

ELEKTRONIZACE ZDRAVOTNICTVÍ

Standard EZ

Dočasného úložiště

v souladu se Zákonem č. 325/2021 Sb. Zákon o elektronizaci zdravotnictví
(dále v textu též Standard)



Projekt Národní centrum elektronického zdravotnictví (registrační číslo
CZ.31.1.01/MV/22_05/0000005)

Tabulka 1 Historie změn

Historie změn			
Verze	Datum	Popis	Zpracoval
0.10	20.5.2025		

Tabulka 2 Krycí list

Dokumen t	Standard elektronického zdravotnictví –Dočasné úložiště
Status	V rámci x. porady vedení Ministerstva zdravotnictví konané dne xx.xx.2025 schváleno ministrem zdravotnictví ČR
Distribuc e	Ke zveřejnění
Schválil	

1	Standard Dočasně úložiště	6
1.1	Úvod	6
1.1.1	Definice Dočasněho úložiště	6
1.1.2	Cíle a vize	6
1.1.3	Strategie – zdůvodnění architektury	6
1.2	Rozsah působnosti	7
1.2.1	Specifikace řešení	7
1.2.2	Legislativní kontext	8
1.3	Definice aktérů	9
1.3.1	Pacient	9
1.3.2	Zdravotnický pracovník	9
1.3.3	Poskytovatel zdravotních služeb	10
1.3.4	Zdravotní pojišťovna	10
1.3.5	Statistický ústav (ÚZIS ČR)	11
1.3.6	Systém	11
1.4	Možnosti využití služeb Dočasněho úložiště pro aktéry	11
1.4.1	Poskytovatel zdravotních služeb (PZS)	11
1.4.2	Zdravotnický pracovník	11
1.4.3	Pacient	12
1.4.4	Zdravotní pojišťovna	12
1.4.5	Statistický ústav (ÚZIS ČR)	13
1.5	Všeobecné podmínky využití služeb Dočasněho úložiště	13
1.6	Technické a provozní podmínky Dočasněho úložiště	13
1.6.1	Podmínky uchovávání a výmazu dat	14
1.6.2	Odpovědnost a právní důsledky	14
1.7	Funkční specifikace	14
1.7.1	Entita záznamy	14
1.7.2	Služby úložiště	16
1.7.3	Případy užití služeb	16
1.7.4	Služby příjmu záznamů evropské interoperability	24
1.8	Implementační specifikace	24
1.8.1	Klíčové požadavky:	24
1.8.2	Povinné technologie:	24
1.8.3	Rozhraní, specifikace pro interoperabilitu a datovou komunikaci	24
1.8.4	Obsahové a technické požadavky na záznamy	43
1.8.5	Souvislosti s dalšími službami EZ	45
1.9	Kybernetická bezpečnost	45
1.9.1	Obecné a legislativní požadavky	45
1.9.2	Úroveň bezpečnosti	47
1.9.3	Definice rolí	47
1.9.4	Požadavky na bezpečnostní opatření	47

Seznam zkratek a pojmů

Zkratka	Vysvětlení
Zkratka	Vysvětlení
AD	Active Directory
AIS	Ambulantní informační systém
API	Application Programming Interface
B2B	Business-to-Business
DASTA	Datový standard pro předávání dat mezi informačními systémy zdravotnických zařízení
DDoS	Distributed Denial of Service
DRP	Disaster recovery plán
DÚ	Dočasné úložiště
EHDS	Evropský prostor pro zdravotní data
eHN	European e-Health Network – Evropská síť elektronického zdravotnictví
EP	Elektronický posudek
eREG	Registry resortu zdravotnictví
EZ	Elektronické zdravotnictví
EZKarta	Mobilní aplikace EZKarta
EZCA	Certifikační autorita elektronického zdravotnictví (MZČR)
FHIR	Fast Health Interoperability Resources, standard sdružení HL7
GUI	Grafické uživatelské rozhraní (graphical user interface)
HL7	Health Level Seven
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IČP	Identifikační číslo pracoviště
IČZ	Identifikační číslo zařízení – poskytovatele zdravotních služeb
ID ZP	Identifikátor zdravotnického pracovníka
IHE	Integrated the Healthcare Enterprise
IS	Informační Systém
ISO	International Organization for Standardization
ISSS	Informační systém sdílené služby (MVČR)
IT	Informační Technologie
ITI	Information Technology Infrastructure
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
JSU	Jednotná správa uživatelů
KIS	Klinický informační systém
KPI	Klíčové ukazatele výkonnosti (key performance indicators)
KRP	Kmenový registr pacientů
KRPZS	Kmenový registr poskytovatelů zdravotních služeb
KRZP	Kmenový registr zdravotnických pracovníků
KZR	Kmenové zdravotnické registry (projekt v rámci EZ)

LIS	Laboratorní informační systém
MHD	Mobile Access to Health Documents
MV ČR	Ministerstvo vnitra ČR
MZ ČR, MZČR	Ministerstvo zdravotnictví ČR
NCMNK	Národní centrum pro medicínské nomenklatury a klasifikace
NCEP, NCPeH	Národní kontaktní místo pro elektronické zdravotnictví National contact Point for eHealth
NCEZ	Národní centrum elektronického zdravotnictví
NČLP	Národní číselník laboratorních položek
NIA	Národní identifikační autorita
NIS	Nemocniční informační systém
NIS2	Network and Information Systems Directive 2
NPEZ	Národní portál elektronického zdravotnictví (projekt v rámci EZ)
NRPZS	Národní registr poskytovatelů zdravotních služeb
NRZP	Národní registr zdravotnických pracovníků
NZIP	Národní zdravotnický informační portál
NZIS	Národní zdravotnický informační systém
OHA	Odbor Hlavního architekta eGovernmentu
OID	Object Identifier
OWASP	Open Worldwide Application Security Project
PDF	Portable Document Format
PZS	Poskytovatel zdravotních služeb
REST	Representational State Transfer
RO	Registr oprávnění (dříve Systém správy souhlasů) anebo Registr práv a mandátů (projekt v rámci EZ)
RID	Resortní identifikátor pacienta, resp. identifikátor pacienta podle Zákona č. 325/2021 Sb., o elektronizaci zdravotnictví, §2, odst. (2) z Kmenového registru pacientů
ROB	Registr obyvatel (ISZR)
ROS	Registr osob (ISZR)
RÚIAN	Registr územní identifikace, adres a nemovitostí
SDVP	Systém dříve vyslovených přání
SEZ	Služby Elektronického Zdraví
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SoNIA	Soukromoprávní NIA (bankovní identita)
SpSZZ	Systém pro sdílený zdravotní záznam
SSO	Jednotné přihlášení (single sign-on)
SVS	Služby výměnných sítí / Sharing Value Sets
TLS	Transport Layer Security
UAT	User Acceptance Testing
UI	User Interface
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier

ÚZIS ČR	Ústav zdravotnických informací a statistiky ČR
XDS	Cross-Enterprise Document Sharing
XML	eXtensible Markup Language
ZPo	Zdravotní pojišťovna
ZP	Zdravotnický pracovník
ZZ	Zdravotnické zařízení

Seznam příloh

Příloha č.	
Příloha č. 1	
Příloha č. 2	
Příloha č. 3	
Příloha č. 4	

1 Standard Dočasné úložiště

1.1 Úvod

1.1.1 Definice Dočasného úložiště

(1) Tato kapitola vymezuje obecné podmínky využívání služeb Dočasného úložiště (dále v textu jen „DÚ“) v rámci elektronického zdravotnictví České republiky (dle Zákona č. 325/2021 Sb., o elektronizaci zdravotnictví).

DÚ je provozováno v souladu se **zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví**, a dalšími souvisejícími právními předpisy a slouží k dočasnému uchování a výměně elektronických zdravotnických záznamů mezi oprávněnými subjekty.

(2) Provozovatelem DÚ je **Ministerstvo zdravotnictví České republiky** (dále jen „provozovatel“), které vykonává správu DÚ jako **významného informačního systému veřejné správy** a jako správce osobních údajů ve smyslu **zákona č. 110/2019 Sb., o zpracování osobních údajů**, a **Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)**.

(3) DÚ je součástí **informační infrastruktury elektronického zdravotnictví České republiky** a podléhá regulaci **zákona č. 181/2014 Sb., o kybernetické bezpečnosti**, a souvisejících prováděcích předpisů, zejména **vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti**.

(4) Přístup k DÚ je umožněn pouze oprávněným subjektům, které splňují podmínky stanovené právními předpisy a technickými specifikacemi provozovatele, a to prostřednictvím **rozhraní pro programové zpracování (API)** nebo **portálového přístupu (webová aplikace)**.

1.1.2 Cíle a vize

Tento dokument stanovuje standardy, požadavky a doporučení pro Dočasné úložiště v rámci elektronizace zdravotnictví. Cílem je zajištění interoperabilního, bezpečného a efektivního řešení pro správu zdravotnické dokumentace ve výměnných sítích.

Cílem Dočasného úložiště je umožnit bezpečné a standardizované dočasné ukládání zdravotnických záznamů a jejich zpřístupnění autorizovaným subjektům. Hlavní vizí je integrace s klíčovými systémy elektronického zdravotnictví a zajištění souladu s legislativními požadavky, zejména Zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví.

1.1.3 Strategie – zdůvodnění architektury

Strategie Dočasného úložiště se opírá o principy bezpečnosti, dostupnosti a interoperability. Využívá moderní technologie pro správu, přenos a zabezpečení zdravotnických záznamů.

Architektura Dočasného úložiště je založena na distribuovaném a škálovatelném modelu, který umožňuje:

- **Bezpečné ukládání a přístup k datům** na základě ověřených standardů (např. FHIR).

Standard AAFD	Strana 6/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- **Šifrování a kontrolu integrity** zdravotnických záznamů pomocí certifikovaných metod.
- **Interoperabilitu s národními a evropskými systémy** elektronického zdravotnictví (EHDS).
- **Auditní a logovací mechanismy** pro monitorování přístupů a změn v uložených datech.

Tento dokument dále specifikuje detaily implementace Dočasného úložiště, včetně jeho technických, bezpečnostních a provozních parametrů.

1.2 Rozsah působnosti

1.2.1 Specifikace řešení

Dočasné úložiště (DÚ) je klíčovou součástí infrastruktury elektronického zdravotnictví v rámci výměnných sítí zdravotnických informací. Slouží k dočasnému ukládání a distribuci zdravotnické dokumentace mezi poskytovateli zdravotních služeb, zdravotními pojišťovnami a dalšími autorizovanými subjekty.

V souladu s Nařízením (EU) 2016/679 je provozovatelem řešení a správcem osobních údajů (Controller) Ministerstvo zdravotnictví České republiky (jako organizační složka státu), a to ze zákona 325/2021 Sb., Zákon o elektronizaci zdravotnictví.

Hlavním cílem DÚ je zajistit bezpečné, efektivní a standardizované zpracování elektronických zdravotnických záznamů po dobu nezbytně nutnou pro jejich předání mezi subjekty oprávněnými k jejich přístupu. Maximální doba pro uložení zdravotnické dokumentace je 30 dní, s výjimkou eŽádanek, jejichž platnost je nastavena na 3 roky dle novelizace Zákona č. 325/2021 Sb., o elektronizaci zdravotnictví.

DÚ je součástí Národního plánu elektronického zdravotnictví a jeho architektura je navržena s ohledem na bezpečnost, interoperabilitu a škálovatelnost v souladu s platnou legislativou ČR a EU (např. GDPR, NIS2, EHDS).

Dočasné úložiště je **centrální úložiště zdravotnických dat**, které podporuje následující klíčové funkcionality:

- **Ukládání zdravotnické dokumentace** v elektronické podobě, včetně metadat (FHIR, CDA, XML, PDF).
- **Bezpečné předávání dokumentace mezi poskytovateli zdravotních služeb a zdravotními pojišťovnami** prostřednictvím zabezpečených API a portálového řešení.
- **Validace a ověření identit** odesílatele a adresáta prostřednictvím **Kmenového registru zdravotnických pracovníků (KRZP), Kmenového registru poskytovatelů zdravotních služeb (KRPZS) a Registru práv a mandátů.**
- **Zajištění integrity a autenticity dat** prostřednictvím elektronických podpisů a certifikovaných hashovacích funkcí.
- **Možnost auditování a monitoringu přístupů** v souladu s požadavky zákona o kybernetické bezpečnosti a GDPR.
- **Notifikace oprávněných subjektů o nově uložených či přijatých dokumentech** pomocí centrálního notifikačního systému.

Standard AAFD	Strana 7/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

1.2.2 Legislativní kontext

Dočasné úložiště zdravotnických dat je zřízeno v souladu se zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví, který upravuje podmínky pro elektronické zpracování, sdílení a ochranu zdravotnických informací v České republice. Tento zákon stanovuje rámec pro Národní plán elektronického zdravotnictví, jehož cílem je zajistit bezpečnou, efektivní a interoperabilní výměnu zdravotnických dat mezi poskytovateli zdravotní péče, zdravotními pojišťovnami a státní správou.

