FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš, Ph.D.
Student:	Ladislav Marko
Thesis title:	Custom OpenSSL provider based on CNG
Branch / specialization:	Computer Security and Information technology
Created on:	5 June 2023

Evaluation criteria

1. Fulfillment of the assignment

▸ [1] **assignment fulfilled**
[2] assignment fulfilled with minor objections
[3] assignment fulfilled with major objections
[4] assignment not fulfilled

The assignment proved far more challenging than originally expected, mostly due to the rather poor documentation of OpenSSL in general and its providers concept in particular.

2. Main written part

80/100 (B)

For the most part, the written part contains the information that it should and is up to the requirements as to its technical state (despite minor grammatical errors). It does supplement the rather sparse OpenSSL documentation rather well, which is good. My only real complaint relates to section 3.6 which is too short and the examples provided don't quite work unless some specific undocumented circumstances are met (e.g. to actually establish a connection, the openssl s_client example needs a -CAfile argument, and the -cert argument is at least confusing if not incorrect).

3. Non-written part, attachments

85/100 (B)

The non-written part consists mainly of the code for the CNG provider itself. Its code is cleanly written and well documented. Some potential for errors remains, such as the use of malloc in places where calloc would be more suitable (e.g. cng_signature_newctx). I also noticed some issues that are outside of the scope of the thesis but would need to be fixed before the provider became practically usable (e.g. if the user has any smartcard-based certificate installed, the provider will ask for that smartcard to be inserted even if its certificate is not actually needed for the particular operation).

The main problem is that the materials provided make it difficult to actually demonstrate the provider created: The provider itself is made available in a binary form, but unfortunately in a debug build which has a dependency on the debug runtimes which are not available to most users. The demonstration client is not compiled at all and cannot be parametrized outside of changing the source code and rebuilding the application. It would also be nice if more than 512 bytes of the output were displayed. In effect, the reader has to expend a non-trivial amount of work before he or she can see the provider in action.

4. Evaluation of results, publication outputs and awards 90/100 (A)

I am a little on the fence here. The provider is not as-yet entirely ready for practical use, but at the same time it's main functionalities work and represent a really valuable additions to OpenSSL. The fact that we finally have a reasonably well documented provider that is able to complete a rather complex scenario is great for all users of OpenSSL, because even with its minor issues the provider can already act as a stepping block for future providers, even if it didn't evolve any further. But I am confident that it will evolve and add more functionalities.

5. Activity of the student

▸ [1] **excellent activity**

[2] very good activity

[3] average activity

[4] weaker, but still sufficient activity

[5] insufficient activity

6. Self-reliance of the student

▸ [1] **excellent self-reliance**

[2] very good self-reliance

[3] average self-reliance

[4] weaker, but still sufficient self-reliance

[5] insufficient self-reliance

The overall evaluation 95 /100 (A)

We knew from the beginning that the assignment would be difficult, but we didn't quite appreciate just how difficult it will prove. Still, the student persevered and eventually turned in a solution that solves all the required tasks. It may not be perfect in some minor aspects, but its core functionality is there and works as it should. The issues are minor and should be easy enough to fix since they mostly relate to documentation and testing. Considering the difficulty of the task, I am convinced the student deserves the grade of A-excellent.

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.