Počítačové siete - Bezpečnostný certifikát :)

Elektronický dokument, ktorým sa preukazuje totožnosť jeho držiteľa. Obsahuje údaje o tom, pre koho a kedy bol vyhotovený, dokedy je platný, ktorá certifikačná autorita ho vydala a na aký účel.

Najslabším miestom kryptovanej komunikácie je bezpečnostný certifikát. Útočník, ktorý chce odpočúvať komunikáciu medzi používateľom a serverom, totiž potrebuje získať kľúč, ktorým bude celá komunikácia kryptovaná. Ten sa odosiela v prvých fázach komunikácie na základe overenia bezpečnostného certifikátu.

Mnohí používatelia predpokladajú, že každý certifikát je podpísaný, je správny a pre nich bezpečný. Neuvedomujú si, že certifikát mohla vydať aj útočníkova certifikačná autorita na úplne iné účely než ako je prezentované. Z tohto faktu vyplýva **potreba kontroly ako certifikátu a jeho vydavateľa, tak i jeho držiteľa**.

Šifrovaná komunikácia ↑

Elektronický podpis, odtlačok (hash), certifikačná autorita ↓

