Klíčování EMV platebních terminálů podle PCI DSS normy

Bc. Vít Osička

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav počítačových a komunikačních systémů

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Vít Osička**
Osobní číslo:	**A18742**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**Kombinovaná**
Téma práce:	**Klíčování EMV platebních terminálů podle PCI DSS normy**
Téma práce anglicky:	**EMV Payment Terminal Keying According to the PCI DSS Standard**

Zásady pro vypracování

1. Zpracujte literární poznatky z oblasti platebních terminálů.
2. Analyzujte současný stav klíčování EMV platebních terminálů ve vybrané společnosti.
3. Vypracujte projektové řešení s cílem navrhnout proces klíčování EMV platebních terminálů podle PCI DSS normy.
4. Současně vytvořit dokumentaci k dané problematice.
5. Zhodnoťte přínosy projektu.

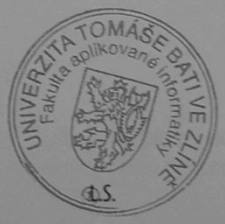
Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. Praha: Albatros, 2006, 340 s. Oko. ISBN 8000018888.
2. CHEN, Zhiqun. Java Card technology for smart cards: architecture and programmer's guide. Boston: Addison-Wesley, 2000. ISBN 0201703297.
3. AUMASSON, Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017. ISBN 1593278268.
4. Smart card basics ? A short guide (2019). Gemalto World leader in Digital Security [online]. 2019, 7. října 2019 [cit. 2019-11-14]. Dostupné z: https://www.gemalto.com/companyinfo/smart-cards-basics
5. PÍŠA, Rudolf. Třicet let platebních karet v Česku a Slovensku. Das Media, 2019. ISBN 9788097251932.

Vedoucí diplomové práce: **doc. Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **13. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**



doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 11.8.2020 Vít Osička, v. r.

ABSTRAKT

Diplomová práce se specializuje na návrh klíčování EMV platebních terminálů podle PCI DSS normy ve vybrané společnosti. V teoretické části jsou rozebrány literární poznatky týkající se problematiky. V praktické části je provedena analýza současného stavu klíčování platebních terminálů a jsou zde představeny jednotlivé komponenty, které vedou, jako celek k novému návrhu klíčování. Nové řešení je zaměřeno hlavně na zjednodušení a urychlení celého procesu. Hlavní úspora času lze sledovat využitím bezdrátové technologie NFC a odlišným přihlašováním do klíčovacího zařízení. U nového řešení lze pozorovat i zlepšení bezpečnosti, kdy je využito 3DES algoritmu s 3DES klíčem, namísto 2DES klíče, který byl využitý v rámci původního řešení.

Klíčová slova: platební terminál, klíčování, PCI DSS norma, 3DES, NFC

ABSTRACT

The master thesis specializes in the design of key injection process of EMV payment terminals according to the PCI DSS standard in a selected company. The theoretical part discusses the literature on the issue. In the practical part, an analysis of the current state of key injection process of payment terminals is performed and the individual components of key injection process are introduced, which lead, as a whole, to a new key injection process design. The new solution is mainly focused on simplifying and speeding up the whole process. The main time savings can be seen by using NFC wireless technology and different logins to the keying device. With the new solution, an improvement in security can also be observed, where a 3DES cipher with a 3DES key is used, instead of the 2DES key, which was used in the original solution.

Keywords: payment terminal, key injection process, PCI DSS, 3DES, NFC

Tím to bych rád poděkoval panu doc. Ing. Romanu Šenkeříkovi, Ph.D. za vedené mé diplomové práce a poskytnutí cenných rad a připomínek.

Dále bych chtěl poděkovat vybrané společnosti, za možnost vypracování diplomové práce a za cenné rady při jejím zpracování.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době je placení platební kartou na platebních terminálech téměř už samozřejmostí u většiny obchodníků. Aby byl celý platební proces bezpečný, je třeba dodržovat PCI DSS bezpečnostní normy a využívat zabezpečené terminály, pracující s klíči.

Diplomová práce je zaměřená na návrh klíčování EMV platebních terminálů podle PCI DSS normy ve vybrané společnosti. Výsledkem této práce je návrh procesu klíčování, včetně dokumentace a vizualizace klíčovací aplikace.

Diplomová práce se dělí na dvě stěžejní části, a to na teoretickou a praktickou. V rámci teoretické části je stručně popsaná historie platebních terminálů a platebních karet, dále je zde stručný úvod do kryptografie a šifrování, PCI DSS normy a je zde představen koncept klíčování EMV platebních terminálů jiné společnosti.

V praktické části je představena vybraná společnost, hlavně z pohledu produktového portfolia, pro kterou je návrh klíčování realizován. Dále je představeno současné řešení klíčování EMV platebních terminálů, jaké vybraná společnost využívá. Další stěžejní částí praktické části diplomové práce je návrh nového řešení klíčování, včetně popisu celého procesu klíčování.

V následující části je vytvořená dokumentace a návrh klíčovací aplikace, včetně popisu jednotlivých kroků, které jsou nutné pro správné naklíčování platebního terminálu. Závěr práce je zaměřen na přínosy navrhnutého řešení a porovnání jednotlivých bodů nově navrhnutého řešení s původním.

I. TEORETICKÁ ČÁST

1 EMV PLATEBNÍ TERMINÁL A EMV TRANSAKCE

Platební terminál je zařízení, které dokáže zpracovat kontaktní, magnetické a s přítomností bezkontaktní čtečky i bezkontaktní karty. Součástí terminálu může být také PinPad, který obsahuje bezkontaktní čtečku a slouží k zobrazení informací o platbě a k zadávání PINu (Personal Identification Number) použité karty.

Zároveň existuje mnoho poskytovatelů platebních terminálů, mezi ně patří většina velkých bank, jako například ČSOB (Československá obchodní banka) nebo Komerční banka, ale také nebankovní společnosti, například Global Payments nebo Revo. Nabídky od poskytovatelů se liší v ceně za pronájem platebního terminálu nebo v množství částky, která je z každé platby stržena na účet poskytovatele. [1]

1.1 EMV a NON-EMV standard

Následující podkapitola se věnuje dvěma odlišným standardům, a to EMV (Europay, MasterCard a Visa) a NON-EMV.

1.1.1 EMV standard

EMV je standard, podle ISO/IEC 7816 (International Organization for Standardization, International Electrotechnical Commission), který zabezpečuje vzájemnou kompatibilitu mezi platebními kartami a platebními terminály, pokladnami nebo bankomaty. Současně je využívaný v bankovním světě a podléhá PCI DSS auditu, i auditu jednotlivých vydavatelů karet, jako jsou VISA a MasterCard. V rámci standardu jsou definovány kryptografické algoritmy, které jsou dostatečně silné, aby zaručily bezpečnou manipulaci s citlivými daty. Mezi tyto šifry lze zařadit například hešovací algoritmus SHA-1, asymetrickou šifru RSA (Rivest, Shamir, Adleman) nebo symetrickou blokovou šifru 3-DES.

Celkově se jedná o standard, zaručující vysokou bezpečnost, během bankovní platby. Například EMV karty obsahují mnoho informací, umožňují vykonávat kryptografické operace nebo jsou schopny uložit informace o PINu a následně ho ověřit, bez potřeby konektivity. [2]

1.1.2 NON-EMV standard

Tento standard není tak přísný, z hlediska bezpečnosti a nepodléhá bezpečnostním auditům. I proto se zde nevyužívají karty, vydávané bankovními asociacemi. Standard se využívá v nebankovním světě, obzvlášť pro stravenkové, palivové nebo věrnostní karty. Na

NON-EMV kartách jsou uloženy pouze statické informace, jako například číslo karty, držitel karty nebo expirace. Tyto informace jsou pomocí terminálu zaslány dál k online ověření.

1.2 Historie platebních terminálů

Platební terminály vznikly hlavně pro usnadnění práce obchodníků. Ještě v 50. letech 20. století musel obchodník každou kartu, se kterou chtěl kupující platit, telefonicky ověřit s vydavatelskou bankou. Bylo nutné prověření pravosti, platnosti a vlastníka karty. Další usnadnění v platebním procesu přišlo v 60. letech, kdy byl vyvinut mechanický imprinter. Ten jednoduše vytvořil doklad, který obsahoval údaje z karty. Pro vyplacení těchto plateb bylo nutné platební doklady zanést nebo odeslat do vydavatelské banky. [1]

Opravdový průlom ve světě platebních terminálů přišel v roce 1979, když společnost VISA (Visa International Service Association), díky platebním kartám s magnetickým proužkem uvedla první POS platební terminál, který uměl zpracovat data z proužku na kartě. Na počátku osmdesátých let začaly vznikat velké společnosti, zabývající se výrobou a vývojem platebních terminálů. Většina těchto firem je aktivní dodnes, mezi největší patří právě VeriFone, Ingenico nebo později založený PAX. Na Obrázku 1 lze vidět jeden z prvních platebních terminálů NETS, který byl uveden do provozu v roce 1980. [1]

Obrázek 1: Jeden z prvních platebních terminálů NETS z roku 1980 [1]

1.3 Rozdělení platebních terminálů

Platební terminály, se kterými se dnes a denně téměř každý z nás setkává, lze rozdělit do několika druhů.

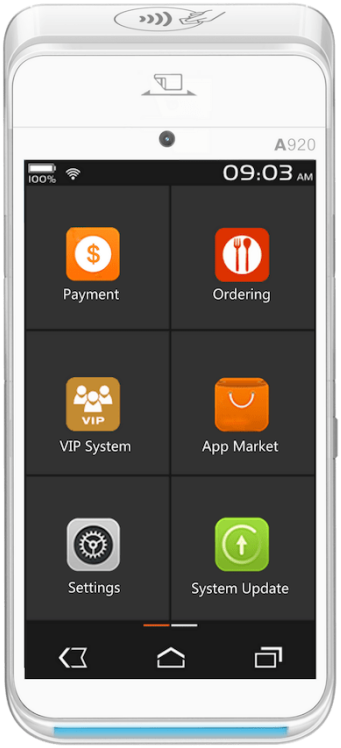
Stacionární platební terminály

Jedná se o terminály, které jsou často součástí větších obchodů. Převážně s nimi nelze manipulovat a často jsou pevně přikotveny. Ve většině případů jsou propojeny s pokladním systémem prodejce, na kterém jsou závislé. Tento druh terminálu je schopen zpracovat všechny druhy plateb, jako jsou čipové, bezkontaktní nebo platby pomocí magnetického proužku. Stacionární terminál, od společnosti Verifone, je znázorněn na Obrázku 2.

Obrázek 2: Terminál Verifone VX 520 [25]

Přenosné terminály

Jak už vyplývá z názvu, jedná se převážně o kompaktní terminály, které jsou pomocí bezdrátových technologií, připojeny do internetu nebo k pokladnímu systému. Převážně se s nimi lze setkat v menších obchodech nebo restauracích. Velkou výhodou je jednoduchá přenositelnost. Součástí také bývá tiskárna účtenek. Na Obrázku 3 je uveden kompaktní a jednoduše přenositelný platební terminál od společnosti PAX, který bývá často využíván i jako revizorské zařízení v dopravních podnicích.



Obrázek 3: Terminál PAX A920 [26]

MPOS terminály

Jedná se o malé terminály, jak lze pozorovat na Obrázku 4, které ovšem umožňují velkou škálu funkcí. Jsou pomocí bezdrátových technologií nejčastěji připojeny k mobilnímu telefonu, který slouží, jako obsluha pro daný terminál. Tyto terminály obsahují pouze certifikované EMV jádro, sloužící ke komunikaci s kartou. Všechny ostatní funkce, jako je zadávání plateb a komunikace s autorizačním centrem, obstarává připojené zařízení. Součástí zařízení bývá také mobilní aplikace, která slouží pro obsluhu MPOS terminálu. Velkou výhodou jsou nízké pořizovací náklady a kompaktnost. Terminály přijímají naprostou většinu karet a poradí si také s technologií NFC (Near Field Communication). Z důvodu malých rozměrů chybí u tohoto druhu terminálu tiskárna účtenek, kdy doklady o zaplacení odesílá obchodník elektronicky.

Obrázek 4: MPOS terminál SumUp [1]

1.4 Terminal management system – TMS

Jak už z názvu kapitoly vyplývá, tak se jedná o systém, pro správu platebních terminálů. Každá společnost, která se zabývá správou platebních terminálů má TMS implementovanou odlišným způsobem, avšak hlavním úkolem TMS je pečovat o síť terminálů a pokrýt tím celý jeho životní cyklus, od založení, naklíčování, až po úpravu konfigurace. Další důležitou funkcí TMS je vzdálená aktualizace aplikací a změna parametrů v terminálu. Veškerý přenos souborů a klíčů je tvořen obvykle pomocí těchto komunikačních protokolů:

- **SFTP** (Secure File Transfer Protocol) – FTP (File Transfer Protocol) přes SSH (Secure Shell);
- **FTPS** (File Transfer Protocol Secure) – FTP přes SSL (Secure Sockets Layer);
- **TCP** (Transmission Control Protocol);

Kromě správy terminálů lze pomocí TMS definovat jednotlivé obchodníky a jejich obchodní místa, povolit nebo zakázat různé vydavatele karet nebo přímo nahrávat soubory do daných terminálů. Moderní TMS obsahují například i GPS (Global Positioning System) informace o platebním terminálu a jeho zobrazení na mapě.

TMS je nejčastěji provozovaný, jako webová aplikace, která je dostupná pouze z vnitřní sítě vybrané společnosti. Systém pro správu terminálů musí splňovat přísná bezpečnostní kritéria, podle normy ISO27000. Tento standard řídí informační bezpečnost v organizacích. I

proto TMS prochází auditorskou kontrolou, pravidelnými penetračními testy a jsou u něj prováděny pravidelné aktualizace.

1.5 Tok EMV transakce

Platební proces probíhá v několika krocích, které jsou popsány níže. Jednotlivé body se odvíjí od druhu transakce a také se liší napříč firmami, základní kroky, které jsou nejčastější, při zpracování EMV platební transakce jsou následující:

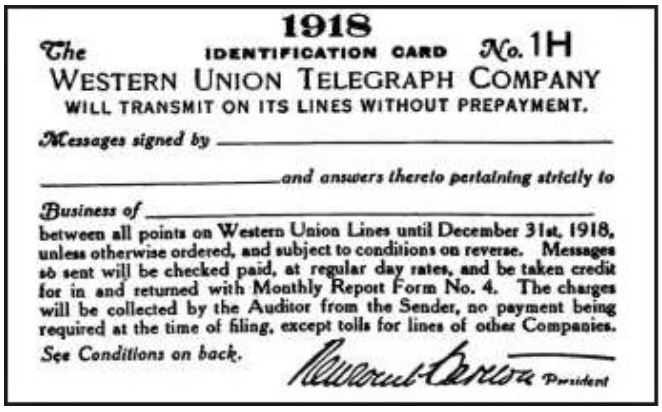
1. Zákazník přiloží kartu k platebnímu terminálu a následně dojde k přečtení dat z platební karty, pomocí terminálové aplikace.
2. Získaná data jsou ověřena v offline režimu, kde se ověří, jestli je použité číslo karty v povoleném rozsahu a zároveň se zkontroluje platný certifikát vydavatele karty.
3. Následně dojde k zahájení platební transakce.
4. V dalším kroku zákazník zadá PIN, podpis nebo dojde k ověření pomocí CVM.
5. Po ověření dojde ke kontrole různých karetních limitů.
6. Pokud je vše v pořádku, terminál schválí transakci. Dále musí dojít ke schválení karty, buď online nebo offline cestou.
7. V dalším kroku dojde k odeslání transakčních dat k autorizaci.
8. Pokud proběhnou všechny předešlé kroky bez problémů, dojde k dokončení úspěšné transakce. [3]

2 PLATEBNÍ KARTY

S platebními kartami se každý setkává téměř každý den. V následujících podkapitolách bude popsaná stručná historie karet, jejich typy, princip fungování a zabezpečení.

2.1 Historie platebních karet

Vůbec první platební karta byla vydána v roce 1914. Za zrodem platebních karet stála americká telefonní a telegrafní společnost Western Union Telegraph Company, jejichž karta je uvedena na Obrázku 5. Dalším milníkem byl rok 1924, kdy firma General Petroleum Corporation of California, dnes známá jako Mobil Oil nabídla svým klientům kreditní kartu, pomocí které mohli platit pohonné hmoty. Následně se do konkurenčního boje v poskytování kreditních karet přidávaly další společnosti, jako například AT&T nebo hotely a restaurace. Ověřenost pravosti majitele karty probíhala na základě porovnání podpisu na kartě a podpisu, který poskytl zákazník. [4]


1918

The IDENTIFICATION CARD No. 1H

WESTERN UNION TELEGRAPH COMPANY

WILL TRANSMIT ON ITS LINES WITHOUT PREPAYMENT.

Messages signed by _____

_____ *and answers thereto pertaining strictly to*

Business of _____

between all points on Western Union Lines until December 31st, 1918, unless otherwise ordered, and subject to conditions on reverse. Messages so sent will be checked paid, at regular day rates, and be taken credit for in and returned with Monthly Report Form No. 4. The charges will be collected by the Auditor from the Sender, no payment being required at the time of filing, except tolls for lines of other Companies.

