

# ELEKTRONIZACE ZDRAVOTNICTVÍ

## Dočasné úložiště

## Účel, funkce a vnější API rozhraní



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

---

**Verze: 00/00**

**Platnost nové verze od: 999**

# Obsah

1	Účel komponenty .....	4
1.1	Funkční přínos v rámci systému .....	4
1.2	Zákonné požadavky, které komponenta naplňuje .....	4
1.3	Cílové skupiny uživatelů .....	6
1.4	UseCase .....	7
2	Funkce komponenty DÚ .....	16
2.1	Přehled hlavních funkcí .....	16
2.2	Vnitřní logika .....	16
2.3	Vazby na jiné komponenty .....	20
3	Vnější rozhraní (API) .....	21
3.1	Popis poskytovaných služeb .....	21
4	Testovací scénáře .....	39
4.1	Přehled testovacích scénářů .....	39
5	Bezpečnostní opatření .....	40
5.1	Způsob zabezpečení komunikace .....	40
5.2	Autentizace .....	40
5.3	Šifrování, auditní logy, role .....	41

## Seznam zkratek a pojmů

Zkratka	Význam
API	Application Programming Interface (rozhraní pro programování aplikací)
B2B	Komunikace typu Business – Business (Systém – Systém) pomocí nevizuálních rozhraní
B2C	Komunikace typu Business – Client (Systém – Uživatel) pomocí vizuálních rozhraní
CDA	Clinical Document Architecture (standard pro strukturování klinických dokumentů)
ČR	Česká republika
DASTA	Český standard pro výměnu zdravotnických dat
DICOM	Digital Imaging and Communications in Medicine (standard pro ukládání a přenos obrazových dat)
DÚ	Dočasné úložiště
EHDS	European Health Data Space (Evropský prostor pro zdravotní údaje)
EU	Evropská unie

EZ	Elektronické zdravotnictví
EZCA	Certifikační autorita elektronického zdravotnictví
FHIR	Fast Healthcare Interoperability Resources (standard pro výměnu zdravotnických dat)
GDPR	General Data Protection Regulation (obecné nařízení o ochraně osobních údajů)
GET	HTTP metoda pro získání dat
HASH	Označení výstupní hodnoty hashovací funkce (pro ověření integrity dat)
HI	Human Interface
HTTP	Hypertextový přenosový protokol
HTTPS	Zabezpečený hypertextový přenosový protokol
ID	Identifikátor
IS	Informační systém
ITI	Integration Technical Infrastructure (technická infrastruktura IHE)
JSON	JavaScript Object Notation (formát pro výměnu dat)
JSU	Jednotná správa uživatelů
KRP	Kmenový registr pacientů
KRZP	Kmenový registr zdravotnických pracovníků
KRPZS	Kmenový registr poskytovatelů zdravotních služeb
KZR	Kmenové zdravotnické registry
MIME	Multipurpose Internet Mail Extensions – je internetový standard, který umožňuje přenášet texty v různých kódováních, binární data a vícedílné zprávy.
NIA	Národní Identitní Autorita
NIS	Nemocniční informační systém
NIS2	Směrnice o bezpečnosti sítí a informačních systémů
NPEZ	Národní plán elektronického zdravotnictví
PDF	Portable Document Format (formát pro sdílení dokumentů)
POST	HTTP metoda pro odeslání dat
PUT	HTTP metoda pro update dat
PZS	Poskytovatel zdravotních služeb
RESTful	RESTful API (API dle principů REST)
RID	Resortní identifikátor pacienta
SONIA	SOukromoprávní Národní Identitní Autorita
TLS	Transport Layer Security (protokol pro zabezpečení komunikace)
URL	Uniform Resource Locator (jednotná adresa zdroje)
ÚZIS ČR	Ústav zdravotnických informací a statistiky České republiky
XML	Extensible Markup Language (značkovací jazyk)
ZP	Zdravotní pojišťovna
ZD	Zdravotnická dokumentace

# 1 Účel komponenty

Cílem Dočasného úložiště (DÚ) 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 Funkční přínos v rámci systému

- DÚ je klíčovou součástí infrastruktury elektronického zdravotnictví v rámci výměnných sítí zdravotnických informací. Slouží k dočasnému ukládání a distribuci ZD mezi poskytovateli zdravotních služeb, zdravotními pojišťovnami a dalšími autorizovanými subjekty.
- DÚ je centrální úložiště zdravotnických dat, které podporuje následující klíčové funkcionality:
  - Ukládání ZD 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 KRZP, KRPZS a RPP.
  - 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.

## 1.2 Zákonné požadavky, které komponenta naplňuje

- 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 č. 325/2021 Zákon o elektronizaci zdravotnictví.
- DÚ je součástí NPEZ a jeho architektura je navržena s ohledem na bezpečnost, interoperabilitu a škálovatelnost v souladu s platnou legislativou ČR a EU (např. GDPR, NIS2, EHDS).
- DÚ 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 NPEZ, jehož cílem je zajistit bezpečnou, efektivní a interoperabilní výměnu zdravotnických dat mezi poskytovateli zdravotní péče, zdravotními pojišťovnami a státní správou. 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 ZD je 30 dní, s výjimkou eŽadank, jejichž platnost je nastavena na 3 roky dle novelizace Zákona č. 325/2021 Sb., o elektronizaci zdravotnictví.
- DÚ 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).

