Ministerstvo
vnitra

MVCRX09AEQMK
prvotní identifikátor

odbor archivní správy a spisové služby

Č. j. MV- 24487-7/AS-2025

Metodický návod pro akreditaci digitálního archivu

Verze 3.0 ke dni 9. 7. 2026

Zpracovali: Vojáček, Dvořák, Prokopová

1) Cíl metodiky a pro koho je určena

Akreditací digitálního archivu se rozumí udělení oprávnění k ukládání archiválií v digitální podobě podle § 60a zákona č. 499/2004 Sb. (dále také jako AZ).
Cílem předkládané metodiky je poskytnout návod pro žadatele, jak připravit konkrétní podklady pro akreditaci digitálního archivu (dále jen „DA“) a jak při podání žádosti postupovat. Metodika se skládá z popisu problematiky akreditačního řízení, přináší odkazy na platnou právní úpravu a normy a doporučení v oblasti digitální archivace. Podrobněji vymezuje náležitosti žádosti tím, že definuje strukturu a rozsah dokládaných skutečností nutných pro akreditaci DA.

Co je předmětem posouzení při akreditačním procesu?

Předmětem posouzení je digitální archiv jako organizace sestávající z osob a technických systémů, která převezme odpovědnost za dlouhodobé uchovávání a dlouhodobou dostupnost informací v digitální formě, jako i za jejich poskytnutí určité cílové skupině. Z tohoto důvodu posouzení zohledňuje organizační, finanční a technické aspekty digitálního archivu.
Součástí posouzení jsou stavebně-technické a bezpečnostních požadavky na objekty (AZ, §61 odst. 2 a 4) v nichž je DA provozován. **Viz Příloha č. 1.**
Součástí této metodiky je seznam dokumentů, jenž žadatel předkládá jako součást žádosti o akreditaci. U každého dokumentu je definováno, jaké minimální informace by měl obsahovat. Tyto informace zahrnují stávající právní požadavky podle zákona č. 499/2004 Sb. Zároveň vycházejí z mezinárodních požadavků pro audit a certifikaci digitálních repozitářů a jejich naplnění posiluje důvěryhodnost digitálního archivu. Posouzení žádosti bude primárně probíhat na základě analýzy těchto dokumentů.
V případě potřeby bude součástí posuzování i předvedení provozu digitálního archivu.
Část podkladů pro akreditaci DA lze nahradit předložením výsledků formální certifikace digitálního repozitáře dle ISO 16363 nebo DIN 31644.

Posouzení DA při akreditačním procesu nenahrazuje audit potažmo certifikaci DA.

Definice okruhu žadatelů

O akreditaci digitálního archivu mohou žádat jen zřizovatelé akreditovaného archivu. Akreditaci nepodléhají digitální archiv Národního archivu a digitální archivy bezpečnostních archivů. O akreditaci mohou žádat osoby, které se chtějí stát zřizovateli archivu. V takovém případě je žádost o akreditaci DA součástí žádosti o akreditaci archivu podle § 58 zákona č. 499/2004 Sb.

Náležitosti žádosti

Žádost o akreditaci DA musí kromě obecných náležitostí podání podle správního řádu obsahovat:

- název a adresu sídla archivu a adresy míst staveb, ve kterých budou umístěna úložiště archiválií v digitální podobě
- podklady pro rozhodnutí, zda archiv splňuje podmínky stanovené v § 61 odst. 2 a 4 zákona č. 499/2004 Sb. (tj. stavebně-technické a bezpečnostní podmínky)
- popis způsobu uložení archiválií v digitální podobě
- koncepci dlouhodobého uchovávání a ochrany dokumentů určených pro předávání do digitálního archivu
- identifikaci ukládaných archiválií v digitální podobě
- seznam metadat týkajících se popisu archiválií v digitální podobě, popisu a evidence archivních souborů a popisu původců v rozsahu údajů stanovených v § 12b a 12c vyhlášky č. 645/2004 Sb.
- návrh provozního řádu digitálního archivu
- potvrzení Národního archivu o úspěšném provedení zkušebního přesunu archiválií v digitální podobě do Národního archivu

Kdo a jak posuzuje?

