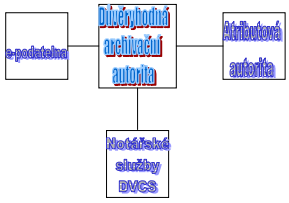
VSAĎTE NA
PARTNERSTVÍ

Důvěryhodná archivační autorita

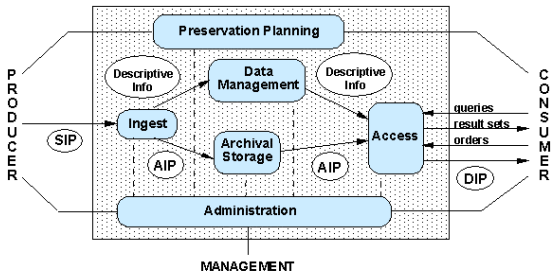
Ing. Jaroslav Pinkava, CSc,

PVT, a. s.
Kovanecká 30/2124, 190 00 Praha 9
tel.: 266 198 111, fax: 284 829 340
e-mail: sales@pvt.cz, web: www.pvt.cz

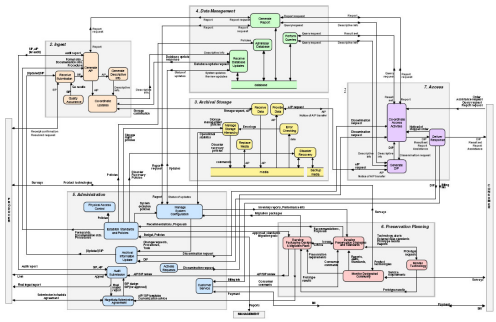
- **Důvěryhodná archivační autorita :**
- **Dva základní aspekty:** digitální archiv
- bezpečnost (krátkodobá, dlouhodobá)



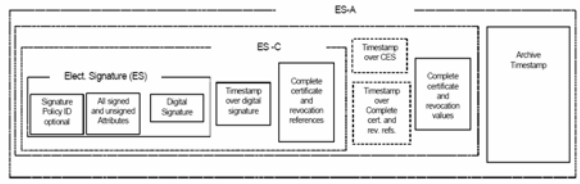
Model funkčních komponent OAIS



Source: Procedures Manual for the Consultative Committee for Space Data Systems (2001)



- Elektronické podpisy, časová razítka,
- ETSI formáty pro dlouhodobé podpisy (BES, EPES, ES-T, ES-C)



- XML podpisy (ETSI 101 903)
- Itans, zřetězené hashe, ERS

- Legislativa, přístupy
- Zákon o archivnictví - vyhláška spisová služba
- vyhláška o archivaci
- smysl legislativního uspořádání (i ele.podpis bez zákona by šlo použít u soudu jako důkaz (ale cena znaleckého posudku, obtížnost dokazování, ochoty soudu se takovýmto dokazováním zabývat).
- akreditace archivační autority - zatím je třeba k tomu vytvořit základy
- (podmínky na podpisový klíč ArchA, bezpečnost informačních systémů,…
- migrace formátů
- vyhláška k časovým razítkům

- Normy
- OAIS (Reference Model for an Open Archival Information System (OAIS) , **který byl vydán jako BLUE BOOK CCSDS 650.0-B-1, January 2002 a v roce 2003 jako norma ISO 14721:2003)**
- ETSI TS 101 733, V.1.5.1, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- rfc.3126, Electronic Signature Formats for long term electronic signatures
- ETSI TS 101 903, v.2.0.2, XML ADvanced Electronic Signatures
- Dokumenty pracovní skupiny Itans (zatím ve formě draftů)
- Norma ISO pro časová razítka, ISO 18014 (má tři části)
- A jiné (bezpečnostní dokumentace, atd.)

- Digitální podpis v éře kvantových počítačů
- Buchmann et al. : Post-Quantum Signatures
- milníky: 1994 - Shorův algoritmus
- 2001 - Implementace na kvantovém počítači (7-qubit - NMR), Chuang et al.
- předpověď za 15-20 let budou kvantové počítače dostatečně velké, aby rozbily
- systémy digitálního podpisu používané v praxi
- RSA, DSA, ECDSA
- pokud do té doby nebudou standardizované algoritmy pro podpis, které odolají kvantovým počítačům - bude zle
- Matematické problémy, které kvantové počítače neumí řešit:
- NP-těžké problémy
- - nalezení nejkratšího vektoru v celočíselné mříži (shortest resp.closest vector problem -SVP resp. CVP) ….. LLL algoritmus, BKZ algoritmus (podpisová schémata Micciancio, NTRU)
- - teorie kódů…minimum weight problem -- je NP-úplný (CFS systém, kódy Goppa)
- - kombinatorická teorie grup: uzlíčkové grupy (signature based on so called conjugacy problem)
- -kvadratické systémy s více proměnnými (soustava rovnic 2.stupně, obecný MQ problém je Np-úplný) - SFLASH (součást aktivity NESSIE)
- -Merklovo schéma (využití hashovacích funkcí)
- -Okamoto - kvantový počítač generuje klíč
- Hledáme podpisové algoritmy s pokud možno co nejkratšími klíči, dostatečně bezpečné a také s širokým spektrem použitelnosti.