HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

THE SOFTWARE COMPANY
abrantix

Machbarkeitsstudie einer Smartphone-App für EMV-kompatible Zahlungen via NFC

Feasibility Study for a Smartphone App to Make EMV-Compatible Payments via NFC

Bachelor Thesis

Abteilung Informatik
Hochschule für Technik Rapperswil
Institut für Internet-Technologien und -Anwendungen

Christian Mäder, Sandro Vogler

Frühjahrssemester 2013

Advisor:	Prof. Frank Koch
Projektpartner:	Abrantix AG
Experte:	Matthias Lips
Gegenleser:	Prof. Dr. Josef Joller

Unser Dank gebührt in erster Line unserem Advisor, Prof. F. Koch, welcher uns während der Arbeit hilfreich zur Seite gestanden hat und unsere Vorhaben unterstützt hat. Speziell im Bereich der Methodik und der wirtschaftlichen Betrachtungsweise hat er uns regelmässig wertvolle Hinweise gegeben und uns dennoch die Freiheit gelassen, das Thema selbstständig zu erarbeiten.

Ausserdem bedanken wir uns bei unserem Gegenleser, Prof. J. Joller, für die rasche und unkomplizierte Hilfe bei Problemen (speziell bei der Beschaffung des Windows Phones) sowie bei unserem Experten, Herr M. Lips für die aufgeschlossene Haltung gegenüber dem Thema.

Weiter möchten wir uns bei der Abrantix AG bedanken, wo wir vom Fachwissen verschiedener Mitarbeiter - insbesondere von Herrn Eckstein und Herrn Vetsch - profitieren konnten. Dank der guten Beziehungen unseres Projektpartners sind wir an Hintergrundinformationen zu einer eher verschlossenen Branche gelangt, was massgeblich zur Qualität der Arbeit beigetragen hat.

Schliesslich danken wir unseren Familien für die Geduld während der Arbeit und deren mentale Unterstützung.

Abstract

This thesis researches the elements required to process an EMV[1] compatible payment transaction at a POS terminal[2] using a smartphone. It takes a solution-oriented view at the issues that have prevented a successful launch up to now.

First, a technological overview is given which covers the most important players in the EMV payment ecosystem. A market survey has been conducted in order to outline the roles of the players in the Swiss market and the linkage between them. Additionally, the possibility of Swiss telecommunication providers acting as TSM[3] has been researched.

Based on these findings, the challenges for a technically successful and commercially viable solution are outlined. Various possible solutions are discussed and weighted against each other.

The chosen approach uses the NFC peer-to-peer mode that acts as a wrapper for the EMV communication. This approach also enables the smartphone and the POS to exchange further data (e.g. for loyalty), making the system more flexible and expandable.

As a proof of concept a prototype has been implemented for which the chosen software architecture and the problems identified have been documented.

Furthermore an assessment of the designed solution regarding processes, cost, time schedule and compliance to regulations has been conducted.

Keywords:

Mobile payment, Banking, NFC, EMV, Secure Element, POS, Terminal, Card emulation, Loyalty program, EFTPOS, Wallet

[1] International specification for payment processing at a POS terminal. EMV uses a chipcard instead of the legacy magnetic stripe.
[2] Payment terminal at the point of sale. The terminal accepts a payment card and handles the authentication of the customer.
[3] Trusted Service Manager. A party which establishes a trust relationship between two or more parties. E.g. between a card issuer and a mobile network provider.

Abstract

Die Thesis untersucht, welche Elemente nötig sind, um mit einem Smartphone EMV[4]-kompatible Zahlungen via NFC an einem POS-Terminal[5] durchführen zu können. Dabei wird lösungsorientiert auf die Problematiken eingegangen, welche bisher einen Markdurchbruch verhindert haben.

In einer Marktuntersuchung werden die in die Wertschöpfungskette involvierten Unternehmen und deren Verbindungen untereinander untersucht. Ebenso werden die Möglichkeiten eines Markteinstieges der Schweizer Mobilkommunikationsanbieter als TSM[6] beleuchtet.

Auf diesen Erkenntnissen aufbauend werden die Herausforderungen für eine technisch und kommerziell machbare Lösung erarbeitet. Die verschiedenen möglichen Lösungen werden diskutiert und miteinander verglichen.

Der ausgewählte Ansatz verwendet den NFC Peer-to-Peer-Modus und kapselt die EMV-Kommunikation. Dieser Ansatz erlaubt es, weitere Daten zwischen dem POS und dem Smartphone auszutauschen (z.B. für Loyalty-Anwendungen), was die Lösung flexibel und erweiterbar macht.

Zum Nachweis der Umsetzbarkeit wurde ein Prototyp entwickelt, dessen Software-Architektur dokumentiert und die angetroffenen Probleme diskutiert.

Weiter wurde die Lösung hinsichtlich Organisation und Prozessen, Wirtschaftlichkeit, Zeitplan und regulatorischen Aspekten beurteilt.

Stichwörter:

Mobile payment, Banking, NFC, EMV, Secure Element, POS, Zahlterminal, Card emulation, Kundenkarte, Bonusprogramm, EFTPOS, Wallet

[4] Internationaler Standard für die Abwicklung von bargeldlosen Zahlungen an einem Zahlterminal. EVM verwendet eine Chipkarte und ersetzt damit den Magnetstreifen.

[5] Zahlterminal an einer Kasse, welches eine Zahlkarte akzeptiert und die Authentisierung des Kunden vornimmt.

[6] Trusted Service Manager. Eine Partei, welche zwischen zwei oder mehreren vermittelt und der alle Parteien vertrauen. Beispielsweise ermöglicht ein TSM, dass der Kartenherausgeber und der Mobilfunkprovider zusammenarbeiten können.

Executive Summary

Introduction

Although the technical concept for contactless payment[7] at POS terminal[8] has been around for some years, the technology has not taken off large scale in Europe yet. One reason for this was the lack of compatible POS terminals causing the card issuer not to be interested in the technology. This first obstacle preventing market penetration seems to be falling away as old POS terminals are currently replaced by their contactless capable successors. Also, newly issued cards come with a contactless capable chip; at the same time, mobile network providers are pushing NFC[9] capable phones.

Problem

Beside these significant efforts, several other issues need to be addressed in order to establish a successful business model. The contactless payment model was developed with a contactless smart card[10] (e.g. a credit card) in mind. Originally, smartphones had not been considered a part of the payment process; the compatibility for these devices was added later.

Smartphones thus use the so-called *card emulation mode*, where they behave just like contactless smart cards, eliminating the necessity to change the protocol on the terminal side.

Research Question

The use of the card emulation mode in almost any smartphone requires being able to control a so called *secure element*, which provides a protected storage of cryptographic keys and other sensitive data. This secure element is either under the control of the mobile device manufacturer (chip soldered onto the circuit board) or the mobile network provider (chip integrated into SIM card).

This causes either the mobile device manufacturer or the mobile network operator to become another stakeholder within the value chain of the payment process. Of course, this situation is undesired by the current stakeholders, mainly the card issuers (in Switzerland, typically a bank).

The aim of this thesis is to give a possible solution for the card emulation dilemma by allowing the issuer to provide mobile payment without involving a third party into the value chain.

Approach and Results

Several possible solutions for the issue have been considered. Each has its drawbacks (financial, logistical or regulatory) and seems, at the time, unlikely to succeed. Additionally, the linkage between the participants involved in the payment process has been found to be unique in Switzerland, which needed to be considered.

Therefore, a completely new approach has been developed. We propose the use of the NFC peer-to-peer Mode in order to overcome problems caused by the card emulation mode. This approach also enables the smartphone and the POS to exchange further data (e.g. for loyalty), making the system more flexible and

[7] Payment by tapping a payment card onto a compatible terminal
[8] Point of Sale payment terminal
[9] Near Field Communication; A standard for wireless data communication
[10] A plastic card containing an antenna from which reader devices may retrieve data when in close proximity

expandable. As the EMV-protocol communication is tunneled, it is completely transparent to the existing parts of the terminal.

In order to proof the technical feasibility of the proposed solution, a prototype has been implemented. Furthermore, an assessment of the designed solution regarding processes, costs and compliance to regulations has been conducted.

Even though the solution fits the Swiss market situation, it is not limited to Switzerland and can technically be deployed anywhere.

Executive Summary

Einleitung

Obwohl bereits seit einigen Jahren technische Lösungen für kontaktlose Zahlungssysteme existieren, konnte sich die Technologie bisher in Europa nicht durchsetzen. Mitverantwortlich dafür war die mangelnde Verfügbarkeit der Hardware; so waren bisher insbesondere nur sehr wenige Bezahlterminals vorhanden, an welchen kontaktlos bezahlt werden konnte. Dieses Hindernis für eine Marktdurchdringung scheint nun wegzufallen: alte POS[11] Terminals werden grossflächig durch Versionen mit der Möglichkeit des kontaktlosen Bezahlens ersetzt. Auch neu ausgegebene Kreditkarten verfügen bereits zunehmend über die Funktionen und Hardware für kontaktloses Bezahlen. Gleichzeitig forcieren die Mobilfunkprovider den Verkauf von NFC[12]-fähigen Smartphones.

Problem

Trotz dieser beachtlichen Bemühungen existieren noch weitere Hindernisse, welche die Etablierung eines erfolgreichen Geschäftsmodells behindern. So wurde die Kontaktlos-Erweiterung ursprünglich nur für kontaktlose Chipkarten[13] (zum Beispiel kontaktlose Kreditkarten) entwickelt. Smartphones wurden erst später in Betracht gezogen und nachträglich eine Lösung entwickelt, um damit bezahlen zu können.

Smartphones verwenden beim Bezahlvorgang den so genannten „Card Emulation Mode“, in dem sie sich gegenüber dem Terminal genau wie eine kontaktlose Chipkarte verhalten. Dadurch mussten aufseiten des Terminals keine Anpassungen vorgenommen werden.

Forschungsfrage

Um auf dem Smartphone den Card Emulation Mode zu aktivieren, ist bei praktisch allen Modellen die Kontrolle über das sogenanntes „Secure Element“ nötig. Das Secure Element bietet einen geschützten Speicherbereich, in welchem kryptografische Schlüssel oder schützenswerte Informationen gespeichert werden können. Diese Secure Element ist entweder unter der Kontrolle des Herstellers des Smartphones (in diesem Fall ein Chip, welcher auf die Platine gelötet ist) oder derjenigen des Mobilfunkproviders (Chip in SIM-Karte integriert).

Dies führt dazu, dass entweder der Mobilfunkprovider oder der Gerätehersteller als weiteren Stakeholder in das Geschäftsmodell integriert werden muss. Dies ist natürlich aus Sicht der bisherigen Stakeholder, speziell der Kartenherausgeber (in der Schweiz typischerweise eine Bank) unerwünscht.

Ziel dieser Thesis ist eine mögliche Lösung für dieses Dilemma aufzuzeigen, welche es dem Kartenherausgeber (Issuer) erlaubt, Mobile Payment[14] anzubieten, ohne zusätzliche Parteien in der Wertschöpfungskette.

Vorgehen und Resultate

Mehrere bestehende Lösungsansätze für das Problem wurden untersucht. Es wurde jedoch festgestellt, dass die bestehenden Ansätze gewichtige Nachteile aufweisen (entweder finanzieller, logistischer oder regulato-

[11] Bezahlterminal im Kassenbereich (Point of Sale)
[12] Near Field Communication. Ein Standard zu drahtlosen Datenübertragung
[13] Eine Kunststoffkarte, welche eine Antenne enthält und von welcher ein Lesegerät Daten auslesen kann, wenn sich die Karte in unmittelbarer Nähe befindet
[14] Kontaktloses Bezahlen mit dem Smartphone

rischer Natur), weshalb es unwahrscheinlich erscheint, dass sich eine der Lösungen in naher Zeit durchsetzen wird. Weiter besteht in der Schweiz eine enge Beziehung zwischen den am Zahlungsprozess beteiligten Unternehmen, welche aufgrund ihrer Einzigartigkeit berücksichtigt werden muss.

Aus diesen Gründen wurde ein neuer Ansatz entwickelt. Wir schlagen vor, den NFC Peer-to-Peer-Modus zu verwenden, um die Probleme des Card Emulation Modes zu umgehen. Dabei wird die EMV-Protokoll-Kommunikation getunnelt, weshalb die Modifikationen für die existierenden Teile des Terminals transparent sind.

Um die technische Machbarkeit der vorgeschlagenen Lösung zu verifizieren, wurde ein Prototyp entwickelt. Weiter wurde die Lösung hinsichtlich Organisation und Prozessen, Wirtschaftlichkeit und regulatorischen Aspekten beurteilt.

Obwohl die Lösung spezifisch für die Anforderungen des Schweizer Markts entwickelt wurde, ist sie nicht darauf limitiert und kann überall eingesetzt werden.

Inhalt

1 Einführung

1.1 Ausgangslage

Im vergangenen Jahr wurden in der Schweiz die ersten Exemplare einer neuen Generation von Bezahlkarten ausgegeben, die kontaktloses Bezahlen ermöglichen. Anders als bei herkömmlichen, chipbasierten Bezahlkarten muss die Karte dabei nicht mehr in das Terminal eingeführt werden, sondern es genügt, diese nahe an eine bestimmte Fläche des Terminals zu halten. Technisch gesehen handelt es sich bei diesen Karten umso genannte *Contactless Smartcards*. Sie verfügen über eine eingebaute Antenne, mit welcher sie drahtlos mit dem Terminal kommunizieren können. Die Karten benötigen dabei keine eigene Batterie; der Chip, welcher für die Kommunikation verantwortlich ist und die notwendigen Daten enthält, wird über das elektromagnetische Feld, welches das Terminal aufbaut, induktiv mit Energie versorgt.

Wie die bisherigen Karten beherrschen auch die Contactless Smartcards kontaktbehaftete Kommunikation. Somit stellt die Drahtlostechnologie eine reine Erweiterung der Nutzungsmöglichkeiten dar. Eine über die Funktionalität der kontaktbehafteten Kartentransaktion hinausgehende Erweiterung hat nicht stattgefunden.

Zur Kommunikation über die Drahtlos-Schnittstelle wird ein auf ISO 14443 basierendes Protokoll eingesetzt. Obwohl die zugehörigen Spezifikationen (beispielsweise [1]) bereits vor über zehn Jahren erstmals publiziert worden sind, haben die Schweizer Issuer erst jetzt begonnen, Kreditkarten mit Funkschnittstellen herauszugeben.

Diese träge Adaption der Technologie seitens der Issuer in Verbindung mit der steigenden Popularität von Smartphones hat dazu geführt, dass bereits mehrere Ansätze von *Wallets* gestartet wurden. Einer breiten Öffentlichkeit wurde das Thema durch *Google Wallet* zugänglich, welches der Internet-Konzern im Jahr 2011 lanciert hat [2]. Spätestens seit diesem Zeitpunkt hat sich um das Thema NFC und Mobile Payment ein regelrechter Hype entwickelt.

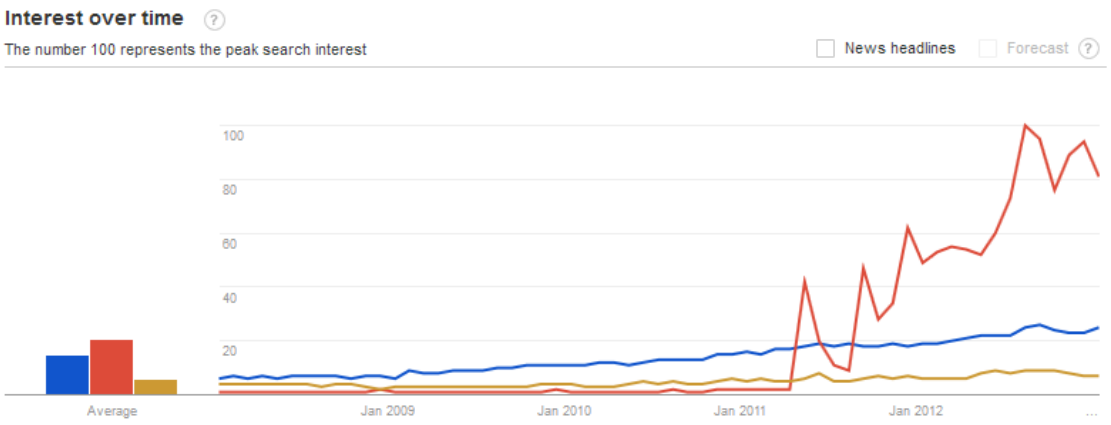

Abbildung 1: Google Trends zeigt die Häufigkeit, nach der ein Begriff auf Google gesucht wurde, im Verlauf der Zeit. Anzahl Aufrufe für die Begriffe “Mobile Payment” (blau), “Google Wallet” (rot) und “PayPass” (gelb) seit 2008 (relative Zahlen). Siehe http://j.mp/nfctrends.

Auch das Marktforschungsunternehmen Gartner nennt NFC in seinem “2012 Hype Cycle for Emerging Technologies” [3] als eine der sich am schnellsten entwickelnden Technologien. Gartner führt NFC auch als eine der Schlüssel-Technologien auf, welche den Umgang von Menschen mit Technologien natürlicher

gestalten werden. So geht Gartner davon aus, dass in Zukunft alle Zahlungen elektronisch abgewickelt werden. Gemäss Gartner wird der Wendepunkt hin zu diesem Szenario erreicht sein, wenn sich NFC Payment und mobiles OTA[15] Payment zu massentauglichen Lösungen entwickelt haben.

Der Business Case ist insofern interessant, weil NFC eine sehr mächtige *enabling technology* ist und die Einsatzmöglichkeiten nicht auf den Finanzsektor beschränkt sind. Es existieren bereits heute Systeme, welchen sich durch Smartphones steuern lassen (beispielsweise Zutrittskontrollsysteme, siehe [4]). Weiter ist auch der Detailhandel sehr interessiert; sie erhoffen sich dank NFC ihre Loyalty Programme aufwerten zu können und damit eine bessere Kundenbindung zu erreichen. Ähnlich möchten Unternehmen aus der Personenbeförderungsbrache ihre Tickets auf das Smartphone bringen, wobei sie wegen des einfacheren Einkaufs über das Internet und des vereinfachten Handlings mit weniger Kosten rechnen [5]. Ein weiterer Einsatzbereich sind Werbeplakate, bei denen die Interaktion mit dem Betrachter verstärkt werden soll und das Werbemedium als Ganzes aufgewertet werden soll [6]. Mögliche Business Cases im NFC-Bereich wurden unter anderem vom NFC Forum zusammengefasst [7].

Die genannten Wallets Apps ermöglichen typisch, mehrere Bezahlkarten auf dem Mobiltelefon zu speichern. Der Bezahlvorgang wird durch das Smartphone abgewickelt, ohne dass die Karte präsentiert werden muss. Konkret wird anstelle der Karte das Gerät an die Antennenfläche des Terminals gehalten.

Dies wird überhaupt erst möglich, weil viele aktuelle Smartphones (im Hochpreissegment praktisch alle aktuellen Geräte, aber auch zunehmend im mittleren Preisspektrum) über NFC verfügen. Der NFC-Standard selbst baut auf dem ISO 14443 Standard auf (siehe auch Appendix II), wodurch Kompatibilität auf dem Physical Layer gewährleistet ist. Dabei stellt der NFC-Standard Kommunikationsprofile für verschiedene Anwendungsfälle zur Verfügung, während ISO 14443 lediglich die Kommunikationsschicht spezifiziert. Damit ist der NFC-Standard also viel stärker an einen Revenue Case gekoppelt, was massgeblich dazu beigetragen hat, dass er sich relativ rasch etablieren konnte.

Wird das Smartphone zum Bezahlen verwendet, muss der NFC-Chip in den sogenannten *Card Emulation Mode* versetzt werden. Dabei imitiert das Smartphone das Verhalten einer ISO 14443-kompatiblen Contactless Smartcard. Der Card Emulation Mode stellt dabei eine Art Fallback dar; so sind in diesem Modus die Funktionalitäten (höhere Protokollschichten) von NFC nicht nutzbar.

Auf dem Chip der Bezahlkarte kann kryptografisches Material sicher gespeichert werden, welches ermöglicht, den Consumer beziehungsweise die Karte zu identifizieren und die Zahlung zu autorisieren. Solche Chips, welche sowohl auf Firmware-Ebene als auch physikalisch besonders gegen unerlaubte Zugriffe gesichert sind, werden als *Secure Element* bezeichnet. Aktuelle Implementierungen von EMV-kompatiblen Wallets verwenden als Secure Element entweder einen auf die Hauptplatine aufgelöteten Chip oder eine spezielle SIM-Karte.

Diese Anforderung stellt insbesondere für die Issuer ein Problem dar: Im aktuellen Ausgabeprozess verfügen sie selbst über die Kontrolle über die Chips in den Karten. Das Bezahlmodell mit dem Smartphone unterscheidet sich aber grundlegend von demjenigen mit Plastikkarten, weil nur ein einziger Chip zur Verfügung steht, welcher mehrere Karten speichert: Während bisher jeder Issuer unabhängig von den anderen seine Karten ausgeben konnte und die Chips darauf nach seinen Vorstellungen programmieren konnte, steht auf dem Smartphone typisch nur ein einziger Chip zur Verfügung, welcher von den Issuern gemeinsam verwendet werden muss.

Daher ist grundsätzlich eine gewisse Kooperation zwischen den Issuern notwendig. Das grösste Problem ist aber, dass dieses Secure Element nicht unter der Kontrolle des Issuers befindet. Weil das Secure Element nur kryptografisch signierte Daten annimmt, kann nur jene Partei, welche das Secure Element zu Beginn eingerichtet (engl. *to provision*) hat (das heisst, den Master Key für dieses besitzt), Daten in diese laden.

[15] Over the Air.

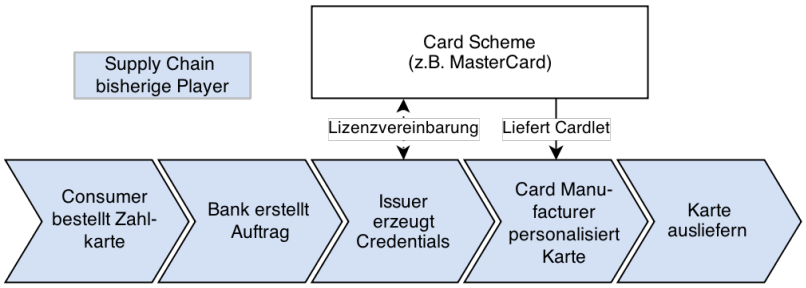

Abbildung 2: Bisherige Supply Chain von Bezahlkarten, bei der der Issuer komplette Kontrolle über das Secure Element auf der Karte hat.