Žadatel podává žádost Ministerstvu vnitra. Ministerstvo samostatně posuzuje jen tyto náležitosti žádosti:

- název a adresa sídla archivu a adresy míst staveb, ve kterých budou umístěna úložiště archiválií v digitální podobě
- podklady pro rozhodnutí, zda archiv splňuje podmínky stanovené v § 61 odst. 2 a 4

Ministerstvo si vyžádá závazné stanovisko Národního archivu k těmto náležitostem žádosti:

- popis způsobu uložení archiválií v digitální podobě
- koncepce dlouhodobého uchovávání a ochrany dokumentů určených pro předávání do digitálního archivu

- identifikace ukládaných archiválií v digitální podobě
- seznam metadat týkajících se popisu archiválií v digitální podobě, popisu a evidence archivních souborů a popisu původců
- návrh provozního řádu digitálního archivu
- potvrzení Národního archivu o úspěšném provedení zkušebního přesunu archiválií v digitální podobě do Národního archivu (Specifikace AIP pro přenos do NDA viz Příloha č. 2)

Národní archiv vydává závazné stanovisko k žádosti o akreditaci DA. Ministerstvo vydá rozhodnutí o akreditaci DA do 1 roku ode dne podání žádosti. Akreditaci DA nelze udělit, jestliže závazné stanovisko Národního archivu ke kterékoliv z náležitostí žádosti je negativní.

2) Odkaz na právní předpisy, normy a doporučení

Právní předpisy:

- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů
- Národní standard pro elektronické systémy spisové služby [Věstník Ministerstva vnitra čá. 85/2024 (část II)]
- vzorový provozní řád archivu oprávněného k ukládání archiválií v digitální podobě [Věstník Ministerstva vnitra čá. 65/2012 (část II)]
- zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů
- zákon č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti
- vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy
- směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2)
- zákon č. 264/2025 Sb., o kybernetické bezpečnosti
- vyhláška č. 334/2025 Sb., o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony
- vyhláška č. 408/2025 Sb., o regulovaných službách

- vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
- vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
- vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu
- vyhláška č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy
- vyhláška č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu
- vyhláška č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
- nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS), ve znění nařízení (EU) 2024/1183, kterým se zřizuje evropský rámec digitální identity (eIDAS 2.0)
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
- zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů
- nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci, AI Act)

Normy a doporučení:

- ISO 14721:2025 Space data and information transfer systems - Open archival information system (OAIS) - Reference model
- ISO 16363:2025 Space data and information transfer systems - Audit and certification of trustworthy digital repositories
- ISO 16919:2025 Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories
- CEN/TS 18170:2025 Functional requirements for the electronic archiving services
- Standardizace komunikace mezi digitálními archivy při předávání archiválií [VMV čá. 89/2024] - Standard výměnného formátu digitálních archiválií verze 1.0 mezi digitálními archivy v České republice, https://mv.gov.cz/soubor/nmet-1-standard-vymenneho-formatu-digitalnich-archivali-v-1-0-mezi-digitalnimi-archivy-v-cr-20241210-pdf.aspx
- Standardizace přenosu informací mezi software, které slouží k popisu archiválií, a digitálním archivem [VMV čá. 90/2024] - Komunikační rozhraní mezi software pro popis archiválií a digitálními archivy, https://mv.gov.cz/soubor/nmet-2-komunikacni-rozhrani-mezi-sw-pro-popis-archivalii-a-digitalnimi-archivy-20241210-pdf.aspx
- Transformace digitálních prostorových dat pro účely trvalého uložení v digitálním archivu - verze 1.0; metodika pro výběr, předání, uložení a trvalé uchování prostorových dat a GIS,

včetně datového balíčku GeoSIP, https://www.nacr.cz/wp-content/uploads/2024/02/Geodata_DEF.pdf

