

# ELEKTRONIZACE ZDRAVOTNICTVÍ

## Žurnál činností

### 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                               | 5  |
| 1.2 | Zákonné požadavky, které komponenta naplňuje                 | 5  |
| 1.3 | Cílové skupiny uživatelů (např. lékaři, pacienti, instituce) | 5  |
| 1.4 | UseCase  | 6  |
| 2   | Funkce komponenty:   | 6  |
| 2.1 | Přehled hlavních funkcí                                      | 7  |
| 2.2 | Vnitřní logika (např. zpracování dat, ukládání, validace)    | 7  |
| 2.3 | Vazby na jiné komponenty                                     | 8  |
| 3   | Vnější rozhraní (API)  | 8  |
| 3.1 | Popis poskytovaných služeb (např. REST API, SOAP, jiná)      | 9  |
| 3.2 | Formát výměny dat (např. JSON, XML)                          | 9  |
| 3.3 | Autentizace/autorizace (např. eIDAS, OAuth2, JWT, NIA...)    | 9  |
| 3.4 | Popis koncových bodů (endpointů) včetně:                     | 9  |
| 3.5 | URL  | 9  |
| 3.6 | Metoda (GET, POST, PUT, DELETE...)                           | 10 |
| 3.7 | Parametry  | 10 |
| 3.8 | Struktura odpovědi   | 13 |
| 3.9 | HTTP kódy a chybové stavy                                    | 13 |
| 4   | Testovací scénáře (volitelné)                                | 14 |
| 4.1 | Přehled testovacích scénářů                                  | 15 |
| 4.2 | Apod.  | 15 |
| 5   | Bezpečnostní opatření  | 15 |
| 5.1 | Způsob zabezpečení komunikace                                | 16 |
| 5.2 | Autentizace  | 16 |
| 5.3 | Šifrování, auditní logy, role                                | 16 |
| 6   | Provozní požadavky (volitelné)                               | 16 |
| 6.1 | Nároky na infrastrukturu                                     | 17 |
| 6.2 | Možnosti škálování   | 17 |

# Seznam zkratek a pojmů

| Zkratka        | Význam  |
|----------------|---|
| <b>AdES</b>    | Pokročilý elektronický podpis – standard pro bezpečné elektronické podpisy.                       |
| <b>API</b>     | Aplikační programové rozhraní – sada funkcí pro komunikaci mezi systémy.                          |
| <b>CPU</b>     | Centrální procesorová jednotka – hlavní výpočetní jednotka počítače.                              |
| <b>ECS</b>     | Elastic Common Schema – jednotné datové schéma pro logy v systému Elastic.                        |
| <b>eIDAS</b>   | Nařízení o elektronické identifikaci a důvěryhodných službách – evropské nařízení pro e-identitu. |
| <b>EZKarta</b> | Elektronická zdravotní karta – mobilní aplikace pro občany k přístupu k údajům v eZdravotnictví.  |
| <b>GUI</b>     | Grafické uživatelské rozhraní – vizuální rozhraní aplikace.                                       |
| <b>HTTP</b>    | Hypertextový přenosový protokol – základní protokol komunikace na webu.                           |
| <b>I/O</b>     | Vstup/Výstup – operace spojené s příjmem a výdejem dat nebo signálů.                              |
| <b>ID</b>      | Identifikátor – jednoznačný údaj pro označení objektu nebo osoby.                                 |
| <b>JSON</b>    | JavaScript Object Notation – textový formát pro výměnu dat ve formě objektů.                      |
| <b>JSU</b>     | Jednotná správa uživatelů – centrální systém pro správu autentizace a autorizace uživatelů.       |
| <b>JWT</b>     | JSON Web Token – otevřený standard pro bezpečný přenos informací v JSON objektu.                  |
| <b>MSSQL</b>   | Microsoft SQL Server – relační databázový systém od společnosti Microsoft.                        |

