

Implementace podpory plateb novými digitálními prostředky

Bc. Tomáš Hanáček

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Bc. Tomáš Hanáček
Osobní číslo: A23310
Studijní program: N0613A140022 Informační technologie
Specializace: Softwarové inženýrství
Forma studia: Prezenční
Téma práce: Implementace podpory plateb novými digitálními prostředky
Téma práce anglicky: Implementation of Support for Payments with new Digital Currencies

Zásady pro vypracování

- Prostudujte současný ekosystém platebních karet a digitálních platebních prostředků založených na QR kódech.
- Popište klíčové rozdíly mezi transakcemi prováděnými platebními kartami a QR kódy.
- Navrhněte architekturu nové služby, která propojí stávající platební ekosystém s podporou digitálních plateb s QR kódy.
- Implementujte prototyp služby v jazyce Java pomocí frameworku Spring Boot.
- Proveďte analýzu a testování navrženého řešení a shrňte dosažené výsledky.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. V. K. Raina, *NFC payment systems and the New Era of transaction processing*. Hershey, PA: Business Science Reference, 2017. ISBN 9781522523079
2. S. Sharma, *Modern API Development with Spring and Spring Boot: Design highly scalable and maintainable APIs with REST, gRPC, GraphQL, and the reactive paradigm*. Birmingham, England: Packt Publishing, 2021. ISBN 9781800562875.
3. S. Sharma, *Mastering Microservices with Java: Build enterprise microservices with Spring Boot 2.0, Spring Cloud, and Angular, 3rd Edition*, 3rd ed. Birmingham, England: Packt Publishing, 2019. ISBN 9781789531251.
4. K. Indrasiri and D. Kuruppu, *Gprc: Up and running: Building cloud native applications with go and java for docker and kubernetes*. O'Reilly Media, 2020. ISBN 9781492058281.
5. J. Bloch, *Effective Java*, 3rd ed. Boston, MA: Addison-Wesley Educational, 2017. ISBN 0134685997.

Vedoucí diplomové práce: **Ing. Tomáš Dulík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **27. října 2024**
Termín odevzdání diplomové práce: **2. června 2025**



L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zabývá implementací podpory plateb novými digitálními prostředky, konkrétně pomocí QR kódů, do stávajícího platebního ekosystému využívajícího standardní platební karty. Hlavním cílem práce je analyzovat současné způsoby zpracování platebních transakcí, identifikovat klíčové rozdíly mezi transakcemi prováděnými platebními kartami a QR kódy a navrhnout architekturu služby, která umožní propojení těchto dvou platebních metod.

Praktická část práce se soustředí na vývoj prototypu služby QRPaymentService v jazyce Java s využitím frameworku Spring Boot. Tato služba bude fungovat jako zprostředkovatel mezi platebním ekosystémem pro platební karty a poskytovateli QR plateb. Součástí implementace je také úprava systému SmartSwitch společnosti Monet+ tak, aby umožňoval směrování autorizací transakcí skrze službu QRPaymentService.

V závěru práce je provedena analýza a testování navrženého řešení, které hodnotí jeho funkčnost, výkonnost a možnosti dalšího rozvoje. Výsledky ukazují, že integrace QR plateb do tradičního platebního systému je realizovatelná a přináší nové možnosti pro modernizaci platebních procesů.

Klíčová slova: QRPaymentService, QR kód, Java, Spring Boot, SmartSwitch, platební systém

ABSTRACT

This diploma thesis deals with the implementation of new digital payment method using QR codes into the existing ecosystem of standard payment cards. The main objective of the thesis is to analyze the current methods of processing payment transactions, identify key differences between transactions using payment cards and QR codes, and propose an architecture of service that will enable the use of these two payment methods.

The practical part of the thesis focuses on the development of a prototype of the QRPaymentService service in Java using the Spring Boot framework. This service will act as an intermediary between payment ecosystems for payment cards and QR payment providers. The implementation also includes modifications of the Monet+ SmartSwitch system to enable authorization routing via the QRPaymentService service.

At the end of the thesis, an analysis and testing of the proposed solution is performed, which evaluates its functionality, performance, and possibilities for further development. The results show that the integration of QR payments into the traditional payment system is feasible and brings new opportunities for the modernization of payment processes.

Keywords: QRPaymentService, QR code, Java, Spring Boot, SmartSwitch, payment system

Chtěl bych poděkovat Ing. Tomášovi Dulíkovi, Ph.D. za odborné vedení, vstřícnost při konzultacích a cenné rady při zpracování této práce.

OBSAH

ÚVOD.....	15
I TEORETICKÁ ČÁST	16
1 PLATEBNÍ KARTY	17
1.1 HISTORIE A VÝVOJ.....	17
1.2 TYPY PLATEBNÍCH KARET	18
1.2.1 Kreditní karty	19
1.2.2 Debetní karty	19
1.2.3 Charge karty	19
1.2.4 Předplacené karty	20
1.2.5 Virtuální karty	20
1.2.6 Co-brandované a partnerské karty	20
1.3 MECHANISMUS FUNGOVÁNÍ	20
1.3.1 Účastníci platebního procesu	21
1.3.2 Detailní průběh platební transakce	21
1.4 BEZPEČNOSTNÍ MECHANISMY	22
1.4.1 Fyzické zabezpečení platebních karet	22
1.4.2 Elektronická a síťová bezpečnost.....	22
1.4.3 Standardy bezpečnosti a compliance	23
1.5 POPLATKY A REGULACE	23
1.5.1 Poplatky spojené s platebními kartami	23
1.5.2 Regulace platebních karet	24
1.6 TRENDY V OBLASTI PLATEBNÍCH KARET	25
1.6.1 Umělá inteligence a bezpečnost plateb	25
1.6.2 Tokenizace a konec ručního zadávání údajů.....	26
1.6.3 Mobilní zařízení jako platební terminály	26
1.6.4 Virtuální karty pro B2B transakce	26
1.6.5 Blockchain a digitální aktiva.....	26
1.6.6 Inovativní design platebních karet	27
1.6.7 Udržitelnost a společenská odpovědnost	27
1.6.8 Evropská platební suverenita a digitální euro	28
2 DIGITÁLNÍ PLATEBNÍ PROSTŘEDKY ZALOŽENÉ NA QR KÓDECH	29
2.1 PRINCIP FUNGOVÁNÍ.....	29
2.2 HLAVNÍ POSKYTOVATELÉ	31
2.2.1 Alipay a WeChat Pay (Čína).....	32
2.2.2 Paytm a PhonePe (Indie).....	32
2.2.3 Apple Pay a Google Pay (globálně)	33
2.2.4 Revolut, Twint, Lydia a další evropské fintech platformy.....	33
2.2.5 Česká republika – QR Platba, ČSOB, Česká spořitelna a GoPay.....	34
2.3 BEZPEČNOSTNÍ ASPEKTY	34

2.3.1	Hlavní bezpečnostní hrozby	35
2.3.2	Ochranná opatření a osvědčené postupy	35
2.4	REGULACE A STANDARDIZACE	36
2.5	TRENDY A BUDOUCÍ VÝVOJ	36
2.5.1	Globální expanze QR plateb.....	36
2.5.2	Integrace s novými technologiemi	37
2.5.3	Evropské iniciativy a tlak na nezávislost	37
2.5.4	Národní standardizace a spolupráce	37
2.5.5	Budoucí vývoj	37
3	MEZINÁRODNÍ STANDARDY	38
3.1	STANDARDY PRO PLATEBNÍ KARTY	38
3.1.1	ISO normy	38
3.1.2	EMV (Europay, Mastercard, Visa) standardy	39
3.1.3	PCI DSS	39
3.2	KOMUNIKAČNÍ PROTOKOLY PRO KARETNÍ PLATBY	40
3.2.1	SPDH (Standard Point of Sale Data Handling).....	40
3.2.2	ISO 8583.....	40
3.2.3	APDU	40
3.2.4	Transportní vrstva a šifrování.....	40
3.3	STANDARDY PRO DIGITÁLNÍ PLATBY A QR KÓDY	41
3.3.1	ISO normy pro QR platby	41
3.3.2	EMV QR Code Specification	41
3.3.3	Standardy pro mobilní a digitální platby	41
3.4	REGULAČNÍ RÁMEC A PRÁVNÍ NORMY	41
3.4.1	Evropské směrnice a právní normy	42
3.4.2	Mezinárodní právní rámec.....	42
3.5	KOMUNIKAČNÍ PROTOKOLY PRO QR PLATBY	42
3.5.1	REST API a JSON formát.....	42
3.5.2	gRPC (Google Remote Procedure Call).....	43
3.5.3	Šifrování a bezpečnost přenosu	44
4	SROVNÁNÍ PLATEBNÍCH KARET A QR PLATEB	46
4.1	RYCHLOST A UŽIVATELSKÝ KOMFORT	46
4.2	BEZPEČNOSTNÍ ASPEKTY	47
4.2.1	Riziko zneužití údajů při transakci	47
4.2.2	Vektor útoku a kontrola uživatele	47
4.2.3	Technologická zranitelnost a vnější hrozby	48
4.2.4	Regulační rámec a standardizace	48
4.2.5	Závěr komparace	48
4.3	DOSTUPNOST A IMPLEMENTAČNÍ NÁKLADY PRO OBCHODNÍKY	49
4.3.1	Platební karty (zavedený standard s vyššími počátečními náklady)	49
4.3.2	QR platby (nízkonákladová a flexibilní alternativa)	49
4.3.3	Závěr komparace	49

4.4	AKCEPTACE NA GLOBÁLNÍM TRHU A REGIONÁLNÍ ROZDÍLY	50
4.5	ENVIRONMENTÁLNÍ DOPAD PATEBNÍCH METOD	51
4.5.1	Výroba a životní cyklus platebních karet.....	51
4.5.2	Ekologické alternativy a inovace	52
4.5.3	QR platby a jejich environmentální profil	52
4.5.4	Směr vývoje a udržitelná budoucnost plateb	52
II	PRAKTICKÁ ČÁST.....	54
5	POUŽITÉ TECHNOLOGIE A VÝVOJOVÉ PROSTŘEDÍ.....	55
5.1	VÝVOJOVÉ PROSTŘEDÍ A NÁSTROJE.....	55
5.1.1	IntelliJ IDEA	55
5.1.2	Postman	55
5.1.3	Windows	55
5.2	PROGRAMOVACÍ JAZYK A FRAMEWORK	55
5.2.1	Java.....	56
5.2.2	Spring Boot	56
5.3	KOMUNIKACE A INTEGRACE	56
5.3.1	REST API.....	56
5.3.2	gRPC	56
5.3.3	Altapay	56
6	EKOSYSTÉM PRO IMPLEMENTACI.....	58
6.1	MONET+.....	58
6.2	SMARTSWITCH.....	58
6.3	MIKROSERVISNÍ ARCHITEKTURA	59
7	NÁVRH ARCHITKTURY	60
7.1	CELKOVÝ TOK TRANSAKCE	62
7.2	STRUKTURA SYSTÉMU	63
7.3	PRÁCE SE STAVY TRANSAKcí	64
7.4	SYNCHRONIZACE A OCHRANA PROTI SOUBĚHU	64
8	IMPLEMENTACE SLUŽBY	66
8.1	PRVNÍ FÁZE (ÚPRAVA SMARTSWITCHE)	66
8.2	DRUHÁ FÁZE (IMPLEMENTACE QRPAYMENT)	67
8.2.1	Vytvoření Spring Boot aplikace.....	67
8.2.2	Napojení knihoven přes Maven	67
8.2.3	gRPC komunikace.....	69
8.2.4	Přijetí a zpracování požadavku ze SMSW	69
8.2.5	Správa transakcí a práce s pamětí	69
8.2.6	Použité datové struktury	70
8.2.7	Zápis a čtení dat	70
8.2.8	Periodické čištění starých záznamů	70
8.2.9	Integrace s platební bránou	71

8.2.10	Webhook implementace	72
8.3	TŘETÍ FÁZE (ÚPRAVA CORE-REST-SIMULATOR)	73
9	ANALÝZA A TESTOVÁNÍ.....	75
9.1	INICIALIZACE QR PLATBY	75
9.2	STAVOVÁ ZPRÁVA PLATBY	75
9.3	WEBHOOK SIMULACE A NOTIFIKACE	76
9.4	TESTOVACÍ SCÉNÁŘE A CHOVÁNÍ	76
ZÁVĚR.....		77
SEZNAM POUŽITÉ LITERATURY		79
SEZNAM OBRÁZKŮ		87
SEZNAM TABULEK.....		88
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		89
SEZNAM PŘÍLOH.....		91

ÚVOD

V posledních letech dochází k dynamickému rozvoji digitálních platebních metod, mezi něž se stále více řadí platby prostřednictvím QR kódů. Zatímco platební karty dominují bezhotovostním platbám, QR kódy nabízejí rychlou a flexibilní alternativu, která si získává popularitu především v mobilních aplikacích a e-commerce. Přestože obě metody mají podobný cíl (provedení bezpečné a rychlé platby), jejich technické řešení se výrazně liší.

Tradiční platební ekosystém je založen na autorizaci transakcí iniciované platebním terminálem, přičemž všechny kroky probíhají v rámci pevně definovaného procesu mezi vydavatelem karty, bankou a obchodníkem. Naproti tomu QR platby spoléhají na přímou interakci mezi mobilním zařízením zákazníka a platební infrastrukturou, což vyžaduje odlišný přístup k ověřování a autorizaci transakcí.

Vzhledem k tomu, že QR platby představují stále významnější alternativu, je nezbytné prověřit možnosti jejich integrace do stávajících systémů postavených na mikroservisní architektuře. Diplomová práce se proto zaměřuje na komplexní porovnání obou přístupů, shrnutí příslušných mezinárodních standardů, a především na návrh a implementaci nové služby podporující platby prostřednictvím QR kódů. Navržená služba je realizována v prostředí založeném na jazyce Java, frameworku Spring Boot a komunikačních technologiích gRPC a REST, s důrazem na škálovatelnost a bezpečnost.

I TEORETICKÁ ČÁST

1 PLATEBNÍ KARTY

Platební karty představují dnes jeden z nejrozšířenějších nástrojů bezhotovostního placení. Umožňují spotřebitelům jednoduše realizovat finanční transakce bez nutnosti manipulace s hotovostí. Jejich popularita tedy vychází především z vysoké míry pohodlí, bezpečnosti a univerzálnosti použití.

Jejich mohutné rozšíření bylo umožněno technologickými inovacemi v oblasti bankovníctví a elektronických systémů a postupně se staly jedním z nejpoužívanějších platebních prostředků na světě. Platební karty dnes slouží nejen jako nástroj pro rychlou úhradu zboží a služeb, ale i jako prostředek pro správu osobních financí a přístup k doplňkovým službám, jako jsou věrnostní programy nebo cestovní pojištění. Rozvoj platebních karet je úzce propojen s vývojem globální platební infrastruktury a bezpečnostních standardů.

1.1 Historie a vývoj

Historie platebních karet sahá do roku 1950, kdy byla představena první univerzální charge karta společností Diners Club (viz Obrázek 1). Tuto kartu vytvořil Frank McNamara spolu se svým právníkem Ralphem Schneiderem jako řešení pro bezhotovostní platby v restauracích. První karta byla akceptována ve 27 restauracích v New Yorku a rychle získala popularitu mezi spotřebiteli. [1] [2]

V roce 1958 vstoupila na trh společnost American Express se svou vlastní charge kartou, která byla jako první vyrobena z plastu namísto papíru, čímž se zvýšila její odolnost a praktičnost. Tímto krokem rozšířila koncept bezhotovostních plateb na mezinárodní úroveň. [3]

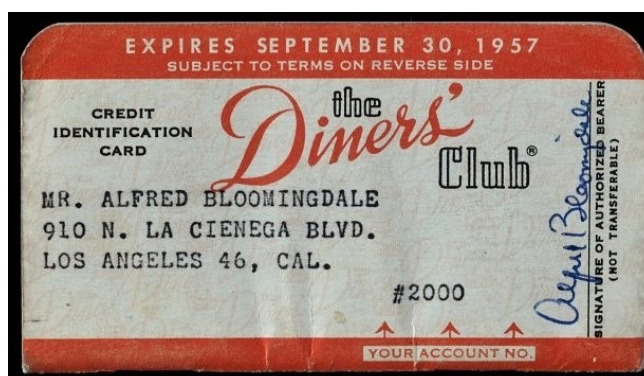
V roce 1966 byla založena asociace Interbank Card Association (ICA), která později uvedla na trh kartu Master Charge, předchůdce dnešní Mastercard. Tato asociace vznikla jako reakce na rostoucí popularitu kreditních karet a potřebu standardizace platebních systémů mezi bankami. [4]

V 90. letech 20. století byla vyvinuta technologie čipových karet známá jako EMV (Europay, Mastercard, Visa). Tyto karty obsahují integrovaný čip, který zvyšuje bezpečnost transakcí a snižuje riziko podvodů. Standard EMV byl postupně přijat po celém světě a stal se novým standardem pro platební karty. [5]

Po roce 2000 se začaly rozvíjet bezkontaktní platební technologie, které umožňují provádět platby pouhým přiložením karty k terminálu. Tato technologie využívá NFC (Near Field Communication) a zrychluje proces placení, zejména u menších částek. První bezkontaktní platební karta byla představena v roce 1995 v Jižní Koreji pro systém hromadné dopravy. [6] [81]

V posledním desetiletí došlo k rozmachu mobilních platebních aplikací a digitálních peněženek, jako jsou Apple Pay a Google Pay. Tyto služby umožňují uživatelům ukládat informace o svých platebních kartách v mobilních zařízeních a provádět platby pomocí smartphonů nebo chytrých hodinek, což dále zvyšuje pohodlí a bezpečnost bezhotovostních transakcí. Apple Pay byl spuštěn v roce 2014, následován Google Pay. [7] [8]

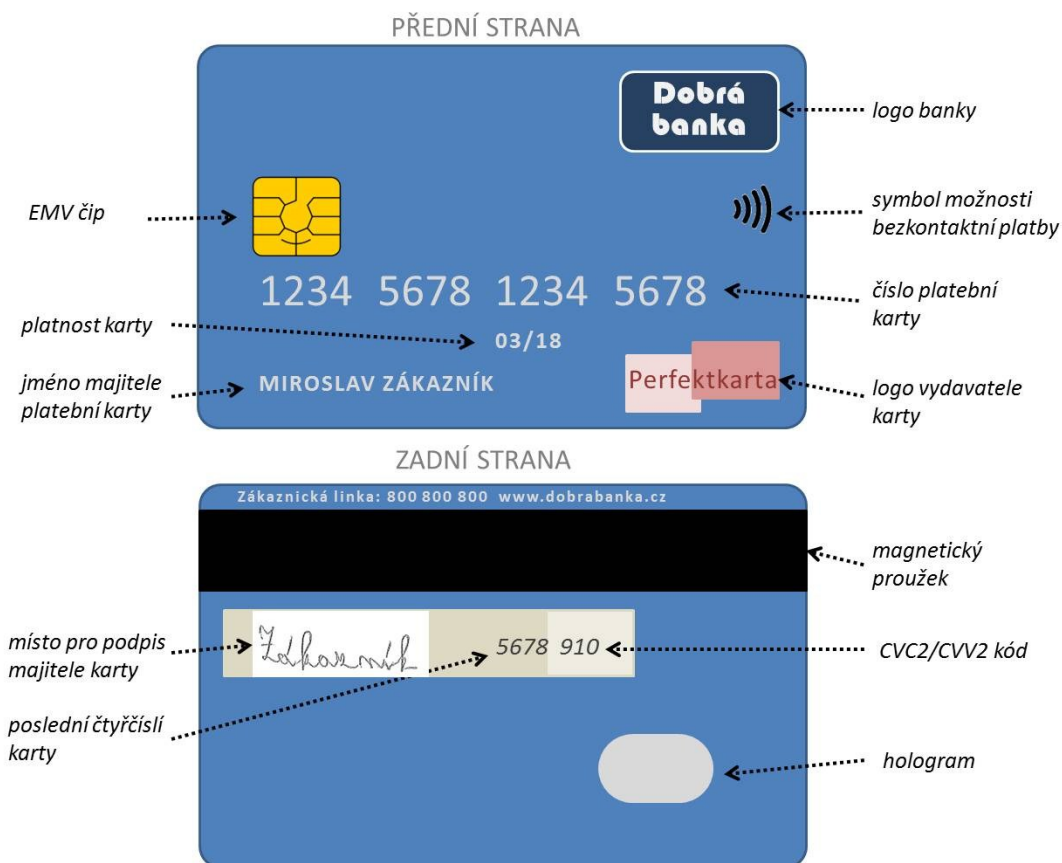
Vývoj platebních karet od jejich vzniku až po současnost ukazuje na neustálou snahu o zlepšení uživatelského komfortu, zvýšení bezpečnosti a adaptaci na nové technologie v oblasti finančních transakcí.



Obrázek 1 1957 Diners Club kreditní karta [9]

1.2 Typy platebních karet

Platební karty lze rozdělit do několika základních kategorií na základě způsobu plateb a vztahu mezi držitelem karty a vydavatelskou institucí.