- Národní standard formátů pro archivaci, https://archi.gov.cz/znalostni_baze:archivni_formaty
- NÚKIB, Minimální požadavky na kryptografické algoritmy. Doporučení v oblasti kryptografické bezpečnosti (průběžně aktualizováno)
- E-ARK specifikace a definice datových balíčků, https://dilcis.eu
- ČSN ISO 15489-1:2016 Informace a dokumentace - Správa dokumentů - Část 1: Pojmy a principy
- ISO 23081-1:2017 Information and documentation - Records management processes - Metadata for records - Part 1: Principles
- ISO 23081-2:2021 Information and documentation - Managing metadata for records - Part 2: Conceptual and implementation issues
- ISO 16175-1:2020 Information and documentation - Processes and functional requirements for software for managing records - Part 1: Functional requirements and associated guidance for any applications that manage digital records
- ISO/TR 21946:2018 Information and documentation - Appraisal for managing records
- ISO 13008:2022 Information and documentation - Digital records conversion and migration process
- ISO 30300:2020 Information and documentation - Records management - Core concepts and vocabulary
- ISO 30301:2019 Information and documentation - Management systems for records - Requirements, včetně Amendment 1:2024
- ISO 30302:2022 Information and documentation - Management systems for records - Guidelines for implementation
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls
- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks
- ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
- ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system

- ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management
- ISO/IEC 42005:2025 Information technology - Artificial intelligence - AI system impact assessment
- ISO/IEC 42006:2025 Information technology - Artificial intelligence - Requirements for bodies providing audit and certification of artificial intelligence management systems
- DIN 31644 Information and documentation - Criteria for trustworthy digital archives
- CoreTrustSeal Trustworthy Data Repositories Requirements
- NDSA Levels of Digital Preservation
- Digital Preservation Storage Criteria
- Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)
- MARKS, Steve: Becoming a Trusted Digital Repository. 2015
- Vysvětlující informace k Pečeti nestoru pro důvěryhodné digitální archivy, 2018, https://nbn-resolving.de/urn:nbn:de:0008-2018071005
- VERMAATEN, Sally - LAVOIE, Brian - CAPLAN, Priscilla: Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment. 2012
- HUTAŘ, Jan et al., Metodika logické ochrany digitálních dat, 2018
- RŮŽIČKA, Michal – MIRANDA, Andrea – HEJTMÁNEK, Lukáš: Metodika bitové ochrany digitálních dat, 2019
- CAPLAN, Priscilla: PREMIS - Jak mu porozumět, 2018, http://www.loc.gov/standards/premis/UnderstandingPREMIS_czech.pdf

BÁRTA, Stanislav (red.) et al., Digitální archivnictví, 2019, https://munispace.muni.cz/library/catalog/book/1407

KOČIŠOVÁ, Pavlína et al., Zachováno navěky? Teorie a praxe dlouhodobého uchování digitálních dokumentů, 2023, https://www.nkp.cz/file/65604f296f06a13ae3a0a67843ff2e70/6470/publikace_zachovano_naveky_text.pdf

3) Doporučená struktura a obsah předkládané dokumentace nutné k posouzení žádosti o akreditaci DA.

