DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

<title>Systémy správy dokumentů</title>

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Pravidla pro jednotlivé sdílené služby, funkční celky a tematické oblasti jsou popsány v části Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivými úřady

Obecně o spisové službě

Orgány veřejné moci a další subjekty, které jsou podle příslušné legislativy zahrnuty do skupiny takzvaných "veřejnoprávních původců", mají za povinnost realizovat správu svých dokumentů formou výkonu spisové služby. Spisovou službou se rozumí veškeré činnosti a procesy týkající se evidence, správy a vyřizování dokumentů. Jedná se o dokumenty v analogové podobě (například listinné dokumenty) a také v digitální podobě (například elektronické dokumenty).

Legislativní rámec pro výkon spisové služby obsahuje Zákon č. 499/2004 Sb., o archivnictví a spisové službě a Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby. Národní standard pro ESSL vydaný ministerstvem vnitra pak stanovuje podrobné technické požadavky na aplikační a byznysové funkce ESSL a ISSD systémů.

U analogových dokumentů je hlavním cílem výkonu spisové služby evidence a správa metadat o těchto dokumentech a veškerých úloh a transakcí, které se s dokumenty činí. U digitálních dokumentů se pak jedná nejen o evidenci a správu metadat, ale také samotných souborů digitálních dokumentů, kterým se v odborné terminologii říká komponenty. Navíc obecně platí teze stanovená prováděcí vyhláškou o spisové službě, že nebrání-li tomu nic podstatného, měly by se na vstupu do organizace analogové dokumenty digitalizovat a dále by se s nimi mělo pracovat jako s digitálními.

Každý povinný subjekt musí

1. Vykonávat spisovou službu tak, že eviduje dokumenty v elektronickém systému spisové služby, nebo v samostatné evidenci naplňující požadavky ESSL.
2. Mít (alespoň jeden) elektronický systém spisové služby, nebo více ESSL.
3. Zajistit integraci ostatních systémů na ESSL pro správu metadat a realizaci úkonů spojených s dokumenty.
4. Vést jmenný rejstřík a přiřazovat subjektům bezvýznamové identifikátory v něm.
5. Řádně uchovávat a spravovat digitální dokumenty a jejich komponenty.
6. Provádět evidenci metadat o spisech a dokumentech a evidenci transakcí u dokumentů v ESSL či v samostatné evidenci splňující požadavky.
7. Realizovat správně procesy při příjmu a odesílání dokumentů, zejména k jejich důvěryhodnosti (ověřovat elektronické podpisy, elektronicky podepisovat, opatřovat časovými razítky, apod.).
8. Prostřednictvím modulu podatelny přijímat a evidovat veškeré doručené dokumenty a zajišťovat odesílání.
9. Zajistit digitální kontinuity evidovaných digitálních dokumentů po celou dobu jejich evidence.
10. Provozovat digitální spisovnu a zajistit uchování také digitálních dokumentů po dobu skartační lhůty.
11. Předávat digitální dokumenty do digitálního archivu s jejich metadaty ve správném tvaru a se všemi požadovanými metadaty.

Digitální kontinuita

Autenticitou dokumentů se rozumí otázka, zda jde o původní dokument: dokument je autentický, pokud nedošlo k žádné jeho změně. V případě elektronických dokumentů dokáží jejich neměnnost (označovanou též jako integritu) zajistit všechny druhy kryptografických elektronických podpisů, pečetí a časových razítek. Tedy zaručený elektronický podpis, stejně jako všechny vyšší druhy elektronických podpisů (zaručený elektronický podpis, založený na kvalifikovaném certifikátu, i kvalifikovaný elektronický podpis), zaručená elektronická pečeť, stejně jako všechny vyšší druhy elektronických pečetí, a také elektronické časové razítko.