Obrázek 2 Popis platební karty [35]

1.2.1 Kreditní karty

Kreditní karta umožňuje držiteli čerpat úvěr od banky nebo finanční instituce do předem stanoveného limitu. Držitel karty může využít bezúročné období (obvykle 14–30 dní), během něhož, pokud celý dluh splatí, neplatí žádné úroky. Po uplynutí tohoto období jsou z nesplacené částky účtovány úroky. Kreditní karty jsou často využívány pro nákupy zboží a služeb, přičemž umožňují flexibilní splácení dluhu. [10]

1.2.2 Debetní karty

Debetní karta je přímo propojena s běžným účtem držitele. Při platbě nebo výběru hotovosti jsou prostředky okamžitě odečteny z účtu. Držitel karty může utratit pouze tolik, kolik má aktuálně na účtu k dispozici. Debetní karty jsou běžně používány pro každodenní transakce, jako jsou nákupy v obchodech nebo výběry z bankomatů. [10]

1.2.3 Charge karty

Charge karta je typ platební karty, která umožňuje držiteli čerpat finanční prostředky s povinností uhradit celou dlužnou částku v plné výši na konci každého zúčtovacího období,

obvykle do 14–30 dnů od obdržení výpisu. Na rozdíl od kreditních karet není umožněno revolvingové splácení a z čerpané částky se neúčtují úroky, pokud je dluh splacen včas. Charge karty jsou často nabízeny bonitním klientům a využívány pro firemní účely. [10]

1.2.4 Předplacené karty

Předplacená karta je platební karta, na kterou si držitel předem nabije určitou částku peněz. Transakce jsou pak omezeny výší tohoto zůstatku. Předplacené karty nejsou vázány na bankovní účet a umožňují kontrolu nad výdaji. Jsou vhodné pro online nákupy, jako dárkové karty nebo pro osoby bez bankovního účtu. [11]

1.2.5 Virtuální karty

Virtuální karta je digitální verze platební karty určená primárně pro online transakce. Neexistuje ve fyzické podobě, ale obsahuje všechny potřebné údaje jako číslo karty, datum expirace a CVV kód. Virtuální karty zvyšují bezpečnost online plateb, protože nejsou fyzicky přítomny a jejich údaje lze snadno měnit nebo omezit. Některé banky umožňují nastavení limitů nebo dočasné deaktivace těchto karet. [12]

Existují i jednorázové virtuální platební karty. Tuto kartu lze vygenerovat do internetového bankovníctví nebo mobilní peněženky pouze na jednu konkrétní platbu a po vykonání jedné platby se automaticky zruší. Velikou výhodou takovéto karty je její vysoká bezpečnost, protože je použita vždy jednou a nikdo ji tak nemůže zneužít. Nevýhodou těchto karet je skutečnost, že nemusí být akceptována a ubchodníků. [12]

1.2.6 Co-brandované a partnerské karty

Co-brandované karty jsou výsledkem spolupráce mezi bankou a konkrétní obchodní společností nebo značkou. Tyto karty často nabízejí speciální výhody, jako jsou slevy, věrnostní body nebo exkluzivní nabídky při nákupech u daného partnera. Například letecké společnosti mohou ve spolupráci s bankami nabízet karty, které umožňují sbírat míle za uskutečněné nákupy. [13]

1.3 Mechanismus fungování

Platební karty představují moderní nástroj umožňující rychlé, efektivní a bezpečné bezhotovostní transakce. Jejich fungování je výsledkem koordinace několika klíčových subjektů, mezi které patří držitelé karet, obchodníci, banky, karetní asociace a

zpracovatelská centra. Tento mechanismus je navržen tak, aby zajišťoval maximální spolehlivost a minimalizoval riziko podvodu či technické chyby.

1.3.1 Účastníci platebního procesu

Platební systém kartou se opírá o součinnost několika klíčových subjektů, z nichž každý má specifickou roli:

- a) Držitel karty (Cardholder) je osoba, která vlastní platební kartu a využívá ji pro bezhotovostní platby.
- b) Obchodník (Merchant) je podnikatel nebo společnost přijímající platby kartou za své zboží nebo služby.
- c) Acquirer je banka nebo finanční instituce, která poskytuje obchodníkovi technické a finanční služby umožňující akceptaci platebních karet.
- d) Issuer představuje banku nebo finanční instituci, která vydala platební kartu držiteli a spravuje jeho účet.
- e) Karetní asociace (Card Networks), jako jsou například Visa, Mastercard či American Express, vytvářejí pravidla fungování celého systému, standardizují bezpečnostní protokoly a poskytují komunikační infrastrukturu mezi účastníky transakcí.

Každý z těchto subjektů je nezbytný pro správné zpracování platební transakce a jejich koordinace je klíčem k zajištění bezpečnosti i efektivity platebního procesu. [14]

1.3.2 Detailní průběh platební transakce

Samotný proces platby kartou probíhá v několika za sebou následujících fázích (viz Obrázek 3), které jsou pečlivě definovány mezinárodními standardy.

V první fázi dochází k inicializaci transakce. Držitel karty fyzicky nebo virtuálně předá údaje o kartě obchodníkovi, který prostřednictvím platebního terminálu (POS zařízení) odešle informace ke zpracování. Tyto informace obsahují číslo karty, datum expirace, bezpečnostní kód a částku transakce.

Následuje fáze autorizace, kdy acquirer předá informace karetní asociaci, která požadavek přeměruje vydavatelské bance. Vydavatelská banka ověří platnost karty, dostupnost finančních prostředků na účtu držitele a bezpečnostní znaky transakce. Pokud je

vše v pořádku, banka autorizuje transakci a zpráva o schválení je odeslána zpět obchodníkovi.

Po autorizaci následuje fáze zúčtování (clearing), kdy jsou souhrnné údaje o uskutečněných transakcích odesílány acquirerem karetní asociaci a následně vydavateli k vypořádání. Nakonec v rámci zúčtování dochází k přesunu finančních prostředků z účtu držitele přes systém karetní asociace na účet obchodníka vedený u acquirera. [15] [16]



Obrázek 3 Schéma platby kartou [17]

1.4 Bezpečnostní mechanismy

Bezpečnost v oblasti platebních karet představuje jeden z nejdůležitějších aspektů jejich používání. Vzhledem k tomu, že karty slouží jako nástroj k přístupu k finančním prostředkům uživatelů, je nezbytné implementovat vícevrstvá bezpečnostní opatření, která minimalizují riziko podvodů, krádeží a neoprávněného přístupu k citlivým datům.

1.4.1 Fyzické zabezpečení platebních karet

Jedním ze základních pilířů bezpečnosti je fyzická ochrana samotné platební karty. Moderní karty jsou standardně vybaveny čipovou technologií EMV, která zásadně zvyšuje bezpečnost transakcí. Čip na kartě při každé transakci generuje jedinečný kód, čímž znemožňuje jednoduché kopírování dat, jaké bylo běžné u starších magnetických proužků. Magnetický proužek však stále zůstává na kartách přítomen z důvodu kompatibility se staršími platebními terminály, přestože jeho bezpečnostní úroveň je ve srovnání s čipem výrazně nižší. Doplňkovým ochranným prvkem jsou také hologramy, speciální potisky a embosování, které slouží k ověření pravosti karty při vizuální kontrole. [18]

1.4.2 Elektronická a síťová bezpečnost

Elektronická ochrana údajů tvoří druhou zásadní linii obrany. Během přenosu dat mezi platebním terminálem, zúčtovací bankou a vydavatelskou bankou je komunikace zabezpečena silným šifrováním. Toto šifrování zabraňuje tomu, aby útočníci mohli zachytit a zneužít citlivé informace. Dalším významným bezpečnostním opatřením je tokenizace, při které jsou citlivé údaje o kartě nahrazeny náhodně generovanými tokeny. Tyto tokeny mají hodnotu pouze v rámci konkrétní transakce a nelze je zneužít mimo jejich původní kontext.

V oblasti internetových plateb se navíc využívá autentizační protokol 3D Secure, který přidává další vrstvu ověření držitele karty, a tím výrazně snižuje riziko podvodů při online nákupu. [19] [20]

1.4.3 Standardy bezpečnosti a compliance

Pro zajištění jednotného a vysokého standardu bezpečnosti musejí všechny organizace, které pracují s daty platebních karet, dodržovat mezinárodní bezpečnostní normy. Nejvýznamnějším z těchto standardů je PCI DSS (Payment Card Industry Data Security Standard), který stanovuje podmínky pro bezpečné ukládání, zpracování a přenos dat o platebních kartách. Organizace, které tento standard nedodržují, riskují nejen ztrátu důvěry zákazníků, ale také vysoké finanční pokuty a právní postihy. Dále se v oblasti bezpečnosti uplatňují standardy EMV, které definují technické požadavky na používání čipových karet a přenos jejich dat s cílem minimalizovat riziko padělání a neoprávněného použití.

1.5 Poplatky a regulace

Platební karty jsou nejen nástrojem pohodlných plateb, ale zároveň představují komplexní ekosystém, ve kterém figurují různé typy poplatků a přísné regulatorní rámce. Správné pochopení tohoto systému je zásadní pro všechny účastníky platebního trhu – od obchodníků přes banky až po koncové uživatele.

1.5.1 Poplatky spojené s platebními kartami

Poplatek, který vzniká při realizaci platby kartou, není jednosložkový, ale skládá se z několika dílčích částí. Prvním a často nejvýznamnějším nákladem je mezibankovní poplatek (interchange fee), který si mezi sebou účtují banka obchodníka (tzv. acquiring banka) a banka držitele karty (tzv. issuing banka). Tento poplatek je odměnou vydavatelské bance za služby související s vydáním a správou karty, ale i za správu rizik a ochranu proti podvodům. V Evropské unii je výše mezibankovního poplatku regulována nařízením (EU) 2015/751 a nesmí překročit 0,2 % z částky transakce u debetních karet a 0,3 % u kreditních karet.

Další součástí poplatku je poplatek kartové asociaci, jako jsou Visa či Mastercard. Tento poplatek pokrývá náklady na technologické zajištění, inovace, marketing a bezpečnost celosvětové infrastruktury karetních plateb. Ačkoliv jeho přesná výše je obchodním tajemstvím, obvykle tvoří menší část celkového poplatku, ale je nezbytný pro správné fungování celého platebního ekosystému.

Poslední složkou je provize platební brány či poskytovatele platební služby, jakým je například GoPay. Tento subjekt si účtuje odměnu za zprostředkování celé platební transakce, včetně technického zajištění bezpečné komunikace, ověření platby a převodu finančních prostředků na účet obchodníka. Výše této provize závisí na obchodních podmínkách poskytovatele a na objemu uskutečněných plateb.

Poplatek účtovaný obchodníkovi tak představuje souhrn těchto tří hlavních složek: mezibankovního poplatku, poplatku kartové asociaci a provize poskytovateli platebních služeb. Obchodník přitom obvykle vidí pouze jednu finální hodnotu poplatku, zatímco rozdělení mezi jednotlivé subjekty probíhá na pozadí systému. [21]

1.5.2 Regulace platebních karet

Regulace trhu platebních karet se v posledních desetiletích stala klíčovým tématem v rámci ochrany spotřebitelů, podpory hospodářské soutěže a zajištění bezpečnosti platebních systémů. Významným milníkem v této oblasti bylo zavedení evropské regulace mezibankovních poplatků prostřednictvím nařízení Evropského parlamentu a Rady (EU) 2015/751 o mezibankovních poplatcích za karetní platební transakce. Toto nařízení stanovilo maximální výši mezibankovního poplatku na 0,2 % hodnoty transakce při použití debetní karty a na 0,3 % při použití kreditní karty. Cílem bylo zabránit nepřiměřeným nákladům pro obchodníky i konečné spotřebitele a podpořit konkurenceschopnost na trhu platebních služeb.

V českém právním rámci je oblast platebních služeb upravena především zákonem č. 370/2017 Sb., o platebním styku, který implementuje směrnici Evropského parlamentu a Rady (EU) 2015/2366, známou jako PSD2 (Payment Services Directive 2). Tento zákon podrobně upravuje pravidla pro poskytování platebních služeb, vydávání elektronických peněz a bezpečnostní požadavky na autentizaci uživatele a ochranu platebních dat. Česká národní banka (ČNB) jako dohledový orgán dohlíží na dodržování těchto předpisů a má pravomoc udělovat sankce v případě jejich porušení.

Další klíčovou oblastí regulace je bezpečnost platebních operací. PSD2 zavedla povinnost poskytovatelů platebních služeb implementovat tzv. silnou autentizaci klienta (SCA, Strong Customer Authentication), což znamená, že každá elektronická platba musí být ověřena pomocí alespoň dvou z následujících prvků: znalosti (například heslo), vlastnictví (například mobilní telefon) nebo inherence (například otisk prstu). Tato

povinnost byla následně doplněna nařízením Komise (EU) 2018/389, známým jako RTS SCA (Regulatory Technical Standards for Strong Customer Authentication).

Evropská unie rovněž reguluje transparentnost informací poskytovaných držitelům karet. Poskytovatelé platebních služeb musí uživatele informovat o všech poplatcích, směnných kurzech a podmínkách poskytovaných služeb s cílem zvýšit transparentnost a umožnit srovnání jednotlivých služeb.

V neposlední řadě je třeba zmínit také aktivity zaměřené na podporu interoperability platebních systémů v rámci EU, zejména v souvislosti s projektem Jednotné oblasti pro platby v eurech (SEPA), jehož cílem je umožnit bezproblémové provádění bezhotovostních plateb v celé Evropské unii za stejných podmínek jako v rámci jednotlivých členských států.

Regulace platebních karet je dynamickou oblastí, která se neustále vyvíjí v reakci na nové technologie, měnící se chování spotřebitelů i vývoj na trhu finančních služeb. Výsledkem těchto regulačních snah je prostředí, které je pro uživatele bezpečnější, transparentnější a konkurenceschopnější, zatímco poskytovatelé služeb musí čelit přísnějším požadavkům na compliance a technologickou inovaci. [22] [23] [24] [25]

1.6 Trendy v oblasti platebních karet

Vzhledem k neustálému vývoji digitálních technologií a měnícím se potřebám spotřebitelů čelí oblast platebních karet zásadním proměnám. Moderní platební systémy se již dávno neomezují pouze na fyzickou plastovou kartu a jednoduchý terminál. V současnosti sledujeme posun směrem k inteligentním, propojeným a bezpečnějším řešením, která reflektují rostoucí důraz na uživatelský komfort, bezpečnostní standardy, regulační požadavky a také ekologickou odpovědnost. Tyto změny jsou poháněny nejen technologickým pokrokem, ale i zvýšenou konkurencí na trhu, expanzí fintech startupů a snahou institucí o větší kontrolu nad platební infrastrukturou. V následujících podkapitolách jsou detailně rozebrány nejvýznamnější současné trendy, které ovlivňují podobu a budoucnost platebních karet.

1.6.1 Umělá inteligence a bezpečnost plateb

S rostoucí hrozbou kybernetických útoků, jejichž globální škody se v roce 2025 odhadují na 10 bilionů USD, se umělá inteligence stává klíčovým nástrojem v oblasti zabezpečení plateb. Společnost Mastercard implementovala systém Decision Intelligence Pro, který analyzuje

miliardy datových bodů a dokáže detekovat podvodné transakce během méně než 50 milisekund, čímž zvyšuje ochranu proti podvodům o přibližně 20 %. [26]

1.6.2 Tokenizace a konec ručního zadávání údajů

Tokenizace, která nahrazuje citlivé údaje o kartách jedinečnými tokeny, se stává standardem v oblasti online plateb. Mastercard plánuje do roku 2030 eliminovat potřebu ručního zadávání čísel karet a ověřovacích kódů při online transakcích, což zvýší bezpečnost a pohodlí uživatelů. [27]

1.6.3 Mobilní zařízení jako platební terminály

Technologie Tap on Phone umožňuje proměnit běžné chytré telefony v plnohodnotné platební terminály, což usnadňuje přijímání plateb zejména malým a středním podnikům. Tato inovace podporuje rozšíření bezkontaktních plateb a zvyšuje dostupnost platebních služeb. [28]

1.6.4 Virtuální karty pro B2B transakce

Virtuální karty, které jsou jednorázově generovány a napojeny na firemní účty, zjednodušují a zabezpečují platby mezi podniky. Automatické schvalování těchto plateb minimalizuje chyby a zlepšuje kontrolu nad firemními výdaji. [29]

1.6.5 Blockchain a digitální aktiva

V posledním desetiletí se technologie blockchainu a digitální aktiva staly zásadním impulsem pro proměnu globálního platebního ekosystému. Blockchain jako distribuovaná databáze umožňuje uchovávat a ověřovat transakce v decentralizovaném prostředí bez potřeby centrální autority. Tato vlastnost z něj činí atraktivní základ nejen pro kryptoměny, ale i pro nové formy digitálních plateb.

Jedním z klíčových přínosů blockchainových platebních systémů je transakční transparentnost a neměnitelnost záznamů, které výrazně zvyšují důvěryhodnost a auditovatelnost celého procesu. Na rozdíl od tradičních karetních nebo bankovních transakcí, které procházejí přes několik zprostředkovatelů, může blockchain umožnit peer-to-peer platby téměř v reálném čase a s nižšími náklady na zpracování. Tento model se osvědčuje zejména v oblasti mezinárodních převodů, kde běžné metody narážejí na vysoké poplatky, omezenou dostupnost a dlouhé zúčtovací časy.

S tím souvisí i rozvoj stablecoinů (kryptoměn navázaných na hodnotu fiat měn), např. USDC, USDT, které představují most mezi klasickými finančními systémy a blockchainovým světem. Stablecoiny umožňují stabilní a předvídatelné zúčtování, což je klíčové pro širší adopci v obchodním prostředí. Některé technologické společnosti a banky již experimentují s jejich využitím při B2B platbách nebo jako likvidní rezervy v digitálních peněženkách.

Dále se rozvíjí koncept centrálních bankovních digitálních měn (CBDC). Tyto digitální měny emitované přímo centrálními bankami (např. digitální euro, e-CNY) mají za cíl přenést důvěru státu do digitálního prostoru a zároveň posílit suverenitu měnové politiky. Z hlediska platebních karet je zajímavý vývoj hybridních modelů, kdy vydavatelé karet integrují podporu CBDC nebo kryptoměnových peněženek do svých produktů (např. Mastercard a Visa spolupracující s kryptoměnovými platformami).

Významnou oblastí, která spojuje blockchain a digitální platby, je Web3 (koncept nové generace internetu), který staví na decentralizovaných technologiích, vlastní správě dat a tokenizaci hodnoty. V tomto prostředí se uživatel stává nejen konzumentem, ale i aktivním účastníkem s přímým vlastnictvím a kontrolou nad svými aktivy. Platby v rámci Web3 probíhají často prostřednictvím kryptopeněženek, které komunikují s decentralizovanými aplikacemi a protokoly, čímž se zcela obchází tradiční platební infrastruktura.

Do budoucna lze očekávat, že digitální identita, interoperabilita blockchainů, škálování transakcí a důraz na regulační rámce budou klíčovými faktory pro širší uplatnění této technologie. Přestože blockchainové platby zatím nedosahují masového přijetí srovnatelného s platebními kartami, jejich potenciál pro redefinici způsobu, jakým dochází k výměně hodnoty, je značný. [27]

1.6.6 Inovativní design platebních karet

Banky experimentují s novými technologiemi v designu platebních karet, jako je integrace OLED displejů, které umožňují vizuální interakci při platbě. Tyto karty využívají bezdrátové nabíjení prostřednictvím NFC a zvyšují uživatelský zážitek. [30]

1.6.7 Udržitelnost a společenská odpovědnost

Finanční instituce integrují udržitelnost do svých produktů, například prostřednictvím platebních karet, které podporují ekologické iniciativy, jako je výsadba stromů za každou

transakci. Tímto způsobem banky reagují na rostoucí poptávku po společensky odpovědných finančních produktech.

1.6.8 Evropská platební suverenita a digitální euro

Jedním z aktuálně velmi diskutovaných témat v oblasti platebních systémů v Evropské unii je snaha o dosažení vyšší míry strategické autonomie a finanční suverenity. Evropská centrální banka (ECB), ve spolupráci s Evropskou komisí, deklarovala záměr postupně omezit závislost na dominantních amerických a asijských poskytovatelích platebních služeb, jakými jsou společnosti Visa, Mastercard, PayPal nebo čínská platforma Alipay. Tyto systémy sice umožňují rychlé a bezpečné provádění plateb, avšak jejich kontrola mimo evropský právní rámec představuje potenciální hrozbu v kontextu geopolitických a regulatorních rizik.

Prezidentka ECB Christine Lagarde v roce 2025 v této souvislosti prohlásila, že Evropa musí pochodovat směrem k nezávislosti skrze vytvoření vlastního platebního systému, jenž by nebyl vystaven vlivu třetích zemí. Vyzdvihla důležitost vytvoření evropské alternativy, která by občanům a podnikům poskytla možnost realizace elektronických transakcí bez nutnosti spoléhat se na zahraniční infrastrukturu.

Z tohoto důvodu je v současnosti intenzivně vyvíjeno tzv. digitální euro (elektronická forma měny vydávaná centrální bankou), které by mohlo sloužit jako doplněk k hotovosti a tradičním bankovním vkladům. Digitální euro má potenciál zjednodušit platby v rámci jednotného evropského trhu, zvýšit jejich bezpečnost, snížit náklady na transakce a zároveň posílit transparentnost finančního systému. Současně by mohlo eliminovat potřebu zprostředkovatelů v některých typech transakcí, což by dále přispělo k autonomii evropského finančního sektoru.

Z technického hlediska se předpokládá, že digitální euro bude fungovat na principu decentralizované infrastruktury a bude implementováno s důrazem na ochranu osobních údajů uživatelů. Rovněž se zvažuje možnost offline použití, které by zvýšilo jeho dostupnost v oblastech s omezeným připojením k internetu.

Přestože vývoj evropské platební infrastruktury čelí řadě výzev, od technické složitosti přes legislativní rámec až po akceptaci ze strany spotřebitelů, představuje digitální euro významný krok směrem k posílení finanční stability a geopolitické soběstačnosti Evropské unie. [31]

2 DIGITÁLNÍ PLATEBNÍ PROSTŘEDKY ZALOŽENÉ NA QR KÓDECH

V posledním desetiletí dochází k zásadní transformaci v oblasti bezhotovostních plateb, a to zejména díky intenzivnímu rozvoji digitálních technologií a narůstajícímu množství chytrých mobilních zařízení mezi běžnými spotřebiteli. V rámci tohoto vývoje se QR kódy etablovaly jako jeden z nejvýznamnějších nástrojů pro iniciaci platebních transakcí, a to zejména v prostředí, kde je vyžadováno jednoduché, rychlé a nízkonákladové řešení.

QR kódy umožňují přenos předem definovaných dat mezi plátcem a příjemcem platby prostřednictvím vizuálního záznamu, který je snadno skenovatelný optickými senzory běžně dostupnými v mobilních telefonech. Na rozdíl od tradičních platebních metod, které často vyžadují drahou infrastrukturu (např. platební terminály nebo čipové karty), je nasazení QR plateb technicky méně náročné a zároveň vysoce škálovatelné, což usnadňuje jejich implementaci i v rozvojových zemích či u malých obchodníků s omezeným rozpočtem.