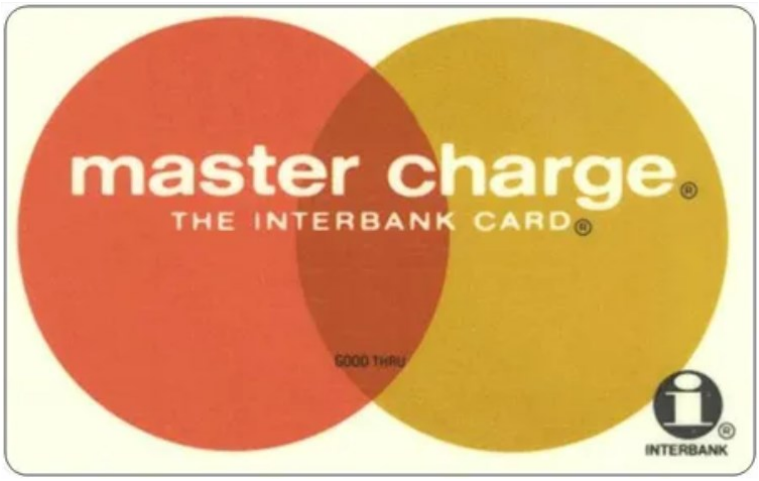
See Conditions on back. _____ President

Obrázek 5: Karta Western Union Telegraph Company [27]

První bankovní platební karta byla vydána bankovní společností The Franklin National v roce 1951. Následně o sedm let později byla společností Bank of America mezi její klienty nabídnuta první platební karta, vyrobená z plastu, takže bylo možné při platbě ověřit pravost karty nejen podpisem, ale i jinými snímači. V začátcích se pro potisk platební karty využívalo technologie sítotisku, poté se ale přešlo na technologii ofset. Karta byla později pojmenována VISA a byla nabízena i dalším bankovním společnostem. [4]

O několik let později, konkrétně v roce 1967 bylo spojením čtyř bank vytvořena společnost Western States Bancard, která začala vydávat karty MasterCharge. Karta je zobrazena níže

na Obrázku 6. Tyto karty si o dva roky později odkoupila firma Interbank Card Association, ze které později vznikla dnes známá bankovní asociace MasterCard.



Obrázek 6: Karta Master Charge – později MasterCard [28]

Právě v těchto letech byly karty vybaveny magnetickým pruhem a postupně se začaly rozvíjet sítě bankomatů a platebních terminálů. V 80. letech banky začaly nabízet čipové karty a velmi oblíbené začaly být debetní karty. V dalších letech vznikly další bankovní i nebankovní systémy, které jsou provozovány dodnes a jsou zaštiťovány společnostmi, jako například: VISA, Europay/MasterCard, American Express, JCB nebo Diners Club. [4]

2.2 Mezinárodní bankovní asociace

Aby mohly banky konkurovat již zaběhlým bankovním systémům American Express a Diners Club, rozhodly se vytvořit mezinárodní bankovní asociace VISA a Europay/MasterCard. Pomocí těchto asociací byla vytvořena efektivní infrastruktura, pomocí které se dalo jednoznačně identifikovat vydavatele karty, ověřit a zpracovat transakce nebo stanovit jednotná pravidla pro používání karet. Obě bankovní asociace jsou vedeny jako neziskové, jejich zisk se odvíjí od počtu realizovaných transakcí, provozovaných služeb a počtu vydaných platebních karet. [5]

2.2.1 Struktura bankovní asociace

Bankovní asociace mají jednoznačně danou strukturu, pomocí které je dosažena vysoká úroveň bezpečnosti, při zpracování transakcí a dalších službách. Nejčastěji s asociacemi spolupracují přímo banky, ale v některých případech se může jednat i o jiné instituce. Asociace mají následující úrovně:

- **Principal Member** – jedná se o společnosti, které přímo zajišťují vydávání platebních karet, provozují sítě bankomatů a zajišťují zúčtovací služby pro obchodníky.
- **Association Member** – jedná se o firmy, které zabezpečují služby, spojené s platebními kartami.
- **Merchant Bank Member** – organizace, které zajišťují příjem bankovních karet a celkově zprostředkovávají platební operace v obchodních sítích. [4]

2.3 Typy platebních karet

Bankovní asociace v dnešní době nabízí mnoho druhů karet, nejčastěji se odlišují typem platby, která pomocí nich lze provést.

2.3.1 Platební karty s magnetickým proužkem

Jedná se o nejstarší platební karty, které umožňovaly realizaci transakce, bez nutnosti ověření podpisu, protože data o majiteli karty jsou přímo v kartě. Platební data jsou uložena na pásku, který se skládá z velkého množství kovových částí, které lze zmagnetizovat a tím uložit požadovaná data. Uložení informací na magnetickém proužku je dané podle normy ISO/IEC 7813. Právě tato norma určuje, že jsou informace o platební kartě uloženy ve dvou nebo třech stopách. Magnetický proužek uchovává základní informace, jako jsou platnost karty, jméno vlastníka a další ověřovací a bezpečnostní prvky. [6]

Kromě magnetického proužku může být na kartě umístěný i podpisový proužek, který slouží k porovnání podpisu na kartě a na účtence, kterou kupující podepíše. Jak je uvedeno výše, každý magnetický proužek se skládá z jednotlivých stop, jejich složení je následující:

- **Stopa 1:** První a zároveň nejstarší část magnetického pruhu slouží k uložení čísla karty a jeho vlastníka.
- **Stopa 2**: Tato stopa byla vyvinuta k odbavení online transakcí. Obsahuje 40 numerických znaků, obsahujících číslo karty.
- **Stopa 3**: Na rozdíl od předešlých stop, které byly určeny výhradně pro čtení, tuto stopu lze přepisovat. Například je zde možné nalézt finanční limit klientovy karty. [7]

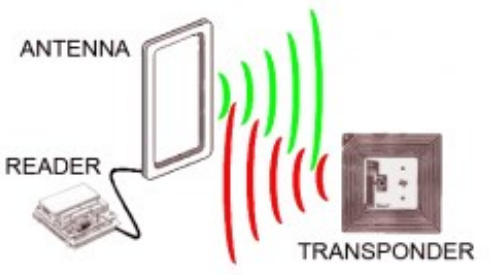
2.3.2 Čipové platební karty

Oproti kartám s magnetickým proužkem čipové karty vynikají hlavně svou bezpečností. Karta nemá schopnost pouze zaznamenávat informace, ale obsahuje v sobě mikropočítač, který je napájen a komunikuje s okolím. Taková karta obsahuje vlastní operační, ale i souborový systém. [6]

2.3.3 Bezkontaktní platební karty

Pro pohodlnou realizaci platby byly vyvinuty platební karty, s bezkontaktním čipem. Aby bylo možné bezkontaktní platbu realizovat, je zároveň nutné mít k tomu určený terminál, který obsahuje bezkontaktní modul. Na trhu jsou momentálně tři největší bezkontaktní platební systémy a to Visa – PayWave, MasterCard – PayPass a American Express – ExpressPay. Pro bezkontaktní platby se využívá převážně dvou technologií a to: RFID (Radio Frequency Identification) a NFC. [8]

V případě RFID se využívá radiofrekvenční identifikace, která bezdrátově identifikuje např. osoby nebo zboží. Princip fungování je založený na komunikaci čtečky a transpondérů, jinak řečeno tagů. Tagy jsou elektromagnetické součástky, které nevyžadují pro svůj provoz mnoho energie, i proto jsou napájeny energií z elektromagnetických vln, které produkuje samotná čtečka karet. Tagy přijímají signál pomocí tagových antén, které energii pohltí a nasměrují ji k čipu, tím ho aktivují. Touto energií se akumulátor u karty nabije a odešle odpověď čtečce. Samotná RFID čtečka obsahuje RF modul, který slouží, jako vysílač, i jako přijímač radiových signálů. Dále je čtečka složená z jednotlivých zesilovačů, modulátorů a demodulátorů, aby byla schopna vysílat a přijímat informace z čipu, jak je znázorněno na Obrázku 7. [9]



Obrázek 7: RFID bezkontaktní technologie [9]

Další a dnes zároveň nejvíce využívaná technologie v rámci bezkontaktních platebních karet je NFC. Celým názvem Near Field Communication vyplývá ze starší a výše uvedené technologie RFID. Velkou výhodou této technologie je, že zařízení mezi sebou bezkontaktně komunikují na velmi malou vzdálenost, takže odposlouchávání nebo nechtěné přiložení např. telefonu nebo karty k platebnímu terminálu je málo pravděpodobné. Tato bezkontaktní technologie pracuje na bázi krátkých radiových vln a je řízená standardem ISO/IEC 14443, ve kterém je zároveň definovaná komunikační frekvence 13,56 MHz. V současné době je tato technologie hojně využívaná nejen u bezkontaktních platebních karet, ale také u telefonů nebo hodinek. [10]

3 KRYPTOGRAFIE A ŠIFROVÁNÍ

Následující kapitola se obecně zaměřuje na šifrování, na základní pojmy v rámci problematiky kryptografie a popisuje jednotlivé druhy šifrování. Šifry obecně slouží k převedení prostého textu do nečitelné podoby. Tento proces by nebyl možný, bez přítomnosti klíče, který slouží k zašifrování a bez kterého by nebylo možné zašifrovaný text přečíst.

3.1 Základní pojmy v oblasti kryptografie

- **Kryptologie:** obecně se jedná o vědní obor, kde je hlavní důraz kladen na utajení obsahu zprávy. Tato vědní disciplína se dělí na dva podobory, a to na kryptografii a kryptoanalýzu. Někdy se k nim připojuje i steganografie. [11]
- **Kryptografie:** tato vědní specializace se zabývá využitím matematických metod u prvků informační bezpečnosti, jako jsou například neporušitelnost (integrita) dat, ověření vlastnictví (původ dat) nebo důvěrnost zprávy. Hlavním účelem kryptografie je uvést výslednou zprávu do nečitelné podoby, pro případ, že dojde k nechtěnému odposlechu třetí stranou. Postupně se tento vědní obor vyvíjel. Na počátku bylo hlavním cílem vyvinout odolné algoritmy, které sloužily k ukrytí přenášené zprávy, následně se v rámci vědní disciplíny přidala nutnost jednoznačného určení osoby odesílatele (identifikace) a ověření správnosti zprávy přijímající stranou (autentizace). [11]
- **Kryptoanalýza:** jedná se o protiklad kryptologie, kdy hlavním cílem není vymyslet algoritmus, který co nejlépe ukryje přenášenou zprávu, ale snaha analyzovat odolnost kryptografických algoritmů. Kryptoanalytikové se snaží narušit kryptografické systémy a získat tím původní podobu zašifrované zprávy. [11]
- **Steganografie:** hlavním úkolem steganografa je ukrytí existence přenášené zprávy. Někdy bývá přenášená zpráva předávaná ve srozumitelné podobě, ale úkolem steganografie je skrytí zprávy, aby o ní útočník neměl žádné informace. [11]
- **Šifrovací (kryptografický) systém:** jedná se o libovolný systém, pomocí kterého dochází k převedení otevřeného textu do nečitelné (šifrované) podoby všem osobám, kromě adresáta. [11]

3.2 Stručná historie kryptologie

Už od začátku bylo hlavním cílem kryptologie utajení přenášené zprávy. Nejdřív bylo šifrování realizované pomocí záměny, jednoduché a dvojité transpozice nebo Vigenerovy šifry. Následně ale bylo třeba odolnější algoritmy, a to hlavně z důvodu druhé světové války a nutnosti přenesení přísně utajených informací. Právě v této době proti sobě stála kryptoanalýza, která sloužila, jako účinná zbraň proti protivníkovi a na druhé straně kryptografie, která sloužila jako ochrana citlivých informací. [12]

Poválečná doba byla hlavně ve znamení Claude E. Shannona a jeho prací The Mathematical Theory of Communication[1] a rok poté díla Communication Theory of Secrecy Systems[2], který bývá považován za základ moderní kryptologie. Zároveň stanovil několik důležitých pojmů v rámci kryptologie, a to entropii jazyka, vzdálenost jednoznačnosti nebo dokázal absolutní bezpečnost Vernamovy šifry. [12]

Dalším důležitým milníkem byla 70. léta, kdy přišla počítačová revoluce. Začaly ve velkém množství vznikat blokové šifry a byla také objevena kryptografie s veřejným klíčem. V této době vznikla v USA veřejná státní šifra DES (Data Encryption Standard), která byla později prolomena nástrojem DES-Cracker. O několik let později byl zveřejněn asymetrický šifrovací systém RSA. V roce 1982 vstoupila kryptologie v povědomí všech vyspělých států. Začaly se konat první mezinárodní konference, díky čemuž se s velkou podporou státních organizací podařilo posunout úroveň kryptologie na vyšší úroveň, až do současného stavu. [12]

3.3 Základní matematické operace v kryptografii

V rámci oboru kryptografie se pracuje se složitými matematickými operacemi, ale jejich základ tvoří převážně základní operace, které jsou součástí všech šifrovacích funkcí.

3.3.1 Logické operace

Jedná se o operace s bity, tedy proměnnými, které můžou nabývat hodnot 1 nebo 0, viz. Tabulka 1. Nejčastěji se vyskytují operace disjunkce (logický součet), exkluzivní disjunkce (XOR), negace nebo konjunkce (logický součin).

---

[1] SHANNON, Claude Elwood a Warren WEAVER. The mathematical theory of communication. Chicago: University of Illionois Press, 1998. ISBN 0252725484.

[2] SHANNON, Communication Theory of Secrecy Systems, Bell Systems Technical Journal,Vol. 28, 1948.

$\wedge - Konjunkce\ (AND),\ \vee - Disjunkce\ (OR),\ \neg - Negace\ (NOT),$
$\oplus - Exkluzivní\ disjunkce\ (XOR)$

Tabulka 1: Pravdivostní tabulka logických operací [29]

A	B	¬A	¬B	A∨B	A∧B	A⊕B
0	0	1	1	0	0	0
0	1	1	0	1	0	1
1	0	0	1	1	0	1
1	1	0	0	1	1	0

3.3.2 Substituce

Další velmi využívanou operací je substituce, která se často značí velkým písmenem ‚S'. Tato operace vstupnímu číslu ‚x' přiřadí podle předem daného pravidla nebo například substituční tabulky jiné číslo $y = S(x)$. V Tabulce 2, která je uvedená níže lze vidět příklad substituce:

Tabulka 2: Příklad substituce [29]

X	0	1	2	3
Y	13	15	7	5

Z tabulky například vyplývá pomocí substituce následující: $S(3) = 5$. [13]

3.3.3 Operace modulo

Následující matematická operace se provádí se dvěma celými čísly, často označovanými ‚c' a ‚n', kdy číslo $n > 0$ je nazýváno modulus. Výsledkem operace modulo je zbytek po celočíselném dělení $(c: n)$. Formální zápis operace je následující. [13]

$$c\ mod\ n = c - q \cdot n, kde\ q = \left\lfloor \frac{c}{n} \right\rfloor$$

3.4 Základní rozdělení šifrování a funkcí

Tato podkapitola se věnuje základnímu rozdělení šifer a popsání jejich funkcí. Šifrování lze rozdělit do tří hlavních bloků, symetrické, asymetrické a jednosměrné šifry.

3.4.1 Jednosměrné funkce

U jednosměrných funkcí se nejedná přímo o utajovací nebo autentizační kryptosystémy, ale jedná se o vztah, pomocí kterého lze pro libovolný vzor ‚x' jednoduše vypočítat obraz, ale zpětně je velice obtížné, až nemožné vypočítat jeho vzor. U jednosměrných funkcí se vytváří otisk originální zprávy, kdy výstupní otisk je závislý na všech bitech vstupního řetězce. Nejčastěji se tyto algoritmy využívají ke kontrole integrity dat, k tvorbě digitálních podpisů nebo k rychlému vyhledávání. [14]

Tento druh funkcí lze rozdělit do dvou kategorií. První z nich jsou kryptografické jednosměrné funkce, mezi které lze zařadit například diskrétní logaritmus eliptických křivek nebo faktorizace součinu prvočísel. Do druhé kategorie spadají hashovací funkce, které slouží k přiřazení krátkého bitového řetězce přenášené zprávě. Tento řetězec následně slouží, jako reprezentant dané zprávy. [13]

Mezi nejvíce využívané algoritmy se řadí SHA-2 a jednosměrná funkce MD5, obě funkce jsou popsány níže.

Algoritmus SHA

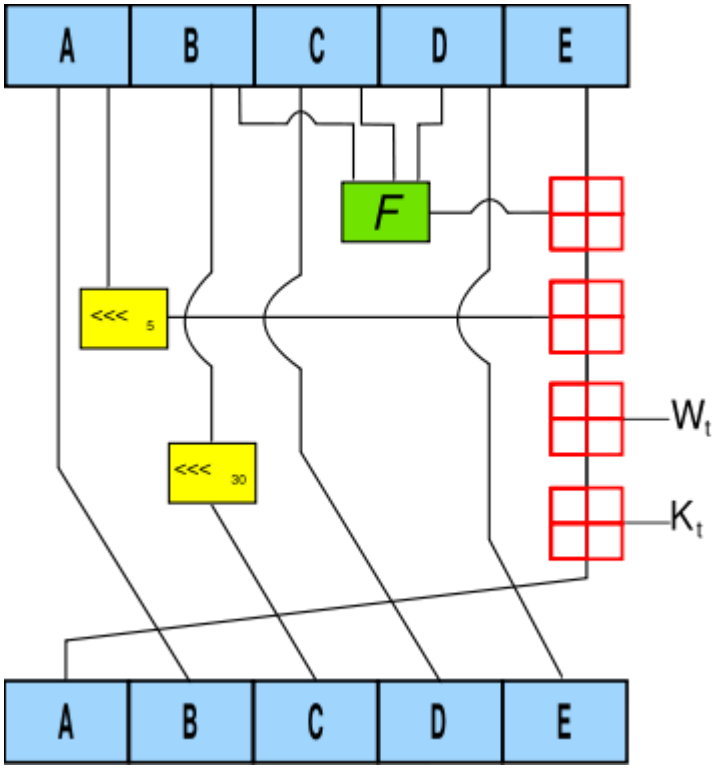
Jedná se o kryptografický hashovací algoritmus, který byl původně navržený Národní bezpečnostní agenturou ve Spojených státech amerických. Celkově existuje pět druhů SHA algoritmu a to SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. Poslední čtyři se označují, jako SHA-2, které je v současnosti využíváno nejvíce, v rámci hashovacích funkcí. [14]

Pro zjednodušení k vysvětlení bude použit algoritmus SHA-1, kde lze lépe vysvětlit princip algoritmu, avšak SHA-2 pracuje na velmi podobném principu.

