ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Design of a Key Management System Architecture for Quantum Key Distribution**
Jméno autora:	**Vojtěch Sobotka**
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra telekomunikační techniky
Oponent práce:	doc. Ing. Jiří Novák, Ph.D.
Pracoviště oponenta práce:	Katedra měření

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Vzhledem k rozsahu technologií, s nimiž se student musel v průběhu řešení BP práce podrobněji seznámit, pokládám zadání práce za nadprůměrně náročné.

Splnění zadání **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání bylo dle mého soudu splněno, implementace všech bodů zadání je v práci podrobně popsána. V některých případech (bod d zadání) je toho dosaženo specifickým způsobem – zde konkrétně využitím Swagger API exploreru.

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student nejprve analyzuje zadání a na základě analýzy navrhuje strukturu a volí komponenty a funkce systému. Následně student postupuje logicky, popisuje jednotlivé části komunikační infrastruktury a způsob řešení dílčích úkolů, jednotlivé kroky jsou dostatečně zdůvodněny. V závěru práce je pozornost upřena na testování jak jednotlivých komponent, tak i systému jako celku. Míra pokrytí implementace testy však evidentně není příliš vysoká, což lze akceptovat pouze s přihlédnutím k faktu, že se jedná spíše o studii proveditelnosti (*proof of concept*).

Odborná úroveň **B - velmi dobře**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

V úvodu práce trochu postrádám alespoň základní porovnání s obdobnými systémy, jejichž struktura a parametry byly publikovány. Tyto informace jsou k dispozici v citované literatuře, nicméně přímé srovnání by pro práci bylo přínosem. Z textu práce je zřejmé, že se student v řešené problematice velmi dobře orientuje, a to jak v aspektech bezpečnostních, tak i síťových. Student dle mého názoru správně zvolil architekturu mikroslužeb, tam, kde je to vhodné, používá strojové generování kódu dle YANG modelu, pozornost věnuje i bezpečnému uložení a mazání sdílených hesel. Ačkoliv aplikace samotná není velmi složitá, její funkční implementace v zadaném prostředí představuje kus dobře odvedené práce. Drobnou výhradu mám k použitým vývojovým prostředkům (JAVA) – pro aplikace tohoto typu by i z pohledu bezpečnosti byl vhodnější např. RUST nebo C/C++.

Formální a jazyková úroveň, rozsah práce **B - velmi dobře**
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.
Práce je správně strukturovaná, formální úroveň považuji za velmi dobrou. Je psána v anglickém jazyce s občasnými drobnými chybami a překlepy, které však nesnižují srozumitelnost textu. V obrázku 4.1 je chyba v popisu kvantové linky – omylem dvakrát uveden klíč **Z** namísto **Y**. Na straně 23 nahoře jsou pro sémanticky totožný prvek komunikačního modelu použity dva různé názvy („*QKD application ID*“ a „*QKD application session ID*“), což je matoucí.

Výběr zdrojů, korektnost citací **B - velmi dobře**
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.
Práce uvádí 21 relevantních zdrojů, které jsou v práci vhodně citovány. K výběru a způsobu jejich citací nemám výhrad kromě reference 13, kde chybí odkaz na zdroj.

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.
Jak z textu práce explicitně vyplývá, navržený a implementovaný systém jako celek funguje. Jelikož se jedná o první ověření koncepce řešení, lze určité drobné nedostatky, které by byly neakceptovatelné v produkční verzi, prominout.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Téma práce považuji za aktuální, student se jeho zpracování velmi dobře zhostil.

Prosím o zodpovězení následujících dotazů:

1. Proč jste se rozhodl využít pro řešení Javu? Nevnímáte toto rozhodnutí jako bezpečnostní riziko?
2. Vícečetné použití symbolu N v obrázku 5.1 je pravděpodobně minimálně matoucí. Pokud se jedná o počet důvěryhodných uzlů (*trusted node*) sítě, pak u počtu aplikací by měl být použit jiný symbol (nebude obecně shodný).
3. Jakým způsobem je implementována registrace důvěryhodného uzlu sítě u řadiče SDN? Jak je zajištěna bezpečnost jejich komunikace?
4. Pokud se nemýlím, je celý koncept omezen na generování a distribuci jednorázového klíče pro použití se symetrickou šifrou. Jak náročné by bylo rozšířit jej o kontinuální distribuci klíče určeného pro OTP (One Time Pad) šifrování?

Předloženou závěrečnou práci hodnotím přes drobné připomínky klasifikačním stupněm **B - velmi dobře.**

Datum: 10.6.2024 Podpis: Jiří Novák