

PROLOG

Datové schránky a jejich dopad

Co jsou datové schránky?



- Datová schránka je krátkodobé úložiště datových zpráv, které ze zákona garantuje:
 - Ověřenou identitu odesílatele i příjemce
 - Doručení datové zprávy příjemci a vytvoření věrohodné doručenký
 - Aplikaci bezpečnostních mechanismů
 - Nastavitelná přístupová práva k datovým zprávám
 - Opatření datové zprávy časovými razítky
 - Auditní protokol o provedených operacích
- Uživatel má více možností přístupu ke své datové schránce
 - Přes webové rozhraní
 - Napojení schránky na informační systém uživatele

Co datové schránky nejsou?

- Systém datových schránek **není e-mail**
 - Nejedná se o univerzální komunikační nástroj (omezení na odesílatele a příjemce)
 - Datové zprávy se nešíří počítačovou sítí od odesílatele k příjemci
 - Technická realizace je odlišná od e-mailové infrastruktury
- Datová schránka **není trvalé úložiště**
 - Přijatou datovou zprávu ponechává systém datových schránek dostupnou jen na určitou dobu (řádově kratší než je předepsaná doba uchování dokumentu)
 - Systém poskytuje jen omezené nástroje pro manipulaci s datovými zprávami
 - Datové schránky neřeší organizaci datových zpráv

Předpověď blízké budoucnosti

- Označení jako „revoluce“ má své opodstatnění
 - Zavedením datových schránek se objem elektronické agendy skokově zvětší
 - Nejedná se o postupné zavádění, ale o přelomový krok
- Málokdo však ví, jaká úskalí projekt skrývá!
 - Není mnoho příležitostí studovat zkušenosti ze srovnatelných projektů
 - Nejsou k dispozici podrobné statistiky
 - Agendové procesy se budou muset přizpůsobit novým pravidlům
- Moment zahájení se neúprosně blíží
 - Času pro testování a ověřování nebude mnoho

Předpokládané důsledky zavedení datových schránek

- Změny ve stávajícím pracovním režimu
 - Nutnost přizpůsobit organizační procesy
 - Rozsáhlejší využívání digitálních podpisů
- Změna myšlení
 - Nahrazení po generace nezměněné formy dokumentů nejnovějšími technologiemi
- Technické změny
 - Stávající informační systémy bude nutné přizpůsobit

ČÁST 1

Elektronické dokumenty a záznamy

Elektronický dokument

- Obecná definice pojmu **dokument**:
„Artefakt zachycující informace reprezentované tak, aby je bylo možné předat dále.“
 - Informace uložená v definované podobě
 - Samotná data nejsou dokument – dokumenty jsou výstupem programů
- Cíl elektronických dokumentů: poskytovat podobné vlastnosti jako listinný dokument
- Nezávislost na nástrojích, pomocí nichž dokument vzniknul
 - Dokument obsahuje úplnou informaci (soběstačnost)
- Přidružená metadata
 - Údaje o dokumentu a okolnostech jeho vzniku