Obecně SHA-1 počítá zmenšenou reprezentaci zprávy o délce 160 bitů. Výsledný hash lze využít pro vstup v rámci digitálního podpisu nebo například u bankovních transakcí a elektronické poště. Hlavní funkcí algoritmu je ověření integrity dat a zároveň jejich autentičnosti. [14]

Algoritmus SHA-1 rozkládá zprávu na posloupnost bitů. Zpráva se rozdělí na bloky o velikosti 512 bitů, z čehož vyplývá 16 slov po 32 bitech. V dalším kroku dojde k doplnění dat, aby dosahovala násobku 64 bitů, kdy posledních 64 bitů je rezervováno pro délku originální zprávy, která vstupuje do algoritmu. Celkově zpráva obsahuje 16*n bloků, kdy platí, že n je větší než 0. Každý blok bývá označován, jako posloupnost $M_1 \dots M_n$. Součástí algoritmu je

tabulka W, do které jsou uloženy jednotlivé zpracované bloky a tabulka K, která je stejná, pro všechny bloky a obsahuje předem specifikované konstanty. Každá tabulka se skládá z 80 řádků. Pro samotný výpočet je použito 5 proměnných A, B, C, D, E a každý datový blok se počítá samostatně. Inicializační hodnoty proměnných jsou vytvořeny z konstant označených $H0 \dots H_4$. V rámci výpočtu dojde 80krát k přepočtu proměnných a výsledky jednotlivých bloků jsou sečteny. Následně jsou k blokům připočteny originální konstanty $H0 \dots H_4$. Výsledek je složen ze 160-ti bitového řetězce, který je složen z pěti slov. Níže uvedený Obrázek 8 reprezentuje jedno opakování funkce SHA-1, včetně popisu použitých pojmů. [14]



Obrázek 8: Algoritmus SHA-1 [14]

A, B, C, D, E – 32 bitové proměnné

<<< - specifikuje rotaci bitů vlevo o určitý počet pozic

F – nelineární funkce

W_t – rozšířené slovo

K_t – konstanta opakování

$index_t$ –iterace opakování

Algoritmus MD5

Jedná se o hešovací algoritmus, který byl navržen v roce 1991 profesorem Ronaldem R. Rivestem. Jeho vznik je odůvodněný nedostatečným zabezpečením algoritmu MD4. Hlavní využití algoritmu je pro ověření integrity dat, během přenosu zprávy, tedy zjištění, jestli byl během přenosu soubor narušený třetí stranou nebo ne. Funkce je například využívaná v Unixových operačních systémech nebo v internetovém standardu RFC 1321. [15]

U algoritmu MD5 může být na vstupu zpráva o libovolné délce, která je rozdělena na jednotlivé bloky o velikosti 512 bitů, konkrétně 16 slov o velikosti 32 bitů. Prvních 448 bitů v bloku patří zprávě a dalších 64 bitů je určených pro specifikaci délky původní zprávy. Ke zprávě je přidán 1 bit, který následují nulové bity, aby bylo dosaženo velikosti zprávy 448 bitů. V rámci výpočtu je využito čtyř proměnných (A, B, C, D), u kterých jsou stanoveny inicializační hodnoty a jejich velikost je 32 bitů. Dále jsou definované čtyři pomocné funkce, jak lze vidět na Obrázku 9, kdy na začátku do funkcí vstupují tři 32bitová slova a na výstupu je jedno slovo o stejné velikosti 32 bitů. [14]

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$

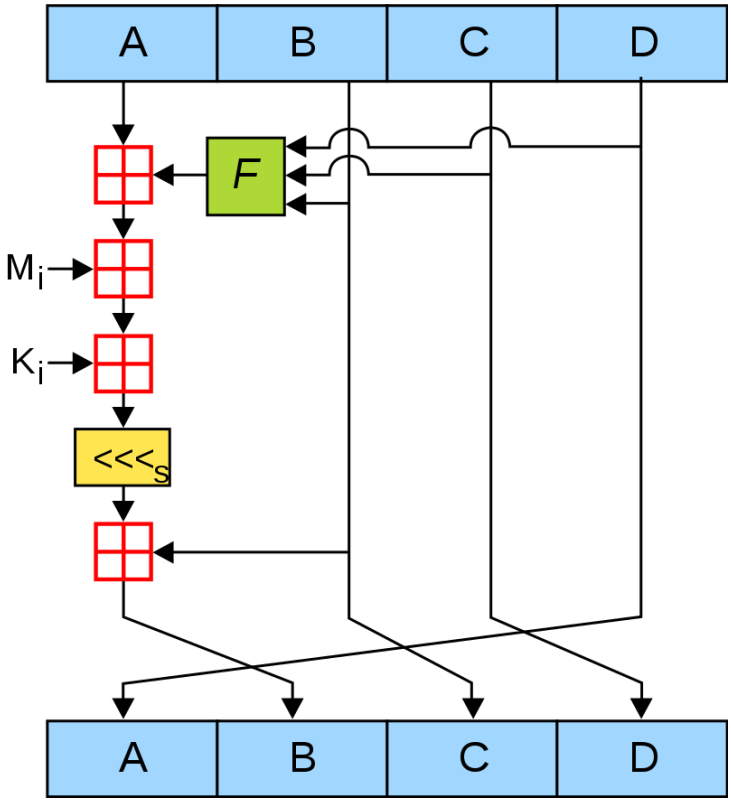
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$

$$H(X,Y,Z) = X \oplus Y \oplus Z$$

$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

$$\wedge - AND,\ \vee - OR,\ \neg - NOT,\ \oplus - XOR$$

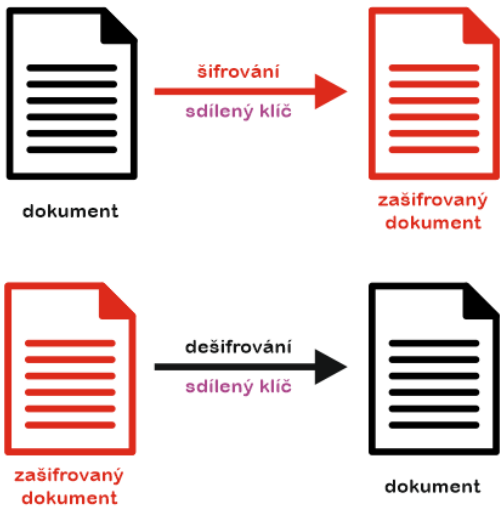
Každá z výše uvedených funkcí je realizovaná 16krát celkem ve čtyřech kolech. Výsledný otisk tvoří proměnné A, B, C a D, ke kterým je přičtena jejich inicializační hodnota. Blok ve schématu označený jako F znázorňuje nelineární funkci, kdy v každé iteraci, která je označena indexem i, je použita jedna funkce, která je odlišná pro všechna kola. Blok M_i o velikosti 32 bitů znázorňuje vstupní zprávu a K_i označuje 32bitovou konstantu, u které se hodnota odvíjí od zvolené operace. [14]



Obrázek 9: Algoritmus MD5 [14]

3.4.2 Symetrické šifrování

Následující druh šifrování funguje na principu využití stejného klíče, pro šifrování i dešifrování, viz. Obrázek 10. Proto je nutné, aby odesílatel i příjemce měli dopředu domluvený klíč, který je nejlépe naprosto náhodný. Odesílatel na začátku pomocí klíče odesílanou zprávu zašifruje a příjemce pomocí stejného klíče zprávu dešifruje.



Obrázek 10: Symetrické šifrování [16]

Jedná se o velice efektivní a rychlé šifrování. Mezi nevýhody symetrického šifrování patří bezpečná distribuce klíče, který je nutný pro šifrování a dešifrování a dále škálovatelnost. Pokud mezi sebou komunikuje 500 osob, potom bude nutné 499 rozdílných klíčů pro vytvoření separátních komunikačních kanálů. Mezi nejznámější symetrické šifry se řadí Advanced Encryption Standard (AES), Data Encryption Standard (DES), respektive 3DES. [16]

Symetrická šifra DES (3DES)

DES symetrický šifrovací algoritmus vznikl v roce 1976, kdy byl přijat americkými bezpečnostními úřady. Tento algoritmus je v upravené formě 3DES využívaný výrobci platebních terminálů. Podle normy PCI DSS je tento šifrovací algoritmus povolený u platebních terminálů do roku 2023, poté bude nahrazený symetrickým algoritmem AES.

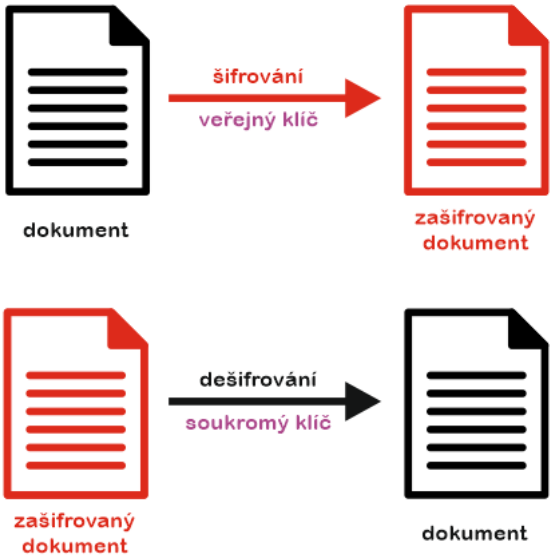
DES spadá do kategorie blokových šifer, tedy nešifrují se data pomocí klíče po jednotlivých bitech, ale šifrovaný text se rozdělí do bloků o stejné velikosti a každý se šifruje zvlášť. Tím se zvyšuje rychlost, ale roste náročnost na implementaci.

Algoritmus je založen na opakujících se matematických operacích, konkrétně v šestnácti opakováních, kterým se říká rundy. Převážně se jedná o matematické operace typu permutace a substituce. Tento proces se kombinuje se sub-klíči, které se sčítají s bloky bitů, pomocí logické operace XOR. Data určená pro šifrování jsou rozdělena do bloků po 64 bitech, se kterými se provádí výše uvedené matematické operace. Nejdříve se provede permutace dat, pomocí připravené tabulky. V dalším kroku, který je v rámci šifrování důležitý se přidá kryptografický klíč, který je přidáván po jednotlivých bitech a dochází k transformaci dat pomocí XOR funkce. Následně se provede nelineární substituce. Vše se provádí v několika rundách. Vícenásobným šifrováním vzniká 3DES šifra, která zvyšuje odolnost proti rozšifrování. [17]

3.4.3 Asymetrické šifrování

Důvodem vzniku asymetrického šifrování bylo omezení sdíleného klíče, který se využívá u symetrického šifrování. Proto se u asymetrického šifrování využívají dva klíče, jeden pro šifrování, druhý pro dešifrování, jak je znázorněno na Obrázku 11. Na začátku odesílatel požádá příjemce o jeho šifrovací klíč, pomocí kterého zašifruje odesílanou zprávu a příjemce pomocí něj následně zprávu dešifruje. Dešifrování není ale možné pouze pomocí šifrovacího klíče. Tento klíč je zaslán společně s šifrovaným objektem, klíči se říká veřejný klíč. Protikladem je soukromý klíč, který je nutné uchovat v tajnosti. Z něj lze odvodit veřejný klíč,

naopak to možné není. Pomocí soukromého klíče si příjemce následně dešifruje zprávu. Asymetrické šifrování má velkou výhodu v tom, že není nutné sdílení soukromého klíče, ale na druhou stranu se zvedá výpočetní náročnost. To řeší kombinace asymetrického a symetrického šifrování. Mezi nejznámější asymetrické šifry patří RSA. [16]



Obrázek 11: Asymetrické šifrování [16]

Asymetrická šifra RSA

Jedná se o algoritmus s veřejným klíčem, který vznikl v roce 1977. Hlavní využití je v rámci elektronického podpisu a obecně šifrování. Bezpečnost RSA šifry je založena na faktu, že rozložení čísla na součin prvočísel (faktorizace) je velmi obtížná matematická operace. [18]

4 HARDWARE SECURITY MODULE (HSM)

Hardware Security Module, zkráceně HSM je specializovaný certifikovaný hardwarový prostředek, určený pro bezpečné uchování a generování klíčů a obecně k vykonávání kryptografických operací.

HSM pokrývá celý životní cyklus klíče, od vytvoření, po šifrování, až po bezpečný transport klíče. Využití HSM je nutné, pro splnění auditorských podmínek, v rámci PCI (Payment Card Industry) zóny.

HSM si lze jednoduše představit, jako uzavřený objekt, který je provozován v důvěryhodném prostředí – bezpečná infrastruktura, bez možnosti zneužití a neoprávněného přístupu. Každé HSM splňuje následující podmínky:

- je postaveno na specializovaném a certifikovaném hardwaru, provozováno ve specializovaných místnostech;
- operační systém, který v nich běží, je zabezpečený a specializovaný na běh v HSM;
- přístup není do celé sítě, ale pouze do omezených částí, které se řídí podle přísných bezpečnostních podmínek. [19]

4.1 HSM Key Management

V rámci hardware security modulu se nikdy nepracuje s nešifrovaným klíčem. Všechny klíče, které jsou v rámci HSM zpracovány jsou šifrovány, pomocí LMK (Local Master Key) klíče, který je uložen v bezpečném prostředí HSM. Dále jsou popsány jednotlivé klíče, které tvoří strukturu HSM. Uvedená nebo velmi podobná struktura se využívá u většiny výrobců, konkrétně je popsáno HSM od společnosti Dymar. [20]

LMK – Local Master Key

Local Master Key lze označit jako hlavní klíč v rámci celého HSM. Slouží, jako ochrana všech ostatních klíčů napříč společností, aby se nešířily v nešifrované podobě. I v případě, že firma, nejčastěji banka vlastní více HSM, tak LMK je vždy jeden, v rámci celé sítě. Skládá se ze setu obvykle 40 DES klíčů. Není určený k šifrování dat, ale jeho hlavní využití je šifrování ostatních klíčů, aby se v rámci HSM nikdy nepracovalo s nešifrovaným klíčem, ani mimo HSM.

Na začátku jsou vygenerovány tři komponenty, které jsou rozděleny mezi tři zaměstnance dané společnosti. Každý zaměstnanec vloží svou komponentu do HSM, pomocí čipové

karty, splňující normu ISO 7816. Obvykle každý zaměstnanec obdrží dvě karty, se kterými udělá totožnou operaci, kdy jedna karta vždy zůstane, jako záložní. Po vložení karty dojde k jejich formátování a každý zaměstnanec vyplní základní údaje, jako jsou PIN, formát času nebo uživatelské jméno.

Jakmile jsou karty všech tří osob naformátovány, opět se postupně vloží do HSM, kde každá osoba zadá PIN a postupně se na karty zapíšou LMK komponenty a ID z HSM. V posledním kroku se karty opět vloží do HSM, kdy zadáním LMK ID, které bylo každé kartě v přechozím kroku přiřazeno a PINu postupně vznikne finální LMK klíč. [20]

ZMK – Zone Master Key

Zone Master Key (ZMK) se využívá v rámci HSM, pokud společnost, například banka potřebuje přepravit klíče k externím firmám, jako jsou například MasterCard nebo Visa. Často se přepravuje např. PIN blok. Pro tento případ se využívá právě ZMK.

Zone Master Key je umístěn v rámci sdílené sítě, mezi HSM a jedním nebo více objekty. Je určen pro to, aby šifroval přenášené klíče. ZMK je šifrován jedním párem LMK. [21]

ZPK – Zone PIN Key

Zone PIN Key (ZPK) slouží k šifrování dat, která jsou přenášena nejčastěji mezi bankou obchodníka a bankou plátce. Pro přenos je ZPK šifrován pomocí Terminal Master Key (TMK) a pro práci, v rámci HSM je šifrován pomocí LMK. [22]

TMK (TTK) – Terminal Master Key

Jedná se opět o klíč, který šifruje další klíč, nikoliv data. Využívá se pro distribuci klíčů v rámci místní sítě například na určitý POS (Point Of Sale) terminál. [20]

TAK – Terminal Authentication Key

Terminal Authentication Key (TAK) slouží k vytvoření a ověření tzv. Message Authentication Code (MAC), pro data přenášená v rámci lokální sítě mezi terminálem a bankou. MAC je kryptografická funkce, v tomto případě sloužící k ověření platnosti dat. [20]

PVK – PIN Verification Key

PIN Verification Key (PVK) se využívá ke generování a ověření pinových dat. Hlavním účelem klíče je potvrzení správnosti PIN kódu. [23]

CVK – Card Verification Key

Card Verification Key (CVK) - principem je tento klíč velice podobný předchozímu PVK, ale namísto generování a ověřování pinových dat, ověřuje data týkající se platební karty. [20]

5 PROCES KLÍČOVÁNÍ PODLE PCI DSS NORMY

Aby bylo možné na platebním terminálu reálně provádět transakce, je nutné, aby splňoval bezpečnostní normy a měl v sobě uložené klíče. Tyto klíče jsou využívány pro šifrovaný přenos, při ověřování transakcí. Samotný proces klíčování se nazývá Key Injection Process.

Klíčování je realizované pomocí klíčovacího zařízení (Key Loading Device – KLD) dodávaného výrobcem terminálů. Samotný proces klíčování probíhá v zabezpečené místnosti pod kamerovým dohledem. V následující podkapitole bude popsán proces klíčování ve společnosti LANDI Commercial Equipment Co., Ltd.

