké záležitosti, Investice, Provoz, Členství v mezinárodních organizacích a Ostatní.* *Každý nový typový spis vytvořený v této věcné skupině je poté automaticky vytvořen s těmito součástmi podle šablony, kterou připraví správcovská role. Spisový znak a skartační režim jsou přidělovány v šabloně například následovně:* *01.2 Věcná skupina původce pro dané typové spisy*

	Typový spis zřizované organizace A (vytvořený podle šablony součástí typového spisu) *01.2.1 Statutární dokumenty a jejich příprava A 10* *01.2.2 Podklady statutárních orgánů a jejich vedení A 10* *01.2.3 Vnitřní předpisy A 5* *01.2.4 Zápisy vedení zasílané na vědomí S 5* *01.2.5 Zprávy a hlášení* *01.2.5.1 Výroční zprávy A 10* *01.2.5.2 Rozbory hospodaření A 10* *01.2.5.3 Audity A 5* *01.2.6 Příprava rozpočtu S 5* *01.2.7 Zaměstnanecké záležitosti A 5* *01.2.8 Investice A 5* *01.2.9 Provoz S 5* *01.2.10 Členství v mezinárodních organizacích A 5* *01.2.11 Ostatní S 5*
3.3.7	ESSL zajistí, že v případě změny šablony typového spisu bude pro tvorbu nových typových spisů uzavřena stávající věcná skupina a zároveň bude otevřena nová věcná skupina pro tvorbu typových spisů založených na změněné šabloně. ESSL zajistí přetřídění otevřených typových spisů z uzavírané věcné skupiny postupem podle požadavku 3.3.4.
3.3.8	ESSL umožňuje správcovské roli v šabloně typového spisu pro konkrétní věcnou skupinu upravit a) názvy součástí typového spisu, b) určené časové období dílu pro každou součást typového spisu, pokud do ní není vložena jiná součást typového spisu.
3.3.9	ESSL umožňuje nastavit určené časové období dílu typového spisu v konkrétní věcné skupině stanovením doby, po kterou má být díl otevřen. *Například: 5 let, školní rok, kalendářní rok.*
3.3.10	ESSL umožňuje zakládat spisy a vkládat spisy do otevřených dílů typového spisu.
3.3.11	ESSL umožňuje správcovské roli změnit název součásti typového spisu v šabloně typového spisu, aniž by se měnila příslušná šablona typového spisu.
3.3.12	ESSL umožňuje uživatelské roli uzavření typového spisu a součásti typového spisu.
3.3.13	ESSL neumožní uzavření typového spisu nebo součásti typového spisu, pokud obsahuje díl typového spisu s neuzavřeným spisem.
3.3.14	ESSL automaticky uzavře díl typového spisu po uplynutí určeného časového období. ESSL při uzavření dílu typového spisu zajistí v příslušné součásti typového spisu automatické otevření nového dílu typového spisu.
3.3.15	ESSL kontroluje, zda jsou v případě uzavření dílu typového spisu uzavřeny i všechny v něm vytvořené nebo do něj vložené spisy. Jestliže tyto spisy uzavřeny nejsou, eSSL

	automaticky vyjme spis z uzavíraného dílu a vloží jej do nově otevřeného dílu v příslušné (otevřené) součásti.
3.3.16	ESSL zabraňuje uživatelské roli zakládat spisy v uzavřeném dílu typového spisu nebo vkládat spisy do uzavřeného dílu typového spisu.
3.3.17	ESSL neumožní přiřazení skartačního režimu typovému spisu; typový spis nemá skartační režim.
3.3.18	ESSL zajistí, že součást typového spisu, do které je v šabloně typového spisu a) vložen díl typového spisu, má v daný okamžik právě jeden skartační režim, b) vložena jiná součást typového spisu, nemá skartační režim.
3.3.19	ESSL v okamžiku otevření dílu typového spisu přiřadí dílu typového spisu skartační režim nadřazené součásti typového spisu.
3.3.20	ESSL zobrazuje informace o dílech typového spisu pouze uživatelské roli, která má k tomu zvlášť přiřazená práva. ESSL při práci s typovými spisy zobrazuje uživatelské roli entity vytvořené nebo vložené v dílech typového spisu jako entity součásti typového spisu, tj. potlačuje zobrazování dílů typového spisu. *Například pokud uživatelská role vkládá spisy do dílu typového spisu, eSSL uživatelské roli znázorní pouze příslušnou součást typového spisu. Uživatelská role nesmí být nucena vyhledávat v rámci součásti typového spisu díl typového spisu.*

3.4 Udržování vazeb mezi entitami

Číslo	**Požadavek**
3.4.1	ESSL zajistí, že entity typový spis, součást typového spisu, díl typového spisu, spis nebo dokument budou otevřeny, založeny, vloženy nebo zatříděny právě do jedné nadřazené entity. U věcné skupiny hierarchicky podřízené jiné věcné skupině toto platí obdobně.
3.4.2	ESSL nedovolí uzavření entity, pokud nejsou uzavřeny všechny jí podřízené entity. ESSL před uzavřením dílu typového spisu všechny v něm otevřené spisy přetřídí do nově otvíraného dílu typového spisu.
3.4.3	ESSL umožňuje správcovské roli hromadně přetřídit (přemístit) veškerý obsah celé věcné skupiny nebo jeho vyznačenou část do jiné věcné skupiny v rámci spisového plánu.
3.4.4	ESSL zajišťuje označení spisů nebo typových spisů přetříděných do jiných věcných skupin novými spisovými znaky. Pro označení součástí typového spisu spisovými znaky platí první věta obdobně.
3.4.5	ESSL umožní roli při přetřiďování spisu rozhodnout, zda budou přetříděny i uzavřené spisy.
3.4.6	ESSL zajistí, že do uzavřené entity není možné vkládat ani z ní vyjímat jiné entity. Výjimkou pro vyjmutí je a) uzavřený díl typového spisu, ze kterého je vyjmut spis za účelem znovuotevření v aktuálně otevřeném dílu typového spisu, b) přetřídění uzavřených spisů podle požadavku 3.1.9.

Číslo	Požadavek
3.4.7	Pokud je dokument zařazený ve spisu přetříděn do jiného spisu, ve kterém je číslo jednací tvořeno na základě a) spisové značky a pořadí dokumentu ve spisu, eSSL přidělí dokumentu nové číslo jednací, b) přiřazeného pořadového čísla v rámci předem určeného časového období podle požadavku 2.7.2, eSSL přidělí dokumentu nové číslo jednací v případě, že původní číslo jednací bylo přiděleno na základě spisové značky a pořadí dokumentu ve spisu.
3.4.8	ESSL zajistí, že po přetřídění podle požadavku 3.4.7 budou požadavek 5.1.8 písm. b) a požadavek 5.2.6 písm. b) realizovány s novým i původním číslem jednacím.
3.4.9	ESSL zajistí, že pokud je přetřiďován spis do jiné věcné skupiny nebo součásti typového spisu, nezmění se způsob přidělování čísla jednacího dokumentům, který byl nastaven při jeho založení (požadavky 2.7.2, 3.1.2 a 3.3.6).

4 ODKAZOVÁNÍ MEZI ENTITAMI

4.1 Křížové odkazy

Číslo	Požadavek
4.1.1	ESSL umožňuje uživatelské roli vytvořit volný křížový odkaz mezi a) spisy, b) dokumenty, c) spisy a dokumenty.
4.1.2	ESSL umožňuje uživatelské roli vytvořit pevný křížový odkaz v případě připojení spisu k jinému spisu, přičemž nezáleží, zda je některý ze spisů uzavřený nebo otevřený.
4.1.3	ESSL nedovolí vytvářet pevné křížové odkazy na spisy založené v dílu typového spisu nebo vložené do dílu typového spisu. Jestliže je do dílu typového spisu vkládán spis obsahující pevný křížový odkaz na jiný spis, eSSL vloží do dílu typového spisu oba spisy, přičemž zároveň odstraní pevný křížový odkaz mezi vkládanými spisy.
4.1.4	ESSL nejpozději při uzavření spisu obsahujícího pevný křížový odkaz podle konfigurace eSSL (požadavek 4.1.5) přetřídí jeden ze spisů do věcné skupiny ke druhému spisu. Jestliže jsou oba spisy (nebo jeden z nich) vkládány do dílu typového spisu, eSSL oba spisy přetřídí do dílu typového spisu a automaticky odstraní pevný křížový odkaz.
4.1.5	ESSL je možné konfigurovat tak, že v případě spisů, mezi nimiž je vytvořen pevný křížový odkaz, a jsou zatříděny v různých věcných skupinách, automaticky při provádění požadavku 4.1.4 všechny tyto spisy přetřídí do věcné skupiny, ve které je zatříděn a) nejdříve založený spis, nebo b) nejpozději založený spis.
4.1.6	ESSL povolí odstranění pevného křížového odkazu pouze zpracovateli. ESSL zajistí zadání důvodu odstranění pevného křížového odkazu.
4.1.7	ESSL umožňuje uživatelské roli hromadně zjistit informace o metadatech alespoň v rozsahu hlavičky metadat entit spojených křížovým odkazem. ESSL umožní tyto entity na základě uživatelských práv znázornit.

