The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

9. Exercise sheet
Hand in solutions until Monday, 23 June 2008.

Exercise 9.1 (Question). (3 points)

Prepare a question that you'd like to ask Sven Marx (gematik) at the ISEB-workshop in Bochum on 25 June. 3

Exercise 9.2 (Proactive processes). (4 points)

For many things it is vital that we can react fast. To allow that we need contingency plans which also need to be tested beforehand. In particular one wants to meet the following requirement: The time to setup a successful attack should be larger than the time to detect and counteract the attack. Do some research on different intrusion detection systems. Describe shortly the various attempts for intrusion detection. Include also the aspects necessary for the electronic health card and decide which types of such systems are suitable. Why is intrusion prevention in general *not* sufficient? 4

Exercise 9.3 (Advanced vs. Qualified Signatures). (2 points)

Look up which requirements an advanced electronic signature (following the German law SigG or the directive 1999/93/EG of the european union) has to fullfil. Descibe the difference between an advanced signature and a qualified signature following the 2

Exercise 9.4 (Full scale protocol). (6 points)

Devise a protocol that 6

- ○ authenticates both partners,
- ○ establishes a common secret,
- ○ and exchanges data.

Consider its security.

Exercise 9.5 (RFC2119). (0+1 points)

Knowing how to write correctly is essential when you want to write your own RFC. Contact RFC2119 and define the words `MUST`, `SHOULD` and `MAY`. Describe the differences of the three words. $\boxed{+1}$