Electronic passport and biometrics, winter 2006

MICHAEL NÜSKEN

7. Exercise sheet
Hand in solutions until Tuesday, 19 December, $12^{\underline{15}}$.

Exercise 7.1 (Key distribution inside Germany). (6 points)

Each state has its own country signing certification authority with a public key $\mathtt{KPu}_{\mathrm{CSCA}}$. This key is transmitted to, say Germany, by diplomatic means. (There might be some messenger with the key in its pocket actually travelling to Germany to hand it to the german CSCA.) This public key is needed in each interface device to check the validity of the corresponding passports.

(i) Find out how this information is distributed. 2

(ii) Discuss the security problems and their solution. 4

Exercise 7.2 (Repetition). (4+2 points)

Review the material that we have discussed in the course so far.

Devise a possible exam exercise. It should be interesting, be simple in the formulation, ask a little knowledge about the subject, require some understanding of the chosen subtopic, enable the responder to show background knowledge, and with some cleverness the last bit should be obtainable. Nevertheless, it should not be too complicated or lenghty to answer. 4 +2

Exercise 7.3 (Exam date). (0 points)

The exam should take place between 26 February and 6 April 2007. Suggest a date. 0