4.2 Druhy dokumentů

Číslo	Požadavek
4.2.1	ESSL udržuje číselník druhů dokumentů. ESSL omezuje definování a udržování číselníku druhů dokumentů výlučně na správcovskou roli.
4.2.2	ESSL zajistí, že dokument má přiřazen nejvýše jeden druh dokumentu.
4.2.3	ESSL umožňuje konfigurovat specifické prvky metadat pro druhy dokumentů. *Například faktury se odlišují použitím metadat čísel účtů.*
4.2.4	ESSL umožní přiřadit druhu dokumentu skartační režim.

5 VYHLEDÁVÁNÍ, VÝBĚR, ZNÁZORNĚNÍ A ZTVÁRNĚNÍ

5.1 Vyhledávání a výběr

Číslo	Požadavek
5.1.1	ESSL při vyhledávání poskytne uživatelské roli pouze informace (metadata nebo obsah komponent), ke kterým má tato uživatelská role oprávněný přístup.
5.1.2	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 5.1.1, 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 typového spisu nebo dokumentu), popřípadě uvede zpracovatele entity, neznázorní však název entity ani jiná metadata, c) znázorní pouze název, druh entity (například u věcné skupiny a dokumentu), datum vytvoření a zpracovatele, nebo d) znázorní název a další metadata entity. *Jiným způsobem vyžádání přístupu, než je uvedeno v požadavku 5.1.1, se myslí zejména pokus o přístup k entitě na základě reference v systému (zahrnutí entity v seznamu nebo výpisu, funkčním dialogu apod.), přímého zadání odkazu na entitu nebo zobrazení entitu zahrnující apod. Rozsah zobrazených informací podle jednotlivých písmen požadavku je řízen kombinací oprávnění uživatele a způsobu vyžádání přístupu k entitám.*
5.1.3	ESSL umožňuje roli podle přístupových oprávnění vyhledat a vybrat a) dokumenty, b) jakoukoli úroveň věcné skupiny, spisu, typového spisu a součásti typového spisu a jejich příslušná metadata.
5.1.4	ESSL poskytuje vyhledávací funkci, která umožňuje v jakékoli vzájemné kombinaci spojit vyhledávací podmínky za použití booleovských operátorů a) A („AND“), b) NEBO („OR“), c) NE („NOT“).
5.1.5	ESSL umožňuje roli podle přístupových oprávnění vyhledávat v metadatech a v obsahu komponent podle numerického, alfanumerického nebo textového řetězce.
5.1.6	ESSL umožňuje roli omezit rozsah vyhledávání na ty věcné skupiny, spisy, typové spisy, součásti typového spisu a případně díly typového spisu, které role určila.
5.1.7	ESSL umožňuje roli stanovit časové intervaly pro vyhledávání, například formou rozsahu nebo počtu dnů.
5.1.8	ESSL zajišťuje vyhledávání a řazení výsledků vyhledávání alespoň podle a) identifikace typového spisu nebo součásti typového spisu, b) čísla jednacího nebo části čísla jednacího dokumentu, c) spisové značky nebo části spisové značky spisu,

Číslo	Požadavek
	d) jednoznačného identifikátoru, e) zpracovatelů, f) data odeslání, g) data doručení nebo v případě vlastních dokumentů data zaevidování, h) označení a identifikace dokumentu provedených odesílatelem, i) názvu (věci) věcné skupiny, dokumentu, spisu, typového spisu nebo součásti typového spisu, j) spisového znaku, k) skartačního režimu, l) způsobu odeslání, m) způsobu doručení.
5.1.9	ESSL umožňuje správcovské roli vyhledávat v transakčním protokolu specifické operace, entity, uživatele, role, časové údaje nebo časové intervaly.
5.1.10	Pokud je vyhledán znepřístupněný dokument, eSSL informuje uživatelskou roli podle přístupových oprávnění o existenci původního dokumentu, případně dokument uživatelské roli zpřístupní na základě zvláštního oprávnění.

5.2 Znázornění a ztvárnění

Číslo	Požadavek
5.2.1	ESSL uživatelské roli pracující s věcnou skupinou, spisem, typovým spisem, součástí typového spisu nebo dokumentem znázorní informace o a) všech hierarchicky nadřazených entitách a b) všech entitách připojených křížovým odkazem.
5.2.2	ESSL zpřístupňuje uživatelské roli obsah věcných skupin, spisů, typových spisů, součástí typových spisů nebo dílů typových spisů k prohlížení bez rozlišování mezi uzavřenými a otevřenými věcnými skupinami, spisy, typovými spisy, součástmi typového spisu nebo díly typového spisu.
5.2.3	ESSL zajistí uživatelské roli ztvárnění metadat dokumentu, spisu, součásti typového spisu a typového spisu vedených v eSSL.
5.2.4	ESSL umožňuje uživatelské roli zobrazit na obrazovce u každého přijatého dokumentu jeho metadata.
5.2.5	ESSL zajistí uživatelské roli ztvárnění základních metadat za účelem vytištění obalu analogových částí spisu nebo dílu typového spisu. Základními metadaty pro ztvárnění jsou alespoň a) spisová značka spisu nebo název typového spisu, b) název součásti typového spisu, c) stručný obsah (předmět, věc) spisu, d) datum založení/uzavření spisu nebo dílu typového spisu, e) jednoznačný identifikátor spisu nebo dílu typového spisu včetně vyjádření ve strojově čitelném kódu,

Číslo	Požadavek
	f) spisový znak, g) skartační režim.
5.2.6	ESSL znázorní uživatelské roli alespoň tato metadata: a) jednoznačný identifikátor, b) číslo jednací dokumentu (požadavek 2.7.4), c) spisový znak, d) část transakčního protokolu zachycující historii entity, zejména oběh, e) spisovou značku spisu, f) název typového spisu a součásti typového spisu, g) datum uzavření věcné skupiny, spisu, typového spisu, součásti typového spisu a dílu typového spisu, h) skartační režim, i) křížové odkazy na jiné entity, j) informaci o umístění analogové části spisu, k) podobu dokumentu (analogová, nebo digitální); jestliže je alespoň jedna z částí dokumentu analogová, podoba celého dokumentu se považuje za analogovou.
5.2.7	ESSL roli podle přístupových oprávnění dále znázorní a umožní ztvárnění za účelem vytištění alespoň a) pevný křížový odkaz vzájemně identifikující spojené spisy, b) u typového spisu seznam všech spisů zařazených do dílů jednotlivých součástí typového spisu v členění po dílech pro jednotlivá určená časová období, c) seznam všech dokumentů ve spisu, jejich jednoznačné identifikátory a čísla jednací.
5.2.8	ESSL pro hromadný tisk zajistí uživatelské roli znázornění údajů stanovených v požadavcích 5.2.3 až 5.2.7.
5.2.9	ESSL zajistí uživatelské roli znázornění seznamu všech spisů nebo typových spisů včetně zatřídění do věcné skupiny.
5.2.10	ESSL zajistí správcovské roli ztvárnění spisového plánu za účelem jeho vytištění.
5.2.11	ESSL zajistí ztvárnění vyhledaných informací podle kapitoly 5.1 nebo znázorněných podle kapitoly 5.2 do komponenty ve výstupním datovém formátu.
5.2.12	ESSL obsah transakčního protokolu za stanovený časový úsek, nejdéle však jeden den, automaticky na konci tohoto časového úseku uloží jako dokument s komponentou v datovém formátu PDF/A nebo XML podle přílohy č. 6, který opatří elektronickou pečetí a elektronickým časovým razítkem podle standardu PAdES nebo XAdES-T. Podepisovanou oblastí XML bude vždy kořenový element, kterým je TransakcniLogSystemu. Tato podepisovaná data budou zapouzdřena v elementu Signature/Object. Syntaxe podpisu bude Enveloping. ESSL automaticky dokument zatřídí do spisu.

Číslo	Požadavek
5.2.13	ESSL zajistí uživatelské roli hromadné ztvárnění metadat jednoho nebo více spisů. Ztvárněný spis obsahuje metadata spisu, metadata vložených dokumentů a metadata komponent alespoň v rozsahu: a) název původce, b) spisový znak, c) skartační režim spisu, d) spisová značka, e) číslo jednací, nebo evidenční číslo ze samostatné evidence dokumentů, f) předmět (věc), g) zpracovatel, h) podepisující komponenty, i) soupis spisů připojených pevným křížovým odkazem, j) soupis spisů připojených volným křížovým odkazem, k) uživatelské poznámky spisu se jménem uživatele a datem, l) příslušné části transakčního protokolu, m) soupis dokumentů ve spisu, n) jednotlivé dokumenty a jejich komponenty. Samostatné komponenty se řadí následujícím způsobem 1) komponenta obsahující údaje podle písm. a) až k), 2) komponenta obsahující příslušnou část transakčního protokolu (písm. l) ztvárněného v PDF/A, který opatří elektronickou pečetí a elektronickým časovým razítkem podle standardu PAdES, 3) komponenta obsahující soupis dokumentů vložených ve spisu (písm. m), 4) jednotlivé dokumenty a jejich komponenty (písm. n). *Například dokumenty se označí třímístným pořadovým číslem počínaje „001“ a každá jejich komponenta se (ve správném pořadí) označí dvoumístným pořadovým číslem komponenty za pomlčkou (například „001–02“).*
5.2.14	ESSL zajistí správcovské roli ztvárnění konfiguračních parametrů za účelem jejich vytištění.
5.2.15	ESSL umožňuje správcovské roli vytvářet seznamy uživatelských rolí a jednotlivých uživatelů pro kontrolu jejich přístupu ke konkrétním entitám a seznamy entit pro kontrolu přístupových práv uživatelů k nim.

