**University of Oslo**
**INF3510 Information Security**
**Spring 2010**
**Workshop Questions**

# *Lecture 3: Key Management and PKI*

## Question 1

a. Why is the management of cryptographic keys such an important issue?
b. Explain which keys need protection, and what they need to be protected against. How can this protection be provided?
c. Briefly list the main issues a key management system must deal with.

## Question 2

a. Draw the diagram showing the key states and transitions between them as described by NIST SP800-57. Explain the diagram.
b. When a key is active, it may be designated to protect only, process only, or both. Referring to the 19 key types described in NIST SP800-57, give two examples of key types that are designed to protect only, two examples of key types that are designed to process only, and two examples of key types that are designed to both protect and process.
c. Explain why key types 17, 18 and 19 are misnomers. Suggest better names for those key types.

## Question 3

Describe reasons why online services can benefit from public-key cryptography? Why is private key cryptography alone not suitable for online services?

## Question 4

a. Explain what is meant by the spoofing problem with respect to public-key cryptography.
b. Clearly explain how digital certificates can provide a solution to the spoofing problem.
c. How much trust can be placed in a digital certificate? Justify your answer.
d. Is a digital signature the same as a digital certificate? Justify your answer.

## Question 5

a. Briefly describe the primary purpose of a public key infrastructure.
b. Describe and contrast the function of each of the following basic components in a PKI system:
- Certification authorities (CA)
- Registration authorities (RA)

## Question 6

a. Distinguish the features of the hierarchical and user-centric PKI models.
b. Outline the relative advantages and disadvantages of these two models.

## Question 7

a. Describe the Browser PKI trust model.
b. List the advantages and disadvantages of this model.

## Question 8

You are here asked to investigate the digital certificate issued to UiO used for access to Fronter at the URL https://blyant.uio.no/. Using either Firefox, Internet Explorer or another other browser, go to that web site. Click on the padlock icon to obtain the certificate information, or if no padlock is visible follow the instructions below:

- MSIE; File → Properties → Certificate
- Firefox: Tools → Page Info → Security →Show certificate

and answer the following questions. You will need to view the details of the certificate to answer some of these.

a. What is the purpose of this certificate?
b. Who is the certificate issued to?
c. Who is the certificate issued by?
d. What is the validity period for this certificate?
e. Which X.509 certificate version is used?
f. Which cryptographic algorithm is used to sign the certificate?
g. What type of public key algorithm is certified, and what is the key size?
h. View the public key itself. Although the key is a 2048 bit RSA key, it appears as a series of digits 0-9 and characters A-F. Explain why the key appears in this format.
i. Look at the certification path (IE) or certificate hierarchy (Firefox).
    - Which Root CA appears at the top of the path?
    - View the Root CA certificate. How does it compare to the UiO certificate, especially with respect to the version numbers, validity period, key size, and signature algorithms used? The detailed values are not important here – the main thing is to get a feeling for what information is stored in the browser and observe the features of the browser PKI.

## Question 9

An alternative means for examining the stored root and intermediate certificates in your browser is via the browser menus. For example

- MS Internet Explorer, select: Tools → Internet Options → Content → Certificates → Root certificates, then you will be able to examine certificates installed in your browser.
- Firefox, select: Tools → Options → Advanced → Encryption → View Certificates

Look through certificates installed in your browser to determine the expiration dates.

a. Which certificates have short lifetimes?
b. Can you find certificates with expiration dates in excess of ten years from now?
c. Can you find certificates which have already expired? What happens when you view these certificates?

## Question 10

a. Why is it important to have a limited cryptoperiod for keys? Give at least four reasons.
b. What is the difference between protection and processing when using keys?
c. Compare the recommended cryptoperiod for private and public signature keys according to NIST SP800-57? Would you say that the validity period of root certificates in web browsers follow the recommendations of NIST SP800-57?