### 1.2.1 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.

### 1.2.2 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 ZD.
- **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 spadají i DÚ.
- **Vyhláška č. 444/2024 Sb., o zdravotnické dokumentaci:** Stanovuje pravidla pro vedení, uchovávání, předávání a likvidaci ZD. Určuje náležitosti ZD, její obsah, formu záznamů.
- **Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti:** Stanovuje konkrétní bezpečnostní opatření, která jsou povinná pro DÚ, jakožto významný informační systém, 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.
- **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 DÚ jakožto poskytovatele základních služeb.

## 1.3 Cílové skupiny uživatelů

Cílovými skupiny uživatelů jsou:

- **Pacient** je fyzická osoba, které jsou poskytovány zdravotní služby, a to na základě jejího souhlasu, nebo v případech stanovených zákonem i bez souhlasu. 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 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).
- **Zdravotnický pracovník** je osoba, která získala odbornou způsobilost k výkonu zdravotnického povolání podle zákona č. 96/2004 Sb., o podmínkách získávání a uznávání způsobilosti k výkonu nelékařských zdravotnických povolání. Tato osoba vykonává činnosti související s poskytováním zdravotní péče, a to v rozsahu stanoveném právními předpisy. Zdravotnický pracovník je oprávněn přistupovat k DÚ prostřednictvím autentizovaných informačních systémů svého poskytovatele zdravotních služeb. Může:
  - Ukládat zdravotnické záznamy do DÚ.
  - Stahovat a zobrazovat Zásilky pacienta, pokud má odpovídající oprávnění.
  - Spravovat obsah dokumentace v souladu s legislativními podmínkami.
- **Poskytovatel zdravotních služeb** je fyzická nebo právnická osoba, která má oprávnění k poskytování zdravotních služeb podle zákona č. 372/2011 Sb., o zdravotních službách. PZS je klíčovým aktérem využívajícím DÚ. Vystupuje jako:
  - Odesílatel zásilky – ukládá dokumentaci do DÚ.
  - Adresát zásilky – přebírá zdravotnické Zásilky jiných PZS.
  - Ověřovatel přístupových práv – využívá KRPZS k ověření oprávnění zdravotnických pracovníků.
- **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 DÚ primárně k:
  - Přístupu ke ZD pro účely revizních kontrol.
  - Ověření poskytovaných zdravotních služeb a jejich souvislostí s nároky pacienta.
  - Kontrole nákladů a efektivity poskytované péče.
- **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. ÚZIS ČR je oprávněn získávat anonymizovaná nebo agregovaná data z DÚ 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.

## 1.4 UseCase

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.

### Poskytovatel zdravotních služeb (PZS)

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

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

**V rámci těchto přístupů k systému DÚ 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

### Zdravotnický pracovník

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

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

**V rámci těchto přístupů k systému DÚ 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

### 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 DÚ může:**

- Stáhnout zázilku
- Vyhledat zázilku
- Zpochybnit zázilku

### Zdravotní pojišťovna

Zdravotní pojišťovny využívají DÚ zejména pomocí:

- **Ext. API DÚ** – pro automatizovanou výměnu dokumentace mezi informačními systémy PZS.
- **Portál DÚ** – pro ruční nahrávání a stahování zázilek zdravotnickými pracovníky.
- **Notifikační služby** – pro upozornění na přijetí nové zázilky.

**V rámci těchto přístupů k systému DÚ může** (vždy pouze v kontextu ke konkrétní zázilce k níž má oprávnění, nikoli ke všem zázilkám)

- Uložit zázilku
- Stáhnout zázilku
- Vyhledat zázilku
- Obdržet notifikace
- Zpochybnit zázilku

### ÚZIS ČR

ÚZIS ČR využívá DÚ 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 zázilek. Nezávislá však přístup k individuálním zdravotním záznamům pacientů.

## **1.4.1 Uložení zázilky do úložiště (přes API)**

### Klíčový popis služby:

- Datový zdroj zázilky je informační systém nebo aplikace které prostřednictvím API ukládá zázilku do DÚ.
- Umožňuje uložit zázilku do DÚ, a to prostřednictvím nevizuálního rozhraní (API) vystaveného DÚ

### Role:

- PZS nebo zdravotní pojišťovna (zdroj Zázilky):
  - Subjekt, jehož jménem zdravotnický pracovník zasílá Zázilku.
- DÚ:
  - Uchovává Zázilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatelé).
- PZS, zdravotní pojišťovna nebo ÚZIS ČR (adresát Zázilky):
  - Příjemce Zázilky, 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 (dle specifikace níže). Potvrdí zaslání Zásilky do DÚ přes jeho externí nevizuální rozhraní pomocí služby /api/v1/zasilka/UlozZasilku/.
- 2) DÚ vykoná:
  - a) Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
  - b) Ověření existence subjektů v KZR:
    - i) Existenci pacienta podle zasláního RID (referenční číslo).
    - ii) Existenci ZP a PZS (zdroje Zásilky).
    - iii) V případě vyplnění adresáta jeho existenci.
  - c) Validaci vstupu:
    - i) Vytvoří kontrolní součet zasilky (hash).
    - ii) Pomocí EZCA vytvoří razítko a pečeť na kontrolní součet.
    - iii) Ověří hash na vstupu (potvrdí konzistenci zasilky na vstupu).
  - d) Uložení Zásilky:
    - i) Uloží zasilku 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.