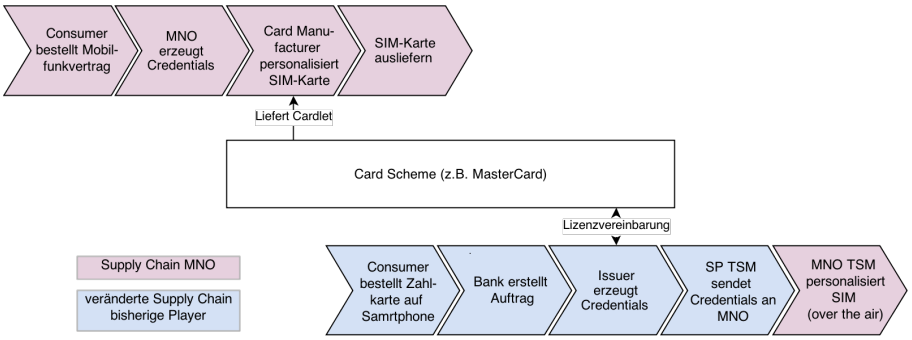

Abbildung 3: Supply Chain mit MNO als TSM. Hierbei verwaltet der MNO das Secure Element. Die bisherigen Player (insbesondere der Issuer) geben einen Teil der Kontrolle an den MNO ab.

Da als Secure Element, wie bereits erwähnt, entweder ein aufgelöteter Chip oder eine SIM-Karte infrage kommen, besitzt entweder der Gerätehersteller oder der Mobilfunkprovider (MNO) den Master Key. Das bedeutet nicht nur eine wesentliche Änderung im Distributionsprozess der Issuer, sondern – und das ist ungleich bedeutsamer – auch, dass ein weiterer Player am Business Case teilnimmt. Dies ist insofern von Belang, als dieser Akteur zusätzliche Gebühren von den Issuern verlangen kann. Dies schmälert dessen Marge, zumal der Consumer kaum bereit sein dürfte, für dieselbe Funktionalität, die ihm die Karte bietet, noch einmal zu bezahlten [8].

Die Issuer (welche häufig Banken oder Tochtergesellschaften dieser sind) suchen, weil ihnen die Gebühren der MNOs zu hoch erscheinen, nach Auswegen aus diesem Dilemma [9]. Diese Situation wird zusätzlich verschärft, da alle drei grossen *Card Schemes*[16] ein strategisches Interesse an dieser Technologie haben und daher Wert darauf legen, dass möglichst viele Kontaktlos-Bezahlkarten in den Umlauf gelangen. Sie erhoffen sich damit eine Aufwertung der Kreditkarte und damit einhergehend mehr Transaktionen und höhere Einnahmen.

1.2 Ziel der Arbeit

Wie aus der Ausganglage hervorgeht, beginnt sich ein Trend hin zu einem NFC-Ökosystem abzuzeichnen; bisher bietet aber noch kein Anbieter in der Schweiz Mobile Payment an. Da der Markt für Mobile Payment noch weitgehend unbewirtschaftet ist, muss davon ausgegangen werden, dass die Reihenfolge, in welchem die Anbieter Lösungen auf den Markt bringen, ein relevanter Faktor für die Aufteilung des Marktes sein wird.

Aus diesem Grund haben die aktuell am Zahlungsprozess beteiligten Unternehmen ein inhärentes Interesse, eine Lösung bereitzuhalten, sobald der Markt bereit ist. Ein zentraler Aspekt dieser Entwicklung ist der Card Emulation Mode, welcher auf den meisten Smartphones nur durch das Secure Element aktiviert werden kann. Bisherige Lösungsansätze verwenden dazu die SIM-Karte, was aber für die bisher im Bezahlkartenprozess involvierten Aktoren ein Verlust von Kontrolle bedeutet.

Ein erstes Ziel dieser Thesis ist, Faktoren zu identifizieren, welche bisher einen erfolgreichen Marktstart von Mobile Payment mit NFC in der Schweiz verhindert haben: Obwohl von den traditionellen Issuer noch keine Lösung auf den Markt gebracht wurde, existieren erstaunlicherweise auch keine Lösungen von Newcomers, welche den bisherigen Zahlungsprozess verändern. Neben den Kräften des Marktes werden auf der technischen Seite die Probleme umrissen, welche sich in diesem Zusammenhang stellen.

Ausgehend von dieser Situationsaufnahme, wird eine Architektur entwickelt, welche die bestehenden Probleme angeht. Der Fokus liegt dabei darauf, einen Lösungsansatz zu entwickeln, welcher es den Issuern ermöglicht, eine Mobile Payment Lösung auf den Markt zu bringen, bei welcher kein weiterer Player in den Zahlungsprozess involviert werden muss.

Dieses zweite Ziel ist direkt aus der Erkenntnis abgeleitet, dass ein weiterer Player die Einführung von Mobile Payment mit NFC verzögert (wegen Aufbau von Schnittstellen, welche zwischen dem neuen und den bisherigen Players nötig sind) oder gar verhindert wird (weil es zu keiner finanziellen Einigung kommt). So wird untersucht, ob es alternative Methoden gibt, welche es möglich machen, das Smartphone als Bezahlkarte zu verwenden, ohne dass ein weiterer Stakeholder in die Wertkette integriert werden muss. Diese Lösungen werden im Hinblick auf eine Realisierung in der Schweiz umrissen und diskutiert.

Dabei sollen sich Lösungen immer im Rahmen der EMV-Spezifikation bewegen. Es wird ein Sicherheitskonzept angestrebt, welches einen Angriff ähnlich schwierig macht, wie Massnahmen, welche dieselben Assets gegen andere Angriffsvektoren schützen (beispielsweise Angriffe auf das Bankkonto via Online-Bank).

[16] Als Card Schemes werden Unternehmen bezeichnet, welche Inhaber einer Marke von Bezahlkarten sind. Beispielsweise werde MasterCard oder Visa als Card Schemes bezeichnet.

Um eine tatsächlich realisierbare Lösung zu finden, werden die Interessen der Marktteilnehmer in der Schweiz bei der Lösungsfindung berücksichtigt.

Zum Nachweis der technischen Machbarkeit wird ein Showcase der vorgeschlagenen Architektur implementiert. Ebenfalls wird die Lösung kritisch diskutiert und ein Fazit gezogen.

2 Ansatz und Methodik

2.1 Vorgehen

Die Thesis besteht aus zwei Teilen: Der erste Teil umfasst eine Studie zur aktuellen Situation des Marktumfeldes von Mobile Payment in der Schweiz. Im zweiten Teil wurde eine Lösung für die gefundenen Probleme ausgearbeitet und die Architektur dokumentiert sowie ein Prototyp entwickelt, der die Lösung implementiert.

Der erste Teil leuchtet in einer empirischen Studie das Umfeld des Forschungsgegenstandes aus.

Dabei wurden die in den Zahlungsprozess involvierten Parteien (Rollen, vgl. Situationsanalyse) anhand von Literaturstudium der einschlägigen Spezifikationen der EMVCo identifiziert. Diese Informationen erwiesen sich aber als zu unspezifisch, um alleine darauf eine Aussage über den Schweizer Markt treffen zu können. Aus diesem Grund wurden Interviews durchgeführt. Diese Form der Wissensbeschaffung wurde gewählt, da sich die Technologie gerade erst im Markt zu etablieren beginnt und noch im Wandel befindet. Somit wäre in diesem Themengebiet geschriebenes Wissen nach dessen Publikation möglicherweise schon wieder veraltet. Weiter existieren auch keine aktuellen, wissenschaftlich verwertbaren Quellen zum Schweizer Markt, welche hätten hinzugezogen werden können.

Die Interviews wurden mit verschieden Vertretern der am Zahlungsverkehr beteiligten Unternehmen geführt. Dabei wurde versucht, deren strategischen Interessen am Markt zu klären und gleichzeitig die Richtung der technischen Entwicklung von Mobile Payment in der Schweiz zu identifizieren. Angewendet wurden ausschliesslich persönliche Interviews. Dies stellte sich als zweckmässigste Form heraus: Da die Interviews insbesondere der Wissensbeschaffung dienen sollten, schied eine schriftliche Befragung aus, da dabei nur ungenügend auf die Antworten der Interviewten hätte eingegangen werden können. Telefonische Interviews wurden nicht in Betracht gezogen, weil befürchtet werden musste, die Gespräche nicht in einer akzeptablen Qualität aufzeichnen zu können.

Bei den Interviewfragen wurden von einer offenen Fragestellung ausgegangen, um allgemeine Informationen des Interviewpartners zu erhalten. Während des Interviews wurde dann zunehmend auf bestimmte interessante Tatsachen mittels mehr und mehr geschlossenen Fragen eingegangen. Für alle Interviews wurde mit dem Gesprächspartner ein Zeitlimit von einer Stunde vereinbart, um die Ergiebigkeit zu erhöhen. Um mögliche Fehler in den Aussagen und inkorrekte Antworten entdecken zu können, sowie eine hohe Qualität und Verlässlichkeit der erarbeiteten Daten zu garantieren, wurden während des Gespräches Kontrollfragen gestellt. Ausserdem wurden bei der Auswertung die Antworten untereinander sowie mit denen anderer Interviewpartner abgeglichen. Bei der Vorgehensweise für die Interviews wurde überwiegend auf Techniken und Vorgehensweisen aus [10] abgestützt. Auf spezielle Techniken wie Angriffsfragen und Suggestivfragen wurde verzichtet.

Ergänzend zu den Interviews wurden branchenunabhängige Hintergrundinformationen in Gesprächen mit Mitarbeitern der Abrantix erarbeitet.

Im Hinblick auf den zweiten Teil, in dem eine eigene Lösung entwickelt wird, wurde die Technik der Empirie angewendet. Es werden darin zwei Ziele verfolgt. Einerseits wurde das vier Parteien Modell hinsichtlich

der daraus entstehenden Probleme auf dem Schweizer Markt untersucht. Die Resultate wurden deduktiv erarbeitet. Andererseits wurden verschiedene existierende Lösungen, welche für die EMV-Referenzmodelle entwickelt wurden und Mobile Payment implementieren, ausgewählt. Anhand dieser wurde mittels der induktiven Methode aufgezeigt, welche Bedürfnisse der Stakeholder diese Lösungen zu befriedigen vermögen und welche durch sie nicht gelöst werden können.

Da der EMV-Standard weltweit angewandt wird und insbesondere in (West-) Europa das dominierende Kartenzahlverfahren darstellt, ergeben sich in diversen anderen Ländern ähnliche Probleme mit der Umsetzung des vier Parteien Modells. Es wurde anhand von diversen Quellen (insbesondere Presseberichten: Es sind noch fast keine solchen Lösungen auf dem Markt verfügbar) untersucht, welche Lösungsansätze für das Problem des Secure Elements ausgearbeitet worden sind. Auch für diese Ansätze wurde mittels induktivem Vorgehen herausgearbeitet, ob und für welche Anforderungen der Marktteilnehmer diese eine Lösung bietet. Für diesen Teil der Arbeit konnte nur das induktive Vorgehen angewendet werden, da wie angedeutet nur sehr beschränkt Literatur zur Verfügung steht.

Auf eine Analyse, wo und unter welchen Bedingungen sich ein bestimmtes Business Modell erfolgreich etablieren liess, wurde verzichtet, da eine solche Untersuchung ausserhalb des Scopes dieser Thesis liegt.

Aufgrund der erarbeiteten Informationen wurde die Fragestellung für den zweiten Teil nach und nach entwickelt. Es wurden gefundene und selbst entwickelte Lösungsvarianten anhand verschiedener Kriterien miteinander verglichen und bewertet. Anhand dieser Resultate wurde eine Variante gewählt und implementiert.

Im zweiten Teil der Thesis wird als empirische Studie ein Prototyp entwickelt, welcher eine neue Lösung für den Umgang mit der Problematik aufzeigt. Dabei wurden verschiedene Lösungsansätze auf verschiedenen Plattformen untersucht. Insbesondere wurden die Smartphone-Betriebssysteme Android und Windows Phone untersucht. Aufgrund der fehlenden NFC-Fähigkeit wurde das iPhone nicht betrachtet.

Die Entwicklung des Prototyps folgte einer modifizierten SCRUM-Methode. Dabei wurde auf die Schätzungstechniken von SCRUM zurückgegriffen, um die einzelnen Funktionalitäten beziehungsweise Arbeitspakete zu bewerten. Weiter wurde die Sprint Methodologie aus SCRUM adaptiert, wobei die Milestones die einzelnen Sprints begrenzen.

Schliesslich wurde die entwickelte Lösung kritisch betrachtet und in Anbetracht der verschiedenen Rahmenbedingungen bewertet. Für diesen Ansatz wurde ebenfalls die induktive Methode angewendet.

2.2 Fokus und Unabhängigkeit

Die Studie wird in Zusammenarbeit mit der Abrantix AG[17] in Zürich durchgeführt. Die Abrantix ist im Bereich der terminalbasierten Zahlungsabwicklung tätig und programmiert im Auftrag von Acquirern Terminal-Software.

Von der Abrantix AG wurde eine Untersuchung gewünscht, welche beleuchtet, welche Rolle das Secure Element bei Mobile Payment Lösungen spielt und ob dieses für EMV-Konformität zwingend notwendig ist. Sollte das SE nicht notwendig sein, sollte eine technische Möglichkeit gesucht werden, auf diese zu verzichten; anderenfalls Alternativen zur Verwendung der SIM-Karte (welche einen weiteren Stakeholder involviert) betrachtet werden. Aufgrund dieser Anforderungen orientiert sich diese am Blickwinkel der bestehenden Stakeholder.

Im weiteren ist die Studie unabhängig von Interessen der Abrantix AG und die entwickelte Lösung universell einsetzbar.

[17] Siehe http://www.abrantix.com.

3 Situationsanalyse

3.1 Kartengeschäft

Aus der Anforderung, dass Debit- und Kreditkarten weltweit akzeptiert werden müssen, ergibt sich, dass eine gewisse Struktur bei den in den Zahlungs- und Abrechnungsprozess involvierten Parteien existieren muss. Diese Struktur ist historisch gewachsen und wurde nachträglich von diversen Gremien (unter anderem den Card Schemes, aber auch anderen, wie beispielsweise [11, pp.14–16]) standardisiert. Aufgrund der historischen Entwicklung werden die im folgenden genannten Rollen und Bezeichnungen auch nicht einheitlich verwendet. Daher dient dieses Kapitel auch der Definition einiger Begriffe für diese Thesis.

Neben der reinen begrifflichen Abgrenzung dienen diese Definitionen auch der Abgrenzung des Business Cases und um einen Überblick über die involvierten Stakeholder zu geben. Die Standardisierungen sind dabei rein normativ und haben im Allgemeinen keine rechtliche Wirkung, weshalb in der Praxis auch gewisse Abweichungen vorkommen. Sie gelten im Kartengeschäft allerdings als Basis für die Verständigung und das Verständnis.

Weil insbesondere die Card Schemes (MasterCard, Visa, etc.) diese Modelle oft gebrauchen, fehlen die Card Schemes in de meisten Darstellungen daher vollständig. Da diese Thesis eine übergeordnete Perspektive einnimmt und sich nicht auf ein bestimmtes Card Scheme abstützt, wurden die bestehenden Modelle um das Card Scheme als Entität ergänzt.

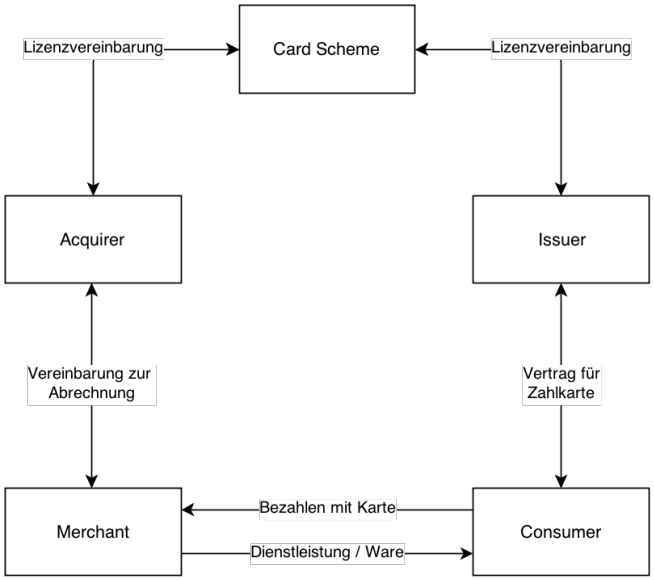

Abbildung 4: Übersicht der Rollen im angestammten Kartengeschäft (Vier Parteien Modell), Angelehnt an [12, p.37]

Grundsätzlich muss zwischen zwei unterschiedlichen Modellen unterschieden werden: dem drei Parteien Modell und dem vier Parteien Modell. Das drei Parteien Modell besteht aus dem Consumer, dem Merchant und dem Issuer. Der Issuer übernimmt dabei die Ausgabe der Karte und verarbeitet gleichzeitig die Zahlungen (Acquirer). Das drei Parteien Modell verliert immer mehr an Bedeutung, da es gewisse Nachteile aufweist [13]:

- Nicht alle Consumer können die Karten in allen Ländern verwenden.
- Merchants haben nur eine begrenzte Auswahl, weil für einen Issuer nur ein nationaler Acquirer oder Verkäufer von Terminals existiert.
- Erhöhte Markteintrittsbarriere, weil nur ein nationaler Acquirer existiert und dieser nicht im Wettbewerb mit anderen steht.
- Begrenzter Wettbewerb (weil der Merchant den Acquirer nicht frei wählen kann).

Aus diesen Gründen forcieren die Card Schemes das vier Parteien Modell. Dabei wird die Rolle des Issuers in zwei dedizierte Rollen aufgeteilt: Der Issuer selbst übernimmt die Ausgabe der Karte, während der Acquirer den Betrieb des Zahlungs-Netzwerks verantwortet. Einer der Vorteile dieses Modells ist, dass mehrere Acquirers in einem Land existieren können und unter diesen ein Wettbewerb entsteht.

Bei diesem Modell werden die Banken selbst nicht erwähnt. Typischerweise stehen aber die Banken hinter den Issuern.

Relevant für die Betrachtung ist ebenfalls der Zahlungsfluss, weil die Parteien hauptsächlich durch die einzelnen Transaktionen ihren Umsatz erzielen. Daher ist diese Eigenheit bei der Betrachtung von neu ins Spiel kommenden Players relevant. Diese “Spielregeln” werden durch das Card Scheme festgelegt.

Bezahlt ein Consumer bargeldlos, so schuldet der Merchant eine Kommission (welche einen bestimmten Prozentsatz des Kaufpreises ausmacht) an den Acquirer. Von dieser Kommission muss der Acquirer einen Teil an den Issuer abgeben, die *Interchangegebühr*. Auch diese Interchangegebühr ist ein prozentualer Anteil des Transaktionsbetrages, typischerweise etwa ein Prozent in der Schweiz [14].

Sowohl Acquirer und Issuer nehmen die Dienstleistungen des Card Schemes in Anspruch und haben einen Lizenzvertrag mit diesem. Dafür schulden sie dem Card Scheme die Lizenzgebühr.

Schliesslich bezahlt der Consumer dem Issuer die Kartengebühr, welche typischerweise jährlich erhoben wird. Im Falle von Gratis-Kreditkarten verzichtet der Issuer, vom Consumer eine Kartengebühr zu verlangen und finanziert sich ausschliesslich über die Interchangegebühren.

3.1.1 Acquirer

Der Acquirer (engl. für Händlerbank) ist der Betreiber eines Payment-Netzwerks. Er sorgt dafür, dass ein Bezahlterminal Bezahlkarten autorisieren, deren Bezugslimite prüfen und eine Zahlung auslösen kann.

Alle ausgelösten Aktionen wie PIN-Validierung, Prüfen der Bezugslimite oder Zahlung werden dabei dem Issuer der Bezahlkarte weitergeleitet und müssen von diesem verarbeitet und bestätigt werden. Einzig bei der sogenannten Offline-Verifikation wird vor Ort, ohne Verbindung zum Issuer eine Authentifizierung durchgeführt.

Damit Zahlungen über das Netzwerk des Acquirers durchgeführt werden können, muss der Acquirer dasselbe Card Scheme unterstützen, wie der Issuer, welcher die Karte ausgestellt hat.

Die Dienstleistungen des Acquirer können auch vom Issuer übernommen werden. In diesem Fall spricht man von einem drei Parteien Modell [13].

Die Schweizer Acquirer Die beiden wichtigsten Acquirer in der Schweiz sind die SIX Multipay und die Aduno. Daneben existieren einige weitere, aber weniger bedeutende, Acquirer.

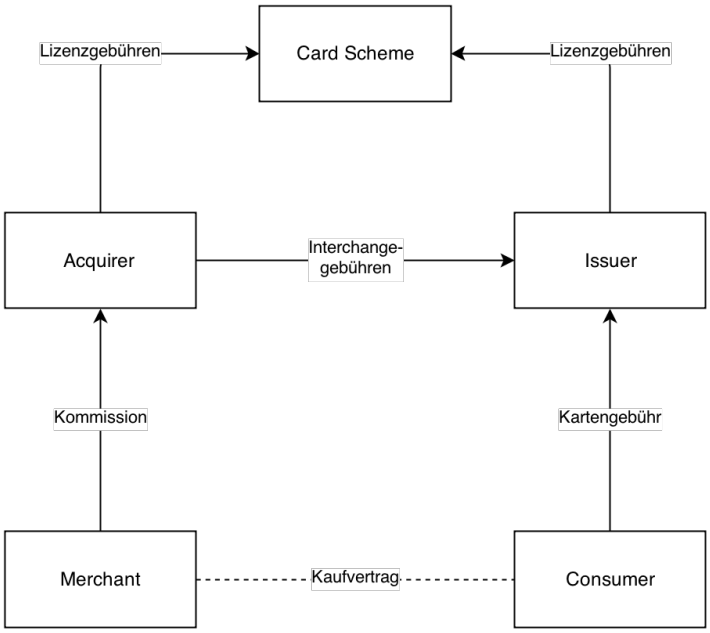

Abbildung 5: Übersicht der Zahlungsströme im angestammten Kartengeschäft (Vier Parteien Modell)

3.1.2 Issuer

Der Issuer (engl. für "Herausgeber"; manchmal auch *Card Issuer*, engl. für "Kartenherausgeber") ist der Herausgeber der Bezahlkarte. Er ist dafür verantwortlich, dass die Karte die richtige Information auf sich trägt und der richtigen Person ausgestellt wird. Er haftet gegenüber dem Merchant für die Auszahlung des Geldes (allerdings kann der Issuer in gewissen Fällen das Risiko auf den Merchant überwälzen). Dies ist insbesondere bei der Kreditkarte relevant, als der Issuer dabei das Risiko des Deckungsausfalles auf sich nehmen muss.

