Certificati e PKI
Esercizi con OpenSSL

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

http://www.dia.unisa.it/professori/ads

Aprile 2017

Esercizi

- Svolgere gli esercizi seguenti in collaborazione con un compagno di corso
- Utilizzare i file di configurazione forniti dal docente
  - **opensslCA.cnf** per quanto riguarda la *CA*
  - **opensslTSA.cnf** per quanto riguarda la *TSA*
  - **opensslUsr.cnf** per quanto riguarda un generico utente

Esercizi

- **Esercizio 1** Creare la propria CA
  - Directory e file
  - Certificato e chiavi
- **Esercizio 2** Generare una richiesta di certificato ed inviarla ad un compagno di corso
- **Esercizio 3** Visualizzare il contenuto della richiesta di certificato
- **Esercizio 4** Generare il certificato (certificato utente) relativo alla richiesta pervenuta
- **Esercizio 5** Visualizzare il contenuto del certificato
- **Esercizio 6** Convertire il certificato utente da formato PEM a formato DER

Esercizi

- **Esercizio 7** Visualizzare il contenuto del certificato codificato in formato DER
- **Esercizio 8** Verificare un certificato utente
- **Esercizio 9** Revocare un certificato utente
- **Esercizio 10** Generare una CRL che includa il certificato revocato
- **Esercizio 11** Visualizzare il contenuto della CRL
- **Esercizio 12** Esportare un certificato in formato PKCS #12