**1.4.2 Vyhledání zasilky (přes API)****Klíčový popis služby:**

- Umožňuje aktérům vyhledat relevantní zasilku dle vyhledávacích kritérií a s respektem k přístupovým právům a předložit seznam vyhledaných záznamů.
- Umožňuje vyhledat relevantní zasilku v DÚ, a to prostřednictvím nevizuálního rozhraní (API) vystaveného DÚ.

**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):
  - Subjekt, jehož jménem zdravotnický pracovník zasílá Zasilku.
- DÚ:
  - 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 (dle specifikace níže) do DÚ přes jeho externí nevizuální rozhraní pomocí služby /api/v1/zasilka/VyhledejZasilku/.
- 3) DÚ vykoná:
  - a) Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
  - b) Ověření existence a souladu právnických a fyzických osob v KZR:
    - i) Existenci pacienta podle zaslaného RID (referenční číslo).
    - ii) Existenci zdr. pracovníka (uživatele).
  - c) Získání rozsahu oprávnění uživatele na ZD pacienta z Registru práv a mandátů.
  - d) Vyhledání Zásilky v metadatech 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 (dle specifikace níže), které vyhovují výběrovým kritériím a rozsahu oprávnění uživatele.
- 4) IS uživatele zobrazí vrácený seznam dokumentů.

### **1.4.3 Stažení zásilky (přes API)**

#### **Klíčový popis služby:**

- Umožňuje stáhnout zásilku z DÚ 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):
  - Subjekt, jehož jménem zdravotnický pracovník zasílá Zásilku.
- DÚ:
  - Uchovává Zásilky a jejich metadata a zajišťuje jejich dostupnost pro oprávněné osoby (uživatele).

### **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 (dle specifikace níže) do DÚ přes jeho externí nevizuální rozhraní pomocí služby /api/v1/zasilka/DejZasilku/{id}.

- 2) DÚ vykoná:
  - a) Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
  - b) Ověření existence a souladu právnických a fyzických osob v KZR:
    - i) Existenci pacienta podle zaslaného RID (referenční číslo).
    - ii) Existenci zdr. pracovníka (uživatele).
  - c) Získání rozsahu oprávnění uživatele na ZD 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 DÚ, DÚ 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.

#### 1.4.4 Zneplatnění zásilky (přes portálový API)

##### Klíčový popis služby:



- Umožňuje označit příznakem relevantní zásilku jako neplatnou prostřednictvím nevizuálního rozhraní (API) vystaveného DÚ. 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):
  - Subjekt, jehož jménem zdravotnický pracovník zasílá Zásilku.
- DÚ:
  - 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) Uživatel (odesílatel Zásilky) pomocí svého IS zašle požadavek na získání aktuálního stavu záznamu Zásilky na DÚ přes jeho externí nevizuální rozhraní pomocí služby /api/v1/zasilka/VyhledejZasilku/, která je identifikována:
  - a) Identifikátorem Zásilky (získán při uložení Zásilky resp. z notifikace o uložení).
  - b) Odesílatelem (PZS, zdravotnický pracovník, zdravotní pojišťovna).
  - c) Identifikátorem pacienta (RID, který je získán z KZR).
- 2) Uživatel (odesílatel Zásilky) pomocí svého IS vytvoří požadavek na zneplatnění Zásilky, která je identifikována:
  - a) Identifikátorem Zásilky (získán při uložení Zásilky resp. z notifikace o uložení).
  - b) Odesílatelem (PZS, zdravotnický pracovník, zdravotní pojišťovna).
  - c) Identifikátorem pacienta (RID, který je získán z KZR).
  - d) Verzí řádku (získána pomocí služby VyhledejZasilku).
- 3) Po potvrzení uživatelem, IS zašle požadavek na zneplatnění Zásilky (dle specifikace níže) do DÚ přes jeho externí nevizuální rozhraní pomocí služby /api/v1/zasilka/ZneplatniZasilku/{id}.
- 4) DÚ vykoná:
  - a) Autentizaci a autorizaci PZS a zdravotnického pracovníka vůči JSU.
  - b) Ověření existence a souladu právnických a fyzických osob v KZR.
    - i) Existenci pacienta podle zaslaného RID (referenční číslo).
    - ii) Existenci zdr. pracovníka (uživatelé).
  - c) Získání rozsahu oprávnění uživatele na ZD pacienta z Registru práv a mandátů.
  - d) Vyhledání Zásilky v metadatach 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.

### 1.4.5 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 DÚ, a to prostřednictvím webového portálu vystaveného DÚ.
- Umožňuje uložit zásilku do DÚ, a to prostřednictvím vizuálního rozhraní (portál – webová služba) vystaveného DÚ.

