DLOUHODOBÁ ARCHIVACE ELEKTRONICKÉ ZDRAVOTNICKÉ DOKUMENTACE

Karel Benák, Jaroslav Brož, Miroslav Novotný, Ladislav Picek, Petr Vondrouš, Lubomír Wurm

Anotace

Článek si klade za cíl informovat o současných právních a technologických aspektech dlouhodobé archivace elektronické formy zdravotnické dokumentace. V kontextu projektu *„Implementace vedení zdravotnické dokumentace ve VFN Praha v čistě elektronické formě"* ukazuje úskalí, s nimiž je nutno počítat při implementaci bezpečného úložiště pro dlouhodobou archivaci. Článek pokládá otázky, které dle mínění autora, ještě čekají na své zodpovězení.

Klíčová slova

elektronická zdravotnická dokumentace, EHR, archivace elektronické dokumentace, dlouhodobý elektronický podpis, LTES

1. Úvodní informace

Elektronická archivace dokumentů jako důsledek dlouhodobého trendu elektronizace pracovních prostředků a procesů se v posledních několika letech zdá masivně nastupovat ve všech sférách společenských aktivit, zdravotnictví nevyjímaje. V souladu s tímto proudem vznikají (někdy poněkud opožděně) i příslušné právní normy upravující nové aspekty manipulace s elektronickými dokumenty. Zejména roky 2008 a 2009 lze považovat za poměrně plodné období jak z pohledu legislativní aktivity na tomto poli, tak i z pohledu projektů financovaných státem (Integrovaný systém datových schránek, Národní standard pro elektronické systémy spisové služby, Národní digitální archiv). V tomto ne zcela právně ustáleném období vznikl i projekt *„Implementace vedení zdravotnické dokumentace ve VFN Praha v čistě elektronické formě"*. Kromě právní analýzy se opíral o používané technické standardy v oblasti elektronického podepisování a archivace. Ačkoli normy a standardy použitelné pro vedení elektronické zdravotnické dokumentace (EZD) jsou obecně dostatečně prověřeny praktickými implementacemi zdravotnických elektronických informačních a komunikačních systémů, lze říci, že oblast dlouhodobé archivace EZD je relativně nová (pomineme-li systémy PACS) a v potřebné šíři neprověřená (vazby na spisovou službu, národní archiv apod.).

Zkratka	Význam
API	Application Programming Interface
BES	Basic Electronic Signature – základní formát digitálního podpisu dle standardu ETSI TS 101 733

Zkratka	Význam
BÚ	Bezpečné úložiště – HW komponenta pro uchovávání EZD v souladu s platnou legislativou
CAS	Content Address (Aware) Storage
CMS	Cryptographic Massage Syntax – PKCS standard
ESS	Enhanced Security Services for S/MIME – RFC 2634
EZD	elektronická zdravotnická dokumentace, zde chápáno jako čistě elektronická forma
ERMS	Electronic Record Management System – elektronický systém spisové služby
ETSI	European Telecommunications Standards Institute
IS	informační systém
LTES	Long Term Electronic Signature – ETSI TS 101 733
NIS	nemocniční informační systém
PKCS	Public-Key Cryptography Standards
QC	Kvalifikovaný certifikát dle ZoEP
RFC	Request For Comment – specifikace pro standardizaci provozu sítě Internet
SASL	Simple Authentication and Security Framework – RFC 4422
VFN	Všeobecná fakultní nemocnice Praha
WORM	Write Once Read Many – typ datového media
XAdES	XML Advanced Electronic Signatures – ETSI TS 101 903
ZD	zdravotnická dokumentace
ZEP	zaručený elektronický podpis ve smyslu zákona ZoEP
ZoAS	Zákon č. 499/2004 Sb., o archivnictví a spisové službě
ZoEP	Zákon č. 227/2000 Sb., o elektronickém podpisu
ZoZL	Zákon č. 20/1966 Sb., o péči o zdraví lidu
ZZ	Zdravotnické zařízení

Tabulka 1 – Termíny a zkratky

2. Východiska řešení dlouhodobé archivace EZD ve VFN

V další části kapitoly bude proveden detailní rozbor požadavků vymezujících implementaci dlouhodobé archivace. Jde o rozbor z pohledu legislativy, standardů tvorby dlouhodobě platných ZEP a z pohledu vlastního provozu NIS.

2.1 Právní požadavky

V dalším textu vycházíme zejména z následujících právních předpisů:

1. Zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů
2. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů,
3. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů, ve znění pozdějších předpisů,
4. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,
5. Vyhláška č. 385/2006 Sb. o zdravotnické dokumentaci.

