Business analýza pro řešení Distribuce dokumentů

Březen 2023

Bezpečnostní kategorie: Veřejné

Obsah

Seznam zkratek

AD	Active Directory – adresářové služby LDAP od firmy Microsoft
AAD	Azure Active Directory – cloudové adresářové služby LDAP poskytované firmou Microsoft
ČJ	Číslo jednací
DAST	Dynamic Application Security Testing – testovací procedura, při které se simulují akce útočníka snažícího se proniknout do aplikace.
DD	Distribuce dokumentů
ERMS	Označení spisové služby provozované v prostředí Správy železnic
eSSL	Označení elektronické spisové služby dle NSESSS
FW	Firewall – síťový bezpečnostní prvek
IDM	Identity Management – Správa identit
IDS	Intrusion Detection System – Systém pro odhalení průniku
IPS	Intrusion Prevention System – Systém prevence průniku
ISSD	Informační systém spravující dokumenty
KB	Kybernetická bezpečnost
KZAM	Klasifikace zaměstnání
NB	Notebook
LDAP	Lightweight Directory Access Protocol – protokol pro ukládání a přístup k datům na adresářovém serveru
NSESSS	Národní standard pro elektronické systémy spisové služby
NÚKIB	Národní úřad pro kybernetickou bezpečnost
O11	Odbor řízení provozu
ODD	Obecná distribuce dokumentů
OWASP	The Open Worldwide Application Security Project – komunita publikující články, metodiky, dokumentaci, nástroje a technologie v oblasti zabezpečení webových aplikací.
PAM	Privileged Access Management – správa a zabezpečení účtů s vysokou úrovní oprávnění
SAP DI	SAP Data Integrator
SAP HR	Personalistický modul systému SAP
SAST	Static Application Security Testing– testovací procedura, při které dochází k analýze zdrojového kódu aplikace, aby byly identifikovaný bezpečnostní slabiny aplikace.
SSO	Single Sign On – Jednotné přihlášení
SŽ	Správa železnic, státní organizace
TLS	Transport Layer Security– je kryptografický protokol sloužící k zabezpečení komunikace na internetu.
ZIP	Souborový formát pro kompresi a archivaci dat

Úvod

Předmět projektu

Předmětem tohoto výběrového řízení je vyvinout a v prostředí SŽ zprovoznit aplikaci, která bude sloužit k distribuci dokumentů evidovaných v eSSL a k prokazatelnému seznámení s nimi. Cílem je plně nahradit současné aplikační komponenty Distribuce dokumentů, EKN a Depeše perspektivním a uživatelsky přívětivým řešením v souladu s legislativou.

Hlavní cíle projektu

Cíl 1: Vybrat spolehlivého partnera (dodavatele) pro vývoj a nasazení aplikace Distribuce dokumentů.

Cíl 2: Oprostit současný systém spisové služby od funkcionalit, které nejsou předmětem atestace systému elektronické spisové služby a vytvořit architektonicky robustní řešení, které budou prostřednictvím webové služby moci využívat i ostatní ISSD.

Cíl 3: Plně nahradit stávající aplikační komponenty Distribuce dokumentů, EKN a Depeše, tak aby nedošlo k degradaci jejich funkcionalit, ale naopak aby byly stávající funkcionality vylepšeny a doplněny a aby byla zlepšena uživatelská přívětivost řešení.

Cíl 4: Zajistit, že nové řešení bude v plném souladu s platnou legislativou ČR, NSESSS i interními předpisy SŽ.

1 Popis stávajícího stavu

Cílem této kapitoly je stručně popsat současné komponenty Distribuce dokumentů, EKN a Depeše.

1.1 Distribuce dokumentů

Modul Distribuce dokumentů je funkcionalita určená pro zpřístupnění digitálních dokumentů jiným uživatelům a útvarům. Funkcionalita je součást současné spisové služby ERMS. Distribuovány mohou být pouze dokumenty evidované v ERMS. Modul využívá spisové uzly (vybrané útvary z organizační struktury SAP HR) jako rozdělovník, přes který se dokumenty distribuují od zpracovatele po koncového příjemce.

1.1.1 Procesy

1.1.1.1 Odeslání a distribuce na koncového uživatele

Zadávat distribuci může pouze zpracovatel dokumentu v ERMS. Pokud se adresát distribuce v organizační struktuře nachází ve spisovém uzlu podřazeném zadavateli distribuce, pak zadavatel dokumentu může poslat distribuci přímo na koncového uživatele.

Pokud zpracovatel zasílá distribuci na spisový uzel, který mu dle organizační struktury není podřízen, pak je distribuce řízena nadřízenými sekretariáty, které mohou povolit distribuci na koncového uživatele nebo ji zastavit.

V případě, že distribuovaný dokument není evidován v ERMS, pak jej zpracovatel může založit přímo v modulu Distribuce dokumentů.

1.1.1.2 Příchozí distribuce

Koncový příjemce zobrazuje jemu distribuované dokumenty na záložce „Příchozí". Uživateli se zobrazuje seznam dokumentů, které mu byly distribuovány. V seznamu uživatel může vyhledávat podle atributů dokumentu. Dále uživatel může zobrazit detail dokumentu – hlavičku dokumentu a obsažené komponenty (soubory). Pokud je u dokumentů povolená redistribuce, uživatel může dokument distribuovat na jiného uživatele (nebo na spisový uzel).

Distribuce dokumentů neobsahuje funkcionalitu prokazatelné seznámení – dokument je považován za přečtený v momentu rozkliknutí detailu dokumentu (není kontrolováno zobrazení komponenty dokumentu).

1.1.1.3 Historie distribuce

Zpracovatel dokumentu a nadřazený sekretariát má oprávnění nahlížet na historii distribuce dokumentu. Je evidováno, kým a komu byla distribuce zadána, validace nadřazenými sekretariáty, a kteří uživatelé zobrazili detail dokumentu.

1.1.2 Nevyhovující oblasti současného řešení

Současné řešení je nevyhovující hlavně v těchto oblastech:

- Funckionalita distribuce dokumentů je součástí ERMS, přestože oběh a distribuce dokumentů nejsou funckionality standardně zajišťované spisovou službou.
- Distribuce dokumentů neumožňuje prokazatelné seznámení.
- Modul neodpovídá požadavkům uživatelské přehlednosti a přívětivosti.

1.2 EKN

Modul EKN (elektronická knihovna normálií) slouží k seznamování zaměstnanců s důležitými dokumenty týkající se řízení provozu (opatření, rozkazy atd.). Toto řešení je velmi podobné Distribuci dokumentů (viz výše) a jde též o součást systému ERMS. Současná Distribuce dokumentů a EKN se liší v následujících oblastech:

- EKN obsahuje funkcionalitu prokazatelné seznámení a je evidováno, že se pracovníci seznámili s komponentami dokumentu.
- EKN pro rozdělovník vedle organizační strukturu ze SAP HR a využívá také alternativní manuálně spravovanou organizační strukturu.

1.2.1 Nevyhovující oblasti současného řešení

Současné řešení je nevyhovující hlavně v těchto oblastech:

- Alternativní organizační strukturu je třeba spravovat manuálně.
- Neexistuje více úrovní prokazatelného seznámení.

1.3 Depeše

Depeše slouží k posílání rychlých a krátkých zpráv pro provozní zaměstnance. Současná aplikace je zcela oddělená od eSSL. Řešení spočívá v posílání emailových zpráv do schránek dopravních kanceláří a externistů.

1.3.1 Nevyhovující oblasti současného řešení

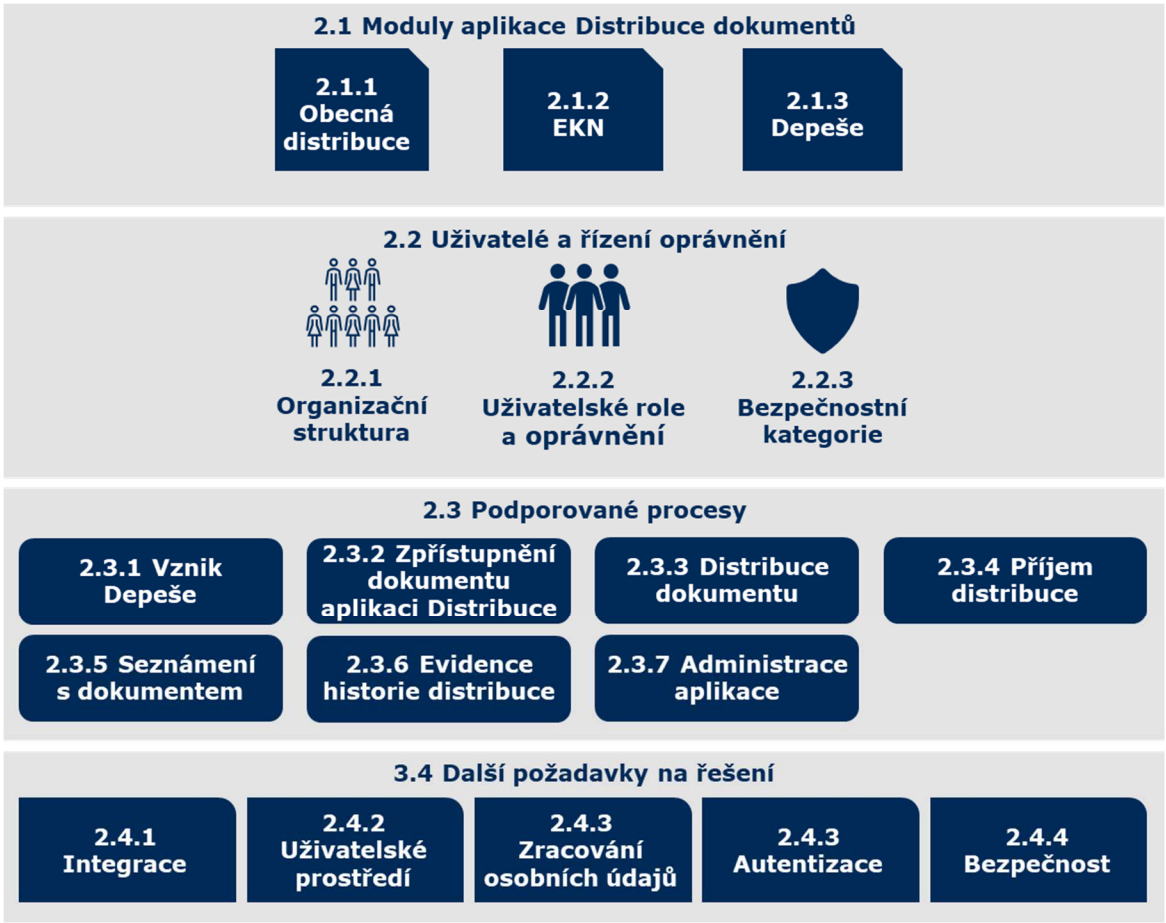
Současné řešení je nevyhovující hlavně v těchto oblastech:

- Depeše nejsou evidovány v eSSL.
- Aplikace Depeše je zastaralá a není ve vlastnictví SŽ.

