Information Systems Security

Exercise Set 2

In order to solve the following problems all technologies are allowed.

1. Prepare a practical example in a selected environment how secret keys are protected. Please send to the lecturer an e-mail with a selected environment (according to what has been agreed on the last classes).
   [2p]

2. Create a simple publicly available web site. Using Let's Encrypt service (`https://letsencrypt.org/`) obtain and install a certificate for the web site. Prepare a short instruction how you did it and send it by an e-mail to the lecturer.
   [3p]

3. Create your own CA and issue a certificate for a web site. Install that certificate and check how your favourite browser behaves. What can be done to make that certificate trusted?
   [3p]

4. Explain what is a self-signed certificate. Issue one and install for a web site. Check how your favourite browser behaves. What can be done to make that certificate trusted?
   [1p]

5. Explain what is certificate pinning and check the role of HPKP header. Prepare a small example to show how it works in practice.
   [1p]

Paweł Rajba