Dočasné úložiště plní roli centrálního bodu pro dočasnou archivaci a přenos elektronických zdravotních záznamů, přičemž musí splňovat přísné požadavky na bezpečnost a ochranu osobních údajů v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a s obecným nařízením o ochraně osobních údajů (GDPR).

Zákon č. 325/2021 Sb., o elektronizaci zdravotnictví

Tento standard spadá pod Standardy elektronického zdravotnictví dle § 2 odst. 6 zákona č. 325/2021 Sb., o elektronizaci zdravotnictví.

Další relevantní legislativní předpisy

- **Národní legislativa**
 - **Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách):** Upravuje pravidla pro poskytování zdravotních služeb, včetně vedení a výměny zdravotnické dokumentace.
 - **Zákon č. 110/2019 Sb., o zpracování osobních údajů:** Implementuje GDPR v České republice a stanovuje pravidla pro zpracování osobních údajů, včetně zdravotnických dat.
 - **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti):** Definuje povinnosti pro subjekty zapojené do kritické informační infrastruktury, kam spadá i DÚ.
 - **Vyhláška č. 444/2024 Sb., o zdravotnické dokumentaci:** Stanovuje pravidla pro vedení, uchovávání, předávání a likvidaci zdravotnické dokumentace. Určuje náležitosti zdravotnické dokumentace, její obsah, formu záznamů.
 - **Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti:** Stanovuje konkrétní bezpečnostní opatření, která jsou povinná pro MZČR, jakožto významného informačního systému, pro prevenci kybernetických hrozeb.
 - **Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích:** Upravuje specifické požadavky zákona o kybernetické bezpečnosti na DÚ, které splňují kritéria pro významný informační systém.
 - **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy:** Vymezuje povinnosti správců informačních systémů veřejné správy, včetně DÚ a stanovuje opatření na ochranu proti kybernetickým hrozbám.
 - **Zákon č. 480/2004 Sb., o některých službách informační společnosti:** Upravuje pravidla pro elektronickou komunikaci a poskytování služeb informační společnosti, relevantní pro provoz DÚ.
- **Legislativa EU**
 - **Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (GDPR):** Stanovuje základní pravidla pro ochranu osobních údajů v Evropské unii.
 - **Nařízení Evropského parlamentu a Rady (EU) 2022/1420 ze dne 14. září 2022, kterým se stanoví rámec pro evropský prostor pro zdravotní data a mění nařízení (EU) 2017/745 a směrnice 2004/23/ES (EHDS):** Stanovuje pravidla pro interoperabilitu a sdílení zdravotnických dat v rámci Evropské unie.

Standard AAFD	Strana 8/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- **Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, ¹o zrušení směrnice (EU) 2016/1148 a o změně nařízení (EU) 2018/1725 a směrnice (EU) 2013/40/EU (NIS2):** Stanovuje pravidla pro kybernetickou bezpečnost v Evropské unii a upravuje pravidla pro zabezpečení DÚ jakožto poskytovatele základních služeb.

1.3 Definice aktérů

1.3.1 Pacient

Pacient je fyzická osoba, které jsou **poskytovány zdravotní služby**, a to na základě jejího **souhlasu**, nebo v případech stanovených zákonem i bez souhlasu.

V souladu se zákonem č. 372/2011 Sb., o zdravotních službách, lze pacienta charakterizovat následujícími znaky:

1. **Subjekt zdravotních služeb** – Pacient je osoba, která využívá zdravotní péči poskytovanou poskytovatelem zdravotních služeb na základě platných právních předpisů.
2. **Právní způsobilost** – Pacient může být osoba plně způsobilá k právním úkonům, ale i osoba nezletilá nebo omezená ve způsobilosti k právním úkonům, za kterou jedná její zákonný zástupce nebo opatrovník.
3. **Práva a povinnosti** – Pacient má právo na svobodnou volbu poskytovatele zdravotních služeb, na informace o svém zdravotním stavu, na ochranu osobních údajů a soukromí, stejně jako povinnost poskytnout součinnost při poskytování zdravotních služeb.
4. **Možnost odmítnutí péče** – Pacient má právo zdravotní služby odmítnout, pokud zákon nestanoví jinak (např. při povinném léčení nakažlivých nemocí).

Pacientem se rozumí nejen osoba, která aktivně vyhledává zdravotní péči, ale i osoba, které jsou zdravotní služby poskytovány v nouzových či neodkladných situacích, například při bezvědomí nebo v jiných stavech znemožňujících vyjádření souhlasu.

Pacient je současně **subjektem údajů** podle **nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)**, které stanovuje pravidla pro ochranu osobních údajů. V rámci zdravotnictví jsou osobní údaje pacienta považovány za **zvláštní kategorii osobních údajů**, která podléhá přísnější ochraně.

Pacient má právo na přístup k dokumentaci uložené v DÚ prostřednictvím **Portálu pacienta** nebo aplikace EZKarta. Může:

- Nahlížet na své zdravotní záznamy a jejich historii.
- Omezit sdílení dokumentace s konkrétními poskytovateli zdravotních služeb.
- Udělovat přístupová práva jiným osobám (např. zákonným zástupcům).

1.3.2 Zdravotnický pracovník

Zdravotnický pracovník je osoba, která získala odbornou způsobilost k výkonu zdravotnického povolání podle **zákona č. 96/2004 Sb.**, o podmínkách získávání a uznávání způsobilosti

Standard AAFD	Strana 9/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

k výkonu nelékařských zdravotnických povolání. Tato osoba vykonává činnosti související s poskytováním zdravotní péče, a to v rozsahu stanoveném právními předpisy.

Podle tohoto zákona existují různé kategorie zdravotnických pracovníků, mezi něž patří:

- **nelékařská zdravotnická povolání s odbornou způsobilostí** (např. všeobecná sestra, zdravotnický záchranář, porodní asistentka, radiologický asistent),
- **nelékařská zdravotnická povolání se specializovanou způsobilostí** (např. sestra pro intenzivní péči, fyzioterapeut se specializací),
- **nelékařská zdravotnická povolání bez odborného dohledu** (např. nutriční terapeut, klinický psycholog),
- **jiné odborné pracovníky** (např. zdravotní laborant, farmaceutický asistent).

Podrobnosti k vykonávaným činnostem těchto profesí stanovuje **vyhláška č. 55/2011 Sb.**, o činnostech zdravotnických pracovníků a jiných odborných pracovníků.

Zdravotnický pracovník je oprávněn přistupovat k DÚ prostřednictvím **autentizovaných informačních systémů** svého poskytovatele zdravotních služeb. Může:

- Ukládat zdravotnické záznamy do Dočasného úložiště.
- Stahovat a zobrazovat Zásilky pacienta, pokud má odpovídající oprávnění.
- Spravovat obsah dokumentace v souladu s legislativními podmínkami.

1.3.3 Poskytovatel zdravotních služeb

Podle § 2 odst. 1 zákona č. 372/2011 Sb., o zdravotních službách, se **poskytovatelem zdravotních služeb** rozumí fyzická nebo právnická osoba, která má oprávnění k poskytování zdravotních služeb podle tohoto zákona.

PZS je klíčovým aktérem využívajícím Dočasné úložiště. Vystupuje jako:

- **Odesílatel zásilky** – ukládá Zásilky do Dočasného úložiště.
- **Adresát zásilky** – přebírá zdravotnické Zásilky jiných PZS.
- **Ověřovatel přístupových práv** – využívá Kmenový registr poskytovatelů zdravotních služeb k ověření oprávnění zdravotnických pracovníků.

1.3.4 Zdravotní pojišťovna

Zdravotní pojišťovna je právnická osoba, která je oprávněna provozovat veřejné zdravotní pojištění na základě zákona č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, a zákona č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách. Tyto instituce zajišťují financování zdravotní péče pro pojištěnce na základě povinného veřejného zdravotního pojištění.

Zdravotní pojišťovna využívá Dočasné úložiště primárně k:

- Přístupu ke zdravotnické dokumentaci pro účely revizních kontrol.
- Ověření poskytovaných zdravotních služeb a jejich souvislosti s nároky pacienta.
- Kontrole nákladů a efektivity poskytované péče.

Standard AAFD	Strana 10/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

1.3.5 Statistický ústav (ÚZIS ČR)

Ústav zdravotnických informací a statistiky České republiky (ÚZIS ČR) je organizační složka státu zřízená Ministerstvem zdravotnictví České republiky, která vykonává činnosti v oblasti zdravotnické informatiky, statistiky a správy zdravotnických dat na základě zákona č. 372/2011 Sb., o zdravotních službách, a dalších souvisejících právních předpisů.

Ústav zdravotnických informací a statistiky ČR (ÚZIS ČR) je oprávněn získávat anonymizovaná nebo agregovaná data z Dočasného úložiště za účelem:

- Sběru a analýzy zdravotnických dat pro účely národního zdravotního výkaznictví.
- Monitorování vývoje zdravotního stavu obyvatelstva.
- Vypracování statistických a analytických přehledů pro Ministerstvo zdravotnictví a další státní instituce.

1.3.6 Systém

Jedná se o technický systém Dočasného úložiště jako takového, který provádí systémovou manipulaci s daty zásilek za účelem provozuschopnosti Dočasného úložiště.

1.4 Možnosti využití služeb Dočasného úložiště pro aktéry

Dočasné úložiště (DÚ) nabízí různé možnosti přístupu a využití služeb pro jednotlivé aktéry elektronického zdravotnictví. Služby DÚ jsou dostupné prostřednictvím API rozhraní, webového portálu nebo mobilních aplikací, a to v souladu se zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví.

1.4.1 Poskytovatel zdravotních služeb (PZS)

Poskytovatelé zdravotních služeb mají přístup k DÚ jako odesílatelé i příjemci zdravotnické dokumentace. Mohou využívat:

- **Ext. API Dočasného úložiště** – pro automatizovanou výměnu dokumentace mezi informačními systémy PZS.
- **Portál Dočasného úložiště** – pro ruční nahrávání a stahování zásilek zdravotnickými pracovníky.
- **Notifikační služby** – pro upozornění na přijetí nové zásilky.

V rámci těchto přístupů k systému Dočasného úložiště může (vždy pouze v kontextu ke konkrétní zásilce, k níž má oprávnění, nikoli ke všem zásilkám):

- Uložit zásilku,
- stáhnout zásilku,
- vyhledat zásilku,
- obdržet notifikace,
- zpochybnit zásilku.

1.4.2 Zdravotnický pracovník

Zdravotnický pracovník využívá služby DÚ v rámci svého pracoviště PZS a může využívat:

Standard AAFD	Strana 11/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- **Ext. API Dočasného úložiště** – pro automatizovanou výměnu dokumentace mezi informačními systémy PZS.
- **Portál Dočasného úložiště** – pro ruční nahrávání a stahování zásilek zdravotnickými pracovníky.
- **Notifikační služby** – pro upozornění na přijetí nové zásilky.

V rámci těchto přístupů k systému Dočasného úložiště může (vždy pouze v kontextu ke konkrétní zásilce, k níž má oprávnění, nikoli ke všem zásilkám):

- Uložit zásilku,
- stáhnout zásilku,
- vyhledat zásilku,
- obdržet notifikace,
- zpochybnit zásilku.

1.4.3 Pacient

Pacienti mají k DÚ přístup prostřednictvím **Portálu pacienta** nebo **mobilní aplikace EZKarta**. Mohou využívat:

- **Portál Elektronického zdravotnictví** – pro zobrazení zásilek.
- **Notifikační služby** – pro upozornění na přijetí nové zásilky.

V rámci těchto přístupů k systému Dočasného úložiště může:

- Stáhnout zásilku,
- vyhledat zásilku,
- zpochybnit zásilku.

1.4.4 Zdravotní pojišťovna

Zdravotní pojišťovny mohou využívat:

- **Ext. API Dočasného úložiště** – pro automatizovanou výměnu dokumentace mezi informačními systémy PZS.
- **Portál Dočasného úložiště** – pro ruční nahrávání a stahování zásilek zdravotnickými pracovníky.
- **Notifikační služby** – pro upozornění na přijetí nové zásilky.

V rámci těchto přístupů k systému Dočasného úložiště může (vždy pouze v kontextu ke konkrétní zásilce, k níž má oprávnění, nikoli ke všem zásilkám):

- Uložit zásilku,
- stáhnout zásilku,
- vyhledat zásilku,
- obdržet notifikace,
- zpochybnit zásilku.

Standard AAFD	Strana 12/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

1.4.5 Statistický ústav (ÚZIS ČR)

Ústav zdravotnických informací a statistiky ČR (ÚZIS ČR) využívá Dočasné úložiště zejména pro:

- **Přístup k anonymizovaným nebo agregovaným datům** pro zdravotnické statistiky.
- **Analýzu vývoje zdravotního stavu populace.**
- **Tvorbu reportů a přehledů pro Ministerstvo zdravotnictví.**
- **Monitorování efektivity elektronizace zdravotnictví.**

ÚZIS ČR využívá **API rozhraní** pro zpracování statistických výstupů a přístup k metadatům uložených záznamů. Nezískává však přístup k individuálním zdravotním záznamům pacientů.