Weiter führt der Issuer auch die Rechnung für den Consumer, also dessen Kundenkonto[18]. Technisch gesehen wird dabei ein Matching zwischen Kartennummer und der Kontonummer durchgeführt. Wichtig ist dieser Aspekt im Zusammenhang mit *Wallets*, da dadurch auch mehrere Karten auf ein Konto verrechnet werden können. Ebenso ist damit *Tokenisation* möglich: Dabei wird für die Zahlung nicht jedes Mal dieselbe Kartennummer verwendet, sondern nach einem bestimmten Muster regelmässig eine neue, "virtuelle" Nummer verwendet. Beispielsweise kann für Zahlungen im Internet für jede Transaktion eine neue Nummer generiert werden. Weil der Issuer für jede Nummer nur genau eine Transaktion akzeptiert, ist die Nummer für Dritte wertlos, auch wenn diese abgegriffen wurde.

Issuer können selbstständige und unabhängige Unternehmen sein oder auch direkt oder indirekt einem Finanzinstitut angegliedert sein.

Die Schweizer Issuer Die drei grössten Issuer in der Schweiz sind das UBS CardCenter, Viseca und Swisscard. Das UBS CardCenter vertreibt die Karten für die UBS und die PostFinance, Viseca hauptsächlich für Raiffeisen und die Kantonalbanken und Swisscard für die Credit Suisse. Dementsprechend sind auch die Besitzverhältnisse dieser Issuer; die Schweizer Issuer werden also primär durch die Banken kontrolliert.

[18] Dabei ist beispielsweise ein Kreditkartenkonto und nicht etwa ein Bankkonto gemeint.

Erwähnenswert ist auch, dass Swisscard der einzige Schweizer Issuer mit einer Lizenz für American Express Karten ist.

3.1.3 Consumer

Der Consumer (engl. für Verbraucher) ist der Endbenutzer des ganzen Systems. Er besitzt die Karte oder das Mobiltelefon, womit bei einem Merchant bezahlt wird. Dazu hat der Consumer Verträge mit mehreren anderen Stakeholdern:

- Er hat einen Vertrag mit einem Finanzinstitut. Dieses gewährt ihm die Möglichkeit, eine Bezahlkarte zu beantragen[19].
- Er hat einen Vertrag mit einem Issuer. Dieser stellt ihm eine (eventuell virtuelle) Bezahlkarte aus, bei der Zahlungen über sein Finanzinstitut verbucht werden.
- Er hat einen Kauf- oder Dienstleistungsvertrag mit einem Merchant, welchen er mit seiner Bezahlkarte entschädigen will.

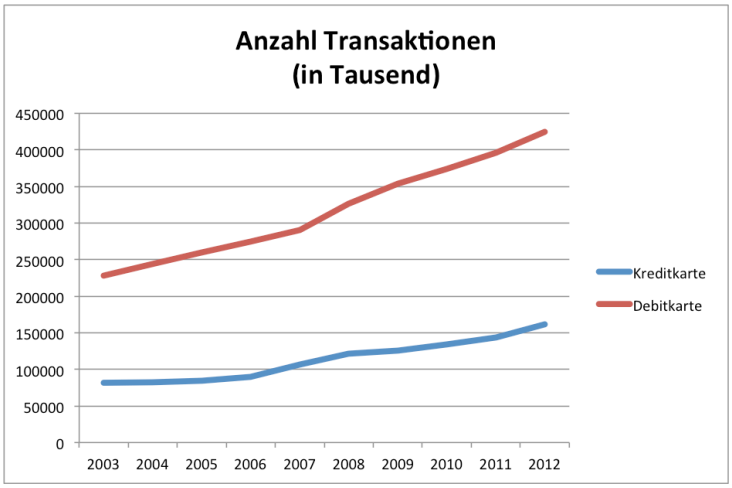

Abbildung 6: Gemäss den Zahlen aus [15, pp.34–37] ist die Schweiz in puncto *Anzahl der Transaktionen* ein Land, dass bevorzugt mit Debitkarten bezahlt.

Der Schweizer Consumer Die Schweiz ist gemäss [15] ein Debit-Markt; das heisst, der Schweizer Consumer bezahlt häufiger mit einer Debit-Karte (beispielsweise *Maestro*), als mit einer Kredit-Karte. Zwar sind die Beträge einer einzelnen Kreditkartentransaktion im Durchschnitt deutlich höher (Fr. 142) als diejenigen einer Debitkarte (Fr. 75), allerdings ist das Transaktionsvolumen von Debitkarten um den Faktor 2.5 grösser als dasjenige von Kreditkarten (Zahlen aus 2012) [15, p.36]. Allerdings zeigt sich als allgemeiner Trend, dass die Kreditkarten in den vergangenen Jahren vermehrt auch für kleinere Beträge eingesetzt wurden.

Weiter hat der Schweizer Consumer eine ausgezeichnete Zahlungsmoral. Gemäss einer im Jahr 2008 von Comparis durchgeführten Studie ist “Schulden machen verpönt” und die meisten Schweizer bezahlen ihre

[19] Nebst Karten, die von Finanzinstituten direkt ausgegeben werden, gibt es auch zahlreiche Karten, die von Drittparteien ausgegeben werden. Hinter all diesen Karten steht aber am Ende wieder ein Finanzinstitut; die Geschäftsbeziehung ist lediglich nicht ganz so offensichtlich.

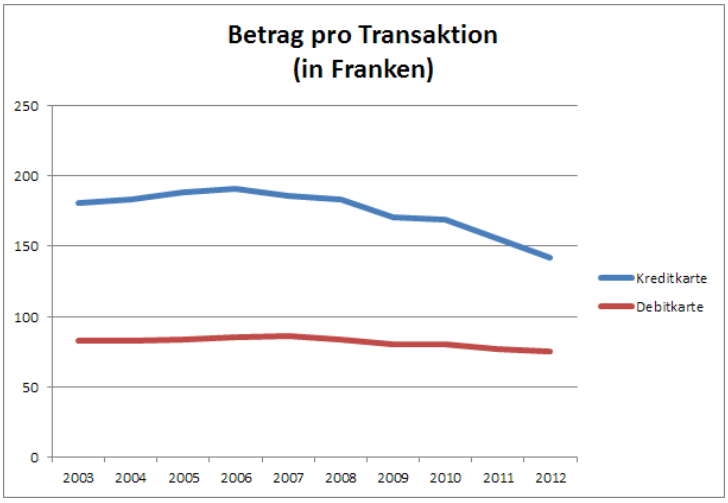

Abbildung 7: Durchschnittlicher Betrag einer Zahlung mit Debit- und Kreditkarte. Es zeigt sich speziell bei Kreditkarten ein Trend zu niedrigeren Beträgen pro Transaktion.

Kreditkarten-Rechnungen pünktlich [16]. So nutzen gemäss der Studie nur etwa 12% der Kunden von zwölf befragten Kreditkartenanbietern die Möglichkeit von Teilzahlung ihrer Rechnung. Dadurch entgehen den Kreditkarten-Unternehmen Zinsen auf ausstehende Beträge.

3.1.4 Merchant

Der Merchant (engl. für Händler) ist der Verkäufer, welcher dem Consumer Waren oder Dienstleistungen verkauft. Damit dem Consumer die Bezahlung mittels Bezahlkarte angeboten werden kann, benötigt der Merchant ein EFT/POS-Terminal. Das Bezahlen per Bezahlkarte ist dabei ein Service des Merchant für den Consumer. Der Merchant verdient normalerweise nichts an einer Kartenzahlung und muss sogar häufig eine kleine Transaktionsgebühr im Bereich von einigen Rappen (bei Debitkarten-Zahlungen) oder wenigen Prozenten (bei Kreditkarten-Zahlungen) bezahlen.

Entweder kauft der Merchant das Terminal und ist damit Eigentümer desselben oder er erhält es kostenlos oder gegen eine Gebühr zur Verfügung gestellt. In einigen Ländern können solche Terminals allerdings nur die Karten eines bestimmten Anbieters akzeptieren. Das führt zur Situation, dass ein Merchant mehrere Terminals benötigt, um Zahlungen von Kunden verschiedener Finanzinstituten annehmen zu können.

Unabhängig von den Besitzmodalitäten muss der Merchant das Bezahlsystem (das Netzwerk) eines Acquirers verwenden, um die Zahlung abzuwickeln zu können.

Die Schweizer Merchants Die Schweiz ist eines derjenigen Länder, in denen ein Merchant das Terminal selbst kauft. Und dank des nationalen Standards EP2 können alle in der Schweiz vertriebenen Terminals mit allen Acquirern betrieben werden. Die Merchants sind dabei bereit, ein modernes und technisch hochwertiges Gerät zu kaufen [17].

Land	Anzahl POS-Terminals pro 1 Mio. Einwohner
Schweiz	19'357
Österreich	12'754
Deutschland	8'693
Frankreich	22'884
Italien	20'692
Niederlande	16'752
Finnland	37'681
Euroraum	19'390

Tabelle 1: Internationaler Vergleich von EFT/POS-Terminaldichten. Zahlen aus 2011, für die Schweiz berechnet aus [18] und [19, p.362], Frankreich aus [20] und [21], Italien aus [20] und [22], andere aus [23, p.59]

Auch liegt die Anzahl der Akzeptanzstellen in der Schweiz etwa im europäischen Durchschnitt. Die direkten Nachbarländer der Schweiz weisen deutlich unterschiedliche Dichten von POS-Terminals auf: Während die Dichte in Italien und Frankreich höher ist, liegt sie in Österreich und besonders Deutschland deutlich niedriger.

3.1.5 Weitere Aktoren

Nebst den Aktoren des vier Parteien Modells existieren noch weitere, welche nicht direkt an der Wertschöpfungskette beteiligt sind.

Card Scheme Ein Card Scheme ist der Lizenzgeber eines Kartensystems und unterhält und definiert das Netzwerk, an welchem alle Issuer und Acquirer angeschlossen sind. Die Wichtigsten im westlichen Raum sind *MasterCard* und *Visa*, sowie *China UnionPay* und das *Japan Credit Bureau* (JCB) im asiatischen Raum.

Card Schemes definieren für ihr Produkt (typischerweise ein Markenname für eine Karte) eigene Regeln, welche über den Rahmen der EMV hinausgehen. Beispielsweise schreiben sie Zertifikatketten, Verschlüsselungs- und Signaturalgorithmen vor, die von den Issuern in den Karten und von den Acquirern in den Terminals und im Backend umgesetzt werden müssen.

Weiter stellen Card Schemes das Netzwerk für die Abrechnung zur Verfügung und ermöglichen damit, dass jede der am Netz teilnehmenden Parteien (Issuer oder Acquirer) mit jeder anderen abrechnen kann. Es wird festgelet, wie ein Acquirer erkennen kann, an welchen Issuer er seine Forderung stellen muss und wie diese genau übermittelt wird. Ebenso werden Abläufe festgelegt, für den Fall, dass der Consumer einer Transaktion widerspricht; wie eine Gutschrift (zum Beispiel aufgrund einer Storno-Buchung) verarbeitet wird, etc. Sowohl der Zahlungsfluss wie auch die Details der Regeln der Card Schemes werden aber im Rahmen dieser Arbeit nicht weiter betrachtet. Dies zugunsten einer direkt auf EMV aufbauenden allgemeingültigen Betrachtungsweise.

Card Schemes in der Schweiz In der Schweiz sind die wichtigsten Card Schemes MasterCard, Visa und American Express. Daneben ist auch noch Diners Club aktiv. Diners Club beschränkt sich in der Schweiz aber auf Kunden mit sehr hohem Transaktionsvolumen.

MasterCard betreibt in der Schweiz zusätzlich noch das Maestro Card Scheme, über das alle Schweizer Debit-Zahlungen abgewickelt werden.

Vermehrt werden, vor allem in touristischen Destinationen, auch China UnionPay und JCB sowie Visa VPAY angenommen. Die asiatischen Consumer weisen meist ein wesentlich höherer Betrag pro Transaktion auf als beispielsweise Schweizer Kunden.

Card Manufacturer Card Manufacturer sind die Produzenten der Chipkarte und fertigen diese gemäss dem Auftrag des Issuers an. Während der Produktion werden die Karten nach Wunsch des Issuers bedruckt, gegebenenfalls geprägt und die Informationen auf den Magnetstreifen und den Chip aufgebracht.

Neben den Bezahlkarten werden auch die SIM-Karten für die MNOs durch die Card Manufacturer hergestellt.

In beiden Fällen reicht die Kette von kryptografischen Schlüsseln, mit welcher neue Daten, die auf den Chip gespeichert werden sollen, signiert werden müssen, bis zum Card Manufacturer.

Card Manufacturer in der Schweiz In der Schweiz sind hauptsächlich Oberthur und Trüb aktiv. Beide fertigen Karten und personalisieren diese, beide haben auch ein eigenes *Card OS* im Angebot.

3.1.6 Prozesse und Bestimmungen

Der elektronische Zahlungsverkehr ist sehr stark reguliert, damit sichergestellt werden kann, dass alle Karten der Welt überall auf der Welt funktionieren.

Dafür hat sich der EMV Standard durchgesetzt. Er baut selbst auf vielen anderen Standards von verschiedenen Gremien auf, darunter ISO und ECMA.

Hauptsächlich verweist EMV auf die Standards ISO 7816, *Integrated Circuit Card*, und ISO 14443, *Proximity cards*. In Ersterem wird das Kommunikationsprotokoll (APDU) zwischen Lesegerät und Chipkarte definiert. Dieselben Kommandos werden auch für Contactless Cards verwendet. ISO 14443 definiert das Low-Level Kommunikationsprotokoll, also den Physical Layer für die Kommunikation.

Details zu den Normen und dem Kommunikationsstack finden sich im Appendix II.

EMV Das *Handbuch der Chipkarten* [24] beschreibt EMV folgendermassen:

> "Die EMV Spezifikation ist eine gemeinsame Spezifikation für Zahlungsverkehrskarten mit Chip sowie dazugehörige Terminals, die ursprünglich von den Firmen Europay, Master Card, Visa und American Express erstellt wurde. Diese Spezifikationen sind zum weltweiten Industriestandard für Kreditkarten, Debitkarten und Börsenkarten (elektronische Geldbörse) avanciert."

EMV legt die Rahmenbedingungen für elektronische Zahlungen per Chip-Karte fest. In vier Teilen, *Bücher* genannt, macht EMV Vorgaben für die physikalische und logische Schicht. Weiter definiert es die minimalen Anforderungen bezüglich Sicherheit.

Die EMV-Spezifikation bildet damit das Grundgerüst für eine herstellerunabhängige Interoperabilität von Geräten (Terminals und Chipkarten). Sie umfasst Regeln über die Betriebsspannung genau so wie Details über die vorzuhaltenden Daten und den Transaktionsablauf einer Zahlung.

Für die Betrachtungsweise ist besonders das *Book 2 – Security and Key Management* relevant. Darin werden die verschiedenen Methoden zur Authentifizierung des Benutzers beschrieben, sowie der Aufbau der Zertifikatketten. Wichtig in Bezug auf Sicherheit ist anzumerken, dass EMV keine Hinweise liefert, *wie* die Schlüssel gespeichert werden sollen. Ebenso ist nicht spezifiziert, wie die Schlüssel verteilt werden. Dies rührt daher, da die EMV zum Zweck hat, die Interoperabilität herzustellen und keine *Best Practices* liefert.

Über EMV hinausgehend haben die Card Schemes eigene und vor allem detaillierter ausgearbeitete Spezifikationen verfasst, die meist deutlich restriktiver sind.

3.1.7 EMV Contactless

EMV Contactless spezifiziert Erweiterungen zu EMV, die es erlauben, Contactless Smartcards zur Zahlung an EFT/POS-Terminals einzusetzen. Der Consumer muss die Karte also nicht mehr in ein Terminal-Gerät einführen. Es reicht, die Karte an eine Sensorfläche zu halten.

Eine Erweiterung der Spezifikation ist daher notwendig, weil unter anderem das Interface völlig anders aufgebaut ist als im kontaktbehafteten Fall. Auf den höheren Schichten ist die Kommunikation allerdings wieder gleich aufgebaut (mittels APDUs gemäss ISO 7816).

Die Spezifikation sieht dabei eine unterschiedliche Behandlung von Transaktionen abhängig von deren Betrag vor. Dabei werden die Transaktionen in *Low Value Transactions* und *High Value Transactions* unterteilt. Relevant ist diese Unterscheidung im Hinblick auf die nötige Authentifizierung des Kunden: Während der Kunde bei High Value Transactions an einem Zahlungsterminal seine PIN eingeben muss, ist dies bei Low Value Transactions nicht nötig.

Der Zweck dieser Unterscheidung ist die Reduktion der für den Zahlvorgang benötigten Zeit. Bei kleineren Beträgen (beispielsweise an der Kasse eines Kiosks) würde die Transaktion durch die Eingabe eines PINs stark verzögert, was die Anzahl bedienter Consumer pro Zeiteinheit mindert. Ausserdem gibt es viele Geräte, bei denen ein PIN-Eingabegerät nicht sinnvoll platziert werden könnte, wie beispielsweise Snack-Automaten oder Parkuhren. Da auf das Pinpad verzichtet werden kann, können Zahlterminals auch kostengünstiger hergestellt werden. Die Geräte fallen damit auch kleiner aus und sie werden zudem resistenter gegenüber Vandalismus.

Da kleine Beträge oft an unbeaufsichtigten Terminals bezahlt werden, kann durch das Weglassen des Pinpads auch ein Ausspionieren des PINs verhindert werden (Skimming). Allerdings muss angemerkt werden, dass beim Skimming neben dem Abgreifen des PINs normalerweise der Magnetstreifen kopiert wird. Bei EMV-Transaktionen kann das kryptografische Material nicht aus dem Chip ausgelesen werden, weshalb die Karte nicht dupliziert werden kann[20]. Ein Aufzeichnen und späteres Abspielen der Daten (*Replay Attack*) verhindert EMV durch spezielle Mechanismen ebenfalls. Da ein Einzugsschlitz fehlt, ist auch das Vortäuschen einer eingezogenen Karte und spätere Verwenden dieser an einem anderen Terminal oder Geldautomat, zusammen mit einem aufgezeichneten PIN, nicht möglich.

[20] Andererseits erlaubt EMV Contactless auch einen Kompatibilitätsmodus, bei welchem anstelle von EMV Transaktionen herkömmliche Magnetstreifen-Informationen übertragen werden. Diesem Risiko sind sich die Issuer aber bewusst [8]. So werde gegenwärtig darüber nachgedacht, diesen Kompatibilitätsmodus nur auf Wunsch des Consumers zu aktivieren (beispielsweise wenn dieser eine Reise in ein Land plant, in welchem Magstripe noch immer ein verbreitetes Verfahren darstellt).

EP2 Seit 1998 entwickelten die wichtigsten Stakeholder im Zahlungssystem der Schweiz einem gemeinsamen Standard für die Datenkommunikation im Bereich von Terminals. Dieser Standard, welchem sich die Stakeholder 2003 unterwarfen, wurde EP2[21] genannt. Seit dem Jahr 2007 führt der Verein *Technical Cooperation ep2* die Weiterentwicklung voran. Im Verein sind wiederum alle wichtigen Stakeholder des Schweizer Kartengeschäfts vertreten.

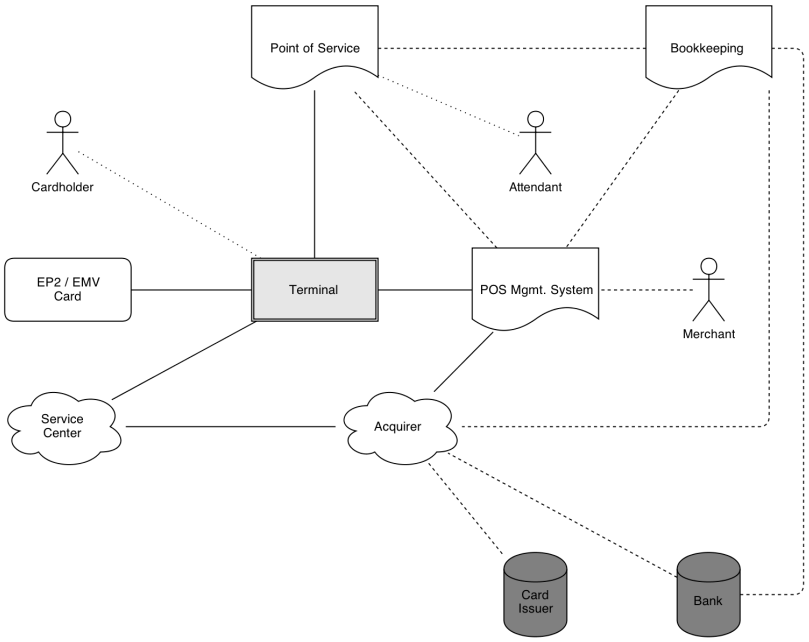

Abbildung 8: Das Diagramm zeigt die Ausdehnung des EP2 Standards. Gut zu erkennen ist, dass sich der Standard rund ums Terminal dreht. Die durchgezogenen Verbindungen werden in EP2 detailliert geregelt; die gestrichelten sind nicht Teil von EP2. Die gepunkteten Linien stellen Anforderungen ans Userinterface dar [25, pp.1–15].

Im Gegensatz zu EMV ist EP2 viel detaillierter ausgearbeitet und stellt das Zahlungsterminal in den Mittelpunkt. So regelt EP2 die Kommunikation zwischen Terminal und EFT/POS-Gerät, aber auch zwischen Terminal und Acquirer, das Userinterface für das Personal und die minimalen technischen Anforderungen an ein Terminal.

EP2 verweist wo möglich auf externe Regulierungen oder greift solche auf und ergänzt diese um genauere Bestimmungen. So verdeutlicht EP2 Bestimmungen aus EMV, die in diesem Detaillierungsgrad auch in den Bestimmungen der Card Schemes zu finden wären.