5.1 Klíčování ve společnosti

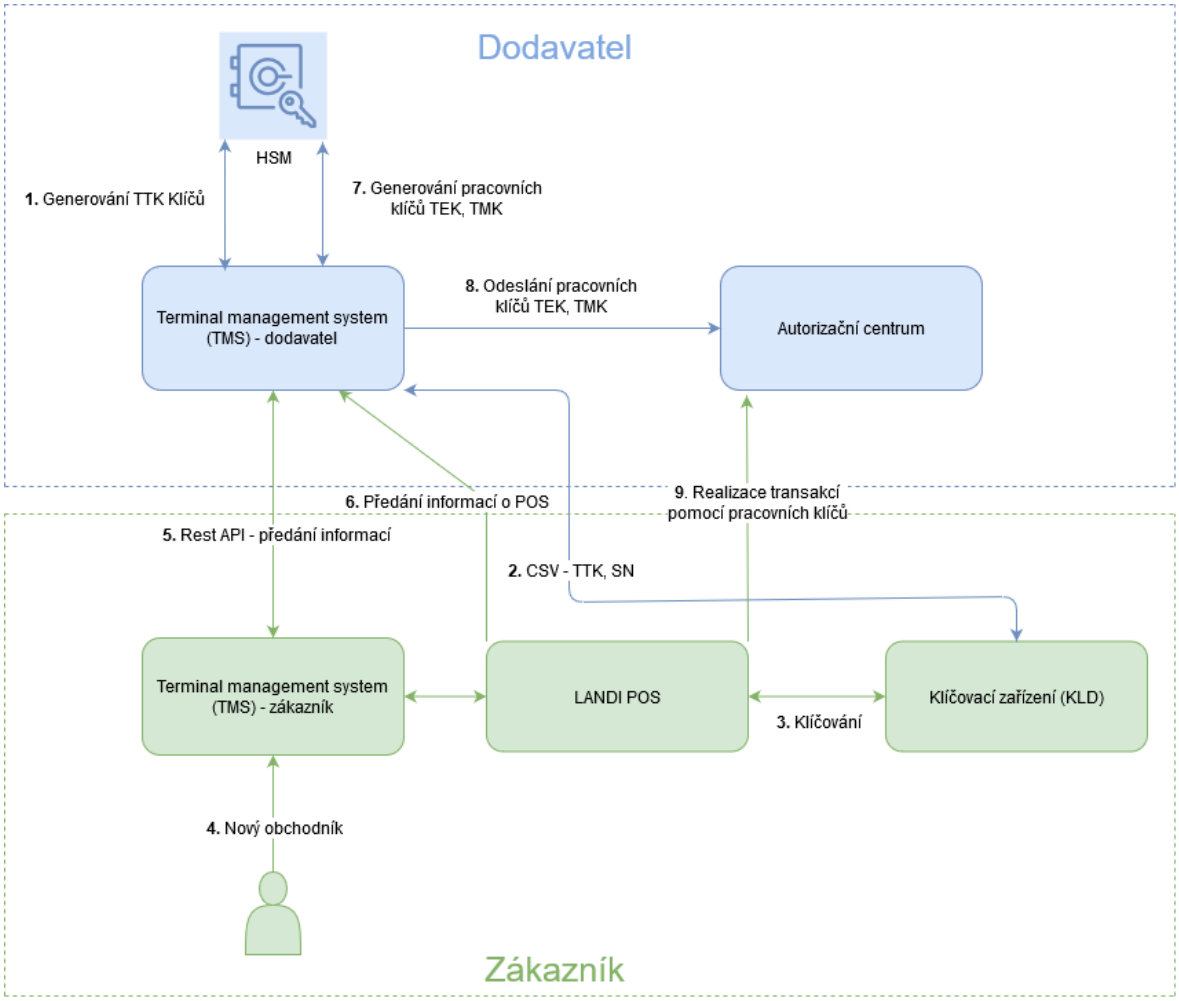
Společnost Landi Commercial Equipment Co., Ltd., dále jen Landi využívá pro klíčování terminálů zařízení KLD, do kterého jsou u zákazníka vloženy pomocí importního souboru TTK klíče, které jsou generované v HSM u dodavatele platebních terminálů. Samotný přenos TTK klíčů od dodavatele k zákazníkovi probíhá v zašifrované formě, pomocí transportního klíče, který je uložený v HSM u dodavatele a následně je vložen do klíčovacího zařízení KLD u zákazníka.

Soubor, který se importuje do klíčovacího zařízení je ve formátu .CSV a obsahuje vždy sériové číslo terminálu a volný TTK klíč. Jednotlivé TTK klíče jsou v importním souboru šifrované transportním klíčem, i z toho důvodu manipulace s klíči nepředstavuje bezpečnostní riziko, takže import souboru do klíčovacího zařízení nemusí probíhat v zabezpečené místnosti. Transportní klíč, který je poskytnutý dodavatelem se zavádí vždy jen jednou do klíčovacího zařízení a celý proces se musí provádět v zabezpečené místnosti u dodavatele.

Samotné klíčování probíhá propojením klíčovacího zařízení KLD s platebním terminálem, pomocí USB kabelu. Pro úspěšné naklíčování POS musí mít klíčovací zařízení zavedeny klíče, s příslušným sériovým číslem terminálu.

Následně dojde k odeslání spárovaných TTK klíčů a sériových čísel terminálů zpět od zákazníka k dodavateli terminálů. Zároveň dochází k založení daného terminálu v TMS u dodavatele terminálu. Při prvním spojení POS a TMS dodavatele dojde k ověření existence TTK klíče pro dané sériové číslo v databázi. Pokud dojde k úspěšnému ověření, přiřadí se dané TTK ke specifickému terminálu. V dalším kroku se propojí přímo POS platební terminál s TMS dodavatele a zašle mu o sobě základní informace, jako jsou sériové číslo a TTK klíč. V rámci TMS dodavatele se vygenerují pracovní klíče, které se odešlou do

autorizačního centra. Tyto klíče jsou nezbytné pro úspěšnou autorizaci plateb. TEK a TMK klíče jsou šifrované pomocí network klíče. Samotný přenos těchto klíčů z databáze do terminálu probíhá v šifrované podobě pomocí TTK klíče. Struktura klíčování je znázorněná v high-level diagramu na Obrázku 12. [24]



Obrázek 12: High-level schéma klíčování společnosti Landi [24]

PRAKTICKÁ ČÁST

6 PŘEDSTAVENÍ SPOLEČNOSTI

Vybraná společnost (dále jen „společnost“) byla založena v roce 1996 s cílem rozvoje a bezpečného provozu čipových karet v bankovním sektoru. Společnost je rozdělena na několik divizí, které mezi sebou úzce spolupracují. Aktuálně je zaměstnáno ve firmě přes 200 zaměstnanců.

6.1 Základní údaje

Od roku 1996, kdy byla společnost založená, se její portfolio rozrostlo. Hned dva roky po založení začala společnost navrhovat koncepci akceptace privátních ale i platebních karet na jednom terminálu.

Na přelomu tisíciletí společnost vybudovala centrální transakční systém, pro jednu z největších českých bank a jako jedni z prvních využili Linux, jako základ řešení v Enterprise prostředí. O několik let později vstoupila společnost do státního sektoru, kdy začala aplikovat digitální identitu do oblasti eGovernmentu.

V Roce 2016 firma spouští, jako druhá v Evropě platbu bankovní kartou ve veřejné dopravě. Následně se koncept platby rozšířil i mimo Evropu, například do Afriky a následně i do Jižní Ameriky.

Momentálně se společnost neustále rozrůstá a stále drží krok s nemodernějšími technologiemi současnosti. [24]

6.2 Divize společnosti

Společnost se dělí na několik divizí, jejichž specializace je rozmanitá.

SmartCards

Následující divize vyvíjí applety pro čipové karty a také aplikace pro vysoce bezpečná identifikační, autentizační a platební řešení. Pro zaručení bezpečnosti se využívá sdílených tajemství, symetrické i asymetrické kryptografie pro systémovou autentizaci nebo například PIN a biometrické aplikace pro vícefaktorovou autentizaci držitele karty. Nezbytnou součástí je také ochrana kryptografických klíčů s čipovou technologií. [24]

Secure Mobile ID

Další odvětví se zabývá vývojem mobilních a webových aplikací, se specializací na platební bankovní sektor. I proto je nutností využívání nejnovějších bezpečnostních technologií, jako například RASP nebo OTP – token v mobilním zařízení (iOS a Android). [24]

EMV Payments

Tato divize se specializuje na realizování výkonných autorizačních a akceptačních platebních systémů. V rámci divize probíhá integrování široké škály POS terminálů, od předních společností, jako jsou Verifone, Ingenico, Pax nebo Terminal Technologies. Z důvodu zpracování vysokého objemu transakcí veškeré zpracování probíhá s využitím HSM a zároveň je dodržená PCI certifikace. [24]

Federated Identity

Další část společnosti se zabývá robustním zabezpečením identity v jednom systému pro více aplikací najednou. [24]

Perso Lab

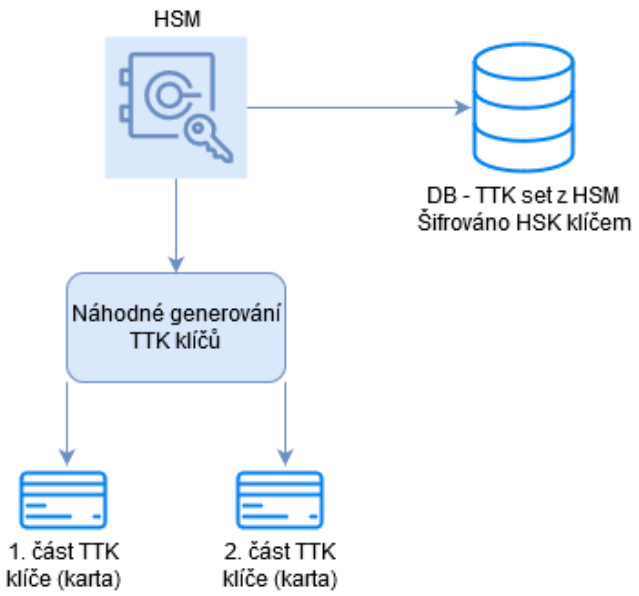
Poslední odvětví společnosti se zabývá vývojem systémů pro personalizaci čipových karet. [24]

7 NÁVRH KLÍČOVÁNÍ PRO VYBRANOU SPOLEČNOST

Cílem diplomové práce je navrhnutí nového systému klíčování EMV platebních terminálů podle PCI DSS normy, včetně klíčovací aplikace a dokumentace. Nový systém klíčování nahradí původní, který je ve společnosti zavedený, ale současně už pomocí původního řešení není možné klíčovat nové druhy terminálů.

7.1 Současné řešení

V rámci současného řešení je klíčování rozděleno na dvě hlavní části. V té první, která je uvedena na Obrázku 13, je znázorněno náhodné vygenerování TTK klíčů v rámci HSM. První a druhá část TTK klíče, respektive jejich komponenty jsou uloženy postupně na klíčovací karty. Každá karta obsahuje několik set komponent a zároveň každou komponentu lze použít pouze jednou. Po vyčerpání jednotlivých komponent, které jsou na kartě umístěné, je nutné použít ke klíčování kartu jinou. Karty jsou později přiděleny technikům, kteří mají na starosti klíčování. Z HSM se komponenty TTK klíčů uloží do databáze. Jednotlivé komponenty TTK klíčů jsou šifrované pomocí HSK klíče, který je sdílený mezi HSM a databází. Komponenty jsou později využity při klíčování platebních terminálů.



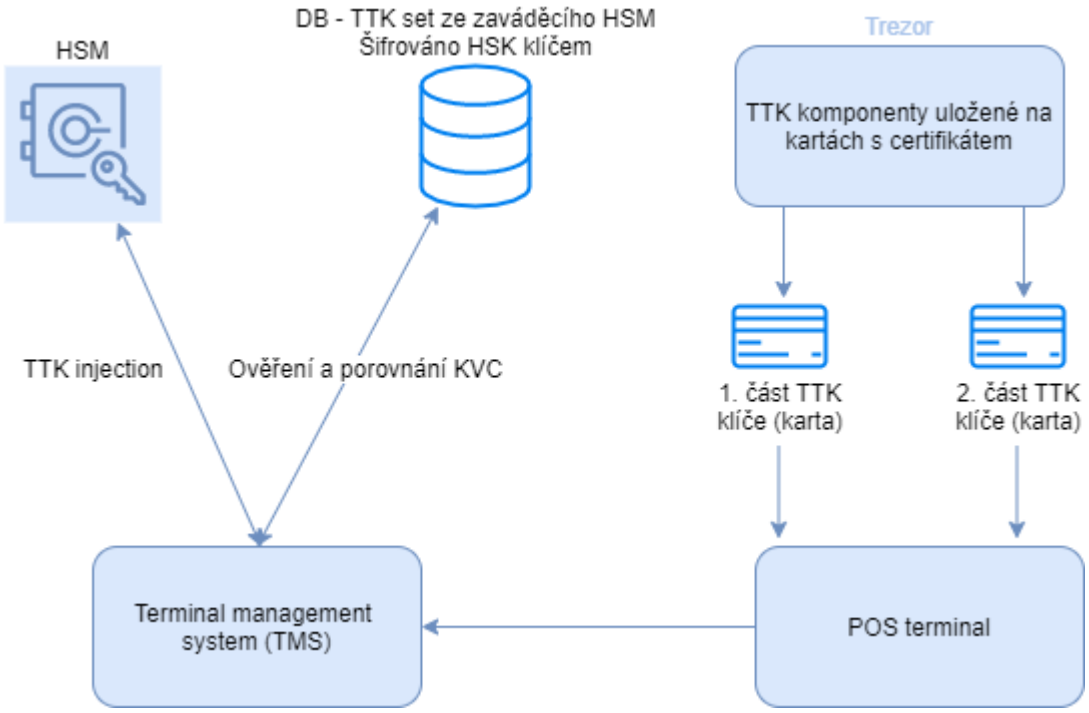
Obrázek 13: Zavedení TTK klíčů [29]

V další fázi dochází přímo ke klíčování EMV platebního terminálu. K procesu klíčování jsou vždy nutní minimálně dva technici, kteří si své karty, které jsou uložené v zabezpečené místnosti v trezoru, vyzvednou a postupně zahájí proces klíčování. Vložením první TTK karty

do terminálu dojde pomocí klíčovací aplikace k ověření platnosti certifikátů na kartě a následně dojde k zadání PIN kódu, který je každému technikovi přidělen přímo ke kartě. Pokud je zadán správný PIN, stejný postup opakuje druhý, respektive třetí technik.

V dalším kroku dojde k vygenerování TTK klíče, který je poskládán z komponent jednotlivých klíčovacích karet vzájemnou operací XOR mezi jednotlivými komponentami. Komponenty jsou uloženy na kartách v čistém tvaru, proto jsou chráněny PIN kódem. Výsledný TTK klíč je vytvořený ze dvou komponent, z důvodu použití 2DES klíče. Následně je TTK klíč uložen do zabezpečené části hardwaru terminálu a zároveň se k němu vytvoří kontrolní součet (KVC).

Potřebné hodnoty, jako jsou kontrolní součet TTK klíče, ID terminálu, čísla klíčovacích karet a jejich komponent jsou odeslány do TMS. V rámci TMS dojde k dohledání komponent klíčovacích karet v databázi TMS a ke složení TTK klíče, včetně výpočtu kontrolního součtu v HSM. Pokud je kontrolní součet u terminálu a TMS totožný, dojde k úspěšnému naklíčování terminálu. Druhý krok klíčování lze vidět na Obrázku 14. První i druhá fáze se provádí v zabezpečené místnosti pod kamerovým dohledem a veškerá manipulace s klíčovacími kartami se důkladně zaznamenává.



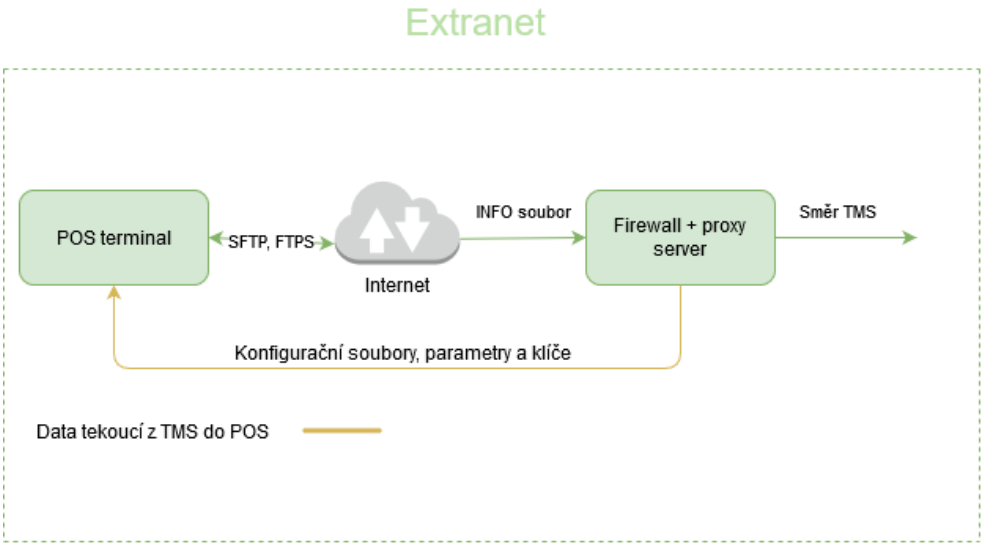
Obrázek 14: Klíčování ve vybrané společnosti – současný stav [29]

7.2 Návrh nového řešení

Hlavní důvodem navrhnutí nového systému klíčování EMV platebních terminálů bylo zjednodušení celého procesu a možnost klíčovat nové druhy terminálů, které by pomocí původního řešení nebylo možné naklíčovat. Zároveň je nutné přejít na bezpečnější formu klíčování, tedy navrhnutí šifrování s využitím 3DES algoritmu s 3DES klíčem. V původním řešení vybrané společnosti je využita 3DES šifra s 2DES klíčem. Pro splnění jedné z podmínek PCI DSS normy probíhá celý proces klíčování v zabezpečené místnosti pod dohledem kamer. Dále jsou veškeré kryptografické operace realizovány pomocí HSM, kdy nedochází k přenosu klíčů nebo dat v otevřené podobě. Samotné nahrání klíčů do terminálů je navrhnuto tak, aby bylo realizováno ve vnitřní síti vybrané společnosti, jak lze vidět na obrázku 16 (Topologie sítě).