#### Role:

- PZS nebo zdravotní pojišťovna (zdroj Zásilky):
  - Subjekt, jehož jménem zdravotnický pracovník zasílá Zásilku.
- DÚ:
  - 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, rozdíl v začátku procesu. Vnitřně na straně DÚ je komunikace komponentů shodná jako při uložení Zásilky přes API. Proto aktivity uvnitř DÚ 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 ČR, 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 DÚ.
- 3) Zdravotnický pracovník (zdroj Zásilky) potvrdí „Ulož Zásilku“.
- 4) Portál zašle Zásilku do DÚ.
- 5) DÚ vykoná zpracování Zásilky a vrátí informaci o výsledku zpracování.
- 6) Portál zobrazí výsledek zpracování uživateli.

### 1.4.6 Zneplatnění zásilky (přes portálový přístup)

#### Klíčový popis služby:

- Umožňuje označit příznakem relevantní zásilku jako neplatnou prostřednictvím vizuálního rozhraní (portál – webová služba) vystaveného DÚ. 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):
  - Subjekt, jehož jménem zdravotnický pracovník zasílá Zásilku.
- DÚ:
  - 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) vybere funkci „Zneplatnění Zásilky“ a potvrdí její vykonání.
- 2) Portál pošle požadavek na zneplatnění Zásilky do DÚ.
- 3) DÚ vykoná zpracování zneplatnění Zásilky a vrátí informaci o výsledku zpracování.
- 4) Portál zobrazí výsledek zpracování uživateli.

### 1.4.7 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 DÚ, a to prostřednictvím vizuálního rozhraní (portál – webová služba) vystaveného DÚ. Následně služba umožní stáhnutí z DÚ prostřednictvím vizuálního rozhraní (portál – webová služba) do koncového zařízení 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.
- DÚ:
  - 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 DÚ je komunikace komponentů shodná jako při vyhledání nebo stažení Zásilky přes API. Proto aktivity uvnitř DÚ nejsou v tomto scénáři popsány.

- 1) Uživatel (adresát Zásilky) vykoná:

- a) Přihlášení se na Portál v roli s oprávněním na stažení ZD (zdravotnický pracovník, pracovník ÚZIS ČR, pracovník pojišťovny).
  - b) Výběr funkce „Seznam Zásilek“.
  - c) Zadáání 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 DÚ.
  - 3) DÚ 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 DÚ.
  - 7) DÚ umožní stažení dokumentu.
  - 8) Portál vykoná stažení dokumentu, zobrazí obsah dokumentu uživateli a umožní jeho uložení do lokálního adresáře uživatele.



## 2 Funkce komponenty DÚ

### 2.1 Přehled hlavních funkcí

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

API podporuje tyto níže popsané služby DÚ:

Služba	Metoda	Popis služby
/api/v1/zasilka/UlozZasilku/	Post	Uložení Zásilky jako sady dokumentů (SubmissionSets).
/api/v1/zasilka/VyhledejZasilku/	Post	Vyhledávání metadat spojených s dokumenty, jako jsou odeslané sady dokumentů (SubmissionSets).
/api/v1/zasilka/DejZasilku/{id}	Get	Získání Zásilky, která splňuje zadané parametry.
/api/v1/zasilka/ZmenZasilku/{id}	Put	Změna Zásilky, která splňuje zadané parametry. Tato služba je aplikována do stažení zásilky. Po stažení zásilky změně zásilky už bude zamezeno.
/api/v1/zasilka/ZneplatniZasilku/	Put	Zneplatnění Zásilky, která splňuje zadané parametry.

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

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

### 2.2 Vnitřní logika

Zásilka představuje základní jednotku výměny součástí ZD vedené v elektronické podobě, její části nebo informace z ní určené k předání v rámci DÚ. 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.

#### **Klíčové vlastnosti entity Zásilka**

- **Unikátní identifikátor** – každá zásilka je označena jedinečným ID, které umožňuje její evidenci a zpětné dohledání.
- **Obsah zásilky** – hlavním prvkem zásilky je dokument obsahující zdravotnické údaje, které jsou v souladu s platnými standardy pro elektronickou dokumentaci.
- **Metadata zásilky** – obsahují informace o odesílateli, příjemci, pacientovi, typu a formátu zásilky, datu vytvoření a dalších charakteristikách důležitých pro zpracování a ověření platnosti zásilky.
- **Doba platnosti** – zásilka je v DÚ uchovávána po definované dobu, která odpovídá legislativním požadavkům a účelu zásilky. Po uplynutí této doby je automaticky odstraněna.



- **Bezpečnostní atributy** – každá zásilka obsahuje hash zasilky pro zajištění integrity a elektronické podpisy pro ověření autenticity dat.
- **Stav zasilky** – zásilka může mít různé stavy (např. přijatá, odeslaná, vyzvednutá, exspirovaná), které umožňují sledování jejího životního cyklu.