|                |  |
|----------------|--|
| <b>NIA</b>     | Národní identitní autorita – centrální orgán pro ověřování identity v eGovernmentu.    |
| <b>NPEZ</b>    | Národní portál elektronického zdravotnictví – hlavní portál pro služby eZdravotnictví. |
| <b>OAuth2</b>  | Otevřený autorizační protokol verze 2.0 – standard pro delegované ověření identity.    |
| <b>PDF</b>     | Přenositelný formát dokumentů – běžný formát pro výstupní reporty systému.             |
| <b>RAM</b>     | Operační paměť s náhodným přístupem – primární paměť počítače.                         |
| <b>REST</b>    | Architektonický styl pro webové služby využívající HTTP protokol (RESTful rozhraní).   |
| <b>Sb.</b>     | Sbírka zákonů – oficiální publikace právních předpisů ČR.                              |
| <b>SOAP</b>    | Protokol pro výměnu zpráv v distribuovaných systémech (webové služby).                 |
| <b>SSD</b>     | úložné zařízení na bázi flash paměti.  |
| <b>SSL</b>     | Zastaralý šifrovací protokol pro zabezpečenou komunikaci (předchůdce TLS).             |
| <b>TLS</b>     | Šifrovací protokol pro bezpečný přenos dat (nástupce SSL).                             |
| <b>URL</b>     | Jednotný lokátor zdrojů – adresa pro přístup k internetovému zdroji.                   |
| <b>XAdES-T</b> | Rozšířený formát elektronického podpisu s časovým razítkem v XML.                      |
| <b>ZČ</b>      | Žurnál činností – centrální evidence realizovaných činností v datovém rozhraní.        |

**Účel:**

*Detailní technicko-funkční dokumentace sloužící architektům systému, programátorům a integračním partnerům.*

**Rozsah:**

*5–20 normostran podle rozsahu funkcí komponenty*

# 1 Účel komponenty:

## 1.1 Funkční přínos v rámci systému

### *Žurnál činností*

*Žurnál činností představuje systém, který slouží k centralizovanému zaznamenávání a uchovávání informací o provedených činnostech v Integrovaném datovém rozhraní oprávněnými osobami. Stejně tak systém Žurnálu činností plní funkci umožňující nahlížet na takto uložené činnosti formou přehledů/evidence činností vztahujících se k dané osobě (pacient / zdravotnický pracovník)*

### *Audit a logovací subsystém*

*Auditní a logovací systém představuje centrální prvek zajišťující zaznamenávání a uchovávání informací o provozních a bezpečnostních událostech. Tento systém umožňuje průkazné uchovávání záznamů o aktivitách uživatelů, systémových procesech a přístupech k datům, a to včetně metadata, jako jsou časové značky, identifikátory uživatelů a typy operací.*

*Stejně tak systém plní funkci umožňující dohled a vyhodnocování těchto záznamů formou přehledů a reportů, které jsou k dispozici oprávněným osobám pro účely bezpečnostního dohledu, forenzní analýzy a případného auditu. Umožňuje tak sledování činností související se systémovým prvkem (např. konkrétní službou nebo databázovým objektem) a zajišťuje nezbytnou míru provozní a bezpečnostní transparentnosti systému.*

## 1.2 Zákonné požadavky, které komponenta naplňuje

### *Žurnál činností*

*Zákonné ukotvení Žurnálu činností je v § 37 dle zákona 325/2021 Sb.*

### *Audit a logovací subsystém*

|                         |   |   |
|-------------------------|---|---|
| Kybernetická bezpečnost | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti   | § 4 (bezpečnostní opatření), § 8 (povinnosti provozovatele), § 25 (evidence činností) |
|                         | Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti | § 18 a § 20 (evidence činností, záznamy a logy)                                       |

## 1.3 Cílové skupiny uživatelů (např. lékaři, pacienti, instituce)

### 1.3.1 Občan – funkce, usecase, jak se ke službě dostane (NPEZ/EZ KARTA..) přínosy

Občan (pacient) bude mít k dispozici centralizované místo, odkud si bude moci pomocí portálu NPEZ nebo mobilní aplikace EZkarta vyžádat evidenci (přehled) činností provedených v Integrovaném datovém rozhraní a vztahujících se k jeho osobě coby pacientovi a to zejména co se týče údaje o času a typu provedené činnosti, stejně tak i jejím účelu a identifikaci původce dané činnosti.