1.5 Všeobecné podmínky využití služeb Dočasného úložiště

Tato kapitola stanovuje obecné podmínky využití služeb Dočasného úložiště (DÚ) v souladu se zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví. Dočasné úložiště je určeno pro bezpečné a standardizované dočasné ukládání zdravotnických záznamů s přístupem oprávněných subjektů.

Využití služeb Dočasného úložiště je podmíněno existencí právního základu a technické způsobilosti. Výhradní oprávněné subjekty s nárokem k přístupu ke službám Dočasného úložiště jsou s přesnou definicí v kapitole 1.3 :

- Pacient,
- poskytovatel zdravotních služeb,
- zdravotní pojišťovna,
- zdravotnický pracovník,
- Ústav zdravotnických informací a statistiky ČR (ÚZIS ČR).

Dočasné úložiště podporuje připojení externích systémů pomocí API nebo portálového přístupu. Každý systém musí splnit bezpečnostní a interoperabilitní požadavky, včetně:

- Autentizace v souladu s pravidly tohoto Standardu.
- Ověření oprávnění vůči registrům KRPZS a KRZP.
- Zabezpečení komunikace (TLS 1.3, OAuth 2.0).

1.6 Technické a provozní podmínky Dočasného úložiště

(1) Všechny subjekty přistupující k DÚ jsou povinny zajistit, že jejich činnost bude v souladu s platnou legislativou, pravidly kybernetické bezpečnosti a zásadami ochrany osobních údajů.

(2) DÚ je provozováno s **garantovanou dostupností** a splňuje standardy informační bezpečnosti, včetně:

a) **Autentizace a autorizace** přístupu validace v **kmenových registrech** (KRPZS, KRZP, RPM);

b) **Šifrování a integrity dat** pomocí elektronických podpisů, certifikovaných hashovacích funkcí a bezpečnostních protokolů (TLS 1.3, OAuth 2.0);

Standard AAFD	Strana 13/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

c) **Auditní záznamy** o všech operacích prováděných v DÚ v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti;

d) **Interoperabilita** na úrovni **národních a evropských zdravotnických systémů**;

e) **Automatizovaná komunikace** mezi DÚ a připojenými informačními systémy prostřednictvím zabezpečeného **API rozhraní**.

1.6.1 Podmínky uchovávání a výmazu dat

(1) Zásilký uložené v DÚ jsou uchovávány **po dobu nezbytně nutnou**, přičemž:

a) Maximální doba uchování činí **30 dnů** od data vložení zásilky;

b) Po uplynutí doby uchování dochází k **automatickému výmazu zásilky**, přičemž tato skutečnost je zaznamenána v auditních záznamech.

1.6.2 Odpovědnost a právní důsledky

(1) Oprávněné subjekty jsou odpovědné za správnost a úplnost zásilek vkládaných do DÚ.

(2) Přístupové údaje k DÚ jsou **nepřenosné** a jejich zneužití může být považováno za **porušení principů kybernetické bezpečnosti** s následnými sankcemi dle platných právních předpisů.

(3) Ministerstvo zdravotnictví nenese odpovědnost za **obsah zásilek vkládaných do DÚ**.

(4) Neoprávněný přístup k DÚ je považován za **porušení zákona č. 181/2014 Sb., o kybernetické bezpečnosti**, a může být postižen podle trestního práva.

(5) V případě incidentu spojeného s únikem osobních údajů nebo narušením bezpečnosti DÚ je provozovatel povinen postupovat v souladu s **Nařízením (EU) 2016/679 (GDPR)** a **zákonem č. 110/2019 Sb., o zpracování osobních údajů**.

1.7 Funkční specifikace

1.7.1 Entita zásilky

Zásilka představuje základní jednotku výměny součástí zdravotnické dokumentace vedené v elektronické podobě, její části nebo informace z ní určené k předání v rámci Dočasného úložiště. Jde o strukturovaný soubor dat, který obsahuje zdravotnická data určená k přenosu mezi oprávněnými subjekty v systému elektronického zdravotnictví. Každá zásilka je vybavena specifickými metadaty, která umožňují její jednoznačnou identifikaci, sledování a bezpečné doručení adresátovi.

1.7.1.1 Klíčové vlastnosti entity Zásilka

- **Unikátní identifikátor** – každá zásilka je označena jedinečným ID, které umožňuje její evidenci a zpětné dohledání.

Standard AAFD	Strana 14/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- **Obsah zázilky** – hlavním prvkem zázilky je dokument obsahující zdravotnické údaje, které jsou v souladu s platnými standardy pro elektronickou dokumentaci.
- **Metadata zázilky** – obsahují informace o odesílateli, příjemci, pacientovi, typu a formátu zázilky, datu vytvoření a dalších charakteristikách důležitých pro zpracování a ověření platnosti zázilky.
- **Doba platnosti** – zázilka je v Dočasném úložišti uchovávána po definované dobu, která odpovídá legislativním požadavkům a účelu zázilky. Po uplynutí této doby je automaticky odstraněna.
- **Bezpečnostní atributy** – každá zázilka obsahuje hash dokumentu pro zajištění integrity a elektronické podpisy pro ověření autenticity dat.
- **Stav zázilky** – zázilka může mít různé stavy (např. přijatá, stažena, zneplatněna), které umožňují sledování jejího životního cyklu.

Zázilky, které jsou předmětem sdílení v Dočasném úložišti budou obsahovat:

1. Dokumenty, které jsou předmětem výměny.
2. Metadata zázilky s informacemi podle metodiky standardu EZ:
 - a. Identifikace pacienta – RID. Identifikace pacienta podle jména, příjmení, datumu narození, rodného čísla, čísla občanského průkazu a validace na Kmenový registr pacientů (KRP).
 - b. Identifikace autora – zdroje Zázilky (ZP, PZS). Validace na Kmenový registr poskytovatelů zdravotních služeb (KRPZS) a Kmenový registr zdravotnických pracovníků (KRZP). Musí být uveden minimálně PZS.
 - c. Identifikace cíle Zázilky (ZP, PZS). Validace na Kmenový registr poskytovatelů zdravotních služeb (KRPZS) a Kmenový registr zdravotnických pracovníků (KRZP). Bude uveden pro Zázilky určené pro konkrétního adresáta.
 - d. Identifikátor zázilky.
 - e. Typ zázilky (klasifikace – výběr z číselníku definuje standard EZ).
 - f. Formát zázilky (výběr z číselníku definuje standard EZ).
 - g. Identifikátory ve zdrojovém systému (volitelná položka).
 - h. Identifikátory souvisejících zázilek.
 - i. Datum a čas vzniku zázilky (předvyplněný aktuální datum a čas).
 - j. Popis zázilky.
 - k. Velikost dokumentu (vyplňuje zasílající systém – IS PZS, IS ZP, Portál, ...).
 - l. Hash dokumentu. (vypočítá a vyplní zasílající systém – IS PZS, IS ZP, Portál, ...).

1.7.1.2 Stavy zázilky

Stavový kód	Povolený aktér pro změnu stavového kódu	Manipulace s daty zázilky na základě stavového kódu
Uložena	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna	uložení do dočasného úložiště
Stažena	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna	stažení z dočasného úložiště do lokálního úložiště daného aktéra, vymazání zázilky dle systémových pravidel
Zneplatněna	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna a to výhradně	označení zázilky atributem neplatná, zobrazení atributu ostatním aktérům

	v roli aktéra, který zasilku uložil	
Smazána	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna, systém	trvalé a nevratné smazání zasilky z dočasného úložiště
Zpochybněna	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna, systém	dočasně zpochybněná zasilka

1.7.2 Služby úložiště

1.7.2.1 Využití API

Rozhraní API slouží k možnosti využití služeb Dočasného úložiště pro systémy a aplikace třetích stran (dále také entity). Tyto entity se k Dočasnému úložišti připojují na základě níže specifikovaného API s dodržением níže popsaných pravidel, včetně bezpečnostních pravidel. Podmínkou je implementace popsaných povinných technologií na straně entit.

API podporuje tyto níže popsané služby Dočasného úložiště:

Služba	Metoda	Popis
/api/v1/zasilka/UlozZasilku/	Post	Služba slouží k uložení Zásilky jako sady dokumentů (SubmissionSets).
/api/v1/zasilka/VyhledejZasilku/	Post	Služba slouží k vyhledávání metadat spojených s dokumenty, jako jsou odeslané sady dokumentů (SubmissionSets).
/api/v1/zasilka/DejZasilku/{id}	Get	Služba slouží k získání Zásilky, která splňuje zadané parametry.
/api/v1/zasilka/ZmenZasilku/	Put	Služba slouží ke změně Zásilky, která splňuje zadané parametry. Tato služba je aplikována do stažení zasilky. Po stažení zasilky změně zasilky už bude zamezeno.
/api/v1/zasilka/ZneplatniZasilku/	Put	Služba slouží ke zneplatnění Zásilky, která splňuje zadané parametry.

1.7.2.2 Využití portálového přístupu

Portálový přístup je rozhraní typu HI (Human Interface) a slouží k využití služeb Dočasného úložiště aktérům, kteří nevyužívají přístup přes API z jiného informačního systému nebo aplikace a chtějí využít webový přístup přímo ke službám Dočasného úložiště.

Portálový přístup realizovaný formou webové aplikace pro desktopový nebo mobilní přístup přes webový prohlížeč poskytuje přístup ke všem službám Dočasného úložiště.

Portálový přístup podporuje tyto níže popsané služby Dočasného úložiště.

1.7.3 Případy užití služeb

1.7.3.1 Uložení zasilky do úložiště (přes API)

Klíčový popis služby:

Standard AAFD	Strana 16/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

Datový zdroj zásilky je informační systém nebo aplikace, které prostřednictvím API ukládá záznam do Dočasného úložiště.

Umožňuje uložit záznam do Dočasného úložiště, a to prostřednictvím nevizuálního rozhraní (API) vystaveného Dočasným úložištěm.

Role:

- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
 - Je subjekt, jejímž jménem zdravotnický pracovník zasílá Zásilku.
- Dočasné úložiště:
 - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatelé).
- PZS, zdravotní pojišťovna nebo ÚZIS ČR (adresát Zásilky):
 - Příjemce Zásilky, například praktický lékař, specialista, zdravotnické zařízení nebo ošetrovatelská služba.

Scénář využití:

1. Zdroj Zásilky pomocí svého IS/aplikace vytvoří Zásilku, která je v souladu s obsahovými a technickými požadavky ([1.8.2. Obsahové a technické požadavky záznamu](#)). Potvrdí zaslání Zásilky do Dočasného úložiště přes jeho externí nevizuální rozhraní pomocí služby [/api/v1/zasilka/UlozZasilku/](#).
2. Dočasné úložiště vykoná:
 - a. Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU (Jednotná správa uživatelů).
 - b. Ověření existence subjektů v KZR (kmenové zdravotnické registry):
 - i. Existenci pacienta podle zaslání RID (referenční číslo).
 - ii. Existenci ZP a PZS (zdroje Zásilky).
 - iii. V případě vyplnění adresáta jeho existenci.
 - c. Validaci vstupu:
 - i. Vytvoří kontrolní součet dokumentů (hash).
 - ii. Pomocí EZCA vytvoří razítko a pečeť na kontrolní součet.
 - iii. Ověří hash na vstupu (potvrdí konzistenci záznamu na vstupu).
 - d. Uložení Zásilky:
 - i. Uloží záznam do Repository.
 - ii. Uloží metadata do Registry.
 - e. Logování události do Žurnálu činností:
 - i. Vytvoří protokol podle specifikace Žurnálu činností.
 - ii. Pomocí EZCA vytvoří razítko a pečeť na protokol.
 - iii. Zašle protokol s pečeti do Žurnálu činností.
 - f. Notifikaci adresáta Zásilky pomocí centrálního notifikačního systému.
 - g. Do auditního logu jsou logovány události:
 - i. Přihlášení uživatele.
 - ii. Ověření konzistence vstupu.
 - iii. Uložení Zásilky.
 - iv. Notifikace.
 - h. Potvrzení úspěšného uložení Zásilky nebo zaslání informace uživateli o neúspěšném uložení i s identifikací a popisem chyby.

1.7.3.2 Vyhledání zásilky (přes API)

Klíčový popis služby:

Umožňuje aktérům vyhledat relevantní zásilku dle vyhledávacích kritérií a s respektem k přístupovým právům, a předložit seznam vyhledaných zásilek.

Umožňuje vyhledat relevantní zásilku v Dočasném úložišti, a to prostřednictvím nevizuálního rozhraní (API) vystaveného Dočasným úložištěm.

Role:

- PZS, zdravotní pojišťovna nebo ÚZIS ČR (adresát Zásilky):
 - Příjemce Zásilky, například praktický lékař, specialista, zdravotnické zařízení nebo ošetrovatelská služba.
- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
 - Je subjekt, jejímž jménem zdravotnický pracovník zasílá Zásilku.
- Dočasné úložiště:
 - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatele).

