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

9. Blatt: Network Protocols and Architectures, WS 14/15

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

Lies den unten angefügten RFC 7169[1] und beantworte folgende Fragen.

(a) Fasse die Kernideen des RFC kurz zusammen.

(b) Beschreibe den semantischen Unterschied beim Setzen des Booleans zu i) TRUE und ii) FALSE, und iii) der Verwendung von Zertifikaten ohne diese Erweiterung.

(c) Diskutiere kurz, wie die Erweiterung in den Verteilungsprozess für X.509-Zertifikate auf Serverseite passt. Zu welchem Zeitpunkt sollte die Erweiterung in das Zertifikat aufgenommen werden? Gibt es dabei rechtliche Einschränkungen?

(d) Entwickle ein cryptographisches Verfahren, das sicherstellt, dass das Flag automatisch auf TRUE gesetzt wird, sobald der Schlüssel kompromittiert oder weiter gegeben wird. Stelle das Verfahren und einen *Sicherheitsbeweis*, dass das Flag weder vom wahren Eigentümer des Schlüssels, noch von Dritten manipuliert werden kann.

Abgabe bis Mittwoch, den 07. Januar 2015 nur bis 14:00 h s. t.

- **Als PDF-Dateien (keine MS-Office- oder OpenOffice-Dateien):** Mittels ISIS hochladen (`https://www.isis.tu-berlin.de/2.0/course/view.php?id=2560`)
- Gib auf deiner Lösung deinen Namen, deine Matrikelnummer **und** den Namen deines Tutors an.

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