6 UKLÁDÁNÍ A VYŘAZOVÁNÍ DOKUMENTŮ

6.1 Skartační režimy

Číslo	Požadavek
6.1.1	ESSL umožňuje výlučně správcovským rolím vytvářet a upravovat skartační režim a přiřazovat ho věcným skupinám, součástem typových spisů a druhům dokumentů. *Tím nejsou dotčeny skartační režimy dokumentů podle předchozí právní úpravy.*
6.1.2	ESSL vyžádá od správcovské role provádějící úpravu nebo znepřístupnění skartačního režimu zadání důvodu úpravy nebo znepřístupnění. *Úpravy skartačního režimu jsou důsledně kontrolovány tak, aby bylo minimalizováno riziko zničení dokumentu jiným způsobem, než který původce stanovil ve svém spisovém řádu.*
6.1.3	ESSL zajistí, že skartační režim uplatňovaný na nově vytvořený dokument, spis, nebo díl typového spisu je děděn a) z mateřské věcné skupiny v případě spisu, b) ze spisu v případě dokumentu vloženého do tohoto spisu, c) z příslušné součásti typového spisu v případě jejího dílu, d) z dílu typového spisu v případě spisu vloženého do tohoto dílu.
6.1.4	ESSL umožňuje správcovské roli vždy přidělit skartační režim každé věcné skupině na nejnižší úrovni hierarchie, součásti typového spisu na nejnižší úrovni hierarchie nebo druhu dokumentu.
6.1.5	ESSL zajistí, že každý skartační režim obsahuje a) jednoznačný identifikátor, b) skartační lhůtu nebo rok vyřazení, c) typ skartační operace (skartační znak „A“ nebo „S“), d) spouštěcí událost.
6.1.6	ESSL umožňuje správcovské roli stanovit pro skartační režim jednu z následujících spouštěcích událostí a) rok vyřízení spisu, b) rok uzavření spisu, typového spisu, součásti typového spisu nebo dílu typového spisu, c) rok založení spisu totožný s rokem jeho evidence, d) rok narození nebo vzniku subjektu, e) externí událost, u které nelze předem stanovit okamžik vzniku spouštěcí události (například formou užití slov „po skončení platnosti smlouvy“, „od likvidace skládky“ nebo „po zahájení insolvenčního řízení“), s počtem let, po jejichž uplynutí eSSL vyzve posuzovatele skartační operace k posouzení, zda již externí spouštěcí událost nastala.
6.1.7	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“),

Číslo	Požadavek
	b) návrh na zničení (dokumenty označené skartačním znakem „S“).
6.1.8	Pokud u dokumentu, spisu nebo dílu typového spisu současně platí různé skartační režimy (s jinou skartační lhůtou nebo s jiným skartačním znakem nebo jinou spouštěcí událostí), vzniká konflikt skartačních režimů. Konflikty vznikají v následujících případech: a) skartační režim se vztahuje ke spisu v dílu typového spisu a k některým dokumentům v těchto spisech, které současně mají skartační režim přidělen na základě druhu dokumentu, b) pokud jsou spisy spojeny pomocí pevných křížových odkazů (požadavek 4.1.2), c) liší se skartační režim spisu a skartační režim v něm zatříděného dokumentu. ESSL před uzavřením spisu nebo dílu typového spisu zajišťuje automaticky vyřešení konfliktů: 1) v případě písm. a) a c) přidělením závažnějšího skartačního režimu. Pokud alespoň jeden ze skartačních režimů v konfliktu obsahuje skartační znak „A“, bude v rámci výsledného skartačního režimu uplatněn skartační znak „A“, v ostatních případech bude uplatněn skartační znak „S“. Ve výsledném skartačním režimu bude uplatněna nejdelší skartační lhůta z konfliktních skartačních režimů. Při stanovení nejdelší skartační lhůty budou zohledněny rovněž spouštěcí události (požadavek 6.1.6). 2) v případě písm. b) postupem stanoveným v požadavcích 4.1.3 a 4.1.4.
6.1.9	Pokud eSSL identifikuje externí spouštěcí událost podle požadavku 6.1.6, která nemá uveden rok, kdy nastala, eSSL po uplynutí lhůty pro kontrolu spouštěcí události počítané od uzavření spisu vyzve posuzovatele skartační operace, aby rozhodl, zda externí spouštěcí událost nastala. Jestliže spouštěcí událost a) nastala, posuzovatel skartační operace zaznamená do metadat spisu rok, kdy pro spis spouštěcí událost nastala; obdobně se postupuje v případě dokumentu, který má přiřazen druh dokumentu obsahující skartační režim s externí spouštěcí událostí, b) nenastala, posuzovatel skartační operace potvrdí eSSL tuto skutečnost; eSSL vyzve znovu k rozhodnutí posuzovatele skartační operace po uplynutí počtu let stanovených při rozhodnutí, zda externí spouštěcí událost nastala. ESSL zajistí, že posuzovatel skartační operace může 1) pro součást typového spisu, pro spisy nebo pro dokumenty zatříděné ve věcné skupině podle předchozí právní úpravy kdykoli hromadně doplnit rok spouštěcí události, 2) individuálně u spisu kdykoli doplnit rok spouštěcí události.
6.1.10	Pokud uplyne skartační lhůta stanovená určitému dokumentu zatříděnému ve věcné skupině podle předchozí právní úpravy, spisu nebo dílu typového spisu skartačním režimem, eSSL vytvoří po vyřešení konfliktů skartačních režimů (požadavek 6.1.8) návrh na jejich vyřazení.

Číslo	Požadavek
6.1.11	ESSL umožňuje řízení procesu výběru dokumentů ve skartačním řízení výlučně posuzovateli skartační operace.
6.1.12	ESSL při přetřídění uplatní dědičnost skartačního režimu z nové mateřské věcné skupiny nebo z nové mateřské součásti typového spisu na přetřiďované spisy nebo dokumenty zatříděné ve věcné skupině podle předchozí právní úpravy.
6.1.13	ESSL umožňuje, aby posuzovatel skartační operace nastavil u věcné skupiny, spisu, typového spisu, součásti typového spisu nebo dílu typového spisu příkaz k pozastavení skartační operace. Toto pozastavení se vztahuje na všechny dceřiné entity věcné skupiny, spisu, typového spisu, součásti typového spisu a dílu typového spisu, na kterém bylo pozastavení skartační operace provedeno, i na entity propojené pevným křížovým odkazem s entitou, kde k pozastavení došlo. V případě dokumentů zatříděných ve věcné skupině podle předchozí právní úpravy se tento požadavek aplikuje obdobně.
6.1.14	ESSL zajistí, že pozastavení skartační operace nepřerušuje plynutí skartační lhůty.
6.1.15	ESSL zabraňuje u entity (včetně jejích dceřiných entit), na kterou je uplatněno pozastavení skartační operace, a) znepřístupnění, b) zařazení do návrhu na vyřazení dokumentů.
6.1.16	ESSL umožňuje posuzovateli skartační operace odstranit pozastavení skartační operace.

6.2 Skartační řízení

Číslo	Požadavek
6.2.1	ESSL na základě pokynu posuzovatele skartační operace vytvoří seznam entit navržených k vyřazení, který je tvořen datovými balíčky SIP podle přílohy č. 2. Datový balíček SIP je tvořen podle požadavku 9.2.2 a na základě volby posuzovatele skartační operace a) neobsahuje komponenty, nebo b) obsahuje komponenty.
6.2.2	ESSL vytvoří seznam entit podle požadavku 6.2.1 tak, aby jej mohl původce a) předat příslušnému archivu na technických nosičích dat, nebo b) vložit na portál pro zpřístupnění archiválií v digitální podobě na základě uživatelského oprávnění posuzovatele skartační operace, nebo c) předat automatizovaně příslušnému archivu prostřednictvím aplikačního rozhraní stanoveného Národním archivem, pokud bylo zveřejněno.
6.2.3	ESSL vždy zaznamená v datovém balíčku SIP vazbu na uložení analogových částí dokumentů a spisů, 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.*

Číslo	Požadavek
6.2.4	Příslušný archiv může v průběhu archivní prohlídky požádat prostřednictvím datové zprávy podle přílohy č. 4 o datové balíčky SIP obsahující komponenty. V takovém případě eSSL na základě seznamu, ve kterém je u identifikátorů entit uvedeno „předložit k výběru“, exportuje datové balíčky SIP s komponentami.
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 entity s vyznačenou operací „vybrat za archiválii“ vytvoří datové balíčky SIP obsahující i komponenty 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 entity 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 entity s vyznačenou operací „vyřadit z výběru“ eSSL vyzve posuzovatele skartační operace k úpravě skartačního režimu, d) u entity s vyznačenou operací „vybrat za archiválii“ nebo „zničit“ eSSL zaznamená Identifikátor skartačního řízení.
6.2.6	ESSL umožní posuzovateli skartační operace stanovit, které entity s vyznačenou operací „vybrat za archiválii“ budou určeny k přenosu. Toto rozhodnutí lze uskutečnit a) jednotlivě pro konkrétní entity, nebo b) hromadně pro všechny entity označené „vybrat za archiválii“.
6.2.7	ESSL zajistí, že pokud byl u spisu realizován požadavek 3.2.10, posuzovatel skartační operace může provést kontroly a související činnosti podle požadavku 3.2.9. *Tento požadavek umožní původci připravit skartační operaci v případě, že je mu příslušným archivem odebrán trvalý skartační souhlas.*
6.2.8	ESSL vyznačí identifikátory digitálního archivu zaslané příslušným archivem v podobě seznamu podle 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 i entity v analogové podobě.*

