CZ.1.07/2.3.00/20.0148 NANOLABSYS
Mezinárodní spolupráce v oblasti „*in vivo*“ zobrazovacích technik
Laboratoř Metalomiky a Nanotechnologií

Vás zve seminář; Cíl 1; ID 247:

Fungování a aplikace elektronického podpisu

Petr Čapek, RNDr. Josef Růžička, Mgr. Michal Horák, Mgr. Ondřej Zítka, Ph.D., Prof. Ing. René Kizek, Ph.D.

Abstrakt

Elektronický podpis je nějaký kousek binárních dat, který lze připojit k dokumentu (například PDF dokumentu, emailu, či požadavku v internetovém bankovnictví). Nemá žádný speciální smysl, jen musí určitým způsobem odpovídat podepisující entitě a obsahu dokumentu. K vytvoření podpisu potřebujeme podpisový klíč. Ten má dvě části – soukromou a veřejnou. Ty lze vytvořit zároveň, ale jedna z druhé nelze spočítat (jinak než zkoušení všech možností, kterých je pro útok příliš). Pomocí soukromé části a dokumentu lze spočítat ona binární data. Pomocí veřejné části a dokumentu lze zkontrolovat, že se jedná o stejný dokument jako byl podepsán a že ona binární data byla vytvořena pomocí odpovídající soukromé části. Pokud tedy dokážeme udržet soukromou část v tajnosti a příjemci dáme naši veřejnou část, máme splněné první dva cíle. Třetí cíl je po technické stránce také jednoduchý, avšak v praxi mírně problematický. V reálném světě k tomu máme občanský průkaz vydaný státní mocí. Obdoba vydavatele občanských průkazů pro podpisové klíče je certifikační autorita. Taková certifikační autorita je entita, které všichni věří a znají její veřejnou část klíče. Tato certifikační autorita poté může vytvářet dokumenty, které obsahují jak veřejnou část něčího klíče, tak jeho identifikační údaje (jako jméno). Takový dokument poté podepíše a předá majiteli. Tomuto dokumentu se říká certifikát.

Středa 06. 08. 2014, od 14:00 – 15:30 h

Ústav chemie a biochemie – NANOLABSYS místnost, Laboratoř metalomiky a nanotechnologií, Zemědělská 1, 613 00 Brno

Kontakt: kizek@sci.muni.cz

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