10. Exercise sheet
Hand in solutions until Monday, 24 July 2017, 09:00

Exercise 10.1 (Doc 9303). (6+3 points)
To answer the following questions consult Doc 9303 and further reading, where required.

Imagine you work for a government, which wants to introduce the eMRTD. You are asked to decide which cryptographic scheme should be used in their Country Signing CA.

List all possible schemes. Which of them is the best? Why? Compare the runtime, the key size and the security of these schemes.

Exercise 10.2 (Security PACE). (8 points)
Find out details about proven security of PACE. (Pretend to report to your colleagues.)


Exercise 10.3 (Myths about e-Passports!?). (0+10 points)


(ii) Judge Myth # 11.

(iii) Verify the numbers in Myth # 33 and present them in bits. Are they reasonable? Why is —according to the author— the low entropy of the MRZ no threat?

(iv) Choose your two favorite myths (except # 11 and # 33) and find for each myth a source in which the myth is claimed to be true. Give a short summary of the source and why it is claimed to be only a myth. Judge the statements made by either sides.