2 Popis požadovaného stavu

Cílem této kapitoly je popsat požadavky SŽ pro účely výběrového řízení na dodavatele aplikace Distribuce dokumentů / Depeše. Tato kapitola bude sloužit jako podklad pro cílový koncept, který bude vypracován vybraným dodavatelem aplikace.

Struktura této kapitoly je pro snadnější orientaci zobrazena na Obrázku 1.



Obrázek 1: Struktura kapitoly 2

2.1 Moduly aplikace Distribuce dokumentů

V cílovém stavu budou současné aplikace/moduly Distribuce dokumentů, EKN a Depeše nahrazeny jedním samostatným systémem. Nový systém bude jednak podporovat tzv. Obecnou distribuci dokumentů (ODD), která bude mít řadu základních vlastností (viz podkapitola 2.1.1). Dále bude systém podporovat speciální typy distribuce splňující specifické požadavky odboru O11 (viz podkapitoly 2.1.2 a 2.1.3).

2.1.1 Obecná distribuce dokumentů

Obecná distribuce dokumentu bude mít následující vlastnosti:

- **Předmět distribuce:** Předmětem distribuce bude dokument nebo spis (entita) řádně evidovaný v eSSL. Distribuovány budou moci být pouze uzavřené koncepty dokumentů. Formát komponent dokumentu k distribuci nebude omezen, ale některé funkcionality budou omezeny datovým formátem souborů (např. konsolidace obsahu z více komponent do jednoho náhledu bude možná pouze pro textové dokumenty atp.).
- **Zadavatel distribuce:** Zadavatelem distribuce bude zpracovatel dokumentu v eSSL nebo správce spisového uzlu nadřazeného zpracovateli dokumentu nebo vedoucí zaměstnanec zpracovatele dokumentu. V případě, že u distribuovaného dokumentu je povolena redistribuce, pak novou distribuci může zadat i příjemce distribuce.
- **Příjemce distribuce:** Příjemcem distribuce může být každý uživatel aplikace (autentizovaný oproti AD).
- **Rozdělovník pro distribuci na koncového uživatele:** ODD bude pracovat s organizační strukturou SŽ v podobě spisových a dalších zvolených distribučních uzlů. Při zadání distribuce se bude možné rozhodnout, zda distribuovat na jmenného uživatele nebo na spisový uzel. V případě distribuce na spisový uzel bude koncový uživatel vybrán správcem spisového uzlu / operátorem. Organizační struktura a výběr distribučních uzlů bude předmětem administrace aplikace.
- **Prokazatelné seznámení:** ODD bude obsahovat funkcionalitu prokazatelného seznámení s dokumentem (viz kapitola 2.3.5)
- **Notifikace:** Uživatel bude o příchozí distribuci notifikován emailem a notifikací v prostředí aplikace.

2.1.2 EKN

Distribuce EKN se bude od Obecné distribuce lišit v následujících oblastech:

- **Zadavatel distribuce:** Zadavatelem distribuce EKN bude vždy pouze zaměstnanec Úseku řízení provozu SŽ s příslušným oprávněním. Jinak se neliší od ODD.
- **Příjemce distribuce:** Příjemce distribuce EKN může být pouze uživatel s příslušným oprávněním.
- **Rozdělovník pro distribuci na koncového uživatele:** Organizační struktura EKN bude též vycházet ze stejné organizační struktury jako ODD, ale bude moci mít nastavené vlastní distribuční uzly. Na rozdíl od ODD nebude možné distribuovat EKN přímo na jmenného uživatele, pokud daný uživatel nespadá do uzlu podřazeného zadavateli distribuce. V takovém případě musí o distribuci na koncového příjemce rozhodnout správce/operátor spisového uzlu.
- **Označení distribuce:** EKN bude pro příjemce i odesílatele vždy jasně rozlišitelná oproti ODD a Depeše.

2.1.3 Depeše

Modul Depeše se bude od Obecné distribuce lišit v následujících oblastech:

- **Předmět distribuce:** Na rozdíl od ODD a EKN bude dokument depeše přímo vznikat a bude spravován v aplikaci Distribuce dokumentů.
- **Zadavatel distribuce:** Zadavatelem distribuce depeše bude vždy pouze provozní zaměstnanec Úseku řízení provozu SŽ s příslušným oprávněním. Jinak se neliší od ODD.
- **Příjemce distribuce:** Příjemce distribuce depeše může být pouze uživatel s příslušným oprávněním. Jinak se neliší od ODD.
- **Rozdělovník pro distribuci na koncového uživatele:** Bude využíván podobný mechanismus jako u EKN s rozdílem, že depeše může být směřována pouze na distribuční uzel a „vyzvedne" ji zaměstnanec, který má právě směnu.
- **Notifikace:** Notifikace o příchozí depeši může být posílána na emailovou schránku distribučního uzlu. Depeši vč. notifikace bude možné zaslat i na koncového příjemce (zejména externisté).
- **Označení distribuce:** Depeše bude pro příjemce i odesílatele vždy jasně rozlišitelná oproti ODD a EKN.

2.2 Uživatelé a řízení oprávnění

2.2.1 Organizační struktura

Organizační strukturou myslíme vnitřní hierarchii organizačních útvarů SŽ a jim přiřazených pozic a jmenných uživatelů. Organizační struktura bude využívána v následujících případech:

- **Přiřazení uživatelských rolí:** Některé uživatelské role budou vázány na pozici v organizační struktuře.
- **Distribuce dokumentů:** Distribuce dokumentů může být směřována nikoliv na jmenného uživatele, ale na distribuční uzel. Dokument v tomto případě bude správcem (operátorem) distribučního uzlu redistribuován na podřízené uzly nebo jmenné uživatele.

Primární zdroj pro organizační strukturu bude systém SAP HR (SAP DI). Dále bude využívána integrace na eSSL prostřednictvím, které budou identifikovány organizační útvary sloužící jako spisové uzly v eSSL.

2.2.1.1 Zdrojová data ze SAP HR

Primární zdroj dat pro organizační strukturu je SAP HR. Synchronizace dat mezi aplikací Distribuce dokumentů a SAP HR bude probíhat denně za použití SAP Data Integrator. SAP DI bude poskytovat kompletní export platné organizační struktury ze SAP HR.

Distribuce dokumentů bude využívat následující data SAP HR:

- **Identity ID:** ID identity zaměstnance
- **Organizační útvary a vztahy mezi nimi:** Aplikace DD bude využívat aktuálně definované organizační útvary a bude pracovat s vazbami podřízenosti a nadřízenosti organizačních útvarů.
- **Pozice zaměstnanců:** Aplikace DD bude ze SAP HR přebírat informace o pozici zaměstnance.
- **Vedoucí zaměstnanci:** Aplikace DD bude definovat roli Vedoucí zaměstnanec na základě role Vedoucí zaměstnanec a Pověřený vedoucí zaměstnanec ze SAP HR.
- **Klasifikace zaměstnání (KZAM):** Aplikace bude využívat klasifikaci zaměstnaní KZAM.
- **Jmenní uživatelé:** K organizačním útvarům, pozicím a KZAM budou přiřazeni jmenní uživatelé.
- **Externí uživatelé:** Příznak, že jmenný uživatel je externí.
- **Kontaktní informace**: Emailová adresa, telefonní číslo a další kontaktní údaje jmenného uživatele.

2.2.1.2 Distribuční uzly

Organizační útvary ze SAP HR budou v aplikaci DD vystupovat jako distribuční uzly. Na distribuční uzly bude možné zadávat distribuci dokumentů. Zároveň budou s uzly svázány některé uživatelské role (správce distribučního uzlu, operátor distribučního uzlu, kontrolor distribučního uzlu). Aplikace bude pracovat s více typy uzlů:

1. **Spisové uzly v eSSL**: Všechny organizační útvary, které jsou v eSSL označeny jako spisové uzly budou v aplikaci fungovat jako distribuční uzly. Synchronizace spisových uzlů mezi eSSL a Distribuce dokumentů bude probíhat pravidelně a automaticky prostřednictvím webové služby eSSL.
2. **Ostatní organizační útvary v SAP HR:** Kromě spisových uzlů můžou distribučními uzly být i organizační útvary, které v eSSL nejsou vedeny jako spisové uzly. Nastavení těchto distribučních uzlů budou provádět správci aplikace/modulu. U jednotlivých modulů může docházet k definici jiných

distribučních uzlů z organizační struktury. Proto aplikace musí být připravena na práci s několika alternativními hierarchiemi distribučních uzlů.

2.2.1.3 Identifikace změn organizační struktury

Aplikace bude připravena na identifikaci změn v organizační struktuře viz požadavky v tabulce níže.