6.3 Přenos, export a import

Číslo	Požadavek
6.3.1	ESSL přenáší, exportuje nebo importuje repliky entit, jejich metadata a příslušné části transakčního protokolu prostřednictvím příslušného schématu XML v příloze č. 7.
6.3.2	ESSL zajistí, aby přenos, export nebo import replik entit byl správcovskou rolí prováděn i hromadně na základě zvolených věcných skupin, spisů, typových spisů nebo součástí typových spisů.
6.3.3	ESSL umožňuje, aby byla tatáž entita exportována více než jednou.
6.3.4	ESSL při přenosu nebo exportu dokumentu, spisu, typového spisu, součásti typového spisu, dílu typového spisu nebo obsahu věcné skupiny provádí následující operace:

Číslo	Požadavek
	a) přenos nebo export repliky obsahu stanovené věcné skupiny, spisu, dokumentu, typového spisu, součásti typového spisu nebo dílu typového spisu, včetně jejich metadat a příslušných částí transakčního protokolu, b) export všech replik hierarchicky nadřazených entit, včetně jejich metadat a příslušných částí transakčního protokolu, c) export replik spisů napojených nebo vložených do exportované nebo přenášené entity pevným křížovým odkazem, včetně jejich metadat a příslušných částí transakčního protokolu, d) přenos replik spisů napojených nebo vložených do exportované nebo přenášené entity pevným křížovým odkazem, včetně jejich metadat a příslušných částí transakčního protokolu, pokud jsou napojené nebo vložené spisy určeny k přenosu, e) ukončení přenosu podle požadavku 6.3.8.
6.3.5	ESSL při importu repliky dokumentu, spisu, typového spisu, součásti typového spisu, dílu typového spisu nebo obsahu věcné skupiny provádí následující operace: a) uživatelskou volbu věcných skupin, do kterých bude import realizován, b) uživatelskou volbu spisových znaků a názvů součástí typových spisů (přejmenování), pokud jsou odlišné od spisových znaků a názvů v cílovém systému, c) případný uživatelský výběr konkrétních replik spisů, typových spisů nebo součástí typových spisů, které mají být importovány, d) import replik entit a jejich metadat včetně pevných křížových odkazů mezi nimi, e) zaznamenání změněných nebo z technických důvodů neimportovaných replik metadat do transakčního protokolu.
6.3.6	ESSL umožní import vyřízených dokumentů zatříděných přímo ve věcné skupině tak, že tyto dokumenty mohou být opět zařazeny ve věcné skupině. *Dokumenty bylo možné zatřiďovat do věcné skupiny podle předchozí právní úpravy.*
6.3.7	Součástí metadat replik entit podle požadavků 6.3.4 a 6.3.5 jsou příslušné záznamy a) jmenného rejstříku, b) číselníku podle požadavku 2.7.3.
6.3.8	ESSL uchovává spisy, typové spisy, součásti typového spisu, díly typového spisu, dokumenty, komponenty a metadata, které jsou přenášeny, a to alespoň do doby potvrzení úspěšnosti ukončeného přenosu jejich replik. Do této doby eSSL umožní opakování přenosu. *U přenesených entit se i po ukončeném přenosu ve zdrojovém systému trvale uchovává hlavička metadat a příslušné části transakčního protokolu.*
6.3.9	ESSL zajistí správcovské roli import a export spisového plánu, věcných skupin a skartačních režimů podle přílohy č. 5.
6.3.10	Pokud eSSL provádí import podle požadavku 6.3.5, spisový znak importované věcné skupiny na základě volby uživatelské role a) zachová v jeho úplnosti,

Číslo	Požadavek
	b) umožní změnit.

7 SPRÁVA A BEZPEČNOST

7.1 Přístup

Číslo	Požadavek
7.1.1	ESSL neumožňuje uživateli provést jakoukoli operaci, nemá-li přidělenu roli s patřičným oprávněním. ESSL musí uživatele úspěšně identifikovat a ověřit.
7.1.2	ESSL umožňuje roli správu přístupových práv k entitám, ke kterým má tato role sama přiřazena přístupová práva.
7.1.3	ESSL umožňuje roli potvrdit, nebo odmítnout přiřazení přístupových práv k jakémukoliv dokumentu, spisu, typovému spisu nebo součásti typového spisu, které jí byly jinou rolí přiřazeny.
7.1.4	ESSL umožňuje roli, která přiřadila přístupová práva k dokumentu, spisu, typovému spisu nebo součásti typového spisu, aby přiřazení zrušila, pokud již nebylo potvrzeno přiřazení.
7.1.5	ESSL do okamžiku uzavření spisu umožní uživatelské roli podle přístupových oprávnění změnit metadata dokumentu a spisu zapsaná uživatelskou rolí. Po uzavření spisu eSSL umožní správcovské roli změnit metadata dokumentu a spisu zapsaná uživatelskou rolí. *Tato funkce umožňuje například spisovně provádět případné opravy chyb uživatelů (například chyby při vkládání dat, chybné zařazení ve věcných skupinách apod.).*
7.1.6	ESSL umožňuje správcovské roli využít konfiguraci oprávnění tak, aby byl konkrétní roli nebo uživateli před stanoveným datem, ke stanovenému datu nebo po stanoveném datu a) omezen přístup ke konkrétním typovým spisům, součástem typových spisů, spisům, dokumentům nebo komponentám, b) omezen přístup ke konkrétním věcným skupinám, c) omezen přístup k určitým vlastnostem a funkcím eSSL (například ke čtení, k aktualizaci nebo k mazání určitých prvků metadat), d) odmítnut přístup do eSSL.
7.1.7	ESSL umožňuje správcovské roli, aby a) přidělovala oprávnění roli a b) přiřadila jednoho nebo více uživatelů k jakékoli roli.
7.1.8	ESSL umožňuje správcovské roli definovat pro role přístupová práva stejně jako pro jednotlivé uživatele a přidělovat role jednotlivým uživatelům. *Tento požadavek umožňuje správcovským rolím spravovat a udržovat soubor přístupových práv spíše pro limitovaný počet rolí, než je udržovat pro velký počet jednotlivých uživatelů.*
7.1.9	ESSL umožňuje posuzovateli skartační operace přetřídění entity v rámci věcných skupin (požadavek 3.1.9), změnu metadat entity (požadavek 7.1.5), nahlížení do komponent entity, pokud je entita uložena ve spisovně.
7.1.10	ESSL umožňuje správu věcných skupin výlučně správcovské roli.

Číslo	Požadavek
7.1.11	ESSL umožňuje správcovské roli vyhledávání, zobrazení a změnu parametrů a nastavení eSSL, alespoň u a) číselníků (požadavky 2.7.3, 4.2.1), b) určeného časového období (požadavek 3.3.9), c) otevírání a uzavírání věcných skupin (kapitola 3.1), d) skartačních režimů (kapitola 6.1) a e) tvorbu šablon typových spisů (požadavek 3.3.6).

7.2 Změny, zničení a znepřístupnění dokumentů

Číslo	Požadavek
7.2.1	ESSL zabraňuje zničení komponenty, dokumentu, spisu, typového spisu, součásti typového spisu nebo dílu typového spisu nebo jejich metadat, s výjimkou zničení a) po dokončeném skartačním řízení, b) na základě uděleného trvalého skartačního souhlasu, c) po úspěšném dokončení přenosu, d) po evidenčním převedení do jiné evidenční pomůcky, e) znepřístupněných dokumentů a spisů, f) samostatné komponenty došlého kontejneru po uzavření spisu, pokud došlo k úspěšnému vyjmutí všech obsažených komponent podle požadavku 2.4.3. Při zničení musí být zachována hlavička metadat podle požadavku 7.2.9.
7.2.2	ESSL zabrání změně komponenty, která byla a) schválena, pokud nedojde k odvolání schválení příslušnou rolí, b) přijata, s výjimkou provádění požadavků 2.4.1 a 2.5.1.
7.2.3	ESSL umožní posuzovateli skartační operace zničení spisu nebo dokumentu na základě trvalého skartačního souhlasu.
7.2.4	Pokud eSSL provádí zničení spisu nebo dokumentu na základě trvalého skartačního souhlasu, eSSL zajistí, aby posuzovatel skartační operace vyznačil do metadat jednoznačný identifikátor nebo číslo jednací rozhodnutí o udělení trvalého skartačního souhlasu. ESSL zajistí, že o zničení lze na základě volby posuzovatele skartační operace vytvořit hlášení podle požadavku 7.3.8. *Požadavek slouží k zajištění průkaznosti oprávnění k uvedenému jednání a zajišťuje častý požadavek příslušného archivu na předkládání informačních hlášení, kterým archiv podmiňuje vydání trvalého skartačního souhlasu.*
7.2.5	ESSL zničí spisy, typové spisy, součásti typového spisu, díly typového spisu, dokumenty, metadata a ztvárnění příslušné části transakčního protokolu, které jsou přenášeny, jestliže obdrží potvrzení o úspěšném ukončení přenosu, a to s výjimkou metadat, která jsou uchovávána v hlavičkách metadat (požadavky 7.2.9 a 7.2.10).
7.2.6	ESSL zničí spisy, typové spisy, součásti typového spisu, díly typového spisu, dokumenty a metadata, které byly určeny ke zničení při skartačním řízení (požadavek

