



Posudek oponenta závěrečné práce

Oponent práce: Ing. Jiří Buček, Ph.D.
Student: Ladislav Marko
Název práce: OpenSSL provider založený na CNG
Obor / specializace: Bezpečnost a informační technologie
Vytvořeno dne: 10. června 2023

Hodnotící kritéria

1. Splnění zadání

- ▶ [1] zadání splněno
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Zadání bylo splněno bez výhrad.

2. Písemná část práce

90 /100 (A)

Obsah práce je informačně bohatý, bez zbytečných částí. Věcná stránka je správná, bez chyb nebo nepřesností. Logická struktura je dobře navázána a text je srozumitelný. V práci bych uvítal podrobněji rozvedenou fázi návrhu včetně nějakého vhodného diagramu.

Použité zdroje jsou relevantní, citace jsou správné a převzaté prvky jsou jasně odlišeny. Použití softwaru a autorských děl je v souladu s licenčními podmínkami. Práce je psána čtivou angličtinou, nenalezl jsem žádné pravopisné ani stylistické chyby.

3. Nepísemná část, přílohy

98 /100 (A)

Přílohou jsou zdrojové kódy studentova providera odděleně od původního stromu zdrojových kódů projektu OpenSSL. Zdrojové kódy jsou přehledné a čitelné, funkce jsou přiměřeně komentované. Zdrojové kódy nejsou podepsané. Bylo by vhodné do každého souboru dát jméno autora.

4. Hodnocení výsledků, jejich využitelnost

100 /100 (A)

Využitelnost výsledků je vysoká, student publikoval svůj projekt na GitHub, a aktivně pracuje na jeho dalším vývoji a získává zpětnou vazbu od dalších uživatelů.

Celkové hodnocení

99 /100 (A)

Studentova práce je zdařilá, student prokázal schopnost samostatné tvůrčí práce a řešení nastalých problémů (nedostatečná dokumentace zejm. projektu OpenSSL), a vytvořil zdařilé dílo, které zveřejnil na serveru GitHub. Již získal zpětnou vazbu od prvních nezávislých uživatelů a také na ni reagoval. Přes některé lehčí nedostatky v písemné části práce hodnotím studentovu bakalářskou práci jako výbornou.

Otázky k obhajobě

V reakcích od uživatelů na GitHub jsem si všiml, že Váš kód má problémy s klíči z kryptosystémů eliptických křivek. Čím to je?

Instrukce

Splnění zadání

Posudte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posudte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posudte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.