Prozess zum Ausstellen einer Bezahlkarte Der Prozess zur Ausstellung einer Bezahlkarte beginnt mit dem Antrag des Consumers für eine solche beim Issuer. Dieser prüft anschliessend den Antrag. Beispielsweise findet bei Anträgen für Kreditkarten die obligatorische Kreditwürdigkeits-Prüfung gemäss *Bundesgesetz über den Konsumkredit (kurz Konsumkreditgesetz, KKG)* statt.

Wird dem Antrag stattgegeben, werden beim Issuer die nötigen Personalisierungsinformationen erzeugt. Diese werden über vom entsprechendem Card Scheme zertifizierte Kanäle an einen Card Manufacturer übermittelt.

[21] Ursprünglich lautete die Bezeichnung *eftpos2000*, daher die Abkürzung.

Der Card Manufacturer stellt anschliessend die Karte gemäss den Spezifikationen des Issuers her. Diese Spezifikationen umfassen normalerweise den Karten- und Chip-Typ, die Daten (inklusive initialer PIN) für Chip und gegebenenfalls Magnetstreifen, die Hochprägung sowie das zu druckende Motiv der Karte. Der Card Manufacturer versendet die Karte anschliessend direkt an den Consumer. Häufig erstellt der Card Manufacturer auch gleich den Brief zum sicheren PIN-Versand und sendet diesen ebenfalls dem Consumer.

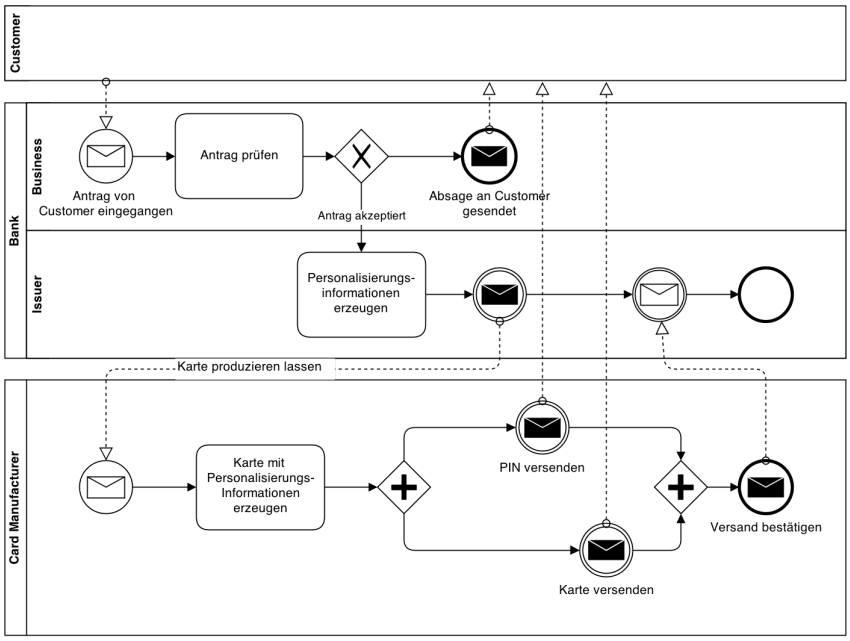

Abbildung 9: Prozess zur Ausstellung einer Bezahlkarte

NFC NFC dient im Falle von EMV Contactless lediglich als *enabling Technology* und stellt selbst keinen Teil der EMV dar. Dabei findet die Kommunikation im Fall von Contactless Smartcards gemäss ISO 14443 statt. NFC verwendet diesen Standard als Basis und bietet die Möglichkeit, auf höhere Protokolllayer zu verzichten (*Card Emulation Mode*).

Es wird an dieser Stelle nicht weiter auf die Funktionsweise von NFC eingegangen; wo diese zur Dokumentation der Lösung relevant ist, wird direkt im entsprechenden Kapitel auf die Details eingegangen. Ein allgemeiner Überblick über NFC findet sich unter Appendix II.

3.2 Mobile Payment Geschäft

Bei Mobile Payment bezahlt der Consumer statt mit einer Karte mit seinem Smartphone, welches anstelle der Karte über die entsprechenden Informationen verfügt.

Zur technischen Realisierung wird auf EMV Contactless zurückgegriffen. Dies bedeutet, dass der in Smartphones eingebaute NFC-Chip in den *Card Emulation Mode* versetzt wird und dem Terminal damit eine Contactless Smartcard vorgaukelt. Mit diesem Ansatz sind aufseiten des Terminals keinerlei Änderungen nötig. Wie im Kapitel Problemdomäne weiter ausgeführt wird, bedingt dieser Ansatz, dass mindestens ein weiterer Stakeholder in das Business Model einsteigt.

Abbildung 10: Das Bild veranschaulicht den Zahlvorgang mit einem Smartphone an einem Terminal. Im Bild das Smartphone *Nokia Lumia 820* sowie ein EFT/POS-Terminal des Typs *Yomani* des französischen Herstellers *Atos Worldline*, welcher zum Informatik-Konzern *Atos* gehört.

Weil sich das Smartphone wie eine Contactless Smartcard verhält, ist das Mobile Payment Geschäft dem Kartengeschäft sehr ähnlich.

3.2.1 Das bilaterale Modell

Erste Versuche mit Mobile Payment fanden während des Internet Booms Ende der 1990er Jahren statt. Die damals eingesetzten Modelle werden als *unilateral* bezeichnet, da sie von einer Partei beherrscht wurden oder die Wertschöpfung der Kerngeschäftsfelder von einer einzigen Partei erbracht wurde. Typische Beispiele für unilaterale Modelle sind Bezahlsysteme, bei denen der Consumer die eingekauften Waren über die Telefonrechnung bezahlt.

Kennzeichnend für die unilateralen Modelle sind, dass für den betreibenden Partner ein einseiger Vorteil entsteht. Die in den 1990er entwickelten unilateralen Modelle konnten sich in dieser Zeit nicht durchsetzen. Daher entstand die Idee, die Vorteile beziehungsweise die Wertschöpfung auf die involvierten Unternehmen zu verteilen. Beim bilateralen Modell kooperieren die Partner (typischerweise eine Bank und ein MNO) um eine bessere Marktposition zu erreichen und um Vorteile für Consumer und Merchant zu schaffen, welche mit unilateralen Modellen nicht möglich wären [26].

Die GSMA schlägt ein solches bilaterales Modell vor; ebenso sind alle bisherigen EMV-kompatiblen Lösungen als bilaterales Modell ausgelegt. Eines der Ziele dieser Thesis ist, ein unilaterales Modell zu entwickeln, in dessen Zentrum die Bank steht.

Wichtig zu bemerken ist, dass die Bezeichnung *bilaterales Modell* nichts über die zu verwendende Technologie aussagt.

3.2.2 Anforderungen an ein Marktmodell

Der Mobile Payment Markt ist ein Markt, der sich noch in der Entwicklung befindet. Daher ist es schwierig, Aussagen darüber zu machen, welche Modelle erfolgreich sein können und welche nicht. Auch internatio-

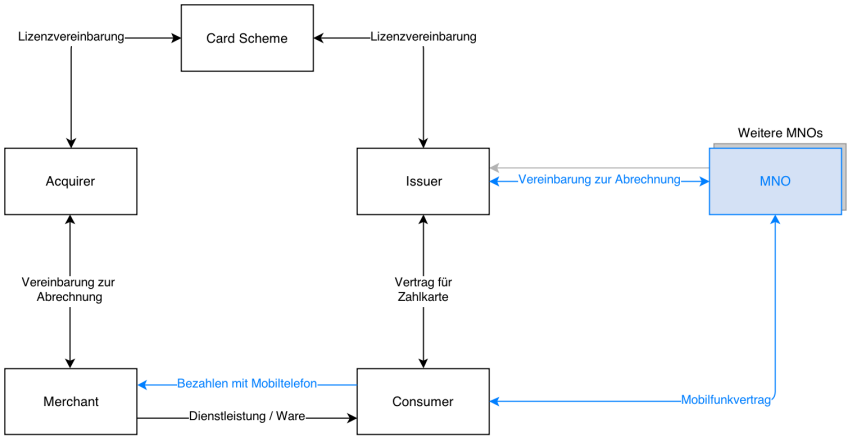

Abbildung 11: Übersicht der Rollen beim Mobile Payment

nale Vergleiche sind heikel, da sich die europäischen Märkte deutlich von beispielsweise dem oft zitierten Beispiel Japan unterscheiden.

Dennoch hat [27] Faktoren zusammengetragen, welche für ein erfolgreiches Geschäftsmodell kennzeichnend sind.

Marktseitige Anforderungen	Kundenseitige Anforderungen
Kritische Masse	Leichter Einstieg
Verteilung der Marktmacht	Einfache Benutzung
Investitionen	Geringe technische Voraussetzung
Kunden-/Händlerkontakte	Flexible Nutzung
Standards	Kompatibilität
Kosteneffizienz	Mehrwert
Reputation/Brand	Zahlungssicherheit

Tabelle 2: Anforderungen an ein erfolgreiches Mobile Payment-Modell (nach [27], mit Anpassungen)

3.2.3 Consumer

Im Vergleich zum Kartengeschäft hat der Consumer nun zusätzliche Geschäftsbeziehungen:

- Er hat ein Gerät von einem Mobile Device Manufacturer mit NFC-Funktionalität, welches eventuell durch einen MNO mitfinanziert wird.
- Er hat einen Nutzungsvertrag mit einem MNO, um dessen Mobilfunk-Dienstleistungen benutzen zu dürfen. Um sein Mobiltelefon gegenüber dem MNO auszuweisen, erhält er eine SIM-Karte.

Verbreitung von Mobiltelefonen in der Schweiz Speziell in der Schweiz ist die Verbreitung von Apples *iPhone* [28] relativ hoch. Apple ist wohl noch der einzige grosse Smartphone-Hersteller, der bisher keines seiner Geräte mit NFC-Funktionalität ausgerüstet hat. NFC ist jedoch Voraussetzung für Mobile Payment an einem Terminal.

Wie [6, pp.23–24] hervorhebt, ist bezüglich des Marktanteils in den kommenden Jahren ein gewisser Ausgleich zu erwarten. Dieser dürfte die Marktlage zugunsten von Android ändern, da Android im Gegensatz zum Betriebssystem des iPhones, *iOS* genannt, von diversen Herstellern eingesetzt wird. Weltweit lässt sich dieser Trend zu mehr verkauften Android-Geräten schon seit einiger Zeit beobachten, was auch aktuelle Untersuchungen von Gartner [29] bestätigen: So konnte Android seinen Vorsprung als weltweit erfolgreichstes Smartphone-Betriebssystem deutlich ausbauen. Der direkte Konkurrent, das iPhone, liegt deutlich zurück. Bemerkenswert ist ebenfalls, dass alle anderen Betriebssysteme nur Nischenmärkte bedienen können.

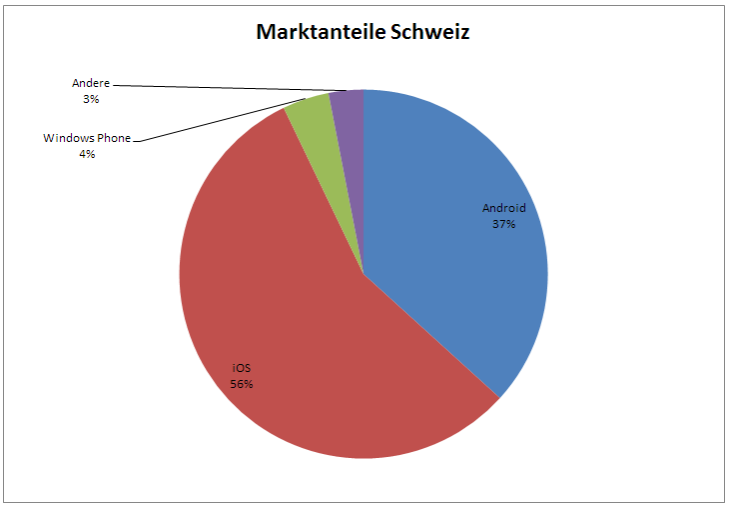

Abbildung 12: Marktanteile von Smartphone Betriebssystemen in der Schweiz. Auffallend ist hier der grosse Anteil von Apple Produkten. Quelle: [28] (Daten aus 2012)

Es ist unwahrscheinlich, dass sich der Schweizer Markt über längere Zeit diesem Trend entzieht. So zeichnet sich zwischen 2012 und 2013 eine Konsolidierung des Marktes in Richtung Duopol (Android und iOS) ab. Allerdings ist die Entwicklung von Windows Phone noch nicht absehbar.

Weiter ist zu erwarten, dass Schweizer Kunden sehr schnell auf andere Modelle als iPhones umsteigen werden, sollte das Interesse an Mobile Payment zunehmen [30]. Ebenso ist möglich, dass Apple in Zukunft NFC-Technologie in seine Smartphones einbauen wird. In diesem Fall ist allerdings nicht klar, welche Funktionen Entwicklern zur Verfügung stehen werden [30].

3.2.4 Acquirer

Je nach gewählter Lösung ändert sich beim Acquirer mit Mobile Payment nichts; gegebenenfalls muss er ein Software-Update auf seinen Terminals einspielen.

3.2.5 Merchant

Falls das Terminal des Merchants über keine Kontaktlos-Schnittstelle verfügt, muss er dieses aufrüsten oder ein neues Terminal kaufen. Im Übrigen ändert sich der Prozess aus Sicht des Merchants nicht.

Weiter kann der Merchant seine Consumer auf die neue Zahlungsmöglichkeit aufmerksam machen. Manche Acquirer unterstützen die Merchants dabei mit Werbematerial oder erlassen die Gebühren für eine bestimmte Zeit für Contactless- und somit auch Mobile Payment-Transaktionen.

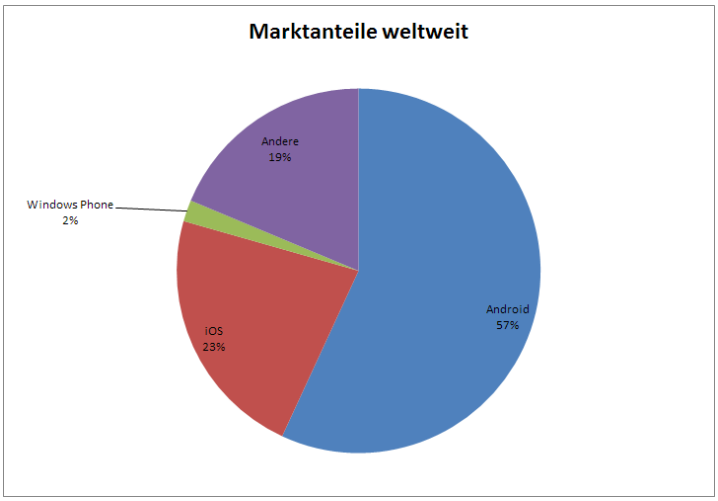

Abbildung 13: Marktanteile von Smartphone Betriebssystemen weltweit. Hier dominiert, im Gegensatz zur Schweiz, Android sehr deutlich. Quelle: [29] (Daten aus 2012)

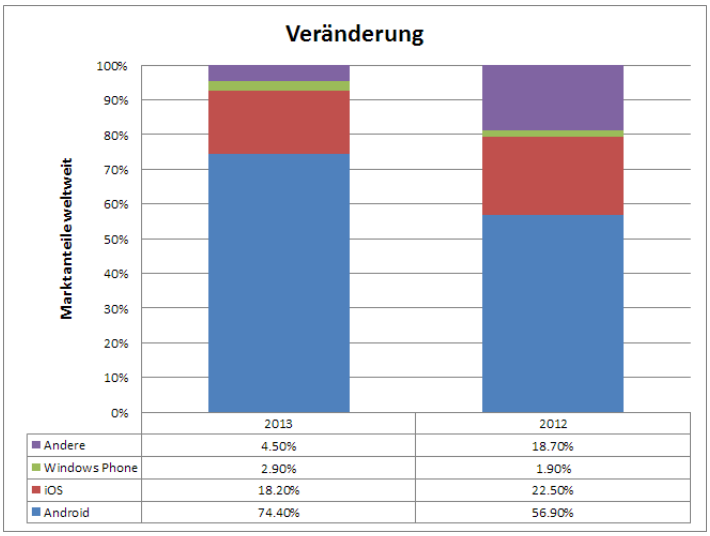

Abbildung 14: Entwicklung der weltweiten Marktanteile der Smartphone Betriebssystemen zwischen 2012 und 2013. Quelle: [29]

3.2.6 Issuer

Der Issuer muss für Mobile Payment Änderungen an seinen Prozessen vornehmen. Je nach gewählter Lösung wird er die Telefonnummer des Consumers erfassen müssen, um diesem die aktuellen Daten auf sein Handy laden zu können. Dazu benötigt er zusätzlich Verträge mit den MNO, damit der Consumer die Daten empfangen und nutzen können.

Wenn ein Lösungsansatz gewählt wird, bei dem Acquirer Modifikationen an der Terminalsoftware vornimmt, dann muss der Issuer zudem Software für die Smartphones der Consumer entwickeln oder einkaufen.

3.2.7 Mobile Network Operator

Der Mobile Network Operator (MNO; engl. für Mobilfunkbetreiber) hat mit dem Consumer eine Vereinbarung zur Erbringung von Mobilfunk-Dienstleistungen wie Telefonie oder mobiles Internet. Um Consumer in seinem Netz identifizieren zu können, müssen diese eine SIM-Karte des MNO benutzen. Eine solche SIM-Karte ist prinzipiell eine Smartcard, auf der Informationen zur Identifikation des Gerätes (und damit des Consumer) im Mobilnetz hinterlegt werden. Karten der neueren Generation bieten aber wesentlich mehr Speicherplatz, womit weitere Daten und Programme hinterlegt werden können. Damit wird es möglich, dass die Programme, welche der Card Manufacturer auf die Smartcard speichert, auch auf die SIM-Karte gespeichert werden können, um damit das Smartphone als Bezahlkarte einsetzen zu können. Zusammen mit der Unterstützung für die Funktechnologie NFC in modernen Smartphones wird es möglich, an einem NFC fähigen Bezahlterminal mit dem Smartphone zu bezahlen. Durch die Kombination dieser beiden Technologien wird das Smartphone zu einer Contactless Smartcard. Im Gegensatz zu einer Smartcard können aber auf dem Smartphone mehrere Karten gespeichert werden, aus welchen über den Bildschirm eine zum Bezahlen gewählt werden kann.

Andere Unternehmen sind beispielsweise Transportunternehmen, Skigebiete oder Konzertticketverkäufer, die einen Teil des freien Platzes für ihre jeweiligen Daten nutzen könnten.

Mobile Network Operator in der Schweiz Der Schweizer Mobilfunkmarkt umfasst die drei Netzbetreiber Swisscom, Orange und Sunrise, sowie einige weitere Brands, die auf den Netzen der genannten Provider agieren. Der Markt umfasste 2010 gemäss BAKOM über neun Millionen aktive SIM-Karten, gemäss (noch provisorischen) Zahlen im Jahr 2011 sogar über zehn Millionen Teilnehmer [31, p.21].

Swisscom Die Swisscom ist mit knapp 60% Marktanteil [31, p.21] der grösste Mitbewerber im Schweizer Mobilfunkmarkt. Die Swisscom entstand aus der ehemaligen PTT und bietet das ganze Spektrum an Dienstleistungen beim Festnetz, beim Mobilfunk sowie beim Breitbandinternet. Weiter bietet die Swisscom noch ein weites Spektrum an Informatik-Dienstleistungen an.

Aufgrund ihrer Grösse und weil sie auch die Grundversorgungskonzessionärin ist, dominiert die Swisscom den Markt deutlich.

Es ist erklärtes Ziel der Swisscom, ihren Kunden das beste Netz respektive die beste Dienstleistung zu bieten [30].

Sunrise Sunrise weist einen Marktanteil von knapp über 20% [31, p.21] im Mobilfunkmarkt aus und ist damit die Nummer Zwei im Markt. Wie Swisscom ist auch Sunrise in allen drei grossen Bereichen des Fern-

meldegeschäfts tätig. Im Gegensatz zu Swisscom konzentriert sich Sunrise auf die Erbringung von Dienstleistungen im Telekommunikationsmarkt.

Orange Der drittgrösste Anbieter ist Orange Schweiz. Orange kann rund 15% [31, p.21] des Marktes für sich beanspruchen. Auch Orange hat neben Mobilfunk Angebote für Festnetztelefonie und Internet.

Weitere Anbieter Weitere nennenswerte Anbieter im Markt sind Lebara mit 2.5% und Lycamobile mit 1% Marktanteil [31]. Beide haben kein eigenes Netz und kaufen diese Dienstleistung ein. Ausserdem werben beide Anbieter stark mit Angeboten für günstige internationale Gespräche und zielen somit vor allem auf Menschen mit Migrationshintergrund und auf Daueraufenthalter.

Die verbleibenden Anbieter sind vor allem im B2B Sektor tätig und kommen zusammen auf die restlichen rund 1.5% Marktanteil [31, p.21].

3.2.8 Trusted Services Manager

Der Trusted Service Manager (TSM; sinngemäss engl. für "Vertrauenswürdiger Dienstleistungserbringer") ist der Vermittler zwischen dem MNO und dem Issuer. Er sorgt dafür, dass der MNO gültige Daten für die Personalisierung der SIM-Karte des Consumers erhält, diese aber nicht einsehen kann.

Ein TSM kann entweder eigenständig sein, oder direkt entweder dem Issuer oder dem MNO angegliedert sein. Es kann auch sein, dass mehrere TSM nacheinander agieren. Zum Beispiel könnte ein TSM die Integration zum Issuer (SPTSM) übernehmen, während ein anderer die Integration zum MNO übernimmt (MNO TSM). Diese geteilte Infrastruktur bietet den Vorteil, dass die Schnittstellen zwischen mehreren Issuern und MNO weniger komplex werden. Des weiteren setzen die MNO bereits intern eine TSM-ähnliche Lösung ein, um die SIM-Schlüssel zu verwalten. Ebenso verfügen die Service Provider über ein TSM, um die Kartendaten an den Card Manufacturer übermitteln zu können.

Die Herausforderung dürfte darin liegen, die beiden TSM-Strukturen kommunizieren zu lassen und die internen Prozesse von MNO und Issuer entsprechend anzupassen.