ID	Popis požadavku
ZOS1	**Identifikace změn organizační struktury** Je požadováno, aby aplikace DD identifikovala změny organizační struktury ze SAP HR na základě rozdílů mezi nově importovanými a posledně nahranými daty. Aplikace bude pracovat se ztrátou validity uživatelů/útvarů v důsledku změn organizační struktury viz kapitola 2.2.1.4.
ZOS2	**Detekce chybného importu dat** Je požadováno, aby aplikace obsahovala kontrolní mechanismus, který bude bránit importu podezřelého množství dat organizační struktury. Řešení bude umožňovat nastavení povolených odchylek počtu záznamů mezi nově importovanými a posledně nahranými daty. Pokud odchylka bude větší než nastavená mez, nedojde k automatického importu dat a pro jeho uskutečnění bude vyžadována akce správce systému.

2.2.1.4 Řešení ztráty validity uživatele/útvaru v důsledků změny organizační struktury

V případě změn organizační struktury, aplikace bude reagovat na ztrátu validity uživatele a organizačního útvaru. Případy ztráty validity a požadovaný postup při výskytu ztráty jsou popsány v podkapitolách níže.

Ztráta validity uživatele

Klíčovými údaji pro posouzení validity uživatele jsou vedle jeho samotné existence také přiřazení k organizačnímu útvaru (“změna pracoviště”) a změna KZAM (“změna pozice, resp. profese”).

Identifikovaná událost	Způsob / postup řešení
Uživatel (Identity ID) nově neexistuje v seznamu zaměstnanců (uživatelů)	Uživatel/uživateli nově nebude možné zaslat distribuci. Stávající distribuce zůstanou zachovány ve stávajícím stavu. Pokud má uživatel přiděleny nějaké vyšší role/oprávnění, bude odpovídající nadřazený uživatel notifikován o ztrátě validity uživatele a budou nabídnuty nástroje pro předání oprávnění na nového uživatele. Pokud dojde k nevalidině vrcholového administrátora, budou notifikování všichni zbývající vrcholoví administrátoři. Do doby vypořádání oprávnění (zahodit/převést) bude účet uveden v přehledu nevypořádaných rolí/oprávnění nevalidních uživatelů. Pokud je uživatel vlastníkem entit eSSL (dokumentů, spisů), bude notifikován příslušný správce daného uzlu a tento správce bude mít nástroje pro provedení změny vlastníka entity. Do doby vypořádání vlastnictví entit bude účet uveden v přehledu nevypořádaných entit eSSL nevalidních uživatelů.

Identifikovaná událost	Způsob / postup řešení
Uživatel (Identity ID) je nově přiřazený do jiného organizačního útvaru.	Pokud má uživatel přiděleny nějaké vyšší role/oprávnění, bude původní odpovídající nadřazený uživatel notifikován o ztrátě validity uživatele a budou nabídnuty nástroje pro předání oprávnění na nového uživatele. Do doby vypořádání oprávnění (zahodit/převést) bude účet uveden v přehledu nevypořádaných rolí/oprávnění nevalidních uživatelů. Pokud je uživatel vlastníkem entit eSSL (dokumentů, spisů), bude notifikován příslušný správce daného uzlu a tento správce bude mít nástroje pro potvrzení vlastnictví entity nebo pro provedení změny vlastníka entity. Do doby vypořádání vlastnictví entit bude účet uveden v přehledu nevypořádaných entit eSSL nevalidních uživatelů.
Uživatel (Identity ID) má nově přiřazený jiný KZAM nebo příznak vedoucí zaměstnanec, přiřazení do organizačního útvaru se zároveň nezměnilo.	Pokud má uživatel přiděleny nějaké vyšší role/oprávnění, bude odpovídající nadřazený uživatel notifikován o ztrátě validity uživatele a budou nabídnuty nástroje pro potvrzení stávajících rolí/oprávnění nebo pro předání oprávnění na nového uživatele. Do doby vypořádání oprávnění bude účet uveden v přehledu nevypořádaných rolí/oprávnění nevalidních uživatelů.
Uživatel (Identity ID) má nově jiné jméno/příjmení nebo vedoucího.	Proběhne pouze automatická aktualizace údaje bez nutnosti další interakce uživatele v aplikaci.

Ztráta validity organizačního útvaru

Klíčovým údajem pro posouzení validity útvaru je pouze jeho samotná existence.

Identifikovaná událost	Způsob / postup řešení
Útvar (kód útvaru) nově neexistuje v hierarchii organizační struktury.	Na útvar / z útvaru nově nebude možné zaslat distribuci. Pokud na daném útvaru existují probíhající (nedokončené) distribuce, bude o tom notifikován zadavatel distribuce, který bude mít standardní nástroje pro případnou definici další distribuce. O ztrátě validity uzlu bude notifikován odpovídající nadřazený uživatel a budou mu nabídnuty nástroje pro odebrání oprávnění uživatelů pro daný uzel nebo pro předání oprávnění uživatelů na nový uzel. Do doby vypořádání oprávnění (zahodit/převést) bude uzel uveden v přehledu nevypořádaných rolí/oprávnění nevalidních uzlů.
Útvar (kód útvaru) má nově jiný název.	Proběhne pouze automatická aktualizace názvu bez nutnosti další interakce uživatele v aplikaci.

2.2.2 Uživatelské role a oprávnění

Aplikace umožní řídit oprávnění k jednotlivým funkcionalitám aplikace na základě uživatelských rolí. Předběžný seznam uživatelských rolí naleznete tabulce níže.

Role	Popis oprávnění	Zdrojový systém / manuální přiřazení role
Uživatel interní	Přístup k dokumentům, které na uživatele byly distribuovány. Oprávnění redistribuovat dokumenty, u kterých je povolena redistribuce.	SŽ AD
Uživatel externí	Přístup k dokumentům, které na uživatele byly distribuovány.	SŽ AD
Vrcholový správce aplikace	Business administrátor aplikace. Nejvyšší oprávnění.	Aplikační administrátor dle AD (privilegovaný účet v AD)
Správce modulu	Správce zodpovědný za celý modul. Nejvyšší v hierarchii distribučních uzlů v daném modulu.	Manuálně vrcholovým administrátorem / Prostřednictvím IDM
- Správce modulu ODD	Správce modulu ODD, definice distribučních uzlů v daném modulu, přidělovat oprávnění správce distribučního uzlu hierarchie ODD.	Manuálně vrcholovým administrátorem / Prostřednictvím IDM
- Správce modulu EKN	Správce modulu EKN, definice distribučních uzlů v daném modulu, přidělovat oprávnění správce distribučního uzlu hierarchie EKN.	Manuálně vrcholovým administrátorem / Prostřednictvím IDM
- Správce modulu Depeše	Správce modulu ODD, definice distribučních uzlů v daném modulu, přidělovat oprávnění správce distribučního uzlu hierarchie Depeše.	Manuálně vrcholovým administrátorem / Prostřednictvím IDM
Zpracovatel dokumentu	Má oprávnění distribuovat dokument, jehož je zpracovatelem. Zpracovatel dokumentu je jedním z atributů dokumentu v eSSL.	eSSL / Prostřednictvím IDM
Správce distribučního uzlu	Správa podřazených distribučních uzlů dle modulu.	Manuálně správcem modulu / správcem nadřízeného uzlu / Prostřednictvím IDM
- Správce distribučního uzlu ODD	Oprávnění distribuovat dokumenty z daného spisového uzlu, redistribuovat dokumenty, které přišly na distribuční uzel. Zobrazení historie distribuce na jeho uzlu (kontrola redistribuce). Má oprávnění udělovat správcovská/kontrolorská/operátorská oprávnění pro jemu podřízené uzly.	Manuálně správcem modulu / správcem nadřízeného uzlu / Prostřednictvím IDM

Role	Popis oprávnění	Zdrojový systém / manuální přiřazení role
- Správce distribučního uzlu EKN	Oprávnění distribuovat dokumenty z daného spisového uzlu, redistribuovat dokumenty, které přišly na distribuční uzel. Zobrazení historie distribuce na jeho uzlu (kontrola redistribuce). Má oprávnění udělovat správcovská/kontrolorská/operátorská oprávnění pro jemu podřízené uzly.	Manuálně správcem modulu / správcem nadřízeného uzlu / Prostřednictvím IDM
- Správce distribučního uzlu Depeše	Oprávnění distribuovat dokumenty z daného spisového uzlu, redistribuovat dokumenty, které přišly na distribuční uzel. Zobrazení historie distribuce na jeho uzlu (kontrola redistribuce). Má oprávnění udělovat správcovská/kontrolorská/operátorská oprávnění pro jeho podřízené uzly. Definice emailových adres pro zaslání notifikace do zástupné schránky při příchozí Depeši.	Manuálně správcem modulu / správcem nadřízeného uzlu / Prostřednictvím IDM
Vedoucí zpracovatele dokumentu	Oprávnění zadat distribuci dokumentu, u něhož je zpracovatelem jeho podřízený, zobrazit historii prokazatelného seznámení u dokumentů, jejichž zpracovatelem je jeho podřízený.	SAP HR
Kontrolor	Oprávnění zobrazit historii distribuce a prokazatelného seznámení na daném uzlu.	Manuálně správcem dist. uzlu / Prostřednictvím IDM
Operátor	Oprávnění redistribuovat dokumenty, které přišly na spisový uzel. Podobné oprávnění jako správce dist. uzlu (bez administrace uzlů).	Manuálně správcem dist. uzlu / Prostřednictvím IDM
Tvůrce Depeše	Uživatel s oprávněním vytvořit a odesílat depeše.	Manuálně správcem distribučního uzlu Depeše / Prostřednictvím IDM
Uživatel Depeše	Uživatel s oprávněním zobrazit dokument depeše.	Manuálně správcem distribučního uzlu Depeše / Prostřednictvím IDM
Tvůrce EKN	Uživatel s oprávněním odesílat distribuce s příznakem EKN.	Manuálně správcem distribučního uzlu EKN / Prostřednictvím IDM
Příjemce EKN	Uživatel s oprávněním přijímat distribuce s příznakem EKN.	Manuálně správcem distribučního uzlu EKN / Prostřednictvím IDM

2.2.2.1 Požadavky na řízení uživatelských rolí

ID	Popis požadavku
URO1	**Definice uživatelských rolí a oprávnění** Aplikace Distribuce dokumentů bude umožňovat řízení oprávnění na základě definovaných uživatelských rolí. Uživatelské role bude možné tvořit a měnit v průběhu produktivního provozu aplikace (výše uvedený seznam je pouze předběžný). Na základě příslušnost k roli bude uživateli udělena množina uživatelských oprávnění. Uživatelská oprávnění budou nedělitelná a jasně definovaná. Finální seznam uživatelských oprávnění řízených aplikací bude vytvořen v rámci cílového konceptu pro vývoj aplikace.
URO2	**Kumulace uživatelských rolí** Aplikace bude umožňovat kumulaci více uživatelských rolí u jednoho uživatele.
URO3	**Přiřazení role uživateli** Aplikace bude umožňovat několik způsobů přiřazení role jmennému uživateli: • Manuálně uživatelem s příslušným oprávnění • Automaticky na základě dat z napojených systémů (AD, SAP HR) • Prostřednictvím IDM.