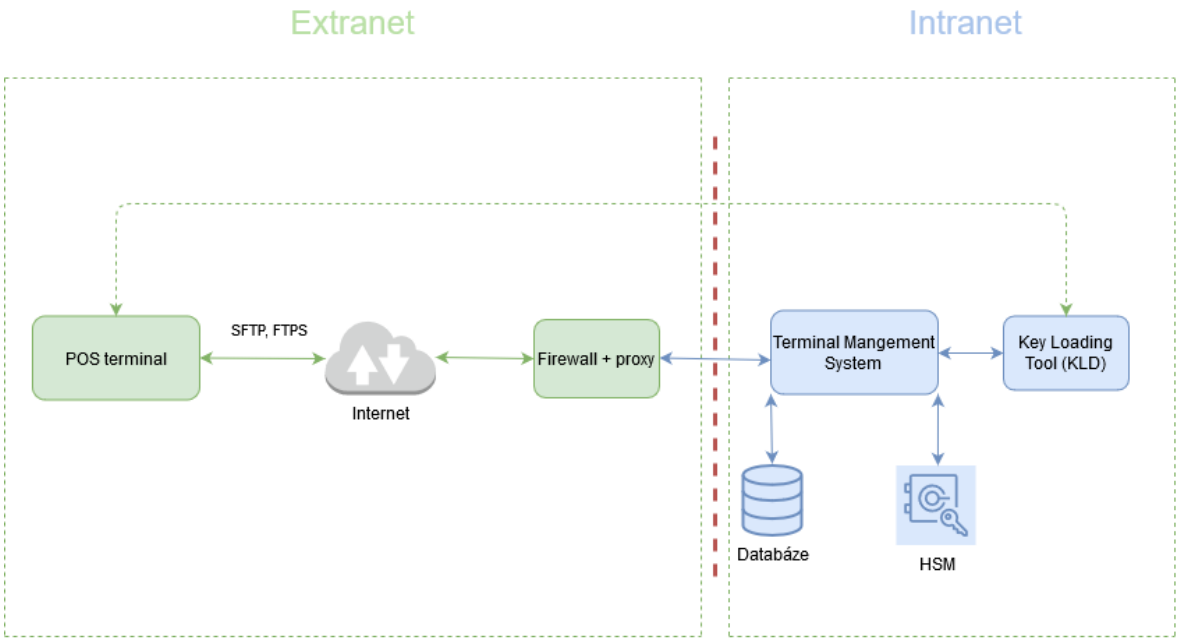
7.2.1 Návrh topologie sítě a komunikace

POS terminály komunikují s terminálovým systémem, který je umístěn ve vnitřní síti společnosti. Komunikace probíhá skrze firewall a proxy server, pomocí komunikačních protokolů SFTP (FTP přes SSH) a FTPS (FTP přes SSL). Aby mohly terminály komunikovat s TMS, je nutné, přihlášení pomocí platného jména a hlesla. Po úspěšném přihlášení dojde k nahrání specifického souboru z terminálu do TMS. Tento soubor obsahuje souhrnné informace o hardwaru a softwaru terminálu. V dalším kroku dojde ke stažení konfiguračních souborů a klíčů z TMS do terminálu. Nakonec dojde k ukončení a odpojení terminálu od TMS. Celá komunikace je znázorněna na Obrázku 15, včetně jednotlivých komponent.



Obrázek 15: Komunikace terminálu se systémem pro jeho správu [29]

Klíčování platebních terminálů opět probíhá ve vnitřní síti vybrané společnosti, která se nachází za komponentami firewall a proxy serverem, jak lze vidět na Obrázku 16. Dále je ve vnitřní síti umístěno HSM a databáze terminálového systému, zařízení pro klíčování a samotný POS terminál, který se klíčuje. Jednotlivé objekty a jejich komunikace v rámci intranetu jsou popsány v dalších kapitolách.



Obrázek 16: Topologie sítě [29]

7.2.2 Návrh komponent využívaných pro klíčování

Následující podkapitola se zaměřuje na popis jednotlivých komponent, které byly vybrány pro klíčování EMV platebních terminálů ve vybrané společnosti.

Firewall a autentizační Proxy server

Tyto části systému jsou určeny k oddělení od veřejného internetu a zpracování příchozích požadavků. Autentizační proxy je aplikační server, který je veřejně dostupný z internetu a mohou k němu veřejně přistupovat zařízení. Počítá se u něj s provozováním v režimu 24/7. Proxy server je schopný obsloužit minimálně desítky paralelních připojení najednou.

Z pohledu komunikujících zařízení funguje aplikační server, jako server komunikace nad protokolem SFTP/FTPS.

Hardware Security Module – HSM

Pro účel uložení hlavního master klíče a dalších šifrovacích klíčů bylo zvoleno HSM od společnosti Gemalto Safenet, které vyniká vysokou bezpečností a vysokým výkonem. V rámci

HSM je naimportovaný tzv. Master KEK Key, který je totožný, jako v klíčovacím zařízení. Master KEK Key bude umístěn servisním technikům na dvou nebo třech komponentách, kteří pomocí nich zavedou Master KEK Key podle standardu PCI DSS do HSM.

Key Loading Device (KLD)

Klíčovací zařízení slouží k bezpečnému zavedení TTK klíče do platebního terminálu. TTK klíč je zároveň první klíč, který slouží k zavedení ostatních klíčů do terminálu. Klíčovacích zařízení existuje více druhů, proto bylo nutné vybrat ten nejvhodnější.

Často využívanými KLD zařízeními jsou ta, u kterých se na začátku u zákazníka importují TTK klíče. Import nejčastěji probíhá pomocí .CSV souboru, ve kterém jsou uvedená sériová čísla platebních terminálů a volné TTK klíče. Následně dochází k propojení platebního terminálů s klíčovacím zařízením a k samotnému přenosu klíčů.

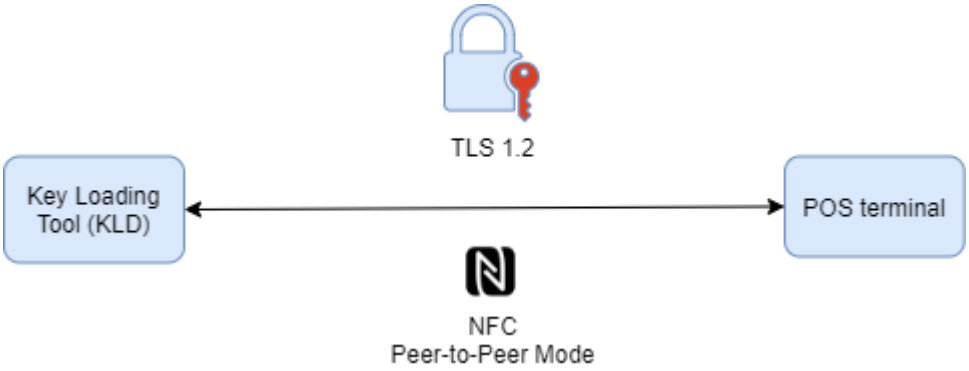
Dalším typem klíčovacích zařízení jsou ta, u kterých se nevkládají předgenerované TTK klíče, ale pouze derivační klíč (Master Key), pomocí kterého se s využitím známého algoritmu generují TTK klíče přímo uvnitř klíčovacího zařízení. Totožný derivační klíč musí být zavedený i ve vybrané společnosti, v rámci které bude probíhat klíčování platebních terminálů. Klíčovací zařízení následně pomocí sériového čísla klíčovaného terminálu a náhodně vygenerované hodnoty vyderivuje TTK klíč – více informací k problematice derivačního algoritmu je obsaženo v kapitole 7.2.5. Tento druh klíčovacího zařízení byl zvolen k návrhu klíčování ve vybrané společnosti, hlavně z důvodu absence nutnosti předgenerování TTK klíčů a práce s .CSV souborem, což usnadňuje celý proces klíčování a dále umožňuje zavedení více Master klíčů. To slouží k tomu, že z jednoho klíčovacího zařízení lze klíčovat terminály více zákazníků a platforem.

POS Terminál

Součástí terminálu, který bude klíčován je klíčovací aplikace KLA (Key Loading Application), která zajistí komunikaci mezi klíčovacím zařízením a samotným terminálem. Aplikace se do terminálu nainstaluje před klíčováním, pomocí instalační aplikace dodávané výrobcem. Nezbytnou funkcí klíčovací aplikace v terminálu je ověření klíčů a dalších součástí, které se z klíčovacího zařízení přenáší do terminálu. Citlivá data, jako je například výsledný klíč, jsou uložena v bezpečném hardwaru terminálu.

7.2.3 Propojení Key Loading Device s POS terminálem

Součástí návrhu klíčování bylo také vybrání nejvhodnější metody propojení POS terminálu s klíčovacím zařízením. Jednou z možností bylo propojení obou zařízení pomocí USB, to ale z důvodu nutnosti vždy propojovat obě zařízení, pomocí kabeláže nebylo z časových a praktických důvodů příliš vhodné. Jelikož POS terminál i klíčovací zařízení podporují technologii NFC, bylo zvoleno právě toto řešení. V rámci NFC byl vybrán Peer-to-Peer mód, který mezi oběma zařízeními vytvoří obousměrnou komunikaci, a tak každé z nich působí jako vysílač i jako přijímač. Zároveň je celá komunikace mezi objekty chráněna kryptografickým protokolem TLS 1.2 (Transport Layer Security), který zabraňuje narušení komunikace a její odposlouchávání. Dále také umožňuje autentizaci mezi zařízeními. Schéma propojení je uvedeno níže na Obrázku 17.



Obrázek 17: Komunikace KLD a POS terminál [29]

7.2.4 Bezpečnostní pravidla a jednotlivé role

V rámci manipulace s klíčovacím zařízením bylo třeba definovat jednotlivá bezpečnostní pravidla a role. Tímto lze například zabránit odmazání klíčů neoprávněnou osobou. Klíčovací zařízení dokáže číst čipové karty, které jsou osobám, které manipulují s klíčovacím zařízením přiděleny. Pomocí těchto karet se při přihlášení rozpozná role daného uživatele a tím se přidělí patřičná oprávnění. Při práci s KLD je nastaven bezpečnostní timeout 15 minut v případě nečinnosti a zároveň je z bezpečnostních důvodů zakázáno pořizování snímků obrazovky. Veškeré aktivity, které jsou realizované v rámci klíčování, se ukládají do auditního logu. Pokud nabyde logovací soubor se záznamy maximální velikosti, nelze naklíčovat další terminál. Soubor se dá buď přímo odmazat ze zařízení, nebo stáhnout na paměťové zařízení. K přihlášení do klíčovacího zařízení, tedy i ke klíčování POS terminálů je vždy třeba minimálně dvou přihlašovacích karet, tedy dvou techniků.

Uživatelské role

Manažer: tato uživatelská skupina definuje jednotlivé uživatele a nastavuje jim výchozí hesla. Dále může spravovat jednotlivé klíče, včetně jejich přidávání a mazání, zároveň vytváří a edituje jednotlivé skupiny klíčů. Lidé v této skupině převážně slouží jako podpora pro operátory. Manažer je schopen měnit hesla jednotlivým operátorům, pomocí kterých se ke klíčovacímu zařízení přihlašují.

Operátor: zde spadají servisní technici, kteří klíčují pomocí klíčovacího zařízení POS terminály. Tato role má pouze oprávnění na vložení klíče do cílového terminálu a zobrazení klíčů v klíčovacím zařízení.

Politika hesel

- Manažer přidělí jednotlivá hesla. Po prvním přihlášení jsou uživatelé vyzváni ke změně výchozího hesla.
- Minimální podmínky pro validní heslo v rámci všech uživatelských skupin je minimální délka aspoň 8 znaků, kdy součástí musí být aspoň jedna číslice a speciální znak.
- Kontroluje se unikátnost hesla v rámci všech uživatelů.
- V případě tří nevalidních pokusů o zadání hesla dojde k zablokování daného uživatele na 30 minut.
- V případě zapomenutého hesla je třeba kontaktovat uživatele s rolí manažer. Pouze ti mají možnost heslo změnit.

7.2.5 Kryptografické operace s klíči a citlivá data

V rámci návrhu je potřeba vygenerovat z hlavního Master klíče, TTK klíč, pomocí kterého jsou následně do terminálu nahrány pracovní klíče. Daný TTK klíč se vytvoří pomocí derivace Master klíče. V rámci terminálů, pro které je celý návrh klíčování realizován, je paměť pro citlivá data, jako jsou klíče o velikosti 1000 B.

Samotný derivační algoritmus se odehrává v rámci klíčovacího zařízení a jeho hlavní funkcí je vygenerování a následné vložení unikátního klíče do POS platebního terminálu. TTK klíče se derivují z Master Klíče. Pro generování TTK klíče pomocí derivačního algoritmu bude využito 3DES blokové šifry s 3DES klíčem, která má v rámci PCI DSS normy podporu do roku 2023. V rámci 3DES šifrování bude využito CBC algoritmu, který je podporovaný

v rámci HSM. Ze vstupních dat je náhodně složený inicializační vektor, který slouží, jako součást pro první blok derivačních dat v rámci operace XOR. Každý blok derivačních dat je šifrovaný pomocí DES algoritmu, kdy celkově jsou použity 3 bloky, to dohromady dává využití 3DES klíče. Kromě prvního bloku jsou pro operaci XOR využity šifrovaná data z předešlého derivačního bloku. Derivační proces je zobrazen na Obrázku 18.

Derivační algoritmus

Samotný algoritmus se skládá z několika komponent:

PID (Product Identificator) – identifikační číslo terminálu 4 B

SN (Serial Number) – seriálové číslo terminálu 4 B

IV (Initialization Vector) – náhodně vygenerovaný vektor 8 B

RND1 – náhodně vygenerovaná data 8 B

RND2 – náhodně vygenerovaná data 8 B

MK (Master Key) – hlavní klíč

DK (Derivation Key) – derivační klíč

Derivační data (DD) jsou složená z jednotlivých prvků:

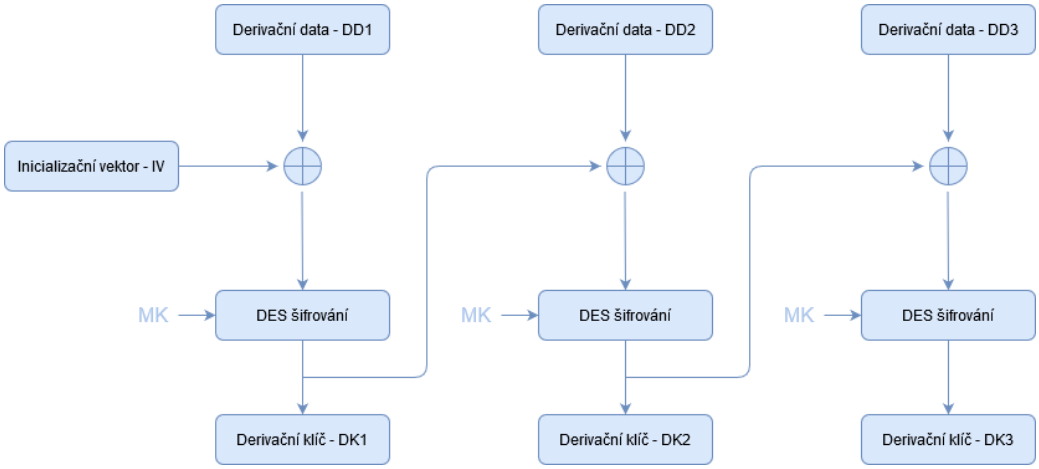
DD = DD1 | DD2 | DD3 (24 B)

DD1 = PID | SN (8B)

DD2 = RND1 (8B)

DD3 = RND2 (8B)

Schéma derivačního algoritmu je následující:



Obrázek 18: Derivační algoritmus [29]

Výsledný TTK klíč se skládá ze tří vyderivovaných klíčů, které prošly třikrát operací XOR a následnou DES šifrou:

Výsledný TTK klíč DK = DK1 | DK2 | DK3, kdy jednotlivé složky jsou následující:

DK1 = DES (MK, IV ⊕ DD1)

DK2 = DES (MK, DK1 ⊕ DD2)

DK3 = DES (MK, DK2 ⊕ DD2)

Uložení výsledného klíče do cílového terminálu

Do cílového POS terminálu se ukládá výsledek derivace, tedy výsledný TTK klíč, který je uložen do zabezpečené části terminálu. Zároveň s ním se z klíčovacího zařízení do terminálu posílají další data, jako je inicializační vektor, náhodná hodnota RND1 a náhodná hodnota RND2, které byly využity v procesu derivace a KVC TTK klíče. Tyto hodnoty již nejsou uložené v zabezpečené vrstvě.