Číslo	Požadavek
	6.2.5 písm. b), a to s výjimkou metadat, která jsou uchovávána v hlavičkách metadat (požadavky 7.2.9 a 7.2.10).
7.2.7	Pokud je v eSSL uplatněna výjimka podle požadavku 7.2.1, eSSL postupuje tak, že dokument zničí spolu s příslušnými metadaty, kromě metadat specifikovaných jako hlavička metadat (požadavek 7.2.9).
7.2.8	ESSL v případě zničení dokumentu nebo spisu automaticky z metadat odstraní vazbu na dokument nebo spis ze všech záznamů ve jmenném rejstříku.
7.2.9	ESSL uchovává hlavičku metadat podle přílohy č. 8, popisující a) typové spisy, b) součásti typových spisů, c) díly typových spisů, d) spisy, e) dokumenty, které byly zničeny nebo přeneseny.
7.2.10	ESSL umožňuje správcovské roli stanovit další metadata, která budou uchována jako hlavička metadat.
7.2.11	ESSL nabízí konfigurační možnost dokumenty a spisy znepřístupnit.
7.2.12	ESSL umožní znepřístupnění dokumentu nebo spisu a) uživateli, který dokument vytvořil a nepředal držení tohoto dokumentu jinému uživateli, nebo v případě, že se jedná o dokument vzniklý podle požadavku 2.1.7, b) správcovské roli v případě dokumentů nezařazených do spisů nebo spisů, které neobsahují dokumenty. ESSL přitom vyžaduje, aby uživatelská nebo správcovská role vyznačila důvod znepřístupnění.
7.2.13	ESSL zajistí, aby se znepřístupněné dokumenty a spisy při znázorňování a vyhledávání jevily jako zničené každé roli s výjimkou posuzovatele skartační operace.
7.2.14	ESSL nedovolí uživatelské nebo správcovské roli provést znepřístupnění dokumentů nebo spisů jako hromadnou operaci.
7.2.15	ESSL zajistí, aby posuzovatel skartační operace mohl znepřístupněné dokumenty nebo spisy – vyjma již zničených – uvést do původního stavu (zpřístupnit).
7.2.16	ESSL umožní posuzovateli skartační operace zničit znepřístupněné dokumenty za stanovené období s výjimkou hlaviček metadat, případně eSSL zajistí automatické zničení znepřístupněných dokumentů po uplynutí lhůty nastavené správcovskou rolí.

7.3 Hlášení o stavu eSSL

Číslo	Požadavek
7.3.1	ESSL poskytuje znázornění stavových hlášení o své správě, stejně jako statistických a jednorázových informací (dále „zprávy“), jejichž prostřednictvím správcovské role

Číslo	Požadavek
	sledují činnost a stav eSSL. Toto je požadováno v celém eSSL a vztahuje se alespoň k a) věcným skupinám, b) spisům, typovým spisům a dokumentům, c) aktivitě uživatelů, d) přístupovým a bezpečnostním oprávněním a e) výběru archiválií (skartačnímu řízení).
7.3.2	ESSL zahrnuje funkce ztvárnění zpráv a jejich vytištění nebo uložení v digitální podobě (například pro zpracování tabulkovým procesorem).
7.3.3	ESSL poskytuje zprávy o celkovém počtu alespoň a) spisů, typových spisů, součástí typových spisů a dílů typových spisů, b) komponent tříděných podle datového formátu, c) dokumentů a spisů v držení uživatele, d) spisů, typových spisů, součástí a dílů tříděných podle přístupových oprávnění, e) spisů, typových spisů, součástí typových spisů a dílů typových spisů obsahujících dokumenty v digitální podobě, tříděných podle souhrnné velikosti všech komponent.
7.3.4	ESSL poskytuje zprávy o fyzickém umístění analogových částí spisů, typových spisů, součástí typových spisů a dílů typových spisů tříděných podle místa uložení.
7.3.5	ESSL poskytuje zprávy alespoň o a) množství přijatých dokumentů, b) množství nově vytvořených věcných skupin a spisů, c) četnosti použití spisových znaků u dokumentů a spisů.
7.3.6	ESSL poskytuje zprávu o výsledcích procesů importu, výběru archiválií, přenosu, exportu, zničení s uvedením věcných skupin, typových spisů, součástí typových spisů, dílů typových spisů, spisů a dokumentů, které byly úspěšně importovány, zničeny, znepřístupněny, přeneseny nebo exportovány, s uvedením případných chyb, které v průběhu procesů nastaly. Popis chyby identifikuje dokumenty, věcné skupiny, typové spisy, součásti typového spisu, díly typového spisu, spisy a dokumenty a s nimi spojená metadata, které nebyly úspěšně importovány, přeneseny, exportovány, zničeny.
7.3.7	ESSL na vyžádání posuzovatele skartační operace poskytuje zprávu, která pro zadané období obsahuje údaje o provedeném znepřístupnění entit podle požadavku 7.2.12 v rozsahu: a) jednoznačný identifikátor znepřístupněného dokumentu a spisová značka spisu, pokud byl dokument do spisu zařazen, b) spisová značka znepřístupněného spisu, c) věc znepřístupněného dokumentu a spisu, d) identifikace uživatele, který dokument znepřístupnil, e) důvod znepřístupnění.

Číslo	Požadavek
7.3.8	ESSL na vyžádání posuzovatele skartační operace poskytuje zprávu, která pro zadané období obsahuje údaje o provedeném zničení entit podle požadavku 7.2.1 písm. a) až d) v rozsahu: a) identifikace posuzovatele skartační operace, b) identifikace vydaného trvalého skartačního souhlasu, c) datum a čas provedení operace zničení, d) počet zničených dokumentů a spisů v rámci dílu typového spisu nebo určeného časového období věcné skupiny, ve které došlo ke zničení entit.
7.3.9	ESSL poskytuje zprávy o množství dokumentů, spisů a dílů typových spisů za stanovené období, kterým ke stanovenému datu uplynula skartační lhůta.

7.4 Transakční protokol

Číslo	Požadavek
7.4.1	ESSL vede po celou dobu provozu transakční protokol a nepřipustí změnu nebo zničení údajů v něm. ESSL na vyžádání správcovské role ztvární úplný obsah transakčního protokolu do XML za zadané časové období. XML schéma transakčního protokolu je popsané v příloze č. 6. *ESSL v případě technických omezení rozdělí ztvárnění transakčního protokolu do více samostatných komponent, přičemž jejich obsahy na sebe musí plynule navazovat. Ztvárnění transakčního protokolu za celou dobu provozu eSSL provádí správcovská role minimálně při ukončení provozu eSSL. Původce nabídne ztvárnění transakčního protokolu místně příslušnému archivu.*
7.4.2	ESSL zapisuje do transakčního protokolu alespoň údaje o přístupu k entitě, pokusu o přístup k entitě, každé změně stavu nebo manipulaci s entitami, změně metadat entity (zaznamená nový stav), včetně uživatelských záznamů a pokynů pro schvalování a oběh entity.
7.4.3	ESSL zapisuje do transakčního protokolu alespoň údaje o vlastních změnách, změnách své konfigurace, nastavení a o změnách uživatelských oprávnění. *Tento požadavek umožňuje jednoznačně identifikovat verzi eSSL a čas jejího nasazení do produkčního provozu, změny konfigurace a nastavení eSSL.*
7.4.4	ESSL zapisuje do transakčního protokolu veškeré automaticky prováděné operace.
7.4.5	ESSL zapisuje do transakčního protokolu veškeré operace se záznamy ve jmenném rejstříku, zejména jejich vytváření, úpravy, zničení a nahlížení na záznamy.
7.4.6	ESSL zapisuje do transakčního protokolu důvod úpravy nebo znepřístupnění skartačního režimu správcovskou rolí podle požadavku 6.1.2.
7.4.7	Pokud posuzovatel skartační operace zavede, nebo odstraní pozastavení skartační operace, eSSL zapisuje do transakčního protokolu a) datum, kdy bylo pozastavení zavedeno, nebo odstraněno, b) identifikaci oprávněného uživatele, c) důvod pozastavení, nebo důvod odstranění pozastavení.

Číslo	Požadavek
7.4.8	ESSL zapisuje změnu spisového znaku věcné skupiny do transakčního protokolu pokud provádí import podle požadavku 6.3.5 a dojde k jeho změně podle požadavku 6.3.10.
7.4.9	ESSL zapisuje do transakčního protokolu údaje o zničení (fyzickém vymazání) dokumentu podle požadavku 7.2.7.
7.4.10	ESSL zajistí, že každý záznam v transakčním protokolu obsahuje údaj o uživateli, který změnu stavu nebo manipulaci provedl, a o času provedení změny nebo manipulace.
7.4.11	ESSL zapisuje do transakčního protokolu údaje o každém přihlášení, nebo odhlášení uživatele bez ohledu na to, zda bylo úspěšné. *Myslí se tím, že v transakčním protokolu jsou údaje též o neúspěšných pokusech, například řetězec znaků zadaný uživatelem do přihlašovacích políček při pokusu o přihlášení.*
7.4.12	ESSL zajišťuje dostupnost transakčního protokolu tak, aby byl na výzvu správcovské role znázorněn a ztvárněn.
7.4.13	ESSL při každé změně komponenty zapisuje do transakčního protokolu její hash a název použité hashovací funkce.