Scénář využití:

1. Uživatel (adresát Zásilky) pomocí svého IS zadá vyhledávací kritéria na získání Zásilek. Vyhledávat může podle položek:
 - a. Identifikátor Zásilky (z notifikace).
 - b. Odesílatel (PZS, zdravotnický pracovník, zdravotní pojišťovna).
 - c. Identifikátoru pacienta (RID, který je získán z KZR).
2. Po potvrzení uživatelem IS zašle požadavek na vyhledání ([1.8.2. Obsahové a technické požadavky zásilky](#)) do Dočasného úložiště přes jeho externí nevizuální rozhraní pomocí služby [/api/v1/zasilka/VyhledejZasilku/](#).
3. Dočasné úložiště vykoná:
 - a. Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
 - b. Ověření existence a souladu právnických a fyzických osob v KZR (kmenové zdravotnické registry):
 - i. Existenci pacienta podle zaslaného RID (referenční číslo).
 - ii. Existenci zdr. pracovníka (uživatele).
 - c. Získání rozsahu oprávnění uživatele na zdravotní dokumentaci pacienta z Registru práv a mandátů.
 - d. Vyhledání Zásilky v metadatach Registry se zohledněním:
 - i. Výběrových kritérií.
 - ii. Rozsahu oprávnění.
 - e. Logování události do Žurnálu činností:
 - i. Vytvoří protokol podle specifikace Žurnálu činností.
 - ii. Pomocí EZCA vytvoří razítko a pečeť na protokol.
 - iii. Zašle protokol s pečeti do Žurnálu činností.
 - f. Do auditního logu jsou logovány události:
 - i. Přihlášení uživatele.
 - ii. Poskytnutí seznamu.
 - g. Vrácení seznamu dokumentů, které vyhovují výběrovým kritériím a rozsahu oprávnění uživatele.
4. IS uživatele zobrazí vrácený seznam dokumentů.

Standard AAFD	Strana 18/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

1.7.3.3 Stažení zásilky (přes API)

Klíčový popis služby:

Umožňuje stáhnout záznam z Dočasného úložiště prostřednictvím nevizuálního rozhraní (API) do koncového informačního systému (aplikace) aktéra k dalšímu lokálnímu zpracování.

Role:

- PZS, zdravotní pojišťovna nebo ÚZIS ČR (adresát Zásilky):
 - Příjemce Zásilky, například praktický lékař, specialista, zdravotnické zařízení nebo ošetrovatelská služba.
- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
 - Je subjekt, jejímž jménem zdravotnický pracovník zasílá Záznam.
- Dočasné úložiště:
 - Uchovává Záznamy a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatelé).

Scénář využití:

1. Uživatel (adresát Zásilky) pomocí svého IS vytvoří požadavek na stažení Zásilky, která je identifikována identifikátorem Zásilky (z notifikace). Po potvrzení uživatelem IS zašle požadavek na stažení ([1.8.2. Obsahové a technické požadavky záznamu](#)) do Dočasného úložiště přes jeho externí nevizuální rozhraní pomocí služby [/api/v1/zasilka/DejZasilku/{id}](#).
2. Dočasné úložiště vykoná:
 - a. Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
 - b. Ověření existence a souladu právnických a fyzických osob v KZR (kmenové zdravotnické registry):
 - i. Existenci pacienta podle zaslání RID (referenční číslo).
 - ii. Existenci zdr. pracovníka (uživatelé).
 - c. Získání rozsahu oprávnění uživatele na zdravotní dokumentaci pacienta z Registru práv a mandátů.
 - d. Vyhledání Zásilky v Repository se zohledněním:
 - i. Identifikátoru Zásilky.
 - ii. Identifikátoru pacienta.
 - iii. Rozsahu oprávnění.
 - e. Validaci Zásilky z Repository:
 - i. Vytvoří kontrolní součet dokumentu (hash).
 - ii. Ověří neporušenost dokumentu vůči kontrolnímu součtu, který byl vytvořen při uložení.
 - iii. Pomocí EZCA vytvoří razítko a pečeť na kontrolní součet.
 - f. Logování události do Žurnálu činností.
 - i. Vytvoří transakční protokol o stažení dokumentace pacienta podle specifikace Žurnálu činností.
 - ii. Pomocí EZCA vytvoří razítko a pečeť na transakční protokol.
 - iii. Zašle transakční protokol s pečeti do Žurnálu činností.
 - g. Notifikaci odesílatele Zásilky pomocí centrálního notifikačního systému o stažení Zásilky.
 - h. Do auditního logu jsou logovány události:
 - i. Přihlášení uživatele.

- ii. Převzetí dokumentu.
 - iii. Stažení Zásilky.
 - iv. Notifikace.
- i. Vrácení požadovaného dokumentu.
3. IS uživatele zobrazí dokument.
4. V případě, že si Zásilku vyzvedli všichni adresáti a typ dokumentu/Zásilky požaduje vymazání Zásilky z Dočasného úložiště, Dočasné úložiště vykoná:
 - a. Smazání Zásilky z Repository.
 - b. Aktualizaci stavu Zásilky v Registry.
 - c. Logování události do Žurnálu činností.
 - i. Vytvoření transakčního protokolu o vymazání Zásilky na pacienta podle specifikace Žurnálu činností.
 - ii. Pomocí EZCA vytvoří razítko a pečeť na transakční protokol.
 - iii. Zašle transakční protokol s pečeti do Žurnálu činností.
 - d. Notifikaci odesílatele Zásilky o vymazání Zásilky pomocí centrálního notifikačního systému
 - e. Do auditního logu jsou logovány události:
 - i. Smazání Zásilky.
 - ii. Notifikace.

1.7.3.4 Zneplatnění zásilky (přes portálový API)

Klíčový popis služby:

Umožňuje označit příznakem relevantní zásilku jako neplatnou prostřednictvím nevizuálního rozhraní (API) vystaveného Dočasným úložištěm. Označení může provést výhradně ukládající aktér. Atribut zásilky "neplatná" je následně prezentován ostatním aktérům jako doprovodná informace (metadata) k dané zásilce.

Role:

- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
 - Je subjekt, jejímž jménem zdravotnický pracovník zasílá Zásilku.
- Dočasné úložiště:
 - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatele).
- PZS, zdravotní pojišťovna nebo ÚZIS ČR (adresát Zásilky):
 - Příjemce Zásilky, například praktický lékař, specialista, zdravotnické zařízení nebo ošetrovatelská služba.

Scénář využití:

1. Uživatel (odesílatel Zásilky) pomocí svého IS zašle požadavek na získání aktuálního stavu záznamu Zásilky na Dočasné úložiště přes jeho externí nevizuální rozhraní pomocí služby [/api/v1/zasilka/VyhledejZasilku/](#), která je identifikovaná:
 - a. Identifikátor Zásilky (získán při uložení Zásilky resp. z notifikace o uložení).
 - b. Odesílatel (PZS, zdravotnický pracovník, zdravotní pojišťovna).
 - c. Identifikátor pacienta (RID, který je získán z KZR).
2. Uživatel (odesílatel Zásilky) pomocí svého IS vytvoří požadavek na zneplatnění Zásilky, která je identifikována identifikátorem Zásilky:
 - a. Identifikátor Zásilky (získán při uložení Zásilky resp. z notifikace o uložení).
 - b. Odesílatel (PZS, zdravotnický pracovník, zdravotní pojišťovna).

Standard AAFD	Strana 20/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- c. Identifikátor pacienta (RID, který je získán z KZR).
- d. Verze řádku (získána pomocí služby VyhledejZasilku).
3. Po potvrzení uživatelem IS zašle požadavek na zneplatnění Zásilky ([1.8.2. Obsahové a technické požadavky zásilky](#)) do Dočasného úložiště přes jeho externí nevizuální rozhraní pomocí služby [/api/v1/zasilka/ZneplatniZasilku/](#).
4. Dočasné úložiště vykoná:
 - a. Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
 - b. Ověření existence a souladu právnických a fyzických osob v KZR (kmenové zdravotnické registry).
 - i. Existenci pacienta podle zaslání RID (referenční číslo).
 - ii. Existenci zdr. pracovníka (uživatele).
 - c. Získání rozsahu oprávnění uživatele na zdravotní dokumentaci pacienta z Registru práv a mandátů.
 - d. Vyhledání Zásilky v metadatech Registry se zohledněním:
 - i. Identifikátoru Zásilky
 - ii. Rozsahu oprávnění.
 - e. Notifikaci adresáta a odesílatele Zásilky o zneplatnění pomocí centrálního notifikačního systému.
 - f. Logování události do Žurnálu činností:
 - i. Vytvoří transakční protokol o zneplatnění dokumentace pacienta podle specifikace Žurnálu činností.
 - ii. Pomocí EZCA vytvoří razítko a pečeť na transakční protokol.
 - iii. Zašle transakční protokol s pečeti do Žurnálu činností.
 - g. Do auditního logu jsou logovány události:
 - i. Přihlášení uživatele.
 - ii. Zneplatnění Zásilky.
 - iii. Notifikace o zneplatnění.
 - h. Vrácení informace o výsledku zneplatnění Zásilky.
5. IS uživatele zobrazí výsledek operace.

1.7.3.5 Uložení zásilky do úložiště (přes portálový přístup)

Klíčový popis služby:

Datový zdroj zásilky je webový prohlížeč (koncového zařízení aktéra), prostřednictvím kterého daný aktér ukládá zásilku do Dočasného úložiště, a to prostřednictvím webového portálu vystaveného Dočasným úložištěm.

Umožňuje uložit zásilku do Dočasného úložiště a to prostřednictvím vizuálního rozhraní (portál – webová služba) vystaveného Dočasným úložištěm.

Role:

- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
 - Je subjekt, jejímž jménem zdravotnický pracovník zasílá Zásilku.
- Dočasné úložiště:
 - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatele).

Scénář využití:

Při uložení Zásilky přes Portál je, oproti uložení přes API – „1.7.3.1 Uložení zásilky do úložiště (přes API)“, rozdíl v začátku procesu. Vnitřně na straně Dočasného úložiště je komunikace

Standard AAFD	Strana 21/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

komponentů shodná jako při uložení Zásilky přes API. Proto aktivity uvnitř Dočasného úložiště nejsou v tomto scénáři popsány.

1. Uživatel (zdroj Zásilky) vykoná:
 - a. Přihlášení se na Portál v roli „zdravotnický pracovník“ nebo „pracovník zdravotní pojišťovny“.
 - b. Výběr funkce „Nová Zásilka“.
 - c. Vyplnění dat o Zásilce:
 - i. Identifikace pacienta (validace na KZR).
 - ii. Identifikace autora Zásilky - zdr. pracovník – přihlášený uživatel (validace na KZR).
 - iii. Identifikace autora Zásilky – PZS nebo zdr. pojišťovna (validace na KZR).
 - iv. Identifikace cíle Zásilky – PZS, zdr. pojišťovna nebo ÚZIS, zdr. pracovník (validace na KZR).
 - v. Typ dokumentu (výběr z číselníku).
 - vi. Formát dokumentu (výběr z číselníku).
 - vii. Identifikátor ve zdrojovém systému (volitelné).
 - viii. Identifikátory souvisejících dokumentů (volitelné).
 - ix. Datum a čas vzniku dokumentu (předvyplněný aktuální datum a čas).
 - x. Popis dokumentu.
 - d. Načtení dokumentu na zaslání.
 - e. Spuštění kontroly Zásilky.
2. Portál vypočítá kontrolní součet dokumentu (hash), velikost dokumentu, vykoná validaci celého vstupu. V případě správnosti umožní zaslání Zásilky do Dočasného úložiště.
3. Zdravotnický pracovník (zdroj Zásilky) potvrdí „Ulož Zásilku“.
4. Portál zašle Zásilku do Dočasného úložiště.
5. Dočasné úložiště vykoná zpracování Zásilky a vrátí informaci o výsledku zpracování.
6. Portál zobrazí výsledek zpracování uživateli.

1.7.3.6 Zneplatnění zásilky (přes portálový přístup)

Klíčový popis služby:

Umožňuje označit příznakem relevantní zásilku jako neplatnou prostřednictvím vizuálního rozhraní (portál – webový služba) vystaveného Dočasným úložištěm. Označení může provést výhradně ukládající aktér. Atribut zásilky "neplatná" je následně prezentován ostatním aktérům jako doprovodná informace (metadata) k dané zásilce. Scénář může být vykonán nad jedním vybraným záznamem a musí mu předcházet vyhledání Zásilky nebo uložení nové Zásilky v případě, že byla uložena chybně.

Role:

- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
 - Je subjekt, jejímž jménem zdravotnický pracovník zasílá Zásilku.
- Dočasné úložiště:
 - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatele).

Scénář využití:

Scénář zneplatnění předpokládá, že uživatel má vybrán právě jeden záznam, jehož je autorem.