### Zásilky, které jsou předmětem sdílení v DÚ budou obsahovat:

- Dokument, který je předmětem výměny.
- Metadata zasilky s informacemi podle metodiky standardu EZ:
  - Identifikace pacienta – RID. Identifikace pacienta podle jména, příjmení, datumu narození, rodného čísla, čísla občanského průkazu a validace na KRP.
  - Identifikace autora – zdroje Zasilky (ZP, PZS). Validace na KRPZS a KRZP. Musí být uveden minimálně PZS.
  - Identifikace cíle Zasilky (ZP, PZS). Validace na KRPZS a KRZP. Bude uveden pro Zasilky určené pro konkrétního adresáta.
  - Identifikátor zasilky
    - Typ zasilky (klasifikace – výběr z číselníku definuje standard EZ).
    - Formát zasilky (výběr z číselníku definuje standard EZ).
    - Identifikátory ve zdrojovém systému (volitelná položka).
    - Identifikátory souvisejících zásilek.
    - Datum a čas vzniku zasilky (předvyplněný aktuální datum a čas).
    - Popis zasilky.
    - Velikost zasilky (vyplňuje zasílající systém – IS PZS, IS ZP, Portál, ...).
    - Hash Zasilky. (vypočítá a vyplní zasílající systém – IS PZS, IS ZP, Portál, ...).

## 2.2.1 Popis datového modelu

default ^

POST /Zasilka/UlozZasilku Your POST endpoint

POST /Zasilka/VyhledejZasilku Your POST endpoint

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

PUT /Zasilka/ZneplatniZasilku/ Your PUT endpoint

PUT /Zasilka/ZmenZasilku/{id} Your PUT endpoint

Schemas ^

Zasilka >

Dokument >

Soubor >

Slozka >

Ciselnik >

- 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 ZD a je součástí aplikační vrstvy systému DÚ.
- Obsahuje hlavní entitu Zasilka a návazné entity: Dokument, Soubor, Slozka, Ciselnik, Strankovani.
- Všechny entity zde uvedené typu **objekt**.

## 1. Entita Zasilka

Popis: Reprezentuje datovou zasilku určenou pro přenos zdravotnických údajů.

### Povinné atributy:

- **nazev** (string): Název zasilky (např. "Lékařská zpráva").
- **stav** (Ciselnik): Stav zasilky (např. "PRIJATA").
- **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:

- **id** (uuid): ID zasilky (při aktualizaci).
- **popis** (string): Podrobnější popis zasilky.
- **rodic** (uuid): ID rodičovské zasilky.
- **udalost** (Ciselnik): Typ události vyvolávající zasilku.
- **verzeRadku** (string, base64): Pro řízení verzí.
- **dokument** (array of Dokument): Seznam dokumentů v zasilce.

## 2. Entita Dokument

Popis: Obsahuje metadata a obsah jednotlivého dokumentu v zasilce.

### Povinné atributy:

- **nazev** (string): Název dokumentu.
- **jazyk** (Ciselnik): Jazyk dokumentu (např. "cs").
- **typ** (Ciselnik): Typ dokumentu.
- **klasifikace** (Ciselnik): Klasifikace dokumentu.
- **pacient** (number): RID pacienta.
- **dostupnost** (boolean): Přístupnost dokumentu.
- **duvernost** (Ciselnik): Úroveň důvěrnosti.
- **hash** (string): Hash pro kontrolu integrity.
- **velikost** (number): Velikost dokumentu v bajtech.

- soubor (Soubor): Obsah dokumentu.

**Volitelné atributy:**

- id (uuid),
- popis (string),
- autor (number),
- poskytovatel (number),
- kod (string),
- mime (Ciselnik),
- vazanyDokument (uuid),
- verzeRadku (string), slozka (Slozka).

**3. Entita Soubor**

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).

**4. Entita Slozka**

Popis: Logické seskupení dokumentů.

**Povinné atributy:**

- nazev (string): Název složky.
- autor (number): ID autora složky.

**Volitelné atributy:**

- id (uuid): ID složky.
- popis (string): Popis obsahu složky.
- verzeRadku (string): Verze pro řízení konkurence.

**5. Entita Ciselnik**

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

**Atributy:**

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

**6. Entita Strankovani**

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

**Atributy:**

- index (number): Číslo aktuální stránky (minimum 1).

- pocet (number): Počet záznamů na stránku (minimum 1).

### 2.2.2 Stavy zásilky

Stavový kód	Povolený aktér pro změnu stavového kódu	Manipulace s daty zásilky na základě stavového kódu
Uložená	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna	uložení do DÚ
Stažená	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna	stažení z DÚ do lokálního úložiště daného aktéra, vymazání zásilky dle systémových pravidel
Zneplatněná	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna, a to výhradně v roli aktéra, který zásilku uložil	označení zásilky atributem neplatná, zobrazení atributu ostatním aktérům
Smazaná	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna, systém	trvalé a nevratné smazání zásilky z DÚ
Zpochybněná	poskytovatel zdravotních služeb, zdravotnický pracovník, zdravotní pojišťovna, systém	dočasně zpochybněná zásilka

## 2.3 Vazby na jiné komponenty

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

## 3 Vnější rozhraní (API)

### 3.1 Popis poskytovaných služeb

Pro zajištění bezpečné, jednoznačné a interoperabilní výměny elektronických zdravotnických dokumentů mezi subjekty systému elektronického zdravotnictví (např. PZS, zdravotní pojišťovny, zdravotní pracovníci) je definováno standardizované technické rozhraní a odpovídající specifikace pro datovou komunikaci.