Díky těmto výhodám si QR platby získaly obrovskou popularitu zejména v Asii, kde se staly dominantní formou bezhotovostního platebního styku. Příkladem mohou být systémy Alipay a WeChat Pay v Číně, které denně zpracovávají miliardy transakcí. V současnosti se však tato technologie rozšiřuje i do dalších částí světa, včetně Evropy, kde je snaha o vytvoření standardizovaného rámce pro její využití v souladu s pravidly SEPA (Single Euro Payments Area).

Cílem této kapitoly je podrobně analyzovat fungování digitálních platebních systémů založených na QR kódech, identifikovat jejich klíčové výhody a rizika, představit hlavní poskytovatele na trhu a zároveň popsat aktuální stav v oblasti regulace a standardizace. Zvláštní pozornost je také věnována otázkám kybernetické bezpečnosti, které s rostoucím významem této technologie nabývají na důležitosti.

2.1 Princip fungování

Digitální platební prostředky využívající QR kódy fungují na principu přenosu předem definovaných dat ve vizuální formě mezi obchodníkem a zákazníkem. Základem této technologie je dvourozměrný čárový kód, který dokáže zakódovat platební informace, jako je částka, měna, identifikátor příjemce, popis platby a případně i další metadata nezbytná pro zpracování transakce. Na rozdíl od tradičních platebních metod, které vyžadují fyzický kontakt s platebním terminálem (např. magnetický proužek, čip nebo NFC čtečka), QR

platby využívají kameru mobilního zařízení k sejmutí platebního kódu, čímž dochází k bezkontaktnímu a vizuálně iniciovanému přenosu dat.

Princip fungování lze rozdělit do dvou základních režimů podle iniciátora platby na statické a dynamické QR kódy. Statické QR kódy jsou předem vygenerované kódy s fixním obsahem, které neobsahují proměnlivá data. Nejčastěji se používají v situacích, kdy částku zadává zákazník ručně, např. u charitativních sbírek, stánkového prodeje nebo fakturačního QR kódu na tištěných dokumentech. Dynamické QR kódy se generují v reálném čase a obsahují specifická data pro každou transakci, včetně konkrétní částky, účelu platby nebo jedinečného ID platby. Tento typ je běžný v e-commerce prostředí nebo v moderních POS systémech, kde se platební QR kód generuje individuálně pro každého zákazníka.

Proces provedení QR platby začíná vytvořením QR kódu, který je následně zobrazen na obrazovce zařízení obchodníka (např. tablet, pokladna, displej) nebo vytištěn na papíře. Zákazník má možnost volby mezi dvěma způsoby provedení platby, podle situace. První postup obsahuje následující kroky. Otevře svou mobilní platební aplikaci (např. bankovní aplikaci nebo samostatnou digitální peněženku), spustí funkci skenování QR kódů a načte zobrazený kód. Po sejmutí dojde k dekodování informací a v případě potřeby zákazník potvrdí částku a provede autorizaci platby. Druhý způsob platby (viz Obrázek 4) nezahrnuje manipulaci s bankovní, ani žádnou jinou aplikací. Tento způsob spočívá pouze v načtení QR kódu kamerou telefonu. Následně je plátce přesměrován na stránky poskytovatele platby, kde si zvolí postup a typ platby (např. Apple Pay, platební karta, GoPay atd.). Odkaz, kam je plátce přesměrován, je principiálně podobný u většiny poskytovatelů plateb, aby se zajistila snadná manipulace.

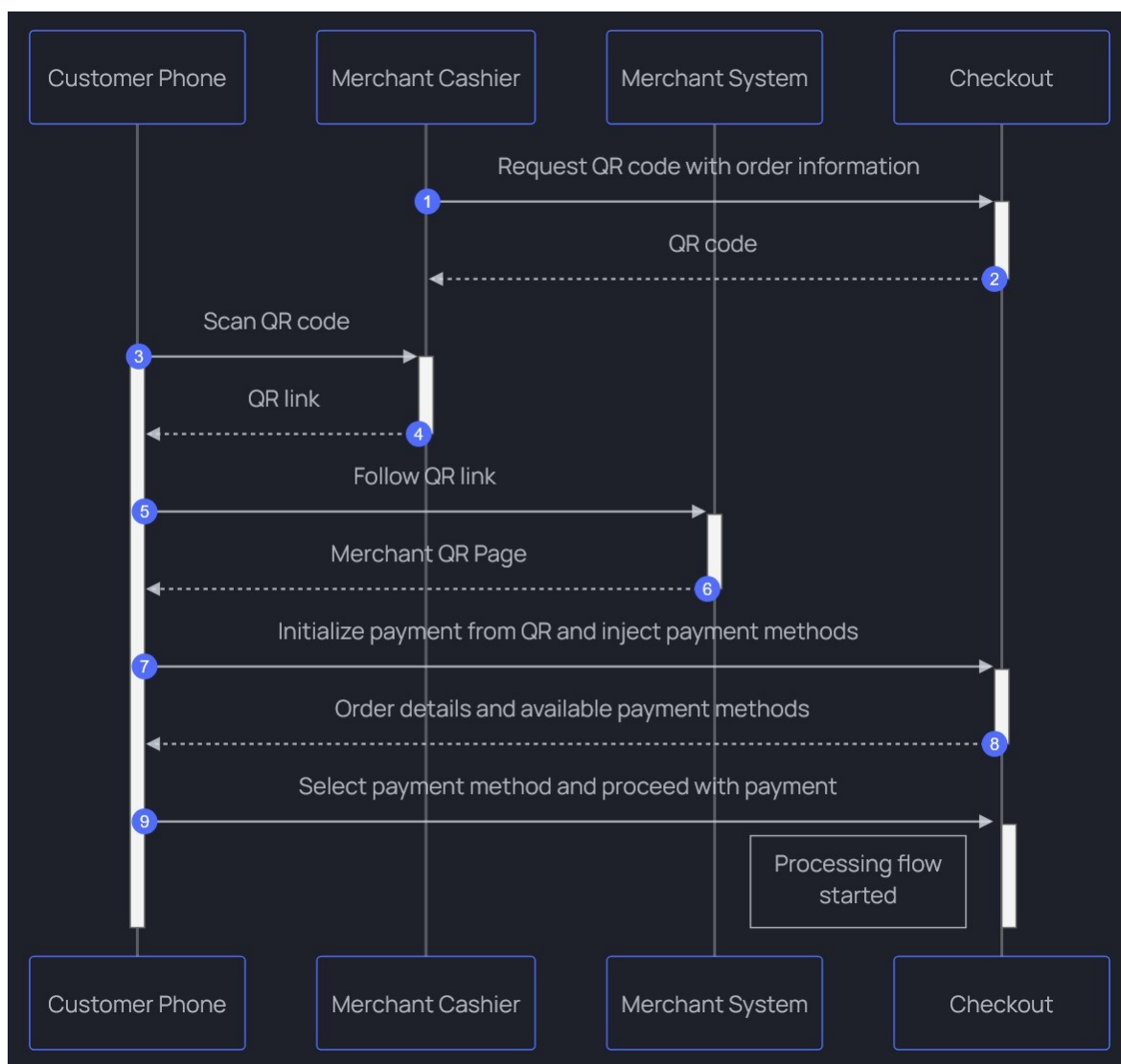
Je důležité poznamenat, že některé platební systémy mohou vyžadovat další kroky, jako je ověření identity nebo potvrzení transakce prostřednictvím SMS zprávy. Bezpečnostní opatření se mohou lišit v závislosti na poskytovateli platebních služeb a na regionu.

Platba je následně odeslána ke zpracování přes platební bránu nebo agregátor, který ověří údaje, iniciuje převod mezi bankovními účty a doručí potvrzení o úspěšné transakci. Celý proces obvykle probíhá v reálném čase nebo s minimální latencí, což umožňuje okamžitou odezvu a vysoký uživatelský komfort.

Z technického hlediska QR kódy pro platby často vycházejí ze specifikací EMVCo QR Code Specification, organizace vytvořená hlavními karetními schématy (Europay, Mastercard, Visa), která stanovuje standardy pro interoperabilní a bezpečné používání QR

kódů v globálním měřítku. Další standardy, jako například ISO/IEC 18004, definují samotnou strukturu a technologii QR kódu jako grafického nosiče informací.

QR platby jsou v mnoha ohledech považovány za bezpečnější alternativu k tradičním způsobům, protože citlivé údaje (např. údaje o kartě) nemusí být předávány mezi stranami přímo. Ve většině implementací je využíván tokenizační mechanismus nebo identifikace skrze unikátní platební ID, což dále přispívá ke zvýšení bezpečnosti transakcí. [32] [33]



Obrázek 4 Proces dynamických QR kódů [34]

2.2 Hlavní poskytovatelé

S rostoucí popularitou QR plateb na globálním i regionálním trhu se rozvíjí široké spektrum poskytovatelů, kteří nabízejí různé modely řešení – od integrovaných platebních bran až po samostatné aplikace pro generování a čtení QR kódů. Tito poskytovatelé se odlišují nejen

geografickým zaměřením, ale také typem nabídky, způsobem zpracování transakcí, úrovní zabezpečení a integrace s ostatními platebními nebo účetními systémy.

2.2.1 Alipay a WeChat Pay (Čína)

Mezi nejvýznamnější globální hráče v oblasti QR plateb jednoznačně patří čínské platformy Alipay a WeChat Pay. Tyto aplikace slouží jako digitální peněženky a QR kódy používají jako primární metodu pro zadávání plateb. Transakce probíhá buď oskenováním QR kódu obchodníka nebo generováním QR kódu uživatelem. Díky jejich rozšíření v čínské společnosti a plné integraci do každodenního života (např. veřejná doprava, restaurace, e-shopy) se QR platby staly normou pro většinu bezhotovostních transakcí v této zemi. [36] [37]



Obrázek 5 Alipay a WeChat [38]

2.2.2 Paytm a PhonePe (Indie)

Indický trh zažívá v posledních letech revoluci v digitálních platbách, částečně díky vládní iniciativě UPI (Unified Payments Interface). Platformy jako Paytm a PhonePe umožňují okamžité bezhotovostní platby prostřednictvím QR kódů, přičemž transakce jsou propojeny přímo s bankovními účty uživatelů. Tento přístup eliminuje potřebu vlastnit debetní či kreditní kartu. Indie se tak stává jedním z nejrychleji rostoucích trhů v oblasti QR plateb. [39] [40]



Obrázek 6 Paytm a PhonePe [41]

2.2.3 Apple Pay a Google Pay (globálně)

Ačkoli jsou Apple Pay a Google Pay primárně spojovány s technologií NFC, obě platformy začínají implementovat i funkci QR plateb. Například v některých regionech umožňuje Google Pay generovat QR kódy pro peer-to-peer platby, což je užitečné zejména v prostředí s omezeným přístupem k NFC terminálům. Tento hybridní model rozšiřuje dosah těchto technologií do oblastí, kde je infrastruktura pro tradiční bezkontaktní platby méně rozvinutá. [42] [43]



Obrázek 7 Apple Pay a Google Pay [44]

2.2.4 Revolut, Twint, Lydia a další evropské fintech platformy

Evropský trh s QR platbami zažívá dynamický růst zejména díky aktivitě fintech společností, které inovují v oblasti digitálního bankovníctví a platebních služeb. Zatímco tradiční banky postupně adoptují QR platby jako doplněk ke standardním bankovním službám, fintech startupy často staví tuto technologii do centra své uživatelské zkušenosti.

Jedním z nejvýznamnějších hráčů je Revolut, britská neobankovní platforma, která nabízí možnost generování QR kódů pro jednoduché a rychlé peer-to-peer platby. Uživatel Revolutu může vygenerovat QR kód s požadovanou částkou a sdílet jej s druhou osobou, která jej načte prostřednictvím mobilní aplikace, čímž se transakce automaticky zpracuje. Tento způsob je využíván nejen v osobní sféře, ale i u drobných podnikatelů pro inkaso plateb bez nutnosti terminálu. [45] [46]

Ve Švýcarsku se významně prosadila aplikace Twint, která byla vyvinuta ve spolupráci švýcarských bank a je široce akceptována ve veřejné dopravě, supermarketech, restauracích i e-commerce. Twint kombinuje QR kódy s přímým napojením na bankovní účet a umožňuje i parkování, dary charitám nebo převody mezi uživateli. Její funkčnost ji řadí mezi nejpokročilejší systémy svého druhu v Evropě. [47] [48]

Dalším příkladem je francouzská aplikace Lydia, která cílí především na mladé uživatele a studenty. Umožňuje rychlé převody peněz pomocí QR kódů a funguje na bázi digitální peněženky s možností připojení bankovního účtu nebo platební karty. Lydia je rovněž oblíbeným nástrojem pro rozdělování účtů v restauracích nebo pro sdílení výdajů v reálném čase. [49]

V Polsku se rozvíjí systém BLIK, který sice primárně využívá šestimístný kód, ale v některých verzích implementace umožňuje také skenování QR kódů pro platby v e-shopech nebo u fyzických obchodníků. BLIK je přímo propojen s největšími polskými bankami, což zajišťuje vysoký stupeň důvěry a dostupnosti. [50]

V neposlední řadě stojí za zmínku i evropská iniciativa European Payments Initiative (EPI), která si klade za cíl vytvořit jednotnou evropskou digitální platební platformu. V její finální fázi se předpokládá plná podpora QR kódů pro bezkontaktní platby i P2P transakce, čímž by Evropa mohla snížit svou závislost na globálních značkách jako Visa nebo Mastercard. [51] [52]

2.2.5 Česká republika – QR Platba, ČSOB, Česká spořitelna a GoPay

Na českém trhu patří mezi významné poskytovatele QR plateb technologie vyvíjené pod značkou QR Platba, která je podporována většinou tuzemských bank. Standard byl zaveden Českou bankovní asociací (ČBA) a umožňuje zákazníkům jednoduše uhradit faktury a složenky načtením QR kódu. Komerční banky jako ČSOB nebo Česká spořitelna tyto možnosti integrují přímo do svých mobilních aplikací. Platební brána GoPay nabízí QR platby obchodníkům v rámci e-commerce řešení, a tím umožňuje zákazníkům rychle platit prostřednictvím internetového bankovníctví. [53] [54]

2.3 Bezpečnostní aspekty

S rostoucím využíváním QR kódů v oblasti digitálních plateb se zvyšuje i potřeba důkladného porozumění bezpečnostním rizikům spojeným s touto technologií. Ačkoli QR

kódy nabízejí pohodlný a efektivní způsob provádění transakcí, jejich nesprávné implementace nebo zneužití mohou vést k vážným bezpečnostním incidentům.

2.3.1 Hlavní bezpečnostní hrozby

Jedním z nejčastějších způsobů zneužití QR kódů je jejich nahrazení škodlivými verzemi, které přesměrovávají uživatele na podvodné webové stránky. Tyto stránky mohou napodobovat legitimní portály a sloužit k získání citlivých údajů, jako jsou přihlašovací informace nebo platební údaje.

Další hrozbou může být skrytý malware, který může být distribuován prostřednictvím QR kódů, které po naskenování spustí stahování škodlivého softwaru do zařízení uživatele. Tento software může získat neoprávněný přístup k osobním datům, monitorovat činnost uživatele nebo dokonce převzít kontrolu nad zařízením.

Útočníci mohou manipulovat s QR kódy tak, aby platby směřovaly na jejich vlastní účty místo na účty legitimních obchodníků. Tato forma podvodu je obzvláště nebezpečná, protože uživatelé si často neuvědomují, že jejich platba byla přesměrována. [55]

2.3.2 Ochranná opatření a osvědčené postupy

Dynamické QR kódy, které jsou generovány pro každou transakci zvlášť, snižují riziko jejich zneužití. Na rozdíl od statických kódů, které mohou být snadno zkopírovány nebo nahrazeny, dynamické kódy poskytují vyšší úroveň bezpečnosti.

Před naskenováním QR kódu by měli uživatelé ověřit jeho původ a vizuálně zkontrolovat, zda nebyl kód přelepen nebo jinak upraven. Tato jednoduchá opatření mohou zabránit mnoha podvodům.

Pro skenování QR kódů by měly být používány pouze oficiální aplikace bank nebo renomovaných poskytovatelů platebních služeb. Tím se minimalizuje riziko stažení škodlivého softwaru nebo přesměrování na podvodné stránky.

Zvyšování povědomí o rizicích spojených s QR kódy a školení v oblasti kybernetické bezpečnosti mohou výrazně snížit počet úspěšných útoků. Informovaní uživatelé jsou méně náchylní k podvodům a lépe rozpoznají podezřelé situace. [56]

V reakci na rostoucí hrozby spojené s QR platbami se regulační orgány a standardizační instituce snaží vytvořit rámce pro bezpečné používání této technologie. Například

organizace EMVCo vydala specifikace pro QR kódy v platebních systémech, které definují požadavky na jejich bezpečné implementace.

2.4 Regulace a standardizace

Regulace a standardizace digitálních platebních prostředků založených na QR kódech se v posledních letech dostávají do popředí zájmu regulačních orgánů i standardizačních institucí. Hlavním cílem těchto snah je zajistit interoperabilitu, bezpečnost a důvěru uživatelů napříč různými regiony a poskytovateli platebních služeb.

Jedním z klíčových aktérů v oblasti standardizace je mezinárodní organizace EMVCo, která vydala specifikace pro použití QR kódů v platebních transakcích (tzv. EMV QR Code Specifications). Tyto specifikace definují strukturu a zabezpečení pro QR kódy, čímž přispívají k jednotnému přístupu napříč trhem. [57]

Na úrovni Evropské unie se v oblasti digitálních plateb uplatňuje obecná regulace služeb informační společnosti a zejména směrnice PSD2, která podporuje otevřenost, bezpečnost a inovace ve finančním sektoru. I když PSD2 přímo neřeší QR platby, vztahuje se na ně v rámci širších pravidel pro autorizaci transakcí a ochranu uživatelských údajů.

V některých zemích mimo EU, jako je Indie (systém Bharat QR) nebo Čína (standardy PBOC pro QR kódy), existují již pokročilé regulační rámce, které stanovují povinné technické a bezpečnostní požadavky na provozovatele QR platebních systémů. [58] [59]

2.5 Trendy a budoucí vývoj

Digitální platební prostředky založené na QR kódech představují rychle se vyvíjející oblast, která reflektuje změny v technologickém pokroku, spotřebitelském chování i regulatorním prostředí. Zatímco QR platby si původně našly své uplatnění zejména v asijských zemích, především v Číně a Indii, v posledních letech se trend jejich adopce rozšiřuje i do Evropy, Severní Ameriky a dalších částí světa.

2.5.1 Globální expanze QR plateb

Vzhledem ke své jednoduchosti, nízkým implementačním nákladům a absenci nutnosti fyzického kontaktu se QR platby stávají atraktivní volbou pro malé a střední podniky, mobilní obchodníky i startupové fintech společnosti. Například podle údajů společnosti Juniper Research se očekává, že objem QR transakcí globálně přesáhne 3 biliony USD do

roku 2025, přičemž většina růstu bude pocházet z rozvojových trhů a rostoucí penetrace chytrých telefonů.

2.5.2 Integrace s novými technologiemi

QR kódy se stále častěji kombinují s dalšími inovativními technologiemi, jako je biometrická autentizace, umělá inteligence, blockchain nebo tokenizace platebních údajů, což přispívá ke zvýšení bezpečnosti i uživatelského komfortu. Některé moderní platformy umožňují například automatickou detekci QR kódu prostřednictvím fotoaparátu telefonu bez nutnosti aktivace specifické aplikace, což zvyšuje rychlost a plynulost platebního procesu.

2.5.3 Evropské iniciativy a tlak na nezávislost

Zásadní trend v evropském prostředí představuje snaha o nezávislost na globálních karetních gigantech, jako jsou Visa a Mastercard. Tento trend potvrzuje například i výrok prezidentky Evropské centrální banky Christine Lagarde, která v roce 2025 apelovala na potřebu vytvoření vlastního evropského platebního systému, jenž by nahradil dominanci amerických společností a posílil digitální suverenitu EU.

2.5.4 Národní standardizace a spolupráce

Dalším trendem je národní standardizace QR plateb, jako je tomu například v Indii (Bharat QR), Singapuru (SGQR) nebo Malajsii (Malaysia's DuitNow QR). Tyto iniciativy si kladou za cíl konsolidovat různá schémata do jednoho interoperabilního systému, čímž se zjednodušuje přístup pro obchodníky a spotřebitele a zároveň se zvyšuje přehlednost regulace a bezpečnost. Podobné kroky začínají podnikat i některé evropské státy – například Francie, Německo a Itálie pracují na společných standardech v rámci EPI (European Payments Initiative). [60] **Chyba! Nenalezen zdroj odkazů.** [59]

2.5.5 Budoucí vývoj

Do budoucna lze očekávat, že QR platby budou hrát stále důležitější roli v oblasti mikro plateb, bezkontaktního městského parkování, hromadné dopravy nebo peer-to-peer převodů. Významnou roli bude hrát také interoperabilita mezi bankovními systémy, fintech aplikacemi a globálními platformami (např. Apple Pay nebo Google Pay), které stále častěji začleňují QR technologie do svých systémů.

3 MEZINÁRODNÍ STANDARDY

Vzhledem k rychlému globálnímu rozvoji digitálních platebních metod, včetně těch založených na QR kódech, se ukazuje jako nezbytné zavádět jednotné mezinárodní standardy, které zajistí interoperabilitu, bezpečnost a důvěru napříč různými regiony, poskytovateli i koncovými uživateli. Standardizace umožňuje, aby QR platby mohly fungovat jednotně bez ohledu na technologického dodavatele, zemi původu nebo konkrétním zařízením koncového uživatele.

3.1 Standardy pro platební karty

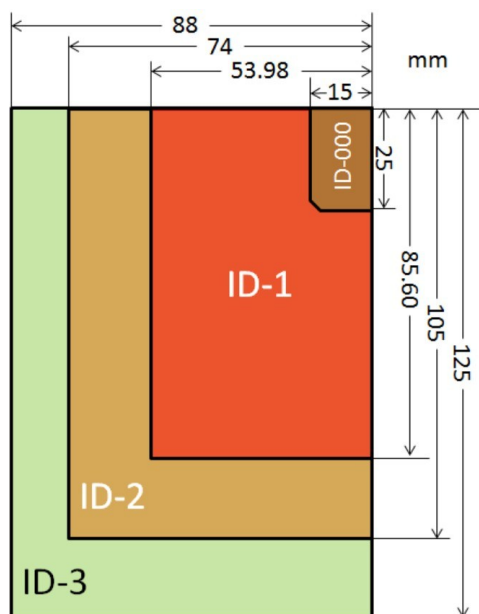
Platební karty zůstávají jedním z nejčastěji používaných nástrojů bezhotovostních plateb. Aby mohly fungovat napříč bankami, terminály a systémy po celém světě, bylo nutné zavést přísné technické a bezpečnostní standardy.

3.1.1 ISO normy

ISO (International Organization for Standardization) hraje významnou roli ve standardizaci fyzických i digitálních parametrů platebních karet. Například norma ISO/IEC 7810 definuje rozměry a fyzické vlastnosti ID karet včetně bankovních karet (viz Tabulka 1 a Obrázek 8). Norma ISO/IEC 7813 specifikuje magnetický proužek, strukturu údajů na kartě a další bezpečnostní prvky. Dále norma ISO/IEC 7816 upravuje komunikaci a strukturu čipových karet, které jsou dnes běžným standardem v oblasti plateb. [62] [63] [64]

Tabulka 1 Rozměry karet podle normy ISO 7810 [65]

Formát	Rozměry	Použití	Formát
ID-1	85.60 × 53.98 mm	Bankovní karty a identifikační (ID) karty	ID-1
ID-2	105 × 74 mm	Francouzské a další ID karty; Viza	ID-2
ID-3	125 × 88 mm	Pasy	ID-3
ID-000	25 × 15 mm	SIM karty	ID-000



Obrázek 8 Rozměry karet podle ISO 7810 [65]

3.1.2 EMV (Europay, Mastercard, Visa) standardy

Standard EMV vznikl jako společný projekt tří hlavních karetních společností (Europay, Mastercard a Visa) a slouží k zabezpečení platebních transakcí pomocí čipových karet. Zásadní výhodou je odolnost vůči podvodům, které byly u magnetických proužků častější.

Standard EMV definuje protokoly pro offline i online ověřování držitele karty (např. PIN nebo podpis), generování kryptografických dat a autentizaci transakcí. Dnes jsou EMV karty a kompatibilní terminály široce rozšířené po celém světě a představují základní kámen pro bezpečnou kartovou infrastrukturu. [66]

3.1.3 PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) je globální bezpečnostní standard, jehož cílem je chránit data držitelů platebních karet v rámci celého platebního procesu. Standard stanoví pravidla pro správu, ukládání, přenos a zabezpečení citlivých údajů, jako jsou čísla karet (PAN), CVV kódy a další.

Standard byl vytvořen Radou PCI SSC (Payment Card Industry Security Standards Council), kterou založily společnosti Visa, Mastercard, American Express, JCB a Discover. [67]

3.2 Komunikační protokoly pro karetní platby

Platební karty, ať už debetní, kreditní či předplacené, spoléhají na specifické komunikační protokoly, které umožňují bezpečný a spolehlivý přenos dat mezi kartou, platebním terminálem (POS) a zúčtovacím centrem.

3.2.1 SPDH (Standard Point of Sale Data Handling)

SPDH byl vyvinut v 80. letech firmou IBM a představoval proprietární standard pro výměnu dat mezi POS terminály a zúčtovacími systémy. Jedná se o binární protokol, který byl navržen pro potřeby maloobchodních řetězců. V dnešní době je SPDH na ústupu a většina implementací je nahrazena modernějšími standardy jako ISO 8583. [68]

3.2.2 ISO 8583

Nejrozšířenějším komunikačním protokolem pro karetní platby je ISO 8583, který definuje formát a způsob přenosu dat mezi jednotlivými komponenty platební infrastruktury. Každá transakce – např. žádost o autorizaci, potvrzení či storno – je reprezentována tzv. zprávou ISO 8583, jež obsahuje sadu datových polí, jako jsou identifikace transakce, číslo karty, částka, kryptografické údaje, apod. Tento standard tvoří základ mnoha současných zúčtovacích systémů a je podporován mezinárodními schématy jako VisaNet (Visa), Banknet (Mastercard) nebo domácími systémy, např. Česká bankovní asociace clearing. [69]

3.2.3 APDU

Na nižší úrovni, v přímé komunikaci mezi čipovou kartou a terminálem (např. při vkládání do čtečky), se používá protokol APDU (Application Protocol Data Unit), definovaný normou ISO/IEC 7816-4. Tento protokol umožňuje výměnu instrukcí mezi terminálem a bezpečnostními prvky čipu (např. autentizace nebo PIN ověření). Pro bezkontaktní platby (NFC) jsou APDU zprávy přenášeny rádiově prostřednictvím standardů ISO/IEC 14443. [70] [71]

3.2.4 Transportní vrstva a šifrování

Data mezi kartou, POS terminálem a back-end servery jsou přenášena přes šifrované spojení, typicky pomocí protokolu TLS (Transport Layer Security). To zajišťuje důvěrnost a integritu dat během přenosu, a chrání tak transakce před odposlechem či manipulací.

3.3 Standardy pro digitální platby a QR kódy

Stejně jako u platebních karet i zde u QR kódů je nezbytná standardizace pro zajištění bezpečné a interoperabilní infrastruktury, kterou si rozebereme níže.

3.3.1 ISO normy pro QR platby

Základem pro strukturu QR kódů je norma ISO/IEC 18004, která specifikuje formát, strukturu dat a kódování samotných QR kódů. Tato norma umožňuje jejich konzistentní generování a dekodování bez ohledu na zařízení nebo aplikaci, což je klíčové pro jejich využití v platebních systémech. [33]

3.3.2 EMV QR Code Specification

EMV QR Code Specification byla představena společností EMVCo v roce 2017 a definuje dva hlavní modely QR plateb:

- a) Merchant-Presented Mode (MPM): obchodník vygeneruje QR kód, který zákazník načte pomocí aplikace.
- b) Consumer-Presented Mode (CPM): zákazník generuje QR kód ve své aplikaci a ten je následně načten terminálem.

Cílem této specifikace je zajistit globální interoperabilitu mezi poskytovateli platebních služeb, bankami a obchodníky. [32]

3.3.3 Standardy pro mobilní a digitální platby

Vedle QR kódů existují také specifikace jako HCE (Host Card Emulation), NFC (Near Field Communication) nebo tokenizační standardy, které umožňují bezpečné mobilní platby prostřednictvím virtuálních karet. Standardy jsou často vyvíjeny v rámci organizací jako je GlobalPlatform, FIDO Alliance či přímo mobilními operačními systémy. [72] [73]

3.4 Regulační rámec a právní normy

Standardy v oblasti platebních technologií jsou úzce provázány s právními předpisy, které upravují bezpečnost, ochranu spotřebitele i interoperabilitu na trhu.

3.4.1 Evropské směrnice a právní normy

V Evropské unii je klíčovou legislativou Směrnice PSD2, která upravuje platební služby v rámci vnitřního trhu. PSD2 stanovuje pravidla pro otevřené bankovníctví, přístup třetích stran k bankovním účtům a posiluje ochranu spotřebitelů.

Dále je důležitá Směrnice NIS2, která ovlivňuje provozovatele kritické infrastruktury včetně poskytovatelů platebních služeb. [22]

3.4.2 Mezinárodní právní rámec

Mimo EU jsou platné různé regulační přístupy dle jurisdikce. Například ve Spojených státech reguluje oblast elektronických plateb zákon Electronic Fund Transfer Act (EFTA) a nařízení Regulation E vydané Fedem. Mezinárodní spolupráce v oblasti regulace probíhá také skrze organizace jako BIS (Bank for International Settlements) či FATF, které nastavují principy boje proti praní špinavých peněz a financování terorismu. [74] [75] [76]

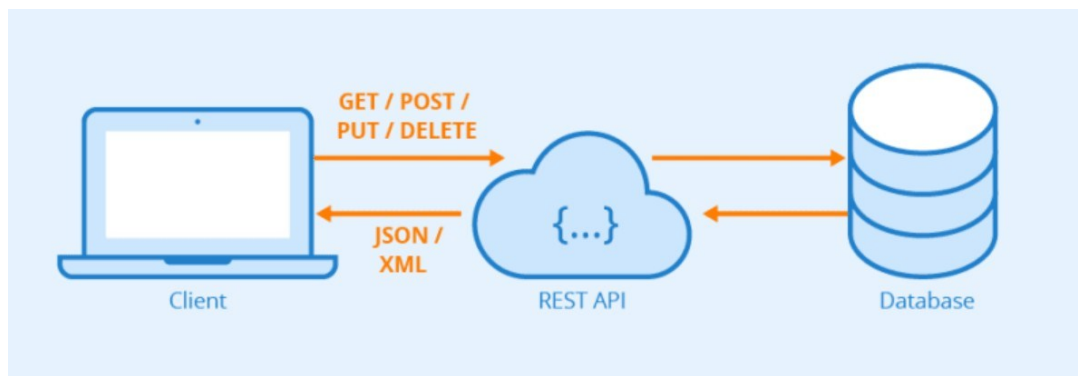
3.5 Komunikační protokoly pro QR platby

QR platby využívají odlišnou architekturu než tradiční karetní transakce. Komunikace probíhá často přes mobilní aplikaci a může se opírat jak o jednoduché HTTP REST API, tak o modernější a výkonnější systémy jako je gRPC, případně hybridní modely přenosu dat.

3.5.1 REST API a JSON formát

Mnoho poskytovatelů digitálních peněženek a platebních brán využívá komunikační architekturu založenou na REST (Representational State Transfer), která umožňuje interoperabilní přístup ke vzdáleným službám přes protokol HTTPS. Data jsou obvykle přenášena ve formátu JSON (JavaScript Object Notation), což přispívá k jednoduché integraci do webových i mobilních aplikací.

REST API umožňuje volání metod jako createPayment, confirmTransaction, nebo getPaymentStatus prostřednictvím URL dotazů, čímž dochází ke generování a zpracování QR kódů v reálném čase. [77]



Obrázek 9 REST API [79]

3.5.2 gRPC (Google Remote Procedure Call)

Novější architektury často nahrazují REST protokolem gRPC, který je efektivnější z hlediska latence a velikosti přenášených dat. gRPC využívá binární protokol Protocol Buffers a běží nad HTTP/2, což umožňuje vyšší efektivitu. Je typický v systémech využívajících mikroservisní architekturu a bývá preferován u systémů s vysokým zatížením nebo reálnými požadavky na odezvu.

Google Remote Procedure Call je moderní RPC framework s otevřeným zdrojovým kódem, který byl vyvinut společností Google. Je navržen pro komunikaci mezi distribuovanými systémy a umožňuje klientovi volat metody na vzdálených serverech jako by šlo o lokální volání funkcí. To značně zjednodušuje implementaci distribuovaných aplikací a přispívá k lepší udržitelnosti a čitelnosti kódu.

Základní princip fungování gRPC spočívá ve smluvně definovaném rozhraní Protocol Buffers. Toto rozhraní slouží k definici struktury zpráv a služeb, které jsou následně kompilovány do konkrétního programovacího jazyka (např. Java, Python). Komunikace probíhá prostřednictvím binárního formátu, což ve srovnání s textovým JSON formátem u REST API výrazně snižuje velikost přenášených dat a zvyšuje rychlost zpracování.

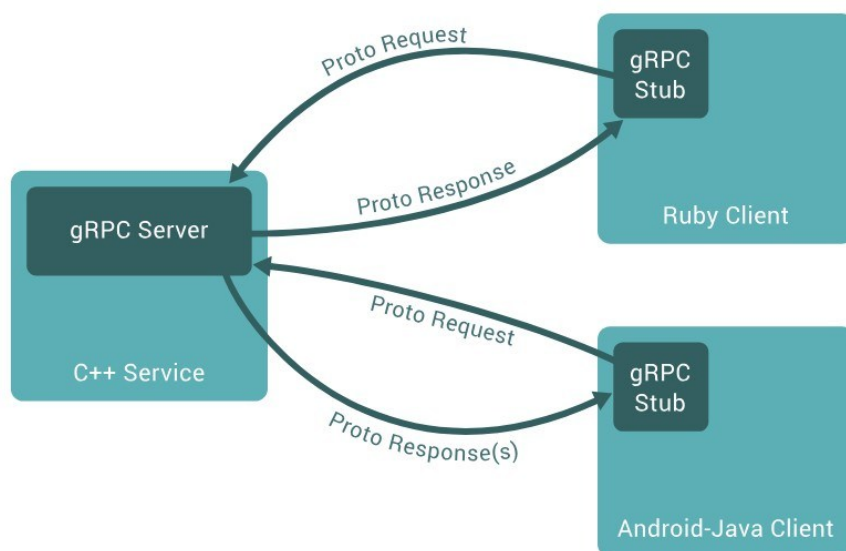
Díky využití protokolu HTTP/2 přináší gRPC řadu technických výhod: multiplexing (paralelní přenos více zpráv v rámci jedné TCP relace), streamování dat (v obou směrech – klient-server a server-klient), server push, a také efektivnější správu připojení. Tyto vlastnosti činí gRPC zvláště vhodným pro aplikace v reálném čase, jako jsou finanční transakce, IoT zařízení nebo strojové učení.

Další výhodou gRPC je jeho silná typová bezpečnost a automatická generace kódu, což zvyšuje produktivitu vývojářů a snižuje riziko chyb způsobených nesprávnou strukturou dat.

Tento přístup podporuje tvorbu dobře strukturovaných rozhraní mezi komponentami systému a usnadňuje verzování API.

Na druhou stranu je třeba zmínit, že gRPC může mít vyšší nároky na počáteční nastavení a vyžaduje podporu specifických nástrojů pro vývoj a ladění. Také ne všechny webové prohlížeče nativně podporují gRPC, což může komplikovat jeho použití ve frontendových aplikacích. Zde se často využívá přechodné řešení zvané gRPC-Web.

Z těchto důvodů je gRPC široce využíváno v prostředích, kde je klíčová výkonnost, škálovatelnost a modularita systému. Typicky v moderních cloudových infrastrukturách, mikroslužbách a finančních systémech s vysokým objemem transakcí. [78] [84]



Obrázek 10 gRPC [78]

3.5.3 Šifrování a bezpečnost přenosu

Transport Layer Security (TLS) je kryptografický protokol, který poskytuje důvěrnost, integritu a autentizaci při přenosu dat přes nezabezpečené sítě, jako je internet. V prostředí platebních služeb je TLS klíčový pro zajištění, že žádná třetí strana nebude schopna odposlechnout nebo změnit přenášené informace mezi klientem a serverem poskytovatele platební služby.

Moderní implementace TLS využívají silné šifrovací algoritmy jako AES a kryptografické hashovací funkce jako SHA-256. Pro výměnu klíčů a autentizaci serverů se používají metody, které zajišťují, že i v případě kompromitace jednoho klíče není možné dešifrovat historickou komunikaci.

Z hlediska implementace musí být všechny komponenty v platebním ekosystému správně nakonfigurovány, aby minimalizovaly zranitelnosti. Servery musí být vybaveny platnými digitálními certifikáty od důvěryhodných certifikačních autorit a musí správně implementovat ověřování certifikátu klientem.

Vzhledem k tomu, že QR platby se často realizují přes veřejné nebo mobilní sítě (např. Wi-Fi, LTE), je jejich zabezpečení ještě důležitější. Útoky typu man-in-the-middle mohou vést ke kompromitaci přenosu, pokud není důsledně používán TLS a nejsou zavedeny další kontrolní mechanismy, jako je ověření domény a kontrola integrity zpráv.

Celkově lze říci, že bezpečný přenos dat je zásadním předpokladem pro důvěryhodné fungování QR plateb. Implementace správného šifrování není pouze technickým požadavkem, ale také součástí regulatorních norem, jako jsou PSD2 a PCI DSS, které kladou důraz na ochranu osobních a finančních údajů během celého životního cyklu transakce.

4 SROVNÁNÍ PLATEBNÍCH KARET A QR PLATEB

Platební karty a QR platby představují dvě výrazně odlišné technologie, které mají společný cíl a to zajistit bezhotovostní převod peněžních prostředků mezi zákazníkem a obchodníkem. Přestože obě formy platby dosahují stejného výsledku, výrazně se liší jak na úrovni uživatelského zážitku, tak v otázkách infrastruktury, bezpečnosti a akceptačních modelů. V následující kapitole budou porovnány z hlediska pěti klíčových kritérií: rychlosti, uživatelského komfortu, bezpečnosti, ekonomické náročnosti na implementaci a míry akceptace na mezinárodním trhu.

4.1 Rychlost a uživatelský komfort

Jedním z nejdůležitějších faktorů ovlivňujících úspěšnost platebního řešení je uživatelský komfort, tedy celková přívětivost, intuitivnost a jednoduchost použití z pohledu koncového uživatele. S tím úzce souvisí také rychlost realizace transakce – ať už ve fyzickém prostředí (např. maloobchodní pokladna), nebo v prostředí digitálním (e-commerce, mobilní platby).

Platební karty, zejména ve své moderní bezkontaktní formě využívající technologii NFC, patří mezi nejpohodlnější a nejrychlejší platební nástroje. Samotný proces transakce často nevyžaduje více než pouhé přiložení karty k terminálu, v řadě případů bez potřeby zadávat PIN, pokud není překročena předem stanovený limit. Díky široké akceptační infrastruktuře a standardizovanému uživatelskému rozhraní je proces pro většinu zákazníků známý a předvídatelný. Významnou roli zde hraje i krátká doba odezvy terminálu, obvykle v řádu jednotek sekund.

Naopak QR platby fungují odlišným způsobem, kdy dochází k interakci mezi mobilním zařízením uživatele a vizuálním kódem zobrazeným obchodníkem nebo systémem. Princip spočívá v tom, že uživatel musí otevřít mobilní aplikaci svého poskytovatele plateb, naskenovat QR kód, případně zkontrolovat a potvrdit částku, a autorizovat platbu prostřednictvím biometrie nebo číselného kódu. Tento proces může být o několik sekund pomalejší než je platba kartou, a to zvláště pokud uživatel musí otevírat speciální aplikaci a ověřovat transakční detaily.

QR platby však vynikají v jiných aspektech uživatelské přívětivosti. Například při online platbách nebo v P2P prostředí umožňují rychlý převod mezi dvěma účty bez nutnosti znát čísla účtů nebo prepisovat dlouhé identifikátory. QR kód v sobě veškerá potřebná data již nese. Navíc jsou přístupné i bez fyzické karty.

V některých regionech, zejména v Asii jsou QR platby díky jejich jednoduché a nenákladné infrastruktuře považovány za dominantní platební metodu, a uživatelská veřejnost je na jejich použití zvyklá. V Evropě zatím představují spíše doplňkový platební kanál s potenciálem dalšího rozvoje.

Z hlediska rychlosti zpracování transakce nejsou mezi těmito metodami zásadní rozdíly. Vše závisí na interním systému poskytovatele a zapojených zúčtovacích institucích. Nicméně ve fyzickém kontaktu s platbou lze konstatovat, že bezkontaktní karty ve většině případů umožňují rychlejší obsluhu než QR skenování.

4.2 Bezpečnostní aspekty

Bezpečnost hraje v oblasti platebních metod klíčovou roli. Platební transakce zprostředkovávají přenos citlivých dat, jako jsou údaje o platební kartě, bankovním účtu, identita uživatele či potvrzení o autorizaci. Zabezpečení těchto informací je nezbytné pro ochranu proti podvodům, zneužití a zajištění důvěry koncových uživatelů. Platební karty a QR platby přistupují k bezpečnosti odlišně. Každá metoda má svá specifika, výhody i slabiny.

4.2.1 Riziko zneužití údajů při transakci

Platební karty, zejména v online prostředí, čelí dlouhodobě vyššímu riziku zneužití údajů. Zejména u tzv. card-not-present transakcí. Útočníkovi často postačí získat číslo karty, datum expirace a CVV kód, aby mohl provést neoprávněnou platbu. Přestože zavedení silné autentizace dle směrnice PSD2 významně snížilo tento typ útoku, riziko zůstává relevantní.

Naproti tomu u QR plateb nedochází k přímému přenosu citlivých údajů. Informace zakódované v QR kódu typicky obsahují pouze identifikátor obchodníka a částku, samotná platba je realizována uvnitř zabezpečené aplikace uživatele. To významně snižuje atraktivitu těchto transakcí pro klasické formy datových útoků.

4.2.2 Vektor útoku a kontrola uživatele

QR platby posilují bezpečnost tím, že uživatel sám aktivně potvrzuje každou transakci na svém zařízení. Platba je tedy realizována pouze tehdy, pokud uživatel daný QR kód nasnímá a schválí, často za použití biometrického ověření. Tím se minimalizuje riziko neautorizovaných plateb např. v důsledku ztráty nebo krádeže platebního prostředku.

Naopak u bezkontaktních plateb kartou je možné provést transakci do určité částky i bez PIN kódu, což může v případě fyzické ztráty karty představovat bezpečnostní riziko. Ačkoliv moderní systémy umožňují rychlou blokaci karty, nežádoucí transakce může být mezitím autorizována.

4.2.3 Technologická zranitelnost a vnější hrozby

Platební karty, zvláště starší typy s magnetickým proužkem, byly v minulosti zranitelné vůči technikám jako skimming nebo útokům na POS terminály. Dnes jsou tyto hrozby výrazně redukovány čipovou technologií EMV a síťovými standardy PCI DSS. Přesto zůstávají obchodníci zodpovědní za správnou implementaci bezpečnostních politik, což může být problematické u menších podniků.

QR platby jsou zase náchylné na tzv. quishing, kdy útočník podvrhne falešný QR kód a přesměruje uživatele na podvodný odkaz nebo ho přiměje autorizovat falešnou platbu. Tento typ útoku lze ztížit použitím dynamických kódů, kryptografických podpisů nebo silnou vizuální identifikací důvěryhodných značek. Zůstává ale výzvou především v případě statických nálepek.