7.2.6 Souhrn principu klíčování

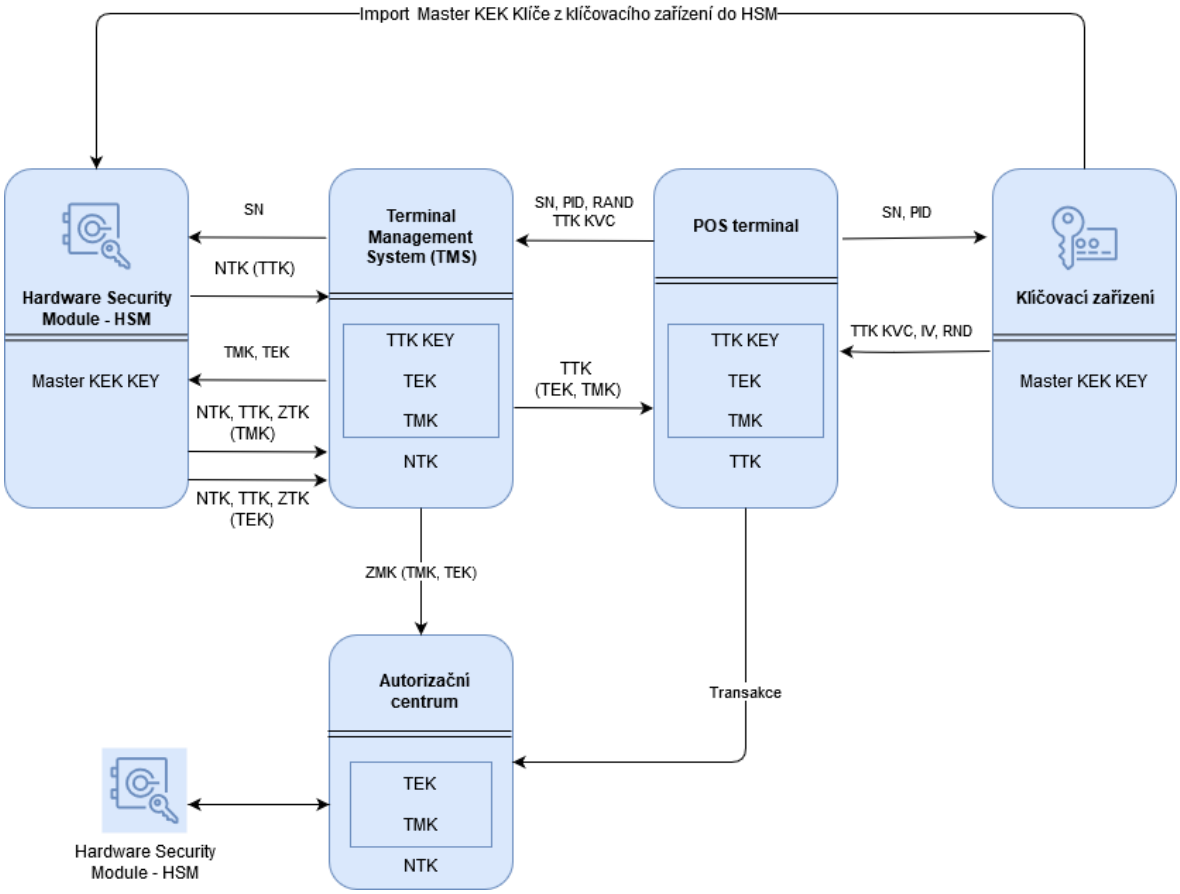
Tato podkapitola shrnuje výše popsané kapitoly do jedné komplexní části. Bude zde popsán princip klíčování a komunikace, včetně přenášení klíčů mezi jednotlivými částmi systému.

Terminál se při klíčování spojí s klíčovacím zařízením, ve kterém je již zavedený Master klíč. Spojení obou zařízení probíhá pomocí NFC bezdrátové technologie, jako je popsáno v kapitole 7.2.3. Stejný Master klíč je zavedený v HSM terminálového systému (TMS) vybrané společnosti. Klíčovacímu zařízení se z terminálu zašle seriálové číslo a identifikační číslo terminálu. Klíčovací zařízení ze sériového čísla, identifikačního čísla, náhodně vygenerovaných hodnot a inicializačního vektoru, pomocí algoritmu vyderivuje z Master klíče, TTK klíč, který je vždy unikátní pro klíčovaný terminál. Vygenerovaný TTK klíč je následně odeslán, včetně jeho KVC, inicializačního vektoru, náhodně vygenerovaných dat (RND1, RND2) do terminálu. Postup derivace a odeslání klíče do terminálu je popsán v kapitole 7.2.5.

V rámci terminálu slouží TTK klíč pro zavedení pracovních TMK a TEK klíčů z TMS. Aby bylo zavedení klíčů možné, je třeba, aby terminál zaslal na TMS následující údaje: sériové číslo, identifikační číslo terminálu, náhodně vygenerovaná data (RND1, RND2), inicializační vektor a KVC TTK klíče. TMS pomocí stejného algoritmu, jako klíčovací zařízení

spočítá TTK klíč a ověří jeho kontrolní součet proti terminálu. Pokud jsou kontrolní součty totožné, odešlou se pracovní klíče TEK a TMK do terminálu. Dále se pracovní klíče pomocí Zone Master Key (ZMK) zavedou z TMS do autorizačního centra, ve kterém probíhá zpracování a ověření plateb.

V každém kroku klíčování se veškeré klíče a data posílají v šifrované formě. V rámci TMS se pracuje s Network Key (NTK), platební terminál šifruje klíče s Terminal Transport Key (TTK) a přímo do autorizačního centra jsou klíče odeslané v zašifrované formě pomocí ZMK. Na Obrázku 19 je znázorněn celý proces.



Obrázek 19: Schéma procesu klíčování terminálu [29]

8 TVORBA DOKUMENTACE A NÁVRH APLIKACE KE KLÍČOVÁNÍ A SPRÁVĚ ROLÍ

Součástí diplomové práce je vytvoření dokumentace ke správě uživatelských rolí v rámci klíčovacího zařízení a k samotnému klíčování EMV platebních terminálů ve vybrané společnosti. Zároveň bylo ale potřeba navrhnout jednotlivé sekce aplikace tak, aby bylo ovládání intuitivní a jednoduché. Samotná dokumentace popisuje obsluhování klíčovacího zařízení, které spravuje jednotlivé uživatele, jejich role a samotné klíčování. Návrh prostředí aplikace a dokumentace probíhal pomocí služby MockFlow, která umožňuje bezplatně vytvářet vizualizace obrazovek.

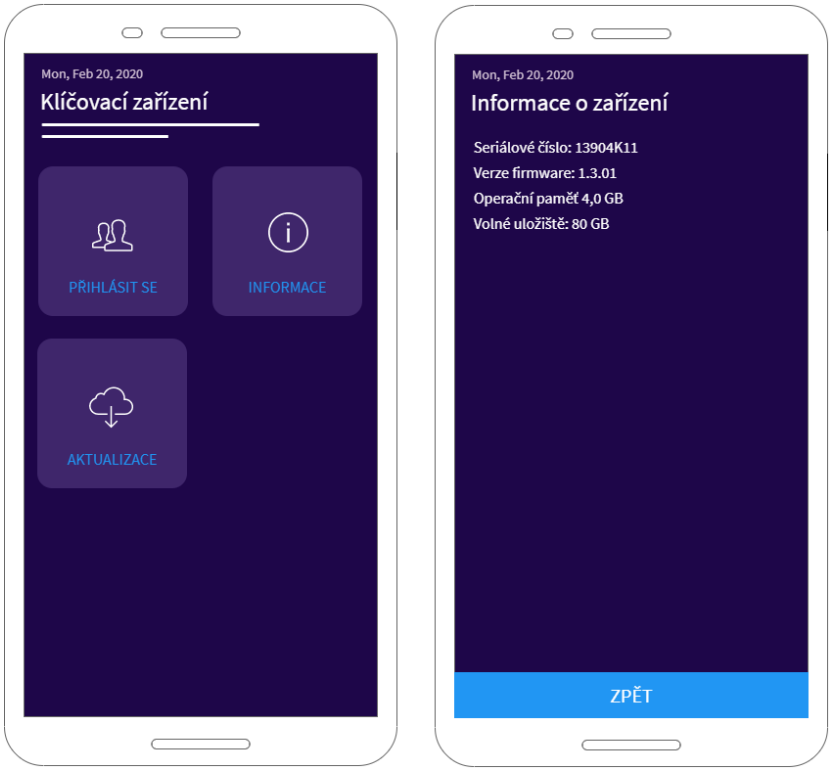
8.1 Přihlášení do klíčovacího zařízení a obsluha aplikace

První spuštění klíčovacího zařízení vždy musí provádět uživatelé s rolí manažer. Pro každou operaci v rámci klíčovacího zařízení jsou nutné minimálně dvě osoby. Součástí klíčovacího zařízení jsou už z výroby zavedené minimálně dvě přihlašovací karty s rolí manažer, aby bylo možné provést prvotní nastavení. Jejich hlavním úkolem je vytvořit další uživatele, včetně přidělení přihlašovacích karet osobám, které budou mít na starosti správu zařízení a klíčování platebních terminálů. Dále se při prvotním nastavení zvolí počet komponent, tedy počet karet, které budou nutné k přihlášení. Vždy to budou dvě nebo tři karty, respektive tři nebo čtyři, vždy je jedna karta vyrobena navíc, aby sloužila jako rezervní, například v případě ztráty.

Úvodní obrazovka, kterou lze vidět na Obrázku 20 vybízí uživatele k několika možnostem. Klíčovací zařízení podporuje WiFi standard, takže má možnost připojení k síti. Volba aktualizace připojí klíčovací zařízení ke vzdálenému serveru, kde porovná aktuálně nahranou verzi klíčovací aplikace, s verzí umístěnou na serveru. Pokud existuje verze novější, dojde k jejímu stažení a instalaci na pozadí. Po úspěšné instalaci je uživatel vyzvaný k restartu aplikace.

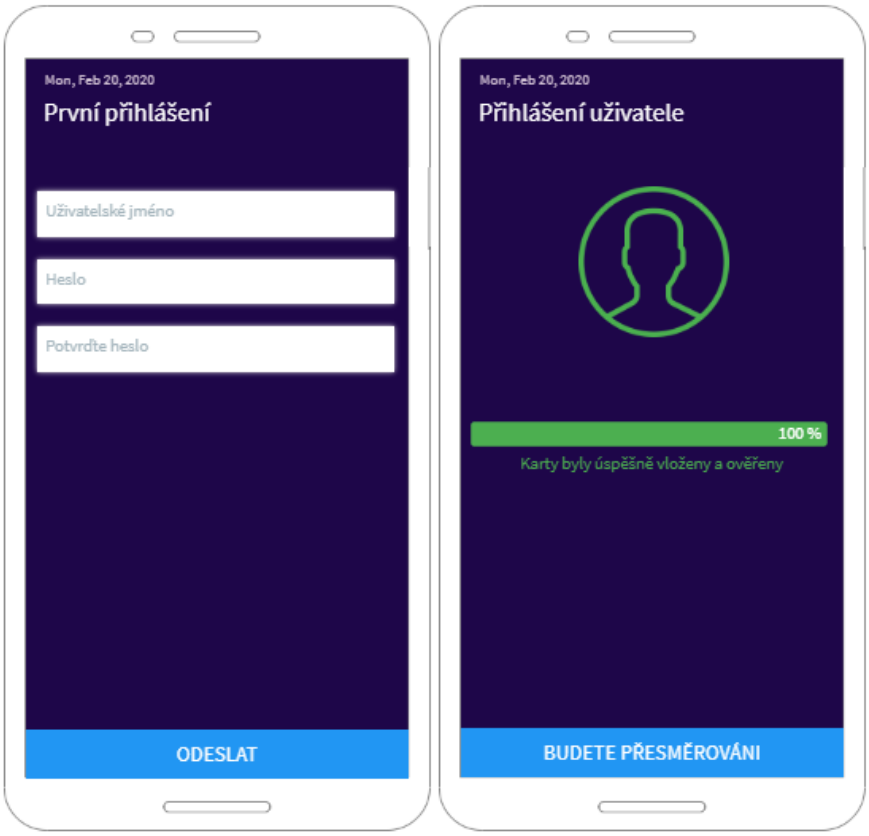
Položka informace zobrazí uživateli základní informace o klíčovacím zařízení, jako jsou seriálové číslo, verze firmware, operační paměť nebo kapacitu volného úložiště. Aby mohl uživatel klíčovací zařízení ovládat, musí ověřit svou totožnost. Každý uživatel, který obsluhuje klíčovací zařízení, má přidělenou kartu, pomocí které se přihlásí. Pro úspěšné přihlášení jsou potřeba vždy minimálně dvě karty, tedy dvě osoby, kterým byly karty přiděleny.

Přihlašovací karty se vkládají do klíčovacího zařízení, které má integrovanou čtečku čipových karet. Vždy po vložení karty je daný uživatel vyzván k zadání hesla.



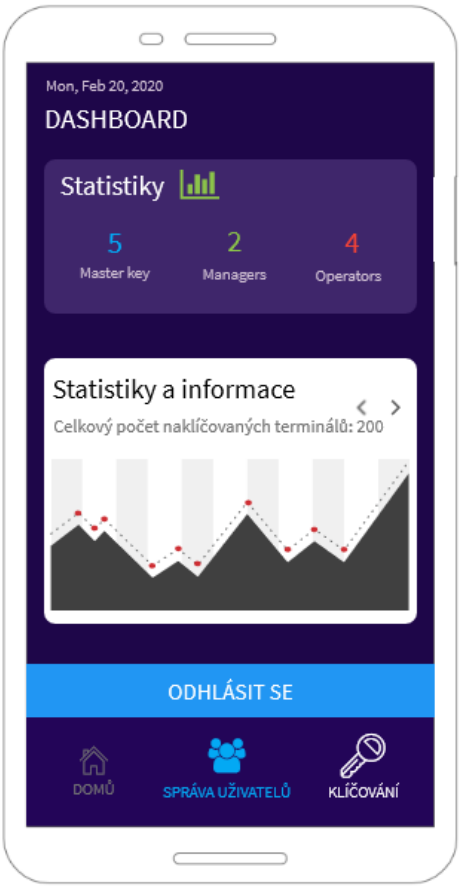
Obrázek 20: Úvodní obrazovka klíčovacího zařízení [29]

Po prvním přihlášení jsou všichni uživatelé vyzváni ke změně hesla a nastavení uživatelského jména. Pokud proběhne úspěšné přihlášení, aplikace o tom uživatele informuje a přesměruje ho na výchozí obrazovku aplikace, jak je uvedeno na Obrázku 21 níže. V případě neúspěšného přihlášení se celý proces opakuje.



Obrázek 21: Úspěšné přihlášení uživatele [29]

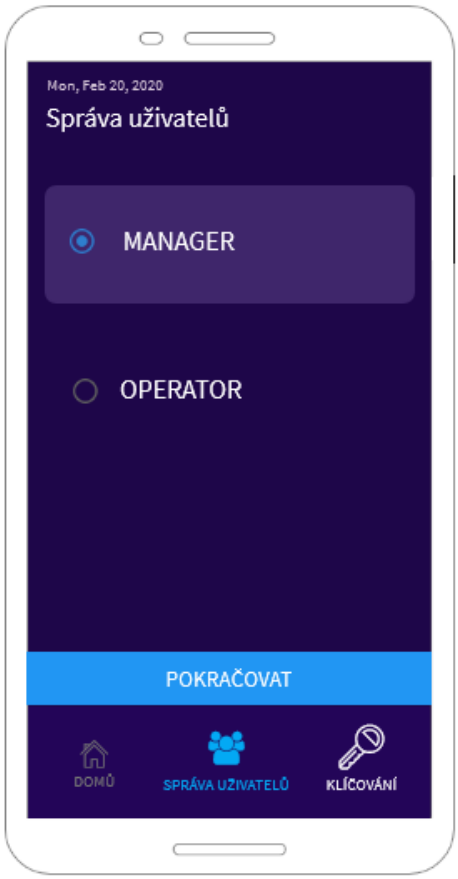
Výchozí obrazovka aplikace obsahuje jednoduchý přehled uživatelů a statistiku klíčování. Dále je na Obrázku 22, v rámci výchozí obrazovky umístěno tlačítko s možností odhlášení z klíčovacího zařízení a navigační menu se třemi položkami: domů, správa uživatelů a klíčování. Položka domů vrátí uživatele na výchozí obrazovku se statistikami.



Obrázek 22: Výchozí obrazovka aplikace [29]

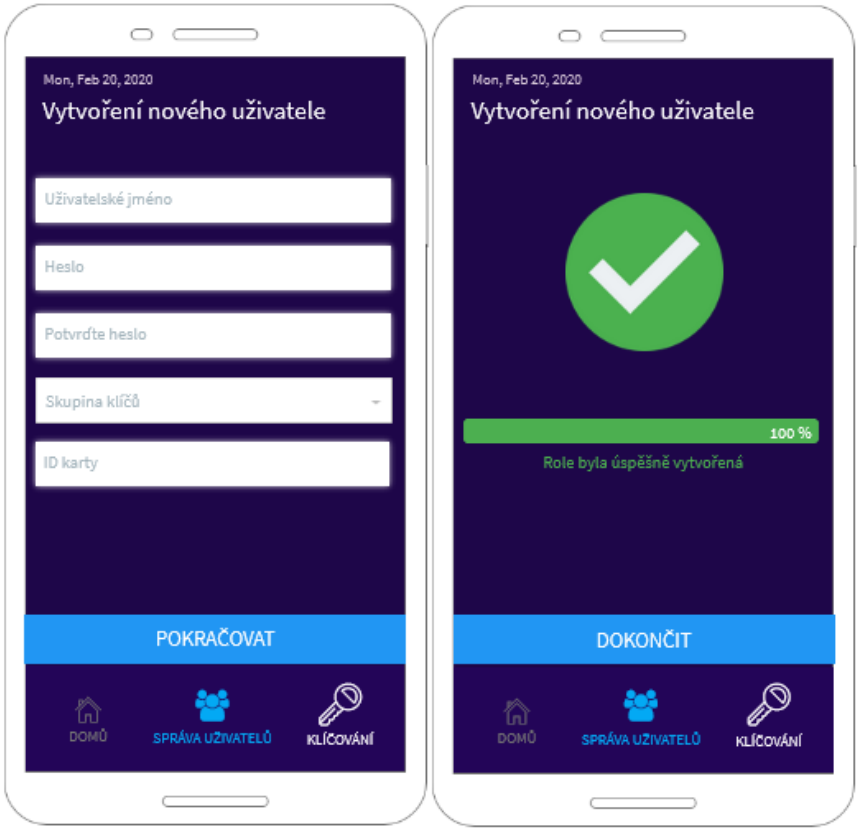
8.2 Správa uživatelů klíčovací aplikace

Položka správa uživatelů umožňuje osobám s rolí manažer vytvářet nové uživatele s rolí manažer a operátor, jak lze vidět na Obrázku 23. Nejdříve uživatel s rolí manažer zvolí, o jakou roli se jedná.