Níže uváděná struktura a obsah předkládané dokumentace vychází z komplexních požadavků na DA, jak je definuje certifikační proces dle Pečeti nestoru.[1]

V zásadě lze rozlišit tři základní okruhy problémů a z toho vyplývající požadavky na dokumentaci:

[1] Vysvětlující informace k Pečeti nestoru pro důvěryhodné digitální archivy, 2018, http://nbn-resolving.de/urn:nbn:de:0008-2018071005

3.1 Koncepce dlouhodobého uchovávání a ochrany dokumentů určených pro předávání do digitálního archivu

Zde žadatel dokládá tato kritéria Pečeti nestoru:
K1 Výběr informačních objektů a jejich reprezentací
K2 Odpovědnost za uchování
K3 Cílové skupiny
K4 Přístup
K5 Interpretovatelnost
K6 Právní a smluvní základ
K7 Právní shoda
K8 Financování
K9 Lidské zdroje
K10 Organizace a procesy
K11 Uchovávací strategie
K12 Krizové řízení a exit plán
K13 Významné vlastnosti
K34 Bezpečnost
Z pohledu digitální archivace zcela zásadní. Tato kritéria musí být v digitálním archivu plně implementována, tj. koncepce je detailně zpracována, organizačně a technicky provedena. Postupy jsou součástí běžícího provozu.

3.2 Popis způsobu uložení archiválií v digitální podobě

Zde žadatel dokládá tato kritéria Pečeti nestoru:
K14 Integrita: Rozhraní pro příjem
K15 Integrita: Funkcionality archivního úložiště
K16 Integrita: Uživatelské rozhraní
K17 Autenticita: Příjem
K18 Autenticita: Uchovávací strategie
K19 Autenticita: Přístup
K20 Technická oprávnění
K33 IT–infrastruktura
K33 musí být plně implementováno. Některá z těchto kritérií mohou být ve stadiu schváleného detailně zpracovaného konceptu a konkrétní postupy jsou zaváděny do běžného procesu. Ostatní musí být plně implementována.

3.3 Seznam metadat týkajících se popisu archiválií v digitální podobě, popisu a evidence archivních souborů a popisu původců

Zde žadatel dokládá tato kritéria Pečeti nestoru:
K21 Vstupní informační balíčky
K22 Převod vstupních informačních balíčků do archivních informačních balíčků
K23 Archivní informační balíčky

K24 Interpretovatelnost archivních informačních balíčků
K25 Převod archivních informačních balíčků do výstupních informačních balíčků
K26 Výstupní informační balíčky
K27 Identifikace
K28 Popisná metadata
K29 Strukturální metadata
K30 Technická metadata
K31 Zaznamenání dlouhodobých uchovávacích strategií
K32 Administrativní metadata
Některá z těchto kritérií mohou být ve stadiu schváleného detailně zpracovaného konceptu a konkrétní postupy jsou zaváděny do běžného procesu. Ostatní musí být plně implementována.

3.4 Požadavky Zákona na portál DA a na správu metadat archiválií

Žadatel dokládá splnění požadavků zákona §18b a §18c.

Žadatel o akreditaci DA doloží:

ad 3.1.

1) Mandát archivu, odpovědnost za uchování a popis cílových skupin. (K1, K2, K3, K6, K7)
Typicky dokládá: zákonná zmocnění, seznam právních předpisů a smluv, opatření k zachování práv (ochrana osobních údajů, autorská a uživatelská práva, etc.), popis cílových skupin a jejich specifických požadavků.
2) Aktuální a dlouhodobá koncept financování. (K8)
Typicky dokládá: aktuální rozpočet, rozpočtový výhled, dlouhodobý koncept financování.
3) Dostatečné a kvalifikované lidské zdroje, koncept jejich rozvoje. (K9)
Typicky dokládá: popis pracovních pozic, přehled míst a koncepci rozvoje pracovníků.
4) Přiměřenou organizační strukturu a z ní vyplývající procesy. (K10)
Typicky dokládá: organizační řád, procesní model, organigram.
5) Krizové řízení a exit plán. (K12)
Typicky dokládá: Krizový plán, případně smlouvu/prohlášení o převzetí závazků jiným subjektem.
6) Bezpečnost (K34)
Typicky dokládá koncept IT bezpečnosti a koncept bezpečnosti infrastruktury.
7) Zajištění přístupu k reprezentacím uložených digitálních objektů pro oprávněné uživatele. (K4)
Typicky dokládá: odkazovací pomůcky (katalogy, inventáře, vyhledávací pomůcky), řád pro užívání, dokumentaci přístupových scénářů dle uživatelských skupin.
8) Zajištění možnosti interpretovat informace obsažené v uložených digitálních objektech (K5, K13)