- Systém DÚ 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.
- Pro komunikaci mezi systémy slouží následující API služby:
  - **/api/v1/zasilka/UlozZasilku/**
    - Metoda: POST
    - Účel: Uložení zásilky do DÚ 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 zásilky na základě jejích identifikátorů.
  - **/api/v1/zasilka/ZmenZasilku/{id}**
    - Metoda: PUT
    - Účel: Úprava zásilky, zejména k evidenci stažení nebo aktualizaci stavu.
  - **/api/v1/zasilka/ZneplatniZasilku/**
    - Metoda: PUT
    - Účel: Označení zásilky jako neplatné s následnou notifikací adresátů.
- Každý end-point podléhá přísné autentizaci a autorizaci pomocí JSU a ověřování subjektů v kmenových registrech, například KRZP a KRPZS.
- Implementační specifikace definuje technické a provozní požadavky na systémy, které se integrují s DÚ elektronického zdravotnictví.

#### Klíčové požadavky:

- **Podpora API** dle specifikace OpenAPI 3.1.0
- **Komunikace přes HTTPS** s TLS 1.2 nebo vyšší
- **Zpracování výjimek** dle standardizovaných HTTP stavových kódů (např. 400, 401, 403, 5XX)

#### Formát výměny dat:

Formát pro výměnu dat je definován JSON.

### Klíčové požadavky výměny dat:

- **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)

### Povinné technologie výměny dat:

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

### Autentizace/autorizace:

Režim Autentizace a autorizace je v rámci DÚ dvojí:

- B2B
- B2C

**Režim B2B** je určen pro oprávněné uživatele zdravotních nebo sociálních služeb, kteří disponují resortním **certifikátem zdravotnického zařízení**. Jedná se o certifikát vydávaný resortní certifikační autoritou každému poskytovateli zdravotních nebo sociálních služeb. Tento certifikát jednoznačně identifikuje přístupující subjekt.

**Režim B2C** je určen pro všechny ostatní typy přístupů – tedy pro případy, kdy účastník nedisponuje resortním certifikátem zdravotnického zařízení, případně jeho NIS či AIS nepodporuje B2B komunikaci s DÚ.

DÚ poskytuje grafické rozhraní implementované v prostředí Portálu občana, kde je uživatel ověřován prostřednictvím NIA, SONIA nebo jiných metod podporovaných portálem. Výsledkem je jednoznačná identifikace uživatele, který je následně propojen se systémem JSU.

V obou popsaných režimech dochází k propojení na systém JSU, v rámci kterého je definována jednoznačná identita uživatele, a tím i jeho role a oprávnění v systému DÚ.

## 3.1.1 Služba UlozZasilku

### Klíčový popis služby:

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

### Role:

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

### Kanonická URL adresa:

URL: [base]/api/v1/zasilka/UlozZasilku/

**Příklad: POST `api.ext.zas.csez.cz/api/v1/zasilka/UlozZasilku/`**

**Request:**

```
{
  "id": 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"
},
"verzeRadku": null,
"dokument": [
  {
    "id": 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":
    "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac84
    9b",
    "velikost": 0,
    "vazanyDokument": null,
    "verzeRadku": "",
    "soubor": {
        "soubor":
        "R0lGODlhAQABAIAAAP//wAAACH5BAEAAAAALAAAAABAAEAAAICRAEAOw==",
        "cesta": null
    },
    "slozka": {
        "id": null,
        "nazev": "Přílohy",
        "popis": "string",
        "autor": 0
    }
}
]
}

```

**Response:**

Kód	201	400	401	403	5xx
Response	Zásilka je uložena	Aplikační chyba	Chyba autorizace vůči DÚ	Přístupující subjekt nemá právo	Nefunkční stav služby

				na volanou službu DÚ	
Body	id (String)				
	verzeRadku (String)				

### 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).

#### Role:

- Odesílatel
  - Subjekt, který dohledává jím zaslané zasilky
- Adresát
  - Subjekt vyhledávající zasilku

#### 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)
- Strankovani:
  - index: první záznam
  - pocet: počet záznamu pro vyhledání

#### Kanonická URL adresa:

URL: [base]/api/v1/zasilka/VyhledejZasilku/

**Příklad: POST `api.ext.zas.csez.cz/api/v1/zasilka/VyhledejZasilku/`**

#### Request:

```
{
  "pacient": 0,
  "autor": 0,
  "prijemce": 0,
  "poskytovatel": 0,
```

```

"datumOd": "2025-04-04T08:43:30.306Z",
"datumDo": "2025-04-27T08:43:30.306Z",
"strankovani": {
  "index": 1,
  "pocet": 10
}
}

```

### Response:

Kód	200	400	401	403	5xx
Response	Zásilka je nalezena ano/ne	Aplikační chyba	Chyba autorizace vůči DÚ	Přístupující subjekt nemá právo na volanou službu DÚ	Nefunkční stav služby
Body	Vid'. Výsledek vyhledání				

