



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



Definice rozhraní pro napojení eSSL a AIS pro potřeby úplného elektronického podání

Národní agentura pro komunikační a informační technologie, s. p.
Zapsaná v Obchodním rejstříku u Městského soudu v Praze, spisová značka A 77322

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz
IČ: 04767543



Obsah

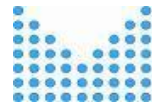
1	Kontext výstupu	1
2	Použité pojmy a zkratky	2
3	Vztažená legislativa a standardy	5
4	Odkazované dokumenty	5
5	Základní východiska problematiky rozhraní ÚEP	6
6	Definice rozhraní pro napojení eSSL a AIS	8
6.1	Obecný popis návrhu rozhraní a logického schématu	8
6.2	Sekvenční diagram ÚEP (ve vztahu eSSL a AIS).....	11
6.3	Popis a charakteristika technických aspektů rozhraní	15
6.3.1	SOAP rozhraní webových služeb	15
6.3.2	REST rozhraní webových služeb	18
6.3.3	HTML link rozhraní	22
6.4	Základní charakteristika ITSP ve vztahu k rozhraními ÚEP	23
7	Detailní popis jednotlivých rozhraní.....	23
7.1	Definice a popis jednotlivých rozhraní pro napojení eSSL v rámci ÚEP	23
7.2	Popis jednotlivých rozhraní ve vztahu k eSSL a ÚEP	26
7.2.1	Webové služby NSESSS.....	26
7.2.2	Webové služby ISDS	27
7.2.3	Interní API eSSL.....	28
7.2.4	Webové služby AIS	30
7.2.5	Webové služby komponenty ÚEP manažer.....	31
7.2.6	Webové rozhraní Formulářového serveru úředníka	32
7.3	Definice a popis jednotlivých rozhraní pro napojení AIS v rámci ÚEP	35
7.4	Popis jednotlivých rozhraní ve vztahu k AIS a ÚEP	37
7.4.1	Datové rozhraní	37
7.4.2	Webové služby NSESSS.....	38
7.4.3	Webové služby ÚEP manažera	40
7.4.4	Úlohové rozhraní.....	41
7.4.5	Stavové rozhraní.....	43



7.4.6	Webové rozhraní Formulářového serveru úředníka	44
7.4.7	Skartační rozhraní.....	46
7.4.8	Webové rozhraní eSSL.....	47

Přehled obrázků a tabulek

Obr. 1 - Schéma aktivit	1
Obr. 2 - Celkové schéma integrace ÚEP komponent bez ESB	9
Obr. 3 - Obecné schéma integrace komponent s využitím ESB	10
Obr. 4 - Obecný (sekvenční) postup obsluhy podání v eSSL a AIS.....	11
Obr. 5 - ÚEP rozhraní eSSL a další integrované systémy	26
Obr. 6 - ÚEP rozhraní AIS a integrované systémy.....	37
Tab. 1 - Vztážená legislativa a standardy	5
Tab. 2 - Odkazované dokumenty.....	5
Tab. 3 – Obecný (sekvenční) postup obsluhy podání v eSSL a AIS	11
Tab. 4 - Typ rozhraní: SOAP	15
Tab. 5 - Typ rozhraní: REST	18
Tab. 6 - Typ rozhraní: HTML link rozhraní	22
Tab. 7 - [eSSL] Webové služby NSESSS (AIFC).....	26
Tab. 8 - [ISDS] Webové služby (AIFC)	27
Tab. 9 - [eSSL] Interní API (AIFC).....	28
Tab. 10 - [AIS] Webové služby (AIFC)	30
Tab. 11 - [UEPM] Webové služby (AIFC).....	31
Tab. 12 - [FSU] Webové rozhraní (AIFC)	32
Tab. 13 - [AIS] Datové rozhraní (AIFC)	37
Tab. 14 - [eSSL] Webové služby NSESSS (AIFC)	38
Tab. 15 - [UPM] Webové služby (AIFC).....	40
Tab. 16 - [AIS] Úlohové rozhraní (AIFC)	41
Tab. 17 - [AIS] Stavové rozhraní (AIFC).....	43
Tab. 18 - [FSU] Webové rozhraní (AIFC)	44
Tab. 19 - [AIS] Skartační rozhraní (AIFC).....	46
Tab. 20 - [eSSL] Webové rozhraní (AIFC) – HTML link	47



1 Kontext výstupu

Tento dokument obsahuje definici všech rozhraní pro napojení elektronické spisové služby (eSSL) a Agendového informačního systému (AIS) pro potřeby úplného elektronického podání a procesování.

Návrh obsahuje i sekvenční schéma k automatickému předávání informací o případných dalších vynucených činnostech vyplývajících ze složitějších životních situací občana.

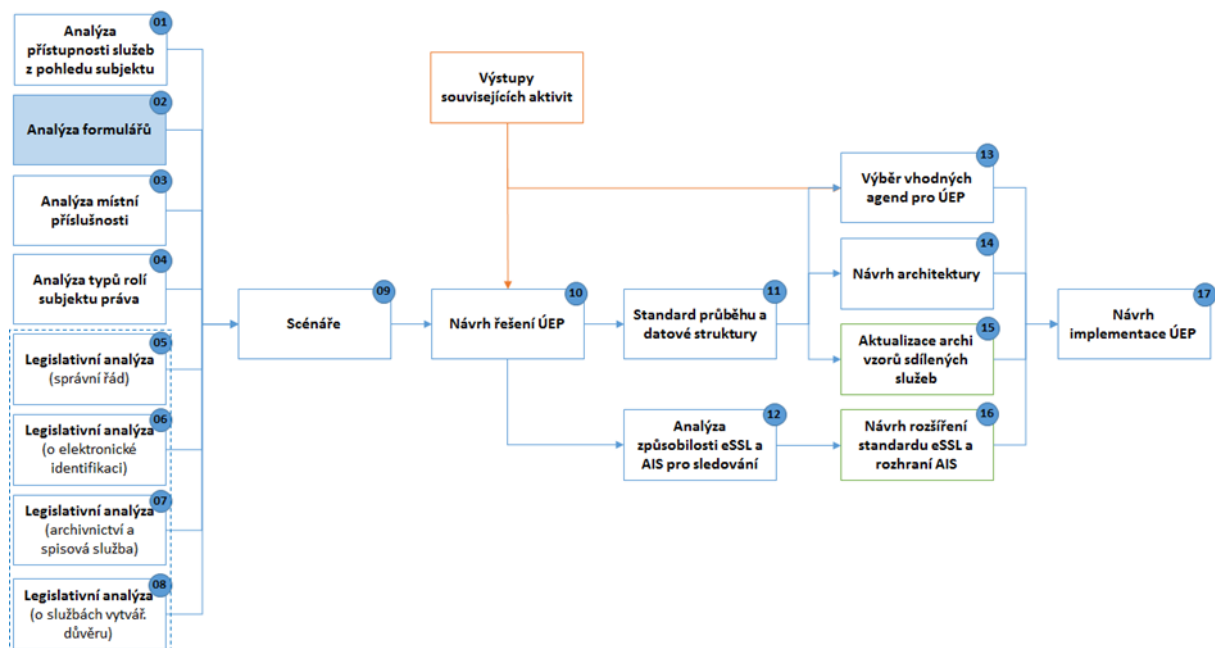
V jednotlivých kapitolách jsou popsána jednotlivá rozhraní a vztah mezi nimi navzájem včetně vazeb a vztahů s jednotlivými komponentami.

Zasazení v rámci projektu

Analýza zapojení eSSL a AIS do celkového řešení ÚEP je jednou z klíčových aktivit v rámci projektu „Vytvoření metodického rámce pro úplné elektronické podání“ k naplnění cíle:

Vytvořit koncepční, metodický a architektonický rámec pro zavádění principu úplného elektronického podání – efektivního využívání prvků elektronické veřejné správy fyzickými a právníckými osobami jakožto klienty služeb veřejné správy.

V rámci jednotlivých aktivit je role analýzy znázorněna na následujícím schématu modře.



Obr. 1 - Schéma aktivit



2 Použité pojmy a zkratky

Pojem/zkratka	Význam
Úplné elektronické podání (ÚEP)	Úplné elektronické podání představuje stav, kdy při elektronickém podání do většiny agend subjekt práva dokládá pouze údaje, které jsou mimo informační systémy veřejné správy, a to výhradně v elektronické podobě. ÚEP řeší i plné elektronické procesování podání klienta veřejné správy.
Úplné elektronické plné procesování (ÚEPP)	Koncept, který logicky navazuje na ÚEP. Řeší všechny fáze obsluhy předmětu podání končící zaslaným výsledkem procesního případu (dokument). ÚEP se jeví jako podmnožina ÚEPP.
Portál veřejné správy (PVS)	Portál ČR, který je svým zaměřením určen pro širokou veřejnost, státní správu a samosprávu, státní i soukromé organizace včetně podnikatelů, živnostníků a cizinců. Portál je rozdělen na čtyři informační sekce pro občany, pro podnikatele, pro cizince a pro orgány veřejné správy.
Klient veřejné správy	Subjekt práva
Portál občana (PO)	Portál občana – interaktivní a transakční část Portálu veřejné správy
Interaktivní a transakční, samoobslužný portál veřejné správy (ITSP)	Portál ÚEP dané organizace veřejné správy, který nabízí on-line služby (elektronické podání)
Elektronická spisová služba (eSSL)	Je informační systém určený ke správě dokumentů ve smyslu ustanovení § 2 písm. l) a § 63 odst. 3 a 4 zákona č. 499/2004 Sb. ESSL je základní evidenční pomůcka spisové služby vykonávané v elektronické podobě. ESSL je vždy nadřazen všem samostatným evidencím používaným na jednotlivém pracovišti. Dokumenty evidované v samostatných evidencích nejsou zpravidla evidovány v ESSL. V ESSL lze spravovat elektronické dokumenty a metadata analogových dokumentů. Pracoviště zabezpečí ESSL proti pozměňování, neoprávněnému nebo nahodilému přístupu, zničení nebo neoprávněnému zpracování údajů, jakož i proti jinému zneužití. Pokud pracoviště používá v ESSL zkratky, je povinno uvést jejich seznam s vysvětlivkami do přílohy svého spisového řádu a tento seznam průběžně aktualizovat.



Agendový informační systém (AIS)	Informační systém veřejné správy, který slouží k výkonu agendy, využívání elektronických formulářů nebo elektronické identifikaci.
Rozhraní ÚEP	
Dokument	Je v širším slova smyslu každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či elektronické, který je spojen s činností původce (byl jím vytvořen nebo mu byl doručen), včetně evidenčních pomůcek jakéhokoli druhu a formy.
Metadata	Obsahují data popisující souvislosti, obsah a strukturu dokumentu a jeho správu v průběhu času.
Webová služba ÚEP	Rozhraní pro technické interakce, více 0
Webové rozhraní ÚEP	Rozhraní pro technické a uživatelské interakce, viz 0
Procesní případ ÚEP	Fáze obsluhy předmětu podání. Jde o plně elektronickou obsluhu ze strany OVS pomocí nástrojů a rozhraní, které usnadňují procesování případu včetně poskytování auditních stop pro řídicí a auditní orgány.
Datová schránka	Je elektronické úložiště, které je určeno k doručování orgány veřejné moci, k provádění úkonů vůči orgánům veřejné moci a k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob, umožňuje-li to povaha dokumentu.
Integrační datová sběrnice (ESB)	Platforma pro řízení datové výměny a orchestrace dat.
Komponenta Procesní manažer (BPM)	Platforma, která zprostředkovává řízení procesu vyřízení procesního případu.
Interaktivní on-line služba (IOLS)	Individuální poskytování personalizovaných informací různými informačními kanály.



Transakční on-line služba (TOLS)	Typicky podání všech typů, včetně provedení platby nebo rezervace termínu pro prezenční jednání, získání potvrzení a doručení rozhodnutí úřadu.
Integrovaná transakční on-line služba (ITOLS)	Propojuje informační, interakční a transakční on-line služby více úřadů dohromady na jednom místě, zakrývající tak pro identifikovaného autentizovaného a autorizovaného klienta skutečnou složitost a komplexnost výkonu působnosti veřejné moci v ČR.
Formulářový server ITSP (FS ITSP)	Formulářový server je klíčová komponenta ITSP, resp. ÚEP. Hlavní úlohou formulářového serveru je poskytnout funkcionality umožňující maximálně efektivně, bezpečně, v minimálním čase a s minimálním úsilím navrhnout, implementovat a provozovat elektronické formuláře dostupné prostřednictvím ITSP. Formulářová komponenta povinně podporuje datové standardy pro definici vzhledu funkcionalit formuláře a datové standardy samotných dat formuláře mimo jiné i dle standardu W3C XForms 2.0. ITSP a v rámci něj formulářový server, je vystavený na straně klienta veřejné správy a slouží jako základní komponenta podání v rámci ÚEP.
Formulářový server úředníka (FSÚ)	Tento formulářový server je sadou funkcionalit rovnocenný FS ITSP. Pomocí rozhraní slouží primárně jako prohlížeč komponenta, ale v některých případech jde i o editaci (doplnění) podání (např. v případě doplnění v rámci bezvadnosti podání).
Subjekt uživatele	Subjekt uživatele, který vlastní identitu, kterou je přistupováno k ITSP. Jedná se fyzickou nebo právnickou osobu. Fyzická osoba může pracovat pro právnickou osobu a do ITSP se hlásí jménem právnické osoby. Tato právnická osoba – subjekt uživatele však může zastupovat další fyzické či právnické osoby – subjekt dat. Při zastupování subjekt uživatele požaduje přístup k datům subjektu dat.
Subjekt dat	Subjektem dat je fyzická anebo právnická osoba, která je právoplatným vlastníkem dat. Data jsou v registrech, AIS či jiných systém spojena s touto osobou a zpravidla obsahují informace o právě této osobě.
OVS	Orgán veřejné správy
eGON Service Bus (eGSB)	Jde o integrační nástroj (specializované sdílené referenční rozhraní ISVS dle zákona o ISVS)
Elektronická podatelna (EPO)	Je zařízením elektronického systému spisové služby umožňující příjem, vyhledávání, předávání a odesílání elektronických dokumentů. Slouží k provádění úkonů prostřednictvím datové schránky a veřejné sítě internet (e-mailu), tj. k příjmu, vyhledávání, předávání a odesílání elektronických dokumentů, které byly prostřednictvím datové schránky nebo internetem doručeny nebo budou jejich prostřednictvím odeslány.



