



Vás zve na workshop IT, Cíl 3; ID 249:

Elektronické podpisy certifikované autoritou informačního systému

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

Abstrakt

Pokud si chceme pořídit klíč a certifikát, záleží k čemu jej chceme používat. Vnitrofiremní komunikaci lze podepisovat certifikáty vydanými vedením firmy. Banky často vydávají certifikáty svým klientům, aby s nimi mohly bezpečně komunikovat. Pokud však chceme mít



certifikát pro běžné používání, musíme si najít nějakou obecně uznávanou autoritu. Pro komunikaci s úřady potřebujeme dokonce kvalifikovaný certifikát, které u nás vydávají tyto autority: První certifikační autorita (ICA), PostSignum (Česká pošta) a Eldentity.

Program workshopu :

1. Klíč a certifikát k dispozici programu, ve kterém chceme generovat podpisy (například emailový klient) a můžeme začít podepisovat dokumenty.

13:00 – 16:30 h





2. Bezpečnost

Samozřejmě je na místě se ptát, jak je tento způsob bezpečný. Přímé kryptografické útoky nejsou známy (například není znám jiný způsob zjištění soukromého klíče z veřejného, než vyzkoušet všechny možné soukromé klíče, což by dnešním počítačům zabralo čas v řádech tisíců až milionů let). To je rozhodně lepší, než u klasického podpisu, věrohodně napodobit něčí podpis je snazší.

16:30 – 18:30 h

Přestávka : 18:30 – 19:00 h

3. Alternativní přístupy

Entita, které věří úplně všichni, je poněkud problematická věc a obvykle nevzniká přirozeně (lze vytvořit například zákonem a všichni jí budou věřit prostě z povinnosti). Proto existují i jiné přístupy.

Kupříkladu systém PGP umožňuje mít veřejný klíč podepsaný více, než jedním soukromým. Každý se za vás může zaručit tím, že vám podepíše váš klíč – tím říká, že věří, že jste to vy. Pokud vám někdo bude tvrdit, že se jmenuje Franta a 5 vašich známých vám to svými podpisy potvrdí, pak mu to můžete docela dobře věřit. Pokud to potvrzují jen 2 vám neznámí lidé, pak je to již méně důvěryhodné.

19:00 – 20:30 h

4. Diskuse a závěr

20:30 – 21:00 h



Středa 03. 09. 2014, od 13:00 – 20:00 h

Ústav chemie a biochemie, Laboratoř metalomiky a nanotechnologií, NANOLABSYS

místnost, 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