### Výsledek vyhledání:

```

{
  "pocet": 10,
  "zasilka": [
    {
      "id": "blea47de-a177-4ade-924e-50c241365be4",
      "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"
  },
  "verzeRadku": "AAAAAAAADPg=",
  "dokument": [
    {
      "id": "b37ae731-3d26-49a6-91f9-acb56538d3ff",
      "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":
    "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac84
    9b",
    "velikost": 0,
    "vazanyDokument": null,
    "verzeRadku": "AAAAAAAADPY=",
```

```

"soubor": {
  "id": "abac085d-6300-4117-ae6a-7ff34a246491",
  "soubor": null,
  "cesta": null
},
"slozka": {
  "id": "76d5cc8e-e1c2-41bd-9331-0cf3bd91ad50",
  "nazev": "Přílohy",
  "autor": 0,
  "datumVytvoreni": "2025-04-10T12:18:18.73",
  "verzeRadku": "AAAAAAAADPc="
}
}
]
}
}

```

### 3.1.3 Služba DejZasilku

#### Klíčový popis služby:

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

#### Role:

- Adresát
  - Subjekt stahující zasilku

#### Parametry vyhledávání:

- id:
  - identifikátor Zásilky.

#### Kanonická URL adresa:

URL: [base]/api/v1/zasilka/DejZasilku/

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

#### Request:

```

{
}

```

#### Response:

Kód	200	400	401	403	5xx
-----	-----	-----	-----	-----	-----

<b>Response</b>	<b>Zásilka je nalezena ano/ne</b>	<b>Aplikační chyba</b>	<b>Chyba autorizace vůči DÚ</b>	<b>Přistupující subjekt nemá právo na volanou službu DÚ</b>	<b>Nefunkční stav služby</b>
<b>Body</b>	<b>Viz Výsledek volání</b>				

**Výsledek volání:**

```
{
  "id": "blea47de-a177-4ade-924e-50c241365be4",
  "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"
},
"verzeRadku": "AAAAAAAADPg=",
"dokument": [
  {
    "id": "b37ae731-3d26-49a6-91f9-acb56538d3ff",
    "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":
"b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac84
9b",
"velikost": 0,
"vazanyDokument": null,
"verzeRadku": "AAAAAAAADPY=",
"soubor": {
  "id": "abac085d-6300-4117-ae6a-7ff34a246491",
  "soubor": null,
  "cesta": null
},
"slozka": {
  "id": "76d5cc8e-e1c2-41bd-9331-0cf3bd91ad50",
  "nazev": "Přílohy",
  "autor": 0,
  "datumVytvoreni": "2025-04-10T12:18:18.73",
  "verzeRadku": "AAAAAAAADPc="
}
}
```

```
    ]
  }
}
```

### 3.1.4 Služba ZmenZasilku

#### Klíčový popis služby:

Služba slouží ke změně Zásilky, která splňuje zadané parametry. Tato služba je aplikována do stažení zásilky. Po stažení zásilky už bude změně zásilky zamezeno. Výsledkem dotazu je ID upravené zásilky obsahující nová změněná data DocumentReference.

#### Role:

- Odesílatel
  - Subjekt s potřebou upravit/opravit zásilku před jejím stáhnutím.

#### Parametry vyhledávání:

- id:
  - identifikátor Zásilky.

#### Kanonická URL adresa:

URL: [base]/api/v1/zasilka/ZmenZasilku/

**Příklad:** PUT /api/v1/zasilka/ZmenZasilku/5c3c2480-7bc5-4272-a9a7-61dbb1a9150f

#### Request:

```
{
  "id": "blea47de-a177-4ade-924e-50c241365be4",
  "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"
},
"verzeRadku": "AAAAAAAADPg=",
"dokument": [
  {
    "id": "b37ae731-3d26-49a6-91f9-acb56538d3ff",
    "nazev": "Lékařská zpráva pacienta",
    "popis": "Lékařská zpráva z ambulantního 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":
  "b1442e85b03bdcaf66dc58c7abb98745dd2687d86350be9a298a1d9382ac84
  9b",
  "velikost": 0,
  "vazanyDokument": null,
  "verzeRadku": "AAAAAAADPY=",
  "soubor": {
    "id": "abac085d-6300-4117-ae6a-7ff34a246491",
    "soubor": null,
```

```

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

```

**Response:**

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

**3.1.5 Služba ZneplatniZasilku****Klíčový popis služby:**

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.

**Role:**

- Adresát
  - Subjekt zneplodňující zásilku

**Parametry vyhledávání:**

- id:
  - identifikátor Zásilky.
- VerzeRadku
  - identifikátor záznamu

**Kanonická URL adresa:**

URL: [base]/api/v1/zasilka/ZneplatniZasilku/

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

**Request:**

```
{
  "id": "blea47de-a177-4ade-924e-50c241365be4",
  "verzeRadku": "AAAAAAAADPg="
}
```

**Response:**

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

## 4 Testovací scénáře

### 4.1 Přehled testovacích scénářů

Kapitola obsahuje přehled navrhovaných testovacích scénářů podle služeb:

#### **UlozZasilku**

- Uložení zásilky s více dokumenty
- Uložení zásilky bez dokumentu
- Uložení zásilky s dokumentem a bez složky
- Uložení zásilky s dokumentem a se složkou

#### **VyhledejZasilku**

- Vyhledání zásilky podle autora
- Vyhledání zásilky podle pacienta
- Vyhledání zásilky podle příjemce
- Vyhledání zásilky podle datumu (od – do)

