Esecurity: secure internet & e-passports, summer 2014
Michael Nüsken

12. Exercise sheet
Hand in solutions until Monday, 7 July 2014, 13:00

Exercise 12.1 (Primary biometric identifier).   (4 points)

In the lecture we discussed "Why ICAO selected the face as primary biometric | 4 |
identifier specified to epassports". Consider the voice of a person as biometric
identifier and comment whether the arguments for the ICAO's decision still
hold or not.

Exercise 12.2 (Restricted Identification).   (10 points)

  (i) Show that Passive Authentication provides a unique identifier to the ter- | 2 |
      minal.

 (ii) Show that Chip Authentication provides a unique identifier to the termi- | 2 |
      nal.

(iii) Without this authentication the terminal cannot trust the chip. How does | 6 |
      Restricted Identification work? In other words: how is guaranteed that
      the remote terminal does only get the sector identifier and no unique
      identifier whatsoever.