SPS – praktická úloha 1.9.2010

Posaďte se za PC s Ubuntu.

- Vygenerujte privátní klíč a certifikát kořenové certifikační autority, která bude mít identická klientem čitelná metadata jako certifikační autorita Kořenová certifikační autorita 2 (CN=PostSignum Root QCA 2,O=Česká pošta, s.p. [IČ 47114983],C=CZ) (je povoleno, aby fingerprint byl jiný)
- Vygenerujte privátní klíč a certifikát podřízené certifikační autority, která bude míst identická klientem čitelná metadata jako certifikační autorita Podřízená certifikační autorita 2 (CN=PostSignum Qualified CA 2,O=Česká pošta, s.p. [IČ 47114983],C=CZ) (je povoleno, aby fingerprint byl jiný)
- Podepište podřízenou autoritou CSR, které vygenerujete s metadaty Vaší osoby (CN=Jméno Příjmení, O=FEL ČVUT,C=CZ)
- Odešlete mail sami sobě a ukažte, že po instalaci certifikátu kořenové certifikační autority mailový klient důvěřuje tomuto elektronickému podpisu
- Pro inspiraci použijte certifikáty ke stažení na adrese http://qca.postsignum.cz/www/authorities.php

Instrukce:

- můžete používat jakoukoliv nápovědu kromě živých bytostí (v místnosti či jinde). Jakmile bude zjištěno, že s někým konzultujete, bude to bráno jako disciplinární přestupek a ze zkoušky půjdete hodně smutní
- všechno co není zadáno a potřebujete, si vymyslete
- časový limit pro vypracování je 120 minut **včetně odevzdání**, poté získáváte 0 bodů, myslete na to že zkoušejících je omezený počet a neumí pracovat paralelně
- odevzdávat můžete jednou – zavoláte učitele, ten oboduje aktuální stav a uvolníte pracoviště dalším

Bodování:

- Nemáte nic z níže uvedeného - F
- Vygenerovali jste certifikát kořenové CA s CN=Česká pošta, s.p. (včetně diakritiky) – E
- Jste schopni touto autoritou cokoli podepsat – D
- Vygenerovali jste certifikát podřízené CA a podepsali ho klíčem kořenové CA – C
- Podepsali jste klíčem podřízené autority svůj certifikát, určený výhradně k digitálnímu podpisu – B
- Ukázali jste v mailovém klientovi podpis, o kterém si klient myslí, že je důvěryhodný – A