2.2.3 Bezpečnostní kategorie

Prostřednictvím aplikace DD budou distribuovány dokumenty více bezpečnostních kategorií (viz tabulka níže).

Úroveň přístupu	Popis	Moduly
Veřejné	Informace je veřejně přístupná nebo byla určena ke zveřejnění. Neoprávněné prozrazení nezpůsobí žádné škody pro SŽ, zainteresované strany, partnery nebo dotčené orgány anebo osoby. Příklady: webové stránky, odborné brožurky, příspěvky do tisku, apod.	ODD, EKN, Depeše
Interní	Informace není veřejně přístupná a tvoří know-how SŽ, ochrana informace není vyžadována žádným právním předpisem nebo smluvním ujednáním. Neoprávněné prozrazení nesmí vést k porušení zákonných povinností, ale může způsobit drobné potíže nebo podřadné provozní nepříjemnosti pro SŽ, zainteresované strany, partnery nebo dotčené orgány anebo osoby. Tyto informace mohou být sdílené mezi určitou skupinou externích osob, aniž by bylo vyžadováno smluvní zajištění mlčenlivosti, nicméně je doporučeno.	ODD, EKN, Depeše
Diskrétní	Informace není veřejně přístupná a její ochrana je vyžadována právními nebo jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů). Neoprávněné prozrazení může způsobit vážný dopad nebo rizika pro SŽ, zainteresované strany, partnery nebo dotčené orgány anebo osoby. Příklady: záznamy obsahující osobní údaje včetně údajů vztahujících se ke mzdovému ocenění, odborné analýzy, informace o posouzení nebo ošetření rizik, přístupová hesla, apod.	ODD

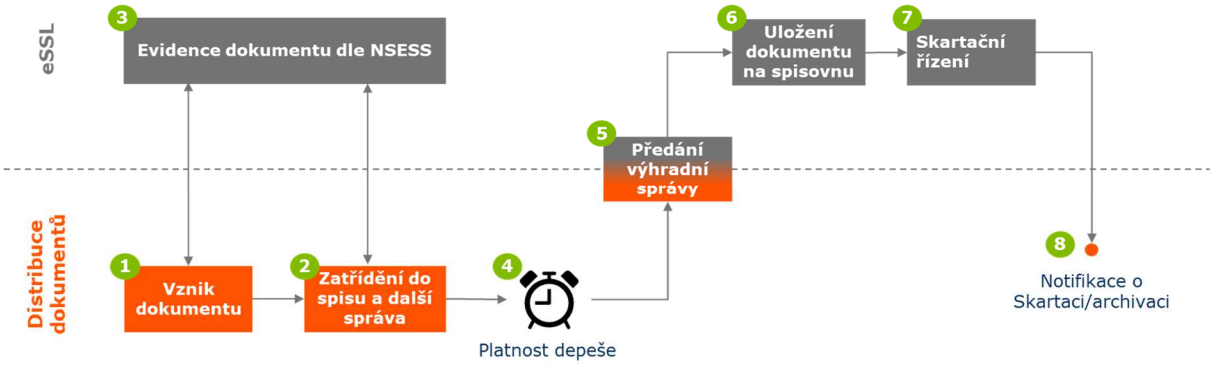
Úroveň přístupu	Popis	Moduly
Velmi diskrétní	Informace není veřejně přístupná a vyžaduje nadstandardní míru ochrany nad rámec předchozí kategorie. Neoprávněné prozrazení může způsobit velmi vážný dopad nebo rizika pro SŽ, zainteresované strany, partnery nebo dotčené orgány anebo osoby. Příklady: strategické obchodní tajemství, citlivé údaje, informace utajované státem.	ODD

2.3 Podporované procesy

V této kapitole jsou popsány budoucí procesy, které budou podporovány aplikací Distribuce dokumentů a požadavky na ně.

2.3.1 Vznik depeše

Vznik dokumentu v aplikaci Distribuce dokumentů bude probíhat pouze v případě Depeší. U ODD a EKN budou distribuovány dokumenty/spisy již zaevidované v eSSL.



Obrázek 2: Schéma procesu Vznik depeše

2.3.1.1 Popis procesu Vznik depeše

Krok	Proces/aktivita	Popis procesu	Aplikace
1	Vznik dokumentu	• Aplikace Distribuce bude obsahovat textový editor, ve kterém dojde k vytvoření depeše. Následně se vytvořený text vygeneruje v jedné komponentě dokumentu formátu PDF/A. • Před samotným vznikem dokumentu dojde k načtení aktuálních číselníků z eSSL (např. věcná skupina, typ dokumentu.) • Většina povinných atributů pro vznik dokumentu bude vyplňovaná automaticky. Všechny dokumenty typu depeše budou patřit do stejné věcné skupiny a budou stejného typu. • Při založení dokumentu dojde k nastavení platnosti dokumentu.	Distribuce dokumentů

Krok	Proces/aktivita	Popis procesu	Aplikace
2	Zatřídění do spisu a další správa	• Všechny vzniklé depeše budou zatříděny do spisu. • K zakládání spisů bude docházet automaticky dle nastavené aplikační logiky. Zpracovatelem spisu bude vždy zpracovatel dané depeše. Přesný mechanismus zatřídění do spisu bude definován až při detailní analýze v rámci přípravy cílového konceptu.	Distribuce dokumentů
3	Evidence dokumentu dle NSESSS	Dokument depeše bude řádně zaevidován a zatříděn do Spisu dle platného NSESSS a platné legislativy.	eSSL
4	Platnost depeše	Depeše budou platné na období nastavené při vzniku depeše. Konec doby platnosti může být nastaven na neurčito. Aplikace bude obsahovat možnost zpětné úpravy doby platnosti depeše.	Distribuce dokumentů
5	Předání výhradní správy	Po uplynutí období vázaného na dobu platnosti depeší ve spisu dojde k uzavření spisu a předání výhradní správy spisu z Distribuce dokumentů na eSSL.	Distribuce dokumentů / eSSL
6	Uložení na spisovnu	Vyřízený spis je předán na spisovnu. Celý proces probíhá na straně eSSL.	eSSL
7	Skartační řízení	Probíhá na straně eSSL. Při archivaci/skartaci dokumentu dojde k výmazu komponent, které tedy nebude možné nadále zobrazovat.	eSSL
8	Notifikace o Skartaci/archivaci	Aplikace Distribuce dokumentů bude notifikována o skartaci/archivaci dokumentu. Distribuce dokumentu dostane odpovídající příznak. Nadále bude možné zobrazit historii distribuce a prokazatelného seznámení.	Distribuce dokumentů

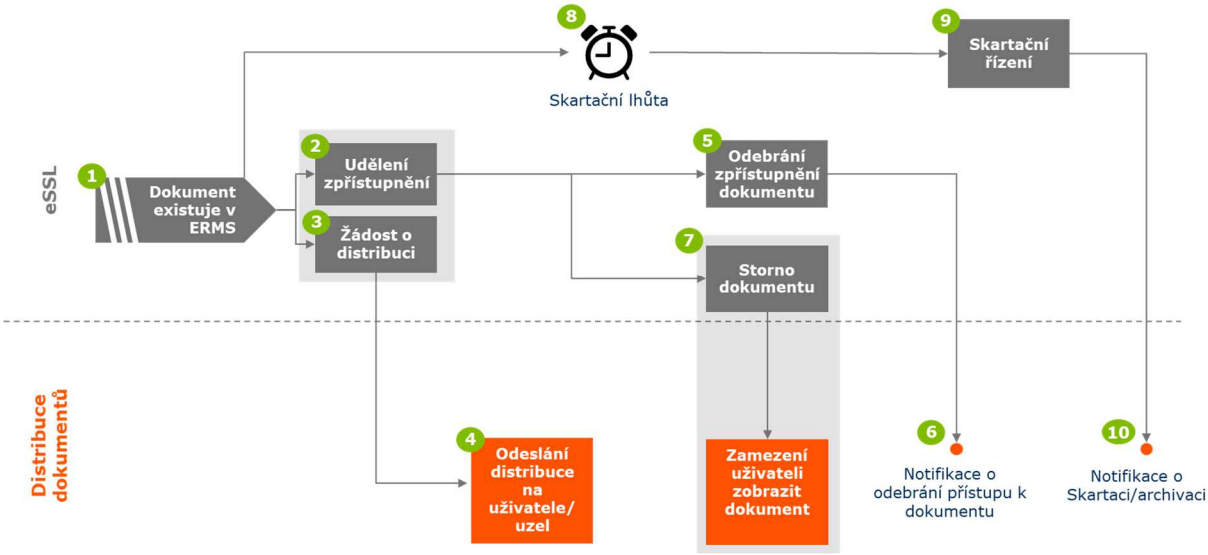
2.3.1.2 Požadavky na podporu procesu Vznik depeše

ID	Popis požadavku
VZD1	**Integrace s eSSL v souladu s NSESSS** Aplikace bude využívat rozhraní eSSL dle NSESSS. Aplikace bude ve vztahu k eSSL vystupovat jako ISSD komunikující zejména v následujících oblastech: • zakládání dokumentů a vkládání do spisů (vč. načtení číselníků), • editace metadat a vlastního obsahu dokumentu, • řešení mimořádných stavů, především storno nebo změny zpracovatele, vyřizování/uzavírání a předání výhradní správy do eSSL.