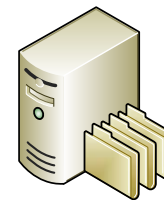
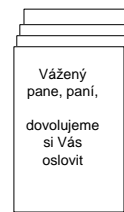
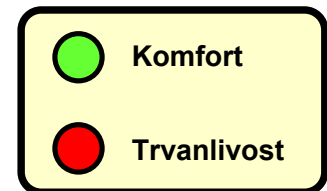
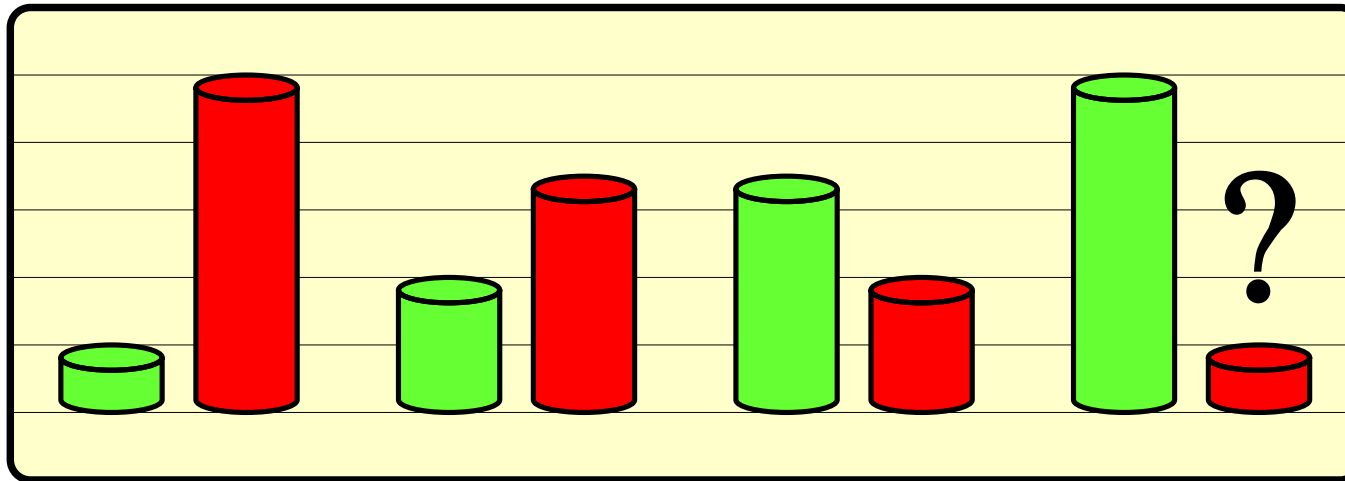
Pojmy Dokument a Záznam

- Definice pojmu **dokument** podle ČSN EN ISO 9000:2005:
„Informace a jejich podpůrné médium.“
 - Živý obsah, může se měnit
- Definice pojmu **záznam** podle téže normy:
„Dokument, v němž jsou uvedeny výsledky nebo v němž se poskytují důkazy o provedených činnostech.“
 - Neměnné svědectví:
 - o obchodní transakci nebo právním závazku
 - o akci, události nebo jiných skutečnostech
 - Záznam se vždy odkazuje na minulost
- Velmi často se mezi pojmy dokument a záznam nerozlišuje!
 - Záznam je jen určitým typem dokumentu

Výhody elektronických dokumentů

- Vyšší komfort
 - Moderní prostředky pro pořizování dokumentů
 - Rychlejší zpracování
 - Snadná katalogizace, správa obsahu, hledání v dokumentech
- Lepší spolupráce
 - Více pracovníků může pracovat na jednom dokumentu
 - Sledování vývoje dokumentu v čase a možnost návratu ke starší verzi
- Nižší náklady
 - Šíření elektronických dokumentů je levné a rychlé
 - I velké množství dokumentů zabírá zanedbatelný prostor

Avšak...



Nevýhody elektronických dokumentů

- Poprvé v historii nestačí k přečtení dokumentu pouze lidské smysly
 - Závislost na mnoha druzích technologií současně
 - Morální stárnutí medií, dokumentových formátů atd. má vliv na čitelnost
- Elektronické dokumenty jsou choulostivé
 - Seběmenší poškození (změna jediného bitu) může znehodnotit celý dokument
- Pojmy „originál“ a „kopie“ ztrácejí význam
 - Originál i duplikáty mají totožné vlastnosti
 - Přenosové medium není s dokumentem fyzicky svázáno

Rizika elektronických záznamů

- Jiné druhy hrozeb oproti listinným záznamům
- Bezpečnost
 - Jen obtížně lze řídit pohyb dokumentů a zabránit jejich duplikaci
 - Zabezpečení je založeno na velmi komplikovaných matematických postupech
 - Zranitelná místa se mohou objevovat i po dlouhé době
- Důvěryhodnost nástrojů
 - Člověk pracuje s (obvykle) vizuální reprezentací informací
 - Skutečná strojová podoba uložené informace: 10011101001111011100100001...
 - Skutečně člověk podepsal to, co chtěl?

O co přijdeme při ztrátě elektronického záznamu?