8 ROZHRANÍ PRO PROPOJENÍ INFORMAČNÍCH SYSTÉMŮ SPRAVUJÍCÍCH DOKUMENTY

8.1 Vazby mezi informačními systémy spravujícími dokumenty

Číslo	Požadavek
8.1.1	Rozhraní umožňuje synchronní i asynchronní komunikaci mezi informačními systémy spravujícími dokumenty původce, přičemž toto rozhraní je realizováno prostřednictvím webových služeb a schémat XSD uvedených v příloze č. 1.
8.1.2	Každý informační systém spravující dokumenty (včetně eSSL) má pro účely komunikace původcem přidělen jednoznačný identifikátor, který je používán pro označení zdroje a cíle komunikace.
8.1.3	Informační systém spravující dokumenty umožňuje, aby identifikace podle požadavku 8.1.2 mohla být rozšířena o zajišťovací prvky, které mohou být volitelně použity při zabezpečení dávek XML.
8.1.4	Rozhraní mezi informačními systémy spravujícími dokumenty je založeno na nedělitelných událostech podle požadavků 8.1.8 a 8.1.10 a pracuje s entitami a jejich metadaty. Každá událost je označena identifikátorem; identifikátor události je jednoznačný v rámci daného systému a jeho součástí je jednoznačný identifikátor systému podle požadavku 8.1.2.
8.1.5	Při synchronní komunikaci volaná strana okamžitě vykoná požadovanou událost. Výsledek události je vrácen volající straně jako výsledek volání webové služby.
8.1.6	V rámci jednoho volání synchronní webové služby podle požadavku 8.1.8 musí být jednotlivá 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.
8.1.7	Při opakovaném příjmu identické události (události s identickým jednoznačným identifikátorem), která již byla jednou úspěšně provedena, musí volaná strana vrátit vždy stejný výsledek. Takové opakování se nesmí považovat za chybu. V případě, že je obsahem události vytvoření nové instance entity (například DokumentZalozeni, SpisZalozeni, DokumentPostoupeniZadost, SpisPostoupeniZadost, OsobaZalozeni), volaná strana událost podruhé nezpracuje, ale pouze volajícímu vrátí stejnou výslednou informaci jako při prvním úspěšném zpracování události.
8.1.8	Rozhraní eSSL poskytuje alespoň následující funkce: a) **SpisZalozeni** – založení spisu nad dokumentem. Je možné založit celý spis i s dokumenty v něm, nebo je spis založen nad existujícím dokumentem. b) **DokumentZalozeni** – zaevidování nového dokumentu přijatého nebo vzniklého v informačním systému spravujícím dokumenty. Nepřenáší kompletní profil dokumentu, ale jen údaje, které dávají smysl při založení popsané typem tProfilDokumentuZalozeni. c) **DokumentPostoupeniZadost** – žádost o postoupení dokumentu (převzetí dokumentu do výhradní správy volajícím systémem). d) **SpisPostoupeniZadost** – žádost o postoupení spisu (převzetí spisu do výhradní správy volajícím systémem). e) **SpisVraceniZadost** – žádost o vrácení spisu do výhradní správy.

Číslo	Požadavek
	f) **ProfilDokumentuZadost** – žádost o poskytnutí detailních informací o dokumentu. g) **DokumentVraceniZadost** – žádost o vrácení dokumentu do výhradní správy. h) **ProfilSpisuZadost** – žádost o poskytnutí detailních informací o spisu. i) **ProfilTypovehoSpisuZadost** – žádost o poskytnutí detailních informací o typovém spisu. j) **TypovySpisZalozeni** – služba pro založení typového spisu. k) **SouborZadost** – žádost o poskytnutí obsahu zadané komponenty (pojem „soubor“ v kontextu popisu rozhraní je identický s pojmem „komponenta“). l) **CiselnikZadost** – žádost o poskytnutí číselníku. Kód (název) číselníku zpravidla odpovídá názvu elementu, k němuž se číselník vztahuje. Pro určení číselníku se používá element IdCiselniku a ne Kod. Položky číselníku mohou přenášet větší množství nepovinných položek podle potřeby. m) **CiselnikySeznam** - služba vrací seznam všech dostupných číselníků. n) **DavkySeznam** – služba umožní volajícímu systému získat seznam dávek, které jsou ve volaném systému pro daný volající systém připraveny. o) **DavkaZadost** – služba umožní volajícímu systému získat z volaného systému dávku. p) **Udalosti** – žádost o okamžité vykonání předaného pole událostí. q) **WsTest** – funkce pro otestování komunikace. Pouze informuje o aktuální dostupnosti volaného systému. r) **PrideleneSeznam** – funkce pro zaslání seznamu všech entit konkrétního uživatele v daném systému. Funkce umožňuje filtrování podle identifikátoru, druhu entity, data vytvoření a data poslední změny. s) **ProfilOsobyZadost** – žádost o poskytnutí detailních informací o osobě ve jmenném rejstříku. t) **OsobaUprava** – žádost o úpravu dat osoby ve jmenném rejstříku. u) **OsobySeznam** – služba pro vyhledání osoby ve jmenném rejstříku. v) **OsobaZalozeni** – založení osoby ve jmenném rejstříku. w) **ermsAsyn** – přenos dávek obsahujících události a zprávy podle požadavku 8.1.9.
8.1.9	Rozhraní v rámci asynchronní komunikace sdružuje události do dávek. Součástí dávek jsou též zprávy o zpracování přijatých událostí. Dávka může obsahovat a) události, b) zprávy, nebo c) události a zprávy.
8.1.10	Rozhraní podporuje příjem alespoň následujících událostí: a) **DokumentZalozeni –** založení nového dokumentu. b) **DokumentUprava** – úprava metadat existujícího dokumentu. c) **DokumentZruseni** – stornování existujícího dokumentu.

Číslo	Požadavek
	d) **DokumentOtevreni** – otevření dříve vyřízeného dokumentu. e) **DokumentVyrizeni** – označení dokumentu za vyřízený. Podle konfigurace jiného informačního systému spravujícího dokumenty, resp. eSSL může být vyřízení dokumentu spojeno také s jeho uzavřením. f) **DokumentPostoupeni** – předání dokumentu do výhradní správy jiného informačního systému spravujícího dokumenty, resp. eSSL (uplatní se vždy, když je předávána výhradní správa, tj. jak při předání z eSSL na informační systém spravující dokumenty, tak při předání z informačního systému spravujícího dokumenty na eSSL nebo mezi dvěma informačními systémy spravující dokumenty. g) **DokumentVraceni** – vrácení zpracování dokumentu do eSSL. Reverzní událost k DokumentPostoupeni. h) **DokumentVlozeniDoSpisu** – vložení dokumentu do spisu. Spis nesmí být uzavřen. i) **DokumentVyjmutiZeSpisu** – vyjmutí dokumentu ze spisu. Dokument a spis musí existovat, spis nesmí být uzavřen. j) **DokumentZmenaZpracovatele** – předání dokumentu jinému zpracovateli. Při předání mezi uživateli je v elementu „Autorizace“ původní zpracovatel, element „Prebirajici“ obsahuje údaje o novém zpracovateli. Při administrativním přidělení je administrátor v elementu „Autorizace“ a v elementu „Prebirajici“ je nový zpracovatel dokumentu. Pokud k události došlo jindy než v okamžiku zaevidování, je možno do elementu „predanoKdy“ uvést skutečné datum události. k) **DokumentExterniSpousteciUdalost** – předání informace, že nastala událost, kterou je podmíněn začátek běhu skartační lhůty. l) **DokumentSkartacniNavrh** – informace o zařazení dokumentu do skartačního návrhu s možností vynuceného vyjmutí ze skartačního návrhu v odpovědi na volání události. m) **DokumentSkartovano** – předání informace, že nad dokumentem proběhlo skartační řízení. n) **SpisZalozeni** – založení spisu. Nepřenáší kompletní profil spisu, ale jen údaje, které dávají smysl při založení popsané typem tProfilSpisuZalozeni. o) **SpisUprava** – úprava metadat existujícího spisu. p) **SpisPostoupeni** – předání spisu do výhradní správy jiného informačního systému spravujícího dokumenty, respektive eSSL. q) **SpisVraceni** – vrácení zpracování spisu do eSSL. Reverzní událost ke SpisPostoupeni r) **SpisOtevreni** – otevření dříve uzavřeného spisu. s) **SpisUzavreni** – uzavření vyřízeného spisu. t) **SpisZruseni** – stornování spisu včetně všech vložených dokumentů. u) **SpisVyrizeni** – vyřízení spisu včetně všech vložených dokumentů. Podle konfigurace eSSL může být vyřízení spisu spojeno také s jeho uzavřením.