ID	Popis požadavku
VZD2	**Tvorba komponenty dokumentu depeše** Aplikace Distribuce dokumentů bude obsahovat textový editor, který bude mít základní funkcionality formátování textu (podobně jako u MS Outlook). Aplikace bude dále obsahovat funkcionalitu vygenerování komponenty dokumentu depeše ve formátu min. PDF/A-2b.
VZD3	**Platnost depeše** Atributy depeše budou obsahovat platnost Od-Do. Aplikace umožní zpětně změnit konec platnosti depeše. Na základě atributu platnost bude probíhat zatřiďování do spisu a uzavírání spisů.
VZD4	**Mechanismus zatřídění do spisu** Je požadována, aby aplikace obsahovala funkcionality nutné pro práci se spisy dle NSESSS. Zejména jde o: • zakládání spisů – možnost zakládání spisů automaticky na základě vydefinovaných spouštěcích událostí (např. uplynutí definované periody nebo založením nové depeše), • zatříděním dokumentu do spisů, • přetřiďování dokumentů mezi spisy (např. při změně platnosti depeše), • uzavírání spisu a předání do výhradní správy eSSL. Práci se spisy musí aplikace provádět automaticky a nebude k ní nutná žádná akce uživatele. Detailní popis práce se spisy a zatřiďování dokumentů bude předmětem detailní analýzy v rámci přípravy cílového konceptu.
VZD5	**Povolení odeslat depeši pouze uživateli s příslušným oprávněním** Aplikace DD bude řídit oprávnění k odeslání depeše a bude jej moci učinit pouze uživatel v roli Tvůrce depeše.

2.3.2 Zpřístupnění dokumentu aplikaci Distribuce dokumentů

Tento proces zahrnuje zpřístupnění dokumentů ve správě eSSL aplikaci Distribuce dokument a následnou komunikaci v případě změny stavu dokumentu.



Obrázek 3: Schéma procesu Zpřístupnění dokumentu aplikaci Distribuce dokumentů

2.3.2.1 Popis procesu Zpřístupnění dokumentu aplikaci Distribuce dokumentů

Krok	Proces / aktivita	Popis procesu	Aplikace
1	Dokument existuje v eSSL	Distribuován může být pouze uzavřený koncept, který je evidován v eSSL.	eSSL
2	Udělení zpřístupnění	Než může být dokument distribuován, musí být uděleno přístupové oprávnění aplikaci Distribuce dokumentů.	eSSL
3	Žádost o distribuci / vyvolání distribuce	Distribuce dokumentů bude poskytovat webovou službu, kterou umožní eSSL/ISSD vyvolat a distribuci dokumentu, který je ve výhradní správě eSSL/ISSD. Distribuci dokumentu ve správě eSSL/ISSD bude možné vyvolat i přímo z aplikace Distribuce dokumentu (po předchozím udělení zpřístupnění dokumentu).	eSSL
4	Odesláni dokumentu na uživatele / uzel	Po zpřístupnění dokumentu bude možné zahájit nad dokumentem distribuci. Aplikace zastaví možnost distribuce u dokumentů, které byly stornovány/skartovány / nebo pokud distribuci bylo odebráno/ukončeno zpřístupnění.	Distribuce dokumentů
5	Odebrání zpřístupnění dokumentu	V eSSL bude existovat možnost, že zpřístupnění dokumentu aplikaci Distribuce bude odebráno.	eSSL

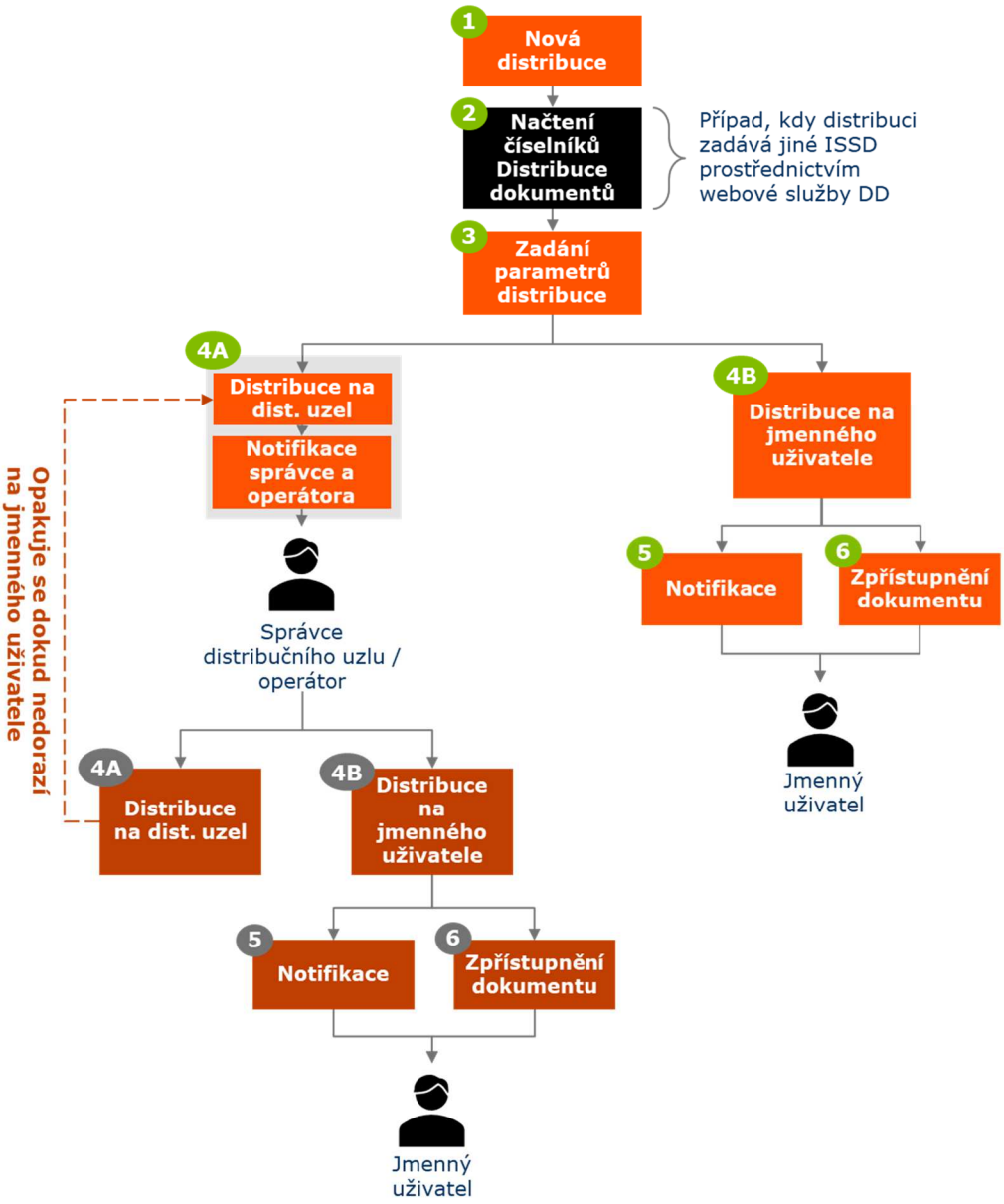
Krok	Proces / aktivita	Popis procesu	Aplikace
6	Notifikace o odebrání přístupu k dokumentu	V případě odebrání přístupu dochází k notifikaci aplikace Distribuce dokumentů.	Distribuce dokumentů
7	Storno dokumentu	Dokument může být v eSSL stornován. Při stornu nedochází k výmazu komponent dokumentu, aplikace zamezí v přístupu ke komponentám uživateli aplikace.	eSSL
8	Skartační lhůta	Atribut skartačního režimu, do kterého daný dokument/spis náleží.	eSSL
9	Skartační řízení	Probíhá v na straně eSSL. Při archivaci/skartaci dokumentu dojde k výmazu komponent, které tedy nebude možné nadále zobrazovat.	eSSL
10	Notifikace o Skartaci/archivaci	Aplikace Distribuce dokumentů bude notifikována o skartaci/archivaci dokumentu. Distribuce dokumentu dostane odpovídající příznak. Nadále bude možné zobrazit historii distribuce a prokazatelného seznámení.	Distribuce dokumentů

2.3.2.2 Požadavky na podporu procesu Zpřístupnění dokumentu aplikaci Distribuce dokumentů

ID	Popis požadavku
ZDA1	**Zpřístupnění dokumentu** Aplikace DD bude pracovat pouze s dokumenty, které ji budou zpřístupněny ze strany eSSL/ISSD. Na základě zpřístupněných metadat dokumentu aplikace DD automaticky identifikuje zpracovatele dokumentu.
ZDA2	**Archivace/Skartace dokumentu** Aplikace bude připravena reagovat na průběh životního cyklu dokumentu v eSSL. V případě archivace/skartace dojde k notifikaci systému DD a distribuce skartovaného dokumentu bude doplněna o příznak „Vyřazeno ve skartačním řízení“.
ZDA3	**Storno dokumentu** Aplikace bude připravena reagovat na stornování dokumentu v eSSL. Aplikace bude načítat informaci o stornu z atributů dokumentu v eSSL. V případě storna bude uživatelům znemožněno nadále zobrazovat komponenty dokumentu.
ZDA4	**Odebrání zpřístupnění dokumentu** Aplikace bude připravena na možnost, že jí bude odebrán přístup k dokumentu aplikací eSSL/ISSD. V rámci aplikace dojde k notifikaci systému DD o odebrání zpřístupnění dokumentu.

2.3.3 Distribuce dokumentů

Proces Distribuce dokumentů zahrnuje zadání distribuce dokumentu a cestu od zadavatele distribuce po koncového příjemce.