4.2.4 Regulační rámec a standardizace

Platební karty jsou pevně ukotveny v mezinárodních standardech a regulacích, které definují jasné povinnosti pro vydavatele, poskytovatele infrastruktury i obchodníky. Bezpečnostní opatření jsou tak dobře kontrolovatelná.

QR platby naproti tomu dosud postrádají jednotný globální rámec. Standardizace a bezpečnostní doporučení existují, ale jejich implementace je v mnoha regionech roztržštěná. Regulace je často v rukou jednotlivých států nebo soukromých iniciativ, což vytváří riziko nejednotnosti v zabezpečení.

4.2.5 Závěr komparace

Platební karty nabízejí vysokou úroveň bezpečnosti díky standardizovanému a kontrolovanému prostředí, ale zůstávají zranitelné při ztrátě fyzické karty nebo při útocích na online platby. QR platby poskytují silnou bezpečnost díky decentralizaci, biometrickému ověření a absenci přenosu citlivých údajů, ale čelí novým formám útoků spojeným s manipulací vizuálními kódy.

4.3 Dostupnost a implementační náklady pro obchodníky

Dostupnost platebních metod a jejich implementační náklady jsou jedním z klíčových faktorů, které ovlivňují rozhodování obchodníků při volbě akceptovaných platebních kanálů. Rozdíly mezi platebními kartami a QR platbami jsou v tomto ohledu značné, ať už jde o technické, nákladové, nebo administrativní aspekty.

4.3.1 Platební karty (zavedený standard s vyššími počátečními náklady)

Přijetí platebních karet vyžaduje od obchodníka určité investice do infrastruktury, zejména pořízení a správu platebního terminálu (POS zařízení). Tato zařízení jsou většinou pronajímána od poskytovatelů platebních služeb, přičemž měsíční náklady závisí na typu terminálu, funkcionalitách a rozsahu služeb. Dalším nákladovým faktorem je transakční poplatek, který si účtuje poskytovatel platebního řešení

Z provozního hlediska představuje systém platebních karet poměrně stabilní a robustní řešení, nicméně jeho zprovoznění může být pro malé podnikatele nákladné a administrativně zatěžující. Některé menší obchodníky tak může odradit jak výše fixních nákladů, tak relativně složitý proces certifikace a napojení na systémy poskytovatelů.

4.3.2 QR platby (nízkonákladová a flexibilní alternativa)

QR platby se oproti tradičním karetním metodám vyznačují výrazně nižšími vstupními náklady. V základní podobě obchodník nepotřebuje žádný specializovaný hardware, postačí mu tak tištěný nebo digitální QR kód, který zákazník nasnímá svým mobilním telefonem. Generování a použití QR kódů je typicky bezplatné, a některé aplikace poskytují obchodníkům tento nástroj bez jakýchkoli poplatků.

Transakční náklady u QR plateb se liší podle poskytovatele, ale bývají obecně nižší než u karet. To činí QR platby obzvláště atraktivními pro malé podniky, trhy a poskytovatele služeb v místech bez terminálové infrastruktury.

Další výhodou je jednoduchost integrace. Nasazení QR plateb nevyžaduje certifikaci platebního zařízení, schválení karetními asociacemi ani složitou smluvní dokumentaci. V některých případech lze QR platby začít akceptovat během několika minut.

4.3.3 Závěr komparace

Z pohledu obchodníků jsou QR platby spojeny s nižšími vstupními i provozními náklady, menší administrativní zátěží a rychlejší implementací. Platební karty na druhé straně nabízejí

vysokou míru důvěryhodnosti a širokou zákaznickou základnu, což z nich činí preferovanou volbu zejména v maloobchodních provozovnách. Výběr mezi těmito metodami by tak měl zohlednit nejen nákladovou stránku, ale i charakter obchodního modelu a očekávání zákazníků.

4.4 Akceptace na globálním trhu a regionální rozdíly

Akceptace různých platebních metod se v globálním měřítku výrazně liší v závislosti na regionálních ekonomických podmínkách, úrovni digitalizace, nákupních zvyklostech spotřebitelů i míře důvěry k jednotlivým typům finančních institucí. Platební karty a QR platby se z tohoto hlediska nacházejí v odlišných fázích rozšíření a technologického přijetí. Zatímco platební karty představují globálně zavedený standard, QR platby zažívají dynamický růst především v rozvíjejících se ekonomikách a mobilně orientovaných trzích.

Platební karty jsou v současnosti jedním z nejrozšířenějších bezhotovostních platebních nástrojů, a to zejména v zemích s vyspělou infrastrukturou pro zpracování plateb – tedy v Severní Americe, Evropě, Japonsku, Jižní Koreji a Austrálii. V těchto regionech je akceptace platebních karet téměř univerzální, ať už v kamenných prodejnách, online prostředí nebo v oblasti služeb. Je však třeba dodat, že i přes globální rozšíření existují země a regiony, kde je přístup ke kartovým schémátům omezený.

Naopak QR platby dosáhly největšího rozmachu v Asijském regionu, kde se staly dominantní metodou elektronických transakcí zejména v zemích jako Čína, Indie, Thajsko nebo Indonésie. V Číně tvoří QR platby páteř maloobchodních transakcí. Díky nízkým nákladům, jednoduchosti a integraci s bankovními účty jsou QR platby v těchto zemích preferovaným způsobem každodenních transakcí, od pouličních prodejců po velké obchodní řetězce. Na rozdíl od Asie je přijetí QR plateb v Evropě a Severní Americe zatím spíše omezené a rozvíjí se pomalejším tempem. V těchto regionech dominuje kartový ekosystém podporovaný dlouhodobými investicemi do infrastruktury a důvěrou spotřebitelů i obchodníků v bezpečnost a spolehlivost karetních transakcí.

Zatímco platební karty zůstávají základním pilířem globálních bezhotovostních plateb, QR platby se staly flexibilní a nákladově efektivní alternativou v regionech s vysokou penetrací chytrých telefonů a slabší terminálovou infrastrukturou. Regionální rozdíly v akceptaci nejsou jen technologického rázu, ale také výsledkem kulturních, ekonomických a regulatorních faktorů. Do budoucna lze očekávat, že QR platby budou i v Evropě a Severní Americe nabývat na významu.

4.5 Environmentální dopad platebních metod

V souvislosti s rostoucím tlakem na udržitelnost a společenskou odpovědnost podniků se i oblast platebních metod dostává do centra pozornosti z hlediska svého environmentálního dopadu. Ačkoli jsou platby vnímány převážně jako digitální služba, fyzické aspekty některých platebních nástrojů, zejména plastových platebních karet, představují nezanedbatelnou zátěž pro životní prostředí.

4.5.1 Výroba a životní cyklus platebních karet

V současné době je globálně v oběhu více než 25 miliard platebních karet a ročně jich je nově vyrobeno přibližně 6 miliard. Drtivá většina těchto karet je produkována z tzv. „panenského“ polyvinylchloridu (PVC), který se vyrábí z fosilních surovin, zejména ropy. Tento materiál je sice levný a odolný, avšak zároveň ekologicky problematický, a to jak z hlediska emisní stopy při výrobě, tak i z hlediska komplikované likvidace na konci životního cyklu. Platební karta standardního typu má průměrnou životnost přibližně 3 až 5 let a poté je zpravidla skartována a uložena na skládku nebo spálena, přičemž recyklace je zatím v praxi realizována jen minimálně.

Výroba platební karty zahrnuje několik energeticky náročných fází: výrobu plastového substrátu, tisk a personalizaci, integraci čipu nebo magnetického proužku, laminaci, testování a balení. Tento proces je dále zatížen emisemi skleníkových plynů, spotřebou vody, chemikálií a generováním výrobního odpadu. Největší podíl environmentální zátěže přitom připadá na počáteční fázi výroby materiálu a následně na jeho zpracování.

V reakci na tyto problémy byla v roce 2018 založena iniciativa Greener Payments Partnership (GPP), kterou vede společnost Mastercard ve spolupráci s klíčovými technologickými partnery v oblasti karetních technologií (např. IDEMIA, Thales, G+D). Cílem této iniciativy je minimalizovat ekologickou stopu platebních karet prostřednictvím přechodu na alternativní materiály a zavedení principů cirkulární ekonomiky.

Podle odhadů Mastercard by přechod na ekologičtější materiály umožnil každoročně eliminovat až 16 000 tun emisí CO₂, což odpovídá emisím přibližně 3 500 osobních automobilů. Z pohledu cirkulární ekonomiky se navíc snižuje i množství odpadu a snižuje tlak na spotřebu primárních surovin.

Navzdory nesporným výhodám však implementace ekologických karetních řešení čelí několika výzvám. Patří mezi ně vyšší výrobní náklady na jednotku, omezená globální

dostupnost certifikovaných materiálů, nižší odolnost některých ekologických alternativ a potřeba nových výrobních technologií. Navíc je třeba řešit i otázku certifikace bezpečnostních parametrů těchto alternativních karet, zejména v kontextu standardů EMV a PCI DSS. **Chyba! Nenalezen zdroj odkazů.**

4.5.2 Ekologické alternativy a inovace

V reakci na výše uvedené skutečnosti některé karetní společnosti a banky zavádějí ekologičtější varianty platebních karet. Mezi tyto iniciativy patří například karty z recyklovaného plastu, biologicky rozložitelné karty, digitální karty. Tyto alternativy snižují ekologickou zátěž, avšak stále narážejí na otázku širší akceptace, výrobní ceny a nutnosti fyzické přítomnosti karty v určitých situacích.

4.5.3 QR platby a jejich environmentální profil

Digitální platební metody založené na QR kódech, zejména ty provozované prostřednictvím mobilních zařízení, se vyznačují podstatně nižší materiálovou a logistickou náročností. Uživatel k provedení platby využívá stávající zařízení (mobilní telefon), které nevyžaduje speciální fyzickou infrastrukturu jako čtečky karet nebo plastové médium.

QR platby rovněž eliminují potřebu tisknout účtenky a snižují spotřebu papíru a toneru. Dále není nutné distribuovat fyzické terminály obchodníkům, což z pohledu emisní a materiálové stopy znamená zásadní přínos, zejména v rozvojových oblastech, kde by jinak bylo nutné zavádět nákladnou infrastrukturu.

Je však důležité poznamenat, že i digitální technologie mají svůj ekologický dopad. Spotřeba energie mobilních zařízení, datových center a přenosové infrastruktury se promítá do celkové uhlíkové stopy, byť v absolutních číslech je tento dopad v přepočtu na jednotlivou transakci výrazně nižší než u karet.

4.5.4 Směr vývoje a udržitelná budoucnost plateb

Vzhledem k výše uvedeným aspektům lze očekávat, že v budoucnu dojde k dalšímu posunu směrem k udržitelnějším platebním metodám. Trend digitalizace spolu s tlakem na ESG (Environmental, Social, and Governance) reporting vede banky a fintech společnosti k tomu, aby investovaly do zelených inovací. Příkladem je iniciativa Green Payments Alliance, která si klade za cíl vytvořit rámec pro měření a snižování uhlíkové stopy digitálních platebních systémů.

Z dlouhodobého hlediska by mohly být QR platby, případně tokenizované digitální platby na bázi chytrých zařízení, preferovaným standardem nejen z pohledu pohodlí a bezpečnosti, ale i environmentální udržitelnosti. Tento vývoj však závisí na úrovni digitalizace společnosti, dostupnosti technologií a regulační podpoře.

II PRAKTICKÁ ČÁST

5 POUŽITÉ TECHNOLOGIE A VÝVOJOVÉ PROSTŘEDÍ

Tato kapitola se zaměřuje na popis vývojových nástrojů, programovacího jazyka, frameworku a komunikačních technologií, které byly využity při návrhu a vývoji systému v rámci praktické části této diplomové práce. Cílem je objasnit důvody výběru konkrétních nástrojů a jejich přínos pro efektivní a bezpečnou implementaci podpory QR plateb do stávajícího systému podporujícího platební karty.

5.1 Vývojové prostředí a nástroje

Pro implementaci řešení byly zvoleny vývojové nástroje, které umožňují efektivní vývoj, testování a ladění aplikace.

5.1.1 IntelliJ IDEA

IntelliJ IDEA představuje jedno z nejpoužívanějších integrovaných vývojových prostředí (IDE) pro vývoj v jazyce Java. Nabízí širokou škálu funkcí, jako je automatické doplňování kódu, kontrola syntaxe v reálném čase, refaktoring, integrovaná správa verzí a pokročilé nástroje pro práci s frameworky jako je Spring Boot. Použití IntelliJ IDEA zefektivňuje vývoj aplikace, zvyšuje produktivitu vývojáře a podporuje moderní softwarové inženýrství.

5.1.2 Postman

Postman je populární nástroj pro testování a validaci REST API. Umožňuje simulaci HTTP požadavků, sledování odpovědí serveru, testování funkcionality endpointů a ověřování bezpečnostních mechanismů. Byl použit při vývoji backendových služeb pro ověřování správné komunikace mezi klientskými částmi aplikace a serverem, a to především během vývoje platební logiky.

5.1.3 Windows

Vývoj probíhal v operačním systému Microsoft Windows 11, který zajišťuje kompatibilitu s širokou škálou vývojových nástrojů a zároveň nabízí stabilní prostředí. Prostředí bylo navrženo tak, aby reflektovalo běžné provozní podmínky moderního vývoje.

5.2 Programovací jazyk a framework

K implementaci aplikace byl zvolen programovací jazyk Java v kombinaci s frameworkem Spring Boot. Tato volba reflektuje potřebu robustního, bezpečného a škálovatelného řešení pro backendovou část systému.

5.2.1 Java

Java je objektově orientovaný, multiplatformní jazyk, který je široce využíván při vývoji podnikových systémů, zejména v oblasti finančních služeb. Je známý pro svou stabilitu, silný typový systém, rozsáhlou knihovni podporu a širokou komunitu. Díky podpoře Javy ze strany velkých korporací je zajištěna dlouhodobá udržitelnost řešení. [85]

5.2.2 Spring Boot

Spring Boot je rozšířením populárního frameworku Spring a slouží ke zjednodušení vývoje aplikací pomocí přednastavených konfigurací. Umožňuje rychlý vývoj REST API služeb, integraci s databázemi, zajištění bezpečnostních mechanismů (např. pomocí Spring Security) a podporuje modulární architekturu. V rámci této práce byl použit pro vývoj serverové části aplikace a správu aplikační logiky. [82]

5.3 Komunikace a integrace

Pro zajištění komunikace mezi jednotlivými komponentami systému byly použity moderní integrační technologie, které reflektují současné trendy v oblasti vývoje distribuovaných systémů.

5.3.1 REST API

REST (Representational State Transfer) API je architektonický styl pro návrh webových služeb. Umožňuje jednoduchou a přehlednou komunikaci mezi klientem a serverem pomocí standardních HTTP metod. V rámci této práce je REST API klíčovým prvkem pro spojení poskytovatele plateb s backendem. [82]

5.3.2 gRPC

gRPC (Google Remote Procedure Call) je moderní open-source rámec pro vzdálené volání procedur založený na protokolu HTTP/2 a protokolu Protobuf (Protocol Buffers). Nabízí vysoký výkon, efektivní serializaci dat a podporu pro více jazyků. gRPC byl zvažován jako alternativa k REST pro případné vnitřní mikroslužby, zejména z důvodu své efektivity v prostředí s nízkou latencí a vysokým objemem transakcí. [82]

5.3.3 Alipay

Alipay představuje poskytovatele platebních bran a řešení pro zpracování online plateb. V této práci byl použit jako příklad reálné integrace s externím platebním systémem

prostřednictvím REST API. Altapay umožňuje realizaci online plateb kartou, QR platby, sledování stavu transakcí, provádění refundací a správu obchodních toků, což z něj činí robustní a bezpečné řešení pro online platby.

6 EKOSYSTÉM PRO IMPLEMENTACI

Tato kapitola popisuje softwarové a technologické prostředí, ve kterém byla realizována praktická část diplomové práce. Konkrétně se jedná o vývoj a úpravu služeb v rámci infrastruktury společnosti Monet+, která se dlouhodobě specializuje na vývoj řešení v oblasti digitálních plateb, elektronické identifikace a bezpečnosti transakcí.

Vzhledem k důvěrnosti vnitřní architektury a použitých systémů nebude některý kód ani architektura popsána detailně, ale pro účely této práce budou uvedeny úpravy v zobecněné a přístupné podobě. Cílem je demonstrovat praktické aspekty vývoje v prostředí firmy zabývající se digitálními platbami a ukázat způsob nasazení moderních technologií.

6.1 Monet+

Společnost Monet+ je předním českým dodavatelem technologií v oblasti bezpečných elektronických transakcí. Její produkty a řešení se používají ve finančním sektoru, veřejné správě a dalších odvětvích, kde je vyžadována vysoká úroveň zabezpečení a důvěryhodnosti.

Ve vývojovém procesu klade Monet+ důraz na škálovatelnou architekturu, bezpečnost dat, modulární design a schopnost adaptace na regulativní rámce. Během vývoje této diplomové práce byl klíčový kontakt s vývojovým týmem společnosti, který poskytl technickou podporu a umožnil zapojení do konkrétních úkolů souvisejících s implementací digitálních platebních metod.

6.2 SmartSwitch

SmartSwitch představuje směrovací a transakčně orientovaný systém, který slouží jako klíčový prostředník mezi jednotlivými službami v rámci ekosystému platebních řešení. Tento systém umožňuje efektivní směrování požadavků.

Je navržen jako vysoce modulární a rozšiřitelný, což umožňuje pružně reagovat na nové požadavky trhu, změny v regulaci nebo specifika různých typů transakcí. V rámci diplomové práce bylo možné analyzovat způsob konfigurace směrovacích pravidel, jejich vyhodnocování a propojení s aplikačními službami.

SmartSwitch podporuje připojení prostřednictvím různých komunikačních protokolů, čímž zajišťuje interoperabilitu mezi staršími a moderními systémy. Díky tomu slouží jako důležitá integrační vrstva v architektuře společnosti Monet+.

6.3 Mikroservisní architektura

Jedním z hlavních architektonických principů používaných v rámci implementačního prostředí Monet+ je mikroservisní architektura. Tento přístup spočívá v rozdělení systému na menší, nezávislé komponenty (mikroslužby – anglicky „microservice“), které spolu komunikují prostřednictvím definovaných API rozhraní, nebo pomocí protokolu gRPC. Každá mikroslužba je zodpovědná za konkrétní doménovou funkcionalitu a může být vyvíjena, testována, nasazována a škálována nezávisle na ostatních částech systému. [83]

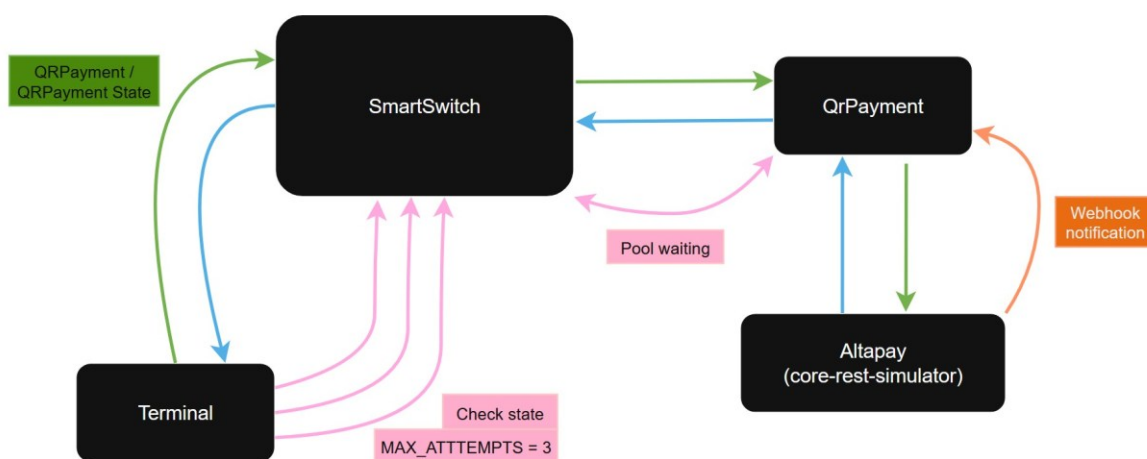
V rámci práce byl modifikován již existující kód, který je součástí modulu SMSW (SmartSwitch) a byla vytvořena nová mikroslužba, která slouží jako pomyslný most mezi již zmiňovaným SMSW a externím poskytovatelem QR plateb, přičemž byly respektovány interní standardy společnosti týkající se logování, bezpečnosti a struktury kódu. Ukázkové části kódu uvedené v další části práce jsou částečně anonymizovány nebo upraveny tak, aby neporušovaly firemní tajemství.

7 NÁVRH ARCHITKTURY

V této kapitole je podrobně popsán návrh architektury rozšíření systému pro podporu plateb pomocí QR kódů, implementovaný v rámci firmy Monet+. Cílem bylo rozšířit stávající infrastrukturu SmartSwitch (dále jen SMSW) o novou službu umožňující bezproblémové zpracování QR plateb, a to při zachování vysoké úrovně robustnosti, škálovatelnosti a bezpečnosti celého řešení.

