Esecurity: secure internet & e-cash, summer 2015

MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Monday, 11 Mai 2015, 11:59

Exercise 5.1 (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 5.2 (Zero-Knowledge). (10 points)

Read Quisquater, Quisquater, Quisquater, Quisquater, Guillou, Guillou, Guillou, Guillou, Guillou, Guillou & Berson (1989) to one of your children. Alternatively take one of your fellow students.

(i) Write down the protocol in a form appropriate for computer science students rather than for children. 4

(ii) Prove for this protocol the following three properties: 6

- If the prover's claim is true, the verification returns true — always.
- If the prover's claim is false, the verification fails — with high probability.
- The verifier does not learn anything about the private information.

References

JEAN-JACQUES QUISQUATER, MYRIAM QUISQUATER, MURIEL QUISQUATER, MICHAËL QUISQUATER, LOUIS GUILLOU, MARIE ANNICK GUILLOU, GAÏD GUILLOU, ANNA GUILLOU, GWENDOLÉ GUILLOU, SOAZIG GUILLOU & TOM BERSON (1989). How to Explain Zero-Knowlegde Protocols to Your Children. In *Advances in Cryptology: Proceedings of CRYPTO 1989*, Santa Barbara, CA, number 435 in Lecture Notes in Computer Science, 628–631. Springer-Verlag. ISSN 0302-9743. URL `http://dx.doi.org/10.1007/0-387-34805-0_60`.