Service Provider TSM ("SP TSM") Der Service Provider TSM ist meist ein Card Manufacturer. Er ist dafür verantwortlich, dass die Daten des Issuer korrekt verschlüsselt respektive signiert sind und auf eine Chip-Karte (Bezahlkarte oder SIM) geladen werden können. Im Falle von Mobile Payment leitet er die Daten dem zuständigen MNO TSM weiter. Diese Entscheidung trifft er anhand der Telefonnummer, die er mit dem MNO TSM abgleichen muss.

MNO TSM Der MNO TSM ist meist dem MNO angegliedert. Er sorgt dafür, dass die verschlüsselten oder signierten Daten des SP TSM sicher auf die SIM-Karte des Consumers gelangen.

Das Swisscom Modell Der Personalisierungsprozess, wie ihn sich die Swisscom vorstellt, würde für die Issuer nur wenige Änderungen an den eigenen Systeme bedingen. Die Issuer können weiterhin die bestehenden Kanäle zur Informationsübermittlung zu den Card Manufacturers (wie Trüb oder Oberthur) verwenden. Neu müsste noch die Telefonnummer des Kunden übermittelt werden, damit die Daten schliesslich der SIM-Karte der Kunden zugeordnet werden können.

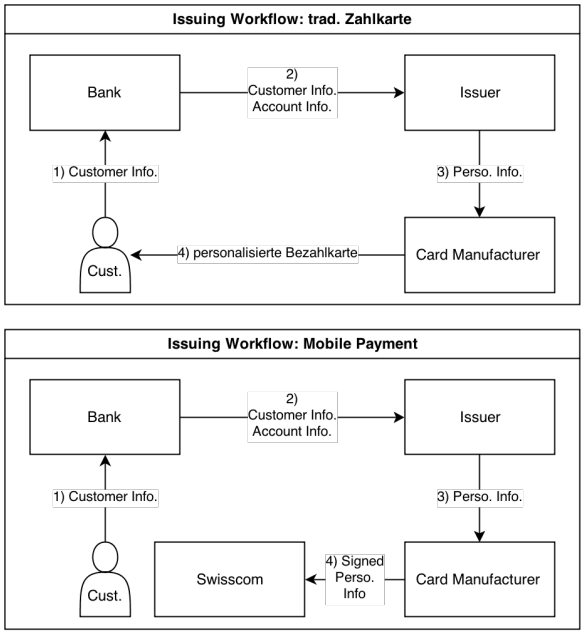

Abbildung 15: Das TSM Modell, wie es sich die Swisscom vorstellt, in vereinfachter Form.

Um dies umsetzen zu können, hat die Swisscom einen neuen Kommunikationskanal zum Manufacturer Trüb aufgebaut. Über diesen Kanal werden die vom Issuer eingereichten Daten an die Swisscom übermittelt, von wo aus sie dann auf die Endgeräte geleitet werden [32].

Es gäbe im Personalisierungsprozess des Mobile Payment also vier Parteien: Den Issuer (bestehend), den SP TSM (bestehend), den MNO TSM (neu) und den MNO (bestehend, neu im Prozess)[22]. Zwischen Issuer und Issuer TSM bestehen bereits Gateways. Die Interfaces zwischen Issuer TSM und MNO TSM und zwischen MNO TSM und MNO wären neu, betreffen aber nur den MNO, respektive den MNO TSM.

3.2.9 Weitere Stakeholder

Mobile Device Manufacturer Der Mobile Device Manufacturer (engl. für Mobiltelefonhersteller) stellt das Smartphone her. Er sorgt dafür, dass die unterschiedlichen Technologien miteinander zusammenarbeiten können.

Einige Manufacturer haben begonnen, Mobile Devices mit fest auf der Hauptplatine verbauten Secure Elements auszuliefern. Diese Secure Elements kontrollieren sie ausschliesslich selbst. Es entsteht insofern eine ähnliche Situation wie mit den Secure Elements auf der SIM-Karte, als das ein Issuer mit externen Partnern verhandeln muss.

3.2.10 Prozesse und Bestimmungen

Die im Bereich Mobile Payment relevanten Bestimmungen sind im Wesentlichen dieselben wie beim Kartengeschäft. Ebenso sind die Prozesse einander ähnlich.

[22] Diese vier Parteien sind nicht zu verwechseln mit den vier Parteien des Zahlungsverkehrs!

Zu den Bestimmungen des Kartengeschäfts kommen noch einige Anforderungen der Card Schemes hinzu, auf die aber nicht weiter eingegangen wird.

Prozessbeschreibung: Ausstellen der Personalisierungsinformationen auf eine SIM-Karte
Genau wie bisher ergreift der Kunde die Initiative, wenn er eine Bezahlkarte auf sein Handy ausgestellt haben möchte. Diese Anfrage geht schliesslich beim Issuer ein. Dies kann aber über Dritte, zum Beispiel über den MNO oder eine Bank, geschehen.

Der Issuer prüft den Antrag genau gleich, wie er einen herkömmlichen Karten-Antrag prüft. Wird dem Antrag stattgegeben, erzeugt der Issuer die Personalisierungsinformationen und leitet diese an den SP TSM weiter. Der SP TSM muss die Personalisierungs-Informationen signieren, weil er die Hoheit über die kryptografischen Schlüssel für das später eingesetzte Secure Element hat.

Aufgrund von weitergehenden Informationen (beispielsweise die Telefonnummer), welcher der Kunde gemacht hat, kann der Issuer den richtigen MNO TSM wählen und leitet anschliessend die signierten Informationen an diesen weiter. Dort beginnt ein komplexer Prozess, bei dem geprüft wird, ob der Consumer über kompatible Komponenten verfügt, um Mobile Payment einzusetzen. Die dazu notwendigen Informationen liegen im Allgemeinen bereits beim MNO vor: welches Gerät der Kunde hat, ob dieses NFC-fähig ist, ob die SIM-Karte kompatibel, etc. Erfüllen alle Komponenten die Anforderungen, werden die Daten over-the-air in den sicheren Speicher der SIM-Karte geladen und dort aktiviert.

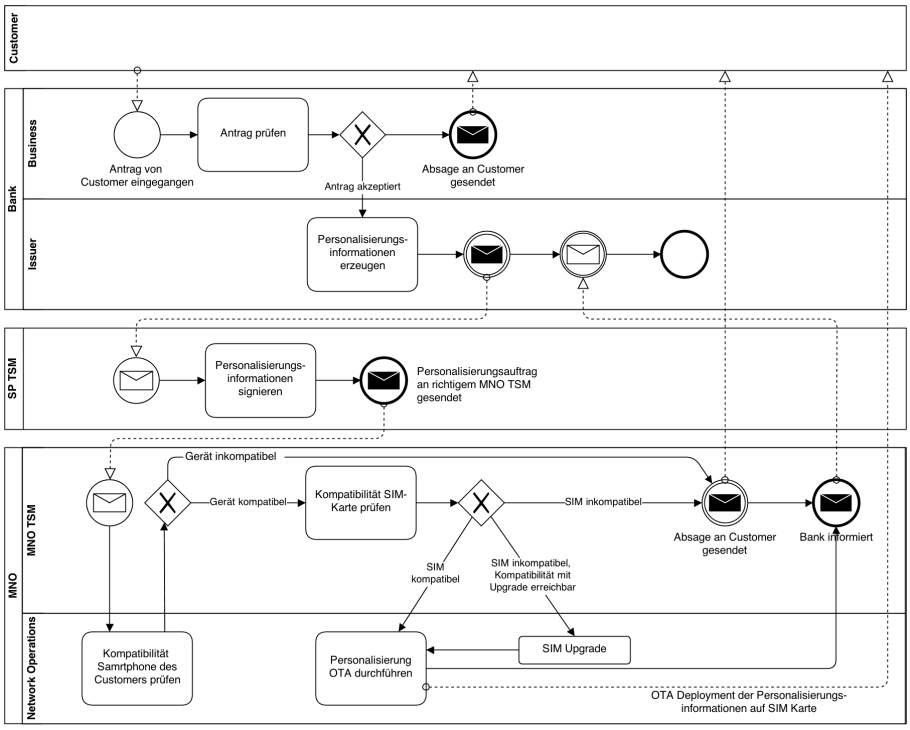

Abbildung 16: Prozess, um die Personalisierungsinformationen auf eine SIM-Karte zu bringen

3.3 Marktsituation

In der Schweiz ist das kontaktlose Bezahlen in der Öffentlichkeit noch kaum bekannt. Dennoch wird hinter den Kulissen bereits stark an entsprechenden Applikationen und Lösungen gearbeitet. Jeder der Marktteilnehmer möchte sich in eine strategisch günstige Ausgangslage bringen und seine Produkte auf den Markt bringen, sobald der Boom einsetzt [8]. Noch halten sich die Anbieter zurück, einzig die Swisscom verspricht, noch in diesem Jahr ein entsprechendes Produkt (Entwicklungsname “TapIt”) auf den Markt zu bringen.

Vergleiche mit anderen Ländern haben gezeigt, dass die Einführung von Mobile Payment mit NFC besonders gut funktioniert, wenn eine enge Vernetzung zwischen Telekommunikations- und Bankbranche existiert. In diesem Zusammenhang wird immer wieder das Beispiel Japan angeführt. Der dortige mobile Payment Markt wird fast vollständig von MNOs kontrolliert (einzige nennenswerte Ausnahme bildet JCB, das Japanische Card Scheme) [33]. Neben der Tatsache, dass die dortigen Banken den Trend nicht erkannt haben, und das Feld den MNOs überlassen haben, ist wichtig zu erwähnen, dass die dortige Telekommunikationsanbieterin NTT DoCoMo ein extrem grosses Unternehmen ist, welches auch Verflechtungen zu Banken hat [30].

In der Schweiz sind diese Verflechtungen nicht gegeben. Auch sind die Banken in der Schweiz bei Weitem grössere Konzerne als die MNOs, also gerade umgekehrt zur Situation in Japan. Beide Seiten (Banken und MNOs) haben wiederholt erwähnt, dass man einer Zusammenarbeit durchaus aufgeschlossen gegenübersteht [8] oder diese sogar explizit im Geschäftsmodell einbindet [32]. Dennoch besteht eine Uneinigkeit über den Preis der von den MNOs angebotenen Dienstleistung (Speicherplatz auf der SIM-Karte). Dies, gepaart mit der Unfähigkeit jeder Seite, eine Lösung alleine auf den Markt zu bringen, zu einer Patt-Situation führt. Das ist ein wesentlicher Grund dafür, weshalb Mobile Payment in der Schweiz noch nicht verfügbar ist.

Die treibende Kraft stellen die Card Schemes dar, welche mit den Issuern Verträge abgeschlossen haben, welche diese zur Ausgabe von kontaktlosen Bezahlkarten verpflichten. Das Interesse der Card Schemes dürfte hauptsächlich in dem erwarteten erhöhten Transaktionsvolumen gründen, welches durch die einfachere nutzbare Technologie ermöglicht wird. In diesem Zusammenhang muss auch die Einführung von Transaktionen ohne Notwendigkeit der PIN-Eingabe (*Low Value Transactions*, vgl. EMV Contactless) gesehen werden, die ebenfalls den Einsatz der Karte vereinfachen und daher die Anzahl der Transaktionen erhöhen dürften.

Die Entwicklung des Marktes u.a. in Japan und den Vereinigten Staaten von Amerika (vgl. Google Wallet) dürfte auch mit einer der Gründe sein, weshalb die Issuer bereits seit einiger Zeit Tests durchgeführt haben. Für die Issuer würde eine Entwicklung wie in Japan bedeuten, dass sie an Marktmacht verlieren würden.

Sollte sich ein bilaterales Modell in der Schweiz durchsetzen, wären die Issuer die Verlierer. Wie in den vorhergehenden Kapiteln ausgeführt, bedeutet die Einführung von Mobile Payment einzig für die Issuer grössere Veränderungen am Prozess.

Die aktuelle Supply Chain fasst die vorhergehenden Kapitel nochmals zusammen: Der Prozess beginnt damit, dass der Consumer eine Bezahlkarte bestellt. Dies tut er in der Schweiz typischerweise bei einer Bank. Die Bank übernimmt die gesetzlich vorgeschriebenen Prüfungen (Konsumkreditgesetz), soweit notwendig und kontrolliert die Identität des Kunden (Geldwäschereigesetz). Weiter vereinbart der Kunde mit der Bank, wie die über die Karte abgewickelten Transaktionen verrechnet werden. Im Falle einer Debitkarte wird der Betrag dem Bankkonto des Kunden direkt belastet, im Falle einer Kreditkarte erst verzögert mittels Lastschrift oder per Rechnung.

Die von der Bank gesammelten Daten werden an den Issuer übermittelt, welcher seinerseits eine Lizenzvereinbarung mit einem der Card Schemes hat und die Karte für eben dieses Scheme ausstellt. Um die Karte

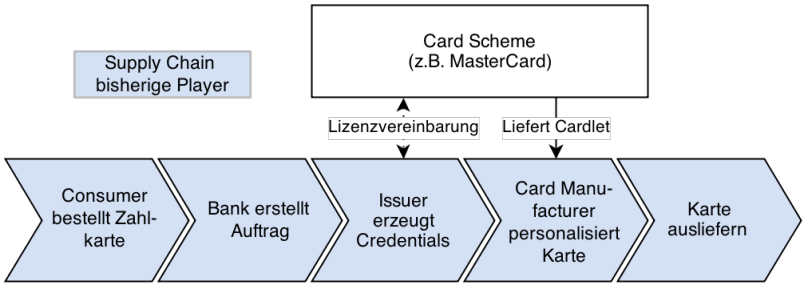

Abbildung 17: Bisherige Supply Chain von Bezahlkarten

erstellen zu können, müssen die von EMV geforderten Credentials erzeugt werden. Dabei können die Vorschriften des Card Schemes die Anforderungen von EMV verschärfen und bestimmen, wie die Credentials an den Card Manufacturer übermittelt werden.

Der Issuer sendet diese Daten weiter an den Manufacturer, der die Karte herstellt. Dabei wird sie bedruckt, geprägt und die Daten werden auf den Chip kopiert. Damit die Karte für das Card Scheme eingesetzt werden kann, muss sich darauf ein Programm befinden, welches die EMV-Transaktion durchführt. Dieses Cardlet wird vom Card Scheme gestellt. Nachdem die Karte erzeugt ist, werden diese und der dazugehörige PIN an den Kunden gesendet.

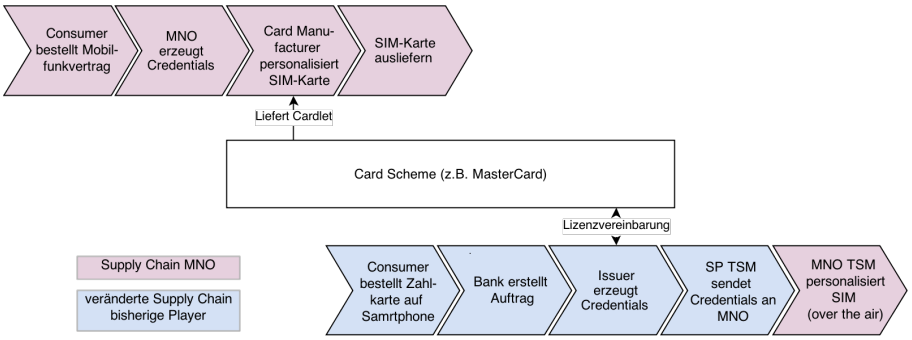

Abbildung 18: Supply Chain mit MNO als TSM

Anders stellt sich die Situation im bilateralen Modell dar: In diesem Fall ist die SIM-Karte bereits vorgängig durch den MNO an den Kunden geliefert worden. Für den MNO bleibt die bisherige Supply Chain weitgehend bestehen. Der wesentliche Unterschied ist, dass beim Personalisieren der SIM-Karte zusätzlich schon vorgängig die Cardlets von mehreren Card Schemes auf die Karte kopiert werden, damit diese später nicht OTA geladen werden müssen.

Für den Issuer ändert sich der Prozess aber deutlich: sein nachgeschalteter Partner ist nun nicht mehr der Card Manufacturer sonder der MNO. An diesen übermittelt er dieselben Daten wie bisher, der MNO übernimmt selbstständig alle weitergehenden Prozesse, bis der Kunde mit seinem Smartphone bezahlen kann. Damit verliert der Issuer ein beträchtliches Stück Kontrolle über den Prozess: Während der Card Manufacturer ein Subunternehmer war, welcher im Auftrag des Issuers die Karte fertigt, agiert der MNO auf Augenhöhe mit dem Issuer. Da der MNO die SIM selbst besitzt und kontrolliert, ist der Issuer nicht mehr “Eigentümer” des Chips, sondern lediglich “Benutzer”.

3.4 Zukünftige Entwicklungen, Visionen

In diesem Kapitel werden einige der aktuell diskutierten Ansätze, wie sich der Mobile Payment Markt entwickeln könnte, diskutiert. Es werden bewusst nur einige wenige Situationen betrachtet, bei welchen eine gewisse Eintrittswahrscheinlichkeit gegeben ist.

Der Markt befindet sich noch in einer Pionierphase, in der verschiedene Modelle ausprobiert werden. Es wird sich erst zeigen müssen, welches von diesen Modellen bei Consumer und Merchant anklang finden wird. Zu guter Letzt ist auch die Stellung der Banken und deren Rolle im angestrebten Geschäftsmodell für eine erfolgreiche Adaption relevant.

Gemäss einer Untersuchung von Ixaris gehen über 70% der Befragten davon aus, dass die Innovation im Payment-Bereich vor allem durch neue Marktteilnehmer bestimmt wird [34, p.4]. Dies muss als alarmierendes Zeichen angesehen werden, besonders, weil die Teilnehmer der Umfrage grösstenteils selbst aus der Branche stammen und über entsprechendes Fachwissen verfügen. Die Jury geht davon aus, dass es von zentraler Bedeutung sein wird, dass Acquirer ("Payment Provider" im Original) eine offene Platform schaffen, mit welcher sich verschiedene Typen von Zahlungen verarbeiten lassen. Ebenso geht sie davon aus, dass in Zukunft unabhängige Zahlsysteme (Person-to-Person-Payments) eine wichtigere Rolle spielen werden.

3.4.1 Neu in dem Markt eintretende Stakeholder

Neben den MNO gibt es einige weitere Stakeholder, die bereits in Geschäftsbereichen tätig sind, welche dem Payment nahe stehen. Es ist durchaus möglich, dass diese in absehbarer Zeit in den Markt eintreten werden.

Wie unter Anforderungen an ein Marktmodell ausgeführt, ist einer der wichtigsten Faktoren für ein erfolgreiches Geschäftsmodell im Payment-Bereich das erreichen einer kritischen Masse. Dies stellt insbesondere eine der Markteintrittsbarrieren der bisherigen Player dar.

Unternehmen wie PayPal oder Facebook verfügen bereits über eine entsprechend grosse Community, welche über dies gut untereinander vernetzt ist (im Falle von PayPal indirekt über die Auktionsplattform ebay). PayPal ist überdies bereits selbst im Payment-Bereich tätig; allerdings werden derzeit die Transaktionen über Kreditkartenanbieter abgerechnet, obwohl es auch möglich ist, auf das eigene PayPal-Konto einzuzahlen.

Eine weitere Herausforderung für neue Stakeholder ist die Universalität des Bankensystems: Praktisch jede Person der westlichen Welt verfügt über mindestens ein Bankkonto und kann prinzipiell Geld an jeden anderen Kontoinhaber überweisen. Anders stellt sich die Situation bei Newcomers dar: Solange nur Beträge zwischen Nutzern des Systems versendet werden können, bedeutet dies immer, dass der Kunde über ein Konto beim jeweiligen Unternehmen verfügen muss. In Anbetracht der Marktmacht der Banken in diesem Bereich könnte es durchaus dazu kommen, dass sich solche Newcomer auf ein gemeinsames Zahlungsschema einigen, damit auch die Benutzer verschiedener Anbieter Geld untereinander überweisen können.

Banken konnten ihr Marktsegment bisher unter anderem deswegen erfolgreich verteidigen, weil sie sich klar positioniert haben als vertrauenswürdige Instanz, welcher der Kunde seine Ersparnisse anvertrauen kann. Ob gerade das immer wieder in die Negativschlagzeilen geratende Unternehmen Facebook dieses Image zu verkörpern vermag, darf bezweifelt werden. Allenfalls könnte dies in Zukunft zu einer vermehrten Trennung zwischen Spar- und Kontokorrentgeld auch bei Privatkunden führen. So würde beispielsweise das Ersparte bei einer Bank angelegt, während die täglichen Zahlungen über PayPal abgewickelt werden. In diesem Fall werden die Player aber selbst zu Banken, was praktisch in allen Staaten rechtliche Konsequenzen im Sinne von regulatorischen Bestimmungen mit sich bringt. Unternehmen wie PayPal besitzen aus diesem Grund bereits eine Bankenlizenz.

Charakterisierend für die Player, welche bereits im Paymentgeschäft tätig sind, ist, dass sie sich auf Geschäftsfelder spezialisiert haben, welche von den Banken nicht oder nur zu schlechten Konditionen abgedeckt werden. Beispiele dafür sind WesternUnion (auf internationale Sofortüberweisungen spezialisiert) oder PayPal, welches vor allem internationale Zahlungen für das Auktionshaus ebay abwickelt. Bemerkenswert ist, dass WesternUnion bereits 2008 in den Mobile Payment-Bereich eingestiegen ist [35]. Das Unternehmen bietet aber ausser Überweisungen zwischen Konten von Kunden auch Avis zur Auszahlung am Schalter an ("Mobile to Cash").

3.4.2 Ablösung von POS-Terminals

Eine weitere mögliche Entwicklung ist, dass die POS-Terminals komplett verschwinden werden. Den Grundstein für dieses Modell legte das US-Unternehmen Square[23], welches ein Gerät anbietet, mit welchem Magnetstreifen mit einem Handy gelesen werden können. Ein App verarbeitet die Daten und eine Bezahltransaktion startet. Mit dem Produkt "Square register" hat das Unternehmen eine einfache Kassenlösung geschaffen, die lediglich ein iPad benötigt. Damit ist keine weitere POS-Infrastruktur notwendig. Da das System auf dem Magstripe-Verfahren aufsetzt, darf bezweifelt werden, dass es sich in Europa durchzusetzen vermag.

Das Konkurrenzunternehmen iZettle[24] bietet ungefähr dasselbe Produkt an, hat aber ein Lesegerät entwickelt, mit welchem der Chip von Bezahlkarten gelesen werden kann, was eine EMV-konforme Zahlung ermöglicht.