3 Vztažená legislativa a standardy

Tab. 1 - Vztažená legislativa a standardy

Název zákona nebo standardu
Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.
Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.
Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.
Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.
Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.
Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce.
Zákon č. 250/2017 Sb., o elektronické identifikaci.
Usnesení vlády České republiky č. 347/2017 k realizaci úplného elektronického podání a povinnému přijímání elektronických faktur.
Zákon č. 111/2009 Sb., o základních registrech

4 Odkazované dokumenty

Tab. 2 - Odkazované dokumenty

Dokument	Soubor	Zkratka dokumentu
Business scénáře ÚEP	eGov_UEP_Business_scenare.docx	UEP_BUSCE
Specifikace požadavků na ÚEP	eGov_UEP_Specifikace_pozadavku.docx	UEP_POZ
Architektonický vzor ÚEP	eGov_UEP_Archiektonicky_vzor_UEP.docx	UEP_ARCH
Technický standard ITSP	eGov_UEP_Technicky_standard_pozadavky.docx	UEP_STITSP



5 Základní východiska problematiky rozhraní ÚEP

Pro potřeby dalšího rozpracování problematiky rozhraní ÚEP je třeba ohraničit a definovat základní východiska, kdy se na těchto východiscích zakládají následná tvrzení, definice a standardy. Za ÚEP je tedy v kontextu rozhraní považováno podání klienta veřejné správy směrem k úřadu veřejné správy, kdy:

- podáním a procesováním se rozumí celý proces realizovaný sadou rozhraní, a to rozhraními obsluhy samotného úkonu podání klientem veřejné správy, přes rozhraní v rámci vnitřního procesu obsluhy podání (jako procesního případu) v rámci celé veřejné správy, až po rozhraní obsluhující doručení elektronického výsledku procesního případu (např. v rámci konkrétní, příslušné agendy),
- data veškerých podání jsou připravena využitím dostupných rozhraní on-line služeb veřejné správy,
- v rámci rozhraní konkrétních on-line služeb se v jednotlivých podáních klienta veřejné správy automaticky doplňují odvozená data, provádějí výpočty a kontroly dat,
- v rozhraní on-line služeb jsou automaticky doplňována známá data a po klientovi není požadováno opakované podávání již jednou poskytnutých dat (striktně dle principu Only Once),
- z rozhraní klienta veřejné správy jsou data podávána přes další rozhraní v podobě standardně strukturovaného a strojově zpracovatelného datového souboru a souvisejících příloh,
- rozhraní jsou pouze digitální, žádná část dat podání není realizována v listinné podobě anebo elektronické podobě, kterou nelze strojově zpracovat a vytěžit data pro následné zpracování v rámci procesního případu ÚEP,
- podání je pomocí různých účelových rozhraní a v celém svém životním cyklu řešeno elektronicky, tzn. nedochází ke konverzi do listinných formátů v průběhu podávání a následného řešení ÚEP případu daným působnostním úřadem,
- z jednoho jednotného prostředí a rozhraní je možné realizovat podání do agend více úřadů či rezortů (tzv. jednotné podání realizované prostřednictvím integrované transakční on-line služby (ITOLS)),
- podání je učiněno rozhraním integrovaným se zákonným kanálem rozhraní datových schránek,
- podání je možné přes rozhraní ITSP a PVS – Portálu občana sledovat během životního cyklu řešení (jako procesního případu) v rámci celé veřejné správy ČR.

Na základě výše uvedených východisek lze pro účel tohoto výstupu konstatovat, že jde výhradně o elektronické podání (dokument) připravené a doručené v rámci prostředí a rozhraními, které nabízí veřejná správa v rámci svých řešení dle standardů určovaných ÚEP (ev. budoucích návazných standardů např. ÚEPP).



Podání je doručeno standardní, zákonnou cestou tedy zákonným kanálem prostřednictvím služeb Informačního systému datových schránek. Doručeno je prostřednictvím rozhraní elektronické podatelny do elektronické spisové služby.

Podání je dále procesováno buď rozhraními a procesními nástroji eSSL, nebo je tato úloha obsloužena rozhraními agendových informačních systémů (AIS).

Informace o procesních stavech jednotlivých podání (bez ohledu na to ve kterých systémech jsou procesovány) jsou následně standardními rozhraními předávány do příslušných centrálních portálů (PVS a ITSP).

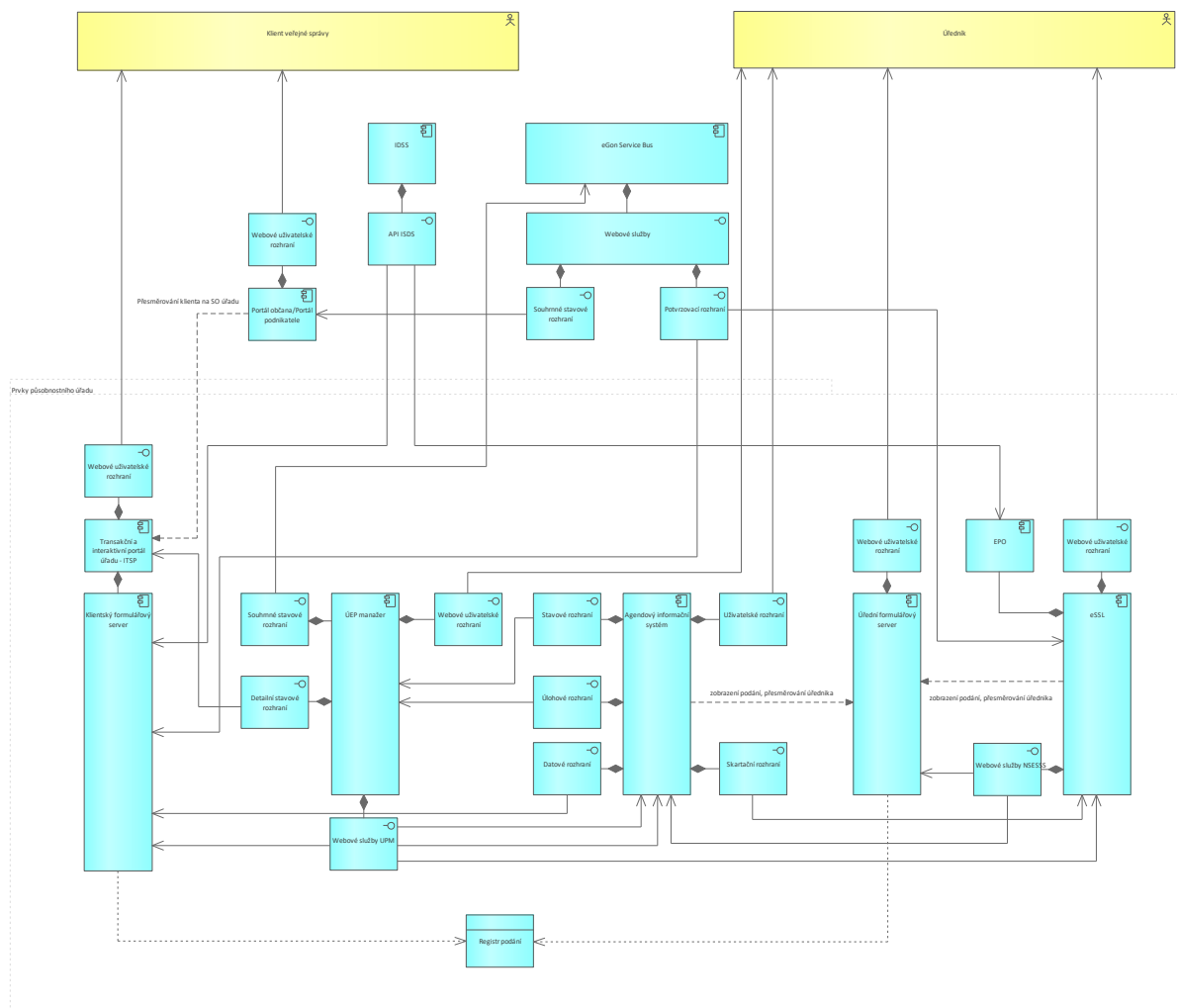
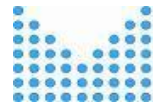
Výsledek (dokument) procesního případu podání je následně doručen příslušným rozhraním zpět klientovi veřejné správy zákonným kanálem.



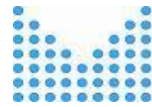
6 Definice rozhraní pro napojení eSSL a AIS

6.1 Obecný popis návrhu rozhraní a logického schématu

Architektura řešení systémové podpory ÚEP se skládá z mnoha logických aplikačních komponent poskytujících specifické služby v oblasti přípravy, odeslání, příjmu, zpracování a sledování stavu podání. Návrh celkové architektury systémové podpory ÚEP je uveden v samostatném dokumentu [UEP_ARCH]. Tento dokument obsahuje popis a specifikaci rozhraní a integrací mezi eSSL a AIS na jedné straně a ostatními aplikačními komponentami ÚEP na straně druhé. Spolupráce komponent ÚEP může být v případě méně rozsáhlých IT prostředí působnostních organizací řešena přímou integrací komponent anebo prostřednictvím integrační platformy ESB. Níže jsou znázorněna schémata integrace a vzájemného využití logických komponent ÚEP a jejich rozhraní při zapojení platformy ESB a pro případ přímé integrace.

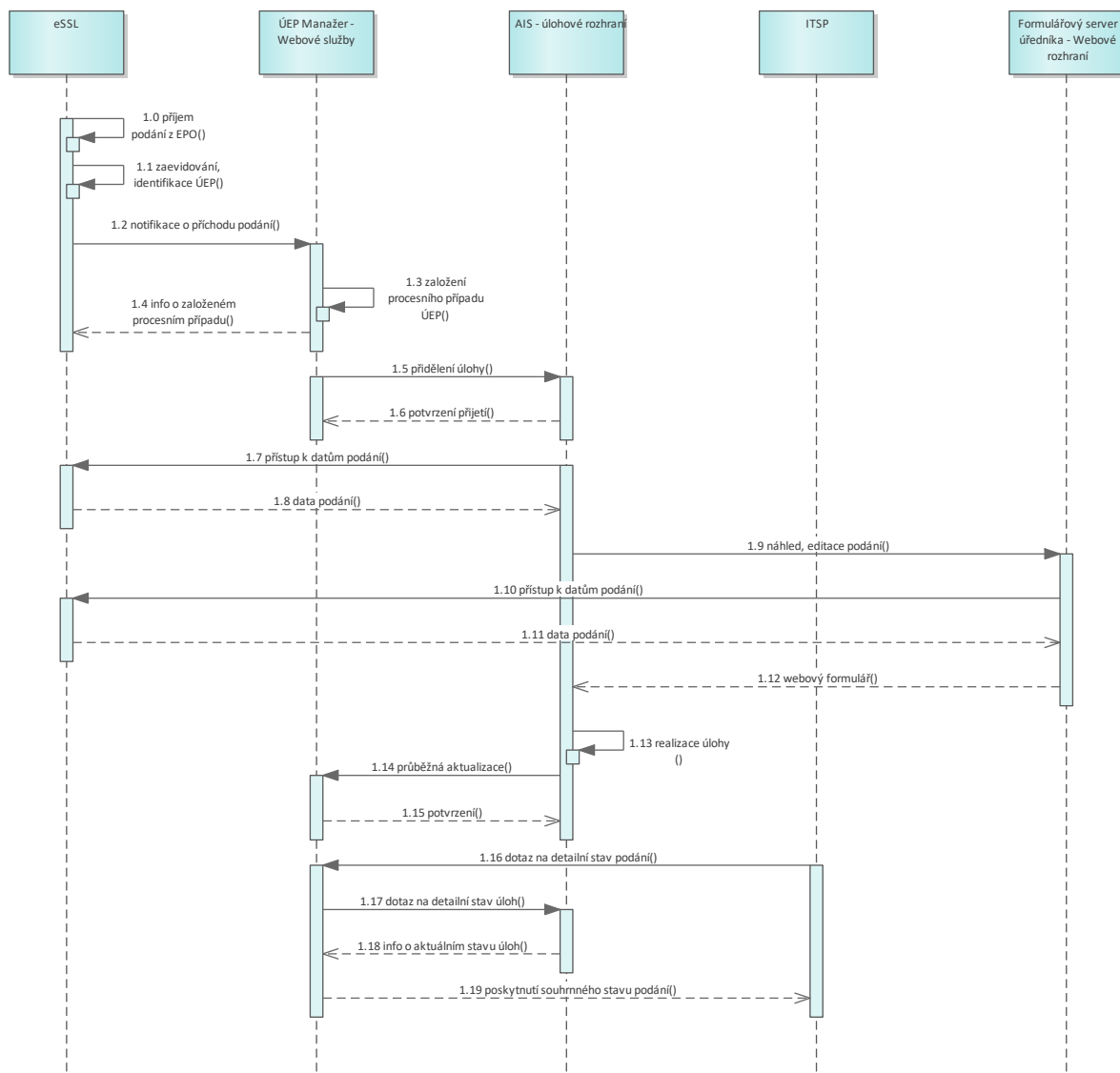


Obr. 2 - Celkové schéma integrace ÚEP komponent bez ESB



6.2 Sekvenční diagram ÚEP (ve vztahu eSSL a AIS)

Na zpracování ÚEP případů spolupracuje více komponent ÚEP. Vzájemná komunikace eSSL, AIS a ostatních integrovaných komponent ÚEP je znázorněna v sekvenčním diagramu na Obr. 4.



