TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze
Prof. Anja Feldmann
Thomas Krenc, Felix Poloczek, Srivatsan Ravi and Philipp Schmidt

9th Assignment: Network Protocols and Architectures, WS 14/15

Question 1: $(10 + 10 + 10 + 0 = 30$ points) *The NSA (No Secrecy Afforded) Certificate Extension*

Read RFC 7169[1] and answer the following questions.

(a) Briefly outline the key ideas presented in the RFC.

(b) Describe the semantic difference between setting the boolean to i) TRUE, ii) FALSE, and iii) not using the extension.

(c) Discuss briefly how the usage of the extension fits within the server side deployment process for X.509 certificates. When is the right time to enable the extension? May there be any legal implications?

(d) Invent a crypographic primitive to automatically change the flag to TRUE in case the key has been compromised. Present your primitive and a *security proof* that the state of the flag can neither be forged by the legitimate key owner nor by any third party.

Due Date: Wednesday, January, 07th 2015 only until 14:00 h s. t.

- **As PDF files (no MS Office or OpenOffice files):** Uploaded via ISIS (`https://www.isis.tu-berlin.de/2.0/course/view.php?id=2560`)
- Put your name, StudentID number (Matrikelnummer) **and** the name of your tutor on your solution.

[1] `https://tools.ietf.org/html/rfc7169`