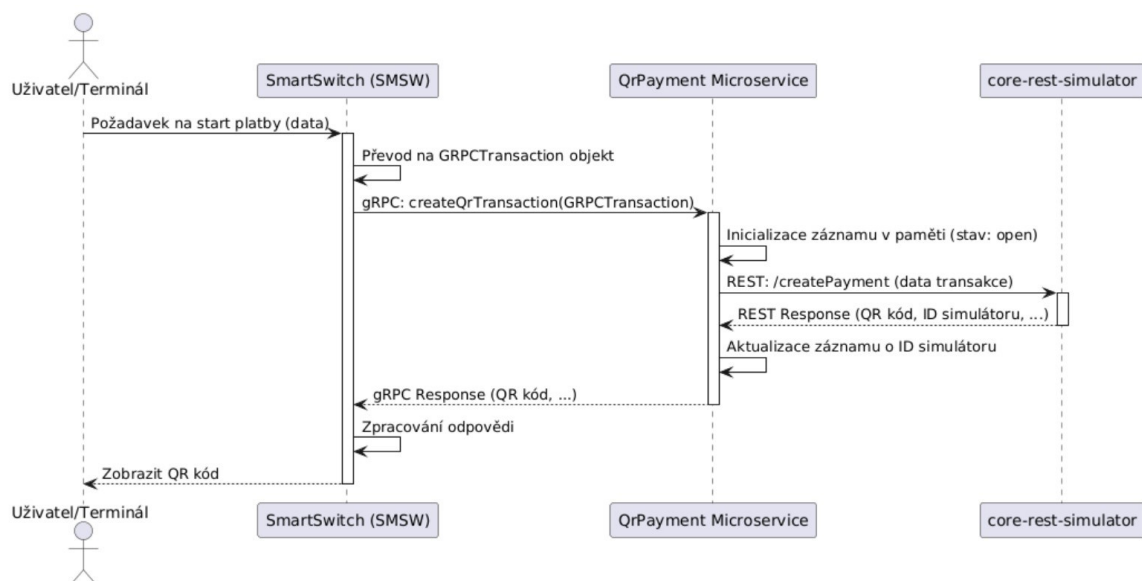
Existující architektura systému SMSW je založena na modulárním zpracování transakcí prostřednictvím kanálů (Inchannel a Outchannel) a přímé komunikaci se systémy třetích stran. Úkolem bylo integrovat podporu pro QR platby s minimálními zásahy do existujícího jádra systému a zároveň navrhnout komponentu, která umožní snadnou budoucí rozšiřitelnost a správu.

Návrh architektury systému pro zpracování QR plateb vychází ze snahy co nejméně zasahovat do stávající infrastruktury SMSW a zároveň umožnit robustní a bezpečné zpracování nového typu transakcí. Celé řešení je postaveno na myšlence zavedení samostatné mikroservisy s názvem QrPayment, která přebírá odpovědnost za obsluhu QR platebních transakcí. Komunikace mezi SMSW a QrPayment je realizována pomocí efektivního binárního protokolu gRPC, což zajišťuje nízkou latenci a vysokou propustnost přenášených zpráv.



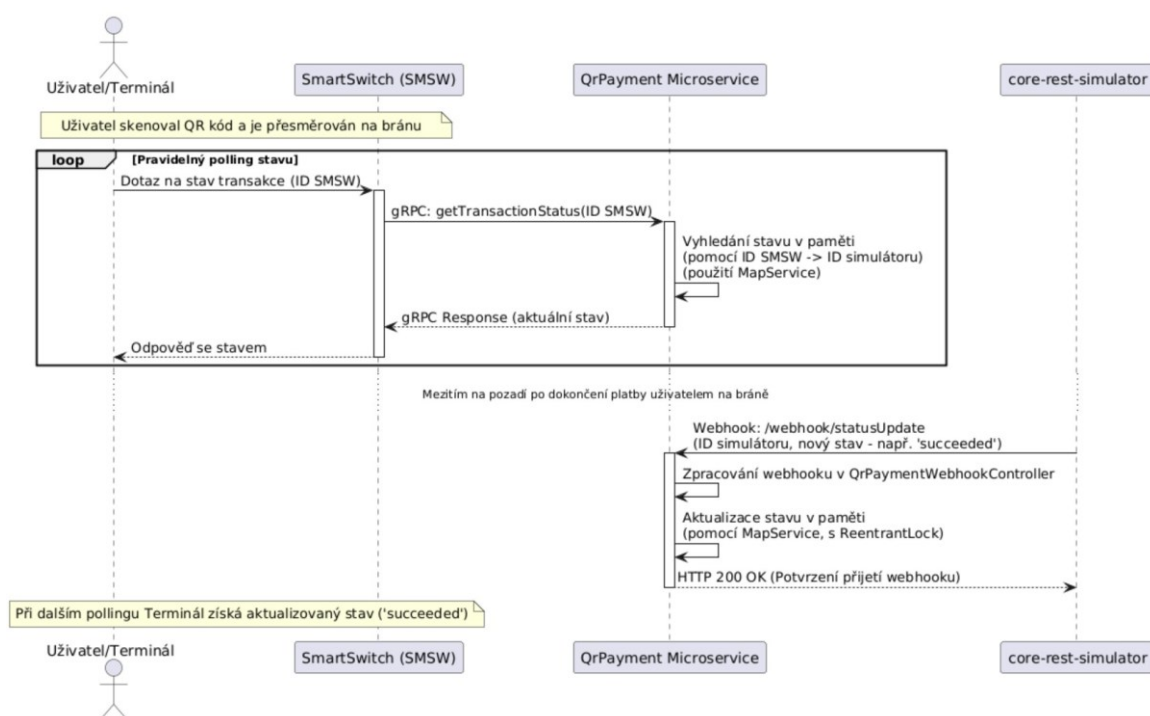
Obrázek 11 Zjednodušený digram procesu QR platby

(zdroj: vlastní)



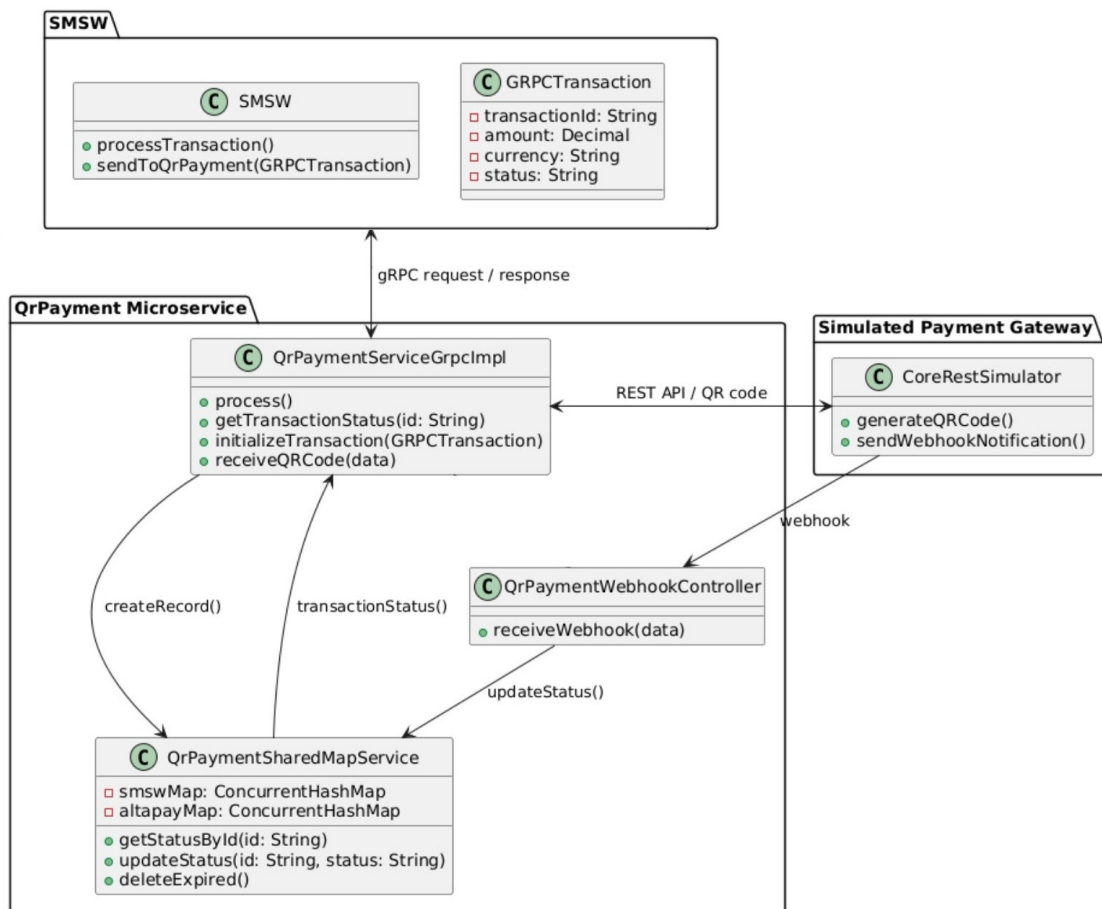
Obrázek 12 Sekvenční diagram: Zahájení QR platby

(zdroj: vlastní)



Obrázek 13 Sekvenční diagram: Dotazování na stav QR platby + webhook

(zdroj: vlastní)



Obrázek 14 Ukázka diagramu tříd: QrPayment + SMSW

(zdroj: vlastní)

7.1 Celkový tok transakce

Celý proces zpracování QR platby začíná ve chvíli, kdy uživatel na platebním terminálu (nebo při testování v prostředí Postman) odešle požadavek na zahájení platební transakce s cílem zobrazit QR kód. Terminál (Postman) odešle požadavek na SMSW, který ho po zpracování v interních modulech převede na objekt typu `GRPCTransaction`. Tento objekt obsahuje všechny potřebné údaje pro další práci s transakcí, včetně unikátního identifikátoru, částky, měny a dalších parametrů.

SMSW následně odešle tento `GRPCTransaction` objekt do služby `QrPayment` prostřednictvím gRPC rozhraní. Po přijetí transakce služba `QrPayment` inicializuje nový záznam seznamu, kde uchovává informace o dané transakci, a provede volání na simulátor externí platební brány, tedy na službu `core-rest-simulator`. Tento simulátor, který v produkčním prostředí nahrazuje reálného poskytovatele Altapay, vytvoří odpověď obsahující QR kód a další nezbytné údaje, které jsou vráceny zpět skrze `QrPayment` do

SMSW. Následně je QR kód předán zpět na platební terminál, kde je uživateli zobrazen k naskenování.

Po naskenování QR kódu a přesměrování uživatele na platební bránu je potřeba sledovat průběh platby. Terminál proto začne v pravidelných intervalech zasílat dotazy na stav transakce do SMSW. Ten opět využívá komunikaci pomocí gRPC a přeposílá požadavky do služby QrPayment, která podle aktuálně uloženého stavu transakce odpovídá. Na konkrétní transakce se dotazujeme pomocí unikátního identifikátoru, který je vytvořen během procesu přesměrování ve službě SMSW. Během tohoto procesu je stav transakce v QrPayment postupně aktualizován na základě webhook notifikací, zaslané core-rest-simulátorem, který tak simuluje reálné chování platební brány.

7.2 Struktura systému

Hlavní komponentou systému, která zajišťuje práci s QR platbami, je služba QrPayment. Tato služba je navržena jako samostatná mikroservisa, aby byla zajištěna nezávislost, snadné škálování a jednoduchá správa jednotlivých částí systému. Uvnitř služby QrPayment se nachází několik klíčových částí, které spolu úzce spolupracují.

První důležitou součástí je třída QrPaymentWebhookController, která je zodpovědná za příjem příchozích webhook notifikací. Přijatá informace webhookem obsahuje informace o změně stavu platby a po jejich přijetí controller aktualizuje odpovídající záznam transakce v interní mapové struktuře.

Druhou klíčovou komponentou je QrPaymentSharedMapService. Tato serviska obsahuje dvě thread-safe mapy typu ConcurrentHashMap. První mapa obsahuje identifikátor transakce z pohledu SMSW a odkaz na druhou mapu, která obsahuje identifikátor transakce z pohledu Altapay simulátoru, kde jsou uchovávány stavy všech aktuálních transakcí. Vzhledem k požadavku na zajištění konzistence dat i při souběžném přístupu z více vláken, je zde využita synchronizační technika pomocí ReentrantLock, která umožňuje řídit přístup při zápisu i čtení.

Další důležitou částí je implementace gRPC serveru prostřednictvím třídy QrPaymentServiceGrpcImpl. Tento server přijímá volání od SMSW, zpracovává příchozí požadavky na zahájení nové transakce nebo na dotazy ohledně stavu existujících transakcí a odpovídá dle aktuálních údajů uložených v paměti.

Pro správu paměťové náročnosti systému a eliminaci starých transakcí, které nebyly ukončeny standardním způsobem (například kvůli chybě při komunikaci), je v QrPayment implementován také scheduler. Tento plánovač v pravidelných intervalech prochází uložené záznamy a maže ty, které jsou starší než stanovená expirační doba. Odstraňování záznamů je implementováno tak, aby nedošlo k mazání záznamů, které jsou aktuálně používány.

Simulace externího systému je řešena prostřednictvím služby core-rest-simulator. Tento simulátor vystavuje REST API, které emuluje chování reálné platební brány Altapay. Po obdržení požadavku vygeneruje QR kód, který následně odešle zpět a v momentě dokončení platby ze strany uživatele odešle webhook notifikaci s výsledkem transakce do služby QrPayment.

7.3 Práce se stavy transakcí

Každá transakce v systému QrPayment prochází několika možnými stavy. V okamžiku vytvoření je transakce nastavena do stavu open, což značí, že QR kód byl vygenerován a čeká se na akci ze strany uživatele. Během této fáze terminál v pravidelných intervalech zasílá dotazy na stav transakce. Pokud dojde ke správnému dokončení platby, je transakce přes webhook aktualizována do stavu succeeded. Tento stav značí, že platba byla úspěšně provedena a proces je kompletní.

Kromě těchto hlavních stavů systém pracuje i s chybovými stavy, například error, failed, canceled, incomplete nebo unknown. Tyto stavy jsou vyhrazeny pro případné výjimečné situace, například při selhání komunikace nebo neočekávaném průběhu transakce, a jejich plná podpora je plánována v rámci budoucího rozšíření systému.

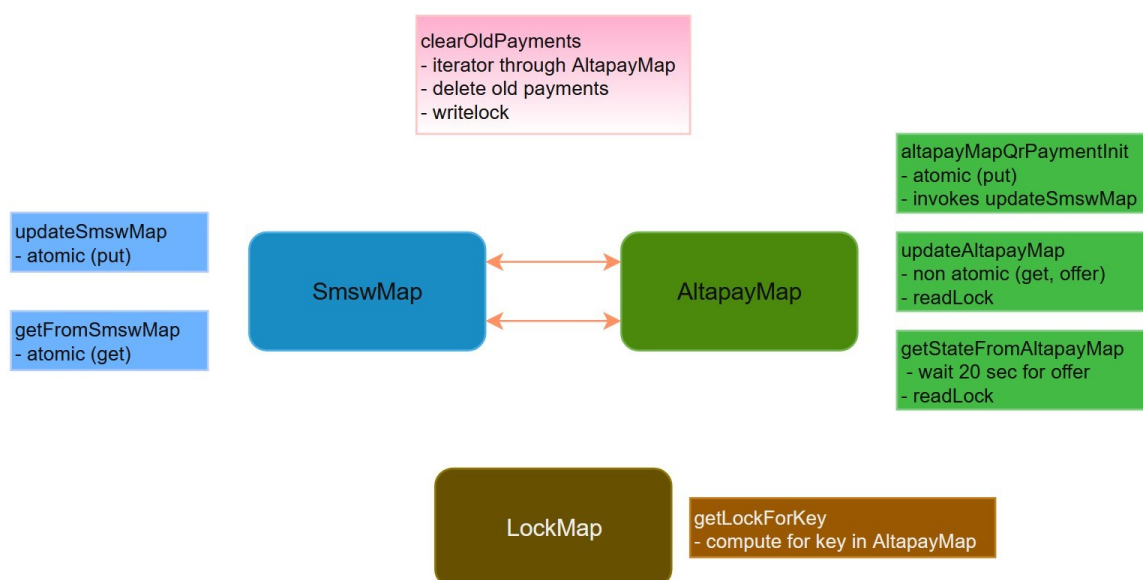
Stav transakce je možné měnit dvěma způsoby. Prvním způsobem je pravidelný polling z terminálu, kdy klient v definovaných intervalech žádá o aktuální stav. Druhým způsobem, který je rychlejší a efektivnější, je asynchronní aktualizace pomocí webhook notifikací. Jakmile core-rest-simulator odešle notifikaci o změně stavu, je záznam o transakci v paměti služby QrPayment okamžitě aktualizován.

7.4 Synchronizace a ochrana proti souběhu

Vzhledem k tomu, že služba QrPayment pracuje s asynchronními dotazy, bylo nezbytné zajistit dostatečnou úroveň ochrany proti souběhu. Pro tento účel byla zvolena kombinace dvou technologií. Primární datová struktura, která uchovává informace o transakcích, je

ConcurrentHashMap. Jedná se o implementaci mapy optimalizovanou pro práci s více vlákny, která umožňuje bezpečné čtení i zápis bez nutnosti globálního zamykání celé mapy.

Pro některé operace, kde je potřeba atomicky aktualizovat více údajů najednou (například při aktualizaci stavu na základě webhooku), je navíc použit synchronizační mechanismus pomocí ReentrantLock. Tento zámek umožňuje řízení přístupu ke konkrétnímu záznamu, čímž minimalizuje riziko souběhu a zároveň udržuje vysoký výkon systému. Další vrstvou ochrany systému je zmíněný scheduler, který v pravidelných intervalech prochází mapu transakcí a odstraňuje záznamy, které překročily definovanou expirační dobu. Tím je zajištěno, že v systému nezůstávají mrtvé transakce, které by mohly v čase degradovat jeho výkon.



Obrázek 15 Zobrazení metod které operují nad QrPaymentSharedMapService

(zdroj: vlastní)

8 IMPLEMENTACE SLUŽBY

Samotná implementace probíhala v programovacím jazyce Java. Tento jazyk byl zvolen nejen pro svou širokou komunitní podporu a robustnost, ale také pro snadnou integraci s ostatními technologiemi využívanými v rámci celého systému, jako je například gRPC nebo Spring Boot framework. Díky tomu bylo možné zajistit vysokou efektivitu vývoje a zároveň si udržet dobrou čitelnost a rozšiřitelnost výsledného kódu.

Vývoj služby začal vytvořením základní architektury projektu, která reflektovala předem definované komunikační a funkční požadavky. Projekt byl strukturován jako typická vícevrstvá aplikace, s jasně oddělenými vrstvami pro přijímání požadavků (controller), obchodní logiku (service) a datové modely (model). Toto rozdělení usnadňuje údržbu kódu, testování jednotlivých částí systému a případné budoucí rozšiřování funkcionality.

8.1 První fáze (úprava SmartSwitche)

V první fázi bylo nutné upravit existující službu SMSW, do které byla přidána podpora platby přes QR kód. Jelikož není možné tuto část plně popsat z důvodu zachování firemního tajemství, bude v této části stručně nastíněn cíl potřebných úprav, které v rámci této fáze proběhly.

Tato implementace zahrnovala vytvoření nového odchozího kanálu a rozšíření tříd, které definují základní strukturu transakcí ve SMSW. Rozšíření tříd proběhlo o nové property, které definují, o jakou transakci se jedná, aby s ní mohlo být patřičně naloženo a mohla tak být správně nasměrována na odchozí kanál, který ji přepošle dál. V našem případě do QrPayment.

Uvnitř SMSW je každá transakce převedena do univerzálního tvaru, díky čemuž můžeme s různými typy transakcí nakládat jednotně. Tento univerzální tvar transakce je převeden v odchozím kanále, který se stará o správné odeslání transakce, na tvar potřebný pro odeslání přes protokol gRPC. Transportní protokol vyžaduje definování objektů pomocí souborů s koncovkou *.proto (proto files). Na základě těchto souborů byly následně pomocí nástrojů jako protoc vygenerovány potřebné Java třídy, které slouží k efektivnímu zpracování příchozích a odchozích gRPC zpráv. Objekt ve tvaru vhodném pro gRPC komunikaci, je pojmenovaný jako GRPCTransaction. Tato podoba transakce obsahuje všechny důležité data a je odeslaná dál přes již zmíněný gRPC protokol do QrPayment.

8.2 Druhá fáze (implementace QrPayment)

Druhá fáze představovala implementaci nové samostatné služby QrPayment. Hlavním úkolem této služby bylo přijímat požadavky od SMSW prostřednictvím gRPC, dále je zpracovávat a následně komunikovat s platební bránou pomocí REST API.

8.2.1 Vytvoření Spring Boot aplikace

Základ nové služby byl založen pomocí frameworku Spring Boot, který nabízí rychlý vývoj moderních mikroservisních aplikací. Implementace nové služby QrPayment nezačala tvorbou aplikace „from scratch“, ale modifikací již existujícího projektového základu, který byl poskytnut firmou Monet+. Tento základ představuje kostru Spring Boot aplikace, která slouží pro vytváření nových interních projektů v rámci společnosti. Hlavní výhodou tohoto přístupu je sjednocení struktury projektů, snadnější údržba a zajištění souladu s interními standardy vývoje.

V rámci této fáze bylo nutné provést detailní přejmenování všech důležitých částí projektu, včetně názvů balíčků, tříd, modulů a konfiguračních souborů. Aplikace je založena na frameworku Spring Boot a její hlavní vstupní bod je definován třídou Application, která implementuje rozhraní ServletContextInitializer. Ve třídě Application je explicitně nastaveno:

- a) Povolení plánovače úloh pomocí anotace `@EnableScheduling`, což umožňuje implementaci plánovaných procesů, například mazání expirovaných transakcí.
- b) Specifikace skenovaných balíčků pomocí `scanBasePackages`, kde byly vyjmenovány relevantní části projektu určené k načtení.
- c) Vyloučení nepoužívaných automatických konfigurací, které nebyly pro službu QrPayment relevantní.
- d) Nastavení cookie session ID při startu servletu na hodnotu QR-PAYMENT-JSESSIONID.

8.2.2 Napojení knihoven přes Maven

Následuje fáze napojení potřebných knihoven a závislostí pomocí nástroje Maven. Tato část implementace je klíčová pro správnou funkčnost služby QrPayment, protože zajišťuje dostupnost všech potřebných komponent pro samotnou logiku aplikace, komunikaci s platební bránou i se službou SMSW.