Typicky dokládá: popis strategií dlouhodobého zachování interpretovatelnosti, koncept plánování uchovávání, dokumentaci významných vlastností uložených digitálních objektů.
9) Strategické činnosti související s uchováním (K11)
Typicky dokládá: strategický plán uchování.

ad 3.2

1) Popis funkcionalit rozhraní pro příjem, archivního úložiště a uživatelského rozhraní, jež zajišťují integritu uchovávaných informací a umožňují posouzení autenticity reprezentací dat. (K14-K19).
Doporučujeme popsat po jednotlivých modulech (Příjem, Archivní úložiště, Přístup) - vždy integritu + autenticitu.
Typicky dokládá: technické dokumentace rozhraní, popis workflow, ukládací koncepce, koncept bitové ochrany, koncept zpřístupňování, monitoring a dokumentace všech změn reprezentací.
2) Technická oprávnění k přejímaným reprezentacím tak, aby po jejich převzetí mohla být prováděna všechna nutná opatření bez technických omezení (např. kódování, ochrana proti kopírování).
Typicky předkládá: dohody s producenty, popis přezkoumání technických omezení.
3) Popis IT infrastruktury, tj. zavedení technických a bezpečnostních opatření specifikovaných v K13-K26. Vlastní IT infrastruktura archivu nebo (z části) IT infrastruktura provozovaná poskytovatelem služeb, sestává z hardware, rozvodů, software a rozhraní, které jsou nutné k provozu digitálního archivu. (K33)
Typicky dokládá: Technická dokumentace, grafické znázornění IT infrastruktury.

ad 3.3

1) Specifikace metadat – popisná, strukturální, technická a administrativní (K28, K29, K30 a K32)
Typicky dokládá: Specifikace metadat, odkazy na použité směrnice a standardy
2) Specifikace SIP, AIP a DIP. Specifikace převodu SIP do AIP a AIP do DIP. (K21, K22, K23, K25, K26)
Typicky dokládá: Specifikaci informačních balíčků, popis procesů převodu.
3) Zajištění interpretovatelnosti AIP (K24)
Typicky dokládá: Plány uchovávání, dokumentace provedených migrací, specifikace emulátorů popř. emulačních prostředí.
4) Zaznamenání postupů při činnostech souvisejících s uchováním (K31)
Typicky dokládá: koncept zaznamenání postupů při činnostech souvisejících s uchováním – obvykle dle PREMIS

ad 3.4.

Pro posouzení naplnění požadavků dle §18b a §18c Zákona žadatel:
1) předloží dokumentaci řešení jednotlivých požadavků,
2) řešení demonstruje v praxi.

Přílohy:

1) Stavebně-technické a bezpečnostní podmínky
2) Struktura AIP pro přenos do NDA
3) Vysvětlující informace k Pečeti nestoru pro důvěryhodné digitální archivy, 2018.

Tento metodický návod v plném rozsahu nahrazuje Metodický návod č. 2/2022 pro akreditaci digitálního archivu.

PhDr. Daniel Doležal, Ph.D.
ředitel

Ministerstvo vnitra
Nad Štolou 3, 170 34 Praha 7
IČ: 00007064, posta@mv.gov.cz, T: +420 974 811 111
ID DS: 6bnaawp, mv.gov.cz

Elektronický podpis: 10.7.2026
Certifikát autora podpisu:
Jméno: PhDr. Daniel Doležal Ph.D.
Vydal: NCA SubCA1/RSA 10/2023
Platnost do: 22.9.2028 10:16 +02:00