



Hodnocení vedoucího závěrečné práce

Vedoucí práce: Mgr. Jan Starý, Ph.D.
Student: Ihor Salov
Název práce: Crypto pro FITCoin
Obor / specializace: Webové a softwarové inženýrství, zaměření Softwarové inženýrství
Vytvořeno dne: 27. srpna 2021

Hodnotící kritéria

1. Splnění zadání

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

Práce splňuje zadání, ale

2. Písemná část práce

70/100 (C)

V teoretickém úvodu (asymetrické klíče) jsou vynechány detaily, část 2.4 o digitálním podpisu v podstatě jen cituje vzorečky bez dalšího vysvětlení.

Rešerše crypto knihoven (kapitola 3) by mohla být důkladnější, kromě licence a hlavního API by stálo za to porovnat i samotnou implementaci, bezpečnostní historii, užitelnost a zdokumentovanost. Obligátní volba LibreSSL (jakožto forku OpenSSL) je v pořádku, ale mohla by být důkladněji zdůvodněná. Rovněž podstatné rozdíly mezi LibreSSL a OpenSSL se mlčky přejdou.

Kapitola 4 navrhuje přirozené rozšíření základních struktur o podpisy a jejich kontrolu, kapitola 5 pak jejich implementaci.

Kapitola 6 popisuje provedené testy.

Práce je psána česky, což není autorův rodný jazyk, obsahuje množství překlepů a gramatických prohřešků, ale čtení samotného obsahu to nebrání.

3. Nepísemná část, přílohy

70 /100 (C)

Hlavním výsledkem je implementace digitálního podpisu při platbách pomocí FITcoin. Tato implementace je prokazatelně funkční (otestováno). Po provedených změnách by bylo na místě upravit strukturu ještě dále, například když nyní vstup transakce obsahuje veřejný klíč, není nutné, aby obsahoval též jeho hash (jako dosud).

4. Hodnocení výsledků, jejich využitelnost

70 /100 (C)

Práce je přirozeným rozšířením projektu FITCoin, totiž vnáší do utrácení mincí samotné kryptografické ověřování původu.

5. Aktivita studenta

- [1] výborná aktivita
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- ▶ [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

6. Samostatnost studenta

- [1] výborná samostatnost
- [2] velmi dobrá samostatnost
- ▶ [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Celkové hodnocení

71 /100 (C)

Práce je implementační, proto se kloním spíše k vytvořenému softwaru než k nedostatkům písemné části, a práci hodnotím jako průměrnou.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posudte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posudte schopnost studenta samostatně tvůrčí práce.

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.