Report on cryptography

Task description

Your task is to write an analysis of the research paper provided in the task. The paper provides a description of a system for electronic resident identity card. Your task is to identify if the proposed system is worth considering for implementation in Estonia. Your analysis should contain clearly marked answer to the following questions:

- Does the system proposed in the paper satisfy all the stated system requirements (from Section 2.2). Provide a short explanation and reasoning for each requirement.
- Identify if there are additional inconsistencies in the system or in the system description.
- Provide conclusion, summarising if the system should be implemented as a real-life project.

You report should be **maximum 2 page long**, excluding title page, references and appendices (only typeset solutions are accepted). Your report should be well-formed containing clearly marked answers to the questions stated above. All the used sources and materials should be properly referenced. In case of plagiarism will be detected, the report will be graded with 0 points ans reported to the dean's office.

Grading

The maximum points for this task is 15. The evaluation criteria is the following:

- The report provides clear answers to stated questions (max 3 points)
- The report **correctly** identifies relevant cryptographic security problems (max 10 points). You get 0.7 points for each correct security problem identified, but no more than 10 points in total.
- The report has correct formatting, containing all the required references (max 2 points)

Cryptographic Security Problems include attacks that you can identify on the system, incorrect cryptographic primitives proposed to be used (counts as one security problem for each category of primitives – encryption, signing, key establishment), missing details or explanations for important parts of the protocol.