### 1.3.2 Zdravotní pracovník – funkce, usecase, jak se ke službě dostane (popis NPEZ, API..) přínosy

Zdravotní pracovník bude mít k dispozici centralizované místo, odkud si bude moci pomocí portálu NPEZ nebo mobilní aplikace EZkarta vyžádat evidenci (přehled) činností provedených v Integrovaném datovém rozhraní a vztahujících se k jeho osobě coby zdravotnímu pracovníkovi a to zejména co se týče údaje o času a typu provedené činnosti, stejně tak i jejím účelu a identifikaci původce dané činnosti.

## 1.4 UseCase

### 1.4.1 Záznam realizovaných činností

- **Zdrojový systém** vytvoří datovou zprávu při provedení činnosti.
- Pokud činnost podléhá evidenci dle zákona 325/2021 Sb. (§ 37), je zpráva rozšířena o další atributy.
- **Zpráva je odeslána** přes API auditního systému.
- Pokud obsahuje sekci pro Žurnál činností, je tato část **automaticky oddělena** a předána do Žurnálu činností

## 2 Funkce komponenty:

### 2.1 Přehled hlavních funkcí

Komponenta Žurnál činností plní funkci důvěryhodného registru o provedených činnostech v integrovaném datovém rozhraní.

Systém umožňuje:

- Zaznamenání činností oznámených oprávněnými systémy.
- Dlouhodobé uchování záznamů s garancí integrity a neměnnosti.
- Generování přehledových reportů o činnostech vztahujících se ke konkrétním osobám (pacient, zdravotník).
- Upozorňování uživatelů o dostupnosti reportů prostřednictvím systému notifikací.
- Zajištění souladu se zákonem č. 325/2021 Sb. a bezpečnostními standardy (AdES, XAdES-T, elektronická pečeť a časové razítko).

Auditní a logovací subsystém centralizuje sběr, správu, uchovávání a analýzu logů z aplikačních systémů, databází a síťových prvků.

Systém umožňuje:

- Jednotný přístup k auditním a aplikačním logům.
- Korelaci událostí z různých zdrojů.
- Detekci bezpečnostních incidentů a anomálií.
- Generování přizpůsobených reportů podle cílové skupiny (admini, bezpečnostní tým, management).
- Notifikace v reálném čase na základě definovaných pravidel (např. opakované neúspěšné přihlášení).

### 2.2 Vnitřní logika (např. zpracování dat, ukládání, validace)

Komponenta Žurnál činností

- **Příjem dat:** prostřednictvím Kafka topicu nebo REST API, obě varianty používají jednotný JSON formát.
- **Validate:** systém kontroluje strukturu a mandatory atributy, včetně kontroly HASH hodnoty záznamu.
- **Ukládání:** validované záznamy jsou uloženy do MSSQL databáze.
- **Agregace:** HASH hodnoty záznamů jsou periodicky seskupovány do XML obálek (XAdES-T) a opatřeny elektronickou pečeti a razítkem.
- **Exspirace:** záznamy jsou uchovávány 2 roky, po uplynutí lhůty jsou automaticky skartovány.
- **Publikace:** systém umožňuje asynchronní požadavky na publikaci reportu o realizovaných činnostech ve formátu PDF.
- **Upozornění:** uživatel je informován o vygenerovaném reportu přes systém notifikací.
- **Retence:** PDF report je uložen pouze v Dočasném úložišti po dobu 30 dní, následně je odstraněn.