Obrázek 4: Schéma distribuce dokumentu od zadavatele po koncového příjemce

2.3.3.1 Popis procesu Distribuce dokumentů

Krok	Proces / aktivita	Popis procesu	Aplikace
1	Nová distribuce	Zadavatel distribuce zahájí novou distribuci a vybere dokument/dokumenty, které chce distribuovat.	Distribuce dokumentů / Jiný systém za využití webové služby Distribuce dokumentů

Krok	Proces / aktivita	Popis procesu	Aplikace
2	Načtení číselníků Distribuce dokumentů	Systém vyžívající webové služby Distribuce dokumentů si načte číselníky potřebné pro zahájení distribuce (zejména distribuční uzly a uživatele, na které je možné distribuci provést)	Jiný systém za využití webové služby Distribuce dokumentů
3	Zadání parametrů distribuce	Před odesláním distribuce zadavatel vyplní povinné parametry (Modul, Věc, Doba trvání distribuce, Možnost redistribuce, Adresát distribuce atp.)	Distribuce dokumentů / Jiný systém za využití webové služby Distribuce dokumentů
4A	Distribuce na distribuční uzel	Zadavatel distribuce bude moci zvolit distribuci na distribuční uzel. V tomto případě dojde k notifikaci správce distribučního uzlu a operátora, kteří následně rozhodnou o další distribuci dokumentu. Správce nebo operátor vybere, zda distribuovat na jiný distribuční uzel nebo na jmenného uživatele nebo na distribuční seznam.	Distribuce dokumentů / Jiný systém za využití webové služby Distribuce dokumentů
4B	Distribuce na jmenného uživatele	Zadavatel distribuce bude moci zvolit distribuci jmenného uživatele. V tomto případě se dokument přímo zpřístupní uživateli.	Distribuce dokumentů / Jiný systém za využití webové služby Distribuce dokumentů
5	Notifikace	1. Emailová notifikace: Uživatel (jmenný / role na uzlu) při nové příchozí distribuci bude notifikován emailem. Notifikační email bude obsahovat URL, které bude odkazovat na detail distribuce v aplikaci Distribuce dokumentů. 2. Notifikace v aplikaci: O nové distribuci bude uživatel notifikován i přímo v aplikaci Distribuce dokumentů.	Distribuce dokumentů
6	Zpřístupnění dokumentu uživateli	Dojde k zpřístupnění dokumentu koncovému uživateli.	Distribuce dokumentů

2.3.3.2 Rozdíly v procesu Distribuce dokumentu v případě EKN

V případě EKN bude omezena možnost odeslání distribuce na jmenného uživatele: V případě, že příjemce náleží k distribučnímu uzlu, který není podřízen zadavateli distribuce, distribuce bude zaslána na nadřízený distribuční uzel příjemce (nikoliv přímo na koncového příjemce).

2.3.3.3 Rozdíly v procesu Distribuce dokumentu v případě modulu Depeše

- **Externí příjemci:** Stejně jako v ODD – přímý výběr adresáta a zaslání emailové notifikace na kontaktní adresu.
- **Interní příjemci:** Odesílatel ani distribuční uzel nezná jméno uživatele, kterému je depeše určená, protože neví, kdo má z daného uzlu právě směnu. Proto v okamžiku, kdy depeše dojde na cílový distribuční uzel, bude odeslána emailová notifikace do zástupné emailové schránky daného distribučního uzlu.

2.3.3.4 Požadavky na podporu procesu Distribuce dokumentu

ID	Popis požadavku
DDA1	**Oprávnění k zahájení distribuce nad dokumentem** Aplikace umožní zadat novou distribuci pouze uživateli, který je v eSSL evidován jako zpracovatel dokumentu nebo správci spisového uzlu, k němuž je zpracovatel dokumentu přiřazen nebo vedoucímu zpracovatele dokumentu (dle SAP HR).
DDA2	**Zadání parametrů distribuce** Aplikace bude umožnovat zadání následujících parametrů distribuce: ▪ **Modul:** Obecná distribuce / EKN / Depeše. ▪ **Věc:** Několikaslovný popis předmětu distribuce. ▪ **Trvání distribuce:** Od – Do. Trvání distribuce je možné nastavit na neurčito a zpětně změnit. ▪ **Možnost redistribuce:** Zpracovatel může povolit příjemcům distribuce dokument redistribuovat na další uživatele. ▪ **Adresát distribuce:** Distribuční uzel nebo jmenný uživatel / distribuční seznam. ▪ **Úroveň prokazatelného seznámení:** Požadavek na prokazatelné seznámení k dané distribuci. ▪ **Poznámka k distribuci**: Volitelný průvodní text k distribuci. V případě redistribuce dokumentu může dojít ke změně parametrů distribuce (vč. modulu a úrovně prokazatelného seznámení). Tato změna se nepromítne do parametrů původní distribuce, ale pouze do redistribuce. Příklad: Distribuce modulu ODD přijde na spisový uzel a správce spisového uzlu se rozhodne, že jej redistribuuje na podřízené uživatele s příznakem EKN. **Upozornění:** Popsané parametry distribuce jsou předběžné a jejich finální podoba bude rozhodnuta až během cílového konceptu v rámci projektu implementace.
DDA3	**Distribuce nad spisem nebo nad souborem dokumentů** Aplikace bude podporovat distribuci několika dokumentů nebo celého spisu.
DDA4	**Distribuční seznamy** Aplikace bude podporovat zakládání distribučních seznamů složených z jmenných uživatelů napříč distribučními uzly a z jednotlivých distribučních uzlů. Administrátoři distribučních uzlů budou moci distribuční seznamy sdílet s jimi podřízenými uživateli. Seznam bude tvořen uživatelsky vhodným způsobem: Např. uživatelé a uzly budou moci být do seznamu přidáni např. vybráním několika distribučních uzlů nebo vyfiltrováním uživatelů dle KZAM.

ID	Popis požadavku
DDA5	**Cesta distribuce od odesílatele k příjemci v modulu Obecná distribuce** Distribuci dokumentu bude možné odeslat na: • **Na distribuční uzel**: O odeslání na jmenného uživatele nebo na další distribuční uzel, který následně rozhodne správce distribučního uzlu nebo operátor. • **Na jmenného uživatele:** Zadavatel přímo rozhodne, že distribuci zašle na interního nebo externího jmenného uživatele. Distribuci bude možné odeslat i na kombinaci distribučních uzlů, jmenných uživatelů a distribučních seznamů. Aplikace zabrání situaci, při které by uživateli byl stejný dokument distribuován několikrát.
DDA6	**Cesta distribuce od odesílatele k příjemci v modulu EKN** Bude probíhat obdobně jako u ODD s rozdílem, že pokud příjemce náleží k distribučnímu uzlu, který není podřízen zadavateli distribuce, distribuce bude zaslána na nadřízený distribuční uzel příjemce (nikoliv přímo na příjemce). Zadavatel bude moci zvolit jmenného příjemce a systém automaticky distribuci zašle na uzel odpovídající vybranému příjemci.
DDA7	**Cesta distribuce od odesílatele k příjemci v modulu Depeše** Bude probíhat obdobně jako u ODD s rozdílem, že depeše nebudou směřovány na interní jmenné uživatele ale na distribuční uzel. Jmenný uživatel se o nové depeši dozví emailovou notifikací na zástupnou schránku distribučního uzlu.
DDA8	**Redistribuce dokumentu příchozího na dist. uzel** Aplikace bude obsahovat vhodné uživatelské prostředí pro práci Správce distribučního uzlu a Operátora. Správce distribučního uzlu / Operátor zadá redistribuci dokumentu obdobně jako zadavatel distribuce: Opět bude mít možnost distribuovat na distribuční uzel, jmenného uživatele nebo prostřednictvím distribučního seznamu.
DDA9	**Redistribuce dokumentu** Aplikace bude umožňovat příjemci distribuce její redistribuci v případě, že redistribuce bude povolena zadavatelem distribuce.
DDA10	**Distribuce diskrétních a velmi diskrétních dokumentů** Aplikace bude připravena na distribuci diskrétních a velmi diskrétních dokumentů následovně: • Při zadání distribuce nad diskrétním nebo velmi diskrétním dokumentem bude zadavatel upozorněn na bezpečnostní kategorii dokumentu a bude muset potvrdit, že daný dokument opravdu chce distribuovat. • Příjemce distribuce obdrží v emailové notifikaci pokyny k zacházení s diskrétním a velmi diskrétním dokumentem.

2.3.4 Příjem distribuce dokumentů

2.3.4.1 Požadavky na podporu procesu Příjem distribuce dokumentů

ID	Popis požadavku
PDD1	**Řazení distribucí do schránek** Prostředí aplikace Distribuce dokumentů bude obsahovat adresářovou strukturu pro rozřazení příchozích a odchozích distribucí. Automaticky budou distribuce uživateli řazeny do schránek dle modulů Obecná distribuce / EKN / Depeše. Dále bude uživatel moci řadit distribuce do vlastní struktury a bude moci skrýt distribuce, se kterými již nepracuje. Prostředí bude pro usnadnění práce připomínat uživatelské rozhraní MS Outlook.
PDD2	**Vyhledávání a řazení distribuovaných dokumentů** Uživatel bude moci přijaté a odeslané depeše vyhledávat dle parametrů distribuce a metadat dokumentu.
PDD3	**Náhled a stažení dokumentu** Po provedení distribuce dokumentu bude adresát distribuce oprávněn stáhnout komponenty dokumentu na svůj lokální disk, v případě více komponent u jednoho dokumentu vše jako ZIP. V případě, že komponenty jsou ve formátu PDF/A, bude možné komponenty nahlédnout přímo v aplikaci Distribuce dokumentů. Komponenty budou pro náhled uloženy v krátkodobé cache a budou smazány po ukončení dané relace.
PDD4	**Konsolidovaný náhled dokumentu** U dokumentů ve formátu PDF bude uživateli nabídnuto vygenerování konsolidovaného náhledu všech komponent. Konsolidovaný náhled bude uložený v krátkodobé cache a bude smazán po ukončení dané relace.