2.1.1 Dlouhodobá autenticita a použitelnost

Zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů ukládá požadavek na vybavení každé samostatné části EZD ZEP a použitelnost archivované EZD po celou dobu archivace.

2.1.2 Doba archivace a způsob skartace

Doba archivace a způsob skartace ZD vyplývá z vyhlášky č. 385/2006 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů. ZD nesmí být zničena jinak, než v rámci skartačního řízení. To je definováno ve skartačním řádu, jež je přílohou výše zmíněné vyhlášky. Skartační řízení probíhá jednou ročně a během něj je posuzována potřebnost ZD pro poskytování zdravotní péče po uplynutí skartační lhůty (min. 5let). Pokud je dokumentace nepotřebná, je navržena ke zničení. Skartační návrh posuzuje skartační komise, která rozhodne s konečnou platností o prodloužení skartační lhůty (min. o 5let) nebo dá pokyn ke zničení dokumentace (po předchozím výběru a odevzdání archiválií do Národního archivu). Základní skartační lhůty jsou stanoveny skartačním řádem dle typu zdravotnické dokumentace a oblasti zdravotní péče, do níž spadá. Např. u léčby duševních poruch je tato lhůta stanovena na 100 let po narození a u pitevního protokolu, který slouží pro účely soudního lékařství, je stanovena na 150let.

Vlastní průběh skartace upravuje vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby, pokud se na vedení EZD vztahuje ZoAS.

2.1.3. Ochrana osobních údajů

Právní status obsahu archivované EZD je upraven zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a zákonem č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů. Zákonné požadavky na ochranu osobních údajů a řízený a dokladovatelný přístup k EZD jsou prakticky stejné jako u „živé" EZD.

Z pohledu implementace lze na základě výše uvedeného vyvodit následující požadavky:

- **P1:** EZD musí být dostupná teoreticky neomezeně dlouho, tedy i nezávisle na NIS.
- **P2:** Informační obsah EZD musí být čitelný teoreticky neomezeně dlouho.
- **P3:** Informační obsah EZD musí být původní, archivací nezměněný.
- **P4:** Musí být prokazatelné teoreticky neomezeně dlouho (tedy nezávisle na NIS), zda je ZEP na EZD platný.
- **P5:** Pouze oprávněné osoby mohou přistupovat k archivované EZD a to specificky jen k té části EZD, do níž jsou oprávněni nahlížet nebo ji jinak použít.
- **P6:** Veškeré přístupy k archivované EZD musí být trvale zaznamenané z pohledu přistupující osoby, cíle přístupu, způsobu a času přístupu.

Splnění těchto požadavků reálně fungujícím systémem není možné garantovat na neomezeně dlouhou dobu již jen z důvodu omezené doby životnosti reálných elektronických systémů a s přihlédnutím k faktu, že vývoj informačních technologií a zpětnou kompatibilitu technických standardů nelze predikovat na déle než zhruba deset let.

Problém dlouhodobé garance se týká i vlastního právního řádu a to zejména norem typu vyhláška, která v tomto případě upravuje skartační lhůty ZD.

Proto jsme nuceni navrhnout koncepci BÚ na principu „best effort" s výhledem dlouhodobé garance požadavků v řádu desítek let.

2.1.4 Provozní požadavky

Z pohledu nakládání se zdravotnickou dokumentací lze detekovat následující požadavky na implementaci BÚ:

- **P7:** Podpora procesu skartačního řízení – zejména možnost vyhledat k danému datu samostatné části EZD, jimž uplyne skartační lhůta.
- **P8:** Možnost automatizace bezpečného rušení obsahu dle předem daných pravidel (politik).
- **P9:** Možnost agregace různých typů dat do souvisejících celků (spisů) a jejich jednotnou správu (např. sdružování textových, kryptografických a obrazových dat vztahujících se k jednomu léčebnému výkonu či pacientu).
- **P10:** Odolnost proti poruše jakékoli technické komponenty.
- **P11:** Rozšiřitelnost co do kapacity i redundance komponent (např. možnost vybudovat záložní BÚ).
- **P12:** Řešení musí být otevřené pro budoucí aplikace vyžadující archivaci elektronické dokumentace ve shodě s legislativou.

2.2 Požadavky standardizace

V této oblasti jsou podstatné standardy pro zajištění dlouhodobé autenticity, dostupnosti a bezpečnosti procesů souvisejících s celým životním cyklem elektronické dokumentace.