Obr. 4 - Obecný (sekvenční) postup obsluhy podání v eSSL a AIS

Tab. 3 – Obecný (sekvenční) postup obsluhy podání v eSSL a AIS

Název komunikace	Využitě rozhraní	Popis komunikace
------------------	------------------	------------------



1.0 příjem podání z EPO	Interní rozhraní eSSL	Z EPO jsou manuálně nebo automaticky předána do eSSL data podání
1.1 zaevidování, identifikace ÚEP	Interní funkcionality eSSL	eSSL na základě metadat datové zprávy provede zatřídění a zaevidování dokumentu, případně je tato operace provedena manuálně, pokud eSSL nepodporuje automatické operace tohoto druhu. Využitím metadat eSSL identifikuje dokumenty obsahující data ÚEP.
1.2 notifikace o příchodu podání	Webové služby UPM	eSSL notifikuje komponentu ÚEP manažer o příchodu nového podání. Obsahem notifikace jsou metadata o obdrženém dokumentu. Samotná data podání nejsou předávána.
1.3 založení procesního případu	Vnitřní funkcionality UPM	ÚEP manažer založí nový procesní případ podání.
1.4 informace o založeném procesním případě	Webové služby UPM	ÚEP manažer zašle zpět eSSL potvrzení o založení procesního případu. Jedná se o synchronní odpověď na obdržené volání.
1.5 přidělení úlohy	Úlohové rozhraní AIS	ÚEP manažer zavolá webové rozhraní AIS s požadavkem na obsluhu konkrétní ÚEP úlohy.
1.6 potvrzení přijetí	Úlohové rozhraní AIS	AIS potvrzuje přijetí ÚEP úlohy.
1.7 přístup k datům podání	eSSL NSESSS	Pokud je potřeba v rámci zpracování úlohy v AIS přistoupit k datům ÚEP, přistupuje k nim AIS jménem přihlášeného uživatele využitím standardních služeb dle standardu NSESSS. Pokud je vyžadován pouze náhled dat bez předání do AIS, je obsluha AIS přesměrována na uživatelské webové rozhraní eSSL.
1.8 data podání	eSSL NSESSS	eSSL vrátí AIS požadovaná data podání. V případě, že je



		komunikace zprostředkována ESB a je požadován pouze subset ÚEP informací, může ESB provést transformaci či extrakci dat do podoby požadované AIS.
1.9 náhled, editace podání	HTML link – webové rozhraní Formulářového serveru úředníka	Pokud řešitel v rámci obsluhy ÚEP úlohy v AIS požaduje náhled na ÚEP data, je přesměrován na formulářový server úředníka, který data úředníkovi zobrazí ve shodné podobě, v jaké je zadával koncový klient veřejné správy.
1.10 přístup k datům podání	eSSL NSESSS	AIS v aktivitě 1.9 nepředává data podání formulářovému serveru úředníka. AIS nemusí nutně daty ÚEP disponovat. AIS požádá Formulářový server úředníka o zobrazení podání s uvedením identifikátoru podání. Formulářový server úředníka si za účelem zobrazení dat podání vyžádá data přímo z eSSL využitím standardního rozhraní eSSL dle NSESSS.
1.11 data podání	eSSL NSESSS	eSSL vrátí Formulářovému serveru úředníka požadovaná data eSSL
1.12 webový formulář	Webové rozhraní Formulářového serveru úředníka	Formulářový server úředníka zobrazí řešiteli formulář s daty podání. V okamžiku ukončení zobrazení odstraní data podání obdržená z eSSL.
1.13 realizace úlohy	Interní funkcionality AIS	S využitím systémové podpory AIS odpovědní řešitelé realizují svěřené úlohy.
1.14 průběžná aktualizace	Webové služby UPM	AIS notifikuje o dokončení a průběhu realizace svěřených úloh komponentu ÚEP manažer.
1.15 potvrzení	Webové služby UPM	Přijetí notifikace ÚEP manažerem je potvrzeno AIS ve formě odpovědi na volání AIS.
1.16 dotaz na detailní stav podání	Stavové rozhraní UPM	V případě požadavků na zobrazení aktuálního stavu



		podání ze strany klienta veřejné správy anebo řešitele ÚEP v úřadu, je dotaz položen komponentě ÚEP manažer, která doptává všechny zúčastněné AIS na stav obsluhy jim svěřených úloh.
1.17 dotaz na detailní stav úloh	Stavové rozhraní AIS	V reakci na požadavek na zobrazení aktuálního stavu podání doptává ÚEP manažer využitím stavového rozhraní AIS všechny AIS zúčastněné na procesu obsluhy procesního případu na detailní stav obsluhy svěřených ÚEP úloh.
1.18 informace o aktuálním stavu úloh	Stavové rozhraní AIS	AIS vrací shodně, standardně strukturované informace o stavu svěřených ÚEP úloh.
1.19 poskytnutí souhrnného stavu podání	Stavové rozhraní UPM	V okamžiku, kdy ÚEP manažer obdrží informace o stavu zpracování ÚEP úloh ve všech zúčastněných AIS, zkompletuje tyto informace a poskytne v konsolidované podobě zpět ITSP.



6.3 Popis a charakteristika technických aspektů rozhraní

Pro integraci eSSL, AIS a ostatních komponent ÚEP je využito několik technologických typů rozhraní:

- SOAP rozhraní webových služeb pro načítání, zápis dat a volání vzdálených metod,
- REST rozhraní webových služeb pro načítání a případně zápis dat,
- HTML link rozhraní pro přeměrování uživatele z rozhraní jedné komponenty ÚEP do rozhraní jiné komponenty ÚEP,
- webové rozhraní.

Požadavky na implementaci jednotlivých technologických typů rozhraní jsou uvedeny v následujících kapitolách.

6.3.1 SOAP rozhraní webových služeb

Preferovaným způsobem integrace a komunikace mezi komponentami ÚEP je využití SOAP webových služeb. SOAP webové služby pracují s daty ve formátu XML, který je i nativním formátem standardu XForms, jež je zároveň využit pro výstavbu ITSP. SOAP a XML dále poskytuje prověřené a efektivní metody validace dat, konzumentských požadavků a odpovědí zdrojových systémů.

Parametry a požadavky na SOAP rozhraní využitě pro integrace v rámci ÚEP jsou uvedeny v Tab. 4.

Tab. 4 - Typ rozhraní: SOAP

Typ rozhraní: SOAP	
Využití	<p>SOAP rozhraní je v rámci integrace ÚEP komponent využito pro:</p> <ul style="list-style-type: none"> ▪ načítání dat (např. číselníků) z jiné komponenty ÚEP, ▪ modifikace dat spravovaných jinou komponentou ÚEP, ▪ pořizování dat spravovaných jinou komponentou ÚEP, ▪ mazání dat spravovaných jinou komponentou ÚEP, ▪ vzdálené volání metod, ▪ notifikace stavů a změn stavů v rámci procesu zpracování ÚEP případů.
Integrace	<p>V případě přímé integrace mezi komponentami ÚEP musí být SOAP rozhraní implementováno na straně zdrojové ÚEP komponenty.</p> <p>V případě, kdy je pro integraci zvolena integrační platforma ESB, může být využito nativní rozhraní ÚEP komponenty, přičemž SOAP rozhraní musí být implementováno a publikováno na ESB.</p> <p>Organizace s rozsáhlou IT infrastrukturou provozující větší počet informačních systémů zapojených do procesů ÚEP by měly integrovat aplikační komponenty ÚEP využitím integrační sběrnice ESB. Je tak zamezeno přímé integraci systémů a vytvoření tzv. „full mash“ integrace, která je velmi obtížně udržitelná a spravovatelná.</p>



Způsob autentizace a autorizace.	<p>Autentizace na úrovni systémů je realizována klientským systémovým certifikátem. V případě, kdy komunikace probíhá přímo mezi jednotlivými hlavními komponentami je pro konzumentské komponenty vydán klientský certifikát podepsaný autoritou, které zdrojová komponenta důvěřuje. Zdrojová komponenta udržuje autorizační informace a provádí autorizaci na základě informací z certifikátu přístupujícího konzumentského systému. Zdrojová komponenta musí podporovat načtení informací o certifikátu a předání těchto informací do procesu autorizace (např. ve formě http header). Doporučeným atributem z klientského certifikátu využitým pro autorizaci je sériové číslo certifikátu. Pro autentizaci a autorizaci je vhodné vytvořit interní certifikační autoritu, která bude klientské certifikáty vydávat a podepisovat. Při generování certifikátů je možné požadovat vygenerování certifikátu s vlastním sériovým číslem. Doporučeným postupem je využití unikátního GUID v podobě hexadecimálního čísla (v textové reprezentaci).</p> <p>V případě využití ESB provádí autorizaci volání na základě klientského certifikátu ESB. Na straně ESB může být implementována mediační sekvence provádějící autorizaci volání, kterou lze jednoduše začlenit do jakékoli implementované a publikované služby. Zdrojová ÚEP komponenta umožňuje jakékoliv volání ze strany ESB, jelikož důvěřuje autentizaci a autorizaci provedené na straně ESB. ESB provádí autentizaci a autorizaci konzumentských systémů stejným způsobem jako zdrojová komponenta, tedy způsobem popsáným výše.</p>
Využití rozhraní	Rozhraní je využito ÚEP komponentami v případě přímé integrace anebo ESB v situaci, kdy je komunikace s ÚEP komponentami zprostředkována ESB. Konzumentem služeb je ale v obou případech ITSP.

Dostupnost	<p>Dostupnost rozhraní musí odpovídat SLA konzumentských systémů a míře dopadu případné nefunkčnosti rozhraní na služby poskytované klientským systémem. V případě selhání rozhraní, musí rozhraní vrátit odpovídající HTTP error kód, SOAP chybu v případě selhání na úrovni SOAP anebo business chybu v těle SOAP odpovědi, v případě, že došlo k business chybě rozhraní.</p> <p>V případě plánované odstávky rozhraní (kdy není dostupná celá služba rozhraní, tedy např. celé HA řešení rozhraní), musí být provoz přesměrován na jinou komponentu vracející přesně definovanou zprávu s informací o nedostupnosti rozhraní. Všechny ostatní komponenty ÚEP detekují takovou zprávu a reagují dle požadavků specifických pro jednotlivé komponenty (např. zobrazením konkrétní chybové zprávy klientovi).</p>
------------	--



Odezva	SOAP rozhraní by mělo v synchronním módu obsloužit požadavek do 5 sekund. V případě delší odezvy by měla být využita asynchronní komunikace. Konzumentské ÚEP komponenty poskytující uživatelské rozhraní koncovým klientům v případě asynchronní služby zobrazí uživateli indikátor probíhající operace (např. progress spinner) informující o probíhající operaci případně s doplňující zprávou o možnosti delšího trvání příslušné operace.
Typ rozhraní	Rozhraní může komunikovat v synchronním i asynchronním módu. V případě asynchronního módu je komunikace realizováno dvěma voláními: <ul style="list-style-type: none">▪ volání zdrojového systému konzumentskou komponentou, resp. zaslání požadavku,▪ volání konzumentského systému zdrojovou komponentou, resp. zaslání odpovědi. V případě asynchronního rozhraní tedy musí být implementovány SOAP webové služby jak na straně zdrojové ÚEP komponenty, tak na straně konzumentské ÚEP komponenty.
Monitoring	Doporučenými monitorovanými parametry rozhraní a zároveň parametry, které je vhodné ukotvit v případné smlouvě o poskytování služeb provozu (SLA/katalogové listy) jsou: <ul style="list-style-type: none">▪ dostupnost - doporučeným způsobem monitoringu dostupnosti SOAP ÚEP rozhraní je pravidelné spouštění end-to-end testů, tedy simulování operací konzumentské ÚEP komponenty. Za tímto účelem musí být pro každé rozhraní definován minimálně jeden testovací scénář, nemající dopad na obsluhovaná data a maximálně reprezentativně vypovídající o stavu SOAP rozhraní. End-to-end test je vhodné spouštět s minimální periodicitou 15 minut,▪ odezva - odezvu je vhodné monitorovat dvěma způsoby:<ol style="list-style-type: none">a. end-to-end testem výše uvedeným způsobem, přičemž test mimo dostupnosti sleduje i odezvu vybraných kroků testovacího scénáře,b. sledováním reálných volání - všechna provedená volání, resp. základní informace o volání jako jsou, datum a čas zahájení volání, datum a čas dokončení volání a status obsluhy volání jsou zapisována do transakčního logu, nad kterým jsou pravidelně reportovány doby obsluhy a průměrné doby obsluhy požadavků.
Obsluha chyb	Rozhraní musí obsluhovat 3 typy chyb: <ul style="list-style-type: none">▪ chyby autentizace a autorizace,▪ technické chyby rozhraní,▪ business chyby rozhraní.



	<p>V případě chyby autentizace, tedy přístupu bez platného klientského certifikátu, je odmítnuto připojení k rozhraní na úrovni webového či aplikačního serveru (ERR_BAD_SSL_CLIENT_AUTH_CERT).</p> <p>V případě platného certifikátu, ale neautorizovaného volání, vrátí rozhraní konzumentské komponentě chybový kód HTTP 401 (Unauthorized) a zároveň zapíše do auditního žurnálu záznam o neautorizovaném volání.</p> <p>V případě technické chyby musí rozhraní vrátit odpovídající chybový HTTP response code (zejména 500 INTERNAL SERVER ERROR) s odpovídající textovou zprávou informující konzumentskou ÚEP komponentu o příčině selhání.</p> <p>V případě business chyby je klientovi z pohledu komunikace vrácena standardní validní odpověď, přičemž v těle SOAP odpovědi je uvedena přesně strukturovaná informace o vniklé business chybě. Konzumentská ÚEP komponenta chybu v odpovědi identifikuje a na chybu reaguje dle předem definovaného postupu.</p>
--	---

6.3.2 REST rozhraní webových služeb

Pro specifické případy komunikace komponent tvořících systémovou podporu ÚEP v úřadech může být využita REST (Representational state transfer) architektura rozhraní webových služeb. Parametry a požadavky na REST rozhraní využité pro integrace v rámci ÚEP jsou uvedeny v Tab. 5.

Tab. 5 - Typ rozhraní: REST

Typ rozhraní: REST	
Využití	<p>REST rozhraní může být v rámci integrace ÚEP komponent využito pro:</p> <ul style="list-style-type: none"> ▪ načítání dat (např. číselníků) z jiné komponenty ÚEP využitím metody HTTP GET - Rozhraní může být využito pro načítání dat v případech, kdy požadavek na data neobsahuje velké množství parametrů. V případě dotazu obsahujícího velký počet předávaných parametrů, kde existuje riziko překročení maximální délky URL, která je akceptována firewally či jinými prvky, je doporučeným typem rozhraní SOAP. Vložení více parametrů do BODY HTTP GET není podporováno. V případě využití REST HTTP GET je preferovaným formátem odpovědi XML, které je zároveň nativním formátem, se kterým pracuje ITSP. Pokud je vyžadováno, je možné využít i JSON formát odpovědi. V takovém případě ITSP provádí konverzi mezi JSON a XML, což s sebou přináší dodatečnou režii. Preferovaným formátem odpovědi je proto XML, ▪ modifikace dat spravovaných jinou komponentou ÚEP využitím metody HTTP PUT - V případě že rozhraní vrátí v reakci na PUT požadavek nějaký zdroj, je preferovaným