## Auditní a logovací subsystém

- **Ingest dat:** logy jsou odesílány do Apache Kafka pomocí Kafka klienta, Filebeat nebo REST API.
- **Transformace:** pomocí Logstash jsou logy parsovány, obohaceny a filtrované.
- **Ukládání:** zpracované logy jsou ukládány do OpenSearch, indexované podle typu a časového období.
- **Vizualizace:** pomocí OpenSearch Dashboard lze tvořit grafy a přehledy o chybách, latenci, aktivitě.
- **Standardizace:** všechny zprávy využívají Elastic Common Schema (ECS) pro jednotnou strukturu.
- **Fallback mechanismus:** při nedostupnosti Kafky jsou logy dočasně ukládány lokálně a později replikovány.
- **Bezpečnost:** přenos dat je šifrován (TLS), přístup řízen pomocí rolí.

## 2.3 Vazby na jiné komponenty

Komponenty jsou prepojeny s viacerými systémovými prvkami:

- **Dočasné úložiště** – určené na uloženie výstupných reportov.
- **Systém notifikací** – informuje používateľa o pripravených dokumentoch.
- **Jednotná správa užívateľů (JSU)** – zabezpečuje autentizáciu a autorizáciu osôb.
- **Národní portál elektronického zdravotnictví (NPEZ)** a aplikácia **EZKarta** – koncoví konzumenti publikovaných údajov.



## 3 Vnější rozhraní (API)

### 3.1 Popis poskytovaných služeb (např. REST API, SOAP, jiná)

REST API služby Žurnálu činnost pro přijetí požadavku na generování přehledu realizovaných činností z aplikace EZKarta a z NPEZ (Národní portál elektronického zdravotnictví)

Pro další centrální systémy jsou k dispozici topic v KAFKA, které je součástí auditního a logovacího subsystému:

- Zdrojové systémy zapisují do vstupních topiků.

### 3.2 Formát výměny dat (např. JSON, XML)

Formát všech zpráv v API i v systému je JSON.

### 3.3 Autentizace/autorizace (např. eIDAS, OAuth2, JWT, NIA...)

### 3.4 Popis koncových bodů (endpointů) včetně:

| Název služby              | Metoda                      | Funkce  |
|---------------------------|-----------------------------|---|
| REST API Žurnálu činností | PublikujRealizovaneCinnosti | Generování a publikace PDF reportu realizovaných činností |
| Kafka rozhraní            | —                           | Middleware pro přenos zpráv a událostí mezi systémy       |

#### Služba: REST API – PublikujRealizovaneCinnosti

**Účel:** Přijímá požadavky na generování přehledového PDF reportu o realizovaných činnostech.

#### Služba: Kafka

**Účel:** Zápis auditního záznamu do centrálního logování a žurnálu činnosti

## 3.5 URL

Base URL služeb podle katalogu ...TODO

## 3.6 Metoda (GET, POST, PUT, DELETE...)

POST

## 3.7 Parametry

Daná datová zpráva PublikujRealizovaneCinnosti.log metody „PublikujCinnostiZurnalu“ slouží pro zaslání požadavku na vygenerování přehledu realizovaných činností do PDF reportu:

### PublikujRealizovaneCinnosti.log zpráva - návrh struktury

```
{
  "requestID": "98eed688-cfd7-4a18-9ec2-b667ae7d8289",
  "activeParticipant": {
    "userID": "JSU_48eed688-cfd7-4a18-9ec2-b667ae7d8289",
    "userName": "Jana Nováková",
    "userIsRequestor": true,
    "networkAccessPointID": "10.1.86.12",
    "networkAccessPointTypeCode": 2,
    "roleIDCode": {
      "csd-code": 113871,
      "codeSystemName": "DCM",
      "originalText": "Person ID"
    }
  },
  "requestorObjectIdentification": {
    "requestorObjectID": "RID^^^OID",
    "requestorObjectTypeCode": 1,
    "requestorObjectTypeCodeRole": 1,
    "requestorObjectIDTypeCode": {
      "csd-code": 2,
      "codeSystemName": "DCM",
      "originalText": "Patient Number"
    }
  },
  "reportTimeFrame": {
```

```
"dateFrom": "2024-01-01T00:00:00.000+01:00",  
"dateTo": "2025-01-01T00:00:00.000+01:00"  
},  
"requestorSourceIdentification": "NPEZ"  
}
```