- Různé druhy hodnot:
 - Právní
 - Ekonomická
 - Administrativní
 - Historická
- Odpovídající následky ztráty záznamu
 - Zpochybnitelnost právních úkonů
 - Správní nebo trestní postih
 - Finanční ztráty
 - Narušení chodu instituce

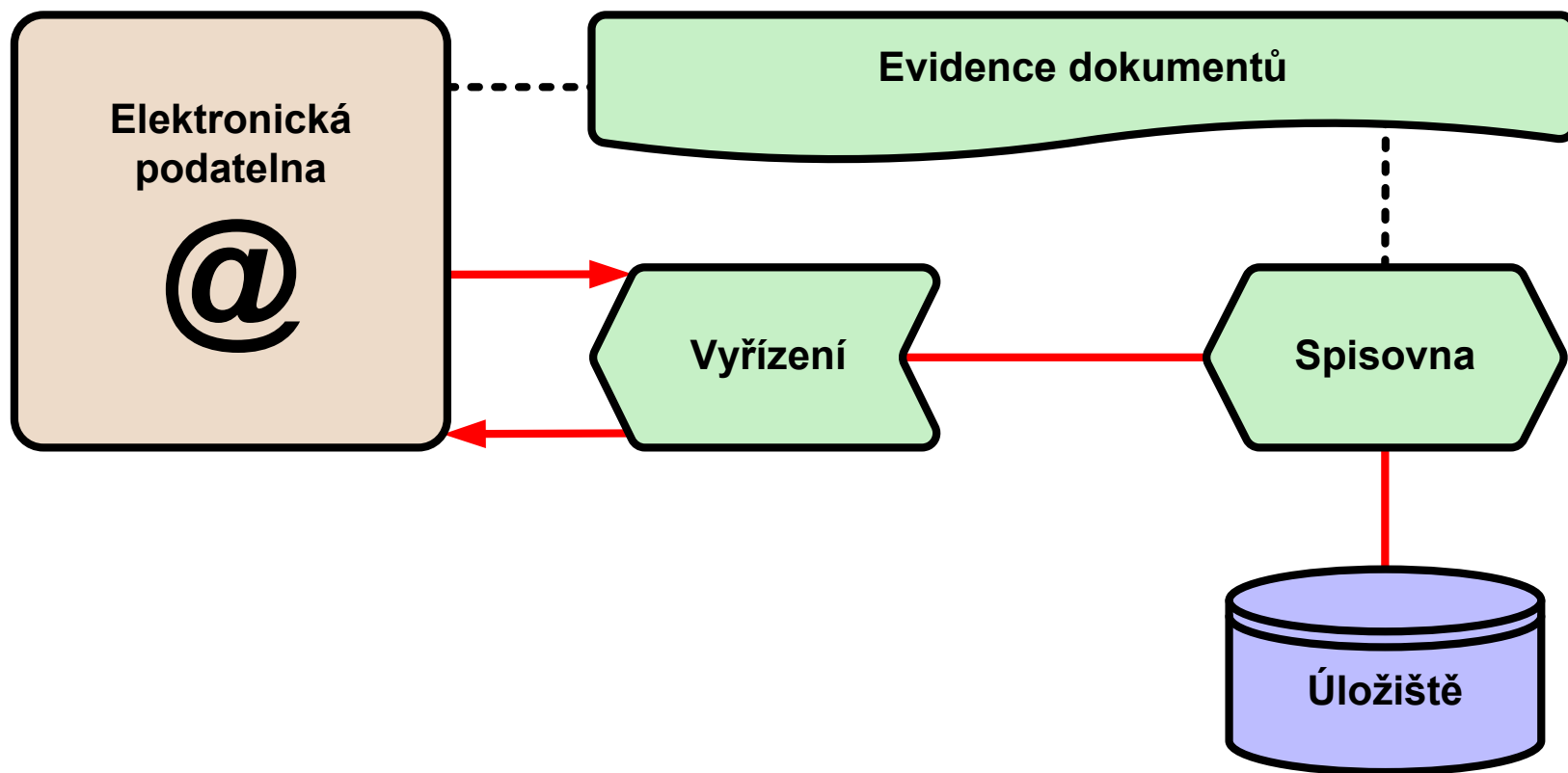
ČÁST 2

Digitalizace agend

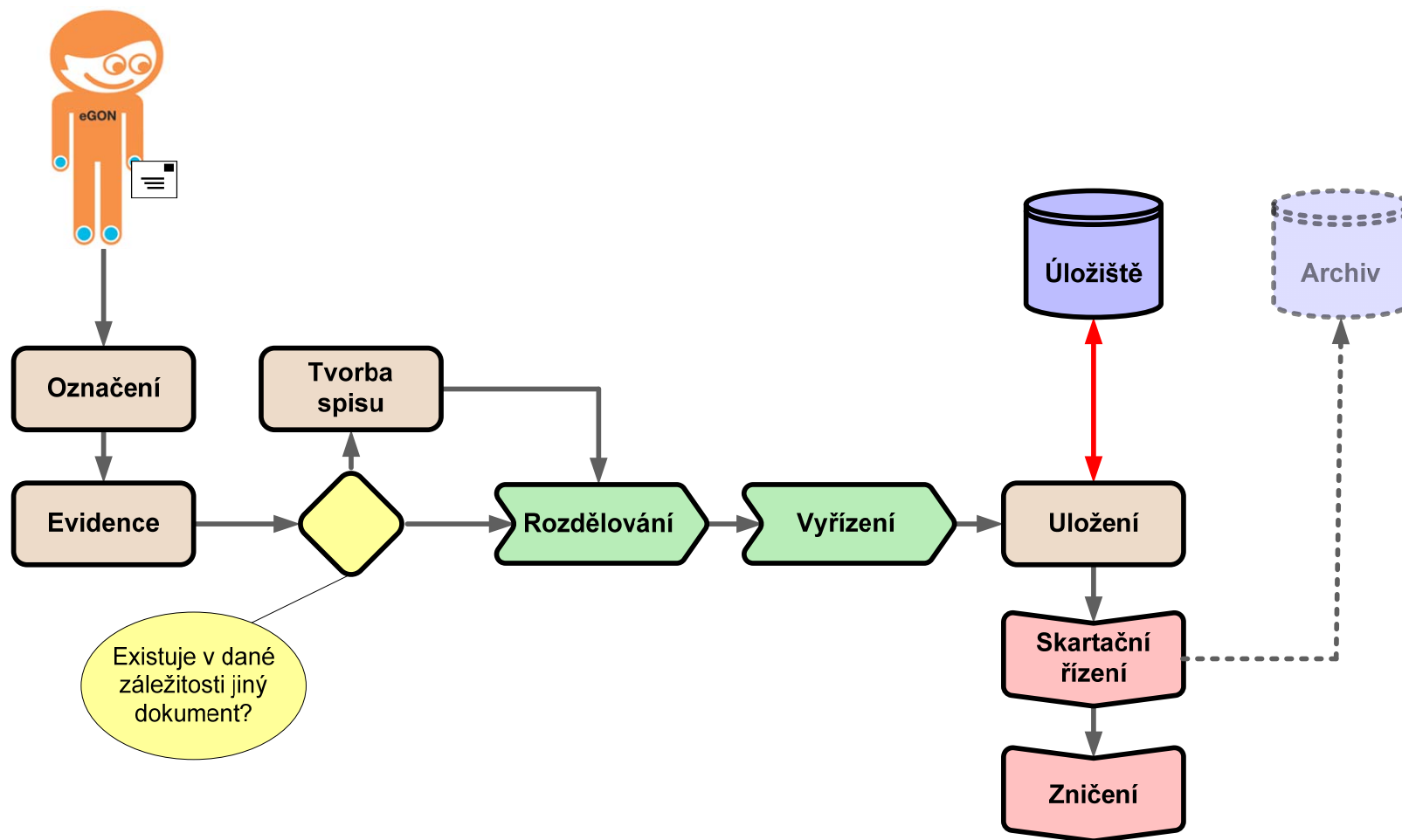
Nárůst objemu elektronických dokumentů

- Instituce budou v blízké budoucnosti pracovat s kvanty dokumentů, k nimž nebude existovat papírová verze
 - Podle druhu instituce může jít i o desetitisíce dokumentů ročně!
- S těmito nehmotnými dokumenty však bude potřeba nakládat podle zákona
 - Evidovat pohyb dokumentů a začleňovat dokumenty do spisů
 - Ukládat dokumenty po stanovenou dobu
 - Zajistit neměnnost a prokazatelnost pravosti dokumentů
- Aby instituce dosáhly souladu se zákonem, měly by provozovat elektronickou spisovou službu
 - Novela zákona o archivnictví a spisové službě
 - Vyhláška o podrobnostech výkonu spisové služby