	<p>formátem zdroje XML podobně jako v případě HTTP GET metody,</p> <ul style="list-style-type: none">▪ pořízování dat spravovaných jinou komponentou ÚEP využitím metody HTTP POST - V případě že rozhraní vrací v reakci na POST požadavek nějaký zdroj, je preferovaným formátem zdroje XML podobně jako v případě HTTP GET metody,▪ mazání dat spravovaných jinou komponentou ÚEP využitím metody HTTP DELETE - V případě že rozhraní vrací v reakci na POST požadavek nějaký zdroj, je preferovaným formátem zdroje XML podobně jako v případě HTTP GET metody.
Integrace	<p>V případě přímé integrace mezi komponentami ÚEP a využití REST rozhraní musí být REST rozhraní implementováno na straně zdrojové ÚEP komponenty.</p> <p>V případě, kdy je pro integraci zvolena integrační platforma ESB, může být využito nativní rozhraní ÚEP komponenty, přičemž REST rozhraní může být implementováno a publikováno na ESB za předpokladu, že ESB komponenta provoz REST rozhraní podporuje.</p> <p>Organizace s rozsáhlou IT infrastrukturou provozující větší počet informačních systémů zapojených do procesů ÚEP by měly integrovat aplikační komponenty ÚEP využitím integrační sběrnice ESB. Je tak zamezeno přímé integraci systémů a vytvoření tzv. „full mash“ integrace, která je velmi špatně udržitelná a spravovatelná. V případě, že ESB komponenta nepodporuje provoz REST rozhraní, je možné pro publikaci REST webových služeb využít API gateway.</p>
Způsob autentizace a autorizace.	<p>Autentizace na úrovni systémů je realizována klientským systémovým certifikátem. V případě, kdy komunikace probíhá přímo mezi jednotlivými hlavními komponentami je pro konzumentské komponenty vydán klientský certifikát podepsaný autoritou, které zdrojová komponenta důvěřuje. Zdrojová komponenta udržuje autorizační informace a provádí autorizaci na základě informací z certifikátu přistupujícího konzumentského systému. Zdrojová komponenta musí podporovat načtení informací o certifikátu a předání těchto informací do procesu autorizace (např. ve formě http header). Doporučeným atributem z klientského certifikátu využitým pro autorizaci je sériové číslo certifikátu. Pro autentizaci a autorizaci je vhodné vytvořit interní certifikační autoritu, která bude klientské certifikáty vydávat a podepisovat. Při generování certifikátů je možné požadovat vygenerování certifikátu s vlastním sériovým číslem. Doporučeným postupem je využití unikátního GUID v podobě hexadecimálního čísla (v textové reprezentaci).</p> <p>V případě využití ESB provádí autorizaci volání na základě klientského certifikátu ESB. Zdrojová ÚEP komponenta umožňuje jakékoliv volání ze strany ESB, jelikož důvěřuje autentizaci a autorizaci provedené</p>



	na straně ESB. ESB provádí autentizaci a autorizaci konzumentských systémů stejným způsobem jako zdrojová komponenta, tedy způsobem popsáným výše.
Využití rozhraní	Rozhraní je využito ÚEP komponentami v případě přímé integrace anebo ESB v situaci, kdy je komunikace s ÚEP komponentami zprostředkována ESB.
Dostupnost	Dostupnost rozhraní musí odpovídat SLA konzumentských systémů a míře dopadu případné nefunkčnosti rozhraní na služby poskytované klientským systémem. V případě selhání rozhraní, musí rozhraní vrátit odpovídající HTTP error kód anebo XML (či JSON) zprávu v případě, že došlo k business chybě rozhraní. V případě plánované odstávky rozhraní (kdy není dostupná celá služba rozhraní, tedy např. celé HA řešení rozhraní), musí být provoz přesměrován na jinou komponentu vracující přesně definovanou zprávu z informací o nedostupnosti rozhraní. Všechny ostatní komponenty ÚEP detekují takovou zprávu a reagují dle požadavků specifických pro jednotlivé komponenty (např. zobrazením konkrétní chybové zprávy klientovi).
Odezva	REST rozhraní by mělo v synchronním módu obsloužit požadavek do 5 sekund. V případě delší odezvy by měla být využita asynchronní komunikace. Konzumentské ÚEP komponenty v reakci na návratový HTTP kód 201 zjistí z dočasného zdroje informace o předpokládaném čase obsloužení požadavku (poskytnutí zdroje) a v případě komponenty s uživatelským rozhraní zobrazí uživateli indikátor probíhající operace (např. progres bar) s vizuálním zobrazením uplynulé a očekávané doby zpracování požadavku.
Typ rozhraní	Rozhraní může komunikovat v synchronním i asynchronním módu. V případě asynchronního módu je konzumentskému systému vrácena namísto finální odpovědi odpověď dočasná. Rozhraní by v takovém případě mělo namísto HTTP kódu 201 (Created) vrátit HTTP kód 202 (Accepted). Tento kód informuje klienta, že požadavek byl serverem přijat a převzat ke zpracování, ale požadovaný zdroj není (zatím) připraven. Příprava zdroje vyžaduje nějaký čas. Jako součást odpovědi musí být konzumentskému systému předána adresa umístění dočasného zdroje v Location header. Dočasný zdroj obsahuje informace o stavu přípravy požadovaného zdroje a předpokládaném čase vytvoření zdroje. V okamžiku, kdy je finální zdroj připraven, vrací dočasný zdroj 303 (See other) odpověď spolu s adresou finálního zdroje v Location header.
Monitoring	Doporučenými monitorovanými parametry rozhraní a zároveň parametry, které je vhodné ukotvit v případné smlouvě o poskytování služeb provozu (SLA/katalogové listy) jsou: <ul style="list-style-type: none"> ▪ dostupnost - Doporučeným způsobem monitoringu dostupnosti REST ÚEP rozhraní je pravidelné spouštění end-to-end testů, tedy simulování operací konzumentské ÚEP



	<p>komponenty. Za tímto účelem musí být pro každé rozhraní definován minimálně jeden testovací scénář, nemající dopad na obsluhovaná data a maximálně reprezentativně vypovídající o stavu REST rozhraní. End-to-end test je vhodné spouštět s minimální periodicitou 15 minut;</p> <ul style="list-style-type: none">▪ odezva - Odezvu je vhodné monitorovat dvěma způsoby:<ol style="list-style-type: none">a. end-to-end testem výše uvedeným způsobem, přičemž test mimo dostupnosti sleduje i odezvu vybraných kroků testovacího scénáře,b. sledováním reálných volání. Všechna provedená volání, resp. základní informace o volání jako jsou, datum a čas zahájení volání, datum a čas dokončení volání a status obsluhy volání jsou zapisována do auditního logu, nad kterým jsou pravidelně reportovány doby obsluhy a průměrné doby obsluhy požadavků.
Obsluha chyb	<p>Rozhraní musí obsluhovat 3 typy chyb:</p> <ul style="list-style-type: none">▪ chyby autentizace a autorizace,▪ technické chyby rozhraní,▪ business chyby rozhraní. <p>V případě chyby autentizace, tedy přístupu bez platného klientského certifikátu, je odmítnuto připojení k rozhraní na úrovni webové či aplikační serveru (ERR_BAD_SSL_CLIENT_AUTH_CERT).</p> <p>V případě platného certifikátu, ale neautorizovaného volání, vrátí rozhraní konzumentské komponentě chybový kód HTTP 401 (Unauthorized) a zároveň zapíše do auditního žurnálu záznam o neautorizovaném volání.</p> <p>V případě technické chyby musí rozhraní vrátit odpovídající chybový HTTP response code (zejména 404 NOT FOUND, 400 BAD REQUEST) s odpovídající textovou zprávou informující konzumentskou ÚEP komponentu o příčině selhání.</p> <p>V případě business chyby je klientovi z pohledu komunikace vrácena standardní validní odpověď, přičemž v těle odpovědi je uvedena přesně strukturovaná informace o vniklé business chybě. Konzumentská ÚEP komponenta chybu v odpovědi identifikuje a na chybu reaguje dle předem definovaného postupu.</p>

REST rozhraní musí být implementováno v souladu s best-practices a standardy (zejména standardy ze skupiny RFC 723X) tak, aby metody GET, PUT, POST a DELETE byly využívány v souladu s jejich určením a poskytovaly chování odpovídající standardům.



6.3.3 HTML link rozhraní

Architektura systémové podpory ÚEP je tvořena řadou ÚEP komponent, přičemž velká část komponent publikuje uživatelské rozhraní pro klienty webové správy anebo úředníky. Řešení ÚEP je navrženo tak, aby klient mohl plynule přecházet mezi uživatelskými rozhraními publikovanými různými komponentami ÚEP bez nutnosti autentizace. Zároveň musí jednotlivé komponenty poskytovat shodný vzhled a ergonomie publikovaných obslužných rozhraní, tak aby klient měl pocit, že pracuje v jednom homogenním systému veřejné správy ČR.

Tab. 6 - Typ rozhraní: HTML link rozhraní

Typ rozhraní: HTML link rozhraní	
Využití	HTML link rozhraní je využito pro přesměrování klienta, uživatele rozhraní klientské ÚEP komponenty na uživatelské rozhraní jiné zdrojové ÚEP komponenty.
Integrace	Přesměrování je realizováno HTML odkazem implementovaným jako součást aplikace. Poskytnuté webové uživatelské rozhraní může být zobrazeno ve stejném okně prohlížeče anebo zobrazeno v okně novém.
Způsob autentizace a autorizace.	Rozhraní využívá jednotného systému přihlášení – single sign on (SSO) založené na technologii využívající bezpečnostní tokeny – SAML 2.0, případně WS-Federation, pokud zdrojová komponenta ÚEP nepodporuje SAML. Preferovanou technologií jednotného přihlašování je SAML.
Dostupnost	Dostupnost zdrojového rozhraní musí odpovídat požadavkům klientského rozhraní. V případě nedostupnosti rozhraní způsobené odstávkou či jiným zásahem do zdrojového rozhraní musí zdrojové rozhraní poskytnout jednotně formátovanou a strukturovanou stránku s informacemi zahrnujícími: <ul style="list-style-type: none"> ▪ informace o nedostupnosti, resp. ujištění je nedostupnost evidována anebo plánována, ▪ informace, které služby rozhraní není možné z důvodu nedostupnosti využívat, ▪ plánovaný datum a čas, kdy bude rozhraní opět dostupné.
Odezva	Odezva webových rozhraní ÚEP pro synchronní operace musí být do 5 vteřin. V případě že zdrojové rozhraní není schopno poskytnout první webovou stránku do uvedeného limitu, musí zdrojové rozhraní klientovi zobrazit informace a probíhající operaci a indikátor průběhu.
Monitoring	Rozhraní je vhodné monitorovat simulovaným end-to-end testem, shodným způsobem jako v případě monitoringu celé aplikace. Pro monitoring rozhraní musí být definovat jeden nebo více testovacích scénářů, které využitím stejného URL jako konzumentská komponenta přistoupí ke zdrojovému rozhraní a provádí



	reprezentativní operace, jako by je realizoval skutečný uživatel. Pro každou operaci je vyhodnocována dostupnost a odezva. Minimální doporučenou periodicitou spouštění end-to-end testů je 15 min.
Obsluha chyb	V případě selhání zdrojového rozhraní musí být klientovi zobrazena srozumitelná netechnická chyba rozhraní s odkazem na technickou podporu případně jiný zdroj informací, který pomůže klientovi řešením nastalé chyby. Zároveň je informace zapsána do transakčního logu komponenty poskytující zdrojové rozhraní s uvedením: <ul style="list-style-type: none"> ▪ data a času vzniku chyby, ▪ závažnosti chyby, ▪ technického popisu chyby a případně kódu chyby, ▪ příčiny chyby, pokud byla identifikována.

6.4 Základní charakteristika ITSP ve vztahu k rozhraními ÚEP

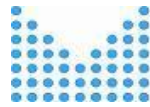
Interaktivní a transakční samoobslužný portál je vstupním bodem ke všem, nebo vybraným on-line službám veřejné správy ČR, nebo dané OVS. Na celonárodní úrovni je provozován centrální interaktivní a transakční, samoobslužný portál veřejné správy rozdělený do sekcí pro občana, podnikatele, cizince a úředníka. Tento portál obsahuje přehled všech životních událostí, úkonů a on-line služeb využitelných pro ÚEP do jednotlivých agend veřejné správy ČR. On-line služby mohou být poskytovány přímo celonárodním portálem veřejné správy anebo ITSP provozovaným na úrovni rezortu, dílčí rezortní organizace nebo v samosprávě. Každá OVS může dle svého uvážení implementovat a provozovat vlastní instanci ITSP, jehož služby jsou odkazovány z celonárodního portálu VS (PVS).

Celý systém je tedy postaven na federaci více portálů OVS. Pro OVS zajišťující výkon agend vyžadujících velké množství on-line služeb, resp. typicky elektronických formulářů, a je zde očekáváno vysoké množství změn on-line služeb či formulářů, je doporučeno implementovat a provozovat vlastní instanci ITSP.

7 Detailní popis jednotlivých rozhraní

7.1 Definice a popis jednotlivých rozhraní pro napojení eSSL v rámci ÚEP

Elektronická spisová služba (eSSL) zastává v procesu zpracování případů ÚEP tyto následující klíčové role:



- realizuje příjem a odesílání podání, resp. modul elektronické podatelny - Příjem a odesílání podání, realizuje rozhraní EPO a rozhraní datových schránek. Podání a odesílání za pomoci datových schránek je majoritní způsob podání. Na straně OVS je zpracování podání realizováno buď automaticky, nebo manuálně. V obou případech dochází k rozpoznání charakteru podání a jeho přidělení buď konkrétní osobě (v případě zpracování procesního případu na straně eSSL), nebo je technicky předán do AIS, kde je následně zpracován jako procesní případ,
- realizuje přiřazení jednoznačného identifikátoru (Č.J – čísla jednacích) a založení spisu včetně jeho jednoznačného identifikátoru, kdy každý procesní případ má svůj spis, do kterého jsou ukládány veškeré dokumenty týkající se daného procesního případu,
- ukládá xml dokumenty v rámci podání do daného spisu - tyto dokumenty nejsou čitelné nativně eSSL nástroji, ale lze je vizuálně přečíst, nebo kontrolovat pomocí komponenty Formulářového serveru úředníka, xml dokument je opatřen kontrolním součtem, aby byla zaručena integrita tohoto dokumentu,
- vytváří záznamy o činnostech nad jednotlivými dokumenty - záznamy tvoří log, který zaznamenává jednotlivé činnosti, které se provádí nad všemi dokumenty,
- poskytuje informace o dokumentech v jednotlivém spisu, přes rozhraní ITSP tak lze autentizovaným uživatelům nahlížet na obsah jednotlivého spisu a ev. si z tohoto spisu stáhnout jednotlivý dokument, nebo jeho opis.
- realizuje kontrolu certifikátů příchozích dokumentů a opatřuje pečeti a časovým razítkem dokumenty odchozí, resp. tuto činnost provádí modul EPO v rámci příjmu podání a odesílání výsledku procesní úlohy,
- poskytuje informace o účastnících řízení - tyto informace přes rozhraní konzumuje ITSP v rámci modulu účastníci řízení, který je schopen informovat klienta veřejné správy o účastnících řízení. Tuto informaci vytváří buď vnitřně přímo eSSL, nebo ji vyčítá pomocí rozhraní z příslušného AIS,
- předává podání k procesnímu zpracování - rozhraním předává podání k dalšímu zpracování dané komponentě (ÚEP manažer) ta následně předává celý případ k řešení do AIS, a to formou metadat, přístup k dokumentům následně realizuje AIS přes rozhraní NSESSS – eSSL.
- poskytuje informace ITSP o činnostech a aktivitách nad dokumenty - klient veřejné správy tak může získat ve svém rozhraní informaci týkající se jeho spisu.

