# Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

## 4. Exercise sheet
## Hand in solutions until Monday, 5 May 2014, 13:00

**Exercise 4.1** (X.509). (8 points)

Read RFC 5280 and answer the following questions:

(i) What classes of certificates are there? 2

(ii) What is the basic syntax of X.509 v3 certificates? Describe the `Certificate Fields` in detail. Which signature algorithms are supported? 2

(iii) What is a trust anchor? Can one use different trust anchors? 2

(iv) What conditions are satisfied by a prospective certification path in the path validation process? 2

**Exercise 4.2** (Security notion for a public key infrastructure). (0+16 points)

We have sketched a public key infrastructure in the course. (Actually, ignoring revocation...) +16

(i) Formulate a meaningful security notion: What are task, means and limitations for the attacker?

(ii) Argue that the vulnerabilites described in the course are covered by that definition as limitation or consequence of the security notion.