Zjednodušený pohled na spisovou službu



Životní cyklus dokumentu ve spisové službě



Řízení životního cyklu informací

- Information Lifecycle Management
 - Zahrnuje předpisy, procesy, postupy a nástroje, na jejichž základě se informace pohybuje v prostředí IT infrastruktury, aby bylo dosaženo rovnováhy mezi obchodní hodnotou informace a využitými technologiemi.
- Pět typických fází životního cyklu
 - Tvorba informace / Příjem informace
 - Šíření informace
 - **Vyřizování**
 - Správa (evidence, zakládání spisů...)
 - **Uložení**

Fáze vyřizování

- Obsah dokumentů se může často měnit
- K obsahu se přistupuje relativně často
 - Modelová situace pro nástroje ECM (podniková správa obsahu)
- Dokumenty jsou ukládány:
 - průběžně (v různých verzích)
 - krátkodobě
 - do ad hoc úložišť
 - lokální disky pracovních stanic
 - diskové svazky lokální sítě
 - systémy pro správu obsahu
 - **centrální úložiště dokumentů**

ČÁST 3

Důvěryhodné úložiště

Důvěryhodné úložiště

- Důležitý prvek elektronické spisové služby
- Novela zákona o archivnictví a spisové službě, § 69a:
*„Uchovávání dokumentu v digitální podobě provádí určený původce postupem zaručujícím **věrohodnost** původu dokumentu, **neporušitelnost** jeho obsahu a **čitelnost** dokumentu, a to včetně údajů prokazujících existenci dokumentu v digitální podobě v čase. Tyto vlastnosti musí být zachovány po dobu skartační lhůty dokumentu.“*

Základní vlastnosti důvěryhodného úložiště

- Ukládá dokumenty spolu s metadaty
- Poskytuje mechanismy pro organizaci obsahu
 - Rozdělení na samostatná virtuální úložiště
 - Tvorba spisu (provázání dokumentů pomocí metadat)
- Ručí za důvěryhodnost dat
- Zajišťuje řízení přístupu k uloženým informacím
 - V případě elektronických záznamů zajišťuje jejich neměnnost
- Garantuje čitelnost dat

Požadavek 3: Nepopiratelnost existence

- Pomocí metadat musí být prokazatelné:
 - kdy byl dokument vložen do úložiště
 - že se od té doby nezměnil jeho obsah
- Dostupné nástroje:
 - Zákon 227/2000 Sb. o elektronickém podpisu – mechanismy asymetrické kryptografie
 - Digitální podpis
 - Časové razítko

Požadavek 4: Garance čitelnosti

- Dokument musí být po dobu své platnosti k dispozici v čitelné podobě
- Dostupnost úložiště
 - Monitorování a prosazování SLA
 - Záložní datové centrum
 - Plány obnovy v případě havárie
 - Plány periodické obnovy technického vybavení
- Využití předepsaných formátů
 - Soulad s mezinárodními normami a standardy
 - Velmi dlouhé skartační lhůty: formátová migrace

Požadavek 5: Bezpečnost

- Počítačová bezpečnost
 - Řízení přístupu k informacím
 - Protokolování a audit prováděných operací
 - Prokazatelné zničení odstraněných dokumentů
- Fyzická bezpečnost
 - Zabezpečení datových center
 - Ostraha

Problémy s důvěryhodným úložištěm

- Problém č. 1: **vysoké náklady**
 - Náklady na vybudování důvěryhodného úložiště jsou velmi vysoké
 - Geograficky oddělená datová centra
 - Výkonné technologické zázemí
 - Náklady na provoz nejsou přímo úměrné počtu uložených dokumentů
 - Dodržování SLA
 - Vyškolený personál
 - Postupné nahrazování zastarávajících technologií
- Problém č. 2: **dlouhodobost provozu**
 - Stabilita poskytovatele služeb úložiště
 - Fyzické opotřebení technických prostředků
 - Morální zastarávání datových formátů