Číslo	Požadavek
	v) **SpisZmenaZpracovatele** – předání spisu a všech vložených dokumentů jinému zpracovateli. Při předání mezi uživateli je v elementu „Autorizace“ původní zpracovatel, element „Prebirajici“ obsahuje údaje o novém zpracovateli. Při administrativním přidělení je administrátor v elementu „Autorizace“ a v elementu „Prebirajici“ je nový zpracovatel spisu. Pokud k události došlo jindy než v okamžiku zaevidování, je možno do elementu „predanoKdy“ uvést skutečné datum události. w) **SpisExterniSpousteciUdalost** – předání informace, že nastala událost, kterou je podmíněn začátek běhu skartační lhůty. x) **SpisSkartacniNavrh** – informace o zařazení spisu do skartačního návrhu s možností vynuceného vyjmutí ze skartačního návrhu v odpovědi na volání události. y) **SpisSkartovano** – předání informace, že nad spisem proběhlo skartační řízení. z) **SpisVlozeniDoTypovehoSpisu** – vložení spisu do součásti typového spisu (otevřeného dílu součásti). Součást nesmí být uzavřena. aa) **SpisVyjmutiZTypovehoSpisu** – vyjmutí spisu ze součásti typového spisu. Spis a součást typového spisu musí existovat. Díl typového spisu nesmí být uzavřen. bb) **DoruceniUprava** – změna metadat dokumentu týkajících se informací o přijetí původcem. cc) **VypraveniZalozeni** – vytvoření zásilky pro odeslání dokumentu. Stav nové zásilky je „nevypraveno“. dd) **VypraveniUprava** – úprava metadat zásilky. ee) **VypraveniVypraveno** – předání informace, že zásilka byla vypravena. ff) **VypraveniDoruceno** – zápis informací o doručení k zásilce. gg) **VypraveniZruseni** – stornování zásilky. hh) **VypraveniPredatVypravne** – pokyn k předání zásilky do výpravny k vypravení. ii) **SouborZalozeni** – založení komponenty. Událost je potřeba použít před použitím komponenty v dalších událostech, například DokumentPostoupeni. V události může být předán elektronický obsah přímo nebo pouze odkaz (identifikátor) na soubor a v takovém případě zdrojová evidence dokumentů poskytuje cílové evidenci dokumentů 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“. jj) **SouborNovaVerze** – nahrazení stávající komponenty novou. kk) **SouborZruseni** – odstranění komponenty. ll) **SouborVlozitKDokumentu** – přiložení existující komponenty k dokumentu. mm) **SouborVyjmoutZDokumentu** – odstranění komponenty z dokumentu. Komponenta nesmí být u tohoto dokumentu součástí zásilky, která je předána k vypravení. nn) **SouborVlozitKVypraveni** – určení komponenty, že bude součástí zásilky.

Číslo	Požadavek
	oo) **SouborVyjmoutZVypraveni** – určení komponenty, že nebude dále součástí zásilky. pp) **SouborOdemkniFinal** – událost zruší příznak konečného tvaru komponenty. qq) **OdkazVytvoreni** – vytvoření nebo úprava pevného nebo volného křížového odkazu. rr) **OdkazZruseni** – odstranění pevného nebo volného křížového odkazu. ss) **UzivateleSeznam** – vrací seznam uživatelů systému. tt) **FunkcniMista** – vrací funkční místa jednoho uživatele systému.
8.1.11	V případě zpracování událostí v dávkách při asynchronní komunikaci jsou transakce realizovány na úrovni událostí, nikoliv dávek. Jedná se o rozdíl oproti synchronní komunikaci podle požadavku 8.1.6.
8.1.12	Po odeslání jedné dávky při asynchronní komunikaci 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.
8.1.13	Číslování dávek je unikátní jen pro každou komunikaci přes rozhraní eSSL. Dávky jsou číslovány vzestupnou řadou s přírůstkem 1 (jedna). Pořadová čísla dávek na sebe musí navazovat v nepřerušené, spojité řadě.
8.1.14	Pořadí dávek musí odpovídat pořadí dávek podle položky DatumVzniku uvedené v hlavičce každé dávky.
8.1.15	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 být unikátní pro různé dávky. Počáteční hodnota, přírůstek ani spojitost číselné řady nejsou pro číslování událostí vyžadovány.
8.1.16	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.
8.1.17	Každá dávka musí ve své hlavičce obsahovat identifikaci zdroje a cíle dávky.
8.1.18	Události jsou zpracovávány důsledně v pořadí, ve kterém jsou zapsány v dávce. Toto pořadí (umístění v dávce) musí odpovídat pořadí číselného označení událostí podle požadavku 8.1.15.
8.1.19	Událost musí být zpracována zcela, nebo nesmí být zpracována vůbec. Není přípustné částečné, neúplné zpracování jedné události. Jedná se o obdobu požadavku 8.1.6 pro asynchronní komunikaci.
8.1.20	Událost lze považovat za úspěšně odeslanou a zpracovanou příjemcem pouze v případě, že je zpracování potvrzeno v některé z následujících přijatých dávek.
8.1.21	Dávku lze považovat za zpracovanou pouze v případě, že všechny v ní obsažené události byly protistranou potvrzeny jako úspěšně zpracované.

Číslo	Požadavek
8.1.22	Při potvrzení událostí je povoleno použít následující zjednodušení: Pokud je potvrzeno úspěšné zpracování poslední události v dávce, potom jsou tímto potvrzena úspěšná zpracování všech událostí této dávky.
8.1.23	Komunikace podle požadavku 8.1.1 probíhá prostřednictvím protokolu https. Jako vyšší stupeň zabezpečení může https server při komunikaci vyžadovat autentizaci klienta klientským certifikátem.
8.1.24	ESSL umožňuje zabezpečení integrity dat přenášených XML dávek elektronickou pečetí ve standardu podle platných právních předpisů. Použití nebo nepoužití tohoto zabezpečení závisí na konkrétní vazbě a eSSL musí umožňovat toto nastavení samostatně pro každou vazbu na jiný informační systém spravující dokumenty. Vztah mezi 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 informačním systémem spravujícím dokumenty.
8.1.25	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 8.1.27.
8.1.26	Systém s aktuálně nevýhradní správou může požádat voláním synchronní metody rozhraní o postoupení spisu a/nebo dokumentu z výhradní správy druhého systému do své výhradní správy. Této žádosti o postoupení výhradní správy spisu a/nebo 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.
8.1.27	ESSL musí obsahovat správcovskou funkci, která zruší příznak výhradní správy entity informačním systémem spravujícím dokumenty (zejména v případě nefunkčnosti tohoto systému). U každé této servisní operace je třeba evidovat důvod a zaznamenat jej spolu s ostatními metadaty operace do transakčního protokolu.
8.1.28	V rámci konfigurace vazby mezi eSSL a informačním systémem spravujícím dokumenty 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 alespoň o následující metadata: 1) uživatel („provedlKdo“, „novyZpracovatel“, „VlastniKdo“), 2) spisový a skartační plán („SpisovyPlan“), 3) spisový znak („SpisovyZnak“), 4) druh dokumentu („DruhDokumentu“), 5) podací deník („PodaciDenik“), 6) způsob vyřízení spisu nebo dokumentu („ZpusobVyrizeni“), 7) skartační režim, 8) spouštěcí událost.

Číslo	Požadavek
8.1.29	ESSL umožní pomocí rozhraní postoupit entitu ke zpracování informačnímu systému spravujícímu dokumenty na žádost uživatele podanou prostřednictvím informačního systému spravujícího dokumenty. Uživatel informačního systému spravujícího dokumenty si může vyžádat seznam přidělených dokumentů, spisů a součástí typových spisů prostřednictvím informačního systému spravujícího dokumenty bez toho, že by musel pracovat s eSSL.
8.1.30	Identifikátor entity přiděluje vždy ten informační systém spravující dokumenty, který entitu zaeviduje jako první. Ostatní systémy musí identifikátor převzít.
8.1.31	Označení zdroje identifikátoru podle požadavku 8.1.30 je shodné s identifikací podle požadavku 8.1.2 a musí být v rámci původce unikátní.
8.1.32	V případech, kdy je nutné mezi eSSL a informačním systémem spravujícím dokumenty vyměňovat, popřípadě modifikovat metadata nad rámec specifikace jednotlivých funkcí (požadavek 8.1.8) nebo událostí (požadavky 8.1.10 a 8.1.11), 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 informačním systémem spravujícím dokumenty.

9 METADATA

9.1 Obecné požadavky na metadata

Číslo	Požadavek
9.1.1	ESSL umožňuje správcovské roli stanovit další metadata entit nad rámec přílohy č. 8 a definovat, který prvek metadat je povinný a který volitelný.
9.1.2	ESSL podporuje alespoň následující formáty prvků metadat: a) alfabetické, b) alfanumerické, c) numerické, d) časové, e) logické („ANO/NE“).
9.1.3	ESSL umožňuje správcovské roli stanovit, které hodnoty prvků metadat mají být zapsány a udržovány ručně a které výběrem z číselníku.

