Certificado digital

- Um certificado digital é um arquivo que contém a identidade de um indivíduo ou entidade e a sua chave pública.
- O certificado digital é emitido por uma entidade certificadora, a partir de uma rede de confiança (web of trust) descentralizada.

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Solicita conexão via SSL/TSL



Cliente



Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}



Servidor

Comunicação segura

SSL – Secure Socket Layer

TSL - Transport Layer Security

Solicita conexão via SSL/TSL

\ ←

Cliente

Retorna certificado digital com chave pública K_{pub} $E(K_{pub}, K_{sessão})$



Servidor