1. Uživatel (zdroj Zásilky) v vybere funkci „Zneplatnění Zásilky“ a potvrdí její vykonání.

Standard AAFD	Strana 22/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

2. Portál pošle požadavek na zneplatnění Zásilky do Dočasného úložiště.
3. Dočasné úložiště vykoná zpracování zneplatnění Zásilky a vrátí informaci o výsledku zpracování.
4. Portál zobrazí výsledek zpracování uživateli.

1.7.3.7 Vyhledání a stažení zásilky (přes portálový přístup)

Klíčový popis služby:

Umožňuje aktérům vyhledat relevantní zásilku dle vyhledávacích kritérií a s respektem k přístupovým právům, a předložit seznam vyhledaných zásilek.

Umožňuje vyhledat relevantní zásilku v Dočasném úložišti, a to prostřednictvím vizuálního rozhraní (portál – webová služba) vystaveného Dočasným úložištěm. Následně služba umožní stáhnutí z Dočasného úložiště prostřednictvím vizuálního rozhraní (portál – webová služba) do koncového zařízení aktéra k dalšími lokálnímu zpracování.

Role:

- PZS, zdravotní pojišťovna nebo ÚZIS ČR (adresát Zásilky):
 - Příjemce Zásilky, například praktický lékař, specialista, zdravotnické zařízení nebo ošetrovatelská služba.
- Dočasné úložiště:
 - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatele).

Scénář využití:

Při vyhledání a stažení Zásilky přes Portál je (oproti stažení přes API) rozdíl v začátku procesu. Vnitřně na straně Dočasného úložiště je komunikace komponentů shodná jako při vyhledání nebo stažení Zásilky přes API. Proto aktivity uvnitř Dočasného úložiště nejsou v tomto scénáři popsány.

1. Uživatel (adresát Zásilky) vykoná:
 - a. Přihlášení se na Portál v roli s oprávněním na stažení zdr. dokumentace (zdravotnický pracovník, pracovník ÚZIS, pracovník pojišťovny).
 - b. Výběr funkce „Seznam Zásilek“.
 - c. Zadání vyhledávacích kritérií, kterými mohou být:
 - i. Identifikátor Zásilky (z notifikace).
 - ii. Identifikace pacienta (validace na KZR).
 - iii. Identifikace odesílatele Zásilky - zdr. pracovník (validace na KZR).
 - iv. Identifikace odesílatele Zásilky – PZS (validace na KZR).
 - v. Typ dokumentu (výběr z číselníku).
 - vi. Formát dokumentu (výběr z číselníku).
 - d. Potvrzení vyhledání dokumentů.
2. Portál zašle dotaz do Dočasného úložiště.
3. Dočasné úložiště vykoná vyhledání podle zadaných kritérií a vrátí seznam dokumentů.
4. Portál zobrazí výsledek zpracování uživateli.
5. Uživatel vybere jeden dokument a potvrdí jeho stažení.
6. Portál zašle dotaz na stažení do Dočasného úložiště.
7. Dočasné úložiště umožní stažení dokumentu.
8. Portál vykoná stažení dokumentu, zobrazí obsah dokumentu uživateli a umožní jeho uložení do lokálního adresáře uživatele.

Standard AAFD	Strana 23/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

1.7.4 Služby příjmu zásilek evropské interoperability

Služba Dočasného úložiště umožňuje ukládání EHR doručené v rámci interoperability zdravotnických záznamů Evropské unie prostřednictvím Národního kontaktního místa pro elektronické zdravotnictví – elektronické služby určené pro přeshraniční i vnitrostátní výměnu zdravotnických údajů, a to těm aktérům, kteří nemají na úrovni centrálních služeb elektronického zdravotnictví evidovanou Akreditovanou afinitní doménu (AAfD) jako svoji domovskou (atribut HCID). Bližší specifikace je uvedena ve Standardu elektronického zdravotnictví – Standard Akreditovaných afinitních domén.

Ukládání tohoto typu EHR zásilek do Dočasného úložiště se řídí tímto pravidlem:

- Pokud existuje platný záznam na úrovni Centrálních služeb elektronického zdravotnictví o příslušnosti daného PZS k některé z Akreditovaných afinitních domén (ve smyslu existence platnému HCID záznamu), je daná zásilka EHR ukládána do příslušné AAfD
- Pokud výše uvedený záznam není nalezen, je zásilka uložena do Dočasného úložiště příslušnému PZS. Je využit scénář 1.7.3.1 Uložení zásilky do úložiště (přes API).

1.8 Implementační specifikace

Implementační specifikace definuje technické a provozní požadavky na systémy, které se integrují s Dočasným úložištěm elektronického zdravotnictví.

1.8.1 Klíčové požadavky:

- **Podpora API** dle specifikace OpenAPI 3.1.0.
- **Komunikace přes HTTPS** s TLS 1.2 nebo vyšší.
- **Autentizace a autorizace** prostřednictvím Jednotné správy uživatelů (JSU).
- **Validace dat** vůči Kmenovým registrům (KRP, KRPZS, KRZP).
- **Formát dokumentů:** PDF, CDA, DICOM apod., s odpovídajícím MIME typem.
- **Zabezpečení integrity** pomocí hash hodnoty a elektronického podpisu (EZCA).
- **Logování událostí** do Žurnálu činností včetně časového razítkování.
- **Zpracování výjimek** dle standardizovaných HTTP stavových kódů (např. 400, 401, 403, 5XX).

1.8.2 Povinné technologie:

- RESTful služby
- JSON jako výměnný formát
- Base64 kódování binárních dat (dokumenty)

Rozhraní musí být implementováno tak, aby podporovalo celý životní cyklus zásilky: vytvoření, uložení, vyhledání, změnu, stažení a zneplatnění.

1.8.3 Rozhraní, specifikace pro interoperabilitu a datovou komunikaci

Pro zajištění bezpečné, jednoznačné a interoperabilní výměny elektronických zdravotnických dokumentů mezi subjekty systému elektronického zdravotnictví (např. PZS, zdravotní

Standard AAfD	Strana 24/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

pojišťovny, zdravotní pracovníci) je definováno standardizované technické rozhraní a odpovídající specifikace pro datovou komunikaci.

Systém Dočasného úložiště poskytuje dvě formy rozhraní:

- **API rozhraní (RESTful API)** – určeno pro systémy třetích stran (např. nemocniční IS), umožňuje strojové volání služeb.
- **Portálové (webové) rozhraní** – určeno pro manuální použití uživateli (lékaři, pacienti, pracovníci pojišťoven), realizované jako webová aplikace.

1.8.3.1 API rozhraní

Pro komunikaci mezi systémy slouží následující API služby:

- **/api/v1/zasilka/UlozZasilku/**
Metoda: POST
Účel: Uložení zasilky do Dočasného úložiště s validací dat, výpočtem kontrolního součtu a vytvořením digitálního razítka.
- **/api/v1/zasilka/VyhledejZasilku/**
Metoda: POST
Účel: Vyhledávání zásilek na základě zadaných kritérií (identifikátor, informace o pacientovi a odesílateli).
- **/api/v1/zasilka/DejZasilku/{id}**
Metoda: GET
Účel: Stažení konkrétní zasilky na základě jejího identifikátoru.
- **/api/v1/zasilka/ZmenZasilku/**
Metoda: PUT
Účel: Úprava zasilky, zejména k evidenci stažení nebo aktualizaci stavu.
- **/api/v1/zasilka/ZneplatniZasilku/**
Metoda: PUT
Účel: Označení zasilky jako neplatné s následnou notifikací adresátů.

Každý end-point podléhá přísné autentizaci a autorizaci pomocí JSU (Jednotná správa uživatelů) a ověřování subjektů v kmenových registrech, například KRZP a KRPZS.

1.8.3.1.1 Služba UlozZasilku

Klíčový popis služby:

Služba slouží k uložení Zasilky jako sady dokumentů (SubmissionSets). Tato služba je ekvivalentem dotazu Simplified Publish [ITI-105]. Odesílatel Zasilky používá HTTP zadávací dotaz k uložení Zasilky. Dotaz je parametrizován podle standardu FHIR.

Pro uložení zasilky se ID hodnota a hodnota verze Řádku zadávají jako "null" ve smyslu příkladu uvedeného níže. Hodnoty budou doplněny do záznamu po zaevidování ze strany dočasného úložiště. Po uložení zasilky odesílateli je vrácen GUID a verzeRadku pro případ zneplatnění nebo změny zasilky. Bez správné hodnoty verze Radku nelze záznam upravovat. Tento údaj slouží pro ochranu před mylnými dotazy. Číselníkové hodnoty použité při voláních je třeba stáhnout z Terminologického serveru v příslušné aktuální verzi.

Prostřednictvím služby UlozZasilku lze zaslat i více souborů zařazených do složek s maximální velikostí zasilky 80MB.

Standard AaFD	Strana 25/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

Role:

- Odesílatel
 - Je subjekt, jehož jménem zdravotnický pracovník zasílá Zásilku.
- Adresát
 - Ošetřující zdravotnický pracovník, který přijímá jménem PZS Zásilku

Request:

```
{
  "id": null,
  "verzeRadku": null,
  "nazev": "Lékařská zpráva",
  "popis": "Lékařská zpráva z vyšetření",
  "stav": {
    "kod": "PRIJATA",
    "verze": "1.0"
  },
  "typ": {
    "kod": "LEKZPRAVA",
    "verze": "1.0"
  },
  "klasifikace": {
    "kod": "LABVYS",
    "verze": "1.0"
  },
  "odbornost": {
    "kod": "LABORATOR",
    "verze": "1.0"
  },
  "datumOd": "2025-02-12T09:32:46.114Z",
  "datumDo": "2025-03-12T09:32:46.114Z",
  "autor": 0,
  "zdravotnickýPracovník": 0,
  "poskytovatel": 0,
  "pacient": 0,
  "ispzs": "Nemocniční informační systém XY",
  "adresat": 0,
  "adresatTyp": {
    "kod": "PZS",
    "verze": "1.0"
  },
  "dostupnost": true,
  "rodic": null,
  "udalost": {
    "kod": "VYSETRENI",
    "verze": "1.0"
  },
  "dokument": [
    {
      "id": null,
      "verzeRadku": null,
      "nazev": "Lékařská zpráva pacienta",
      "popis": "Lékařská zpráva z ortopedického vyšetření",
      "jazyk": {
```

```

    "kod": "cz",
    "verze": "1.0"
  },
  "typ": {
    "kod": "LEKZPRAVA",
    "verze": "1.0"
  },
  "klasifikace": {
    "kod": "LABVYS",
    "verze": "1.0"
  },
  "kod": "string",
  "autor": 0,
  "poskytovatel": 0,
  "pacient": 0,
  "dostupnost": true,
  "duvernost": {
    "kod": "ZDRAVZAZNAM",
    "verze": "1.0"
  },
  "format": {
    "kod": "PDF",
    "verze": "1.0"
  },
  "mime": {
    "kod": "application/pdf",
    "verze": "1.0"
  },
  "hash":
  "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac849b",
  "velikost": 0,
  "vazanyDokument": null,
  "soubor": {
    "soubor":
  "R01GODlhAQABAIAAAP//wAAACH5BAEAAAAALAAAAABAAEAAAICRAEAOw==",
    "cesta": null
  },
  "slozka": {
    "id": null,
    "nazev": "Přílohy",
    "popis": "string",
    "autor": 0
  }
}
]
}

```

Response:

Kód	201	400	401	403	5xx
-----	-----	-----	-----	-----	-----

Standard AAFD	Strana 27/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

Response	Zásilka je uložena	Aplikační chyba	Chyba autorizace vůči Dočasnému úložišti	Přístupující subjekt nemá právo na volanou službu Dočasného úložiště	Nefunkční stav služby
Body	id (String) verzeRadku (String)				

1.8.3.1.2 Služba VyhledejZasilku

Klíčový popis služby:

Služba slouží k vyhledávání metadat spojených s dokumenty, jako jsou odeslané sady dokumentů (SubmissionSets). Tato služba je ekvivalentem následujících dotazů FindSubmissionSets v transakci Registry Stored Query [ITI-18] (viz ITI TF-2: 3.18.4.1.2.3.7.2).

Vyhledávání zásilky je prováděno na základě data vytvoření zásilky. Ve vyhledávaném seznamu se následně nacházejí pouze záznamy před ukončením data platnosti nebo zásilky, které nebyly zneplatněny/zpochybněny. Seřazení záznamů je na základě data vytvoření, kde nejnovější údaj je na prvním místě.

Role:

- Odesílatel
 - Subjekt, který dohledává jím zaslané zásilky
- Adresát
 - Subjekt vyhledávající zásilku.