9.2 Požadavky na metadata datových balíčků SIP

Číslo	Požadavek
9.2.1	ESSL zajistí vytvoření datového balíčku SIP přílohy č. 2 skládajícího se z adresáře (složky) a) pro provedení skartačního řízení (výběr archiválií), b) pro předání dokumentů do archivu. *Datový balíček SIP (`LABEL="Datový balíček pro předávání dokumentů a jejich metadat do archivu"`) vytvořený podle písm. b) může být použit i pro provedení skartačního řízení (pro výběr archiválií).*
9.2.2	ESSL zajistí, že datový balíček SIP je tvořen a) právě jedním dílem typového spisu, a to případně včetně entit, které k němu byly podle předchozí právní úpravy připojeny pevnými křížovými odkazy, b) právě jedním spisem, c) spisy, pokud jsou navzájem propojeny pevnými křížovými odkazy, d) právě jedním samostatným dokumentem, pokud byl podle předchozí právní úpravy zatříděn přímo do věcné skupiny. *Písmeno d) se použije obdobně i na dokumenty samostatné evidence dokumentů, která sama nevytváří spisy.*
9.2.3	ESSL zajistí, že datový balíček SIP obsahuje veškerá metadata a komponenty vložených entit.
9.2.4	ESSL zajistí, že součástí datového balíčku SIP jsou příslušné části transakčního protokolu ve formátu XML, které se týkají vložených entit.
9.2.5	ESSL zajistí, že adresář (složka) obsahuje soubor XML a případně adresář pro uložení dalších komponent. Do adresáře pro uložení dalších souborů, pokud je vytvářen, se vždy vkládají alespoň všechny verze komponenty, které již jsou ve výstupním datovém formátu.

Číslo	Požadavek
9.2.6	ESSL zajistí, že soubor XML je pojmenován „mets.xml“. *Příklad:* *jednoznacny_nazev_sip [dir]* *|-mets.xml*
9.2.7	ESSL zajistí, že každý soubor XML popisuje právě jeden datový balíček SIP. Není možné v jednom souboru XML popisovat více datových balíčků SIP.
9.2.8	ESSL zajistí, že základní logická struktura souboru XML podle přílohy č. 2 odpovídá předepsanému schématu XML METS 1.12. Obsah souboru XML je dále specifikován podmínkami použití prvků schématu XML METS podle přílohy č. 2, část 2. Tyto podmínky jsou závazné pro určení správnosti datového balíčku SIP.
9.2.9	ESSL zajistí, že znakovou sadou souboru XML je Unicode/UCS v kódování UTF 8 bez BOM (Byte order mark).
9.2.10	ESSL zajistí, že komponenty se ukládají do adresáře (složky) s názvem „komponenty“. *Příklad:* *jednoznacny_nazev_sip [dir]* *|-komponenty [dir]* *|-nazev_souboru_pdfA.pdf* *|-mets.xml*
9.2.11	ESSL zajistí, že datový balíček SIP je komprimován do souboru v datovém formátu ZIP. ESSL zajistí, že soubor ZIP je pojmenován stejným způsobem jako adresář (složka) datového balíčku SIP. *Příklad:* *jednoznacny_nazev_sip.zip* *|- jednoznacny_nazev_sip [dir]* *|-komponenty [dir]* *|-nazev_souboru_pdfA.pdf* *|-mets.xml*
9.2.12	ESSL zajistí, že název datového balíčku SIP je v rámci eSSL jedinečný, přičemž obsahuje pouze písmena latinské abecedy bez diakritiky, čísla a znaky „_“ (podtržítko) a „–“ (pomlčka) a jeho délka nepřekročí 64 znaků.
9.2.13	ESSL zajistí, že v případě použití datového balíčku SIP pro předávání dokumentů a jejich metadat do příslušného archivu se hodnoty metadat neliší od metadat použitých v datovém balíčku SIP pro provedení skartačního řízení, s výjimkou informací o ukládacích jednotkách, množství, komponentách a skartačním řízení. Datový balíček SIP pro předávání dokumentů a jejich metadat do příslušného archivu musí vždy obsahovat alespoň komponenty, které byly do výběru navrženy a které byly vybrány za archiválie. Datový balíček SIP může obsahovat komponenty navíc, například jinou verzi komponenty, komponentu s novým pořadovým číslem apod.

Číslo	Požadavek
	Datové formáty všech komponent předávaných k trvalému uložení do příslušného archivu se řídí Formátovými pravidly Národního archivu. Aktuální Formátová pravidla Národního archivu jsou dostupná na https://portal.nacr.cz/cro/uvodni-stranka/formatova-pravidla-narodniho-archivu/

9.3 Přílohy

Číslo	Název	Poznámka
1	Schéma XML pro výměnu dokumentů a jejich metadat (WS API)	Schéma je určeno pro výměnu dokumentů a jejich metadat mezi informačními systémy spravujícími dokumenty a eSSL, přičemž se použije také pro export, import a přenos dokumentů. V tom případě se využijí pouze datové prvky definované ve schématu.
2	Schéma XML pro vytvoření datového balíčku SIP a pro zaznamenání popisných metadat uvnitř datového balíčku SIP	Příloha vznikla sloučením původních příloh č. 2 a 3. V příloze je odkazováno na standard METS.
3	Struktura popisných metadat pro automatizované zpracování dokumentu	Příloha naplňuje požadavky 2.4.3, 2.4.5 a 2.8.5.
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 ztvárnění transakčního protokolu	Schéma je určeno pro ztvárnění obsahu transakčního protokolu nebo příslušné části transakčního protokolu.
7	Schéma XML pro migraci dat mezi elektronickými systémy spisové služby	Schéma je určeno pro migraci dat mezi elektronickými systémy spisové služby, migraci dat při spisové rozluce nebo migraci dat ze starého do nového systému (exit plán). Příloha naplňuje požadavky 2.1.4, 2.7.3, 6.3.1, 6.3.4, 6.3.5 a 6.3.6.
8	Metadata entit	Popis metadat jednotlivých entit a metadat tvořících hlavičku metadat.

10 DOKUMENTACE ŽIVOTNÍHO CYKLU

10.1 Dokumentace informačního systému spravujícího dokumenty

Číslo	Požadavek
10.1.1	Dokumentace informačního systému spravujícího dokumenty vedená původcem obsahuje alespoň tyto údaje: a) název a verze informačního systému spravujícího dokumenty jako obchodního produktu (pokud je informační systém spravující dokumenty tvořen více obchodními produkty, pak musí být uvedeny všechny názvy obchodních produktů a jejich verzí), b) obchodní firma dodavatele informačního systému spravujícího dokumenty, c) datum uvedení informačního systému spravujícího dokumenty do zkušebního provozu, d) datum uvedení informačního systému spravujícího dokumenty do řádného provozu, e) datum získání atestu eSSL a verze eSSL pro kterou atest platí, f) početní nebo kapacitní omezení uváděná dodavatelem, alespoň tato: - nejvyšší možný počet dokumentů, které je možné uložit a zpracovat v celém systému za stanovené časové období podle požadavku 2.7.2, - nejvyšší možný počet dokumentů, které je možné vložit do jednoho spisu vedeného v systému, - nejvyšší možný počet spisů, který je možné založit a zpracovat v celém systému za stanovené časové období podle požadavků 2.7.2 a 3.3.9, - maximálně možná datová velikost komponenty, - nejvyšší možný počet uživatelů, - nejvyšší možný počet uživatelských a správcovských rolí, - nejvyšší možný počet věcných skupin a jejich úrovní hierarchie, které je možné založit a zpracovat v celém systému, - nejvyšší možný počet skartačních režimů, které je možné založit a zpracovávat v celém systému. g) informace, zda byla do informačního systému spravujícího dokumenty migrována data z předcházejícího systému, a charakteristika těchto dat (zejména v jakém časovém rozmezí byla v dřívějším systému pořizována), h) informace, zda je informační systém spravující dokumenty pouze evidencí, nebo spravuje komponenty, i) odkaz na jiný informační systém spravující dokumenty, pokud je informační systém spravující dokumenty s ním propojen, a informace, zda se tak děje prostřednictvím rozhraní podle kapitoly 8.1, j) informace o významných změnách informačního systému spravujícího dokumenty (například informace o změnách datové struktury a migracích eSSL na jeho nové verze), k) datum ukončení provozu informačního systému spravujícího dokumenty,

	l) technická charakteristika informačního systému spravujícího dokumenty, zejména použité technologie a databáze, m) věcná charakteristika informačního systému spravujícího dokumenty, zejména určení části agendy původce, na niž se vztahuje (rozsah zpracovávaných dat), n) přehled právních předpisů vztahujících se k obsahu informačního systému spravujícího dokumenty, pokud se nejedná o eSSL, o) údaje o poskytování otevřených dat nebo přístupu externích subjektů do informačního systému spravujícího dokumenty, p) přehled správcovských rolí a správců informačního systému spravujícího dokumenty a jejich zařazení v organizační struktuře původce, q) přehled uživatelských rolí a jejich charakteristika.
10.1.2	Dokumentace informačního systému spravujícího dokumenty vedená původcem musí být uložena v takové podobě, která zajistí její dostupnost a čitelnost lidskými smysly i v případě havárie informačního systému spravujícího dokumenty. *Požadavek neznamená, že předepsaná dokumentace musí být pouze v listinné podobě. Dokumentace může být i v elektronické podobě, ale musí být uložena mimo informační systém spravující dokumenty, kterého se týká.*
10.1.3	ESSL vede po celou dobu provozu detailní popis umožňující původci identifikovat a) verzi atestované eSSL (případně všech jejích částí), b) aktuálně provozovanou verzi eSSL nasazenou v produkčním prostředí, c) popis a rozsah změn provozované eSSL oproti atestované verzi, d) jaké patche byly aplikovány a e) zda byla s novou verzí změněna funkčnost eSSL, s uvedením důvodů a důsledků těchto změn pro původce.