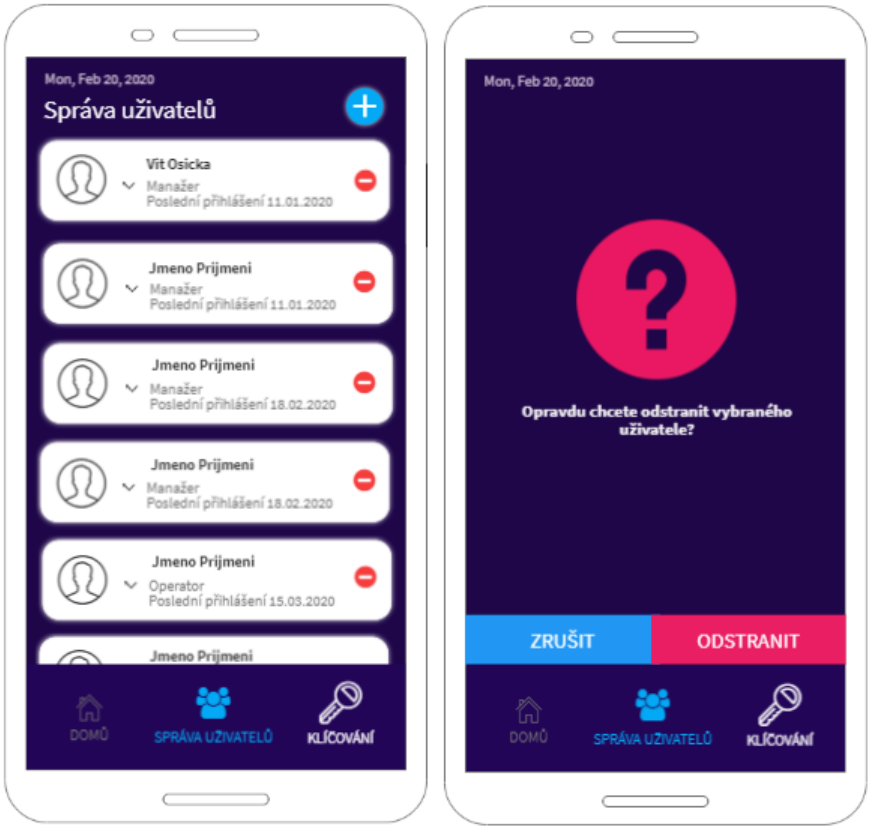
Obrázek 23: Vytvoření nového uživatele [29]

V dalším kroku manažer vyplní uživatelské jméno a heslo, které musí splňovat bezpečnostní politiku dané společnosti, jak je uvedeno v kapitole 7.2.4. Dále je třeba zvolit skupinu klíčů, do které bude uživatel zařazený, tím se mu určí, jaké specifické zákazníky nebo platformy bude klíčovat. Uživatel bude moct spadat do více skupin klíčů. Nakonec je třeba vyplnit ID přihlašovací karty, která bude uživateli přiřazená a pomocí které se bude přihlašovat do klíčovacího zařízení. Dané ID je uvedeno přímo na kartě a je v rámci vybrané společnosti unikátní. Pokud vyplní tato povinná pole a splní validační požadavky, dojde k úspěšnému vytvoření nového uživatele, jak je znázorněno na Obrázku 24.



Obrázek 24: Úspěšné vytvoření nového uživatele [29]

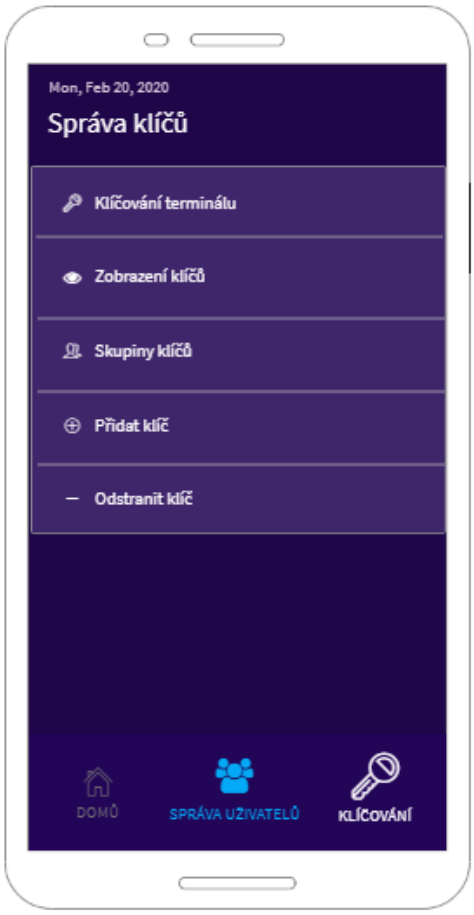
Součástí položky správy uživatelů je také jejich celkový přehled, kde je zobrazeno uživatelské jméno, role a datum posledního přihlášení daného uživatele. Tento přehled se zobrazuje pouze uživatelům s rolí manažer. Zároveň je součástí správy uživatelů možnost existujícího uživatele odstranit. Opět je to umožněno pouze technikům s rolí manažer a vždy jsou před odstraněním vyzvaní k potvrzení, protože se jedná o nevratnou operaci. Celý tento proces lze vidět na Obrázku 25.



Obrázek 25: Zobrazení všech uživatelů v klíčovací aplikaci [29]

8.3 Klíčování

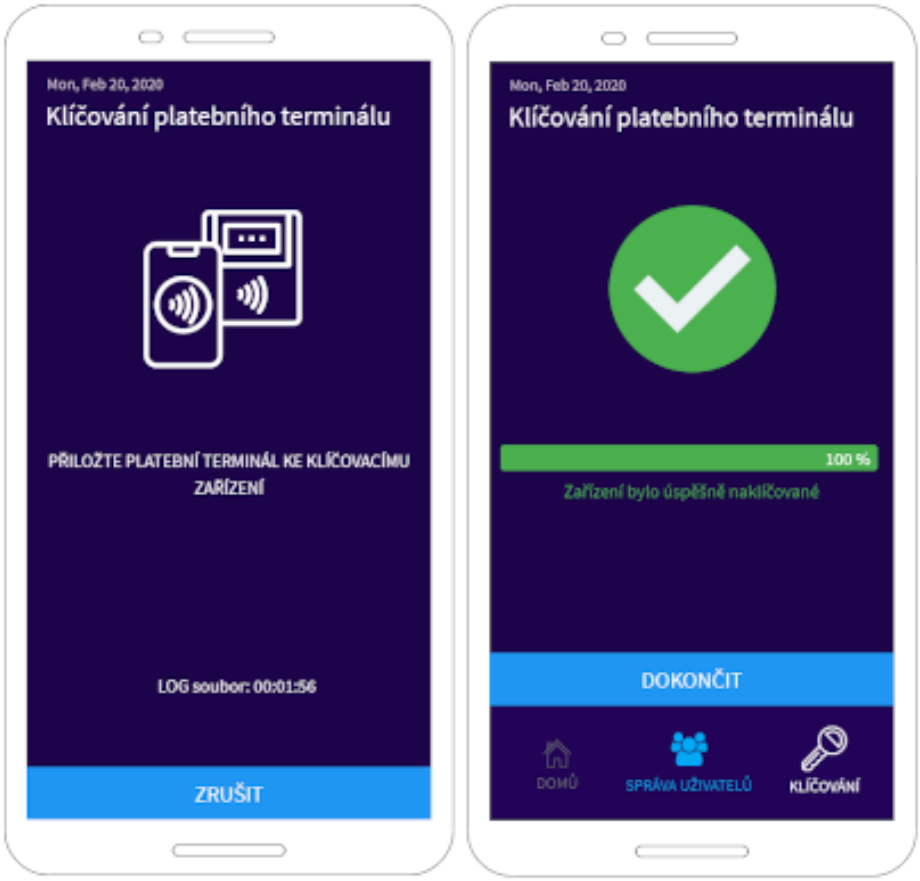
Položka klíčování, která je dostupná všem uživatelským rolím, nabízí správu klíčů a klíčování EMV platebních terminálů. Samotná správa klíčů je dostupná pouze manažerům, pouze ti mohou klíče přidávat, odstraňovat nebo upravovat skupiny klíčů. Zobrazení klíčů a klíčování mohou provádět všichni uživatelé. Správa klíčů, pro roli manažer je znázorněná na Obrázku 26.



Obrázek 26: Správa klíčů pro roli manažer [29]

Hned první možnost z nabídky umožní naklíčovat EMV platební terminál. V rámci této volby jsou veškeré činnosti logovány a ukládány do lokálního uložiště klíčovacího zařízení.

Při zvolení možnosti klíčování terminálu z nabídky klíčování, vyzve klíčovací zařízení k přiložení platebního terminálu. Pokud jsou obě zařízení úspěšně spárovaná, dojde k přenosu potřebných dat, jak z POS teminálu do klíčovacího zařízení, tak naopak. Tento proces je popsaný v kapitole 7.2. Pokud není proces klíčování narušen nebo nedojde k jiné chybě, je klíčování dokončeno, jak lze vidět na Obrázku 27. Zároveň jsou technici o výsledku informovaní zvukovou signalizací.



Obrázek 27: Klíčování platebního terminálu [29]

V průběhu klíčování se ukládají do logu informace, v jakém stavu a fázi se aktuálně technik nachází a s jakým výsledkem operace skončila. Informace ze zařízení jsou následující:

Čekám na přiložení zařízení – klíčovací zařízení čeká na přiložení terminálu, pokud k tomu nedojde do stanovené doby, proces klíčování je automaticky přerušen.

Identifikuji zařízení – klíčovací zařízení zjistí, jestli je přiložený terminál kompatibilní.

Čekám na přijatá data – klíčovací zařízení čeká, až mu terminál pošle nezbytná identifikační data.

Zpracovávám přijatá data – klíčovací zařízení zpracovává přijatá data z terminálu a ověřuje jejich správnost.

Derivace TTK klíče – v tomto kroku dochází k derivaci TTK klíče, jak je popsáno v kapitole 7.2.5.

Probíhá klíčování – v této fázi probíhá klíčování EMV platebního terminálu.

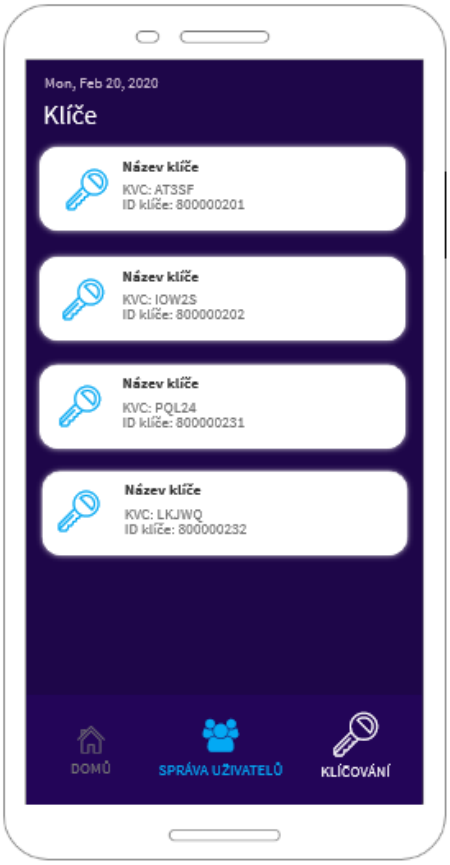
Klíčování dokončeno – platební terminál byl úspěšně naklíčovaný.

Klíčování přerušeno – během procesu klíčování došlo k chybě a nemohl být dokončen.

Záznamy se do logovacího souboru ukládají při každé provedené operaci v průběhu klíčování. Formát logování je uveden na následujícím příkladu:

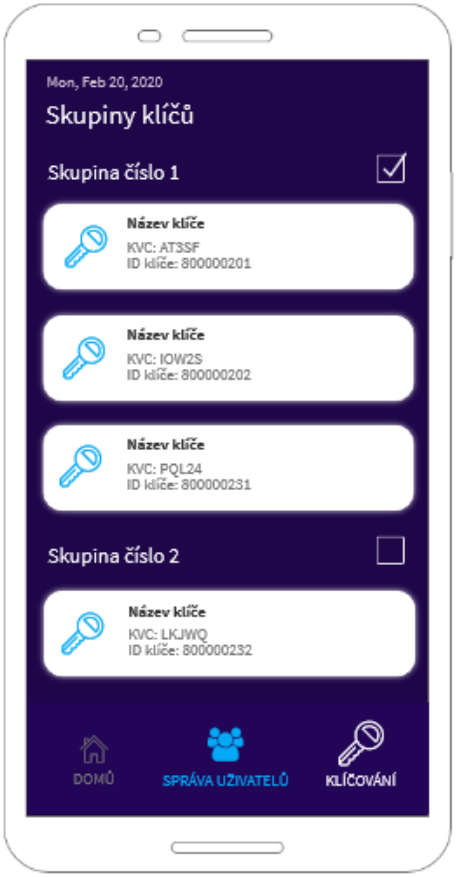
2020-03-21 11:34:15,325 – Identifikuji zařízení – CRITICAL – Přiložené zařízení není kompatibilní s klíčovacím zařízením

Další položkou v nabídce správa klíčů, je jejich zobrazení, jak je uvedeno na Obrázku 28. Zde se zobrazují základní informace o klíčích, jako jsou jejich název, KVC klíče a ID klíče, které je přiděleno danému master klíči.



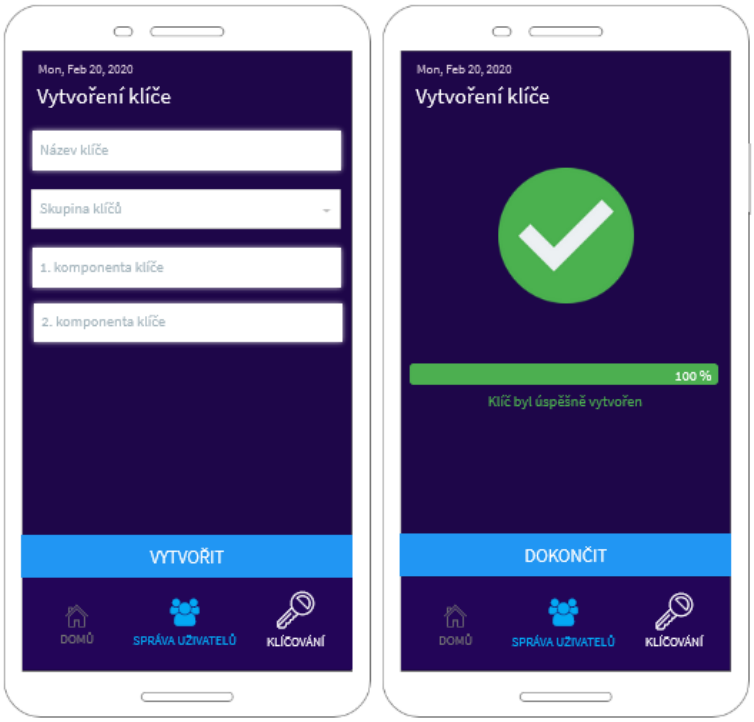
Obrázek 28: Zobrazení klíčů v klíčovacím zařízení [29]

Další možností pro uživatele s rolí manažer je správa skupin klíčů. Tato funkce byla do aplikace navrhnuta z důvodu usnadnění práce s klíči. Manažer může jednoduše operátorovi nastavit, jaké klíče budou pro něj povolené a jaké ne. Tím tedy přiřadí specifické operátory k určitým zákazníkům, viz. Obrázek 29.