2.3.4.2 Požadavky na podporu procesu Příjem distribuce dokumentů specifické pro modul Depeše

ID	Popis požadavku
PDD5	**Zobrazení depeše ze zástupné schránky** Uživatel bude moci otevřít dokument po kliknutí na URL odkaz obsažený v emailové notifikaci příchozí do zástupné schránky distribučního uzlu.
PDD6	**Zobrazení depeše z aplikace Distribuce dokumentů** Uživatel v roli Uživatel Depeše bude moci zobrazit depeši přímo v aplikaci Distribuce dokumentů. Aplikace mu umožní vyfiltrovat depeše na základě zvoleného distribučního uzlu a zvoleného data platnosti.
PDD7	**Náhled a stažení dokumentu** Komponentu dokumentu půjde v aplikaci nahlédnout nebo stáhnout stejně jako u Obecné distribuce nebo EKN.

2.3.5 Prokazatelné seznámení

Aplikace Distribuce dokumentů bude obsahovat funkcionalitu prokazatelné seznámení, díky které bude možné zpětně s vyšší mírou prokazatelnosti doložit, že se uživatel s dokumentem seznámil.

2.3.5.1 Požadavky na podporu procesu Prokazatelné seznámení

ID	Popis požadavku
PSZ1	**Úrovně prokazatelného seznámení** Požadovaná úroveň prokazatelného seznámení bude definována při zadání distribuce nad dokumentem. Úrovně prokazatelného seznámení budou následující: 1. **Bez požadavků:** U dokumentu není požadováno, aby se s ním uživatel prokazatelně seznámil. 2. **Základní míra prokazatelnosti**: Přihlášený uživatel potvrdí seznámení se s dokumentem kliknutím na tlačítko (nebo obdobným způsobem). 3. **Zvýšená míra prokazatelnosti:** Přihlášený uživatel bude při prohlášení o seznámení se s každým jednotlivým dokumentem nucen prokázat svoji identitu ještě dalším způsobem, typicky: • Elektronickým certifikátem uloženým na prostředku, který má pod svou výhradní kontrolou (zaměstnanecká čipová karta, USB token atp.) • Vícefaktorovým (MFA) ověřením pomocí mobilního telefonu a aplikace MS Authenticator, atp. Uživateli bude umožněno potvrdit seznámení (v úrovních 2 a 3) pouze pokud uživatel projde („proscrolluje“) celý konsolidovaný náhled dokumentu od začátku do konce.
PSZ2	**Auditní záznam v databázi o prokazatelném seznámení** Aplikace bude o prokazatelném seznámení ve všech úrovních řádně vést auditní záznamy v databázi se systémovou časovou značkou.

2.3.6 Evidence historie distribuce

2.3.6.1 Požadavky na podporu procesu Evidence historie distribuce

ID	Popis požadavku
EVH1	**Evidované informace** V historii distribuce budou evidovány minimálně následující informace: • Odesílatel • Příjemce • Záznam cesty distribuce přes spisové uzly • Datum odeslání • Datum zobrazení • Datum a způsob prokazatelného seznámení (pokud bylo požadováno, vč. podrobností o použitém druhém faktoru ověření) **Upozornění:** Jedná se o předběžný návrh a finální podoba bude rozhodnuta až během cílového konceptu v rámci projektu implementace.
EVH2	**Uživatelská oprávnění k evidenci** Je požadováno, aby všichni příjemci distribuce dokumentů měli přístup k historii distribuce a prokazatelného seznámení u daného dokumentu.
EVH3	**Uživatelsky přívětivé zobrazení evidence historie distribuce** Je požadováno, aby zobrazení evidence historie bylo pro uživatele přehledné a přívětivé. Uživatel si bude moci snadno zobrazit historii pouze u uzlů, které ho zajímají (například použití filtru).

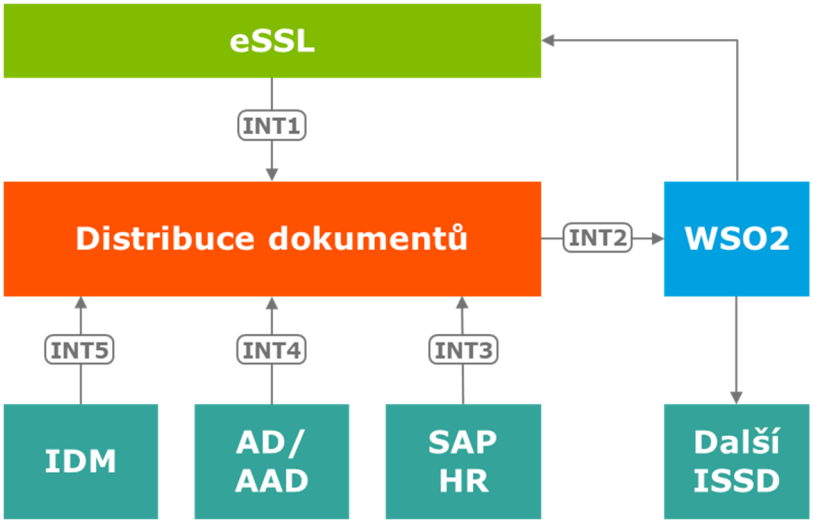
2.3.7 Administrace aplikace

2.3.7.1 Požadavky na podporu procesu Administrace aplikace

ID	Popis požadavku
ADA1	**Administrace distribučních uzlů pro jednotlivé moduly** Aplikace bude obsahovat administrační nástroj pro definici distribučních uzlů pro daný modul. Oprávnění volit distribuční uzly bude mít správce modulu.
ADA2	**Administrace uživatelských rolí** Aplikace bude obsahovat administrační prostředí pro definici a správu uživatelských rolí. Správa uživatelských rolí bude probíhat dle hierarchie distribučních uzlů. Vrcholový správce bude určovat správce modulu, správce modulu bude určovat správce distribučních uzlů, správci distribučních uzlů budou určovat správce podřízených distribučních uzlů, kontrolory a operátory.
ADA3	**Administrace validity útvaru a uživatele** Aplikace bude obsahovat vhodné administrační prostředí pro řešení ztráty validity útvaru a uživatele dle kapitoly 2.2.1.4 Řešení ztráty validity uživatele/útvaru v důsledků změny organizační struktury. Prostředí bude uživatelsky přívětivé a umožní správci řešit ztrátu validity efektivně (např. správce bude moci snadno vybrat všechny nebo některé nevalidní uživatele a rozhodnout o jejich validitě, uzlu, roli atp.). V souvislosti s validitou uzlů bude aplikace poskytovat nástroje pro kontrolu nastavení oprávnění / rolí / uživatelů pro jednotlivé uzly, typicky kontrola uzlů, kde "není žádná obsluha".
ADA4	**Administrace zástupných emailových adres u Depeší** Aplikace bude obsahovat administrační nástroj pro definici emailových adres zástupných schránek v modulu Depeše. Tyto emailové adresy budou spravovat správci distribučních uzlů.

2.4 Další požadavky na řešení

2.4.1 Integrace



Obrázek 5: Integrace

ID	Integrovaný systém	Věcný popis
INT1	ERMS	**Integrace s eSSL v souladu s NSESSS** Je požadováno, aby aplikace Distribuce dokumentů byla integrována s eSSL v souladu s NSESSS. V rámci integrace budou mezi eSSL a DD probíhat interakce v následujících oblastech: • Poskytnutí seznamu spisových uzlů eSSL aplikaci DD • Načtení číselníků z eSSL • Zpřístupnění dokumentu eSSL aplikaci DD • Založení dokumentu/spisu, evidence dokumentu a další správa dokumentu • Předání výhradní správy nad dokumentem • Notifikace o stornu, odebrání přístupu, skartaci/archivaci dokumentu
INT2	WSO2	**Poskytnutí webové služby Distribuce dokumentům dalším systémům** Je požadováno, že aplikace Distribuce dokumentů bude poskytovat dalším systémům webovou službu prostřednictvím integrační sběrnice WSO2. Webová služba bude obsahovat zejména: • Předání distribučních uzlů a adresátů. • Zadání distribuce nad dokumentem. • Poskytnutí informací o historii distribuce. WSO2 bude respektovat NSESSS.
INT3	SAP HR	**Integrace na SAP HR** Aplikace bude integrovaná se SAP HR prostřednictvím SAP Data Integrator. Aplikace DD bude využívat data SAP HR dle 2.2.2.1 Zdrojová data ze SAP HR.

ID	Integrovaný systém	Věcný popis
INT4	AD/AAD	**Autentizace oproti AD/AAD** Aplikace DD bude využívat Active directory k autentizaci uživatele pomocí protokolu Kerberos, nebo OpenID. Při přístupu z vnější sítě bude možná autentizace oproti AAD.
INT5	IDM	**Integrace s IDM** Systém bude nabízet rozhraní Identity managementu dle kapitoly 2.4.1.1 IDM.

Upozornění: Uvedené požadavky na integrace jsou pouze předběžné. Před vlastním projektem implementace dojde k detailní analýze integračního rozhraní.

2.4.2 Uživatelské prostředí

Finální podoba požadavků na uživatelské prostředí bude definována až při detailní analýze v rámci implementace řešení. Řešení bude splňovat minimálně následující požadavky.