ČÁST 4

Outsourcing důvěryhodného úložiště:
Iron-Secure Shared Services

Iron-Secure Shared Services

▪ Iron-Secure

- Ověřené řešení, vysoká úroveň znalosti návrhu a provozu prostředí s vysokou dostupností
- Atest počítačové i fyzické bezpečnosti
- Důsledné využití technik asymetrické kryptografie
- Jednotná metodika, jednotná bezpečnost

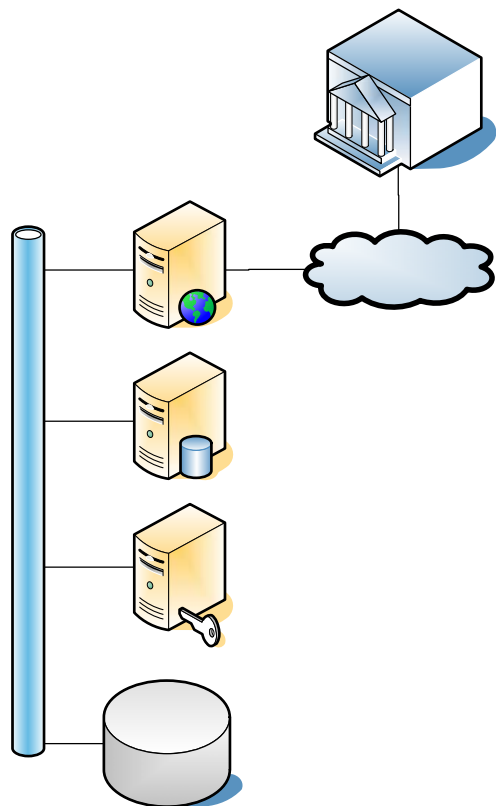
▪ Shared

- Sdílené zabezpečené prostředí pro aplikační systémy pracující s uloženým obsahem a obsah vytvářející

▪ Services

- Zabezpečení parametrů příslušných služeb s kontrolou SLA

Konceptuální struktura ISSS



- Integrační vrstva
 - Poskytuje rozhraní k úložišti ve formě webových služeb
- Vrstva služeb úložiště
 - Provádí vnitřní aplikační logiku důvěryhodného úložiště
- Bezpečnostní vrstva
 - Ověřuje platnost bezpečnostních prvků
 - Řídí přístup k uloženým datům
- Fyzické úložiště
 - Technologická vrstva

Principy řešení ISSS

- ISSS jako služba v prostředí SOA
 - Outsourcing služeb ISSS
 - Dodavatel služby zajišťuje provoz, bezpečnost, dostupnost, rozvoj
 - Snadná integrace do prostředí státní správy
 - Rozhraní webových služeb vyhovuje právním předpisům a technologickým normám
 - Standard EU: **MoReq2**
 - Modul pro elektronické spisovny – důvěryhodné úložiště má přesně definovanou funkci a rozhraní
- Pomoc obcím a krajům
 - Vybudování datového centra pro důvěryhodné úložiště je náročné
 - Využívat outsourcing lze dočasně i dlouhodobě

Výhody řešení ISSS

2/3

- **Převoditelnost**
 - Snadná hromadná migrace dokumentů do systému zpracování
 - Aplikační nezávislost
- **Rozšiřitelnost**
 - Nad důvěryhodným úložištěm lze provozovat nadstavbové služby
 - Možnost napojení na různé informační systémy pracující s dokumenty
- **Akreditovatelnost**
 - Dodavatel a poskytovatel služby disponují relevantními certifikacemi
- **Vyspělost dodavatele a poskytovatele**
 - Kvalitní technické i lidské zdroje
 - Zkušenosti s outsourcingem velkého rozsahu

Výhody řešení ISSS

3/3

- **Integrovatelnost**
 - Principy architektury orientované na služby
- **Ekonomická výhodnost**
 - Optimalizace nákladů na dokument
 - Optimalizace nákladů na provoz
- **Časová proveditelnost**
 - Zdrojově i časově zabezpečitelné krátké lhůty realizace a implementace
 - Řešení založeno na dostupných špičkových technologiích a metodikách

Děkuji za pozornost.