Thesis
Title: Digital Certificate Revocation for the Internet of Things
Author: Samuel Lindemer

Reviewing student
Simon Carlson, scarlso@kth.se

Overall assessment
The report is well structured, contains the necessary background information, and presents novel solutions to a real issue. The methods used are overall well explained and motivated, and the thesis can be used to support further development in the suggested areas.

Abstract
The abstract contains proper motivation and explanation of what has been done in the thesis. However, it mentions that one approach outperforms another under certain conditions, but I failed to find any mention of this or what the conditions are in the thesis. Furthermore, the abstract mentions a third approach that can reduce message sizes to a fraction of the original, but there is no mention of how large this reduction is in the results. Things mentioned in the abstract must be present in the report.

Introduction
The background is well written, properly motivates the problem area, and nicely delimits the thesis project. The research methodology section could be improved so that a reader better understands which methodologies were applied to produce the results. Using the word “analyzed” is too weak to understand this. How did the project plan to obtain the results? There is also no mention of ethics or sustainability.

Subject and problem area
The background chapter contains relevant information and introduces the reader to the concepts needed to understand the rest of the thesis. It is properly supported by references. Section 3.1 explaining the Window of Vulnerability looks like background as it is not something the thesis proposes, and should be in the background chapter instead of methods chapter. Otherwise it is easy to distinguish the works of the author from works of others.

Problem discussion and aim
A more elaborate discussion on why bloom filters were the data structure of choice would help support the work of the thesis. Cuckoo filters are briefly mentioned in the background, but then discarded without proper motivation. In addition, there should be some discussion about choice of data structure, which candidates were considered, and why bloom filters were picked. Restructuring the thesis so that the Fast Certificate Verification chapter becomes part of the method would make more sense. As of now, the two initial methods of the thesis are presented, then an experimental setup for, then comes a new chapter with yet another method. Moving that one section would make it much easier to get a grasp of the three distinct solutions. Otherwise the problem discussion is nicely presented, with three different approaches with their respective benefits and drawbacks presented.

Boundaries
The thesis justifies its delimitations well and follows them.

Disposition
Overall the disposition is well structured, with the exception of the placement of Chapter 4. It should be parts of the methods as it proposes the third solution developed by the thesis. The experimental setup should be presented at the end of the chapter, after presenting all the methods.

Method
The method is appropriate and properly presented. It would be nice with a motivation of why the method was picked above other methods in the introduction, as currently the motivation is a bit vague. Reorganizing the thesis as previously suggested would make the method even clearer.

Data collection
The data collection seems fair and accurate. The experimental setup is well described and makes the reader understand how the proposed solution of the thesis is evaluated. The certificates used in the experiment are presented in Appendix A, but for the experiment to be reproducible a description of how they were generated as well as where to find the source code should be included (assuming it is open source).

Results
The inclusion of Figure 15 might be redundant, as 1) the experiment set out to evaluate energy consumption and 2) execution time and energy consumption are directly correlated. Due to 2), figures 15 and 16 show basically the same results using different units. The analysis matches the contents of the report nicely.

Conclusions and discussion
The conclusions manage to answer the research question and provide insights as to what future work should focus on. However, the conclusions seem to only focus on proxied OCSP versus FCV, with no mention of CRL compression using bloom filters. Some conclusions about CRL compression and when it might be applicable helps motivate the inclusion of CRL compression in the thesis. Also, the abstract mentions that CRL compression can outperform OCSP under certain conditions but the discussion does not.

References
The references are valid and consistent, with the exception of two missing references. These have been pointed out in a hard-copy of the document given to the author.

Language and technical performance
The thesis is very well written with few grammatical errors. There are some inconsistencies with how acronyms are introduced and used, and possibly some acronyms are not needed as they are barely referenced. Inconsistencies and typos have also been pointed out in the hard-copy.