2.2.1 Dlouhodobě platný zaručený elektronický podpis

To, jak lze pomocí časových razítek ošetřovat elektronický podepsané dokumenty před i během jejich archivace specifikuje standard RFC-3126 *(Electronic Signature Formats for long term electronic signatures – LTES),* který byl dopracován ETSI a vydán jako standard ETSI TS 101 733. Formát LTES je nadstavbou nad CMS zabezpečující elektronický podpis tak, aby mohl být verifikován ke konkrétnímu času v minulosti. LTES doplňuje k elektronickému podpisu informace důležité pro verifikaci podpisu v budoucnosti a vše konzervuje pomocí časových razítek.

Obdobně standard ETSI TS 101 903 definuje formát podpisu XML dokumentů a navazuje tak na obecnou specifikaci XMLDsig definovanou konsorciem W3C.

Níže je uveden přehled typů LTES formátu:

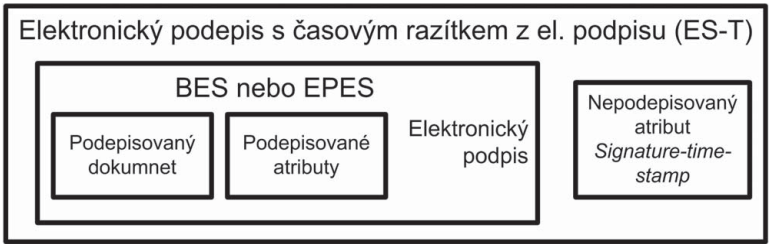
BES *(Basic Electronic Signature)*

BES je z pohledu standardu ETSI TS 101 733 nejjednodušší variantou elektronického podpisu. Jde o elektronický podpis tak jak je znám ze specifikace CMS, doplněný o několik podepisovaných atributů. Obecně v podpisu BES mohou být nepodepisované atributy jako např. kontrasignatura *(CounterSignature)*. Jedinou výjimkou oproti standardu CMS je, že se již vůbec nepředpokládá elektronicky podpis bez podepisovaných atributů.

Formát BES povinně vyžaduje následující atributy:

- *Message Digest*
- *Content Type*
- *Signing Certificate*
- *Other-signing-certificate m*á stejný význam jako *Signing Certificate,* ale umožňuje libovolný algoritmus pro hash. Podpis typu BES pak musí mít povinně jeden z těchto dvou atributů.

ES-T – obsahuje navíc časové razítko (TS) z podpisu typu BES (viz Obrázek 1) *do nepodepisovaných atributů*, pokud TS není vygenerováno v okamžiku podpisu, musí ověřovatel buď TS vygenerovat při příležitosti 1. ověření (které by mělo nastat dostatečně brzy po vytvoření podpisu), nebo udržuje bezpečné časové záznamy o ověřených EP. Nelze zpětně zjistit, zda časové razítko nebylo z podpisu vyňato.



Obrázek 1 – Podpis formátu ES-T

ES-C – jde o *ES-T* doplněný kompletními *odkazy* na validační data (certifikáty a stav jejich revokace) *do nepodepisovaných atributů*. Pokud tato validační data nedodá podepisující osoba, musí je doplnit ověřovatel po 1. ověření EP, jakmile jsou tato data k dispozici (záznam o revokaci certifikátu, konci pozdržení jeho platnosti apod.). Obecně nelze kompletní odkazy na validační data dodat při vytváření podpisu, to lze jen ve zvláštních případech, kdy po vytvoření podpisu typu ES může podepisující osoba dodatečně do podpisu tato data doplnit. Tyto odkazy mají smysl po dobu, kdy jsou CA povinny vlastní validační data archivovat v souladu se svou certifikační politikou. Časové razítko v EP typu ES-T a ES-C zajišťuje platnost certifikátu i v případech, kdy další validační data byla kompromitována po časovém okamžiku vyznačeném čas. razítkem.