Celkové řešení je rozdělené do více modulů, což odpovídá zavedené architektuře Monet+ projektů. Hlavní rodičovský pom.xml soubor definuje projekt jako několika modulovou aplikaci, kde je spravováno několik základních částí:

- a) qr-payment-app – samotná spustitelná aplikace (server)
- b) qr-payment-service – implementace hlavní logiky
- c) qr-payment-model – modely používané v rámci služby
- d) qr-payment-rest – REST vrstva poskytující veřejné API
- e) qr_payment-common – společné utility a konfigurace

V hlavním pom.xml je nadefinováno, že projekt dědí ze spring-boot-starter-parent, verze 3.2.2. Díky tomu je možné využívat všech výhod Spring Bootu v nejnovější verzi, včetně moderního stacku postaveného na Java 17. V části dependencyManagement je centrálně spravován seznam všech hlavních závislostí včetně jejich verzí. Tento přístup umožňuje jednodušší správu verzí napříč jednotlivými moduly a zároveň zajišťuje konzistenci v rámci celého projektu. Níže je možné v krátké ukázce kódu vidět syntaxi nastavení závislostí projektu na konkrétních balíčcích.

```
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>org.json</groupId>
      <artifactId>json</artifactId>
      <version>${json.version}</version>
    </dependency>
    <dependency>
      <groupId>cz.monetplus.smartswitch.grpc</groupId>
      <artifactId>smsw-grpc-base-api</artifactId>
      <version>${grpc.switch.version}</version>
    </dependency>
    <dependency>
      <groupId>io.grpc</groupId>
      <artifactId>grpc-protobuf</artifactId>
      <version>${grpc.version}</version>
    </dependency>
  </dependencies>
</dependencyManagement>
```

8.2.3 gRPC komunikace

Implementace serverové části gRPC služby je realizována ve třídě `QrPaymentServiceGrpcImpl`, která je označena anotací `@GrpcService`. Tato anotace zajistí, že Spring Boot automaticky detekuje tuto třídu jako poskytovatele gRPC služby a zaregistruje ji do běhového prostředí serveru. Serverová implementace dědí od třídy `GRPCQrPaymentServiceImplBase`, která je generována automaticky na základě definice protobuf souborů.

8.2.4 Přijetí a zpracování požadavku ze SMSW

Hlavní metodou služby je metoda `process`, která slouží k přijímání požadavků typu `GRPCTransaction` a vracení odpovědi stejného typu klientovi. Vstupní parametr `request` obsahuje přijatá data, zatímco `responseObserver` představuje asynchronní kanál pro odeslání odpovědi zpět klientovi. Po přijetí požadavku server nejprve zaznamená základní informace o transakci do logu. Konkrétně identifikátor transakce (`trid`) a typ zpracování (`procType`). Dle typu požadavku systém dále rozlišuje dvě větve zpracování. Těmito větvemi zpracování jsou standardní zpracování nové transakce a žádost o stav platby.

Pokud je typ zpracování nastaven na `QR_CODE_STATUS`, server zjistí aktuální stav příslušné transakce ze sdílené paměťové mapy (`sharedMapService`). V případě úspěšného dohledání transakce je následně na základě jejího stavu vygenerována odpověď s příslušným výsledkem zpracování (`ACCEPTED` nebo `FAIL`). Tato odpověď je sestavena metodou `processResponseForStatus` a odeslána klientovi.

Pokud požadavek není žádostí o stav, systém předá objekt `GRPCTransaction` ke zpracování prostřednictvím služby `QrPaymentBaseOnlineMessageSender`. Výsledek je poté zachycen a odeslán zpět klientovi za pomoci gRPC.

8.2.5 Správa transakcí a práce s pamětí

Správa stavu platebních transakcí v systému je klíčová pro zajištění správné funkcionality, bezpečnosti a škálovatelnosti celé aplikace. V projektu je tato odpovědnost svěřena službě `QrPaymentSharedMapService`, která poskytuje mechanismy pro ukládání, aktualizaci, dohledávání a čištění dat. Tato služba efektivně kombinuje práci s vlákny, správu konkurentního přístupu k datům a periodickou údržbu.

8.2.6 Použité datové struktury

Hlavními používanými datovými strukturami jsou tři kolekce typu `ConcurrentHashMap` (`smswMap`, `altapayMap` a `lockMap`). První kolekce `smswMap` mapuje identifikátory platebních transakcí vytvořené ve SMSW na interní identifikátory systému `Altapay`. Druhá kolekce `altapayMap` uchovává objekty `QrPaymentStateQueueItem`, které obsahují časové razítko vytvoření záznamu a frontu (`ArrayBlockingQueue`) pro uchovávání stavu platby. Třetí kolekce `lockMap` spravuje instanci `ReentrantReadWriteLock` pro každý klíč v systému, čímž umožňuje bezpečný paralelní přístup k jednotlivým záznamům bez rizika nekonzistence dat.

8.2.7 Zápis a čtení dat

Služba poskytuje metody pro aktualizaci, zápis a čtení z obou hlavních map. Metoda `updateSmswMap` zapisuje novou dvojici klíč-hodnota do `smswMap`. Aktualizace je provedena přímo, neboť `ConcurrentHashMap` zaručuje bezpečnost operací v prostředí více vláken.

Při aktualizaci `altapayMap` je situace komplexnější, přičemž je logika implementovaná v metodě `updateAltapayMap`. Nejprve je získán `read lock` pro daný klíč, aby se zabránilo nekonzistentním zápisům. Následně je nová hodnota nabídnuta do fronty (`ArrayBlockingQueue`) existujícího objektu `QrPaymentStateQueueItem`. Pokud nabídnutí selže, tak je situace zalogována.

Pro potřeby klientských požadavků na ověření stavu platby implementuje služba metodu `getStateFromAltapayMap`. Tato metoda se pokouší načíst a odebrat první dostupný stav z fronty spojené s daným klíčem. Čekací mechanismus využívá maximálně dvacetisekundové blokující čekání na nové údaje. Pokud během této doby není nový stav dostupný, metoda vrátí prázdný objekt a příslušné varování je zaznamenáno do logu. V případě, že přečtená hodnota indikuje úspěšnou platbu, dojde k vyčištění souvisejících záznamů ze všech tří map.

8.2.8 Periodické čištění starých záznamů

Aby nedocházelo k nekontrolovanému růstu paměťové náročnosti systému, služba implementuje metodu `clearOldPayments`. Tato metoda je spouštěna automaticky každých 30 sekund. Jejím úkolem je procházet všechny položky v `altapayMap` a vyhodnocovat jejich stáří na základě rozdílu aktuálního času a uloženého časového razítka spojeného s transakcí.

Pokud nad daným klíčem, který přesáhl dobu své povolené existence, neprobíhá žádná operace, která by blokovala proces odstranění, tak je transakce vymazána společně se všemi spojitostmi.

```
@Scheduled(fixedRate = 30 * 1000)
public void clearOldPayments() {
    Log.info("Running scheduled task to clear old payments...");

    Iterator<Map.Entry<String, QrPaymentStateQueueItem>> iterator = altapayMap.entrySet().iterator();
    while (iterator.hasNext()) {
        Map.Entry<String, QrPaymentStateQueueItem> entry = iterator.next();
        String altapayKey = entry.getKey();
        QrPaymentStateQueueItem queueItem = entry.getValue();

        Duration duration = Duration.between(queueItem.getDttm(), LocalDateTime.now());
        if (duration.toSeconds() >= 70) {
            ReentrantReadWriteLock lock = getLockForKey(altapayKey);
            if (!lock.isWriteLocked() && lock.getReadLockCount() == 0) {
                lock.writeLock().lock();
                try {
                    iterator.remove();
                    smswMap.entrySet().removeIf(smswEntry -> smswEntry.getValue().equals(altapayKey));
                    lockMap.remove(altapayKey);
                    Log.warn("Removed expired payment with altapayKey '{}'.", altapayKey);
                } finally {
                    lock.writeLock().unlock();
                }
            } else {
                Log.warn("Skipped deletion of expired payment with altapayKey '{}' => LOCKED", altapayKey);
            }
        }
    }

    Log.info("Scheduled task to clear old payments completed.");

    Log.info(">>> smswMap: {}", smswMap.toString());
    Log.info(">>> altapayMap: {}", altapayMap.toString());
}
```

Obrázek 16 Ukázka kódu metoda clearOldPayments

(zdroj: vlastní)

8.2.9 Integrace s platební bránou

V rámci realizace QR plateb je klíčovou součástí systému integrace s externí platební bránou. V této diplomové práci je pro tuto komunikaci využitý simulátor platební brány Altapay, se kterým systém komunikuje prostřednictvím HTTP rozhraní. Integrace je realizována ve třídě QrPaymentBaseOnlineMessageSender, která implementuje veškerou potřebnou logiku pro zasílání požadavků a zpracování odpovědí.

Komunikace probíhá asynchronně pomocí HTTP POST požadavků. Sestavení těla požadavku je realizováno metodou buildRequestFormData. Každý požadavek je sestaven parametry, jako jsou identifikace terminálu, podpis, specifikace metody, časová značka a další ve formátu JSON. Po odeslání požadavku se systém pomocí CompletableFuture objektu vrací k asynchronnímu zpracování odpovědi. Výsledné HTTP odpovědi jsou

zpracovávány metodou `processResponse`, která nejprve kontroluje stavový kód odpovědi a poté analyzuje obsah odpovědi zakódovaný v XML formátu.

XML odpověď je parsovaná pomocí standardních knihoven, přičemž se získávají klíčové hodnoty jako `TraceId`, `State`, `Status`, `Code`, `OrderId`, `SettlementAmount` a další. Tyto hodnoty jsou následně využity k aktualizaci interního modelu transakce.

Kromě zpracování odpovědi je v systému kladen důraz i na robustní zachytávání a ošetření chybových stavů. Speciální metodou `handleHttpExceptions` jsou zpracovávány různé typy výjimek. Pro různé typy chyb jsou pak určeny různé návratové kódy, které umožňují centrální řízení dalších kroků transakční logiky.

Dále je implementována podpora pro detekci a ošetření nestandardních situací na straně platební brány, například neočekávaných nebo chybových HTTP status kódů (400, 500). Tyto situace jsou zpracovány metodou `processErrorResponse`, která se snaží extrahovat více informací z těla odpovědi a adekvátně je reflektovat v modelu transakce.

8.2.10 Webhook implementace

Pro zajištění zpětné komunikace platební brány se systémem obchodníka byla implementována služba typu webhook. Webhook je mechanismus, který umožňuje externí službě (v tomto případě platební bráně Altapay) notifikovat systém o změnách stavu transakcí. Tím se eliminuje potřeba aktivního dotazování a zajišťuje se včasná a efektivní aktualizace dat o transakcích.

Webhook je realizován prostřednictvím REST API pomocí anotací `@RestController` a `@RequestMapping` ve frameworku Spring Boot. Třída `QrPaymentWebhookController` definuje HTTP endpoint, který je dostupný metodou POST. Přijatý požadavek obsahuje datovou strukturu ve formátu JSON, jež reprezentuje informace o transakci.

Pomocí objektu `Optional` se provádí bezpečná extrakce potřebných údajů z objektu JSON. Konkrétně jsou získávány hodnoty stav transakce a identifikátor transakce. Pokud je hodnota `state` (stav transakce) k dispozici, je prostřednictvím služby `QrPaymentSharedMapService` aktualizována interní mapa `AltapayMap`, která uchovává aktuální stavy transakcí. Tím se systém obchodníka dozví, že daná transakce změnila svůj stav. Celý proces je zabalen v bloku `try-catch`, aby bylo možné zachytit a zalogovat případné chyby vzniklé během zpracování nevalidních nebo neúplných dat. Bez ohledu na výsledek zpracování je na požadavek webhooku vždy vrácena odpověď s HTTP kódem 200. Tento

přístup je běžnou praxí při implementaci webhooků, neboť minimalizuje riziko opakovaného zasílání notifikace platební branou.

```
@PostMapping("/webhook")
public ResponseEntity<Void> handleWebhook(@RequestBody Map<String, Object> jsonObject) {
    Log.info("Webhook received: {}", jsonObject);

    try {
        String state = Optional.ofNullable(jsonObject)
            .map(m -> (Map<String, Object>) m.get("data"))
            .map(data -> (Map<String, Object>) data.get("transaction_info"))
            .map(transactionInfo -> (String) transactionInfo.get("state"))
            .orElse(null);

        String trade_id = Optional.ofNullable(jsonObject)
            .map(m -> (Map<String, Object>) m.get("data"))
            .map(data -> (Map<String, Object>) data.get("transaction_info"))
            .map(transactionInfo -> (String) transactionInfo.get("trade_id"))
            .orElse(null);

        if (state != null) {
            Log.info("Transaction state: {}", state);
            sharedMapService.updateAltapayMap(trade_id, state);
        } else {
            Log.warn("Missing or invalid 'state' in transaction_info.");
        }
    } catch (Exception e) {
        Log.error("Error processing webhook payload: ", e);
    }

    return ResponseEntity.ok().build();
}
```

Obrázek 17 Ukázka kódu metoda handleWebhook

(zdroj: vlastní)

8.3 Třetí fáze (úprava core-rest-simulator)

Ve třetí fázi integrace bylo nezbytné upravit projekt core-rest-simulator, který slouží jako nástroj pro simulaci poskytovatele služeb Altapay. Tyto úpravy umožnily vytvoření realistického testovacího prostředí, ve kterém lze ověřovat chování systému bez nutnosti přímého propojení s produkční infrastrukturou poskytovatele platebních služeb. Zásahy v této fázi zahrnovaly jak návrh nových datových struktur, tak implementaci podpůrné logiky ve službách a kontrolerech.

V první řadě byly definovány nové datové třídy, tzv. Data Transfer Object (DTO), které představují formální popis struktury vstupních požadavků a výstupních odpovědí. Mezi vytvořené třídy patří QrPaymentRequest, která reprezentuje kompletní vstupní požadavek, a QrPaymentRequestData, která slouží jako vnořený objekt obsahující podrobné informace o samotné QR platbě, jako je částka, měna, popis platby, notifikační URL, identifikátor objednávky, platební metoda, její specifikace a časový limit. Dále byly vytvořeny třídy

QrPaymentResponse, QrPaymentResponseHead, QrPaymentResponseBody a QrPaymentResponseData, jejichž kombinací vzniká odpověď, kterou vrací simulátor zpět.

Implementace podpůrné logiky proběhla v rámci servisní vrstvy, konkrétně ve třídě AltaPayService. V této třídě byla implementována metoda processRequest_qrPayment, která zajišťuje kompletní zpracování příchozích požadavků na QR platbu. Na začátku této metody dochází k přípravě pomocných metadat, jako je generování unikátního identifikátoru transakce (UUID) a zaznamenání časového údaje o vytvoření požadavku. Poté je zavolána metoda processRequest, která integruje proces generování odpovědi. Odpověď je vytvořena pomocí metody createBaseResponse_forQrPayment, která vytváří výstupní objekt QrPaymentResponse s předdefinovanými hodnotami, jež odpovídají odpovědi reálné platební brány.

Součástí implementace bylo rovněž rozšíření kontroleru AltaPayController o nový HTTP endpoint dostupný pod cestou /qrCode. Tento endpoint je určen pro příjem požadavků typu POST. Veškerá data jsou předávána v poli s názvem data, které obsahuje JSON řetězec reprezentující obsah požadavku na QR platbu. Tento JSON je následně programově převeden do objektu typu QrPaymentRequestData, jenž je v rámci aplikační logiky doplněn o základní metadata. Výsledný objekt QrPaymentRequest je následně předán metodě processRequest_qrPayment ve třídě AltaPayService, která vrací odpověď ve formě instance třídy QrPaymentResponse. Tato instance je následně převedena do formátu XML, který odpovídá očekávanému formátu volající aplikace.

Tato fáze přinesla zásadní zlepšení v oblasti testovatelnosti a validace procesu QR plateb. Díky těmto úpravám bylo možné emulovat celý proces od příjmu požadavku až po odeslání odpovědi, včetně možnosti simulace různých scénářů, jako jsou úspěšné i neúspěšné platby.

9 ANALÝZA A TESTOVÁNÍ

V této části práce byla provedena důkladná analýza a následné testování implementace prostřednictvím vícevláknového scénáře simulujícího reálné chování platebních terminálů. Cílem testování bylo ověřit funkčnost, stabilitu a výkonnost implementovaného systému při zpracování hromadných transakcí v různých konfiguracích. Testovací prostředí bylo navrženo tak, aby co nejvěrněji simulovalo reálné nasazení systému v provozu.

Testovací procedura byla realizována pomocí třídy `MassTermWorker`. Z hlediska samotného testování je možné nakonfigurovat QR platby, i současné dotazování na stavy již realizovaných QR plateb. Jedním z klíčových parametrů testování byla možnost spouštět transakce v dávkách, což umožnilo efektivní škálování a přehledné vyhodnocení výkonu na větším objemu dat. Tato třída implementuje rozhraní `Runnable`, což umožňuje její paralelní spouštění prostřednictvím vláken. Každá instance představuje simulaci jednoho fyzického platebního terminálu.

V metodě `runOneBatch` probíhá inicializační handshake se serverem a následně se odesílají zprávy v závislosti na konfiguraci. Výsledky transakcí se zaznamenávají pro účely vyhodnocení výkonu a zpětné komunikace. Pokud jsou přítomny identifikátory a trace ID, jsou tyto data uloženy do fronty pro případné odeslání webhook notifikací.

9.1 Inicializace QR platby

Metoda `sendQrPaymentMessage` slouží k odeslání žádosti o platbu pomocí QR kódu. Probíhá zde sestavení zprávy s transakčním kódem 37, která obsahuje klíčové identifikátory jako je typ platby, částka, měna a adresa URL. Tímto způsobem se definuje, že se jedná o platbu QR kódem. Uvedená URL adresa je pouze lokálním testovacím koncovým bodem. Po sestavení zprávy je provedeno její odeslání metodou `sendAndReceive`, která zajišťuje kryptografickou komunikaci se serverem pomocí 3DES šifrování.

9.2 Stavová zpráva platby

Následující metoda `sendQrPaymentStateMessage` slouží k odeslání stavového dotazu na základě původní QR platby. Transakční kód v tomto případě odpovídá hodnotě 38, která je v systému vyhrazena pro stavové požadavky.

Nejdůležitějším prvkem této zprávy je použití hodnoty `SequenceNumberOriginal`, která jednoznačně identifikuje původní transakci, jejíž stav má být ověřen. Stejně jako v předchozím případě i zde je zpráva odeslána na server a výsledek je zaznamenán do logu.

9.3 Webhook simulace a notifikace

V případě QR plateb je implementován i mechanismus zpožděné notifikace prostřednictvím webového volání webhook. Tento mechanismus je spuštěn paralelně v samostatném vlákně prostřednictvím metody `startWebhookNotificationThread`. Po obdržení hodnoty `Trace ID`, transakce čeká náhodně dlouhou dobu v rozpětí 10 až 90 sekund a následně odešle HTTP POST požadavek na předem definovanou adresu.

```
//Předdefinovaná adresa pro odeslání webhook notifikace  
URL url = new URL("http://localhost:9090/api/altapay/webhook");
```

Tímto způsobem je simulováno chování reálných externích platebních bran, které po nějaké době zpětně informují o výsledku transakce.

9.4 Testovací scénáře a chování

Pro testování bylo definováno několik scénářů, které se lišily zejména v počtu transakcí a počtu paralelních vláken (terminálů). Testování zahrnovalo simulaci běžného provozu (např. 100 QR plateb současně). V případě neúspěšného dokončení transakce systém opakuje finalizační požadavek až třikrát (`MAX_ATTEMPTS = 3`), přičemž každá iterace zaznamenává reakční čas a stavový kód.

Testy prokázaly, že komponenta je schopna zvládat vysoký počet současných požadavků, správně odesílat transakce i dotazy na jejich stav a efektivně pracovat s notifikacemi od externího poskytovatele plateb. QR platby byly řádně identifikovatelné, časově měřitelné a odpovědi byly v naprosté většině případů zpracovány do několika setin sekundy.

ZÁVĚR

Diplomová práce se komplexně zabývala problematikou platebních karet a digitálních platebních prostředků, se zvláštním důrazem na platby realizované prostřednictvím QR kódů. Cílem práce bylo nejen analyzovat technologické, bezpečnostní a regulační aspekty těchto platebních metod, ale také navrhnout, implementovat a otestovat systém podporující zpracování QR plateb v prostředí reálného platebního ekosystému.

V teoretické části byla nejprve provedena důkladná analýza historie, typologie a principu fungování platebních karet, včetně zapojení jednotlivých účastníků transakčního procesu a bezpečnostních standardů, jako jsou EMV, PCI DSS nebo ISO 8583. Dále byla pozornost věnována moderním digitálním platebním metodám, zejména těm, které využívají QR kódy, včetně globálních i lokálních poskytovatelů jako Alipay, Paytm, Apple Pay nebo QR Platba v Česku. Byly popsány jejich technologické principy, bezpečnostní opatření, regulační rámec i aktuální trendy.

Samostatná kapitola byla věnována mezinárodním standardům a komunikačním protokolům, jež tvoří nezbytný základ pro interoperabilitu systémů a bezpečný přenos dat v rámci karetních i digitálních plateb. V této části byly podrobně popsány jak tradiční protokoly, tak i moderní rozhraní REST API, či gRPC. Následně bylo provedeno systematické srovnání platebních karet a QR plateb z hlediska rychlosti, bezpečnosti, nákladů, globální akceptace a technologických i společenských aspektů.

Praktická část se zaměřila na návrh, implementaci a testování funkčního řešení pro zpracování QR plateb v prostředí systémů společnosti MONET+. Zde byla využita mikroslužbová architektura a technologie Java se Spring Boot frameworkem. Byla navržena nová komponenta QrPayment pro zpracování požadavků, notifikací a stavových dotazů pomocí gRPC a REST API a zároveň upraven stávající systém SmartSwitch. Byly implementovány bezpečnostní mechanismy, efektivní správa transakcí, periodické čištění paměti a logika práce s různými stavy transakce.

Zásadním přínosem práce je rozsáhlý testovací framework, který umožňuje spouštět paralelní testy simulující desítky terminálů. Bylo ověřeno generování QR platby, dotaz na její stav a zpracování notifikace. Výsledky testů potvrdily vysokou stabilitu, výkonnost a konzistenci navrženého systému. Práce tedy nejen prokázala technickou realizovatelnost navrženého řešení, ale zároveň přispěla ke zmapování praktických výzev při integraci QR plateb do reálného prostředí.

