



## POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

**Jméno studenta:** Jan Brož

**Název práce:** Emulace čipové karty pomocí technologie NFC

**Autor posudku:** Tomáš Kozel

**Cíl práce:** Cílem práce je vytvoření nezávislého platebního systému, ve kterém bude mobilní telefon vystupovat v roli bezkontaktní platební karty. Pro autentizaci uživatele a přenos transakčních dat bude využito rozhraní NFC v režimu Host Card Emulation (HCE). V rámci zabezpečení aplikace bude navrženo a implementováno několik autentizačních mechanismů. Cílem je vybrat nejvhodnější variantu z hlediska bezpečnosti a pohodlí uživatele.

Povinná kritéria hodnocení práce	Stupeň hodnocení					
	A	B	C	D	E	F
Práce svým zaměřením odpovídá studovanému oboru	x					
Vymezení cíle a jeho naplnění	x					
Zpracování teoretických aspektů tématu	x					
Zpracování praktických aspektů tématu	x					
Adekvátnost použitých metod	x					
Hloubka a správnost provedené analýzy	x					
Práce s literaturou	x					
Logická stavba a členění práce	x					
Jazyková a terminologická úroveň	x					
Formální úprava a náležitosti práce	x					
Vlastní přínos studenta	x					
Využitelnost výsledků práce v teorii (praxi)	x					

### Díličí připomínky a náměty:

K práci mám pouze drobné připomínky:

- V poděkování se mluví o bakalářské práci a vedoucí práce, místo o vedoucím.
- V diagramech na s. 47 je částka transakce typu float, což není nejvhodnější reprezentace finančních částek díky malé přesnosti.
- Na s. 67 v tab. 3 je uváděna rychlost autentizace při využití symetrického a asymetrického šifrování, avšak v metodice měření chybí zmínka o počtu opakování měření a typu uváděné (střední hodnoty).

### Celkové posouzení práce a zdůvodnění výsledné známky:

Práce je věnována velmi zajímavé problematice emulace bezkontaktní platební karty pomocí čipu NFC mobilního telefonu. Student systematicky popisuje problematiku šifrování, zabezpečení přenosu i hardwarových technologií pro blízkou bezdrátovou komunikaci. Vše účelně kombinuje v prototypu platebního systému postaveného na technologiích, jako jsou NFC, Android, Spring apod. Ve všech částech prokazuje velmi dobrou orientaci v použitých technologiích, vhodně je kombinuje a vyhodnocuje a řeší bezpečnostní rizika jednotlivých řešení. Tím prokazuje schopnost integrovat poznatky z řady oblastí studia, potažmo ICT. Práce je zdařilá i po formální stránce, splňuje požadavky metodických pokynů i zadání práce.

**Otázky k obhajobě:**

1. Jak bylo prováděno měření rychlosti autentizace z hlediska statistického?
2. Jaké jsou možnosti praktického využití navrženého systému?

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: A**

**V Hradci Králové, dne 7. září 2016**

---

podpis