ES-X – jde o rozšíření formátu ES-C, které je vhodné v případech, kdy ověřovatel nemá přístup k certifikátu podepisující osoby, ke všem certifikátům CA tvořící certifikační řetězec nebo ke všem vztažným informacím o stavu revokace certifikátu. V takovém případě jsou možné dva přístupy řešení:

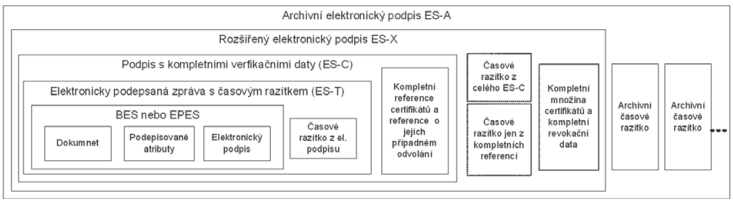
- Všechny položky validačních údajů jsou součástí EP. Certifikáty se ukládají do atributu *Certificate-value*s a revokační informace do atributu *Revocation--values*. Pokud alespoň některý z atributů *Certificate-values* nebo *Revocation-values* je v elektronickém podpisu přítomen, pak jde o podpis E*S-X Long*.
- K údajům formátu ES-C je přidáno časové razítko *do nepodepisovaných atributů*. Tento formát má 2 varianty:
  ES-X 1 – časové razítko přes validační data (ochrana pro případ kompromitace certifikátů v certifikačním řetězci), časové razítko a samotný digitální podpis.
  ES-X 2 – časové razítko pouze přes validační data

ES-A *(archivní elektronický podpis)*

Pokud by došlo vlivem dlouhodobé archivace k nebezpečí, že:

- klíče a ostatní kryptografická data použitá pro vytvoření *ES-C* se stanou slabými,
- algoritmy se stanou zranitelnými,
- certifikáty časových razítek exspirují,

pak lze EP všech typů vybavit novým tzv. archivačním časovým razítkem ze všech důležitých atributů s pokud možno silnějším kryptografickým algoritmem nebo delšími klíči. Další archivní časová razítka se přidávají za stávající dokument. Počítají se nejen z původní zprávy (např. ES-X), ale i ze všech předchozích archivních časových razítek. Celou strukturu znázorňuje Obrázek 2.



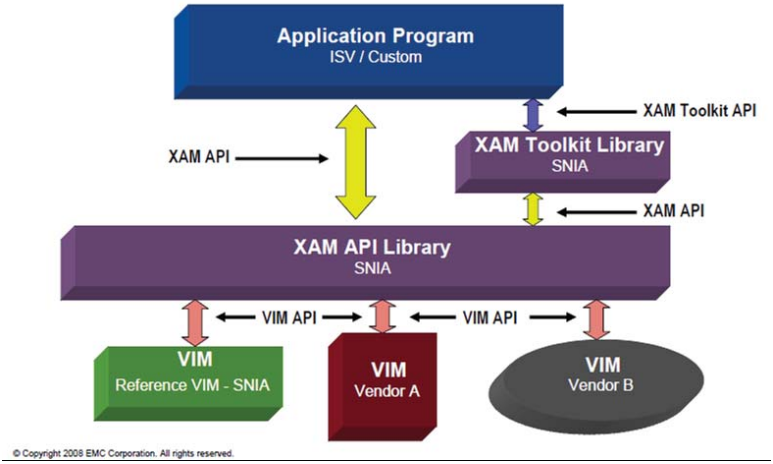
Obrázek 2 – Podpis formátu ES-A

2.2.2 Standardy přístupu k archivačním zařízením

Průmyslové standardy v oblasti zařízení pro ukládání dat (storage) definuje asociace SNIA (Storage Networking Industry Association), z jejíhož popudu vznikl standard XAM (eXtensible Access Metod). Standard je zaměřen na přístup k fixnímu datovému obsahu, typicky k archivovaným datům. Definuje architekturu přístupu k archivovaným datům a sadu API funkcí včetně referenčních implementací v jazycích C a Java.
Principy architektury XAM:

1. Datové objekty (XSet) jsou z pohledu aplikace popsány svou unikátní adresou (XUID – XAM Unique ID), která je nezávislá na jejich fyzické lokaci
2. Datové objekty jsou „obaleny" strukturovanými (XML) aplikačními metadaty s vyznačeným datovým type (MIME-type) umožňujícími snazší manipulaci s vlastním informačním obsahem
3. Modulární architektura umožňuje výrobci storage dodat SW Plug-in modul, který splňuje specifikaci VIM API (Vendor Interface Module API), a tím je příslušné úložné zařízení dostupné stávajícím aplikacím.
4. Je definována množina správcovských rysů a vlastností pro neměnná data (zachování neměnnosti dat, žádost o datový obsah, vymazání obsahu apod.)

Architektura XAM představuje v podstatě třívrstvý model. Nejnižší vrstva je představována **VIM Plug-in moduly**, umožňujícími připojení úložného zřízení (storage). Střední vrstva je reprezentována knihovnou funkcí a nástrojů pro provádění potřebných operací s datovými objekty v úložištích prostřednictvím standardizovaného **VIM API**. Tyto funkce a nástroje jsou přístupné nejvyšší, aplikační vrstvě prostřednictvím standardizovaného API (**XAM API** a XAM Toolkit API). Architektura je znázorněna níže na Obrázku 3.



Obrázek 3 – Architektura XAM

3.Koncepce BÚ ve VFN

Koncepce BÚ pro dlouhodobou archivaci EZD vycházela z požadavků specifikovaných zadavatelem:

1. Navržený systém musí v době spuštění do provozu odpovídat platným právním předpisům upravujícím vedení EZD,
2. v případě nedostatečnosti právního rámce bude řešení vycházet z principu „best practice" a tento přístup bude ověřen nezávislým auditem,
3. není požadováno převedení stávající neelektronické zdravotnické dokumentace do elektronické formy a její archivace,
4. systém musí být otevřený pro archivaci i jiného druhu dokumentace, než je EZD.

V současné době se z pohledu media nabízí tři přístupy ke koncipování BÚ:

1. Datové nosiče typu WORM založené na optickém nebo magnetickém záznamu.
2. Standardní datové úložiště typu WORM založené na magnetickém záznamu.
3. Specializované datové úložiště typu CAS

Zatímco první dva přístupy nabízí práci s archivovanými daty pouze na úrovni souborového systému, třetí přístup – CAS – pohlíží na fixní data jako na objekty, jež lze doplnit metadaty pro flexibilní vyhledávání a automatizaci práce na bázi politik. Tento přístup se nám jevil vhodný z pohledu výše uvedených požadavků **P7**, **P8** a **P9**. Zejména pak tento přístup umožňuje realizovat systemizovanou elektronickou analogii papírové kartotéky, v níž jsou složky k danému pacientovi obsahující různorodé typy a fragmenty zdravotnické i nezdravotnické dokumentace a provázat ji přímo s aplikační databází (lze pak archivovat i jen určité položky databázové tabulky). Zařízení typu CAS implementuje veškeré potřebné nástroje pro práci s datovými objekty v interním OS a publikuje pouze API pro využití poskytované funkčnosti externím aplikacím. Zařízení tohoto typu existují na trhu již zhruba 10 let, nicméně standardizace přístupové architektury představovaná specifikací XAM je poměrně mladá. Po zvážení přínosů a rizik využití vyzrálého ale proprietárního rozhraní API proti relativně nové ale standardizované specifikaci XAM jsme zvolili cestu standardu XAM zejména s ohledem na požadavky **P1**, **P2** a **P12**.

3.1 Volba archivačního zařízení

Při volbě archivačního zřízení typu CAS podporujících standard XAM jsme narazili na několik produktů, připadajících v úvahu. Interním výběrovým řízením jsme zvolili zařízení Centera Governance Ed., které je k dispozici v portfoliu produktů společnosti EMC2 od r. 2002 (akvizice holandského výrobce). Představuje průkopnické řešení v oblasti CAS, jež pracuje s mnoha miliardami objektů, čímž překonává problémy se škálovatelností tradičních souborových systémů.

Architektura

Základním architektonickým rysem je vysoká redundance komponent s možnost budovat záložní systém pro případ totálního selhání primární lokality.

Stavební entitou úložiště EMC2 Centera je tzv. uzel (node) sestávající z řídicího SW (CenteraStar) a diskového pole RAID5 tvořeného vysokokapacitními (1TB, 2TB) SATA disky. Každý uzel disponuje duální síťovou konektivitou a duálním napájením. Každý uzel komunikuje po IP síti protokolem TCP.
Uzly jsou dvojího typu:

1. Storage node – spravují diskové pole
2. Access node – vybavené navíc přístupovou logikou k datovým objektům – jsou vždy zdvojeny.

Sestava 4 uzlů formuje základní jednotku systému, Centera klastr, který je rozšiřitelný vždy po dvou uzlech. Jeden klastr může obsahovat až 32uzlů. V rámci klastru je prováděn automatický load-blancing.