Parametry vyhledávání:

- Pacient:
 - RID identifikátor pacienta, kterému seznam náleží.
- Autor:
 - Identifikátor autora Zásilky, který Zásilku vytvořil.
- Příjemce:
 - Identifikátor příjemce Zásilky.
- Poskytovatel:
 - Identifikátor poskytovatele, který Zásilku vytvořil.
- DatumOd:
 - Datumové ohraničení nejstaršího datumu vytvoření Zásilky. (Např. Od 01.01.2004)
- DatumDo:
 - Datumové ohraničení nejmladšího datumu vytvoření Zásilky. (Např. Do 31.12.2020)
- Stránkování:

Standard AAFD	Strana 28/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- page: první záznam
- size: počet záznamu pro vyhledání

Request:

```
{
  "pacient": 0,
  "autor": 0,
  "prijemce": 0,
  "poskytovatel": 0,
  "datumOd": "2025-04-04T08:43:30.306Z",
  "datumDo": "2025-04-27T08:43:30.306Z",
  "strankovani": {
    "page": 1,
    "size": 10
  }
}
```

Response:

Kód	200	400	401	403	5xx
Response	Zásilka je nalezena ano/ne	Aplikační chyba	Chyba autorizace vůči Dočasnému úložišti	Přístupující subjekt nemá právo na volanou službu Dočasného úložiště	Nefunkční stav služby
Body	Viz Výsledek vyhledání				

Výsledek vyhledání:

```
{
  "pocet": 1,
  "zasilka": [
    {
      "id": "blea47de-a177-4ade-924e-50c241365be4",
      "verzeRadku": "AAAAAAAADPg=",
      "nazev": "Lékařská zpráva - změna",
      "popis": "Lékařská zpráva z vyšetření - změna",
      "stav": {
        "kod": "PRIJATA",
        "verze": "1.0"
      },
      "typ": {
        "kod": "LEKZPRAVA",
        "verze": "1.0"
      },
      "klasifikace": {
        "kod": "LABVYS",
        "verze": "1.0"
      }
    }
  ],
}
```

Standard AAFD	Strana 29/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

```

"odbornost": {
  "kod": "LABORATOR",
  "verze": "1.0"
},
"datumOd": "2025-02-12T09:32:46.114",
"datumDo": "2025-03-12T09:32:46.114",
"datumVytvoreni": "2025-04-10T12:18:18.73",
"autor": 0,
"zdravotnickýPracovník": 0,
"poskytovatel": 0,
"pacient": 0,
"ispzs": "Nemocniční informační systém XY",
"adresat": 0,
"adresatTyp": {
  "kod": "PZS",
  "verze": "1.0"
},
"dostupnost": true,
"rodic": null,
"udalost": {
  "kod": "VYSETRENI",
  "verze": "1.0"
},
"dokument": [
  {
    "id": "b37ae731-3d26-49a6-91f9-acb56538d3ff",
    "verzeRadku": "AAAAAAAADPY=",
    "nazev": "Lékařská zpráva pacienta",
    "popis": "Lékařská zpráva z ortopedického vyšetření",
    "jazyk": {
      "kod": "cz",
      "verze": "1.0"
    },
    "typ": {
      "kod": "LEKZPRAVA",
      "verze": "1.0"
    },
    "klasifikace": {
      "kod": "LABVYS",
      "verze": "1.0"
    },
    "kod": "string",
    "autor": 0,
    "poskytovatel": 0,
    "pacient": 0,
    "dostupnost": true,
    "duvernost": {
      "kod": "ZDRAVZAZNAM",
      "verze": "1.0"
    },
    "format": {
      "kod": "PDF",
      "verze": "1.0"
    }
  }
]

```

```

    },
    "mime": {
      "kod": "application/pdf",
      "verze": "1.0"
    },
    "hash":
    "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac849b",
    "velikost": 0,
    "vazanyDokument": null,
    "soubor": {
      "id": "abac085d-6300-4117-ae6a-7ff34a246491",
      "soubor": null,
      "cesta": null
    },
    "slozka": {
      "id": "76d5cc8e-e1c2-41bd-9331-0cf3bd91ad50",
      "verzeRadku": "AAAAAAAADPc=",
      "nazev": "Přílohy",
      "autor": 0,
      "datumVytvoreni": "2025-04-10T12:18:18.73",
    }
  }
]
}

```

1.8.3.1.3 Služba DejZasilku

Klíčový popis služby:

Služba slouží k získání Zásilky, která splňuje zadané ID zásilky. Tato služba je ekvivalentní dotazům FindDocumentsByReferenceId z transakce "Registry Stored Query" [ITI-18].

V případě zavolání služby DejZasilku je daný datum stažení automaticky zapsáno do registru zásilek. Stažením zásilky se zásilky upraví i datum platnosti záznamu na aktuální den. V daný den je možné nadále stažení příslušné zásilky pro eliminaci případných technických problémů při stahování zásilky. Následující kalendářní den bude však příslušná zásilka již nedostupnou. Prodloužení platnosti zásilky bude možné následně provést výhradně prostřednictvím admin portálu MZ ČR. Každé stažené zásilky je zaznamenáno. Stažení zásilky mění automaticky stav zásilky na "Stažena"

Role:

- Adresát
 - Subjekt stahující zásilku

Parametr pro stáhnutí zásilky:

- id:
 - identifikátor Zásilky.

Standard AAFD	Strana 31/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

Příklad: GET /api/v1/zasilka/DejZasilku/b1ea47de-a177-4ade-924e-50c241365be4

Request:

```
{
}
```

Response:

Kód	200	400	401	403	5xx
Response	Zásilka je nalezena ano/ne	Aplikační chyba	Chyba autorizace vůči Dočasnému úložišti	Přístupující subjekt nemá právo na volanou službu Dočasného úložiště	Nefunkční stav služby
Body	Viz Výsledek volání				

Výsledek volání:

```
{
  "id": "blea47de-a177-4ade-924e-50c241365be4",
  "verzeRadku": "AAAAAAAADPg=",
  "nazev": "Lékařská zpráva - změna",
  "popis": "Lékařská zpráva z vyšetření - změna",
  "stav": {
    "kod": "PRIJATA",
    "verze": "1.0"
  },
  "typ": {
    "kod": "LEKZPRAVA",
    "verze": "1.0"
  },
  "klasifikace": {
    "kod": "LABVYS",
    "verze": "1.0"
  },
  "odbornost": {
    "kod": "LABORATOR",
    "verze": "1.0"
  },
  "datumOd": "2025-02-12T09:32:46.114",
  "datumDo": "2025-03-12T09:32:46.114",
  "datumVytvoreni": "2025-04-10T12:18:18.73",
  "autor": 0,
  "zdravotnickýPracovník": 0,
  "poskytovatel": 0,
  "pacient": 0,
  "ispzs": "Nemocniční informační systém XY",
  "adresat": 0,
  "adresatTyp": {
    "kod": "PZS",

```

```

    "verze": "1.0"
  },
  "dostupnost": true,
  "rodic": null,
  "udalost": {
    "kod": "VYSETRENI",
    "verze": "1.0"
  },
  "dokument": [
    {
      "id": "b37ae731-3d26-49a6-91f9-acb56538d3ff",
      "verzeRadku": "AAAAAAAADPY=",
      "nazev": "Lékařská zpráva pacienta",
      "popis": "Lékařská zpráva z ortopedického vyšetření",
      "jazyk": {
        "kod": "cz",
        "verze": "1.0"
      },
      "typ": {
        "kod": "LEKZPRAVA",
        "verze": "1.0"
      },
      "klasifikace": {
        "kod": "LABVYS",
        "verze": "1.0"
      },
      "kod": "string",
      "autor": 0,
      "poskytovatel": 0,
      "pacient": 0,
      "dostupnost": true,
      "duvernost": {
        "kod": "ZDRAVZAZNAM",
        "verze": "1.0"
      },
      "format": {
        "kod": "PDF",
        "verze": "1.0"
      },
      "mime": {
        "kod": "application/pdf",
        "verze": "1.0"
      },
      "hash":
      "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac849b",
      "velikost": 0,
      "vazanyDokument": null,
      "soubor": {
        "id": "abac085d-6300-4117-ae6a-7ff34a246491",
        "soubor": null,
        "cesta": null
      },
      "slozka": {

```

```

    "id": "76d5cc8e-e1c2-41bd-9331-0cf3bd91ad50",
    "verzeRadku": "AAAAAAAADPc="
    "nazev": "Přílohy",
    "autor": 0,
    "datumVytvoreni": "2025-04-10T12:18:18.73",
  }
}
]
}
}

```

1.8.3.1.4 Služba ZmenZasilku

Klíčový popis služby:

Služba slouží ke změně Zásilky. Tato služba je aplikována do prvního stažení zásilky. Po stažení zásilky už změně zásilky bude zamezeno. Výsledkem dotazu je ID upravené zásilky obsahující nová změněná data DocumentReference. Změnit nelze zneplatněnou zásilku. Každá změna zásilky je zaznamenána.

Role:

- Odesílatel
 - Subjekt s potřebou upravit/opravit zásilku před jej stáhnutí.

Parametry vyhledávání:

- id:
 - identifikátor Zásilky.
- verzeRadku
 - identifikátor záznamu

Příklad: PUT /api/v1/zasilka/ZmenZasilku/

Request:

```

{
  "id": "blea47de-a177-4ade-924e-50c241365be4",
  "verzeRadku": "AAAAAAAADPg=",
  "nazev": "Lékařská zpráva - změna",
  "popis": "Lékařská zpráva z vyšetření - změna",
  "stav": {
    "kod": "PRIJATA",
    "verze": "1.0"
  },
  "typ": {
    "kod": "LEKZPRAVA",
    "verze": "1.0"
  },
  "klasifikace": {
    "kod": "LABVYS",
    "verze": "1.0"
  }
}

```

Standard AAFD	Strana 34/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

```

},
"odbornost": {
  "kod": "LABORATOR",
  "verze": "1.0"
},
"datumOd": "2025-02-12T09:32:46.114",
"datumDo": "2025-03-12T09:32:46.114",
"datumVytvoreni": "2025-04-10T12:18:18.73",
"autor": 0,
"zdravotnickýPracovník": 0,
"poskytovatel": 0,
"pacient": 0,
"ispzs": "Nemocniční informační systém XY",
"adresat": 0,
"adresatTyp": {
  "kod": "PZS",
  "verze": "1.0"
},
"dostupnost": true,
"rodic": null,
"udalost": {
  "kod": "VYSETRENI",
  "verze": "1.0"
},
"dokument": [
  {
    "id": "b37ae731-3d26-49a6-91f9-acb56538d3ff",
    "verzeRadku": "AAAAAAAADPY=",
    "nazev": "Lékařská zpráva pacienta",
    "popis": "Lékařská zpráva z vyšetření",
    "jazyk": {
      "kod": "cz",
      "verze": "1.0"
    },
    "typ": {
      "kod": "LEKZPRAVA",
      "verze": "1.0"
    },
    "klasifikace": {
      "kod": "LABVYS",
      "verze": "1.0"
    },
    "kod": "string",
    "autor": 0,
    "poskytovatel": 0,
    "pacient": 0,
    "dostupnost": true,
    "duvernost": {
      "kod": "ZDRAVZAZNAM",
      "verze": "1.0"
    },
    "format": {
      "kod": "PDF",

```

```

    "verze": "1.0"
  },
  "mime": {
    "kod": "application/pdf",
    "verze": "1.0"
  },
  "hash":
    "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac849b",
    "velikost": 0,
    "vazanyDokument": null,
    "soubor": {
      "id": "abac085d-6300-4117-ae6a-7ff34a246491",
      "soubor": null,
      "cesta": null
    },
    "slozka": {
      "id": "76d5cc8e-e1c2-41bd-9331-0cf3bd91ad50",
      "verzeRadku": "AAAAAAAADPc="
      "nazev": "Přílohy",
      "autor": 0,
      "datumVytvoreni": "2025-04-10T12:18:18.73",
    }
  }
}
]
}
}

```

Response:

Kód	200	400	401	403	5xx
Response	Zásilka je změněna ano/ne	Aplikační chyba	Chyba autorizace vůči Dočasnému úložišti	Přístupující subjekt nemá právo na volanou službu Dočasného úložiště	Nefunkční stav služby
Body	id (String) verzeRadku (String)				

1.8.3.1.5 Služba ZneplatniZasilku
Klíčový popis služby:

Standard AAFd	Strana 36/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

Služba slouží ke zneplatnění Zásilky, která splňuje zadané parametry. Výsledkem dotazu je ID a verze řádku. Zásilku po zneplatnění není možné stáhnout nebo znovu zneplatnit. Zneplatnění zásilky mění automaticky stav zásilky na "Zneplatněna". Každé zneplatnění zásilky je zaznamenáno. Datum konce platnosti zásilky není upravováno. Z bezpečnostních důvodů je třeba zaslat spolu s ID zásilky i příslušnou verzi řádku.

