Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

9. Exercise sheet
Hand in solutions until Monday, 29 June 2009.

Any claim needs a proof or argument.

Exercise 9.1 (PKI). (6 points)

Before Bob can communicate with Alice he needs her public key.

(i) So Alice sends her public key in plaintext over the internet to Bob. Should Bob now use and trust it? Argue. [1]

(ii) Charlie has published his public key in various newspapers. You've got copies of two independent newspapers containing it. A comparison shows that Charlie's public key is identical in both copies. Should you now trust Charlie's signatures that you verify with his key? Argue. [2]

(iii) Explain how Charlie can convince Bob in a more elegant way that his public key is authentic. [2]

(iv) Explain an advantage of a hierarchic PKI. [1]

Exercise 9.2. (2 points)

(i) How does *Active Authentication* work? [1]

(ii) Where and how are the Active Authentication Keys generated? (If applicable refer to the procedure in Germany.) [1]

Exercise 9.3 (PKD). (3 points)

Gather the following information on the PKD of the ICAO.

(i) Who has access to the PKD and how are requests processed? [2]

(ii) Is it possible to access the root public keys of a country's CSCA? Why, do you think, is that so? Think political! [1]

Exercise 9.4 (PKI threats). (5 points)

(i) Concerning the Key Management, several threats are possible. Think about countermeasures for a denial of service attack. [1]

[1] (ii) How is the threat of copying the data on the card (cloning) dealt with in Passive and Active Authentication?

[1] (iii) How and when is the privacy of the card holder at risk? Which traces may be left behind?

[1] (iv) Concerning mathematical threats, take a look at the required Security Levels (bit lengths) in the face of Moore's law.

[1] (v) Though breaking a hash function may be considered hard, assume that collisions can be easily produced. How might this enable fraud?