RAIN
Nad uzly se vytváří z pohledu datové redundance pole typu RAIN (Redundant Array of Independent Nodes). Jde o gridovou architekturu, která umožňuje škálovat úložný prostor až přes 128 uzlů a dosahovat efektivní úložné kapacity stovek TB. Skutečná kapacita Centery závisí jednak na kapacitě zvolených diskových jednotek a dále na algoritmu zajištění redundance v poli RAIN. Uzly mohou být osazeny různými typy disků, čímž je umožněna automatická migrace datových objektů ze starších uzlů na technologicky novější. Na výběr jsou dva režimy zajištění redundance dat:

- V režimu CPM (Content Protection Mirroring) dochází k vytváření kopií datových objektů na různých uzlech. Tento režim disponuje vysokou redundancí na úkor efektivního datového prostoru.
- V režimu CPP (Content Protection Parity) se data rozkládají přes 7 uzlů včetně paritní informace. Tento druhý režim spoří datový prostor na úkor redundantních dat a ke své činnosti potřebuje systém s nejméně 8mi uzly.

Několik klastrů Centera může vytvářet nadřazené celky (geoklastry).

3.2 Zajištění dlouhodobé platnosti ZEP
Platnost ZEP obecně nelze doložit v době, kdy nejsou platná data pro ověření ZEP, konkrétně podobě exspirace nebo zneplatnění QC či certifikátů nadřazených. Aby bylo možné z dlouhodobého hlediska ověřit platnost elektronického podpisu, je třeba mít důkaz o existenci podpisu před jistým časovým okamžikem v minulosti. Tím vyloučíme pochyby typu podvržení ZEP k EZD někdy později, kdy příslušné certifikáty pozbyly své platnosti. Takovým důkazem je časové razítko vytvořené z elektronického podpisu, které vydá důvěryhodná autorita pro vydávání časových razítek (TSA). Časové razítko poskytuje možnost ověřit platnost elektronického podpisu za těchto předpokladů:

1. Zdroj času je důvěryhodný.
2. Podpis je ověřován v periodě platnosti certifikátu časové autority, jež časové razítko vydala. Předpokládáme 10ti letou platnost certifikátu TSA.
3. Jsou k dispozici validační data – podpisový certifikát včetně všech certifikátů v certifikační řetězci, seznam odvolaných certifikátů, certifikát časové

autority včetně všech nadřazených certifikátů a seznamy odvolaných certifikátů certifikačních a časových autorit.

Časové razítko z elektronického podpisu se k elektronickému podpisu přidává do struktury CMS jako nepodepisovaný atribut. Může být přidáno uživatelem uzavírajícím a podepisujícím EZD, nebo jej automaticky doplňuje úloha dávkového zpracování spuštěná na externím aplikačním serveru. Dostatečná frekvence spouštění této úlohy zajistí vybavení ZEP časovým razítkem s maximálním zpožděním několika hodin.

Bezprostředně před vlastní archivací elektronického dokumentu reprezentujícího samostatnou část ZD dochází k ověření platnosti ZEP vč. časového razítka (lze využít on-line či off-line ověření stavu certifikátu). Do archivačního zařízení pak putují společně s podepsaným dokumentem ve formě metadat i následující validační informace:

- stav ověření platnosti ZEP
- podpisový QC
- všechny certifikáty v certifikační cestě QC
- aktuální seznam odvolaných certifikátů (CRL)
- certifikát TSA včetně nadřazených certifikátů
- CRL certifikátů certifikačních autorit a časové autority

Klíčovým momentem, na němž toto řešení staví, je nezpochybnitelnost obsahu archivovaného v daném čase, tedy i nezpochybnitelnost validačních údajů archivovaných spolu s EZD. V případě nutnosti ověřit podpis v budoucnu bude možné příslušná validační data ke konkrétnímu dokumentu získat na základě příslušných metadat, a vlastní validační data lze v rámci archivu uchovávat pouze v jedné instanci (deduplikace).

Tím se vyhýbáme nutnosti vytvářet podpisy ve formátu LTES typu ES-A, které mají následující diskvalifikační faktory:

- potřeba obnovy validovatelnosti podpisu dodatečným opakovaným časovým razítkováním,
- LTES je oproti CMS poměrně málo rozšířený – možné problémy s přenositelností ZEP.