Role:

- Adresát
 - Subjekt zneplatňující zásilku

Parametry vyhledávání:

- id:
 - identifikátor Zásilky.
- verzeRadku
 - identifikátor záznamu

Příklad: PUT /api/v1/zasilka/ZneplatniZasilku/

Request:

```
{
  "id": "b1ea47de-a177-4ade-924e-50c241365be4",
  "verzeRadku": "AAAAAAAADPg="
}
```

Response:

Kód	200	400	401	403	5xx
Response	Zásilka je zneplatněna ano/ne	Aplikační chyba	Chyba autorizace vůči Dočasnému úložišti	Přistupující subjekt nemá právo na volanou službu Dočasného úložiště	Nefunkční stav služby
Body	id (String) verzeRadku (String)				

1.8.3.2 Portálové rozhraní

Portálový přístup zajišťuje vizuální interakci uživatelů s Dočasným úložištěm:

Standard AaFD	Strana 37/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- **Funkce přihlášení a role:** Uživatelé se přihlašují pomocí svých přístupových údajů a role (např. zdravotnický pracovník, pracovník pojišťovny) jsou ověřovány proti JSU.
- **Uživatelské akce:** Ukládání záznamů, otevření, vyhledávání, stažení nebo zneplatnění se provádějí prostřednictvím intuitivního grafického rozhraní s okamžitou zpětnou vazbou a notifikacemi.
- **Logování a audit:** Veškeré operace prováděné prostřednictvím portálu jsou logovány a pravidelně auditovány tak, aby byla zajištěna konzistentnost a bezpečnost výměny dat.

1.8.3.3 Standardy interoperability

Systém je navržen v souladu s následujícími specifikacemi a standardy:

- **IHE XDS.b** – základní rámec pro výměnu dokumentů mezi systémy (registry a repozitáře)
- **HL7 CDA (Clinical Document Architecture)** – pro strukturované zdravotnické dokumenty
- **HL7 FHIR (Fast Healthcare Interoperability Resources)** – podpora budoucího přechodu na moderní interoperabilní rozhraní
- **ISO/IEC 17090** – pro elektronické podpisy, důvěrnost a integritu
- **OpenAPI 3.1.0** – pro specifikaci API služeb

1.8.3.4 Datová komunikace a bezpečnost

Veškerá komunikace probíhá přes zabezpečené HTTPS kanály a je šifrována dle požadavků eIDAS a GDPR. Zároveň veškerá komunikace je aj logována.

Bezpečnostní opatření:

- Autentizace přes jednotnou správu uživatelů (JSU)
- Oprávnění validována proti Kmenovým registrům (KRP, KRPZS, KRZP)
- Kontrola integrity pomocí hash hodnot a elektronických pečeti (EZCA)
- Uchovávání protokolů o každé transakci v Žurnálu činností

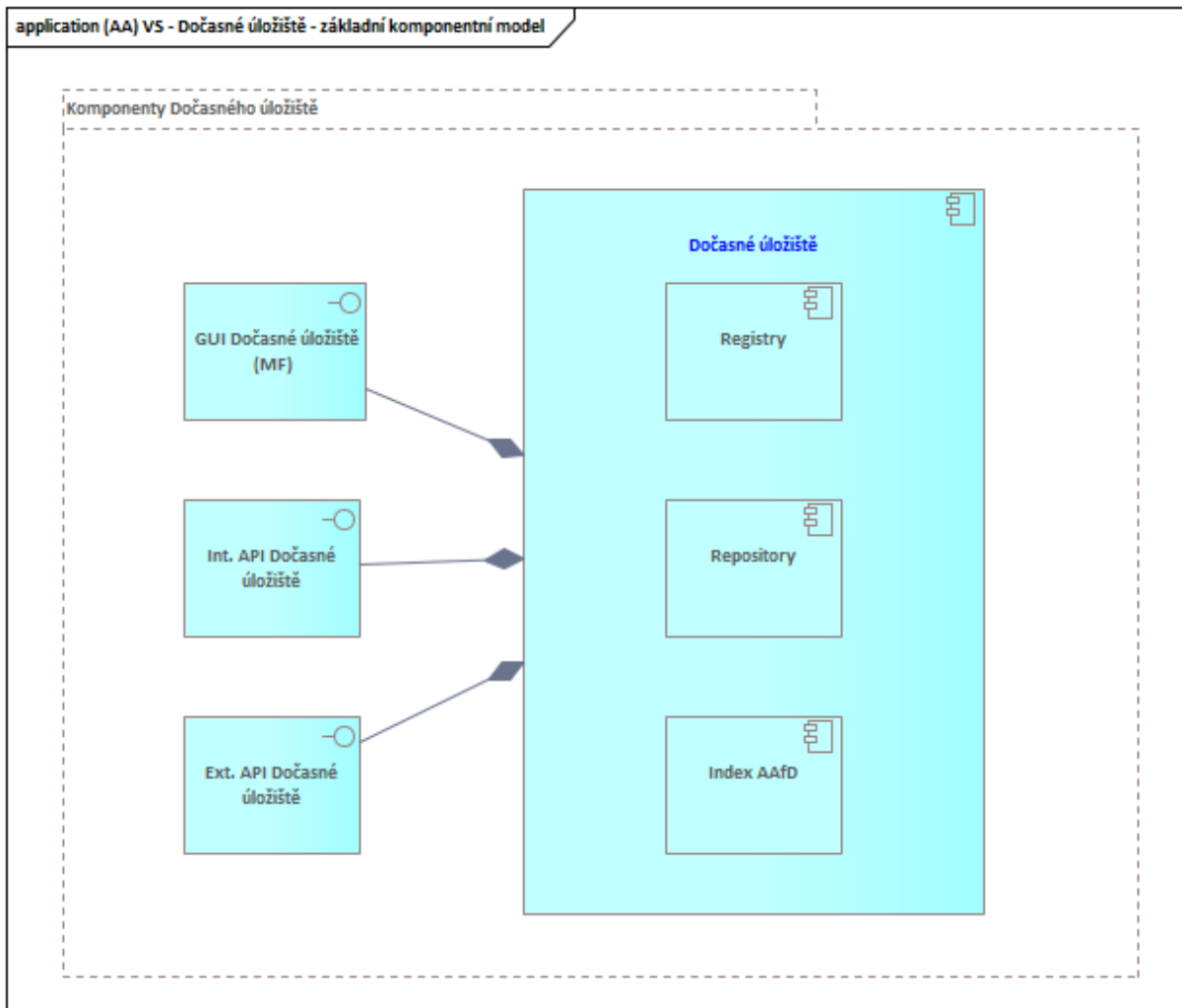
1.8.3.5 Architektura a principy

Systém Dočasného úložiště je navržen jako **modulární a škálovatelná architektura**, umožňující bezpečné a standardizované ukládání, výměnu a správu elektronických zdravotnických dokumentů.

Architektonické principy:

- **Modularita** – oddělené komponenty pro registry, repozitáře, autentizaci a audit
- **Interoperabilita** – podpora standardů IHE, HL7, FHIR, OpenAPI
- **Bezpečnost** – vícevrstvá ochrana, řízení přístupu, elektronická pečeť, auditní logy
- **Důvěryhodnost** – validace subjektů vůči Kmenovým registrům, kontrola integrity dat
- **Otevřenost** – rozhraní pro externí systémy (API) a uživatele (portál)
- **Evidenční transparentnost** – všechny operace jsou zaznamenávány a auditovány

Standard AAFD	Strana 38/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1



Komponenty systému:

- **Registry** – uchovávají metadata zásilek
- **Repository** – ukládá vlastní obsah dokumentů
- **API Gateway** – rozhraní pro přístup externích IS
- **Portál** – webové rozhraní pro ruční práci s dokumenty
- **Auditní vrstva** – logování a sledování všech akcí
- **Notifikační služba** – zajišťuje doručení oznámení adresátům

Architektura je navržena s ohledem na budoucí rozšiřování a napojení na evropské infrastruktury elektronického zdravotnictví.

1.8.3.5.1 Typy rozhraní

Komunikační architektura podporuje dva hlavní přístupy:

- **RESTful API:** Umožňuje asynchronní komunikaci mezi systémy pomocí standardních HTTP/HTTPS protokolů. API end-pointy jako `/api/v1/zasilka/UlozZasilku/` nebo `/api/v1/zasilka/DejZasilku/{id}` definují jasné operace pro ukládání, vyhledávání

Standard AAfD	Strana 39/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

a stažení zásilek. Tento přístup usnadňuje integraci mezi systémy a zaručuje pružnou výměnu dat.

- **Portálové rozhraní (Human Interface – HI):** Umožňuje přístup pomocí webového prohlížeče, což je výhodné zejména pro subjekty, které nemají implementovaná interní řešení pro API komunikaci. Portálové řešení přináší uživatelsky přívětivé prostředí, které se propojuje s backendovým systémem stejným způsobem jako API.

1.8.3.5.2 Zabezpečená komunikace

Architektura klade důraz na bezpečnost dat a komunikací:

- **Šifrování:** Veškeré přenosy probíhají pomocí HTTPS, což zajišťuje šifrovanou komunikaci a ochranu před odposlechem.
- **Autentizace a autorizace:** Každý přístup do systému podléhá přísnému ověření pomocí autentizačních tokenů a certifikátů. Validace probíhá nejen na úrovni uživatelského přihlášení, ale také v rámci každé operace volané přes API nebo portál.
- **Digitální podpisy a hash:** Každá zpráva je chráněna pomocí kontrolních součtů a digitálních podpisů, které slouží k ověření integrity a autenticity přenášených dat.

1.8.3.6 Popis datového modelu

default

POST /api/v1/Zasilka/UlozZasilku Your POST endpoint

POST /api/v1/Zasilka/VyhledejZasilku Your POST endpoint

GET /api/v1/Zasilka/DejZasilku/{id} Your GET endpoint

PUT /api/v1/Zasilka/ZneplatniZasilku Your PUT endpoint

PUT /api/v1/Zasilka/ZmenZasilku Your PUT endpoint

Schemas

Zasilka >

Dokument >

Soubor >

Slozka >

Ciselnik >

Strankovani >

Datový model definuje strukturu entity **Zásilka** a jejích vazeb na další datové struktury, především dokumenty, číselníky a přílohy. Model je navržen pro účely elektronické výměny zdravotnické dokumentace a je součástí aplikační vrstvy systému Dočasného úložiště.

Standard AAFD	Strana 40/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

Obsahuje hlavní entitu Zasilka a návazné entity: Dokument, Soubor, Slozka, Ciselnik, Strankovani.

1.8.3.6.1 Entita Zasilka

Typ: objekt

Popis: Reprezentuje datovou zasilku určenou pro přenos zdravotnických údajů.

Povinné atributy:

- id (uuid): ID zasilky (při aktualizaci).
- verze_radku (string, base64): Pro řízení verzí.
- nazev (string): Název zasilky (např. "Lékařská zprava").
- stav (Ciselnik): Stav zasilky (např. "Uložena").
- typ (Ciselnik): Typ zasilky.
- klasifikace (Ciselnik): Kategorizace dle standardu IHE.
- datumOd (datetime): Datum zpřístupnění zasilky.
- datumDo (datetime): Datum ukončení dostupnosti zasilky.
- autor (number): ID autora zasilky.
- zdravotnickýPracovník (number): ID zdravotnického pracovníka.
- poskytovatel (number): ID poskytovatele péče.
- pacient (number): RID pacienta.
- ispzs (string): Název informačního systému odesílatele.
- adresat (number): ID příjemce zasilky.
- adresatTyp (Ciselnik): Typ adresáta (např. "PZS").
- dostupnost (boolean): Označení, zda je zasilka přístupná.

Volitelné atributy:

- popis (string): Podrobnější popis zasilky.
- rodic (uuid): ID rodičovské zasilky.
- udalost (Ciselnik): Typ události vyvolávající zasilku.
- dokument (array of Dokument): Seznam dokumentů v zasilce.

1.8.3.6.2 Entita Dokument

Typ: objekt

Popis: Obsahuje metadata a obsah jednotlivého dokumentu v zasilce.

Povinné atributy:

- id (uuid), popis (string),
- verze_radku (string),
- nazev (string): Název dokumentu.
- jazyk (Ciselnik): Jazyk dokumentu (např. "cs").
- typ (Ciselnik): Typ dokumentu.
- klasifikace (Ciselnik): Klasifikace dokumentu.
- autor (number)
- pacient (number): RID pacienta.
- dostupnost (boolean): Přístupnost dokumentu.

Standard AAFD	Strana 41/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- duvernost (Ciselnik): Úroveň důvěrnosti.
- hash (string): Hash pro kontrolu integrity.
- velikost (number): Velikost dokumentu v bajtech.
- soubor (Soubor): Obsah dokumentu.

Volitelné atributy:

- poskytovatel (number),
- kod (string),
- mime (Ciselnik),
- vazanyDokument (uuid),
- slozka (Slozka)

1.8.3.6.3 Entita Soubor

Typ: objekt

Popis: Ukládá samotný binární obsah dokumentu.

Atributy:

- id (uuid): ID zásilky (volitelné).
- soubor (string, base64): Obsah dokumentu ve formátu base64.
- cesta (string): Cesta k souboru na externím úložišti (volitelné).

1.8.3.6.4 Entita Slozka

Typ: objekt

Popis: Logické seskupení dokumentů.

Povinné atributy:

- id (uuid): ID složky.
- verze_radku (string): Verze pro řízení konkurence.
- nazev (string): Název složky.
- autor (number): ID autora složky.

Volitelné atributy:

- popis (string): Popis obsahu složky.

1.8.3.6.5 Entita Ciselnik

Typ: objekt

Popis: Obecný typ pro reprezentaci výběrových hodnot (např. typy zásilek, stavy, jazyky).