## Příklad volání REST API pro zápis do auditního logu

curl -X POST

```
"http://<KAFKA_REST_PROXY_HOST>:<PORT>/topics/vzorovy_topic_audit_log" \  
-H "Content-Type: application/vnd.kafka.json.v2+json" \  
-d '{  
  "records": [  
    {  
      "value": {  
        "@timestamp": "2025-01-28T10:15:30.123+01:00",  
        "event": {  
          "kind": "event",  
          "category": "healthcare",  
          "type": "creation",  
          "action": "C",  
          "outcome": "0",  
          "id": "ab20b1cf-0fa0-4e0b-aa73-2a7b8404b17b",  
          "reason": "Pro uživatele XYZ byl vytvořen zdravotní záznam ABC."  
        },  
        "correlation": {  
          "id": "ab20b1cf-0fa0-4e0b-aa73-2a7b8404b17b"  
        },  
        "service": {  
          "name": "NIS.FNBrno"  
        },  
        "host": {  
          "hostname": "10.1.86.12"  
        },  
        "source": {  
          "ip": "10.1.86.12"  
        },  
        "user": {  
          "id": "JSU_48eed688-cfd7-4a18-9ec2-b667ae7d8289",  
          "name": "Jana Nováková"  
        },  
      },  
    ],  
  }  
}
```

```
"patient": {
  "id": "RID^^^OID"
},
"diagnosis": {
  "code": "100001"
},
"zurnal_cinnost": {
  "event": {
    "idCorrelation": "ab20b1cf-0fa0-4e0b-aa73-2a7b8404b17b",
    "message": "Pro uživatele XYZ byl vytvořen zdravotní záznam ABC.",
    "eventIdentification": {
      "eventActionCode": "C",
      "eventDateTime": "2025-01-28T10:15:30.123+01:00",
      "eventOutcomeIndicator": 0,
      "eventTypeCode": {
        "csd-code": 100001,
        "codeSystemName": "MZCR.Audit",
        "originalText": "Vytvoření dokumentu EZD"
      }
    },
  },
  "activeParticipant": {
    "userID": "JSU_48eed688-cfd7-4a18-9ec2-b667ae7d8289",
    "userName": "Jana Nováková",
    "userIsRequestor": true,
    "networkAccessPointID": "10.1.86.12",
    "networkAccessPointTypeCode": 2,
    "roleIDCode": {
      "csd-code": 113871,
      "codeSystemName": "DCM",
      "originalText": "Person ID"
    }
  },
  "auditSourceIdentification": "NIS.FNBrno",
  "participantObjectIdentification": [
    {
      "participantObjectID": "RID^^^OID",
      "participantObjectTypeCode": 1,
      "participantObjectTypeCodeRole": 1,
      "participantObjectIDTypeCode": {
        "csd-code": 2,
        "codeSystemName": "DCM",
        "originalText": "Patient Number"
      }
    }
  ]
}
```

```

    }
  ]
},
"eventHash": {
  "hashAlgorithmOid": "2.16.840.1.101.3.4.2.3",
  "hash":
    "4d3a69d78d1a732da167e75f1bf8fed5c6d0467e24b9b986bd1ef4e3600e7c69bb024bd
    94b6d2a1b95c036f9ed56a06f053bede742ac4e58b55392e1c89ecb2a"
  }
},
"message": "Pro uživatele XYZ byl vytvořen zdravotní záznam ABC."
}
}
]
}'

```

## 3.8 Struktura odpovědi

KAFKA API = odpověď

```
[ {
  "partition": 0,
  "offset": 42 } ]
```

| Pole      | Význam   |
|-----------|--|
| partition | Číslo partície Kafka topicu, kam byla zpráva zapsaná               |
| offset    | Poradové číslo správy v rámci daný partície (offset = unikátní ID) |