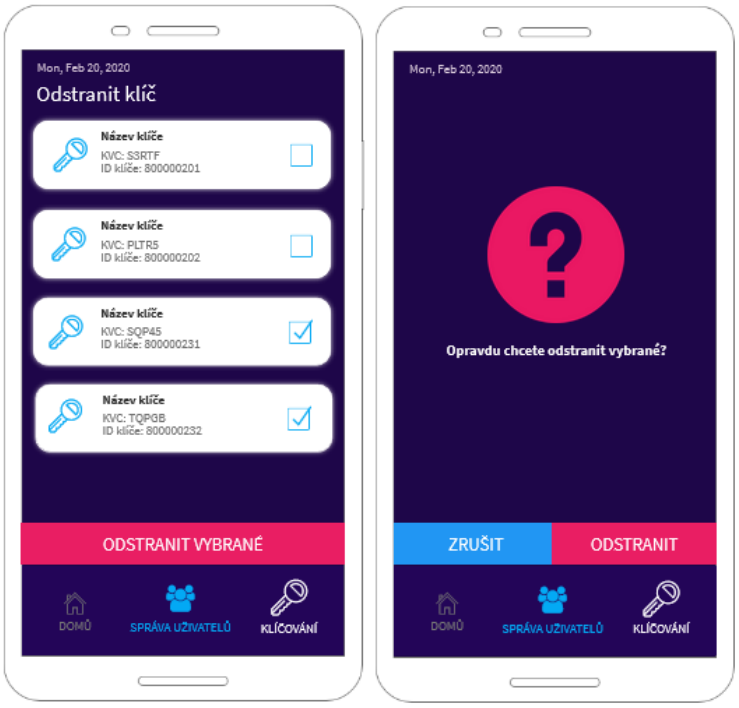
Obrázek 29: Správa skupin klíčů [29]

Další položkou ve správě klíčů je jeho vytvoření. Pokud je nutné klíčovat terminály například pro více společností, je třeba vytvořit více klíčů. Pro vytvoření klíče je nutné zadat název klíče, který musí být unikátní, v rámci všech klíčů, následně vybrat skupinu, do které má klíč spadat a vložit komponenty daného klíče. Každý manažer, který má za úkol zavést nový klíč do klíčovacího zařízení má přidělenu jednu komponentu, která je uložena v tištěné podobě v trezoru v rámci zabezpečené místnosti. Ze zadaných komponent vznikne výsledný klíč. Počet komponent se odvíjí, od prvního nastavení klíčovacího zařízení, kdy se právě počet komponent zvolí. Pokud jsou splněná validační kritéria a klíčovací zařízení spočítá správné KVC, dojde k úspěšnému vytvoření klíče, tuto situaci lze vidět na Obrázku 30.



Obrázek 30: Vytvoření nového klíče [29]

Poslední položkou ve správě klíčů je odstranění klíče. Tato možnost je opět pouze pro uživatele s rolí manažer. V prvním kroku uživatel vybere klíč, který chce odstranit a v kroku druhém musí volbu potvrdit. Lze odstranit více klíčů najednou avšak tato operace je nevratná. Operace odstranění klíče je znázorněna na Obrázku 31.



Obrázek 31: Odstranění klíče [29]

9 PŘÍNOSY NAVRHNUTÉHO ŘEŠENÍ

Následující kapitola popisuje hlavní přínosy navrhnutého řešení, oproti původnímu procesu klíčování ve vybrané společnosti. Postupně rozebírá jednotlivé části klíčovacího procesu a uvádí přínosy nebo rozdíly oproti původnímu řešení.

9.1 Klíčovací karty

V původním řešení docházelo k odečítání klíčovacích komponent z klíčovacích karet, při každém jejich použití. Proto byla v případě jejich vyčerpání nutná opětovná výroba, to zvyšovalo, jak časové, tak finanční náklady procesu klíčování. Pro představu na jedné klíčovací kartě je umístěno 300 komponent, kdy TTK klíč se skládá ze dvou nebo více karet. Z toho vyplývá, že pro naklíčování 300 terminálů budou třeba minimálně dvě karty. Pokud by bylo třeba naklíčovat například 3000 terminálů, už by bylo třeba vyrobit minimálně 20 klíčovacích karet s TTK komponentami. V nově navrhnutém řešení slouží karty pouze k přihlášení ke klíčovacímu zařízení a k odečítání komponent nedochází, proto není nutná jejich obnova a tím dochází k finanční i časové úspoře.

9.2 Propojení klíčovacího zařízení a platebního terminálu

Volba propojení klíčovacího zařízení a EMV platebního terminálu, pomocí bezdrátové technologie NFC urychlí proces klíčování téměř o tři čtvrtiny. Jeden z důvodu je ten, že není nutné propojovat obě zařízení pomocí kabeláže, ale stačí zařízení k sobě pouze přiložit. Další důvod je ten, že není vždy nutné zadávat PIN klíčovací karty, při procesu klíčování, ale pouze při přihlášení do klíčovacího zařízení.

9.3 Implementace pro více zákazníků

V rámci původního řešení klíčování bylo nutné pro každého zákazníka a jeho platformu vyrobit a držet v trezoru specifické klíčovací karty, pro několik techniků.

U nově navrhnutého řešení slouží karty pouze k přihlášení do klíčovacího zařízení. Pro každého zákazníka, pro kterého jsou klíčovány platební terminály, se vloží do klíčovacího zařízení odlišný master klíč, pomocí kterého se vygeneruje TTK klíč. Součástí nového řešení je i jednoduchá správa klíčů, včetně jejich skupin, jak je uvedeno v kapitole 8.3.

9.4 Využití více šifrovacích algoritmů

Návrh řešení využívá v procesu derivace pomocí 3DES algoritmus, z důvodu podpory tohoto algoritmu, v rámci platebních terminálů. V roce 2023 bude podle PCI DSS normy použití tohoto algoritmu zakázané, i proto je návrh řešení připraven tak, že pro použití do budoucna podporovaného šifrovacího algoritmu AES bude stačit úprava v rámci šifrovací knihovny.

9.5 Správa uživatelů a klíčů

V původním řešení byla správa uživatelů, respektive i klíčů řešena přidělením specifických klíčovacích karet s komponentami technikům, kteří měli na starosti klíčování. Součástí nového návrhu klíčování je i správa uživatelů a klíčů, přímo v aplikaci, která je určená pro klíčovací zařízení.

ZÁVĚR

Tato diplomová práce se zabývá problematikou návrhu systému klíčování EMV platebních terminálů podle PCI DSS normy pro vybranou společnost. Práce byla rozdělena na dvě stěžejní sekce, a to na teoretickou a praktickou.

V teoretické části byla provedena literární rešerše věnující se stručnému popisu platebních karet a terminálů, včetně jejich typů a historie. Dále zde byla rozebrána problematika EMV a NON-EMV standardu a s tím související tok EMV transakce. V dalších podkapitolách byly představeny základní pojmy z oblasti kryptografie a šifrování, včetně historie, rozdělení a základních matematických operací. Z důvodu nutnosti splnění přísných PCI DSS norem jsou veškeré kryptografické operace vykonávány v rámci HSM (Hardware Security module), i proto jsou v teoretické části popsány jednotlivé klíče a komponenty, se kterými se v rámci HSM pracuje. Na závěr první části je teoreticky popsán princip klíčování, včetně příkladu klíčování platebních terminálů ze společnosti Landi Commercial Equipment Co., Ltd.

Na začátku praktické části je stručně popsaná firma, pro kterou je návrh klíčování EMV platebních terminálů realizován. U vybrané společnosti je popsané hlavně její produktové portfolio. Hned v další kapitole byla provedena analýza současného stavu klíčování EMV platebních terminálů ve vybrané společnosti. Aktuálně společnost využívá řešení, které je rozděleno na dvě hlavní části. V části první se náhodně generují TTK klíče, v rámci HSM, kdy jednotlivé komponenty TTK klíče jsou postupně uloženy na klíčovací karty, které jsou přiděleny technikům. Každou komponentu na kartách lze využít pouze jednou. Druhá část současného řešení se zabývá klíčováním, které probíhá v zabezpečené místnosti, kdy k naklíčování jsou potřeba vždy minimálně dva technici. Každý technik musí postupně vložit klíčovací kartu do terminálu, kdy dojde k ověření platnosti certifikátů na kartě a k zadání PIN kódu. Pokud ověření a zadání projde v pořádku, dojde k vygenerování TTK klíče, který je složený z operace XOR jednotlivých komponent klíčovacích karet. Následně se výsledný klíč i s dalšími informacemi uloží do zabezpečené části hardwaru terminálu.

Další kapitola je zaměřená na návrh nového řešení klíčování EMV platebních terminálů. Přáním společnosti bylo navrhnout systém klíčování, pomocí kterého bude možné naklíčovat nové typy terminálů a také zefektivnit celý proces. V rámci této kapitoly byla navrhnutá topologie sítě a komunikace mezi jednotlivými prvky systému. O oddělení vnitřní sítě společnosti, ve které je umístěný systém pro správu terminálů a klíčovací zařízení se stará firewall a autentizační proxy server. Tento server je veřejně dostupný a počítá se u něj

s provozováním v režimu 24/7 s možností obsluhovat minimálně desítky paralelních připojení najednou. Dále je součástí této kapitoly popsáno propojení mezi klíčovacím zařízením a platebním terminálem, kdy bylo zvoleno propojení pomocí bezdrátové technologie NFC s módem Peer-to-peer, takže je mezi oběma zařízeními vytvořen obousměrný komunikační kanál. Nezbytnou součástí návrhu jsou i jednotlivá bezpečnostní pravidla a definice rolí, které figurují při obsluze klíčovacího zařízení. Pro splnění auditních požadavků byla také navržena optimální politika hesel a veškeré aktivity realizované v rámci klíčovacího zařízení jsou ukládány do auditního logu.

V rámci návrhu klíčování byly popsány jednotlivé kryptografické operace s klíči a citlivými daty. V této kapitole byl popsán princip derivace výsledného TTK klíče, včetně jeho uložení do zabezpečené části hardwaru platebního terminálu.

Podle požadavků společnosti byl vytvořen návrh klíčovací aplikace, včetně dokumentace k aplikaci a k procesu klíčování. Byl kladen důraz, aby byl popis stručný a výstižný, i proto jsou jednotlivé prototypy náhledů obrazovek aplikace klíčovacího zařízení popsány přehlednou formou.

V poslední kapitole byly popsány přínosy navrhnutého řešení. Cílem návrhu bylo zjednodušit celý proces klíčování a eliminovat čas, který je ke klíčování nutný. Vybraným propojením klíčovacího zařízení a platebního terminálu, pomocí bezdrátové technologie NFC bylo ušetřeno téměř tři čtvrtiny z celkového času, který je nutný pro kompletní klíčovací proces. K urychlení procesu přispělo hlavně to, že není nutné obě zařízení propojovat pomocí kabeláže a vždy zadávat PIN ke klíčovacím kartám. Zde lze počítat i s finanční úsporou, protože nedochází k opotřebení konektorů. Další výhodou nově navrženého systému je využití přihlašovacích karet. Ty jsou u nového systému nutné pouze k přihlášení do klíčovacího zařízení. U původního řešení se jednotlivé komponenty, které byly umístěny na klíčovacích kartách, odečítaly při naklíčování terminálu. Proto bylo nutné při vyčerpání komponent vyrábět nové klíčovací karty. Zde lze také pozorovat finanční úsporu nově navrhnutého řešení.

V neposlední řadě umožňuje klíčovací zařízení správu více master klíčů, takže lze klíčování jednoduše aplikovat pro více zákazníků a jejich platformy. Nové řešení také zvyšuje bezpečnost, díky správě uživatelů a možnosti přidělovat klíče specifickým uživatelským rolím.

SEZNAM POUŽITÉ LITERATURY

[1] PLESKAČ, Matěj. Platební terminál: jak vybrat ten správný pro vaší provozovnu? Inspirum [online]. Inspirum, 2018 [cit. 2020-02-26]. Dostupné z: https://blog.inspirum.cz/jak-vybrat-platebni-terminal/

[2] CHEN, Zhiqun. Java Card technology for Smart Cards: architecture and programmer's guide. Boston: Addison-Wesley, 2000. ISBN 0201703297.

[3] How EMV Chip and PIN Technology Contributes to Security. SumUp [online]. Londýn, 2019 [cit. 2019-11-09]. Dostupné z: https://sumup.com/emv-credit-card-chip/

[4] JUŘÍK, Pavel. Svět platebních a identifikačních karet. 2. přeprac. vyd. Praha: Grada, 2001. ISBN 8024701952.

[5] PÍŠA, Rudolf. Třicet let platebních karet v Česku a Slovensku. Das Media, 2019. ISBN 9788097251932

[6] VYCHODIL, Josef. Princip a zabezpečení platebních karet [online]. 2015, 6 [cit. 2020-02-15]. Dostupné z: http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/0/princip-a-zabezpeceni-platebnich-karet-1-1-1/

[7] JUŘÍK, Pavel. Platební karty: magnetický proužek. Idnes.cz | Zpravodajství [online]. 2005 [cit. 2020-02-15]. Dostupné z: https://www.idnes.cz/finance/banky-a-sporeni/platebni-karty-magneticky-prouzek.A051130_173803_fi_osobni_zal

[8] Smart card basics – A short guide (2020) [online]. 19.2.2020 [cit. 2020-02-26]. Dostupné z: https://www.gemalto.com/companyinfo/smart-cards-basics

[9] Jak funguje RFID technologie. Aledo [online]. [cit. 2020-02-18]. Dostupné z: https://www.aledo.cz/prumyslova-identifikace/jak-funguje-rfid-technologie/

[10] DOSEDĚL, Tomáš. Pojď trochu blíž: popis technologie NFC [online]. 22.8.2012 [cit. 2020-02-26]. Dostupné z: https://www.mobinfo.cz/pojd-trochu-bliz-popis-technologie-nfc/

[11] VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. Praha: Albatros, 2006, 340 s. Oko. ISBN 8000018888

[12] KLÍMA, Vlastimil. Moderní kryptografie [online]. 11.4.2007 [cit. 2020-02-26]. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2007.pdf

[13] BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015. ISBN 9788072049257.

[14] Hashovací funkce. University information system of Mendel University in Brno [online]. [cit. 2020-02-26]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7029

[15] AUMASSON, Jean-Philippe a Matthew D. GREEN. Serious cryptography: a practical introduction to modern encryption. San Francisco: No Starch Press, [2017]. ISBN 1-59327-826-8.

[16] Symetrické a asymetrické šifrování. NaPočítači.cz [online]. 2018 [cit. 2019-11-07]. Dostupné z: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueid-gOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/

[17] Symetrická kryptografie. University information system of Mendel University in Brno [online]. [cit. 2019-11-06]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7026

[18] MATĚJOVÁ, Lucie. RSA [online]. [cit. 2020-02-23]. Dostupné z: http://www.kryptografie.wz.cz/data/RSA.htm

[19] Hardware security module. Sefira [online]. 2019 [cit. 2019-11-05]. Dostupné z: https://www.sefira.cz/hsm-bezpecne-uloziste-klicu/

[20] HSM and Various Keys Used. Netz Technology Solutions [online]. 2018 [cit. 2019-11-05]. Dostupné z: http://netzts.in/retail-payments-domain/hsm-lmk-zmk-tmk-pvk-cvk/

[21] Importing ZPK and ZMK into Thales Payshield 9000 HSM. Gunvant kathrotiya A log of dev life [online]. 2016 [cit. 2019-11-10]. Dostupné z: http://www.gunvant.net/2016/03/25/Importing-ZPK-and-ZMK-into-Thales-Payshield-9000-HSM.html

[22] Dynamic Key Exchange Models. Andy Orrock | Payment Systems [online]. 2007 [cit. 2019-11-11]. Dostupné z: https://www.andyorrock.com/2007/04/dynamic_key_exc.html

[23] Financial Service Components Overview. Oracle Documentation [online]. 2010 [cit. 2019-11-09]. Dostupné z: https://docs.oracle.com/cd/E19321-01/819-5536-12/4_FS.html

[24] Interní materiály vybrané společnosti

[25] VeriFone VX520 Credit Card Reader Unboxing & Review. Merchant Maverick [online]. 2020, 30.03.2020 [cit. 2020-04-03]. Dostupné z: https://www.merchantmaverick.com/verifone-vx-520-credit-card-reader-unboxing-and-review/

[26] A920Android SmartPOS. *PAX Technology* [online]. 2020 [cit. 2020-04-05]. Dostupné z: https://www.paxtechnology.com/a920

[27] Vyznáte se v platebních kartách? *BNÚ* [online]. [cit. 2020-04-07]. Dostupné z: http://www.bnu.cz/clanek/9-vyznate-se-v-platebnich-kartach

[28] The Evolution of the Credit Card: From Paper to Plastic to Virtual. *Relatively Interesting* [online]. 2018 [cit. 2020-04-03]. Dostupné z: https://www.relativelyinteresting.com/evolution-credit-card-paper-plastic-virtual/?utm_source=org

[29] Vlastní zpracování

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Advanced Encryption Standard.

CSV Comma-separated values.

CVK Card Verification Key.

CVM Cardholder Verification Methods.

ČSOB Československá obchodní banka.

DES Data Encryption Standard.

DK Derivation Key.

DSS Data Security Standard.

EMV Europay, MasterCard, VISA.

FTPS File Transfer Protocol Security.

GPS Global Positioning System

HSM Hardware Security Module.

HW Hardware.

IEC International Electrotechnical Commission.

ISO International Organization for Standardization.

IV Initialization Vector.

KLA Key Loading Application

KLD Key Loading Device.

KVC Key Value Check.

LMK Local Master Key.

MAC Message Authentication Code.

MD Message Digest.

MK Master Key.

MPOS Mobile Point of Sale.

NFC Near Field Communication.

NTK Network Key.

PCI Payment Card Industry.

PID Product Identificator.

PIN Personal Identification Number.

POS Point of sale.

PVK PIN Verification Key.

RASP Runtime Application Self-Protection.

RFID Radio Frequency Indentification.

RND Random.

RSA Rivest, Shamir, Adleman.

SFTP Secure File Transfer Protocol.

SHA Secure Hash Algorithm.

SN Serial Number.

SSH Secure Shell.

SSL Secure Sockets Layer.

TAK Terminal Authentication Key.

TCP Transmission Control Protocol.

TEK Terminal Encryption Key.

TLS Transport Layer Security.

TMK Terminal Masker Key.

TMK Terminal Master Key.

TMS Terminal Management System.

TPK Terminal PIN Key.

TTK Terminal Transport Key.

TTK Terminal Transport Key.

VISA Visa International Service Association.

ZMK Zone Master Key.

ZMK Zone Master Key.

ZPK Zone Pin Key.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK