

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Nástroj pro generování a ověřování zabezpečených emailů ve standardech S/MIME a PGP
Jméno autora:	Kirill Khakimov
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra telekomunikační techniky
Vedoucí práce:	Ing. Tomáš Vaněk, Ph.D.
Pracoviště vedoucího práce:	Katedra telekomunikační techniky

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání	náročnější
<i>Hodnocení náročnosti zadání závěrečné práce.</i>	
Práce vyžadovala jak teoretické znalosti v oblasti aplikované kryptografie (certifikáty X.509, protokoly S/MIME, PGP), tak schopnost analýzy cizího kódu, ale i návrh a implementaci nového řešení.	

Splnění zadání	splněno
<i>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.</i>	
Student splnil zadání práce. Vytvořený systém je funkční a použitelný pro potřeby výuky.	

Zvolený postup řešení	správný
<i>Posuďte, zda student zvolil správný postup nebo metody řešení.</i>	
Student pracoval na řešení velmi samostatně, nicméně bych uvítal častější konzultace v průběhu realizace výsledného produktu, aby se vyhnul dodatečnému předělávání.	

Odborná úroveň	A - výborně
<i>Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.</i>	
Odborná úroveň práce (část věnovaná technologiím certifikátům, protokolům S/MIME a PGP) je dobrá, student se v rámci své práce podrobně seznámil s principy asymetrické kryptografie a práce s knihovnou OpenSSL.	

Formální a jazyková úroveň, rozsah práce	C - dobře
<i>Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.</i>	
Jazyková úroveň je dobrá, k teoretické části také nemám připomínky, nicméně část věnovaná praktické realizaci systému je velmi stručná a určitě by mohla být podrobnější. Práce využívá L ^A T _E Xovou šablonu FEL, takže po této stránce je zpracování bez připomínek.	

Výběr zdrojů, korektnost citací	A - výborně
<i>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.</i>	
Student správně cituje používané zdroje.	

Další komentáře a hodnocení	
<i>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.</i>	

Výsledným dílem, které student odevzdal jsem byl příjemně překvapen, protože student byl schopen zanalyzovat nedokumentované stávající řešení kombinující bashové skripty, Perl a PHP a vytvořit moderní webovou aplikaci, která kromě reimplementace existující funkcionality přidala i schopnost generovat a automaticky verifikovat emailovou komunikaci zabezpečenou protokolem PGP (včetně např. získávání veřejných PGP klíčů z externích úložišť projektu OpenPGP). Škoda, že student nevěnoval větší úsilí také tomu, aby vše, co prakticky udělal, také patřičně popsal ve své bakalářské práci.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Student v rámci bakalářské práce analyzoval existující systém pro generování individuálních sem. prací, provedl návrh nového systému s výrazně rozšířenou funkcionalitou, který následně naimplementoval a odzkoušel. Dodaný systém je funkční a po malých úpravách (dokumentace a lepší konfigurovatelnost) bude moci být nasazen při výuce. Nad rámec zadání pak student vytvořil nástroj pro generování certifikátů umožňující generovat různým způsobem nevalidní certifikáty.

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

Datum: 31.5.2022

Podpis: