PONDĚLÍ 31. LEDNA 2012, 9.00 – 16.00 HOD.

Co vám ve škole neřekli a v zákonech nenajdete: bezpečná implementace elektronických podpisů v praxi

- Úvod
  - šifrování a podepisování
  - modelový příklad: objednávka a její potvrzení
  - desatero bezpečného návrhu
- Ideová východiska
  - prokazatelně správný systém
  - Data pod kontrolou uživatele
- Existující standardy
  - kryptografická primitiva (SHA, RSA, AES)
  - PKCS#7, S/MIME, podpis PDF
- Právní aspekty
  - orgány veřejné moci, ZoEP, VoEP
  - soukromé subjekty
- Certifikační autority
  - jak vytvořit certifikační autoritu a proč to nedělat
  - akreditované a kvalifikované CA podle ZoEP
  - ostatní komerční CA
  - Self-signed certifikáty
- Změny klíčů
  - proč certifikáty časem vyprší
  - jak zařídit práci s návaznými certifikáty
  - verzování klíčů
  - trvalá udržitelnost
- Časová razítka
  - proč se bez nich neobejdeme
  - jak za ně neplatit (příliš)
- Papírování
  - neopisujte, čemu nerozumíte
  - jak napsat funkční smlouvu a podmínky
  - dokumentace pro nezávislého ověřovatele
- Nebuďte na to sami
  - každý systém potřebuje oponenturu

MICHAL A. VALÁŠEK, HLAVNÍ SOFTWAROVÝ ARCHITEKT, ALTAIRIS, S.R.O., PRAHA

ÚTERÝ 1. ÚNORA 2012, 9.00 – 16.00 HOD.

Podepisování a ověřování elektronických podpisů na PDF dokumentech

S jakými druhy podpisů a razítek se lze setkat u PDF dokumentů?

- Viditelné, neviditelné, tisknutelné a netisknutelné podpisy
- Schvalující a certifikační podpisy
- Prázdné podpisy
- Ruční podpisy
- Podpisová a archivní časová razítka

Co je potřeba vědět o elektronických podpisech?

- Jaké jsou podmínky pro platnost a neplatnost podpisu?
- Co znamená, když výsledek ověření zní: nevím?
- Jak se pozná, zda je elektronický podpis kvalifikovaný nebo jen zaručený
- Jakou roli hraje faktor času? jakou roli hraje časové razítko?
- Jakou roli hrají revokační informace a jejich (ne)dostupnost
- Možnost vkládání revokačních informací do elektronických podpisů
- Koncepce dlouhodobých elektronických podpisů

Nastavení Adobe Readeru pro ověřování podpisů

- Volba úložiště důvěryhodných certifikátů
- Instalace certifikátů autorit
- Volba posuzovaného okamžiku
- Nastavení způsobu vyhodnocování revokačních informací

Praktické ověřování podpisů na PDF dokumentech – na příkladech

- Podpis, založený na již expirovaném certifikátu
- Podpis, založený na revokovaném certifikátu
- Podpis s vloženými revokačními informacemi

Nastavení Adobe Readeru pro podepisování

- Možnosti podepisování a připojování časových razítek v Adobe Readeru
- PDF dokumenty odemknuté pro změny v Adobe Readeru
- Volba úložiště a umístění soukromého klíče a certifikátů
- Nastavení autority časového razítka
- Vkládání revokačních informací
- Konkrétní příklady podepisování PDF dokumentů

RNDR. ING. JIŘÍ PETERKA, NEZÁVISLÝ PUBLICISTA, PRAHA