Beide Unternehmen sind noch in der Start-up-Phase und die Lösungen werden von den angestammten Players vehement bekämpft. Dass beide Lösungen aber von sich behaupten, von den Card Schemes zertifiziert zu sein, deutet darauf hin, dass die Card Schemes solchen neuen Ideen nicht gänzlich abgeneigt gegenüberstehen.

Der Grund für die Akzeptanz von Card Schemes dürfte darin liegen, weil dadurch ihr Geschäftsmodell nicht gefährdet, sondern gefördert wird. Da die Geräte die Zahlungen über Kreditkarte vornehmen, führt jede damit ausgeführte Transaktion zu Mehrumsatz bei den Card Schemes. Für Acquirer ist die Zusammenarbeit mit solchen Unternehmen ein zweischneidiges Schwert: Auf der einen Seite können sie dadurch auch einen Mehrumsatz erzielen, auf der anderen Seite kanibalisieren sie damit das eigene Geschäft mit POS-basierten Zahlungen. In Ländern, wie der Schweiz, in denen der Merchant das Terminal kauft, ist dies umso gravierender, weil dadurch auch die Anzahl abgesetzter Terminals sinkt.

Aktuell dürften solche Lösungen vor allem für kleine Unternehmen wie Boutiquen, Dienstleister und Gastgewerbe, wo keine zentrale Infrastruktur existiert, interessant sein. Es ist zwar unwahrscheinlich, dass grosse Detailhändler in absehbarer Zeit auf solche Systeme umschwenken werden. Zu stark ist die Integration der Kassenlösungen in die ERP-Infrastruktur solcher Unternehmen. Dies stellt aber kein prinzipielles Hindernis dar; es wäre durchaus möglich, ein auf Tablets basierendes Kassensystem zu entwickeln, welches über die Serversysteme des Herstellers eine Schnittstelle für dessen ERP-Systeme bietet. Ein mögliches Problem könnte hierbei sein, dass die Daten hierzu auf die Server des Herstellers kopiert werden müssen und daher nicht vollständig auf den Systemen des Merchants verarbeitet werden können.

3.4.3 Verwenden anderer Übertragungstechnologien

Bestimmte Vertreter von Pionierlösungen beschwören sogar das vorzeitige Ende von NFC herauf [36]. So verwenden einige Ansätze optische Erkennung oder fordern den Nutzer zur Eingabe eines Codes auf. Da-

[23] Siehe https://squareup.com/.
[24] Siehe http://www.izettle.com/.

mit können auch Geräte wie das iPhone berücksichtigt werden, welche nicht über NFC verfügen. Gänzlich von der Hand zu weisen ist dieses Argument nicht. Wie diese Thesis ausführlich darlegt, bringt die Benutzung von NFC teilweise gravierende Probleme bei der Implementation mit sich. Es darf nicht vergessen werden, dass NFC lediglich eine *enabling Technology* ist; sie kann durch andere Technologien wie optische Erkennung (beispielsweise QR-Codes) in den meisten Fällen substituiert werden.

Wie diese Studie auch zeigt, ist auch die vorgeschlagene Lösung mit dem NFC Peer-To-Peer-Modus nicht frei von Problemen. Nach Meinung der Autoren bietet NFC aber die beste User Experience, verglichen mit optischen Lösungen (wie QR) oder mit Lösungen, in welchen ein PIN eingegeben werden muss. Weiter stellt der NFC Peer-To-Peer-Modus die optimale Grundlage dar für ein Zahlungs-Kommunikationsprotokoll, da es spezifisch für die bidirektionale Datenübertragung über die Kontaktlos-Schnittstelle gedacht ist.

3.5 Zusammenfassung

Als Erstes muss festgehalten werden, dass es keinem Player bisher gelungen ist, die Brücke zu den bisherigen Zahllösungen (Bankkonti) zu schlagen. Es ist immer notwendig, eine Vorauszahlung an den Anbieter zu leisten (das heisst, bei diesem ein Konto zu unterhalten) oder die Zahlung über eine Kreditkarte abrechnen zu lassen. WesternUnion löst das Problem, indem es auf Bargeld zurückgreift (Einzahlung direkt am Schalter). Damit stellen die Card Schemes die einzigen Unternehmen dar, welchen es auf globaler Basis gelungen ist, eine enge Bindung ihrer Dienstleistung an das Bankensystem zu erreichen. Diese Enge Bindung könnten die Card Schemes auch nutzen, um auf die Banken Einfluss zu nehmen, damit sie nicht durch eine andere Lösung konkurriert werden.

Daher dürfte jede Lösung, welche versucht, eine direkte Kooperation mit den Banken zu etablieren von den Card Schemes massiv bekämpft werden. Ebenfalls stehen solche Modelle vor dem Problem, das sie eine Kooperation mit unzähligen Banken erreichen müssten.

Modelle, welche Kreditkarten als Abrechnungssystem nutzen finanzieren sich üblicherweise über die Kommission. Weil sie sich dabei als zusätzliches Unternehmen in die Abrechnungskette integrieren, sind die Kommissionen für den Merchant typischerweise höher, was für den Merchant nachteilig ist. Alternativ müssten Gebühren für die Nutzung vom Kunden verlangt werden, was ebenfalls problematisch ist.

Ein allgemeines Merkmal dieser alternativen Zahlungsmethoden ist, dass sie bewusst mit Standards brechen. Die stark regulierte und standardisierte Branche hemmt dadurch die Entwicklung von neuen Ideen. Alternative Zahlungsmodelle setzen auf offene Standards, welche es Drittanbietern ermöglichen, auf dem Modell aufzubauen und eigene, erweiterte Lösungen anzubieten.

Als letzter und vielleicht wichtigster Punkt muss die Sicherheitsfrage gestellt werden. Die EMV-konforme Implementation auf einer Smartcard und auch bei Verwendung eines Secure Elements und des NFC Card Emulation Modes bei Mobile Payment darf als sehr sicher betrachtet werden. Alternative Zahlungsmodelle kommen alle ohne ein Secure Element aus. So wird stets davon ausgegangen, dass die verwendeten Geräte und Software (Betriebssysteme, Apps und Browser) die Sicherheit gewährleisten können. Dagegen geht insbesondere das Mindset von EMV Contactless davon aus, dass das Smartphone-Betriebssystem nicht als ausreichend sicher betrachtet werden kann. Daher kann keine der vorgestellten Visionen die Sicherheit einer Smartcard übertreffen.

Natürlich gilt dies nicht für Lösungen, welche Smartcards lediglich nutzen wie iZettle oder gar auf Magstripe zurückfallen wie Square. Im Falle von iZettle kann die Sicherheitsfrage nicht abschliessend beurteilt werden, da das Unternehmen nicht veröffentlicht, wie die Lösung funktioniert. Es ist möglich, dass der Cardreader über ein Secure Element verfügt und damit schon selbst ein EFT/POS-Terminal darstellt.

4 Betrachtung der Machbarkeit

4.1 Problemdomäne

Bei der Umsetzung einer Lösung müssen diverse Standards und Normen eingehalten werden. Ausserdem gibt es einige technische Hürden, für die es eine Lösung zu finden gilt.

4.1.1 EVM Anforderungen

Aus den EMV-Spezifikationen leitet sich ein wesentlicher Teil der Anforderungen an die Lösung ab.

Allgemein Die ursprünglichen vier Teile des EMV-Regelwerks, *Bücher* genannt, spezifizieren das traditionelle Kartengeschäft mit kontaktbehafteten Bezahlkarten:

- Book 1: Application Independent ICC to Terminal Interface Requirements ([37])
- Book 2: Security and Key Management ([38])
- Book 3: Application Specification ([39])
- Book 4: Cardholder, Attendant, and Acquirer Interface Requirements ([40])

Die für diese Arbeit zentralen Spezifikationen sind die *EMV Contactless* Bücher. Darin wird der sich von der kontaktbehafteten Version unterscheidenden Physical Layer neu definiert und die darauf aufbauende Architektur spezifiziert. Die *EMV Contactless* ist ebenfalls in vier Bücher aufgeteilt.

- Book A: Architecture and General Requirements ([41])
- Book B: Entry Point ([42])
- Books C: Kernel Specifications ([43], [44], [45], [46], [47])
- Book D: Contactless Communication Protocol ([48])

Schliesslich gibt es noch diverse Nebendokumente. Diese werden hier nicht weiter aufgeführt und im Bezug nehmenden Absatz direkt darauf verwiesen.

Für die weitere Betrachtung sind vor allem Book 2 und 3 aus der EMV-Spezifikation, sowie Book A und D aus der EMV Contactless Spezifikation von Bedeutung. Sie definieren die Anforderungen an einen klaren Zahlungsablauf sowie die notwendigen Protokolle dazu.

Mobile Payment Das Mobile Payment im Sinne von Zahlen mit einem Smartphone ist in den EMV-Dokumenten nicht beschrieben. Es ist lediglich das kontaktlose Bezahlen mit einer dafür ausgerüsteten Bezahlkarte beschrieben.

Diese Bestimmungen werden aktuell eins zu eins auf Mobile Payment angewendet, das heisst, das Smartphone in den *Card Emulation Mode* versetzt wird. Die einzelnen Card Schemes haben im Rahmen der EMV Contactless Spezifikationen Vorschriften zu Mobile Payment erlassen. Diese schreiben ebenfalls den Card Emulation Mode als zu verwendende Technologie vor. Darüber hinaus haben zumindest MasterCard und Visa Vorschriften für die zugehörenden Wallet Apps auf den Smartphones verfasst. Beispielsweise schreibt MasterCard in [49, pp.7–34] genau vor, wie sich das Userinterface eines Walles zu verhalten hat. Die EMV

selbst macht für kontaktlose Transaktionen lediglich Vorschriften, wie sich das Interface des Terminals zu verhalten hat [41, pp.69–77].

Neben den Vorschriften von Card Schemes sind für Mobile Payment auch die Spezifikationen zu GlobalPlatform, beispielsweise *Secure Element Access Control* [50], wichtig. Diese regeln die Struktur und den Zugriff auf die als *Secure Element* bezeichneten Speicherchips, wie sie auf Bezahlkarten, in SIM-Karten und Mobiltelefonen zu finden sind.

Nachdem die entsprechenden Dokumente ausgewertet und die Aussagen in den geführten Interviews bestätigt wurden, wurden folgende Hauptpunkte identifiziert, welche im Rahmen dieser Studie betrachtet werden:

- EMV spezifiziert Mobile Payment nicht. Die Bestimmungen des EMV Contactless Standard sind jedoch verbindlich. Mobile Payment Lösungen müssen daher auf die EMV Contactless zurückgreifen, um EMV-kompatibel zu sein.
- Die Anforderung, ein Secure Element verwenden zu müssen, stammt nicht aus der EMV-Spezifikation. Es sind viel mehr die Card Schemes, die beispielsweise verlangen, dass FIPS 140-2 [51] eingehalten werden muss.
- In der EMV Contactless Norm wird *NFC* nicht erwähnt. Es wird lediglich auf den ISO-Standard 14443 verwiesen [41]. Wie in Anhang II dargelegt wird, baut NFC selbst auf ISO 14443 auf. Es kann deshalb im *Card Emulation Mode* eine EMV Contactless kompatible Kommunikation zu einem Terminal hergestellt werden.

4.1.2 Terminal

Bezahlvorgang Grob gesagt wird beim Bezahlvorgang der Betrag, welcher zu bezahlen ist, von der Kasse an das Terminal übermittelt, wodurch dieses eine Transaktion mit eben diesem Betrag startet.

Tatsächlich ist der Vorgang komplizierter. Zuerst wird die Karte mit Strom versorgt und das CardOS gestartet. Danach wird die richtige Bezahl-Applikation ausgewählt. Dieser Auswahlvorgang ist notwendig, da sich mehrere solcher Applikationen auf einer Karte befinden können. Anschliessend wird die Applikation, normalerweise ein Java-Card Applet (daher auch häufig Cardlet oder Applet genannt), gestartet. Nun wird entschieden, wie der Kartenhalter identifiziert werden soll. Dieser Entscheidungsprozess findet aufgrund eines genau spezifizierten Algorithmus statt, wobei schliesslich ein *Candidate* gewählt wird. Häufige Varianten für die Authentifizierung sind PIN oder Unterschrift.

Nun wird die Zahlung durchgeführt. Dazu wird ein Datenblock an die Karte gesendet, der von jener signiert werden muss. Anschliessend wird der signierte Block, genannt Kryptogramm (*Cryptogram* im Original), zusammen mit dem zu bezahlenden Betrag an den Issuer der Karte gesendet und im Normalfall dort verbucht. Es kann aber auch sein, dass die Zahlung nicht durchgeführt werden kann, weil beispielsweise das Guthaben erschöpft ist. In diesem Fall muss das Terminal eine entsprechende Fehlermeldung anzeigen.

Bei Mobile Payment oder Bezahlung mit einer kontaktlosen Karte ist der Vorgang nun zu Ende. Bei der kontaktbehafteten Bezahlung kann der Issuer nun auf die Karte noch Updates (zum Beispiel der Reset von Countern) aufspielen. Erst dann wird die Karte wieder freigegeben.

Verbindungen des Terminals Die Verbindung zum Acquirer wird von EMV nicht näher spezifiziert. In der Schweiz regelt dies der EP2-Standard. Alle in der Schweiz verkauften Terminals unterstützten diesen Standard. Somit kann der Merchant den Acquirer frei wechseln, ohne ein neues Terminal kaufen zu müssen.

Die Verbindung zum EFT/POS-System ist ebenfalls in EP2 geregelt [25]. Das EFT/POS-System hat die Möglichkeit, auf dem Terminal eine Transaktion auszulösen, und kann den Zahlungsbeleg empfangen, um ihn separat ausdrucken zu können.

4.1.3 NFC Card Emulation Mode

Da EMV Contactless nur für *Contactless Smartcards* bestimmt war, muss ein NFC-fähiges Telefon in den *Card Emulation Mode* wechseln, um mit einem EFT/POS-Terminal kommunizieren zu können. Der *Card Emulation Mode* kann aus Sicht von NFC-fähigen Geräten als eine Art Kompatibilitätsmodus betrachtet werden.

Bei modernen Smartphones, allen voran bei den Android-Telefonen, hat aber der *Card Emulation Mode* eine Sonderstellung. Er kann nämlich nicht, wie die anderen beiden Modi *Peer-To-Peer* und *Reader/Writer*, über die Android API angesprochen werden, obwohl dies technisch möglich wäre (siehe [52]). Viel mehr scheint es eine bewusste Design-Entscheidung zu sein, dass nur ein Secure Element den Card Emulation Mode aktivieren darf.

OS	Card Emulation möglich	Bemerkung
Android	nein	Möglich mit CyanogenMod 9.1 und höher
Windows Phone 8	nein	
Blackberry 7.1	ja	
iOS	n/a	Apple-Geräte verfügen über keine NFC-Schnittstelle

Tabelle 3: Verfügbarkeit von Emulation von ISO 14443-4 Type A Tags auf verschiedenen Plattformen [53].

Für eine EMV-kompatible Emulation einer Smartcard, muss das Smartphone ein ISO 14443-4 Type A oder B Target emulieren. Dies ist nur bei Blackberry 7.1 mit dem standardmässig installierten Betriebssystem (*Stock ROM*) möglich. Da der Marktanteil von Blackberry aber sehr gering ist und in den vergangenen Jahren ständig gefallen ist (vgl. Verbreitung von Mobiltelefonen in der Schweiz), scheint eine Lösung, welche ausschliesslich für Blackberry konzipiert ist, nicht marktfähig. Aus diesem Grund wurde die Blackberry-Platform nicht weiter untersucht.

4.1.4 Secure Element

Das Secure Element (SE) ist stark verwandt mit dem Chip auf der Bezahlkarte, jedoch gibt es einige Unterschiede. So ist der Chip nicht wie bei der Karte direkt mit der NFC-Antenne verdrahtet, sondern über ein Protokoll mit dem NFC-Controller eines Smartphones verbunden. Im Falle einer SIM-Karte wird das Single Wire Protocol (SWP) verwendet. Um in den Card Emulation Mode zu gelangen, muss der Controller zuerst vom SE entsprechend konfiguriert werden. Im sogenannten *NFC Mode Switch* erkennt der Controller des Gerätes, welches sich in einem HF-Feld befindet, welches Protokoll die Gegenstelle verwenden möchte [54, pp.102–103]. Wenn die Gegenstelle das native NFC-Protokoll (also Peer-to-Peer oder Reader/Writer) unterstützt, wird der Card Emulation Mode aktiviert (Details zur Erkennung des Feldes finden sich im Anhang

II). Dabei werden die empfangenen Daten direkt via SWP an das SE übermittelt, umgekehrt leitet er die via SWP vom SE empfangenen Daten an das Kartenterminal weiter.

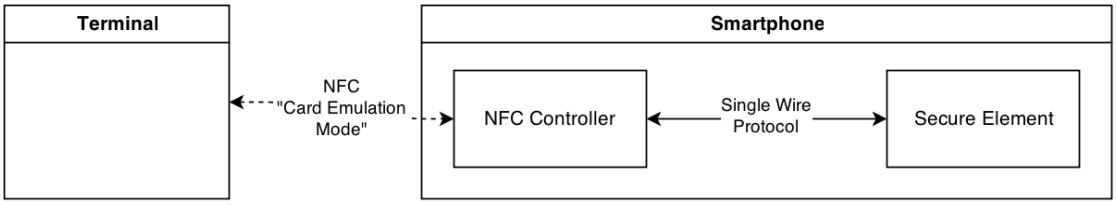

Abbildung 19: Kommunikation vom EFT-POS Terminal zum Secure Element (Im Beispiel bei Verwendung der SIM-Karte als SE)

Laden von Daten in das Secure Element EMV kompatible Bezahlkarten folgen dem ursprünglich von Visa entwickelten GlobalPlatform-Standard. Er sieht zum Einspielen von Programmen (meist Java Card Applets) und Daten auf die Karte eine zentrale Instanz vor. Diese Instanz wird "Card Manager" genannt. [24] Alle Applikationen, die auf dem Chip, und auch beim Secure Element, installiert werden sollen, müssen mit einem Schlüssel signiert werden. Der Card Manager überprüft diese Signatur und installiert die Applikation nur, wenn die Verifikation erfolgreich ist. Dasselbe gilt für Daten, die fest auf dem Chip hinterlegt werden, wie zum Beispiel die Personalisierungsinformationen einer Bezahlkarte. Die Daten und Programme können zusätzlich zur Signatur auch verschlüsselt werden. Nur so kann beispielsweise die Vertraulichkeit beim Nachladen von Daten OTA garantiert werden.

Die Signierung, respektive die Verschlüsselung, von Applets verhindert, dass beliebige Applets und Daten in ein SE geladen werden können. Folglich muss ein Issuer, der ein Applet auf ein SE laden möchte, dieses vom SE-Herausgeber signieren lassen oder das Applet muss gar selbst durch den SE-Herausgeber auf das SE geladen werden. Im Falle vom bilateralen Modell muss der MNO die Daten signieren, damit diese von der SIM akzeptiert werden.

Es gibt verschiedene Möglichkeiten, um ein Secure Element in einem Smartphone unterzubringen. Nachfolgend werden diese benannt, beschrieben und bewertet.

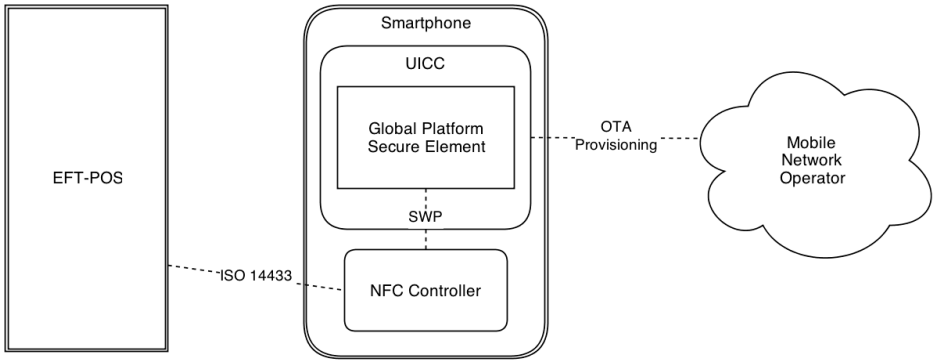

Abbildung 20: Situation, wenn die SIM als Secure Element verwendet wird

Secure Element auf SIM Eine SIM-Karte ist vom Prinzip her nicht anderes als eine Chipkarte. Die heutigen SIM-Karten weisen lediglich einen anderen Formfaktor auf. SIM-Karten haben, wie Chipkarten

auch, einen eigenen Prozessor, ein Betriebssystem sowie einen Datenspeicher. Bisher wird die SIM-Karte verwendet, damit MNOs ihre Kunden im Mobilfunknetz authentifizieren können.

Neuere SIM-Karten besitzen zusätzlichen Speicher und ein angepasstes Betriebssystem, welches es erlaubt, gegenüber dem NFC-Controller als Secure Element aufzutreten.

Wird die SIM-Karte als Secure Element verwendet, ergeben sich dadurch folgende Vorteile:

- Da jedes Smartphone bereits über eine SIM-Karte verfügt, müsste auf keine zusätzlichen Technologien und Geräte zurückgegriffen werden, um das Smartphone für Mobile Payment einsetzten zu können
- Wechselt der Consumer das Mobiltelefon, übernimmt er die SIM-Karte und somit alle darauf gespeicherten Karten-Daten.
- Über spezielle Netz-Kanäle können Daten und Applets "over the air" (OTA) auf die SIM geladen werden und vorhandene aktualisiert werden.