#### **DejZasilku**

- Získání zásilky podle id zásilky

#### **ZmenZasilku**

- Změna zásilky podle id zásilky

#### **ZneplatniZasilku**

- Zneplatnění zásilky podle id zásilky

## 5 Bezpečnostní opatření

Digitální úložiště (DÚ) uplatňuje několik prvků pro zajištění ochrany a integrity dat. DÚ je postaveno na následujících základních principech:

- **Komunikace probíhá výhradně přes protokol HTTPS** s TLS 1.3 (TLS 1.2 je podporováno jen v režimu fallback)
- **Autentizace a autorizace** prostřednictvím Jednotné správy uživatelů (JSU)
- **Validace dat** vůči Kmenovým registrům (KRP, KRPZS, KRZP)
- **Zabezpečení integrity** pomocí hash hodnoty a elektronického podpisu (EZCA)

DÚ nenese odpovědnost za obsahovou správnost Zásilky – tedy samotného souboru. Tato odpovědnost leží plně na straně odesílatele. DÚ však zajišťuje, že jsou implementována dostatečná bezpečnostní opatření, která chrání integritu dat jak při příjmu, tak při odeslání zásilky.

V rámci ochrany dat je rovněž implementován Registr práv a mandátů, jehož nastavení může ovlivnit uložení nebo stažení zásilky. Pokud si pacient nepřeje sdílet určité typy svých zdravotních informací a tyto údaje jsou součástí zásilky, DÚ takovou zásilku nepřijme nebo odmítne její vydání.

Zásilka, kromě samotného obsahu, disponuje metadaty, která (mimo jiné) identifikují pacienta pomocí jeho RID, identifikují odesílající a přijímající subjekt, či jiná data, která jsou uložena v rámci registru centrálních služeb elektronického zdravotnictví. DÚ provádí kontrolu těchto dat a tím zaručuje, že příchozí data jsou v čase úkonu platná a validní.

V případě samotného obsahu dat dochází k využití principů kontrolních hashu, které jsou opatřeny časovými razítky. Tento princip zaručuje poskytnutí garance integrity dat a to:

- V rámci nahrávání do DÚ, tedy přenosu prostřednictvím B2B brány, případně přes grafické rozhraní.
- V rámci samotného DÚ, tedy garanci, že s obsahem zásilky nebylo manipulování v rámci interního úložiště DÚ.
- V rámci stažení zásilky z DÚ, tedy přenosu mezi DÚ a oprávněným příjemcem zásilky, které může být realizováno prostřednictvím B2B, či grafického rozhraní.

### 5.1 Způsob zabezpečení 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 zásilka je chráněna pomocí kontrolních součtů a digitálních podpisů, které slouží k ověření integrity a autenticity přenášených dat.

### 5.2 Autentizace

Režim Autentizace a autorizace je v rámci DÚ dvojitý



- B2B
- B2C

**Režim B2B** je určen pro oprávněné uživatele zdravotních nebo sociálních služeb, kteří disponují resortním certifikátem zdravotnického zařízení. Jedná se o certifikát vydávaný resortní certifikační autoritou každému poskytovateli zdravotních nebo sociálních služeb. Tento certifikát jednoznačně identifikuje přístupující subjekt.

Poskytovatel může tuto formu přístupu využít v případě, kdy chce s DÚ komunikovat přímo, prostřednictvím B2B rozhraní ze svého NIS či AIS.

Spojení s B2B rozhraním je navazováno prostřednictvím protokolu HTTPS, jehož ověření probíhá na základě uvedeného certifikátu. Pokud je certifikát platný, DÚ naváže spojení se systémem JSU, ve kterém je pro každý subjekt uložen technický uživatel přiřazený ke konkrétnímu certifikátu.

**Režim B2C** je určen pro všechny ostatní typy přístupů – tedy pro případy, kdy účastník nedisponuje resortním certifikátem zdravotnického zařízení, případně jeho NIS či AIS nepodporuje B2B komunikaci s DÚ.

DÚ poskytuje grafické rozhraní implementované v prostředí Portálu občana, kde je uživatel ověřován prostřednictvím NIA, SONIA nebo jiných metod podporovaných portálem. Výsledkem je jednoznačná identifikace uživatele, který je následně propojen se systémem JSU.

V obou popsanych režimech dochází k propojení na systém JSU, v rámci kterého je definována jednoznačná identita uživatele, a tím i jeho role a oprávnění v systému DÚ.

V rámci B2C režimu je navíc uplatňováno ověření vůči Registru práv a povinností (RPP), který umožňuje v systému DÚ nahlížet na data nebo zpracovávat data i jménem jiných fyzických či právnických osob.

## 5.3 Šifrování, auditní logy, role

**Komunikace probíhá výhradně přes protokol HTTPS s TLS 1.3. Zabezpečení integrity je řešeno pomocí hash hodnoty a elektronického podpisu (EZCA)**

Veškeré autentizační a autorizační úkony jsou auditovány a zaznamenávány do Žurnálu činností.

Podporové role jsou:

- PZS
- Zdravotnický pracovník
- Pacient
- Zdravotní pojišťovna
- ÚZIS ČR