Pravostí dokumentu se rozumí otázka, zda dokument pochází od toho, koho považujeme za jeho původce, a obecně se dovozuje z autentizačních prvků, kterými je dokument opatřen. V případě elektronických dokumentů jde o elektronické podpisy, elektronické pečeti a elektronická časová razítka. U nich se nejprve zkoumá (ověřuje) jejich platnost, která je technickým pojmem a je závislá na splnění určitých technických podmínek (podrobněji popsaných v článku 32, resp. 40 nařízení eIDAS). Teprve v případě prokázání jejich platnosti je možné, v závislosti na druhu elektronického podpisu či pečeti, z technické platnosti dovozovat i právní pravost příslušných autentizačních prvků (podpisů a pečetí) , a z ní následně i pravost elektronického dokumentu jako takového.

Digitální kontinuitou elektronických dokumentů se rozumí udržování těchto dokumentů po určitý časový interval v takovém stavu, aby během celého tohoto časového intervalu bylo možné prokázat splnění legislativních požadavků na jejich autenticitu a pravost. Tedy možnost ověřit (technickou) platnost elektronických podpisů, pečetí a/nebo elektronických časových razítek na dokumentech, a z ní dovodit právní pravost dokumentu jako takového. V souvislosti s tím je nutné zdůraznit, že možnost ověřit (technickou) platnost elektronických podpisů a pečetí, stejně jako časových razítek, se s postupem času ztrácí. Jde o základní vlastnost, jakousi časovou pojistku, charakteristickou pro všechny zaručené (a vyšší) druhy elektronických podpisů, pečetí a razítek. Jejím účelem je chránit již vytvořené elektronické dokumenty před zastaráváním a oslabováním kryptografických postupů a algoritmů, použitých u jejich podpisů (ale i pečetí a časových razítek).

Bez této časovém pojistky by po uplynutí určité doby již nebylo možné z technické platnosti dovozovat právní pravost podpisů, a tím ani celých dokumentů: vzhledem k oslabení kryptografických algoritmů, použitých u původně podepsaného dokumentu, by již bylo možné reálně najít (vypočítat) jiný dokument, který je tzv. kolizní vůči původně podepsanému dokumentu. Tedy takový dokument, který má jiný obsah, ale stejný elektronický podpis. Pak by bylo možné přenést elektronický podpis z původně podepsaného dokumentu na onen později vytvořený kolizní dokument, a v obou případech by byl takovýto podpis ověřen jako (technicky) platný – a nebylo by tak již možné spolehlivě prokázat, který dokument je pravý (který byl původně podepsán).

Problematika digitální kontinuity elektronických dokumentů naopak nezahrnuje otázku jejich pravdivosti, neboli správnosti obsahu těchto elektronických dokumentů. Požadavek na dlouhodobě zajištění, resp. dlouhodobé udržování digitální kontinuity elektronických dokumentů se v praxi týká jen těch elektronických dokumentů, u kterých je nějaký důvod pro zachování možnosti prokázat jejich autenticitu a pravost.

Řídící dokumenty

V rámci výkonu spisové služby jsou řídícími dokumenty zejména:

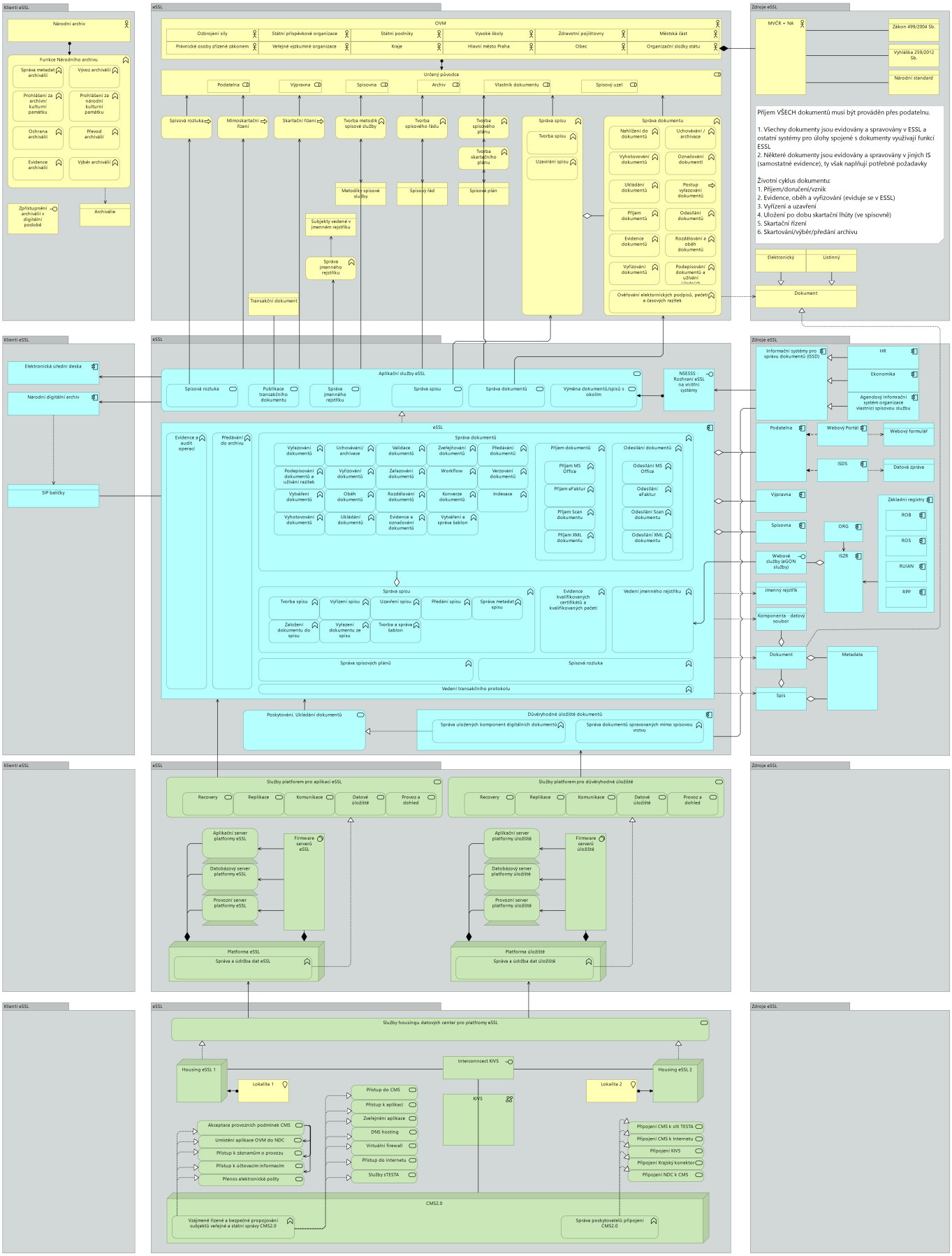
- Legislativa
    1. Zákon č. 499/2004 Sb., o archivnictví a spisové službě
    2. Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
- Technické a architektonické požadavky
    1. Národní standard pro elektronické systémy spisové služby
    2. Národní architektonický plán
- Vnitřní řídící dokumenty úřadu
    1. Spisový řád

    2. Spisový plán
    3. Informační koncepce úřadu
- Dokumentace k elektronickému systému spisové služby
    1. Dokumentace k ESSL
    2. Dokumentace k integracím ESSL
    3. Dokumentace související s výkonem spisové služby

Další zdroje

V souvislosti s výkonem spisové služby existuje celá řada dalších zdrojů informací a metodických dokumentů zejména Ministerstva vnitra a Národního archivu ČR. V rámci Ministerstva vnitra je gestorem Odbor archivnictví a spisové služby (OAS).

Pohled na systém správy dokumentů



eSSL, Spisová služba, Funkční celek, spisovka