4. Úskalí dlouhodobé archivace EZD

4.1. Nový fenomén – elektronická spisová služba

Jak již bylo dříve zmíněno, rok 2009 přinesl nové legislativní úpravy, které, zdá se, významnou měrou zasáhnou do procesu vedení ZD **v čistě elektronické formě**. Právě okamžikem odmítnutí klasické papírové či filmové podoby zdravotnické dokumentace se otevírá prostor pro implementaci ustanovení vyplývajících ze zákona 190/2009 Sb., který novelizuje zákon č. 499/2004 Sb., o archivnictví a spisové službě především s důrazem na výkon spisové služby v elektronické podobě. Prováděcí vyhláška 191/2009 Sb. k tomuto zákonu pak dává návod na zásadní změny ve filosofii práce se zdravotnickým informačním systémem. Mezi tyto změny patří:

1. Dokumentem ve smyslu ZoAS § 2 písm. d) je chápána každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové

či **digitální**, která byla v rámci ZZ vytvořena nebo doručena. Tedy tato obecná definice naznačuje, že veškeré zdravotnické informační systémy bez ohledu na typ zdravotnického provozu (ambulantní, klinický, laboratorní apod.) pracují s dokumenty, které podléhají zákonu o archivnictví v případě, že ZZ je povinno uchovávat dokumenty a umožnit výběr archiválií.

2. ZZ na něž se vztahuje povinnost předkládat dokumenty Národnímu archivu pro výběr archiválií jsou podle ZoAS § 3 také státní příspěvkové organizace (např. FN) a právnické osoby zřízené nebo založené územními samosprávnými celky (např. Krajské nemocnice). Tyto jsou pak povinny dle § 63 vést spisovou službu nejpozději od 1.7. 2012 v elektronické formě.
3. Dokument – v našem případě každá samostatná část EZD vzniklá ve zdravotnickém IS popř. doručená z venčí – musí být již při svém vzniku či doručení označen jednoznačným identifikátorem a evidován v elektronickém systému spisové služby. **Toto ustanovení implikuje potřebu propojit zdravotnické IS a IS spisové služby.**
4. Kromě výše uvedeného musí dojít k přidělení spisového a skartačního znaku v době vytvoření dokumentu (samostatné části EZD). Spisový znak je označení, které zařazuje dokumenty do věcných skupin pro účely pozdějšího vyhledávání a vyřazování. Skartační znak je označení sloužící k posouzení vhodnosti samostatné části EZD k vyřazení v rámci skartačního řízení. **Toto ustanovení klade nové nároky na odborný zdravotnický personál, který musí** v souladu s prováděcí vyhláškou č 191/2009 Sb. **z palety druhů zdravotnické dokumentace** definované vyhláškou č. 385/2006 Sb. **vybrat ten správný skartační znak již při vzniku dokumentu** (zápisu do dekursu, ambulantní karty, operačního protokolu, či žádanky o laboratorní vyšetření apod.). Skartační znak pak dále ovlivňuje skartační lhůtu, **která je navíc v některých případech v čase proměnná** (začíná pro daný spis běžet od doby posledního vyšetření).
5. Vyřazování (skartace dokumentace) se děje v celých spisech, proto musí být zdravotnický IS schopný vytvářet EZD dle této filosofie a skartovat samostatné části EZD v rámci skartace celého spisu. Pojem spis je obecně definován vyhláškou 191/2009 Sb. **IS nakládající s EZD v rámci ZZ by měly být schopny umožnit skartaci i v případě, že je vedena paralelně papírová forma ZD a tato skartace by měla probíhat společně se skartací papírové či jiné „analogové" dokumentace**, což se neděje.
6. Další změna přichází s příjmem zdravotnické dokumentace z vnějšího prostředí (např. zpráva z odborného vyšetření přinesená pacientem). **Každý takový dokument by měl být konvertován do elektronické podoby, a evidován v ERMS a následně přiřazen do NIS ke správnému „spisu".** Podobně je tomu při odesílání EZD do externího prostředí (jinému ZZ, orgánu veřejné moci apod.).

4.2 Datové formáty

Řešení bezpečného úložiště pro EZD vyžaduje volbu vhodného formátu a metadat jak z pohledu programátorské technologie IS, tak z pohledu

analytického – práce s dokumentací v BÚ, které má dva základní cíle:

1. umožnit výstup EZD či její samostatné části v digitální podobě vhodné pro autorizovanou konverzi do podoby papírové,
2. podpořit skartační řízení v rámci spisové služby.

V prvním případě se autorizovanou konverzí zabývá zákon 300/2008 Sb, o elektronických úkonech a autorizované konverzi dokumentů resp. prováděcí vyhláška z 15.6.2009, která stanoví jediný vhodný formát a to PDF v1.3 a vyšší nebo PDF/A. **Toto vnímáme jako poněkud diskriminující zejména z pohledu existujících zdravotnických IS a kolidující s jinými nařízeními, specifikujícími povinný formát XML (např. elektronická preskripce ve vazbě na SÚKL).** Je otázka, zda toto portfolio bude rozšířeno o další možné formáty.

V druhém případě – při výkonu spisové služby takováto omezení neplatí, protože kromě preferovaného formátu PDF/A pro statické textové dokumenty a statické kombinované textové a grafické dokumenty, povoluje vyhláška č. 191/2009 Sb. v § 20 odst. 6 pro výstup též jiné datové formáty.

Další potenciální změna již fungujících IS pro ukládání EZD do bezpečného úložiště vyplývá z povinnosti doplnit spis (EZD daného pacienta) metadaty, která stanoví národní standard pro elektronické systémy spisové služby. Z vyhlášky č. 191/2009 Sb. nevyplývá, že by toto měl zabezpečovat zdravotnický IS, ale je to poměrně logické, protože ERMS by mohl mít problém s modifikací spisu.

4.3. Definice pojmu „bezpečné úložiště"

V souvislosti s dlouhodobou archivací (100 a více let) elektronické dokumentace hovoříme o bezpečném úložišti a vyhýbáme se spojení „bezpečný archiv". Tento pojem je použit specificky v ZoAS. Pojem bezpečné úložiště chápeme jako elektronický systém určený pro dlouhodobé ukládání digitálních dokumentů takovým způsobem, který garantuje jeho integritu a autentičnost v čase. **Otázkou je právě ona garance či „bezpečnost".** Domníváme se, že atribut „bezpečné" úložiště není dostatečně popsán či dokonce standardizován. Při tom garance bezpečnosti se zdaleka netýká pouze zajištění dlouhodobé platnosti elektronického podpisu či vysoké dostupnosti archivačního zařízení a řízení přístupu k němu. Je jisté, že během dlouhodobé archivace bude nutno s digitálním dokumentem pracovat – migrovat jej na technologicky novější úložiště, opakovaně časově razítkovat a konvertovat jeho formát. Tyto procesy bude třeba provádět **„bezpečně".** Ačkoli existují standardy pro budování bezpečného elektronického archivu (např. německá technická směrnice BSI TR 03125), je otázkou nakolik jsou aplikovatelné do prostředí ZZ, která primárně neslouží jako archivy a ani systémy digitálního archivu nehodlají budovat.

5. Závěr

Domníváme se, že je v dnešní době možné budovat „bezpapírovou nemocnici" v tom smyslu, že pokud je digitální podoba ZD technicky k dispozici, legislativně nic nebrání práci s ní. Zároveň ale detekujeme nezcela jasné propojení legislativy upravující oblast archivnictví a spisové služby a oblast vedení

zdravotnické dokumentace v digitální podobě. Spojovací článek mezi těmito dvěma oblastmi vidíme zejména ve vyhlášce 191/2009 Sb., která v § 2 uvádí, že evidenci podle této vyhlášky nepodléhá dokumentace, která nemá „úřední charakter". Které typy zdravotnické dokumentace jsou považovány za úřední a které ne definuje původce ve svém spisovém řádu. Některá ZZ vůbec nepodléhají výkonu spisové služby, ale pravidla nakládání se zdravotnickou dokumentací podle vyhlášky 385/2006 Sb. se na ně vztahují zcela plnohodnotně. Nabízí se otázka, zda by neměl být sjednocen pohled na vedení zdravotnické dokumentace v čistě elektronické formě nezávisle na ZoAS. Producentům zdravotnických IS ale i provozovatelům ZZ a zdravotníkům v nich pracujících by takový pohled jistě přišel vhod.

Literatura

[1.] Sbírka zákonů ČR

[2.] Národní standard pro elektronické systémy spisové služby, Věstník Ministerstva vnitra, částka 76/2009 (část II)

[3.] Pinkas D., Ross J., Pope N.: Electronic Signature Formats for long term electronic signatures, RFC-3126, Network Working Group, September 2001

[4.] Horgan M.: Itroduction to XAM (eXtensible Archiving Method): A New Industry Standard Access Method for Fixed Content, EMC corporation, 2008 https://community.emc.com/servlet/JiveServlet/previewBody/1270-102-2-1403/EMC Introduction to XAM.pdf

[5.] EMC corporation, firemní materiály k EMC Centra, http://www.emc.com/products/detail/hardware/centera.htm

Kontakt:

Ing. Miroslav Novotný
Stapro s.r.o.
Pernštýnské náměstí 51
530 02 Pardubice
tel.: +420467003111
e-mail: *novotny@stapro.cz*