Aber auch folgende Nachteile:

- Läuft das Mobilfunk-Abo aus, oder wird der Netzzugang, beispielsweise infolge Zahlungsverzugs deaktiviert, sind auch die anderen Daten der SIM gesperrt. Dies bedeutet, dass je nach Art der Sperre auch keine Zahlungen mehr vorgenommen werden können [30].
- Wird die SIM-Karte, zum Beispiel infolge eines Defekts, ausgetauscht, müssen alle Applets neu geladen werden.
- Eventuell muss der Kunde zuerst beim MNO eine neue SIM-Karte verlangen, damit er die neuen Funktionen nutzen kann. Die zurzeit ausgegebenen Karten sind nicht für Mobile Payment mit NFC geeignet, weshalb sie ausgetauscht werden müssen. Aufgrund der unklaren Markt-Situation verzichten die Provider vorerst auf einen generellen Austausch der SIM-Karten aller Kunden [55].
- Es ist noch unklar, wie das Deployment durchgeführt werden kann, wenn sich das Smartphone im Ausland (also Roaming benützt) befindet. Dies würde zum Beispiel nötig, wenn der Kunde seine SIM-Karte im Ausland verliert und die darauf vorhandenen Karten gesperrt werden müssen sowie allenfalls eine neue SIM-Karte ausgestellt werden muss.
- Der MNO ist gegebenenfalls verpflichtet, dem Consumer eine neue SIM-Karte auszustellen. Dies hat nebst den Kosten für die SIM vor allem einen zeitlichen Verzug im Deployment-Prozess zur Folge.
- Wird das Mobilfunk-Abo gekündigt, werden auch alle auf der SIM enthaltenen Daten wertlos und müssen beim neuen Anbieter neu angefordert werden. Es muss technisch oder organisatorisch sichergestellt werden, dass die Credentials auf die neue SIM-Karte übertragen (oder neue erstellt) werden oder dem Kunden eine Plastikkarte zugestellt wird, wenn er keinen neuen Mobilfunkvertrag eingeht.
- Für den Consumer kann die Frage nach dem zuständigen Kundensupport verwirrend sein, da neben dem Issuer auch der MNO infrage kommt. Dies ist bei Wallets umso gravierender, weil mit einem Gerät mehrere Karten verwendet werden können und sich daher aus Sicht des Kunden nicht mehr so eindeutig voneinander abheben können.
- Der verfügbare Speicherplatz auf einer SIM-Karte ist beschränkt. Es könnte somit, bei vielen geladenen Karten, zu einem Speicherengpass kommen. Allenfalls müsste dem Consumer somit zugemutet werden, eine bereits installierte Karte zugunsten einer anderen entfernen zu lassen.

Der Ansatz, die SIM als Secure Element zu verwenden, ist die einzige Lösung, bei welchem der MNO ein wichtiger Teil des Prozesses wird. Daher wird diese Lösung auch von sämtlichen MNOs propagiert und gefördert. Der in der Schweiz führende MNO Swisscom hat aus diesem Grund beträchtlich in die Entwicklung

eines entsprechenden Systems sowie Ökosystem investiert [32]. Auch von Sunrise ist bekannt, dass sie bereits erste erfolgreiche Tests im Mobile Payment durchgeführt haben [56]. Allerdings entwickelt die Sunrise nicht wie die Swisscom von sich aus eine Lösung als *First Movers*, sondern folgt eher der Strategie eines *Fast Followers* [55].

Obwohl sich Banken und MNO noch nicht über die Vergütung geeinigt haben, hat diese Lösung die besten Chancen, sich auf breiter Front durchsetzen zu können.

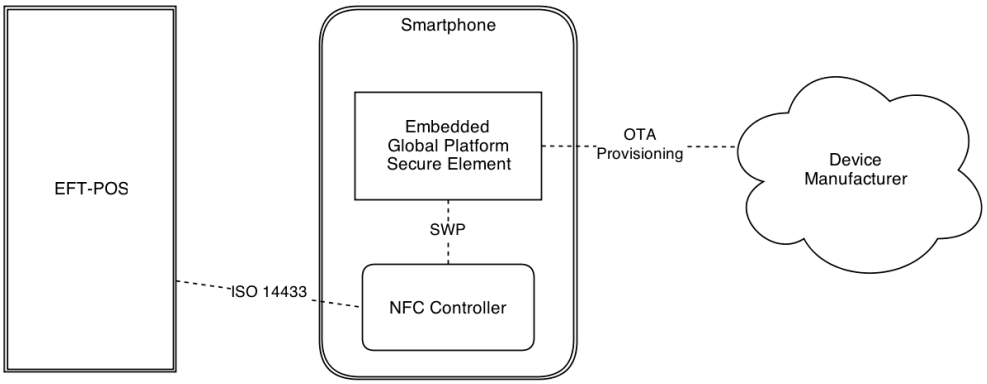

Abbildung 21: Situation, wenn das Secure Element direkt im Mobiltelefon verbaut ist

Embedded Secure Element Eine weitere Variante ist, das Secure Element direkt im Telefon zu verbauen. Es wird dazu direkt auf das Mainboard eines Smartphones aufgelötet oder ist schon im NFC-Controller integriert.

Fast alle Hersteller mit grossen Marktanteilen, die Smartphones mit NFC Funktionalität herstellen, haben bereits Geräte auf den Markt gebracht, in denen ein Secure Element fest verbaut ist [57].

Aus der Perspektive der Bank bietet ein fest verbautes SE nur den Vorteil, dass sie nicht mit einem MNO zusammenarbeiten müssen. Dafür müssen sie sich mit den grossen Herstellern von Mobile Devices einlassen. Nach Meinung von [8] ist dies aber noch die schlechtere Option, da die Banken nicht auf Augenhöhe mit den Unternehmen verhandeln könnten. Sie wären künftigen, beispielsweise strategischen, Änderungen der Hersteller ausgeliefert.

Weitere Nachteile:

- Nicht alle Mobile Telefone haben ein eingebautes SE, es könnten also nur gewisse Telefone für Mobile Payment genutzt werden. Besitzer anderer Geräte wären aussen vor.
- Wenn das Mobiltelefon einen Defekt hat, sind auch die Daten auf dem eingebauten SE verloren.
- Bei einem Austausch des Smartphones müssen alle Daten wieder angefordert werden.
- Dazu müssten auch entsprechende Prozesse implementiert werden, wie der Consumer die Daten wieder auf sein Smartphone laden kann. Je nachdem kann dafür wiederum eine Kooperation mit dem MNO nötig sein.
- Zu einem grossen Teil entscheiden die MNO, welche Mobiltelefone und welche Versionen davon auf den Markt kommen[25]. Die MNO könnten deshalb entscheiden, Geräte mit fest verbautem SE nicht

[25] So bietet beispielsweise Swisscom seit Kurzem nur noch die Version der Telefone an, die über NFC verfügen, wenn es mehrere Ausführungen gibt. [30]

in ihr Angebot aufnehmen und verfügen damit über eine erhebliche Verhandlungsmacht gegenüber dem Issuer.

Aus den genannten Gründen ist es nicht wahrscheinlich, dass sich das Modell mit embedded Secure Element in der Schweiz durchsetzen wird.

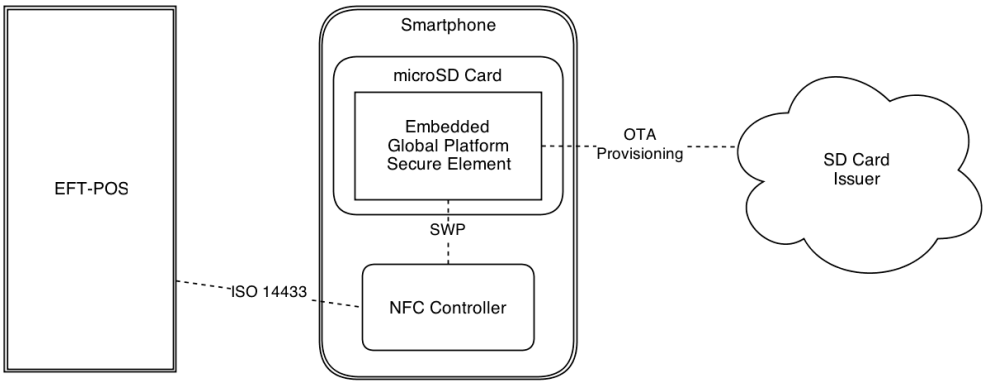

Abbildung 22: Situation, wenn sich das Secure Element auf einer SD-Karte befindet

Secure Element in MicroSD Als weitere Möglichkeit kommt der Einsatz einer SD-Karte als Secure Element in Betracht. Die SD Card Spezifikation sieht vor, dass der Zugriff auf den Flash Speicher gesichert werden kann. Solche SD-Karten, welche über ein zusätzliches Sicherheitsmodul verfügen, werden *Advanced Security SD* (ASSD) genannt [58].

Bei diesen SD-Karten ist ein bestimmter Speicherbereich so eingerichtet, dass er nicht über das normale IO-Interface zugänglich ist und somit nicht direkt über das Filesystem bearbeitet werden kann. Schreib- und Lesezugriffe sind nur über die gesicherten Schnittstellen der ASSD-API zugänglich [59, p.1].

Um auf den geschützten Speicher zugreifen zu können, muss der Host daher diesen speziellen ASSD-Modus beherrschen. Es ist unklar, wie viele aktuell am Markt verfügbaren Geräte diesen Modus unterstützen und damit in der Lage sind, eine SD-Karte als Secure Element zu akzeptieren.

Damit ein sicherer Kommunikationskanal zwischen NFC Controller und SE auf der MicroSD-Karte gegeben ist, ist es aber zwingend notwendig, dass dieser Modus unterstützt wird. Nur dann kann garantiert werden, dass die Kommunikation unabhängig vom Betriebssystem stattfindet und dadurch auch nicht von einem kompromittierten Betriebssystem verändert oder mitgehört werden kann.

Weiter setzt diese Art der Kommunikation natürlich eine physikalische Verbindung zwischen NFC-Controller und dem MicroSD-Controller voraus.

GoTrust SWP MicroSD GoTrust, ein Hersteller von Chip- und SD-Karten mit erhöhten Sicherheitsanforderungen, hat das Problem der fehlenden physikalischen Verbindung durch Überbrücken gelöst.

Dazu muss die SIM-Karte auf ein mit der MicroSD-Karte verbundenes Verbindungsstück geklebt werden. Dieses Verbindungsstück hat auf beiden Seiten die charakteristischen Kontaktflächen einer SIM-Karte. Die SWP-Befehle können von der MicroSD-Karte somit abgefangen werden, und die Karte kann auf SWP Befehle antworten.

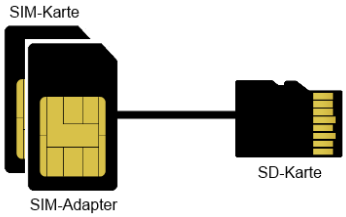

Abbildung 23: Die Grafik zeigt semantisch, dass die MicroSD-Karte über eine physikalische Verbindung mit der SIM-Karte verbunden wird.

Weitere Alternativen Nebst den vorgestellten Varianten gibt es noch einige weitere Alternativen, die hier lediglich der Vollständigkeit halber erwähnt werden:

- Es existieren Sticker, die ein Secure Element und eine RFID-Antenne beinhalten. Sie können dann auf eine beliebige Fläche, zum Beispiel auf den Rücken eines Mobiltelefons, geklebt werden. Diese Lösung stellen aber lediglich Contactless Smartcards dar, die in einem anderen Formatfaktor hergestellt werden. Sie verfügen über keine Verbindung zum Smartphone und können auch nicht durch dieses gesteuert werden.
- Es gibt MicroSD-Karten mit eingebauter RFID Antenne, die den Card Emulation Mode beherrschen.
- Für iPhone Geräte gibt es Schutzhüllen (*Jackets* genannt), die über eine RFID-Antenne verfügen. Die Antenne ist direkt mit einem Secure Element verbunden, welches in Form einer austauschbaren Chip-Karte vertrieben wird und in die Schutzhülle gesteckt werden kann. Zusätzlich kann die Hülle von der Stromversorgung des Gerätes profitieren. Dies stellt im Moment die einzige Lösung für Apples iPhone dar, welches über kein NFC verfügt und auch keinen MicroSD-Slot aufweist.

Zusammenfassung Eine der zentralen Fragen im Umfeld des Secure Element ist, wer dieses kontrolliert. Verdichtet kann man sagen, dass derjenige, welcher das Secure Element kontrolliert, auch den Kunden kontrolliert und sich damit (technisch) einen festen Platz im Zahlungsprozess sichern kann. Dieser Kampf um die Kontrolle ist einer der Gründe, weshalb sich Mobile Payment nur langsam entwickelt.

In Anbetracht seiner Universalität und seiner breiten Verfügbarkeit scheint der Weg, die SIM-Karte als Secure Element zu verwenden, der vorteilhafteste zu sein. Da die SIM-Karte weltweit standardisiert ist und jedes Smartphone über eine SIM verfügt, kann die Wallet-App entsprechen universell eingesetzt werden.

Zwischen Banken und MNO scheint Mobile Payment momentan vor allem wegen finanziell unterschiedlichen Vorstellungen festzustecken. Allerdings haben beide Parteien miteinander bereits erfolgreich Pilotprojekte durchgeführt ([17], [55], [8], [32]). Es ist also durchaus möglich, dass sich das Modell durchzusetzen vermag, der entscheidende Impuls, welcher die Issuer zur Adaption zwingt, dürfte vom Kunden aus gehen.

Technisch gesehen dürfte die Lösung mit einem eingebauten Secure Element die beste sein. Dies gründet im Wesentlichen auf der weniger stark reglementierten Kommunikation mit dem Secure Element. Der Zugriff auf das Secure Element kann von Hersteller relativ leicht in eine API gekapselt werden. Der Zugriff auf die SIM-Karte ist aus Sicht des Applikationsentwicklers relativ komplex und muss über ein spezielles Interface geschehen (das SIM Application Toolkit). Als Nachteil könnte sich herausstellen, dass die APIs von den Smartphone Hersteller gestaltet werden können und daher nicht Geräte übergreifend sind. Dies bedeutet Mehraufwand bei Softwareentwicklung und Wartung, weil Schnittstellen zu verschiedenen Geräten gebaut und getestet werden müssen. Allerdings ist fraglich, ob die Hersteller überhaupt bereit sind, die notwendigen APIs zu öffnen: Dadurch würden sie einen signifikanten Anteil der Kontrolle über den Kunden abgeben.

Solange dies nicht ein Alleinstellungsmerkmal für ein Smartphone darstellt, ist es unwahrscheinlich, dass die Hersteller dazu Hand bieten werden.

Die anderen Lösungsansätze weisen hauptsächlich technische Nachteile auf: So ist die Umsetzung über den SD-Slot aufgrund der unklaren Unterstützung durch die Smartphone-Hersteller problematisch. Weiter ist in diesem Fall auch das Distributionsmodell als kritisch zu beurteilen. Andere, wie beispielsweise der Ansatz von GoTrust, muten geradezu abenteuerlich an. Allgemein kann gesagt werden, dass alle Modelle für Mobile Payment zu einer Veränderung des Distributionsprozesses beim Issuer führen.

4.1.5 Issuer

Wie ausführlich dargelegt, verändert sich das Geschäftsumfeld des Issuer durch die Einführung von Mobile Payment am stärksten.

Die Prozesse zur Kartenerstellung und die Zusammenarbeit zwischen Issuer und Card Manufacturer sind gut eingespielt. Daher können die Prozesse der Issuer kosteneffizient betrieben werden.

Die Lösung, bei der die SIM-Karte als SE verwendet wird, stellt die Issuer vor das Problem, dass sie ihren bisherigen, kostengünstigen Prozess aufgeben müssen und mit einem externen ersetzen. Da der MNO eine Art “Mietpreis” für den Platz auf der SIM-Karte verlangt, entstehen dem Issuer dadurch variable Kosten, welche er nicht weiter beeinflussen kann. Bisher verursachte vor allem der Aufbau der notwendigen Infrastruktur Fixkosten, welche nun relativ wenig Kosten für eine einzelne Karte verursachen. Die Kosten für den Platz auf der SIM schmälern den Gewinn des Issuers. Anderenfalls muss der die Mehrkosten seinem Kunden, also der Bank verrechnen. Da in der Schweiz Issuer und Bank eng verbunden sind, dürfte dies darauf hinauslaufen, dass die Kosten dem Consumer verrechnet werden. Die Issuer gehen nicht davon aus, dass der Kunde bereit sein wird, den von der Swisscom geforderten Preis zu bezahlen [8].

Modelle, welche nach wie vor auf ein physikalisch zu versendendes Objekt (wie beispielsweise eine SD-Karte) setzen, könnten vom Issuer adaptiert werden. Der Prozess unterscheidet sich dabei nicht wesentlich vom bisher durchgeführten. Dabei könnte sich der Issuer zudem in eine strategisch günstige Position bringen, in dem er der Verwalter des Secure Elements wird. Allerdings kranken diese Modelle auch an der unklaren Distributionslage. Da bisher jeder Issuer seine Karten unabhängig versendet, werden sich die Issuer ein Konzept überlegen müssen, welches es ermöglicht, dass mehrere Karten auf ein einzelnes Secure Element gespeichert werden können.

Da sich die Supply Chain der Issuer bei den wenigen Card Manufacturer (welche in diesem Fall die SD-Karten provisionieren) konzentriert, wäre es auch denkbar, dass die Card Manufacturer als Service Provider auftreten. Aus Sicht der Issuer ist dies aber genau so wenig erwünscht, wie dass der MNO den Markt betritt. Auch in diesem Fall würden sie in die Abhängigkeit eines anderen Players rutschen. Mit dem einzigen Unterschied, dass dieser Player schon im Modell tätig ist. Im Rahmen dieser Studie wurde das Geschäftsmodell des Card Manufacturer nicht weiter untersucht. Es können daher keine Aussagen darüber gemacht werden, inwieweit sich für den Card Manufacturer eine Chance ergibt, seine Wertkette zu erweitern.

4.1.6 Benutzer

Die Benutzung der NFC-Funktionalität ist für den Benutzer extrem einfach zu erlernen, da das Berühren mit dem Smartphone sehr intuitiv ist. Andererseits hat NFC eine Vielzahl von Business Cases für verschiedene Industrie- und Dienstleistungszweige hervorgebracht. Beides Gründe dafür, weshalb diese Technologie zurzeit eine erhöhte Aufmerksamkeit zu Teil wird.

Während die meisten Personen bereits mit dem Umgang von kontaktlosen Karten (Badges, Skitickets, Schlüssel-Chips, Studenten-Karten) vertraut sind, fehlt bei vielen noch das Bewusstsein, dass diese Technologie auch in Smartphones eingebaut ist. So haben Untersuchungen von [6] gezeigt, dass Besitzer von aktuellen Smartphones nicht über die verbaute NFC Funktionalität Bescheid wussten, und mit dem Namen oder den gängigen Signeten nichts Korrektes assoziieren konnten.

Es zeigte sich zudem, dass Benutzer zuerst lernen mussten, dass sie das Smartphone praktisch ganz an die Funkfläche halten mussten, damit eine Übertragung zustande kommt (obwohl dies bei drahtlosen Karten gang und gäbe ist).

Das Benutzerverhalten kann aber durch entsprechende Werbung und einfache Piktogramme gut geschult werden. Nach einmaligem Erfolg haben die meisten Consumer die Anwendung bereits verstanden [6].

Das Benutzerverhalten wird im Rahmen der Arbeit nicht weiter betrachtet.

4.1.7 Fazit

Die Gründe für das schleppende Vorankommen von Mobile Payment in der Schweiz haben mehrere Ursachen, welche teilweise ineinandergreifen.

Einerseits ist dies der **Card Emulation Mode**, in welcher der NFC-Controller gebracht werden muss, um eine Zahlung auslösen zu können. Dieser Modus ist bei den meisten Geräten nicht programmatisch erreichbar (kein API). Allenfalls ist es durch Modifikation des Betriebssystems möglich; dabei erlischt aber häufig die Herstellergarantie für das Gerät. Daher ist dies keine Lösung für eine massenmarkttaugliche Software.

Allenfalls ist es durch Ausnützen von Fehler bei der Implementation möglich, die Geräte in den Card Emulation Mode zu bringen; eine solche Lösung funktioniert dann aber nur auf einer bestimmten Version des Betriebssystems, häufig sogar nur auf bestimmten Geräte-Modellen. Daher ist es jederzeit möglich, dass durch ein Update die ausgenutzte Lücke gestopft wird und die Software nicht mehr funktioniert. Weiter muss in einem solchen Fall berücksichtigt werden, dass der Hersteller der Software allenfalls schadenersatzpflichtig wird, wenn er durch das Ausnutzen einer nicht dokumentierten Schnittstelle Schaden am Gerät des Kunden erwirkt.

Dass der Card Emulation Mode nicht für normale Entwickler zugänglich ist, ist sicherlich auch ein hemmendes Element für die Entwicklung von Lösungen im Mobile Payment-Bereich. Es kann gerade im Umfeld der Smartphone-Entwicklung beobachtet werden, dass die Verfügbarkeit von APIs ein wesentlicher Faktor für das Aufkommen von neuen, innovativen Produkten darstellt (beispielsweise Gyroskop-Sensoren).

Aus all diesen Gründen wurde von der Verwendung des Card Emulation Mode abgesehen und eine Lösung gesucht, welche diesen nicht benötigt. Dieser Ansatz bietet auch den Vorteil, dass die volle Funktionalität von NFC ausgeschöpft werden kann (vgl. Lösungswahl).

Der zweite Faktor ist das **Secure Element**. Obwohl durch die EMV nicht vorgeschrieben, wird das Secure Element von allen untersuchten Card Schemes verlangt. Dabei wird allerdings nicht verlangt, dass das Secure Element als Chipkarte ausgestaltet sein muss. Die Card Schemes scheiben lediglich gewisse Anforderungen vor, welche das SE erreichen muss, typischerweise in Form von Verweisen auf andere Standards, wie beispielsweise *PCI DSS*[26] oder *FIPS*[27].

Da es nicht nötig ist, das SE als Chipkarte auszulegen, sind auch Alternativen dazu möglich, sodass auf eine Chipkarte SIM oder ein embedded SE) verzichtet werden kann. Wird das Secure Element ausgelagert

[26] Siehe https://www.pcisecuritystandards.org/security_standards/.
[27] Siehe http://csrc.nist.gov/publications/PubsFIPS.html#140-2.

(beispielsweise in eine Cloud), muss der Zugriff auf diesen Server entsprechend gesichert sein. Die Herausforderung stellt dabei hauptsächlich die Authentifizierung des Benutzers dar, weil sichergestellt werden muss, dass die Credentials nicht kopiert und auch nicht unberechtigt verwendet (zum Beispiel durch eine Malware) werden.

