JAK NA INTERNET

Serverové certifikáty

KLÍČOVÁ SLOVA

certifikát, elektronický podpis, identifikace, identita, šifrování, zabezpečení

OTÁZKY K DISKUZI

1. V jakých případech je nezbytné, aby internetová komunikace byla šifrována?
2. Využíváte vy sami takové internetové služby, při kterých je nutné, aby komunikaci neodposlouchával někdo další? Které?
3. Co znamená, že webová stránka je certifikována?
4. Jak poznáte, že komunikace mezi vámi a webovou stránkou je šifrována, tedy že používá certifikát?
5. Jak poznáme neplatný certifikát?
6. Jak poznáte, že se za majitele webové stránky někdo podvodně nevydává?
7. Věděli byste, jak majitelé webových stránek můžou certifikát získat?
8. Znáte nějaké konkrétní druhy certifikátů?
9. Co bychom měli udělat, pokud webové stránky, kam zadáváme citlivé údaje, nejsou certifikovány?

ÚKOLY

A) Zjistěte, jakou certifikační autoritou byly uděleny certifikáty všem provozovatelům šifrovaných webových stránek, které vy sami používáte. Udělejte ve třídě průzkum, která certifikační autorita je nejčastěji zastoupena.

B) Vyhledejte a popište jakým způsobem probíhá proces certifikace.

C) Vyhledejte a seznamte se s nejčastějšími chybami certifikátů a co tyto chyby znamenají.

DALŠÍ INFORMACE

Certifikační autorita. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-01-27]. Dostupné z: http://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita

Digitální certifikát. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-01-27]. Dostupné z: http://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t

Elektronický podpis. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2014 [cit. 2014-01-27]. Dostupné z: http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis

Klíč (kryptografie). In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-01-27]. Dostupné z: http://cs.wikipedia.org/wiki/%C5%A0ifrovac%C3%AD_kl%C3%AD%C4%8D

Podepisování klíčů. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2013 [cit. 2014-01-27]. Dostupné z: http://cs.wikipedia.org/wiki/Podepisov%C3%A1n%C3%AD_kl%C3%AD%C4%8D%C5%AF