Z celkového pohledu lze konstatovat, že cíle stanovené v úvodu práce byly bezezbytku splněny. Teoretická část poskytla ucelený přehled o současných platebních metodách, technologických standardech a bezpečnostních požadavcích. Praktická část pak nabídla konkrétní řešení, jehož realizace byla úspěšně ověřena a může sloužit jako základ pro další vývoj a nasazení do produkčního prostředí. Získané poznatky jsou uplatnitelné jak v oblasti vývoje platebních systémů, tak při navrhování bezpečných, uživatelsky přívětivých a technologicky efektivních metod digitálního placení.

Do budoucna lze uvažovat o rozšíření systému o napojení na další platební brány. Zároveň se otevírá prostor pro využití pokročilých šifrovacích metod, jako je postkvantová kryptografie, a pro nasazení strojového učení v oblasti prevence podvodů. Vzhledem k dynamickému vývoji v oblasti bezhotovostních plateb představuje téma QR plateb a jejich integrace do moderních systémů nadále atraktivní a perspektivní oblast výzkumu i aplikačního nasazení.

SEZNAM POUŽITÉ LITERATURY

- [1] *The History of the Credit Card*. Online. 2024. Dostupné z: <https://www.swipesum.com/insights/history-of-the-credit-card>. [cit. 2025-05-10].
- [2] *Now You Know: What Was the First Credit Card?* Online. 2016. Dostupné z: <https://time.com/4512375/first-credit-card/>. [cit. 2025-05-10].
- [3] *The surprising history of credit cards: How this tech has evolved and where it's headed*. Online. 2022. Dostupné z: <https://www.cnet.com/personal-finance/credit-cards/features/the-history-of-credit-cards/>. [cit. 2025-05-10].
- [4] *Brand History*. Online. 2024. Dostupné z: <https://www.mastercard.com/brandcenter/en/brand-history>. [cit. 2025-05-10].
- [5] *Enabling Seamless and Secure Contact and Contactless Payments Around the World*. Online. 2022. Dostupné z: <https://www.emvco.com/wp-content/uploads/2022/09/EMV®-Chip-At-A-Glance-EMVCo-eBook.pdf?>. [cit. 2025-05-10].
- [6] *The History of Contactless Payments*. Online. 2024. Dostupné z: <https://www.globalpaymentsintegrated.com/en-us/blog/2020/09/15/the-history-of-contactless-payments>. [cit. 2025-05-10].
- [7] *The evolution of Google Pay: from inception to today*. Online. 2024. Dostupné z: <https://www.linkedin.com/pulse/evolution-google-pay-from-inception-today-magnetiq-bank-bynff/>. [cit. 2025-05-10].
- [8] *Apple Pay and the Evolution of Mobile Payments*. Online. 2024. Dostupné z: <https://www.cenoa.com/blog/evolution-of-mobile-payments-apple-pay>. [cit. 2025-05-10].
- [9] *1957 Diners Club credit card*. Online. In: Mobiletransaction. 2025. Dostupné z: <https://www.mobiletransaction.org/history-of-credit-card-machines/>. [cit. 2025-05-10].
- [10] *Druhy platebních karet*. Online. 2024. Dostupné z: <https://www.finance.cz/ucty-a-sporeni/platebni-karty/abeceda-platebnich-karet/druhy-karet/>. [cit. 2025-05-10].
- [11] *Co je předplacená karta?* Online. 2025. Dostupné z: <https://www.moneta.cz/caste-dotazy/odpoved/co-je-predplacena-karta>. [cit. 2025-05-10].

- [12] *Virtuální platební karta*. Online. 2025. Dostupné z: <https://www.kb.cz/cs/podpora/slovník/vyrazy-zacinajici-na-v/virtualni-platebni-karta>. [cit. 2025-05-10].
- [13] *Co-brandové karty Visa*. Online. 2025. Dostupné z: <https://www.visa.cz/products/cobranded-cards.html>. [cit. 2025-05-10].
- [14] *Transaction Processing Rules*. Online. 2025. Dostupné z: <https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/transaction-processing-rules.pdf>. [cit. 2025-05-10].
- [15] *How the payment process works*. Online. 2025. Dostupné z: <https://sea.mastercard.com/en-region-sea/business/merchants/start-accepting/payment-process.html>. [cit. 2025-05-10].
- [16] *Payment processing explained: What it is and how it works*. Online. 2023. Dostupné z: <https://stripe.com/en-cz/resources/more/payment-processing-explained>. [cit. 2025-05-10].
- [17] POLÁK, Jan. *Schéma placení kartou*. Online. In: Wikipedie. 2013. Dostupné z: https://cs.m.wikipedia.org/wiki/Soubor:Sch%C3%A9ma_placen%C3%AD_kartou.jpg. [cit. 2025-05-10].
- [18] *PCI Security Standards*. Online. 2025. Dostupné z: <https://www.pcisecuritystandards.org/standards/>. [cit. 2025-05-10].
- [19] *What is EMV 3-D Secure*. Online. 2025. Dostupné z: <https://www.emvco.com/emv-technologies/3-d-secure/>. [cit. 2025-05-10].
- [20] *Payment security: An in-depth, actionable guide for businesses*. Online. 2023. Dostupné z: <https://stripe.com/en-cz/resources/more/payment-security>. [cit. 2025-05-10].
- [21] *Z čeho se skládá poplatek při platbě kartou?* Online. 2025. Dostupné z: <https://help.gopay.com/cs/tema/cenik-a-obchodni-podminky/informace-k-poplatkum/z-ceho-se-sklada-poplatek-pri-platbe-kartou>. [cit. 2025-05-10].
- [22] *Vybrané předpisy vztahující se k platebnímu styku*. Online. 2025. Dostupné z: <https://www.cnb.cz/cs/platebni-styk/pravni-predpisy/>. [cit. 2025-05-10].
- [23] *PSD2, revoluce v elektronických platbách*. Online. 2025. Dostupné z: <https://www.unicreditbank.cz/cs/o-bance/PSD2.html>. [cit. 2025-05-10].

- [24] *Nariadení o jednotné oblasti pro platby v eurech*. Online. 2024. Dostupné z: <https://eur-lex.europa.eu/CS/legal-content/summary/single-euro-payments-area-regulation.html>. [cit. 2025-05-10].
- [25] *Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (Text with EEA relevance)*. Online. 2015. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0751>. [cit. 2025-05-10].
- [26] *Okamžité platby a tokenizace. Mastercard představuje 10 trendů, které změni způsob placení v roce 2025*. Online. 2025. Dostupné z: <https://www.bankovnipoplatky.cz/okamzite-platby-a-tokenizace-mastercard-predstavuje-10-trendu-ktere-zmeni-zpusob-placeni-v-roce-2025>. [cit. 2025-05-10].
- [27] *Okamžité platby a tokenizace. Mastercard představuje 10 trendů, které změni způsob placení v roce 2025*. Online. 2024. Dostupné z: <https://www.mastercard.com/news/europe/cs-cz/tiskove-centrum/tiskove-zpravy/cs-cz/2024/prosinec-2024/okamzite-platby-a-tokenizace-mastercard-predstavuje-10-trendu-ktere-zmeni-zpusob-placeni-v-roce-2025>. [cit. 2025-05-10].
- [28] *Platby v roce 2025: AI, blockchain a konec ručního zadávání čísel karet*. Online. 2024. Dostupné z: <https://insmart.cz/platby-v-roce-2025>. [cit. 2025-05-10].
- [29] *Způsoby placení v roce 2025*. Online. 2024. Dostupné z: <https://www.finparada.cz/8642-Platebni-metody-v-roce-2025.aspx>. [cit. 2025-05-10].
- [30] *Spořitelna jako první banka na světě připravila pro herní příznivce limitovanou edici OLED svítící platební karty*. Online. 2025. Dostupné z: <https://www.ceskenovinky.cz/2025/02/03/sporitelna-jako-prvni-banka-na-svete-pripravila-pro-herni-priznivce-limitovanou-edici-oled-svitici-platebni-karty>. [cit. 2025-05-10].
- [31] *'March to independence': Christine Lagarde wants EU to ditch Visa, Mastercard for own platform*. Online. 2025. Dostupné z: <https://www.businesstoday.in/world/us/story/march-to-independence-christine-lagarde-wants-eu-to-ditch-visa-mastercard-for-own-platform-470816-2025-04-05>. [cit. 2025-05-10].
- [32] *EMV QR Code Specifications*. Online. 2020. Dostupné z: <https://www.w3.org/2020/Talks/emvco-qr-20201021.pdf>. [cit. 2025-05-10].

- [33] *ISO/IEC 18004:2024—QR Code Bar Code Symbolology*. Online. 2024. Dostupné z: <https://blog.ansi.org/iso-iec-18004-2024-qr-code-bar-code-symbology/>. [cit. 2025-05-10].
- [34] *Dynamic QR Codes*. Online. In: ALTAPAY. 2025. Dostupné z: <https://documentation.altapay.com/v2/Checkout-API/QRPayments/#dynamic-qr-codes>. [cit. 2025-05-10].
- [35] *Platební karta*. Online. In: Financnigramotnost. 2016. Dostupné z: <https://financnigramotnost.mfcr.cz/cs/penize-a-ucty/bezhotovostni-penize>. [cit. 2025-05-10].
- [36] *Introduction*. Online. 2021. Dostupné z: <https://global.alipay.com/docs/ac/transactionqrnodenew/intro>. [cit. 2025-05-10].
- [37] *About WeChat Pay*. Online. 2025. Dostupné z: https://pay.weixin.qq.com/static_en/home/about.shtml. [cit. 2025-05-10].
- [38] *Cinske-platebni-brany-alipay-wechat-pay*. Online. In: Jougroup. 2025. Dostupné z: <https://www.jouagency.cz/cinske-platebni-brany-alipay-wechat-pay/>. [cit. 2025-05-10].
- [39] *Paytm started the Digital Revolution in India*. Online. 2025. Dostupné z: <https://paytm.com/about-us>. [cit. 2025-05-10].
- [40] *About PhonePe*. Online. 2025. Dostupné z: <https://workat.tech/company/phonepe>. [cit. 2025-05-10].
- [41] *Talkwalker's Battle of the Brands: Paytm Vs PhonePe*. Online. In: Campaignindia. 2019. Dostupné z: <https://www.campaignindia.in/article/talkwalkers-battle-of-the-brands-paytm-vs-phonepe-part-1/450984>. [cit. 2025-05-10].
- [42] *Apple Pay QR Code: How to Make Payments With Your iOS Devices*. Online. 2024. Dostupné z: <https://qr.io/blog/apple-pay-qr-code/>. [cit. 2025-05-10].
- [43] *Pay with a QR code (Singapore only)*. Online. 2025. Dostupné z: <https://support.google.com/googlepay/answer/9984037?hl=en>. [cit. 2025-05-10].
- [44] *Pay with Apple Pay & Google Pay*. Online. In: Flyhighenglish. 2025. Dostupné z: <https://www.flyhighenglish.com/pay-with-apple-pay-google-pay/>. [cit. 2025-05-10].

- [45] *Žádost o platbu Revolut Pro*. Online. 2025. Dostupné z: <https://help.revolut.com/cs-CZ/help/more/revolut-pro/revolut-pro-payment-request/>. [cit. 2025-05-10].
- [46] *About Us*. Online. 2025. Dostupné z: <https://www.revolut.com/discover-our-company/>. [cit. 2025-05-10].
- [47] *Twint*. Online. 2025. Dostupné z: <https://www.twint.ch/en/>. [cit. 2025-05-10].
- [48] *Instructions for business customers*. Online. 2025. Dostupné z: <https://www.twint.ch/content/uploads/2023/04/Instructions-order-TWINT-QR-code-sticker.pdf>. [cit. 2025-05-10].
- [49] *Lydia*. Online. 2025. Dostupné z: <https://www.lydia.me/en>. [cit. 2025-05-10].
- [50] *Blik – platební metoda nezbytná pro polský trh*. Online. 2023. Dostupné z: <https://www.trustpay.cz/blog/blik-platebni-metoda-nezbytna-pro-polsky-trh/>. [cit. 2025-05-10].
- [51] *European Payments Initiative*. Online. 2025. Dostupné z: <https://epicompany.eu/about>. [cit. 2025-05-10].
- [52] *Standardisation of QR-codes for Mobile Initiated SEPA (Instant) Credit Transfers*. Online. 2024. Dostupné z: <https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-06/EPC024-22v2.10%20Standardisation%20of%20QR-codes%20for%20MSCTs.pdf>. [cit. 2025-05-10].
- [53] *QR Platba*. Online. 2025. Dostupné z: <https://www.gopay.com/cs/qr-platba/>. [cit. 2025-05-10].
- [54] *QR Platba*. Online. 2025. Dostupné z: <https://qr-platba.cz>. [cit. 2025-05-10].
- [55] *How safe are QR payment codes?* Online. 2025. Dostupné z: <https://www.paypal.com/uk/money-hub/article/are-qr-payment-codes-safe>. [cit. 2025-05-10].
- [56] *Security considerations for QR codes*. Online. 2024. Dostupné z: <https://www.cyber.gc.ca/en/guidance/security-considerations-qr-codes-itsap00141>. [cit. 2025-05-10].
- [57] *EMV QR Codes*. Online. 2025. Dostupné z: <https://www.emvco.com/emv-technologies/qr-codes/>. [cit. 2025-05-10].

- [58] *The Central Bank of the People's Republic of China*. Online. 2025. Dostupné z: <http://www.pbc.gov.cn/en/3688006/index.html>. [cit. 2025-05-10].
- [59] *What Is Bharat QR Code? Benefits, Setup & Charges Explained*. Online. 2025. Dostupné z: <https://razorpay.com/blog/what-is-bharat-qr-code/>. [cit. 2025-05-10].
- [60] *DuitNow QR*. Online. 2025. Dostupné z: <https://www.duitnow.my/QR/index.html>. [cit. 2025-05-10].
- [61] *Singapore Quick Response Code*. Online. 2024. Dostupné z: <https://www.mas.gov.sg/development/e-payments/sgqr>. [cit. 2025-05-10].
- [62] *ČSN ISO/IEC 7810 (369725) Identifikační karty - Fyzikální charakteristiky*. Online. 2004. Dostupné z: <https://www.technicke-normy-csn.cz/csn-iso-iec-7810-369725-199558.html>. [cit. 2025-05-10].
- [63] *ČSN EN ISO/IEC 7813 (369733) Identifikační karty - Karty pro finanční transakce*. Online. 1997. Dostupné z: <https://www.technicke-normy-csn.cz/csn-en-iso-iec-7813-369733-199602.html>. [cit. 2025-05-10].
- [64] *ISO/IEC 7816-8:2021(en) Identification cards — Integrated circuit cards*. Online. 2021. Dostupné z: <https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-8:ed-5:v1:en>. [cit. 2025-05-10].
- [65] *ISO/IEC 7810*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://cs.wikipedia.org/wiki/ISO/IEC_7810. [cit. 2025-05-10].
- [66] *EMV Technologies*. Online. 2025. Dostupné z: <https://www.emvco.com/emv-technologies/>. [cit. 2025-05-10].
- [67] *PCI Security Standards Council*. Online. 2025. Dostupné z: https://www.pcisecuritystandards.org/about_us/. [cit. 2025-05-10].
- [68] *Standard POS device message specifications manual*. Online. 2011. Dostupné z: https://pors-sw.cz/stazeni/pos/instalace/terminaly/CSOB/aci_spdh_msg_specs_r6v10_0611.pdf. [cit. 2025-05-10].

- [69] ČSN EN ISO 8583 (369740) *Zprávy vytvořené kartou pro finanční transakce - Specifikace výměny zpráv*. Online. 1999. Dostupné z: <https://www.technicke-normy-csn.cz/csn-en-iso-8583-369740-199650.html>. [cit. 2025-05-10].
- [70] *Application Protocol Data Unit (APDU)*. Online. 2025. Dostupné z: https://www.cardlogix.com/glossary/apdu-application-protocol-data-unit-smart-card/?srsltid=AfmBOoq5eC1GZoKFdh_7Idl9FaGH2tB268qvSnIOKgT1grYHuFoUN_JH. [cit. 2025-05-10].
- [71] ČSN ISO/IEC 14443-4 (369760) *Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na blízko - Část 4: Protokol přenosu*. Online. 2012. Dostupné z: <https://www.technicke-normy-csn.cz/csn-iso-iec-14443-4-369760-199707.html>. [cit. 2025-05-10].
- [72] *What is Host Card Emulation (HCE) and HCE Payment?* Online. 2025. Dostupné z: <https://cpl.thalesgroup.com/faq/hardware-security-modules/what-host-card-emulation-hce>. [cit. 2025-05-10].
- [73] *Near field communication (NFC) overview*. Online. 2024. Dostupné z: <https://developer.android.com/develop/connectivity/nfc>. [cit. 2025-05-10].
- [74] *FATF*. Online. 2025. Dostupné z: <https://www.fatf-gafi.org/>. [cit. 2025-05-10].
- [75] *EFTA*. Online. 2025. Dostupné z: <https://www.efta.int/about-efta>. [cit. 2025-05-10].
- [76] *What Is Regulation E in Electronic Fund Transfers (EFTs)?* Online. 2023. Dostupné z: <https://www.investopedia.com/terms/r/regulation-e.asp>. [cit. 2025-05-10].
- [77] *GoPay technická dokumentace*. Online. 2025. Dostupné z: <https://doc.gopay.cz/>. [cit. 2025-05-10].
- [78] *Introduction to gRPC*. Online. 2025. Dostupné z: <https://grpc.io/docs/what-is-grpc/introduction/>. [cit. 2025-05-10].
- [79] *Data flow through services: Rest approach*. Online. In: Dev. 2022. Dostupné z: <https://dev.to/zhukmax/data-flow-through-services-rest-approach-5fdf>. [cit. 2025-05-10].
- [80] *A GUIDE TO ISSUING SUSTAINABLE CARDS*. Online. 2023. Dostupné z: <https://www.mastercard.com/news/media/5onpyesk/a-guide-to-issuing-sustainable-cards-a-gpp-whitepaper.pdf>. [cit. 2025-05-10]

- [81] V. K. Raina, *NFC payment systems and the New Era of transaction processing*. Hershey, PA: Business Science Reference, 2017. ISBN 9781522523079
- [82] S. Sharma, *Modern API Development with Spring and Spring Boot: Design highly scalable and maintainable APIs with REST, gRPC, GraphQL, and the reactive paradigm*. Birmingham, England: Packt Publishing, 2021. ISBN 9781800562875
- [83] S. Sharma, *Mastering Microservices with Java: Build enterprise microservices with Spring Boot 2.0, Spring Cloud, and Angular, 3rd Edition*, 3rd ed. Birmingham, England: Packt Publishing, 2019. ISBN 9781789531251
- [84] K. Indrasiri and D. Kuruppu, *Grpc: Up and running: Building cloud native applications with go and java for docker and kubernetes*. O'Reilly Media, 2020. ISBN 9781492058281
- [85] J. Bloch, *Effective Java*, 3rd ed. Boston, MA: Addison-Wesley Educational, 2017. ISBN 0134685997

SEZNAM OBRÁZKŮ

Obrázek 1 1957 Diners Club kreditní karta [9]	18
Obrázek 2 Popis platební karty [35]	19
Obrázek 3 Schéma platby kartou [17]	22
Obrázek 4 Proces dynamických QR kódů [34]	31
Obrázek 5 Alipay a WeChat [38]	32
Obrázek 6 Paytm a PhonePe [41]	33
Obrázek 7 Apple Pay a Google Pay [44]	33
Obrázek 8 Rozměry karet podle ISO 7810 [65]	39
Obrázek 9 REST API [79]	43
Obrázek 10 gRPC [78]	44
Obrázek 11 Zjednodušený digram procesu QR platby	60
Obrázek 12 Sekvenční diagram: Zahájení QR platby	61
Obrázek 13 Sekvenční diagram: Dotazování na stav QR platby + webhook	61
Obrázek 14 Ukázka diagramu tříd: QrPayment + SMSW	62
Obrázek 15 Zobrazení metod které operují nad QrPaymentSharedMapService	65
Obrázek 16 Ukázka kódu metoda clearOldPayments	71
Obrázek 17 Ukázka kódu metoda handleWebhook	73

SEZNAM TABULEK

Tabulka 1 Rozměry karet podle normy ISO 7810 [65]	38
---	----

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

QR	Quick Response
REST	Representational State Transfer
HTTP	HyperText Transfer Protocol
JSON	JavaScript Object Notation
ICA	Interbank Card Association
EMV	Europay, Mastercard, Visa
NFC	Near Field Communication
CVV	Card Verification Value
POS	Point of Sale
PCI DSS	Payment Card Industry Data Security Standard
EU	Evropská Unie
PSD2	Payment Services Directive 2
NIS2	Network and Information Security Directive 2
ČNB	Česká národní banka
SCA	Strong Customer Authentication
RTS SCA	Regulatory Technical Standards for Strong Customer Authentication
SEPA	Single Euro Payments Area
CBDC	Central Bank Digital Currency
ECB	Evropská centrální banka
ID	Identifikace
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
UPI	Unified Payments Interface
EPI	European Payments Initiative
ČBA	Českou bankovní asociací

PIN	Personal Identification Number
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
SPDH	Standard Point of Sale Data Handling
APDU	Application Protocol Data Unit
TLS	Transport Layer Security
MPM	Merchant-Presented Mode
CPM	Consumer-Presented Mode
HCE	Host Card Emulation
BIS	Bank for International Settlements
EFTA	Electronic Fund Transfer Act
Wi-Fi	Wireless Fidelity
LTE	Long-Term Evolution
PVC	Polyvinylchlorid
GPP	Greener Payments Partnership
ESG	Environmental, Social, and Governance
SMSW	SmartSwitch
XML	eXtensible Markup Language
DTO	Data Transfer Object

SEZNAM PŘÍLOH

Příloha P I: ZIP soubor

PŘÍLOHA P I: STRUKTURA ODEVZDANÝCH DAT („ZIP.ZIP“)

Přiložený ZIP soubor obsahuje:

Adresář **prilohy** – obsahuje adresář projektu qr-payment