Atributy:

- kod (string): Hodnota položky číselníku.
- verze (string): Verze číselníku.

1.8.3.6.6 Entita Strankovani

Typ: objekt

Popis: Používá se při stránkovaném dotazování (např. vyhledávání zásilek).

Atributy:

- page (number): Číslo aktuální stránky (minimum 1).
- size (number): Počet záznamů na stránku (minimum 1).

1.8.4 Obsahové a technické požadavky na zásilky

Zásilka představuje základní jednotku pro výměnu zdravotnické dokumentace v rámci systému elektronického zdravotnictví. Aby mohla být zásilka úspěšně přijata, zpracována a dále distribuována, musí splňovat přesně definované obsahové a technické náležitosti. Tyto požadavky vycházejí ze standardů elektronického zdravotnictví a jsou závazné pro všechny účastníky systému (PZS, zdravotní pojišťovny, ÚZIS, atd.).

1.8.4.1 Obsahové požadavky

Každá zásilka musí obsahovat:

- Jasně definovaný název a popis zásilky.
- Identifikaci pacienta prostřednictvím RID a validaci v Kmenovém registru pacientů.

Standard AAFD	Strana 43/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- Identifikaci autora zasilky a validaci v Kmenovém registru poskytovatelů nebo zdravotnických pracovníků.
- Identifikaci adresáta zasilky (pokud je určena konkrétní osobě/subjektu).
- Typ, formát a klasifikaci zasilky dle číselníků standardu EZ.
- Informaci o době platnosti (datumOd – datumDo).
- Hash dokumentu pro ověření integrity a elektronický podpis.
- Minimálně jeden zdravotnický dokument ve struktuře dle specifikace (včetně metadat a obsahu v Base64).

1.8.4.2 Technické požadavky

- Přenos zasilky probíhá prostřednictvím API rozhraní systému Dočasného úložiště nebo portálového přístupu.
- Každý dokument musí být ve validním formátu (např. PDF, CDA, DICOM, atd.) a doplněn příslušným MIME typem.
- Elektronická identifikace a autentizace účastníků pomocí JSU (Jednotné správy uživatelů).
- Elektronická pečeť a časové razítko na úrovni zasilky i při logování událostí.
- Povinná kontrola integrity dokumentu na vstupu i při přenosu.
- Podpora verzování dokumentů a řízení přístupu dle rolí a oprávnění.

1.8.4.3 Prioritní kategorie EHR (v roli zasilky)

Následující typy dokumentů jsou považovány za prioritní z hlediska interoperability a musí být vždy zasílány ve strukturované podobě s plným dodržением obsahových i technických požadavků:

- **Propouštěcí zpráva**
- **Zpráva z laboratorního vyšetření**
- **Zpráva z obrazového vyšetření**
- **Pacientský souhrn**
- **eŽádanka**

Tyto zasilky podléhají přísnějším požadavkům na čitelnost, strukturu a včasnost doručení, neboť slouží jako klíčové podklady pro rozhodování o zdravotní péči.

1.8.4.4 Další kategorie EHR (v roli zasilky)

Vedle prioritních typů dokumentů je možné do systému zasílat i další kategorie zdravotnické dokumentace, a to za předpokladu dodržení základních obsahových a technických pravidel. Tyto dokumenty mohou být ve volnější nebo nestrukturované podobě, ale i tak musí být správně označeny a zabezpečeny.

Patří sem např.:

- **Ambulantní zpráva**
- **Objednávka laboratorního vyšetření**
- **Objednávka obrazového vyšetření**
- **Záznam o výjezdu zdravotnické záchranné služby**
- **Hlášení výsledků laboratorních vyšetření do NZIS**

Standard AAFD	Strana 44/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

U těchto zásilek se doporučuje, aby jejich formát a klasifikace odpovídaly číselníkům systému, a aby jejich dostupnost byla nastavena dle míry důvěrnosti a potřeby cílového adresáta.

1.8.5 Souvislosti s dalšími službami EZ

1.8.5.1 Portál / EZ Karta

K zásilkám uloženým v rámci Dočasného úložiště je možné přistupovat prostřednictvím mobilní aplikace EZKarta nebo přes Portál elektronického zdravotnictví.

1.9 Kybernetická bezpečnost

Kybernetická bezpečnost definuje pravidla pro ochranu systémů, sítí, zařízení, dat a služeb před kybernetickými hrozbami.

Bezpečnost digitální infrastruktury systému DÚ je zajištěna v souladu s platnou legislativou a s ohledem na nejvyšší standardy ochrany dat uvedených v kontextu platné legislativy a standardu MZČR.

1.9.1 Obecné a legislativní požadavky

Na systém DÚ jsou kladené požadavky na uplatnění obecných principů kybernetické bezpečnosti:

- **Bezpečnostní politika:** definuje interní politiky a odpovědnosti za kybernetickou bezpečnost.
- **Přístupová práva:** přístupy jsou řízeny pomocí certifikátu, případně uživatelských jmen a hesel, kterou jsou vázaný na uživatelské role a práva.
- **Zálohování:** V rámci provozní dokumentace jsou definovány pravidla zálohování, jejich validita a možnosti obnovy, včetně vypracovaného DRP.
- **Monitoring a logování:** systém DÚ disponuje řadou healthchecku, které jsou pravidelně monitorovány a vyhodnocovány, kromě healthchecku jsou zaznamenávány také systémové logy a aplikační logy. Systém DÚ je napojeno na SIEM a Žurnál činnosti.
- **Aktualizace a patchování:** pro systém DÚ vypracovat podrobný plán údržby a aplikace bezpečnostních a aktualizací patchů pro systém i software.

Legislativní předpisy:

- Zákon č. 110/2019 Sb., **o zpracování osobních údajů:** Implementuje GDPR v České republice a stanovuje pravidla pro zpracování osobních údajů, včetně zdravotnických dat.
- Zákon č. 181/2014 Sb., **o kybernetické bezpečnosti** a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti): Definuje povinnosti pro subjekty zapojené do kritické informační infrastruktury, kam spadá i systém DÚ.
- Vyhláška č. 82/2018 Sb., **o kybernetické bezpečnosti:** Stanovuje konkrétní bezpečnostní opatření, která jsou povinná pro MZČR, jakožto významného informačního systému, pro prevenci kybernetických hrozeb.
- Vyhláška č. 317/2014 Sb., **o významných informačních systémech** a jejich určujících kritériích: Upravuje specifické požadavky zákona o kybernetické bezpečnosti na DÚ, které splňují kritéria pro významný informační systém.
- Zákon č. 365/2000 Sb., **o informačních systémech veřejné správy:** Vymezuje povinnosti správců informačních systémů veřejné správy, včetně systému DÚ a stanovuje opatření na ochranu proti kybernetickým hrozbám.

Standard AAFD	Strana 45/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- Zákon č. 480/2004 Sb., **o některých službách informační společnosti**: Upravuje pravidla pro elektronickou komunikaci a poskytování služeb informační společnosti, relevantní pro provoz systému DÚ.

Legislativa EU:

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (**GDPR**): Stanovuje základní pravidla pro ochranu osobních údajů v Evropské unii.
- Nařízení Evropského parlamentu a Rady (EU) 2022/1420 ze dne 14. září 2022, kterým se stanoví rámec pro evropský prostor pro zdravotní data a mění nařízení (EU) 2017/745 a směrnice 2004/23/ES (**EHDS**): Stanovuje pravidla pro interoperabilitu a sdílení zdravotnických dat v rámci Evropské unie.
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, o zrušení směrnice (EU) 2016/1148 a o změně nařízení (EU) 2018/1725 a směrnice (EU) 2013/40/EU (**NIS2**): Stanovuje pravidla pro kybernetickou bezpečnost v Evropské unii a upravuje pravidla pro zabezpečení systému DÚ jakožto poskytovatele základních služeb.

Standard AAFD	Strana 46/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

1.9.2 Úroveň bezpečnosti

S ohledem na citlivost zpracovávaných zdravotnických dat a roli systému DÚ v rámci infrastruktury elektronického zdravotnictví, je systém DÚ dle zákona o kybernetické bezpečnosti, klasifikován jako **Významný informační systém**. V kontextu nově připravovaného zákona a souvisejících prováděcích předpisů vycházejících z NIS2 se bude provoz služby systému DÚ řídit požadavky kladenými na **Poskytovatele regulované služby v režimu vyšších povinností**.

Tato klasifikace s sebou nese specifické povinnosti v oblasti kybernetické bezpečnosti, které je nutné v rámci návrhu a provozu systému DÚ zohlednit. Mezi tyto povinnosti patří organizační a technická opatření. Tyto povinnosti platí v plné podobě pro provozovatele systému DÚ (vyjma oblastí, které nejsou pro toto prostředí relevantní, jako např. § 28 - Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv).

1.9.3 Definice rolí

Hlavní role (funkce) z pohledu kybernetické bezpečnosti v rámci systému DÚ:

- **Provozovatel** systému je Ministerstvo zdravotnictví České republiky (dále jen „provozovatel“), které vykonává správu systému DÚ jako významného informačního systému veřejné správy a jako správce osobních údajů ve smyslu zákona o zpracování osobních údajů, a Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR).
- **Účastník** (uživatel) - každý subjekt nebo osoba, která na základě oprávnění přistupuje ke službám, datům v systému za účelem poskytování, sdílení nebo využívání zdravotnických informací, a to v souladu se zákonem o elektronizaci zdravotnictví.

1.9.4 Požadavky na bezpečnostní opatření

Aby bylo zabráněno možnému úniku dat nebo narušení poskytovaných služeb systému DÚ, musí účastníci (Poskytovatelé Zdravotních Služeb) využívat služby systému DÚ a přistupující k jeho systémům přijmout na své straně taková technická a organizační bezpečnostní opatření, aby byly naplněny minimální bezpečnostní požadavky, a to alespoň v následujícím rozsahu:

- Přístup k systému DÚ probíhá pouze z důvěryhodného a zabezpečeného informačního systému PZS (zajištěno např. používáním ochrany proti škodlivému kódu).
- Informační systém PZS, ze kterého je systém DÚ využíván, je pravidelně aktualizován a chráněn před známými zranitelnostmi.
- Do systému DÚ nejsou nahrávány žádné soubory, které obsahují škodlivý kód (např. malware, trojské koně apod.).
- Každý uživatel nebo systém přistupující k systému DÚ je jednoznačně identifikován a přístupové údaje nejsou sdíleny mezi více uživateli. Účastník musí pro komunikaci se systémem DÚ používat důvěryhodné certifikáty EZCA pro B2B i B2C komunikaci.
- Přístupové údaje (např. přístupové tokeny, certifikáty) jsou bezpečně uchovávány a chráněny proti zneužití.
- Každý přístup do dočasného úložiště je prováděn přes zabezpečené komunikační kanály a systém přistupující k systému DÚ musí podporovat moderní šifrovací protokoly (TLS 1.2+).
- Účastník provozovateli systému DÚ bezodkladně hlásí veškeré kybernetické bezpečnostní incidenty týkající se systémů přistupujících k systému DÚ, poskytuje součinnost při řešení kybernetických incidentů a předává provozovateli systému DÚ aktualizované kontaktní údaje osob zajišťujících tuto součinnost.
- PZS přijímá přiměřená opatření k ochraně svých systémů proti kybernetickým hrozbám (např. používání antivirového řešení, firewallu, omezení administrátorských oprávnění).

Standard AAFD	Strana 47/48
Ministerstvo zdravotnictví ČR	Číslo revize 0.1

- Zaměstnanci nebo zástupci PZS, kteří pracují s dočasným úložištěm, jsou obeznámeni se zásadami kybernetické hygieny (např. bezpečné zacházení s přístupovými údaji, rozpoznání phishingu).
- Účastník provádí bezpečnostní monitoring všech prvků infrastruktury, které přistupují k systému DÚ, identifikuje a řídí bezpečnostní události.
- PZS uchovává záznamy o přístupech k dočasnému úložišti, pokud to umožňuje jeho technické prostředí.
- Servery přistupující k B2B rozhraní systému DÚ jsou dostatečně odolné proti kybernetickým útokům (např. hardening OS, řízení zranitelností) a jsou pravidelně aktualizovány.
- Síťová a komunikační infrastruktura účastníka použitá k přístupu k systému DÚ je chráněna proti moderním kybernetickým hrozbám, použitím technologií jako jsou firewally.
- Účastník zajišťuje, že zdravotní pracovníci nevyužívají systému DÚ způsobem, který je v rozporu se zásadami bezpečného chování v digitálním prostředí (šíření malware, nezákonného obsahu atd.).
- **Systémy a aplikace přistupující k systému DÚ jsou vyvíjené bezpečným způsobem a podrobené dostatečným bezpečnostním testům.**
- Zdravotní pracovníci účastníka musí absolvovat pravidelné bezpečnostní školení (např. vzdělávací kurz NUKIB pro zdravotnictví).

Rozsah všech nasazených opatření by měl odpovídat povaze a velikosti poskytovatele zdravotnických služeb.