ID	Popis požadavku
UZP1	**Uživatelské rozhraní (UI)** Cílem je vytvořit rozhraní, které poskytuje jednoduchou, srozumitelnou a pohodlnou interakci uživatele s informačním systémem. Je požadováno, aby uživatelské prostředí splňovalo následující zásady: • standardní ovládací prvky • uživatelské rozhraní jednoduché a přehledné • konzistentní prostředí • účelné rozvržení obrazovek • barvy a písma dle grafického manuálu • hierarchie daná typograficky • informování uživatele, co systém právě dělá • odpovídající tvar a velikost ovládacích prvků • kódování znaků UNICODE • datumové položky dle českého standardu „DD.MM.RRRR" • jednotný vizuální styl (pro některé projekty dle korporátní identity) • responzivní design webových aplikací
UZP2	**Uživatelský prožitek (UX)** UX aplikace Distribuce dokumentů musí mít následující vlastnosti: • cílem je efektivní uživatel • návodné ovládání • ergonomie • jednoduché, intuitivní • pravidla přístupnosti, tam kde je požadováno • zobrazování relativních a požadovaných dat rychlost odezvy (doba zpracování požadavku od uživatele by na serveru neměla přesáhnout 0,5s, tak aby celková doba odezvy uživatelský ovládacích prvků byla kratší než 0,8s. V případě, že je předpokládaný čas odezvy delší než 0,8s, ale kratší než 2s bude uživateli zobrazen wait cursor a pokud bude předpokládaný čas odezvy delší než 2s bude pro informaci uživatele použit progress bar zobrazující průběh operace.

2.4.3 Požadavky na zpracování osobních údajů

ID	Popis požadavku
ZOP1	**Zpracování dat dle požadavků legislativy (vč. GDPR)** Navržené řešení bude v souladu s požadavky vyplývajícími z platné legislativy ČR vč. GDPR a vnitřní směrnice SŽ SM097[1] .

2.4.4 Požadavky na autentizaci

ID	Popis požadavku
AUT1	**Požadavky na autentizaci** Při přihlášení z vnitřní sítě SŽ bude aplikace umožňovat SSO (Single Sign-On). Autentizace bude probíhat pomocí protokolu Kerberos, nebo OpenID proti Active Directory (AD). Vedle SSO bude možné se přihlásit manuálně zadáním uživatelského jména (přidělený AD – doménový účet) a příslušeného hesla. Při přihlášení z vnitřní sítě nebude požadováno vícefaktorové ověření.
AUT2	**Autentizace při přihlášení z externí sítě** Při přihlášení z externí sítě bude požadováno, aby došlo k vícefaktorovému ověření uživatele: • 1. faktor: Zadání uživatelského jména (přidělený AD – doménový účet) a příslušeného hesla. • 2. faktor: Ověření pomocí aplikace MS Authenticator nebo jiného druhého faktoru ověření v souladu prostředky KB SŽ. Autentizace bude probíhat pomocí protokolu Kerberos, nebo OpenID proti AD/AAD.

2.4.1 Bezpečnostní požadavky

2.4.1.1 IDM

Systém bude nabízet minimálně následující rozhraní Identity managementu:

- **CreateUser** – Vytvoření uživatele
- **ActivateUser** – Aktivace uživatele
- **DeactivateUser** – Deaktivace uživatele
- **ReadUser** – Čtení informací o uživateli
- **UpdateUser** – Aktualizace informací o uživateli
- **RoleList** – Seznam aplikačních rolí v systému
- **AddRole** – Přiřazení aplikačních rolí uživateli
- **RemoveRole** – Odebrání aplikační role uživateli
- **RemoveRoleAll** – Odebrání všech aplikačních rolí uživateli
- **UserRoleList** – Seznam aplikačních rolí uživateli
- **UserList** – Seznam uživatelů systému

Bližší informace o rozhrání budou poskytnuty vítězi výběrového řízení.

[1] Veřejné směrnice SŽ naleznete na https://www.spravazeleznic.cz/o-nas/vnitrni-predpisy-spravy-zeleznic/dokumenty-a-predpisy.

2.4.1.2 PAM

PAM bude využíván pro přístup privilegovaných uživatelů. V systému se pro něj nepředpokládá zvláštní rozhraní, pokud bude administrace probíhat prostřednictvím webového rozhraní / tenkého klienta.

2.4.1.3 Kryptografie

Šifrování přenosu informací mezi 2. a 3. vrstvou musí probíhat prostřednictvím protokolu TLS verze 1.3. s kryptografickými algoritmy v souladu s aktuálně platným doporučením NUKIB[2]. Pro autentizaci vůči 3. vrstvě musí být použit certifikát dodaný zadavatelem.

Šifrování přenosu informací mezi 1 a 2. vrstvou musí probíhat prostřednictvím protokolu TLS verze 1.3. s kryptografickými algoritmy v souladu s aktuálně platným doporučením NUKIB. Pro autentizaci může být použit interní certifikát.

V případě, že spolupracující komponenty neumožňují provoz TLS 1.3. Může být použito TLS 1.2. do změny stavu.

2.4.1.4 Logování

Logovány budou zejména činnosti sběru dat. Logování musí probíhat v souladu s požadavky §22 vyhlášky 82/2018 SB. Mimo logování pro provozní a další účely aplikace musí být zaznamenávány tyto události:

- přihlášení (a odhlášení) k podpůrným aktivům (Uživatelé / Administrátoři),
- činnosti prováděné Administrátory (s využitím privilegovaných oprávnění):
    - k jakému zařízení přistoupili,
    - jaké otevřeli soubory a dokumenty (včetně logů),
    - změny konfigurace,
    - změny souborů,
    - v případě Uživatelů logování pokusů o přístup k těm souborům či dokumentům, ke kterým nemají přístupová oprávnění
    - apod.,
- činnosti vedoucí ke změně přístupových oprávnění:
    - změna hesla včetně pokusů o jejich provedení,
    - reset hesla včetně pokusů o jejich provedení,
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti Uživatelů:
    - zadání nesprávného přihlašovacího jména oprávněným Uživatelem,
    - zadání nesprávného hesla oprávněným Uživatelem,
    - zadání nesprávného přihlašovacího jména neoprávněnou osobou či strojem,
    - zadání nesprávného hesla neoprávněnou osobou či strojem,
    - pokus o přistoupení k souborům / dokumentům, ke kterým nemají oprávnění
    - apod.,
- zahájení a ukončení činností podpůrných aktiv,
- automatická varovná nebo chybová hlášení podpůrných aktiv:
    - HW (PC, NB, servery, virtuální servery, síťové prvky, sandbox, FW, IDS / IPS, Proxy atd.),
    - SW (aplikace / informační systémy), apod.,
- deaktivace běhu technických prostředků:

[2] Aktuální doporučení NUKIB naleznete na https://www.nukib.cz/cs/infoservis/doporuceni/

    - antivirový systém,
    - FW,
    - IDS / IPS apod.,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech:
    - přístup k logům,
    - pokusy o smazání logů,
    - pokusy o změnu logů apod.,
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení,
- specifika prostředí MS:
    - změna / přidání / odstranění záznamů v registrech,
    - změna / přidání / odstranění služeb (včetně start, stop a způsobu spouštění),
    - změna / přidání / odstranění / konfigurace ovladačů či aplikací,
    - změna / přidání / odstranění / konfigurace zařízení,

Záznam událostí musí formou logů obsahovat (v případě, že to informační systém / aplikace / zařízení umožňují):

- jednoznačnou identifikaci účtu provádějícího akci,
- činnosti informačního systému / aplikace / zařízení,
- datum, čas a podrobnosti důležitých událostí, například přihlášení a odhlášení,
- identitu nebo umístění zařízení, pokud je to možné, a identifikátor informačního systému / aplikace / zařízení,
- záznamy o úspěšných a odmítnutých pokusech o přístup k informačnímu systému / aplikaci / zařízení,
- záznamy o úspěšných a odmítnutých pokusech o přístup k datům a dalším zdrojům,
- změny konfigurace informačního systému / aplikace / zařízení,
- použití systémových nástrojů a aplikací,
- použití účtů s privilegovanými oprávněními,
- soubory, ke kterým bylo přistupováno, a typ přístupu,
- síťové adresy a protokoly,
- poplachy vyvolané systémem řízení přístupu,
- aktivace a deaktivace ochranných systémů, jako jsou antivirové systémy, sandbox, IDS / IPS, FW, Proxy atd.),
- záznamy transakcí provedených Uživateli v informačních systémech / aplikacích.

Systém logování musí podporovat napojení na budovaný log management a logování musí probíhat v některém ze standardních formátů. Logy samotné, musí být chráněny proti neoprávněnému přístupu a změně, aby byla zachována jejich Integrita a autenticita. Pro účely logování musí docházet k pravidelné (nejméně jednou za 24 h) synchronizaci systémového času.

Logování se bude řídí kapitolou 12 Provozní politiky prvků v působnosti systému řízení bezpečnosti informací, která bude poskytnuta vítězi výběrového řízení

2.4.1.5 Zálohování a obnova

Zálohování bude probíhat na úrovni OS oddíly aplikačních serverů formou Image jednou denně. Datové oddíly jsou zálohovány formou File Increment jednou denně.

Parametry zálohování dle požadavků dostupnosti naleznete v tabulce níže.

Požadavky na dostupnost	Frekvence záloh	Doba uložení záloh	Další požadavky	Frekvence testování
1	1x za týden plný	3 měsíce	---	2 roky
2	1x za den inkr. 1x za týden plný	3 týdny 3 měsíce	---	2 roky
3	1x za hodinu inkr. 1x za den plný 1x za měsíc plný	1 týden 3 týdny 3 měsíce	Využití redundance důležitých systémů	1 rok
4	1x za hodinu inkr. 1x za den plný 1x za měsíc plný	1 týden 3 týdny 3 měsíce	Využití redundance se zrcadlením v návrhu řešení. Zajištění náhradních technických aktiv v určeném čase.	1 rok

Z důvodu bezpečnosti a v souladu s požadavky NÚKIB musí být zajištěno offline uložení záloh.

Zálohování se bude řídí kapitolou 10 Provozní politiky prvků v působnosti systému řízení bezpečnosti informací, která bude poskytnuta vítězi výběrového řízení.

2.4.1.6 Použití komponent

Použité komponenty musí být v aktuální verzi a instalovanými bezpečnostními záplatami.

2.4.1.7 Bezpečnostní testy

Řešení musí projít před uvedením do provozu bezpečnostními testy dle standardů OWASP a testy SAST, DAST. Průchod testy bez nálezů je podmínkou akceptace díla.