



## ***Lecture 3: Key Management and PKI***

### **Question 1**

- Why is good management of cryptographic keys such an important issue?
- Three main key categories are: i) symmetric secret keys, ii) asymmetric public keys and iii) asymmetric private keys. Explain which type of security services/protections (i.e. confidentiality, integrity and authenticity) that is/are required for each key category.
- Describe security mechanisms/methods that can be used to implement the required security service/protection for keys.
- Briefly list the main processes/steps of key management.

### **Question 2**

- Explain the diagram for key states and transitions between key states, as illustrated in NIST SP800-57, Figure 5, p.85.  
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>
- 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.
- Explain why key types 17, 18 and 19 are misnomers. Suggest better names for those key types.

### **Question 3**

- Why is it important to have a limited cryptoperiod for keys? Give at least four reasons.
- What is the difference between protection and processing when using keys?
- 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?
- Assuming practical QC by 2030, is the validity period of the root certificates meaningful?

### **Question 4**

- What is the spoofing problem with respect to public keys?
- Explain how digital certificates can provide a solution to the spoofing problem.
- Which are the conditions for having trust in a digital certificate? Justify your answer.
- Is a digital signature the same as a public-key certificate? Justify your answer.

### **Question 5**

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

### **Question 6**

Access to the stored root certificates in your browser(s) is via the browser menus. Look through root certificates installed in your browser to determine the expiration dates.

- a. What is the number of root certificates? Does this differ e.g. between Firefox and Chrome?
- b. Which certificates have short lifetimes?
- c. Can you find certificates with expiration dates in excess of ten years from now?
- d. Can you find certificates that have already expired? What happens when viewing them?

### **Question 7**

What is the difference between standard server certificate and EV server certificates?

### **Question 8**

- a. Why is certificate revocation necessary ?
- b. Which problem is solved with the “Must-Staple Protocol” ?

### **Question 9**

- a. Which problem is solved with CA Authorization and Certificate Transparency ?
- b. Where is the CA Authorization policy stored ?
- c. What must the domain owner do in order to make sure that its CA Authorization policy is followed?
- d. What must the domain owner do if it discovered that the CA Authorization policy has been breached?