## 3.9 HTTP kódy a chybové stavy

http 201 – úspěšné odeslání požadavku

http 401 – chyba autentizace

http 404 – chybná URL, nenalezeno

http 500 – neočekávaná chyba

## **4 Testovací scénáře (volitelné)**

### **4.1 Přehled testovacích scénářů**

### **4.2 Apod.**

## 5 Bezpečnostní opatření

### 5.1 Způsob zabezpečení komunikace

- **Šifrování přenosu:** Veškerá komunikace mezi systémy (REST API, Kafka) je šifrována pomocí TLS (SSL/TLS šifrování).
- **Integrita dat:** Pro zajištění integrity se používá HASH kontrola každého záznamu. Systém ověřuje vypočtený HASH oproti zaslané hodnotě.
- **Podepisování bloků:** Skupiny záznamů jsou opatřeny resortní elektronickou pečeti a časovým razítkem (XAdES-T).

### 5.2 Autentizace

#### 5.2.1 Autentizace systémů zapisujících auditní logy a záznamy do Žurnálu činnosti

- Přístup přes TLS s klientským certifikátem
- Každý systém má přiřazený konkrétní topic pro zápis (auditní logy, záznamy do ZČ)

#### 5.2.2 Autentizace uživatele při požadavku na generování reportu činností

- Autentizace probíhá prostřednictvím JSU (Jednotná správa uživatelů) – zajišťuje validaci identity
- Při zpracování požadavku systém ověřuje, že přístupový účet odpovídá evidované osobě

### 5.3 Šifrování, auditní logy, role

Auditní logy jsou:

- Centralizovaně ukládány (Kafka → Vector → OpenSearch)
  - V souladu s Elastic Common Schema (ECS)
- Dostupnost: systém musí být dostupný 99,99 % pro zápis a 99,9 % pro čtení.
- Záznamy jsou uchovávány po dobu 2 let dle legislativy, poté automaticky skartovány.
- PDF reporty nejsou trvale uchovávány v systému – po doručení do Dočasného úložiště jsou po 30 dnech mazány.



## 6 Provozní požadavky (volitelné)

### 6.1 Nároky na infrastrukturu

- **Apache Kafka**
  - Slouží jako middleware pro ingest logů z aplikací a systémů.
  - Nutnost vysoké propustnosti (~500 zpráv/s) a replikace pro odolnost.
  - Fyzické i virtuální servery s optimalizací na diskové I/O a síť.
- **Vector**
  - Předzpracování zpráv: parsování, enrichování, routování.
  - Nutná kapacita pro běh více pipeline paralelně při vyšší zátěži.
- **OpenSearch**
  - Vyhledávání a analýza logů.
  - Škálovatelné nasazení: více uzlů pro vyrovnaní zátěže a redundanci.
  - Vyžaduje SSD disky, rychlé I/O, vysokou RAM a CPU.
- **Žurnál činnosti**
  - Ukládání do MSSQL databáze.
  - Periodické podepisování agregovaných bloků – nutnost výpočetního výkonu a zabezpečeného úložiště.
- **REST API + GUI**
  - Externí přístup pro požadavky a správu.
  - Očekává se vysoká dostupnost (99.9 % pro čtení, 99.99 % pro zápis).
  - Podpora horizontálního škálování prostřednictvím load balanceru.

### 6.2 Možnosti škálování

#### 6.2.1 Kafka

- **Horizontální škálování** přidáním brokerů a partition.
- Oddělené topicity podle typu zpráv (audit, aplikační, žurnál).
- Možnost replikace pro zvýšení odolnosti.

#### 6.2.2 OpenSearch

- **Škálování pomocí uzlů (nodes)** – datové, master a ingest uzly.
- Automatické vyvažování indexů.
- Retenční politika dat

#### 6.2.3 MSSQL (Žurnál)

- Vertikální škálování (výkon CPU, paměť, storage).

- Nasazení v clustrovém řešení

Všechny komponenty jsou navrženy tak, aby podporovaly asynchronní zpracování a vysokou propustnost bez ztráty dat.