The art of cryptography, summer 2016

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Monday, 30 May 2016, 11:59

Exercise 6.1 (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 6.2 (DNSSEC KSK Rollover). (0+8 points)

Read http://www.heise.de/netze/meldung/DNSSEC-Verfahren-fuer-Schluesseltausch-in-der-Rootzone-festgelegt-3208629.html and summarize. (First hand information can be found at https://www.icann.org/resources/pages/ksk-rollover.) +8

In particular: What is the problem? What is the purpose of DNSSEC and its root-key? Why is it so complicated to exchange it? Which consequences could a manipulation have?