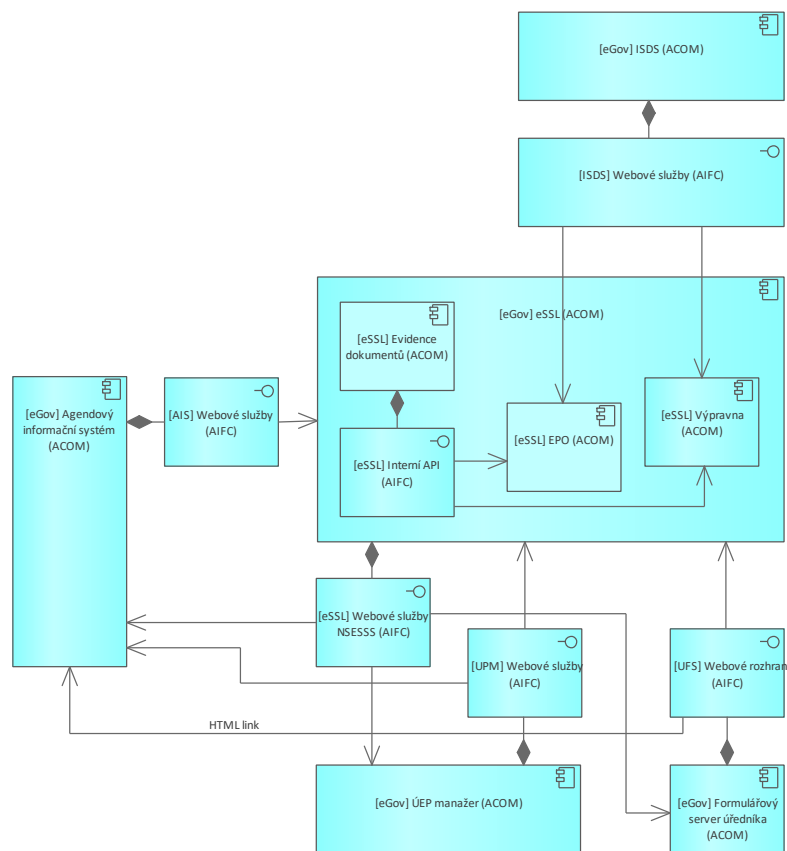
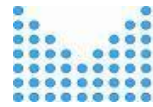


Za účelem výkonu výše uvedených činností a rolí je eSSL integrována s následujícími komponentami architektury ÚEP:

- interakční a transakční, samoobslužný portál – komponenta umožňující klientovy veřejné správy využít on-line služby za účelem podání, které odešle Datovou schránkou, webovým rozhraním na pozadí,
- datové schránky – eGOV komponenta umožňující zasílání zpráv (pro tento případ podání) mezi jednotlivými OVS a klienty a OVS, včetně všemi subjekty práva navzájem,
- ÚEP manažer – logická komponenta zajišťující řízení procesu zpracování procesních případů ÚEP v úřadu,
- formulářový server úředníka – komponenta poskytující náhledové a editační funkcionality nad ÚEP formuláři pro úředníky působnostní organizace.

Rozhraní a integrované systémy jsou znázorněny na schématu Obr. 5 - ÚEP rozhraní eSSL a další integrované systémy.

Uvedené schéma zachycuje přímé integrace mezi eSSL a dalšími komunikujícími systémy. V případě rozsáhlé organizace veřejné správy s velkým množstvím agendových systémů a dalších IT služeb je vhodné integraci realizovat využitím služeb centrální integrační platformy Enterprise Service Bus (ESB) procesy a jejich orchestraci pak platformou pro pokročilé řízení procesů např. platformou Business Process Managementu apod.



Obr. 5 - ÚEP rozhraní eSSL a další integrované systémy

7.2 Popis jednotlivých rozhraní ve vztahu k eSSL a ÚEP

7.2.1 Webové služby NSESSS

Tab. 7 - [eSSL] Webové služby NSESSS (AIFC)

Název rozhraní: [eSSL] Webové služby NSESSS (AIFC)	
Účel	<p>ÚEP manažer pro řízení ÚEP v průběhu řízení procesu zpracování ÚEP případu může vkládat nové dokumenty do eSSL. Příkladem je protokol o provedení kontroly obdržných ÚEP dat, který je vytvořen samostatnou kontrolní komponentou anebo manuálně odpovědným řešitelem.</p> <p>V případě, že řešitel v AIS anebo eSSL požaduje zobrazit data ÚEP, je přeměrován na Formulářový server úředníka (FSU). FSU následně zavolá webové služby eSSL dle standardu NSESSS a požádá o vrácení dokumentu, či více dokumentů, tvořících data ÚEP. FSU využije</p>



	<p>obdržená data a zobrazí řešiteli data ve formuláři shodném s formulářem, který využil i klient veřejné správy pro přípravu dat podání.</p> <p>Data podání jsou na FSU držena v dočasné paměti, pouze po dobu existující session přihlášeného řešitele. Po ukončení session jsou data z FSU odmazána.</p> <p>Agendový informační systém přijímá v rámci zpracování podání od komponenty ÚEP manažer pouze metadata o novém podání. Datový formát nového podání je standardem ÚEP, a tudíž ho příslušný AIS zpracuje a uloží ke zpracování.</p> <p>K samotným datům podání (formuláři) přistupuje rozhraním přímo do eSSL příslušný AIS, identitou úředníka, který v AIS pracuje na základě přidělení procesního případu ÚEP. Veškeré předávání dat se realizuje využitím standardního rozhraní webových služeb dle NSESSS. Stejně tak se realizuje čtení podání v eSSL tímto rozhraním pomocí komponenty FSÚ.</p> <p>V případě, že úředník obsluhující procesní případ komunikuje s klientem a podání v rámci ITSP je toto rozhraní to, přes které je tato komunikace realizována a to tak, že je daný dokument uložen a následně zaslán klientovi veřejné správy zákonným kanálem (Datová schránka).</p>
Zdrojový systém	eSSL
Technologie rozhraní	Webové služby SOAP dle standardu NSESSS
Způsob autentizace	Musí odpovídat standardu NSESSS
Využití rozhraní	Mimo AIS je rozhraní využito komponentou ÚEP manažer a FSU
Funkcionality rozhraní	Funkcionality dle standardu NSESSS
Význam (priorita) rozhraní pro ÚEP	V případě nedostupnosti rozhraní lze přijímat ÚEP ze strany klientů veřejné správy, není však možné podání obsluhovat a zpracovávat.
Požadovaná dostupnost	Rozhraní eSSL je v rámci řešení ÚEP využito pro přístup k dokumentům a komponentám tvořícím jednotlivá podání a pro vložení generovaných dokumentů do evidence dokumentů. V obou případech se jedná o proces zpracování podání obsluhovaný úředníky působnostní organizace. Pro účely ÚEP je minimální dostupnost eSSL rozhraní po celou pracovní dobu řešitelských útvarů ÚEP.
Požadovaná odezva	Při plánování požadavků na odezvu musí být uvažováno se standardem NSESS
Typ rozhraní	Synchronní i asynchronní
Monitoring	Rozhraní je vhodné monitorovat v souladu s obecnými principy monitoringu uvedenými v kapitole 0.

7.2.2 Webové služby ISDS

Tab. 8 - [ISDS] Webové služby (AIFC)



Název rozhraní: [ISDS] Webové služby (AIFC)	
Účel	<p>Toto rozhraní v rámci ÚEP typicky využívá komponenta EPO, které je ve většině součástí komponenty eSSL. EPO je technicky implementovaná jako samostatný modul, který načítá nové příchozí zprávy z ISDS a identifikuje, využitím metadat datové zprávy, obsahující data ÚEP. EPO přes toto rozhraní zároveň v rámci ÚEP odesílá i dokumenty (jako výstupy procesního případu) do klientovi datové schránky (nebo do kanálu, který klient určí pro komunikaci v rámci svého profilu).</p> <p>Do EPO daného OVS je tedy zaslán prostřednictvím DS datový soubor podání včetně metadat, které obsahují minimálně:</p> <ul style="list-style-type: none"> ▪ unikátní číslo (v rámci veřejné správy) podání obsahující např. označení ÚEP ITSP ze kterého podání bylo učiněno apod., ▪ data o klientovi veřejné správy, který dané podání provedl vč. čísla DS, ▪ datum odeslání podání z daného ITSP, doručení do datové schránky OVS, ▪ v případě podání na základě již existujícího procesního případu metadata obsahují i Č.J nebo číslo spisu daného procesního případu.
Zdrojový systém	ISDS
Technologie rozhraní	Webové služby SOAP dle Provozního řádu ISVS a příslušného aktuálního Věstníku MV
Způsob autentizace a autorizace	Dle Provozního řádu ISVS a dalších standardů ISDS
Využití rozhraní	eSSL, resp. EPO
Funkcionality rozhraní	Funkcionality rozhraní se řídí dle Provozního řádu a dalších standardů ISDS
Význam (priorita) rozhraní pro ÚEP	Kritická – v případě nedostupnosti tohoto rozhraní nedochází obecně k doručení podání vůči dané OVS
Požadovaná dostupnost	Jelikož se jedná o rozhraní garantované na vyšší úrovni na úrovni 7x24 je tato min. garantovaná maximální dostupnost pro ÚEP plně dostačující.
Požadovaná odezva	Provozní řád a další standardy konstatují odezvu ve vteřinách.
Typ rozhraní	Synchronní a asynchronní
Monitoring	S odkazem na Dodržování přiměřenosti nebude toto rozhraní aktivně monitorováno a bude o něm uvažováno jako o vysoce dostupné garantované službě.

7.2.3 Interní API eSSL

Tab. 9 - [eSSL] Interní API (AIFC)

Název rozhraní: [eSSL] Interní API (AIFC)



Účel	<p>V rámci rozhraní ISDS dochází k doručení dokumentu a metadat, kterých jsou uloženy informace nezbytné ke zpracování podání ÚEP do technicky samostatné komponenty EPO v rámci eSSL.</p> <p>V EPO je v rámci rozhraní interní API konfigurované jako automatická akce. Ta na základě informací poskytnutých v rámci metadat datové zprávy, vloží data podání v podobě dokumentu do evidence dokumentů v eSSL a dokument zatřídí dle spisového řádu dané organizace veřejné správy.</p> <p>Pokud EPO, resp. eSSL působnostní organizace nepodporují automatické zpracování a zaevidování ÚEP dat jako dokumentu v eSSL, provede tento úkon, zaevidování dokumentu, obsluha EPO. Jak již bylo uvedeno v případě automatického i manuálního zadání je dokument vložen do evidence dokumentů v eSSL využitím interního API eSSL.</p> <p>Interní API slouží i v případě odesílání ve vztahu k výpravně, která využívá rozhraní webových služeb ISDS. Výsledný dokument procesního případu, který má odejít klientovi elektronicky pomocí zákonného kanálu, tedy datovou schránkou, předá tento dokument výpravně která tento dokument rozhraním webové služby ISDS pošle do datové schránky klienta, který učinil podání a kterého se procesní případ týkal.</p>
Zdrojový systém	eSSL (komponenta Evidence dokumentů)
Technologie rozhraní	Interní API rozhraní
Způsob autentizace a autorizace	V rámci autentizace a autorizace jsou využívány metody v rámci eSSL.
Využití rozhraní	EPO
Funkcionality rozhraní	<ul style="list-style-type: none"> ▪ vyčítá hodnoty z metadat DS, ▪ vložení dat do Evidence dokumentů na základě metadat. ▪ akce automatického zpracování a zatřídění dle spisového řádu. ▪ ošetření chybových stavů. ▪ předává výsledný dokument výpravně ke zpracování, tedy odeslání do DS
Význam (priorita) rozhraní pro ÚEP	Při nefunkčnosti tohoto API nebude funkční automatické zakládání ÚEP případů, podání však fungovat bude. V případě nedostupnosti API je možné provádět ruční zatřídování, což není efektivní a produktivní a musí se počítat s omezením zpracování velkého počtu podání.
Požadovaná dostupnost	Pro účely ÚEP je minimální dostupnost interního API rozhraní po celou pracovní dobu řešitelských útvarů ÚEP daného OVS.
Požadovaná odezva	Jde o interní rozhraní požadovaná doba odezvy rozhraní je do 1 sekundy.
Typ rozhraní	API
Monitoring	Rozhraní je vhodné monitorovat v souladu s obecnými principy monitoringu uvedenými v kapitole 0.



7.2.4 Webové služby AIS

Tab. 10 - [AIS] Webové služby (AIFC)

Název rozhraní: [AIS] Webové služby (AIFC)	
Účel	<p>Primární, referenční dokumenty jsou vždy drženy v rámci komponenty eSSL. V rámci AIS vznikají a jsou evidovány výhradně pracovní kopie dokumentů. V AIS se mohou být přechodnou dobu evidovány pracovní kopie dokumentů z eSSL. Tyto kopie a pracovní podoby dokumentů by měly být z AIS odmazány v okamžiku, kdy nejsou na straně AIS již tato data potřeba. Je tedy nutné řídit veškeré dokumenty procesního případu bez ohledu na místo kde je dokument uložen. Jediný nástroj pro uplatnění skartačního plánu (skartační lhůta a znak) je eSSL.</p> <p>Pro potřeby skartace poskytuje AIS rozhraní pro notifikaci požadavku na skartování dokumentu, prostřednictvím kterého eSSL požádá o skartování dokumentu. Po uplynutí skartační lhůty je třeba odmazat z AIS veškeré verze dokumentů, na které se vztahuje skartace nebo archivace. eSSL musí zahrnovat funkcionalitu umožňující uvedenou akci volat.</p>
Zdrojový systém	AIS
Technologie rozhraní	Webové služby SOAP anebo REST, případně nativní rozhraní AIS v případě, že je komunikace zprostředkována integrační platformou ESB a požadované služby jsou implementovány na platformě ESB.
Způsob autentizace a autorizace	Autentizace a autorizace prostřednictvím klientského systémového certifikátu v souladu s popisem uvedeným v kapitole 6.3.1 a 6.3.2. Pro volání skartačního rozhraní bude autorizován pouze systém eSSL.
Využití rozhraní	eSSL
Funkcionality rozhraní	<ul style="list-style-type: none"> ▪ příjem požadavku na smazání jednoho či více pracovních dokumentů z pracovního úložiště dokumentů v AIS, ▪ v případě, že je dokument v okamžiku volání v AIS upravován anebo je s dokumentem jinak manipulováno tak, že není možné dokument okamžitě odstranit, musí tento případ zaznamenat a v rámci AIS zaevidovat požadavek na smazání dokumentu a provedení této akce ihned, jak bude dokument uvolněn, ▪ smazání dokumentů z AIS zaznamenat minimálně však: <ol style="list-style-type: none"> a. datum a čas, b. jméno/a dokumentu, c. číslo spisu.
Význam (priorita) rozhraní pro ÚEP	V případě nedostupnosti tohoto rozhraní nedochází k odmazání dokumentů a mohou být porušena pravidla vyplývající ze zákonných povinností dané OVS. Případným výpadkem není dotčena možnost klientů veřejné správy podávat ÚEP kanálem ani výkon procesů zpracování ÚEP případů.



Požadovaná dostupnost	Požadovaná dostupnost může být s ohledem na dopady nižší než v případě ostatních ÚEP komponent.
Požadovaná odezva	Odezva není kritický faktor tohoto rozhraní.
Typ rozhraní	Synchronní s podporou přechodu do asynchronního režimu.
Monitoring	Je doporučen obecný monitoring webových rozhraní v souladu s popisem uvedeným v kapitole 0.

