Assignments on PKI

Your task is to write a summary of one standard from the collections available at

- https://datatracker.ietf.org/wg/pkix/,
- https://datatracker.ietf.org/wg/dane/,
- https://datatracker.ietf.org/wg/trans/,
- or any other RFC from one of the groups of the Security Area (sec, https://datatracker.ietf.org/wg/#sec) as explained in the lecture.

Your submission should summarize the RFC / Internet Draft, give some background on the topic (why do we care?), give a brief reasoning about the security of the suggested scheme / protocol, and discuss pros and cons – especially those related to security.

You must hand in your first and second preferred choice (signed and encrypted by mail to a.t.huelsing@tue.nl with the subject starting with "[AppliedCrypto]"; see, e.g., http://www.win.tue.nl/applied_crypto/2017/ for the public key)

before Thursday, November 30th, 23:59.

This is a strict deadline and I will not accept any late submissions! Whenever possible you will get one of your choices. The topic will be assigned to you till Monday, December 4th.

I only accept emails that are encrypted and signed; if you have trouble to set up PGP, please take a look at https://ssd.eff.org/.

You are asked to write a paper of at least 3, *at most* 5 pages of text using 11pt font. It is suggested to use the Springer LNCS style file from http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0, which will be mandatory for the second assignment. Graphics, protocol flow diagrams, other figures as well as tables and long item lists are subtracted from the length. Your paper should be on a reasonably high level, i.e., no very technical details (no ASN.1 please). You should focus on cryptographic and/or PKI aspects. Write your own text, from which it becomes clear that you understand the matter and that you can think, reason and write sensibly about it.

A note on copying, plagiarism and citing.

Copying text not written by yourself is not allowed (with the exception of *citing*, see below). This holds for text from the material to be studied, and also from other (web-)publications. This rule includes *plagiarism* (copying text written by somebody else while making it appear as if it is written by you), but is not limited to that, i.e., it is not allowed to copy substantial amounts of text from other sources, even when you do add proper referencing. You should write yourself.

Citing is a different matter, and is of course allowed, but should be used with caution, if used at all. Citing can be defined as: copying a small amount of text with proper referencing, that supports, and not replaces, your own text.

Providing proper references to all your sources is mandatory.

The paper will be judged on understandability, sensible argumentation, and also on readability. Adding your own well argued views, comments and criticism will be appreciated.

Deadline: **Sunday, December 17th, 23:59**.
Allowed languages: English.

Deliver your paper in electronic form by e-mail, signed and encrypted, to a.t.huelsing@tue.nl as a pdf document, again the subject line starting with "[AppliedCrypto]".