7.2.5 Webové služby komponenty ÚEP manažer

Tab. 11 - [UEPM] Webové služby (AIFC)

Název rozhraní: [UEPM] Webové služby (AIFC)	
Účel	Zpracováním dokumentu podání v rámci eSSL začíná akce obsluhy podání. Pro tyto účely je vybudované rozhraní komponenty ÚEP manažer, které volá komponenta eSSL za účelem založení nového procesního případu ÚEP, nebo realizaci volání za účelem aktualizace již existujícího procesního případu (nebo informace v rámci tohoto případu apod.). Toto platí pro případ, že se podání obsluhuje přímo v rámci eSSL. V případě zpracování podání v AIS, přijímá AIS volání k založení případu nebo dalším akcím, ze strany komponenty ÚEP manažer. Takovou úlohou může být požadavek na zpracování dat ÚEP případu, modifikace dat v registrech a jiných datových zdrojích obsluhovaných AIS, požadavek na validaci ÚEP dat atd. Na straně eSSL existuje funkcionality zajišťující volání rozhraní webových služeb a předání metadata o dokumentu/podání ÚEP. Samotná data ÚEP se v rámci volání nepředávají. K datům ÚEP přistupují řešitelské systémy (typicky AIS) využitím rozhraní standardních webových služeb eSSL NSESSS. Přístup k datům v eSSL musí být vždy zaznamenán dle NSESSS.
Zdrojový systém	ÚEP manažer
Technologie rozhraní	SOAP nebo REST (případně nativní rozhraní komponenty ÚEP manažer, pokud je využita integrační sběrnice ESB)
Způsob autentizace a autorizace	Obecná autentizace systémovým klientským certifikátem a následná autorizace v souladu s popisem uvedeným v kapitole 0.
Využití rozhraní	Rozhraní je využito komponentou eSSL
Funkcionality rozhraní	Tímto rozhraním je rozhraní na straně komponenty ÚEP manažer, která realizuje plné elektronické, procesní zpracování daného ÚEP případu. Úlohy vyplývající ze specifických procesů obsluhy různých typů podání (různé agendy, úkony, odlišné formuláře) jsou natolik odlišné, že není efektivní navrhnout a implementovat jednotné úlohové rozhraní vyhovující všem těmto specifickým požadavkům. V případě, že procesního zpracování není účasten AIS, je komponenta ÚEP manažer zároveň zpracovatel a procesní platforma realizující procesní případ. Z rozhraní tak přicházejí jednotlivé úlohy a komponenta ji autonomně zpracovává (procesuje) a výsledné



	<p>dokumenty ukládá zpět do eSSL prostřednictvím níž komunikuje s klientem. Existuje-li AIS zúčastněný na procesu obsluhy ÚEP případů předává tuto úlohu tato komponenta dál ke zpracování do AIS. Mezi základní obecné funkcionality poskytované tímto rozhraním lze zařadit:</p> <ul style="list-style-type: none"> ▪ předání informací o novém podání, resp. dokumentu či více dokumentech a souvisejících komponentách v eSSL, a požadavek na zpracování podání komponentou ÚEP manažer nebo AIS, ▪ požadavek na vytvoření jiné úlohy obsluhované buď komponentě ÚEP manažer, nebo AIS, která není navázaná na samotná data ÚEP (např. různé žádosti, administrativní aktivity atd. nevyžadující data podání), ▪ požadavek na kontrolu dat ÚEP, kdy komponenta ÚEP manažer nebo AIS ověřují bezvadnost podání, ▪ požadavek na realizaci různých výpočtů, doplnění a transformací dat atd. v průběhu zpracování procesních případů.
Význam (priorita) rozhraní pro ÚEP	<p>Rozhraní je nezbytné pro obsluhu procesních případů ÚEP. V případě nedostupnosti rozhraní nemůže komponenta ÚEP manažer postupovat v procesu zpracování podání a generovat a přidělovat procesní úlohy. V takovém případě je zastaven elektronický proces zpracování všech typů ÚEP. Možnost učinění podání klienty veřejné správy tímto není dotčena.</p>
Požadovaná dostupnost	<p>Proces zpracování podání je obsluhován úředníky působnostní organizace. Pro účely ÚEP je tedy minimální dostupnost rozhraní po celou pracovní dobu řešitelských útvarů ÚEP podílejících se na obsluze typů podání využívajících komponentu ÚEP manažer a AIS.</p>
Požadovaná odezva	<p>Pro synchronní rozhraní je požadovaná odezva do 2 sekund. V případě operace s delší dobou odezvy je třeba rozhraní navrhovat a budovat jako asynchronní.</p>
Typ rozhraní	<p>Synchronní či asynchronní dle popisu uvedeného v kapitole 0.</p>
Monitoring	<p>Rozhraní je vhodné monitorovat v souladu s obecnými principy monitoringu uvedenými v kapitole 0.</p>

7.2.6 Webové rozhraní Formulářového serveru úředníka

Tab. 12 - [FSU] Webové rozhraní (AIFC)

Název rozhraní: [FSU] Webové rozhraní (AIFC)	
Účel	<p>Pro případ, že má odpovědný řešitel zájem zobrazit data ÚEP uložené v eSSL, musí být v rámci eSSL dostupná funkcionality a související akce, po které je uživatel přesměrován (samostatným oknem) na webové rozhraní Formulářového serveru úředníka. Náhled na data</p>



	<p>podání je pouze v režimu pro čtení. Úředník má možnost zobrazit data podání ve shodné podobě, v jaké jsou zobrazeny i koncovému klientovi z důvodu poskytování hladších asistenčních služeb klientovi. Náhled je pouze v režimu pro čtení. V rámci přesměrování požadavku je předán i atribut obsahující unikátní číslo podání, které má být zobrazeno.</p> <p>Na FSU je řešitel případu přesměrován spolu s SSO tokenem, a to bez nutnosti samostatného přihlášení. Samotná data podání nejsou posílána jako součást přesměrování. K požadovaným datům a dokumentům aktivně přistupuje FSU, za pomoci standardního NSESS rozhraní v rámci eSSL.</p>
Zdrojový systém	FSU
Technologie rozhraní	HTML link. Přesměrování klienta na Formulářový server úředníka následováním HTML link odkazu.
Způsob autentizace a autorizace	Jednotné přihlášení cestou SAML v souladu s obecným popisem v kapitole 6.3.3. Autorizaci přístupů úředníků k jednotlivým typům podání a jejich oprávnění pro práci s daty podání řídí eSSL s využitím autorizačních informací evidovaných v samostatném systému Formulářového serveru úředníka, adresářových službách (např. LDAP), či v jiných autorizačních systémech působnosti organizace.
Využití rozhraní	Rozhraní je využito AIS a eSSL a umožňuje uživatelům obou těchto systémů přístup k on-line webovým formulářům prezentujícím data ÚEP
Funkcionality rozhraní	<p>Mezi hlavní funkcionality rozhraní patří:</p> <ul style="list-style-type: none"> ▪ poskytování náhledu na data podání – zobrazení XML dokumentů a souvisejících komponent tvořících data podání, ▪ zaznamenání přístupu k dokumentu, ▪ poskytování vizuální podoby formulářů, prostřednictvím kterých jsou pořizována data podání, pro účely poradenství, možnost úředníka vyplnit formulář za klienta atd.
Význam (priorita) rozhraní pro ÚEP	V případě nedostupnosti rozhraní nebudou mít řešitelské útvary působnostních úřadů možnost zobrazovat data podání, pořizovat nová data podání, resp. asistovaná podání. Dojde tak ke zpomalení a postupnému zastavení procesu obsluhy procesních případů ÚEP. Možnost podání klientů veřejné správy, využitím jakéhokoliv kanálu, včetně ÚEP, není v takovém případě dotčena.
Požadovaná dostupnost	Formulářový server úředníka je využit pouze úředníky působnosti organizace. Pro účely ÚEP musí být tedy minimální dostupnost rozhraní Formulářového serveru úředníka po celou pracovní dobu řešitelských útvarů ÚEP.
Požadovaná odezva	Webové rozhraní Formulářového serveru úředníka, je webové rozhraní pro uživatele – úředníky. Maximální odezva webového rozhraní by měla být do 2 sekund, v limitních případech do 5 sekund.
Typ rozhraní	Synchronní webové rozhraní.



Monitoring	Je doporučen obecný monitoring webových rozhraní v souladu s popisem uvedeným v kapitole 0.
------------	---



7.3 Definice a popis jednotlivých rozhraní pro napojení AIS v rámci ÚEP

Agendový informační systém (AIS) zastává v procesu zpracování případů ÚEP několik rolí:

- **Poskytuje data pro automatické předvyplnění a průběžné doplňování známých dat** ve formulářích publikovaných na ITSP. Automatické doplnění dat je v souladu z jedním ze základních principů návrhu a výstavby on-line služeb veřejné správy, principem „Only Once“, tedy, že veškerá data budou po klientech veřejné správy požadována pouze jednou;
- **Zajišťuje systémovou podporu pro výkon úloh v rámci procesu zpracování ÚEP případů.** AIS je v této roli jedním ze systémů, které se podílí na obsluze případu ÚEP. Za účel provedení svěřených úloh může AIS obdržet kompletní nebo část dokumentů (a komponent) tvořících data ÚEP případu. AIS může po přechodnou dobu udržovat pracovní verzi dokumentů a souvisejících komponent tvořících data ÚEP s tím, že originální referenční verze těchto dat jsou stále evidována v systému eSSL. AIS za účelem zpracování obdrží a eviduje výhradně pracovní kopii dokumentů, kterou udržuje pouze po dobu nezbytně nutnou pro výkon svěřené ÚEP úlohy anebo do doby, kdy je eSSL požádán o odstranění pracovní verze dokumentů a souvisejících komponent. Vzhledem k tomu, že AIS v takovém případě neeviduje jedinou, referenční verzi dokumentů, tedy že referenční verze dokumentů je řádně evidována v eSSL, **není AIS v kontextu ÚEP považován za ISSD dle národních standardů eSSL NSESSS.** Jako součást systémové podpory umožňuje AIS náhled na data podání ve struktuře a formátu, ve které data podal klient veřejné správy;
- **Koordinuje aktivity nezbytné pro realizaci svěřené ÚEP úlohy.** Pokud se na realizaci svěřené úlohy v AIS podílí více řešitelských týmů či řešitelů, zajišťuje AIS koordinaci těchto řešitelských týmů či řešitelů včetně dozoru realizace dílčích aktivit a souvisejících termínů;
- **Spravuje agendová/oborová data** typicky evidovaná ve specializovaných informačních systémech – registrech. Jednou z úloh přidělených AIS v procesu zpracování případu ÚEP je aktualizace agendových dat v příslušném registru. AIS na základě příchozích ÚEP dat provede odpovídající aktualizace evidencí. Nedílnou součástí funkcionality AIS je tzv. dávkování změn dat, jejich verzování a možnost odvolání či modifikace dávky změn, jež byly provedeny v rámci zpracování ÚEP úlohy, jak je uvedeno dále v dokumentu;
- **Pomáhá připravovat výstupní dokumenty vznikající v průběhu zpracování případů ÚEP.** Všechny výstupní dokumenty vytvořené v AIS musí být řádně vloženy do eSSL. V AIS může po přechodnou dobu existovat draft anebo pracovní verze dokumentu. Každá referenční verze dokumentu však musí být předána do eSSL. I v případě předání referenční verze dokumentu do eSSL, může v AIS po přechodnou dobu existovat pracovní verze takového dokumentu. Pracovní verze může být uchovávána po dobu možných zásahů a úprav poslední referenční verze dokumentu anebo do doby, kdy eSSL aktivně nepožádá o odstranění dokumentu a souvisejících komponent;

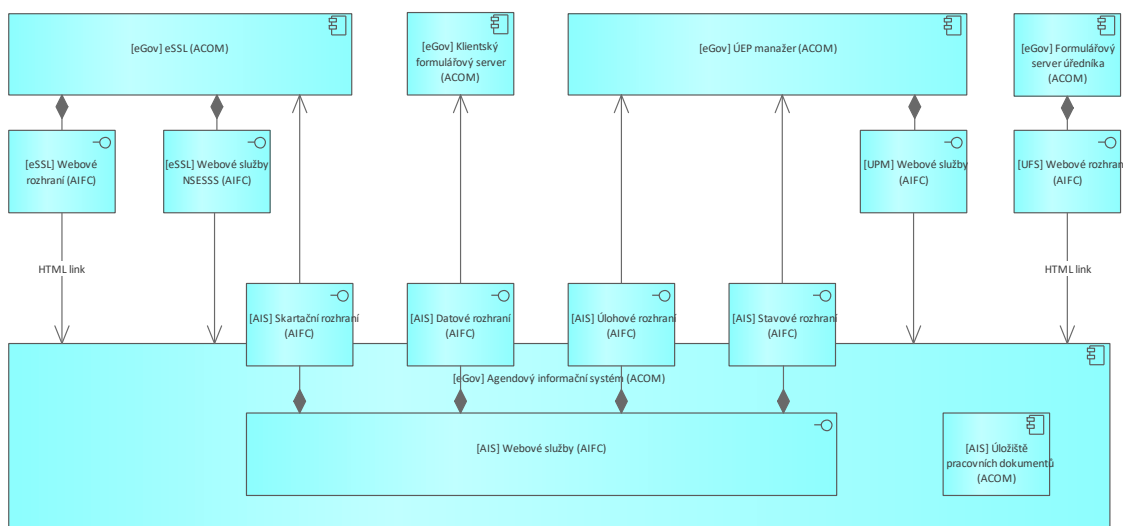


- **Poskytuje informace o stavu zpracování ÚEP úloh v AIS.** AIS poskytuje informace, v jakém stavu je realizace svěřené ÚEP úlohy. Příkladem může být stav zaevidované žádosti, dokončení modifikací dat v registrech, ale i informace o vadách podání, pokud byly v průběhu zpracování v AIS identifikovány. Mimo stavu AIS poskytuje i informace o útvaru a případně i kontaktní osobě, která přidělenou úlohu v AIS aktuálně řeší.

Za účelem výkonu výše uvedených rolí je AIS integrován s následujícími komponentami architektury ÚEP:

- klientský formulářový server – komponenta ITSP poskytující formuláře pro klienty veřejné správy,
- ÚEP manažer – logická komponenta zajišťující řízení procesu zpracování procesních případů ÚEP v úřadu,
- eSSL – elektronický systém spisové služby úřadu,
- formulářový server úředníka – komponenta poskytující náhledové a editační funkcionality nad ÚEP formuláři pro úředníky působnostní organizace.

Rozhraní a integrované systémy jsou znázorněny na schématu **Chyba! Nenalezen zdroj odkazů..** Uvedené schéma zachycuje přímou integraci mezi AIS a komunikujícími systémy. V případě rozsáhlé organizace veřejné správy s velkým množstvím agendových systémů a IT služeb je vhodné integraci realizovat využitím služeb centrální integrační platformy Enterprise Service Bus (ESB).



Obr. 6 - ÚEP rozhraní AIS a integrované systémy



7.4 Popis jednotlivých rozhraní ve vztahu k AIS a ÚEP

7.4.1 Datové rozhraní

Tab. 13 - [AIS] Datové rozhraní (AIFC)

Název rozhraní: [AIS] Datové rozhraní (AIFC)	
Účel	Prostřednictvím tohoto rozhraní poskytuje AIS známá data, která lze automaticky předvyplnit do formulářů v samoobslužném portálu. Známá data zahrnují jak kmenová oborová data konkrétní agentury, tak např. data sdílených číselníků evidovaných v AIS. Za známá data jsou zároveň považována i data, která byla vypočtena anebo jinak odvozena z údajů předaných ze strany ITSP jako součást volání rozhraní a údajů v AIS. ITSP, resp. logika ÚEP formuláře, v takovém případě může volat Datové rozhraní AIS za účelem vypočtení anebo jiného odvození údajů, které ITSP předá AIS jako součást volání. Typicky se jedná o data vložená klientem do formuláře, na základě kterých AIS dovodí jiná data a předá je zpět ITSP pro automatické doplnění do formuláře.
Zdrojový systém	Agendový informační systém (AIS)
Technologie rozhraní	V případě přímé integrace mezi AIS a ITSP je rozhraní implementováno ve formě SOAP anebo REST webových služeb. V případě, kdy je pro integraci zvolena integrační platforma ESB, může být využito nativní rozhraní AIS, přičemž požadované SOAP anebo REST webové služby mohou být implementovány a publikovány na ESB. ESB v takovém případě může komunikovat s AIS libovolným způsobem, který AIS podporuje.
Způsob autentizace a autorizace	Autentizace na úrovni systémů je realizována klientským systémovým certifikátem v souladu s postupem uvedeným v kapitole SOAP rozhraní webových služeb. AIS provádí autorizaci na úrovni přístupu k datům na základě informací obdržených jako součást volání rozhraní. Povinným parametrem volání je jednoznačný identifikátor subjektu uživatele a subjektu dat, pro který jsou data požadována. V případě, že formulář na straně ITSP požaduje data pro více subjektů dat, musí být pro každý subjekt dat provedeno samostatné volání.
Využití rozhraní	Rozhraní je využito ITSP v případě přímé integrace anebo ESB v situaci, kdy je komunikace s ITSP zprostředkována ESB. Konzumentem služeb je ale v obou případech ITSP.
Funkcionality rozhraní	<ul style="list-style-type: none"> ▪ přijímá identifikátor subjektu uživatele ITSP, který žádá o data, ▪ přijímá identifikátor subjektu dat, tedy subjektu, jehož data jsou žádána, a autorizuje požadavek na data, resp. oprávnění subjektu dat přistupovat k požadovaným datům,



	<ul style="list-style-type: none"> ▪ přijímá identifikátor volání z ESB (Correlation ID) pokud je pro komunikaci s ITSP využita ESB sběrnice, Požadavek na data je zapsán do transakčního logu AIS. Záznam v logu obsahuje minimálně: <ol style="list-style-type: none"> a. identifikátor subjektu uživatele, b. identifikátor subjektu dat, c. volané rozhraní, služba či metoda, d. předané parametry, e. datum a čas volání, f. výsledek autorizace požadavku, g. status volání, h. correlation ID ESB, pokud je ESB pro integraci využito, ▪ Poskytuje pouze ta data, na která má subjekt dat nárok ▪ Podporuje: <ol style="list-style-type: none"> a. Vrácení požadovaných dat v podobě: <ol style="list-style-type: none"> i. skalární hodnoty, ii. objektu, iii. seznamu skalárních hodnot či objektů; b. V případě seznamu: <ol style="list-style-type: none"> i. vrácení všech nalezených záznamů ii. stránkování nalezených záznamů a vrácení požadovaného rozsahu stránek iii. vrácení filtrovaného seznamu záznamů dle omezujících kritérií předaných jako součást požadavku
Význam (priorita) rozhraní pro ÚEP	Kritické
Požadovaná dostupnost	Požadovaná dostupnost musí odpovídat dostupnosti ITSP, který čerpá data z AIS za účelem automatického doplnění dat do formulářů.
Požadovaná odezva	Pro synchronní do 5 ti sekund, u asynchronní dle složitosti operace s povinně zobrazeným hlášením o časové náročnosti probíhající operace.
Typ rozhraní	Synchronní s podporou přechodu do asynchronního módu.
Monitoring	Rozhraní je vhodné monitorovat v souladu s obecnými principy monitoringu uvedenými v kapitole 0.

7.4.2 Webové služby NSESSS

Tab. 14 - [eSSL] Webové služby NSESSS (AIFC)

Název rozhraní: [eSSL] Webové služby NSESSS (AIFC)	
Účel	Rozhraní webových služeb standardu NSESSS je v rámci ÚEP integrace a komunikace s AIS využito pro:



	<ul style="list-style-type: none"> ▪ načítání dokumentů a komponent za účelem jejich zpracování v průběhu výkonu ÚEP úloh v AIS - Komponenta ÚEP manažer přiděluje AIS prostřednictvím Úlohového rozhraní novou úlohu zpracování ÚEP dat s odkazem na dokument v eSSL a případně s metadaty dokumentu (komponenty tvořící dokument nejsou předávány). AIS v případě potřeby využije rozhraní webových služeb NSESSS pro načtení dokumentu, metadat o dokumentu a všech potřebných komponent z eSSL. V případě, že je pro integraci využita integrační platforma ESB a AIS požaduje pouze část dokumentu anebo jinak transformovaný dokument z eSSL může být na straně ESB implementována webová služba zprostředkávající komunikaci s eSSL, která provede potřebné manipulace s dokumentem a jeho komponentami. Příkladem je transformace XML dat podání, extrakce vybraných hodnot z XML atd. AIS může trvale uchovávat metadata dokumentu. Úlohou AIS je poskytnout agendově specifický pohled na dokumenty, který není schopen poskytnout systém eSSL. AIS tedy vede svou vlastní evidenci základních metadat o dokumentu tříděných a seskupených dle věcných kritérií v AIS, agendově specifický rejstřík dokumentů. Mimo evidence metadat může AIS po přechodnou dobu uchovávat i pracovní kopie komponent dokumentů načtených z eSSL. Pracovní kopie může uchovávat pouze po dobu, kdy jsou na straně AIS potřeba anebo maximálně do doby, kdy si eSSL prostřednictvím Skartačního rozhraní explicitně vyžádá smazání dokumentu. ▪ vkládání nových referenčních dokumentů a jejich verzí do eSSL - V průběhu obsluhy ÚEP úloh v AIS mohou být vytvářeny nové výstupní dokumenty. Dokument je v okamžiku vniku považován za pracovní a zůstává pracovní do doby, než je dle procesu v AIS prohlášen za referenční. Prohlášení dokumentu, resp. jeho některé verze, za referenční zakládá povinnost vložit tento dokument do evidence dokumentů v eSSL.
Zdrojový systém	eSSL
Technologie rozhraní	Webové služby SOAP dle standardu NSESSS.
Způsob autentizace a autorizace	Musí odpovídat standardu NSESSS.
Využití rozhraní	Mimo AIS je rozhraní využito komponentou ÚEP manažer.
Funkcionality rozhraní	Funkcionality dle standardu NSESSS.
Význam (priorita) rozhraní pro ÚEP	V případě nedostupnosti rozhraní lze přijímat ÚEP ze strany klientů veřejné správy, není však možné podání obsluhovat a zpracovávat.



Požadovaná dostupnost	Rozhraní eSSL je v rámci řešení ÚEP využito pro přístup k dokumentům a komponentám tvořícím jednotlivá podání a pro vložení generovaných dokumentů do evidence dokumentů. V obou případech se jedná o proces zpracování podání obsluhovaný úředníky působnostní organizace. Pro účely ÚEP je minimální dostupnost eSSL rozhraní po celou pracovní dobu řešitelských útvarů ÚEP.
Požadovaná odezva	Při plánování požadavků na odezvu musí být uvažováno se standardem NSESS.
Typ rozhraní	Synchronní a asynchronní.
Monitoring	Rozhraní je vhodné monitorovat v souladu s obecnými principy monitoringu uvedenými v kapitole 0.

7.4.3 Webové služby ÚEP manažera

Tab. 15 - [UPM] Webové služby (AIFC)

Název rozhraní: [UPM] Webové služby (AIFC)	
Účel	Prostřednictvím tohoto rozhraní AIS informuje komponentu ÚEP manažer o změně stavu a postupu v obsluze úlohy svěřené AIS. Prostřednictvím tohoto rozhraní má dále AIS možnost vstupovat do procesu zpracování ÚEP, žádat o vytvoření dalších úloh a jejich přidělení jiným zúčastněným agendovým systémům atd.
Zdrojový systém	ÚEP manažer
Technologie rozhraní	SOAP webové služby.
Způsob autentizace a autorizace	Autentizace klientským certifikátem v souladu s popisem uvedeným v kapitole 6.3.1. Komponenta ÚEP manažer provádí autorizaci příchozích požadavků. Na straně komponenty ÚEP manažer jsou připravena pravidla definující mimo jiné: <ul style="list-style-type: none"> ▪ který systém může aktualizovat procesní případ určitého typu, ▪ který systém může žádat o založení nového procesního případu určitého typu, ▪ který systém v jakých procesech může žádat o vytvoření nové úlohy a přidělení úlohy jinému AIS.
Využití rozhraní	Rozhraní využívají AIS a ostatní systémy poskytující systémovou podporu zpracování procesních případů ÚEP. Rozhraní zároveň využívá i eSSL pro založení nových procesních případů na základě příchozích podání.
Funkcionality rozhraní	Rozhraní poskytuje funkcionality pro AIS a další systémy podílející se na procesu zpracování ÚEP případu. Funkcionality umožňují AIS a ostatním komponentám ÚEP interagovat s procesem zpracování ÚEP případu. Rozhraní: <ul style="list-style-type: none"> ▪ přijímá notifikace o změně stavu úlohy přidělené AIS či jiné ÚEP komponentě,



	<ul style="list-style-type: none"> ▪ přijímá další informace evidované v procesním případě související s obsluhou úlohy přidělené AIS či jiné ÚEP komponentně, ▪ přijímá požadavky na založení nových procesních případů ÚEP či procesních případů ostatních podpůrných procesů ÚEP, ▪ přijímá požadavky na založení nové procesní úlohy s možností přidělení jinému AIS či jiné ÚEP komponentě.
Význam (priorita) rozhraní pro ÚEP	Rozhraní zajišťuje příjem informací z AIS a jiných ÚEP komponent o postupu zpracování konkrétních ÚEP případů. V případě nedostupnosti tohoto rozhraní nebudou moci zúčastněné komponenty informovat a aktuálním stavu svěřených úloh a proces zpracování ÚEP případů tak bude zastaven. Příjem podání za strany klientů veřejné správy v případě nedostupnosti tohoto rozhraní není dotčen.
Požadovaná dostupnost	Proces zpracování podání je obsluhován úředníky působnostní organizace. Pro účely ÚEP je tedy minimální dostupnost rozhraní po celou pracovní dobu řešitelských útvarů ÚEP.
Požadovaná odezva	Požadovaná doba odezvy rozhraní je do 2 sekund.
Typ rozhraní	Synchronní
Monitoring	Standardní monitoring SOAP rozhraní v souladu s popisem uvedeným v kapitole 0.

7.4.4 Úlohové rozhraní

Tab. 16 - [AIS] Úlohové rozhraní (AIFC)

Název rozhraní: [AIS] Úlohové rozhraní (AIFC)	
Účel	Prostřednictvím tohoto rozhraní AIS přijímá od komponenty Manažer ÚEP úlohy obsluhy ÚEP případu. Úlohou může být požadavek na zpracování dat ÚEP případu, modifikace dat v registrech a jiných datových zdrojích obsluhovaných AIS, požadavek na validaci ÚEP dat atd. Úlohové rozhraní na straně AIS je implementováno dle specifických požadavků AIS a obsluhovaného procesního případu ÚEP.
Zdrojový systém	AIS zapojený do procesu zpracování ÚEP.
Technologie rozhraní	SOAP nebo REST (případně nativní rozhraní AIS, pokud je využita integrační sběrnice ESB).
Způsob autentizace a autorizace	Obecná autentizace systémovým klientským certifikátem a následná autorizace v souladu s popisem uvedeným v kapitole 6.3.1 a 6.3.2.
Využití rozhraní	Rozhraní je využito komponentou ÚEP manažer.



Funkcionality rozhraní	<p>Úlohovým rozhraním je jakékoliv rozhraní na straně AIS, které je nezbytné pro plné elektronické zpracování ÚEP případu. Úlohy vyplývající ze specifických procesů obsluhy různých typů podání (různé agendy, úkony, odlišné formuláře) jsou natolik odlišné, že není efektivní navrhnout a implementovat jednotné úlohové rozhraní vyhovující všem těmto specifickým požadavkům. Na straně AIS zúčastněných na procesu obsluhy ÚEP případů mohou být implementována sdílená rozhraní a služby pro obsluhu více typů podání anebo jednoúčelové služby specifické pro konkrétní typ podání. Preferovaným postupem je implementace víceúčelových univerzálních služeb. Návrh a univerzálnost těchto služeb je plně v kompetenci působnostních úřadů a týmů odpovědných za provoz a rozvoj dotčených AIS. Mezi základní obecné funkcionality poskytované Úlohovým rozhraním lze zařadit:</p> <ul style="list-style-type: none">▪ předání informací o novém podání, resp. dokumentu či více dokumentech a souvisejících komponentách v eSSL, a požadavek na zpracování podání v AIS,▪ požadavek na vytvoření jiné úlohy obsluhované v AIS, která se neváže k samotným datům ÚEP (různé žádosti, administrativní aktivity atd. nevyžadující data ÚEP),▪ požadavek na kontrolu dat ÚEP, kdy AIS ověřuje bezvadnost podání, přičemž výstupem je i informace o možnosti zpracování podání na straně AIS (např. ověřuje, že podání není v kolizi s jiným v minulosti učiněným podáním),▪ požadavek na realizaci různých výpočtů, doplnění a transformací dat, atd. v průběhu zpracování procesních případů.
Význam (priorita) rozhraní pro ÚEP	<p>Rozhraní je nezbytné pro obsluhu procesních případů ÚEP. V případě nedostupnosti rozhraní nemůže komponenta ÚEP manažer postupovat v procesu zpracování podání a generovat a přidělovat procesní úlohy. V takové případě je zastaven proces zpracování všech typů ÚEP, na kterých se dotčené úlohové rozhraní AIS podílí. Možnost učinění podání klienty veřejné správy tímto není dotčena.</p>
Požadovaná dostupnost	<p>Proces zpracování podání je obsluhován úředníky působnostní organizace. Pro účely ÚEP je tedy minimální dostupnost rozhraní po celou pracovní dobu řešitelských útvarů ÚEP podílejících se na obsluze typů podání využívajících dílčí Úlohové rozhraní AIS.</p>
Požadovaná odezva	<p>Pro synchronní rozhraní je požadovaná odezva do 2 sekund. V případě operace s delší dobou odezvy je třeba rozhraní navrhovat a budovat jako asynchronní.</p>
Typ rozhraní	<p>Synchronní či asynchronní dle popisu uvedeného v kapitole 6.3.2.</p>
Monitoring	<p>Rozhraní je vhodné monitorovat v souladu s obecnými principy monitoringu uvedenými v kapitole 0..</p>



7.4.5 Stavové rozhraní

Tab. 17 - [AIS] Stavové rozhraní (AIFC)

Název rozhraní: [AIS] Stavové rozhraní (AIFC)	
Účel	Prostřednictvím tohoto rozhraní AIS poskytuje detailní informace o aktuálním stavu zpracování svěřené ÚEP úlohy.
Zdrojový systém	AIS
Technologie rozhraní	Webové služby SOAP nebo REST, případně nativní rozhraní AIS pokud jsou požadované webové služby implementovány na integrační platformě ESB.
Způsob autentizace a autorizace	Obecná autentizace klientským certifikátem dle postupu uvedeného v kapitole 0.
Využití rozhraní	Rozhraní je využito komponentou ÚEP manažer, která dále poskytuje souhrnný stav podání (konsolidovaný ze všech AIS a dalších komponent ÚEP podílejících se na zpracování podání) ITSP. Komponenta ÚEP manažer dále prostřednictvím vlastního uživatelského rozhraní anebo rozhraní jiných integrovaných systémů poskytuje informace o souhrnném a detailním stavu obsluhovaných úloh aktérům v rolích Koordinátor ÚEP a Řešitel ÚEP.
Funkcionality rozhraní	Prostřednictvím tohoto rozhraní AIS poskytuje shodně strukturované, detailní informace o stavu každé svěřené ÚEP úlohy zahrnující: <ul style="list-style-type: none"> ▪ identifikátor ÚEP úlohy, ▪ ÚEP identifikátor podání, ▪ datum a čas vzniku úlohy, ▪ stav úlohy (Přijato, Probíhá zpracování, Obsluženo, Přerušeno, Zrušeno), ▪ výsledek zpracování úlohy (pokud již byla dokončena) obsahující výčtové hodnoty indikující řádné dokončení a dokončení s chybou, ▪ identifikace osoby aktuálně odpovědné za obsluhu úlohy v AIS a jméno osoby, která celý případ vyřizuje. <p>AIS může v rámci jednoho procesního případu ÚEP obsluhovat více svěřených úloh. Proto jako součást jednoho dotazu ze strany komponenty ÚEP manažer může být doptáván stav více svěřených úloh, avšak pouze úloh souvisejících s jedním procesním případem ÚEP.</p>
Význam (priorita) rozhraní pro ÚEP	Komponenta ÚEP manažer publikuje webové služby, které jsou volány v okamžiku dotazu klienta veřejné správy na detailní stav zpracování podání ITSP. Komponenta ÚEP Manažer v reakci na příchozí požadavek zavolá Stavové rozhraní všech AIS, podílejících se na zpracování ÚEP případu, zpracuje odpověď a předá souhrnnou informaci jako součást odpovědi ITSP. Odpověď obsahuje standardně strukturovaný přehled všech úloh s detaily uvedenými



	<p>výše. V případě, že některé ze stavových rozhraní nevrátí validní odpověď, vrátí komponenta ÚEP Manažer v části informací pro dotčené úlohy informaci o nedostupnosti rozhraní, důvodu a předpokládaném datu a času opětovné dostupnosti rozhraní, pokud jsou tyto informace na straně AIS dostupné.</p> <p>Nedostupnost stavového rozhraní kteréhokoliv z AIS systémů zúčastněných na obsluze procesního případu má za následek degradaci služeb poskytovaných koncovému klientovi veřejné správy.</p> <p>Zároveň dochází k degradaci služeb poskytovaných řešitelským týmům v působnostních úřadech, které tak přichází o možnost sledovat aktuální informace a stav obsluhy jednotlivých procesních případů ÚEP.</p>
Požadovaná dostupnost	Dostupnost rozhraní musí odpovídat dostupnosti ITSP a on-line služeb pro klienty veřejné správy. Zároveň musí dostupnost odrážet požadavky a pracovní dobu řešitelských týmů v působnostních úřadech podílejících se na zpracování procesních případů ÚEP.
Požadovaná odezva	Požadovaná odezva pro synchronní rozhraní je do 2 sekund v limitních případech do 5 sekund. V případě delší doby odezvy je třeba využít asynchronní rozhraní. Trvání operace a její průběh je pak prezentován klientovi veřejné správy v souladu s obecným popisem SOAP a REST rozhraní uvedeným v kapitole 0.
Typ rozhraní	SOAP nebo REST, případně nativní rozhraní AIS, pokud jsou požadované webové služby implementovány na integrační platformě ESB.
Monitoring	Doporučeným způsobem monitoringu je využití obecného end-to-end a transakčního monitoringu dle parametrů uvedených v kapitole 0.

7.4.6 Webové rozhraní Formulářového serveru úředníka

Tab. 18 - [FSU] Webové rozhraní (AIFC)

Název rozhraní: [FSU] Webové rozhraní (AIFC)	
Účel	<p>Webové uživatelské rozhraní Formulářového serveru úředníka je v průběhu zpracování procesních případů ÚEP využito pro:</p> <ul style="list-style-type: none"> ▪ náhled na data podání v režimu pouze pro čtení - Z AIS má úředník možnost zobrazit data podání ve shodné podobě, v jaké jsou zobrazena i koncovému klientovi. Ve výchozím stavu je náhled v režimu pouze pro čtení. Úředník má možnost přejít do režimu úprav s požadavkem na zdůvodnění zásahu do dat podání. ▪ modifikaci dat podání úředníkem v případě řešení vad podání, s klientem veřejné správy - Úředník v rozhraní



	<p>Formulářového serveru úředníka obdrží náhled formuláře v identickém zobrazení, v jakém je formulář prezentován i koncovému klientovi. Tato skutečnost usnadňuje komunikaci vad podání a konzultace v průběhu vyplňování elektronických formulářů. Jsou-li úředníkem provedeny zásahy do dat podání, jsou nová data k dispozici v ITSP i klientovi veřejné správy, který má možnost opravu dat potvrdit opakovaným odesláním podání (opravným či zcela novým).</p> <ul style="list-style-type: none">▪ pořízení dat podání došlých jiným než ÚEP kanálem (typicky listinná podání) úředníkem - Návrh řešení ÚEP předpokládá, že všechna podání, nejenom ta učiněná prostřednictvím ÚEP, bude možné plně elektronicky zpracovat. Za tímto účelem budou všechna podání převedena do formátu ÚEP anebo pořízena úředníkem ve formátu ÚEP využitím Formulářového serveru úředníka. Z pohledu úplného elektronické zpracování podání pak bude irelevantní, kterým kanálem a v jaké formě bylo podání klienta veřejné správy doručeno působnostnímu úřadu. Zpracování na straně AIS a dalších systémů proběhne ve všech případech zcela totožně. Vedlejšími přínosy jsou:<ul style="list-style-type: none">a. klientovi veřejné správy je možné poskytnout náhled na všechna podání a jejich stav, nejenom na podání učiněná ÚEP kanálem,b. podání učiněné mimo kanál ÚEP je možné v budoucnu na ITSP přepoužít klientem veřejné správy pro vytvoření opravného anebo zcela nového podání a jeho zaslání již ÚEP kanálem.
Zdrojový systém	Formulářový server úředníka.
Technologie rozhraní	HTML link. Přesměrování klienta z AIS na Formulářový server úředníka následováním HTML link odkazu.
Způsob autentizace a autorizace	Jednotné přihlášení cestou SAML v souladu s obecným popisem v kapitole 6.3.3. Autorizaci přístupů úředníků k jednotlivým typům podání a jejich oprávnění pro práci s daty podání řídí Formulářový server úředníka s využitím autorizačních informací evidovaných v samostatném systému Formulářového serveru úředníka, adresářových službách (např. LDAP), či v jiných autorizačních systémech působnostní organizace.
Využití rozhraní	Rozhraní je využito AIS a eSSL a umožňuje uživatelům obou těchto systémů přístup k on-line webovým formulářům prezentujícím data ÚEP.
Funkcionality rozhraní	Mezi hlavní funkcionality rozhraní patří: <ul style="list-style-type: none">▪ poskytování náhledu na data podání – zobrazení XML dokumentů a souvisejících komponent tvořících data podání,



	<ul style="list-style-type: none"> poskytování formulářů podání pro úředníky působnostní organizace umožňující modifikovat podání a ve spolupráci s klientem veřejné správy pracovat na odstranění vad podání či jiných nedostatků v podání, poskytování formulářů, prostřednictvím kterých jsou pořizována data podání, která nebyla ve výchozím stavu doručena ÚEP kanálem. <p>Formulářový server úředníka a ITSP pracují nad stejnou databází podání. Tzn., že klient veřejné správy i úředník vždy přistupují ke shodným datům, a že změny provedené kteroukoliv ze stran jsou okamžitě viditelné druhé straně. Provedení změny na ITSP či ve Formulářovém serveru úředníka není považováno za úpravu podání. Potvrzení provedených úprav musí provést klient veřejné správy opakovaným odesláním upravených dat podání.</p>
Význam (priorita) rozhraní pro ÚEP	V případě nedostupnost rozhraní nebudou mít řešitelské útvary působnostních úřadů možnost zobrazovat data podání, provádět úpravy a pořizovat nová data podání. Dojde tak k zastavení procesu obsluhy procesních případů ÚEP. Možnost podání klientů veřejné správy, využitím jakéhokoliv kanálu, včetně ÚEP, není v takovém případě dotčena.
Požadovaná dostupnost	Formulářový server úředníka je využit pouze úředníky působnostní organizace. Pro účely ÚEP musí být tedy minimální dostupnost rozhraní Formulářového serveru úředníka po celou pracovní dobu řešitelských útvarů ÚEP.
Požadovaná odezva	Webové rozhraní Formulářového serveru úředníka, je webové rozhraní pro uživatele – úředníky. Maximální odezva webového rozhraní by měla být do 2 sekund, v limitních případech do 5 sekund.
Typ rozhraní	Synchronní webové rozhraní.
Monitoring	Je doporučen obecný monitoring webových rozhraní v souladu s popisem uvedeným v kapitole 0.

7.4.7 Skartační rozhraní

Tab. 19 - [AIS] Skartační rozhraní (AIFC)

Název rozhraní: [AIS] Skartační rozhraní (AIFC)	
Účel	Skartační rozhraní publikuje AIS pro eSSL. eSSL prostřednictvím tohoto rozhraní žádá o smazání všech pracovních verzí dokumentů/komponent evidovaných v pracovním úložišti dokumentů v AIS. Požadavek na smazání dokumentů je iniciován zejména z důvodů uplynutí skartačních lhůt na straně eSSL, případně z jiných důvodů souvisejících s provozem eSSL.
Zdrojový systém	AIS



Technologie rozhraní	Webové služby SOAP anebo REST, případně nativní rozhraní AIS v případě, že je komunikace zprostředkována integrační platformou ESB a požadované služby jsou implementovány na platformě ESB.
Způsob autentizace a autorizace	Autentizace a autorizace prostřednictvím klientského systémového certifikátu v souladu s popisem uvedeným v kapitole 0. Pro volání skartačního rozhraní bude autorizován pouze systém eSSL.
Využití rozhraní	Rozhraní je využito pouze eSSL.
Funkcionality rozhraní	Rozhraní přijímá požadavek na smazání jednoho či více pracovních dokumentů z pracovního úložiště dokumentů v AIS. V případě, že je dokument v okamžiku volání v AIS upravován anebo je s dokumentem jinak manipulováno tak, že není možné dokument okamžitě odstranit, je úlohou AIS zaevidovat požadavek na smazání dokumentu a provést zmazání dokumentu ihned, jak bude dokument uvolněn.
Význam (priorita) rozhraní pro ÚEP	V případě nedostupnosti tohoto rozhraní nedochází k odmazání dokumentů a mohou být porušena pravidla vyplývající ze zákonných povinností dané OVS. Případným výpadkem není dotčena možnost klientů veřejné správy podávat ÚEP kanálem ani výkon procesů zpracování ÚEP případů.
Požadovaná dostupnost	Požadovaná dostupnost může být s ohledem na dopady nižší než v případě ostatních ÚEP komponent.
Požadovaná odezva	Odezva není kritický faktor tohoto rozhraní.
Typ rozhraní	Synchronní.
Monitoring	Je doporučen obecný monitoring webových rozhraní v souladu s popisem uvedeným v kapitole 0.

7.4.8 Webové rozhraní eSSL

Tab. 20 - [eSSL] Webové rozhraní (AIFC) – HTML link

Název rozhraní: [eSSL] Webové rozhraní (AIFC) – HTML link	
Účel	Webové rozhraní eSSL poskytuje náhled pro čtení na dokumenty evidované v eSSL. Úředník pracující v AIS prostřednictvím tohoto rozhraní přistupuje k náhledům dokumentů, nebo jejich komponentám v eSSL. V AIS může být vytvořen agendově specifický rejstřík, nebo katalog dokumentů. V případě, že dokument není evidován v AIS jako pracovní dokument a obsluha AIS požaduje náhled na originální dokument či spis v eSSL, je obsluha AIS prostřednictvím tohoto rozhraní přesměrována na webové rozhraní eSSL. Tento přístup je zaznamenáván do transakčního logu eSSL.
Zdrojový systém	eSSL
Technologie rozhraní	HTML link. Přesměrování klienta z AIS na webové rozhraní eSSL následováním HTML link odkazu.



Způsob autentizace a autorizace	Rozhraní využívá jednotného systému přihlášení – single sign on (SSO) založené na technologii využívající bezpečnostní tokeny – SAML 2.0, případně WS-Federation, pokud zdrojová komponenta ÚEP nepodporuje SAML. Preferovanou technologií jednotného přihlašování je SAML. Pokud eSSL systém nepodporuje SSO využitím SAML či WS-Federation, může být využita i jiná metoda autentizace podporovaná eSSL (např. basic autentizace). V takovém případě však nebude možné využít systém jednotného přihlašování a řešitelé budou nuceni se k webovému rozhraní eSSL opakovaně přihlašovat.
Využití rozhraní	Rozhraní je využito AIS a dalšími ÚEP komponentami vyžadujícími přístup k dokumentům a komponentám v AIS.
Funkcionality rozhraní	Mezi hlavní funkcionality rozhraní patří: a. poskytování náhledu na data podání – zobrazení XML dokumentů a souvisejících komponent tvořících data podání, b. zaznamenání přístupu k dokumentu, c. poskytování vizuální podoby formulářů, prostřednictvím kterých jsou pořizována data podání, pro účely poradenství, možnost úředníka vyplnit formulář za klienta atd. přesměrováním uživatele na služby Formulářového serveru úředníka.
Význam (priorita) rozhraní pro ÚEP	Při nedostupnosti daného rozhraní nebude schopna obsluha ÚEP - úředník přistoupit v jakémkoli režimu k datům podání v eSSL a nebude možné vizuálně kontrolovat položky podání.
Požadovaná dostupnost	Rozhraní je využíváno pouze úředníky dané OVS. Pro účely ÚEP musí být tedy minimální dostupnost tohoto rozhraní po celou pracovní dobu řešitelských útvarů ÚEP.
Požadovaná odezva	Webové rozhraní je určeno pro uživatele – úředníky. Maximální odezva webového rozhraní by měla být do 2 sekund, v limitních případech do 5 sekund.
Typ rozhraní	Synchronní webové rozhraní.
Monitoring	Je doporučen obecný monitoring webových rozhraní v souladu s popisem uvedeným v kapitole 0.