Einen wichtigen Faktor für die Sicherheit des Card Emulation Modes stellt die direkte Verbindung zwischen SIM-Karte und NFC-Controller dar. Da diese beiden Elemente über eine dedizierte Leitung verbunden sind, ist es technisch nicht möglich, dass das Betriebssystem die übertragenen Daten manipulieren oder abhören kann. Daher bietet dieser Ansatz einen hohen Schutz gegen ein mit Viren infiziertes Betriebssystem. Allerdings ist es möglich, dass der NFC-Controller zum Ziel des Angriffs wird und es damit möglich wird, dass die Kommunikation zwischen SIM-Karte und Controller kompromittiert wird. Ebenso sind Angriffe auf die SIM-Karte (bzw. das Secure Element) denkbar, welche ja ebenfalls über eine Schnittstelle zum Betriebssystem verfügt. Ein Analyse der Sicherheit liegt allerdings nicht im Scope dieser Thesis.

Daher scheint die Verwendung der SIM-Karte zur Steuerung des Card Emulation Mode offensichtlich, weil damit beide Probleme angegangen werden können.

Auch die **Device Manufacturer**, welche die NFC-Chips in die Geräte einbauen und entscheiden, ob das Gerät beispielsweise den ASSD-Modus unterstützt, spielen ein Rolle. Für sie entsteht durch Mobile Payment die Möglichkeit, das Secure Element anzubieten und damit selbst zu einem unverzichtbaren Teil des Zahlungsprozess (TSM) zu werden. Durch das Business-Model entsteht für den Hersteller kein Grund, ein Secure Element in das Gerät zu verbauen und dann die Kontrolle an jemand anderen abzugeben. Jeder Teilnehmer des Ökosystems möchte einen Teil der Kontrolle über dieses behalten.

Ein letztes Kennzeichen der Problemdomäne ist der Unwille der **Issuer** (beziehungsweise den dahinter stehenden Banken), sich mit den MNO auf ein gemeinsames Business Modell zu einigen. Genau wie die Probleme bei der Umsetzung (also der Aktivierung des Card Emulation Mode) stellt das (ökonomisch verständliche) Sträuben der Issuer gegen Veränderungen an ihrem Geschäftsmodell ein Grund dar, weshalb sich Mobile Payment bisher in der Schweiz nicht durchsetzen konnte. Zwar hat sich Swisscom sichtlich Mühe gegeben, die bestehenden Player möglichst in ihre Lösung einzubringen (vgl. Swisscom Tapit). Das Kooperationsmodell ist sehr gut durchdacht, behält möglichst viele bisherige Schnittstellen bei und erleichtert damit die Einführung für die bestehenden Parteien.

Der bei den bestehenden Lösungen dominierende Evolutionsgedanke (statt Revolution) ist gleichzeitig die grösste Schwäche des Models. Das Ziel, möglichst alle bisherigen Parteien im Business Modell zu belassen führte nicht wie gewünscht zur allgemeinen Akzeptanz (wobei unklar ist, inwieweit das Zögern der Issuer Säbelrasseln ist). Ein derartiges Ansinnen hat auch zwangsläufig eine Kostensteigerung zur Folge: Da nun mehr Akteure in der Wertekette sind, wovon keiner bereit sein dürfte, auf Gewinne, welche er im angestammten Geschäft gemacht hat, zu verzichten, wird der Service für den Consumer teuerer. Dies untermauern auch Aussagen auch den durchgeführten Interviews mit den Issuern [8], [17].

Als Letztes müssen auch die **hohen Markteintrittsbarrieren** für neue Marktteilnehmer erwähnt werden. Da der Zahlungsprozess stark reguliert ist, ist es für einen Newcomer nicht einfach, mit den Banken in Konkurrenz zu treten. Bisher konnten sich nirgends auf der Welt alternative Zahlsysteme in grossem Stil durchsetzten, welche nicht direkt oder indirekt auf den Banken aufsetzen. Eine Alternativwährung stellt *BitCoin* dar, welche in den vergangenen Wochen auch in den Massenmedien Aufmerksamkeit gefunden hat. Es darf aber bezweifelt werden, dass sich daraus eine langfristig existierende Währung ergibt. Allerdings ist BitCoin in den vergangenen Monaten vermehrt wegen angeblicher Geldwäscherei in Verruf geraten.

So greifen auch scheinbar unabhängige grosse Zahldienstleister wie *PayPal* auf das Abrechnungssystem von Kreditkarten zurück. Allerdings ist es bei PayPal auch möglich, Geld auf ein PayPal-Konto zu überweisen. Dies zeigt exemplarisch, wie abhängig das europäische Zahlungssystem von den bestehenden Lösungen ist und wie schwierig es ist, eine neue Lösung zu etablieren. Die Tatsache, dass im Wesentlichen Banken den

Zahlungsablauf kontrollieren und wie erwähnt stark mit den Issuer verbunden sind, führt dazu, dass die Banken über die vergangenen Jahre erfolgreich Eintrittshemmnisse aufbauen konnten.

4.2 Bisherige Produkte und Ansätze

Das Rollout von Terminals, an welchen kontaktlos bezahlt werden kann, ist derzeit im Gang. Allerdings ist diese Funktion noch nicht an allen Terminals aktiviert [17]. So beispielsweise noch nicht an den Billettautomaten des Zürcher Verkehrs Verbundes oder auch den Terminals bei Ikea.

Ebenso werden kontaktlose Bezahlkarten schon seit Mitte 2012 herausgegeben und können an entsprechenden Terminals zum kontaktlosen Bezahlen eingesetzt werden.

Es sind bereits einige Bezahlsysteme am Markt, welche Mobile Payment unterstützen oder dies vorhaben. Alle dieser Lösungen lassen sich an den aktuellen Terminals einsetzen, was bedeutet, dass sie auf den *Card Emulation Mode* (siehe NFC Card Emulation Mode) zurückgreifen. Wie im Kapitel Problemdomäne erwähnt wird, bringt dieser Modus einige Probleme mit sich. Konkret setzen all diese Lösungen voraus, dass mindestens ein weiterer Stakeholder am Zahlungsprozess teilnimmt.

Im Folgenden werden die wichtigsten Lösungen kurz vorgestellt.

4.2.1 MasterCard PayPass

MasterCard nennt sein Bezahlsystem *PayPass* und nutzt diese Bezeichnung für kontaktloses Bezahlen im Allgemeinen. Momentan wird nicht zwischen Bezahlen mit Karte und Smartphone unterschieden, eventuell wird in Zukunft die Lösung für Smartphones unter dem Namen *Tap&Go* vermarktet [60].

Die Lösung für Smartphones ist aber noch nicht öffentlich erhältlich, sondern befindet sich noch in einem geschlossenen Test [61]. Aus diesem Grund sind auch nur wenige Informationen darüber erhältlich, wie das System funktioniert.

In [61] wird erwähnt, dass der Kunde das Smartphone direkt von der Bank erhalten soll. Dies lässt keinen Rückschluss darauf zu, wie der Deployment-Prozess für die Credentials aussieht oder wo und wie diese auf dem Smartphone gespeichert werden. Da es im europäischen Umfeld eher unwahrscheinlich ist, dass sich eine Bank als Verkäufer von Mobiltelefonen etabliert, muss davon ausgegangen werden, dass es sich dabei um den Deployment-Prozess für die Testphase handelt und bei der Markteinführung auf ein anderes Konzept gesetzt wird.

MasterCard stellt ein SDK bereit, mit welchem Wallet-Programme für Geräte mit Android- und Blackberry-Betriebssystem entwickelt werden können. Das SDK ist allerdings nur unter strengen Auflagen erhältlich, weshalb kein Evaluation stattfinden konnte [61].

4.2.2 Visa PayWave

PayWave ist ein sehr ähnliches Produkt wie PayPass: So verwendet Visa den Namen ebenfalls vornehmlich für Karten.

Auch der Entwicklungsstand ist dem von MasterCard ähnlich. So ist ein SDK erhältlich, um Wallets für virtuelle PayPass-Karten zu entwickeln. Im Gegensatz zu MasterCard ist das SDK aber öffentlich (gegen eine entsprechende Gebühr) erhältlich. Kommerzielle Produkte sind derzeit nicht bekannt. Insbesondere existiert kein Produkt, welches das PayPass SDK verwendet und auf dem Schweizer Markt erhältlich ist.

Für PayPass sind auch einige Architekturdokumente erhältlich [62], ohne dass zur Einsicht eine Entwicklerlizenz nötig ist. Daraus geht hervor, dass sich auch Visa an einer Umsetzung in Zusammenarbeit mit dem MNO orientiert. Im Weiteren sind die Ausführungen vage, insbesondere wird nicht darauf eingegangen, wie sich Visa die Kooperation zwischen Issuer und MNO genau vorstellt. Visa legt sich explizit nicht fest, wie das SE technisch zu realisieren ist, und lässt offen, ob es sich auf der SIM, im Gerät oder auf einer MicroSD-Karte befindet). Jedoch wird die Option, das SE in die Cloud zu bringen, nicht erwähnt.

Da sich Visa - wie MasterCard - an den bereits bekannten Modellen orientiert, wurde auf eine weitere Untersuchung der Funktionsweise verzichtet. Es ist davon auszugehen, dass die SDKs von MasterCard und Visa im Wesentlichen als Grundlage für Testapplikationen und zum erleichterten Umsetzen von den UI-Guidelines der Card Schemes dienen sollen.

4.2.3 Google Wallet

Im Mai 2011 präsentierte Google erstmals sein Produkt *Wallet* [2], welches einiges an Aufmerksamkeit auf sich gezogen hatte. Damit war es in Amerika erstmals einer breiten Öffentlichkeit möglich, Mobile Payment zu verwenden.

Prinzipiell ermöglicht Google Wallet das Bezahlen mit Kreditkarten von verschiedenen Partnern. Vorerst ist es aber nur möglich mit einer Prepaid MasterCard zu bezahlen [63]. Ausserdem können Kunden von Citibank eine normale MasterCard auf das Smartphone laden und damit bezahlen. Momentan ist Google Wallet auf den US-amerikanischen Markt beschränkt.

Dass es selbst einem Megakonzern wie Google innerhalb von zwei Jahren nicht gelungen ist, weitere Banken zur Zusammenarbeit zu bewegen, zeigt symptomatisch das Problem, an welchem das System krankt: Für die Stakeholder (allen voran die Issuer) gibt es zu wenig Anreize das System einzusetzen, weil sie dabei Marge einbüssen [64].

Neben der Bezahlfunktion erlaubt es Google seinen Partnern auch, andere Formate wie beispielsweise Gutscheinkarten im Wallet anzubieten [65, pp.19–23].

Technisch wird beim Google Wallet jede Bezahlung über eine von Google herausgegebene MasterCard abgewickelt, und erst in einem weiteren Schritt der eigentlichen Kreditkarte belastet. Dies ermöglicht eine grosse Flexibilität und verhindert, dass bei jeder neu ausgestellten Karte ein OTA-Update des SE nötig wird. Google Wallet geht damit deutlich weiter als die anderen Ansätze, indem Google selbst einen Teil der Zahlungsabwicklung übernimmt und nicht nur das Secure Element zur Verfügung stellt. Dieser Ansatz abstrahiert von der zugrunde liegenden Zahlarchitektur, was die Verwendung durch Entwickler vereinfachen kann und die Lösung universeller macht. Allerdings birgt diese Strategie umso mehr die Gefahr, dass sich die bisherigen Stakeholder in ihrem Geschäftsmodell angegriffen fühlen und daher die Lösung nicht unterstützen. Dies wäre eine mögliche Erklärung, weshalb Google ausser Citibank noch keinen weiteren Partner vorweisen kann.

Eine weitere technische Feinheit ist, dass Google Wallet mit dem Magstripe Datensatz arbeitet, und nicht, wie die Konkurrenz, mit dem EMV-Verfahren, welches bei PayPass / PayWave und auf den Chipkarten zum Einsatz kommt.

4.2.4 Swisscom Tapit

Swisscom entwickelt zurzeit *Tapit*, ein Wallet-System, welches Funktional dem Wallet von Google ähnlich ist. Es soll “mit mindestens einer Bezahlkarte” [32] im Oktober 2013 auf den Markt kommen.

Swisscom fungiert somit als *First Mover* im Markt und wird voraussichtlich als erster Player eine Wallet-Lösung auf den Schweizer Markt bringen. Um eine Adaption am Markt zu erreichen, ist das System offen definiert; Swisscom stellt dabei die SIM-Karte als Secure Element seinen Kunden zur Verfügung. Verschiedene Anbieter können anschliessend Applikationen entwickeln, welche auf die SIM-Karte als SE zurückgreifen. Allerdings gewährt Swisscom den Anbietern keinen direkten Zugriff auf die SIM-Karte, sondern verwaltet die Applets der Anbieter selbst. Vermutlich hat diese Entscheidung nebst sicherheitstechnischen Überlegungen auch zum Ziel, die Kontrolle über die SIM-Karte nicht abgeben zu müssen. Weiter kann Swisscom auch einen höheren Preis fordern, weil sie damit auch mehr Service übernehmen [32][30].

Mit dem offenen Design sollen mit Tapit neben Bezahllösungen auch andere Systeme, wie beispielsweise Zugangssysteme, Studentenkarten, Billette oder Abonnements entstehen. Swisscom verlangt von jedem Anbieter pro aktivierte Karte eine regelmässige Gebühr für die Infrastruktur und als Entschädigung für die Entwicklungskosten [30].

Im Unterschied zu Google versucht Swisscom, die Geschäftsmodelle der bisherigen Player möglichst unangetastet zu belassen. Das gesamte Ökosystem, welches von Swisscom aufgebaut wurde, ist darauf ausgelegt, die bestehenden Strukturen möglichst unangetastet zu lassen. So soll der Issuer beispielsweise weiterhin über dasselbe Interface die Personalisierungsinformationen an seinen bisherigen Card Manufacturer (Swisscom arbeitet hierzu mit Trüb zusammen) liefern können.

Weitere technische Informationen über das Produkt werden nicht publiziert. Aufgrund der Interviews konnte allerdings noch in Erfahrung gebracht werden, dass Tapit auf einer Basisapplikation der Firma Nexpert basiert, welche dann von Swisscom selbst weiterentwickelt wurde [17].

4.3 Umsetzungsmodelle

Um eine Lösung für die unter Problemdomäne erläuterten Schwierigkeiten zu finden, werden mehrere verschiedene Szenarien erörtert. Nachfolgend werden Ansätze für eine Umsetzung vorgestellt, die geeignet sind, einen oder mehrere Aspekte der Hindernisse zu beseitigen. Dabei wird primär betrachtet, ob der Lösungsansatz geeignet ist, das primäre Forschungsziel zu erreichen, dass der Issuer nicht auf die Kooperation mit einem unliebsamen Partner angewiesen ist.

Weiter werden im Rahmen einer umfassenden Betrachtungsweise die Herausforderungen des Ansatzes und die Vor- und Nachteile diskutiert.

Die Betrachtung erfolgt dabei aus dem Blickwinkel der Forschungsfrage, also mit Fokus auf die Finanzindustrie.

4.3.1 Klassisch

Es wird das von den MNO und der GSMA propagierte Verfahren umgesetzt. Als Speicher für die Credentials wird ein in einer SIM-Karte integriertes Secure Element genutzt. Da ein Secure Element vorhanden ist, kann der *Card Emulation Mode* zur Datenübertragung genutzt werden.

Die Personalisierung findet über das Mobilfunknetz des MNO statt, der die SIM-Karte herausgegeben hat. Dieser, oder ein Dritt-Anbieter, stellen eine App zur Konfiguration des Secure Elements zur Verfügung (*Wallet*-App).

Herausforderung Für die Umsetzung muss das Smartphone mit einer SIM-Karte ausgerüstet werden, welche über einen genügend grossen Speicher verfügt, damit alle Applets Platz finden.

Für die Entwicklung müsste somit eine entsprechende SIM-Karte zur Verfügung stehen. Ausserdem müssten die kryptographischen Schlüssel der SIM-Karte bekannt sein, damit das Applet auf die Karte hochgeladen werden kann. Dazu wäre ausserdem ein entsprechendes Karten-Gerät notwendig.

Vorteil Dieser klassische Ansatz wurde von mehreren Stakeholdern (MNO und Issuern) in der Schweiz gestestet und funktioniert, ohne dass Änderungen oder Anpassungen auf der Terminal-Seite notwendig sind. Es kann sicher ein Showcase entwickelt werden. Das gesammelte Wissen ist wertvoll, da, zumindest zu in den kommenden Jahren, dieser Ansatz auch von allen Stakeholdern technisch unterstützt wird.

Nachteil Der Ansatz löst das untersuchte Problem nicht, da der Issuer eine Kooperation mit dem MNO eingehen muss.

Der Ansatz bietet keine Antwort auf die Aufgabenstellung. Er liefert lediglich ein Showcase.

4.3.2 Secure Element Emulation

Das Secure Element würde durch Software emuliert; zum Übertragen der Daten allerdings weiterhin auf den *Card Emulation Mode* gesetzt. Dazu sind Änderungen im Betriebssystem nötig.

Herausforderung Eine solche Veränderung müsste, damit sie sinnvoll wird, in den Hauptentwicklungszweig des Betriebssystems eingebracht werden. Da solche aber zur Hauptsache von Unternehmen betreut werden und diese kein Interesse haben, ihre eingebauten Secure Elements und ihre Partner (MNOs) zu Konkurrenz zu machen, scheint eine Integration unwahrscheinlich.

Vorteil Alle Apps könnten fortan ein eigenes virtuelles Secure Element mit sich bringen.

Nachteil Da eine permanente Integration ins Betriebssystem unwahrscheinlich ist, müsste eine eigene Version dessen unter Leitung der Issuer entwickelt, gewartet und bei den Kunden installiert werden. Dies ist sehr unrealistisch.

4.3.3 Shared Cardlet

Es wird, wie bei der klassischen Variante, ein Applet im Secure Element (SIM-Karte oder intern) installiert. Dieses Applet würde aber so programmiert sein, dass es von verschiedenen Unternehmen benutzt werden könnte und diese sich die Kosten teilen würden.

Bevor das Smartphone zum Zahlen an das Terminal gehalten wird, muss der Benutzer über eine App entscheiden, welches Karte er nun benutzen will. Eine Standard-Karte wäre auch denkbar.

Wird nun das Gerät zum Bezahlen ans Terminal gehalten, sendet das Secure Element die Daten der zuvor ausgewählten Karte ans Terminal.

Bei den Gesprächen mit der Swisscom hat sich herausgestellt, dass sie dieses Verfahren für die Bezahlfunktionen verwendet, damit der beschränkte Speicherplatz auf der SIM möglichst gut ausgenutzt werden kann. Verschiedene Datensätze pro Karte sind kleiner als ein eigenes Applet pro Bezahlkarte.

Herausforderung Es müsste Wissen über die Entwicklung von Applets für Bezahlkarten erarbeitet werden. Ein solches Applet müsste zudem vom entsprechenden Card Scheme erstmal zertifiziert werden.

Vorteile Das Verfahren funktioniert auch ohne aktive Internetverbindung, wie dies im Ausland der Fall sein kann. Der Anwender hat die volle Kontrolle und hat seine persönlichen Daten jederzeit bei sich.

Nachteile Es ist fraglich, ob die schweizer MNO ein solches Applet von einem externen Anbieter zulassen würden, zumal Swisscom bereits den gleichen Ansatz gewählt hat.

4.3.4 Shared Cardlet - Variante “at back-end”

Im Gegensatz zur vorherigen Variante wird hierbei immer mit der gleichen Karteninformation am Terminal bezahlt. Erst beim Verbuchen der Zahlung wird unterschieden, über welches Konto verbucht werden soll.

Herausforderung Das Wissen über Backend-Infrastruktur müsste zuerst erarbeitet werden. Es ist ausserdem nicht klar, wie und wann der Benutzer entscheiden soll, welches Konto er belasten möchte.

Vorteile Gegen diese Variante kann ein MNO keine technischen Einwände erheben. Die Umsetzung erfolgt im Backend, welches unabhängig von jenen ist.

Nachteile Für proaktives oder reaktives Auswählen des Kontos müsste Internet zur Verfügung stehen, was gerade im Ausland nicht immer gegeben ist.

Es ist auch unklar, wie beispielsweise eine Storno-Buchung umgesetzt werden könnte, bei der Geld zurückerstattet wird.

4.3.5 Tunneling

Beim Tunneling-Ansatz wird das gesamte EMV-Protokoll über ein anderes NFC-Protokoll übertragen, anstatt auf den *Card Emulation Mode* zurückzugreifen. Im konkreten Fall wird dabei der *Peer-To-Peer*-Modus von NFC verwendet. Dazu müssen die EMV Rohdaten in NDEF Nachrichten gekapselt werden. Das beim Peer-To-Peer-Modus verwendete Protokoll *SNEP* beherrschen fast alle NFC fähige Smartphones.

Der Peer-To-Peer-Modus wurde deswegen gewählt, weil dieser Modus als einziger explizit für bidirektionale Kommunikation vorgesehen wurde. Für den vorgesehen Anwendungsfall stellt dieser Modus daher die erste Wahl dar.

Es müsste die Terminal-Software angepasst werden sowie ein kompatibler Smartphone-Client entwickelt werden.

Auch müssen die Timing-Restriktionen eingehalten werden. Die Timing Restriktionen sind bei EMV aber sehr grosszügig ausgelegt. So ist es beispielsweise überhaupt erst möglich, eine Relay Attacke, wie in [65] beschrieben, durchzuführen.

Herausforderung Gewisse Änderungen an bestimmten Teilen der Terminalsoftware bedürfen einer Zertifizierung durch die entsprechend unterstützten Card Schemes. Diese Teile dürfen nicht verändert werden.

Das sichere Speichern der Karteninformationen auf dem Mobiltelefon stellt eine weitere Herausforderung dar, weil nicht auf ein SecureElement zurückgegriffen werden kann.

Vorteile Die Kommunikation wird über einen kontrollierbaren Kanal abgewickelt, auf dem auch weitere Informationen übertragen werden könnten. Die EMV-Daten stellen dabei lediglich einen bestimmten Typ von Daten dar, der übertragen werden kann. Beispielsweise könnte so Loyalty-Funktionen einfach eingebaut werden oder es könnte bei einem Parkplatz die Nummer des Parkfelds, auf dem der Consumer sein Fahrzeug abgestellt hat, von der Parkuhr dem Smartphone mitgeteilt werden.

Nachteile Terminal-Update Termine gibt es nur einige wenige im Jahr. Die Software muss viel stabiler ausgelegt und fehlertoleranter entwickelt werden, was zusätzlichen Aufwand bedeutet.

Durch Anpassen der Terminal-Software wird diese komplexer und damit schwerer zu zu warten.

4.3.6 Tunneling – Variante Cloud

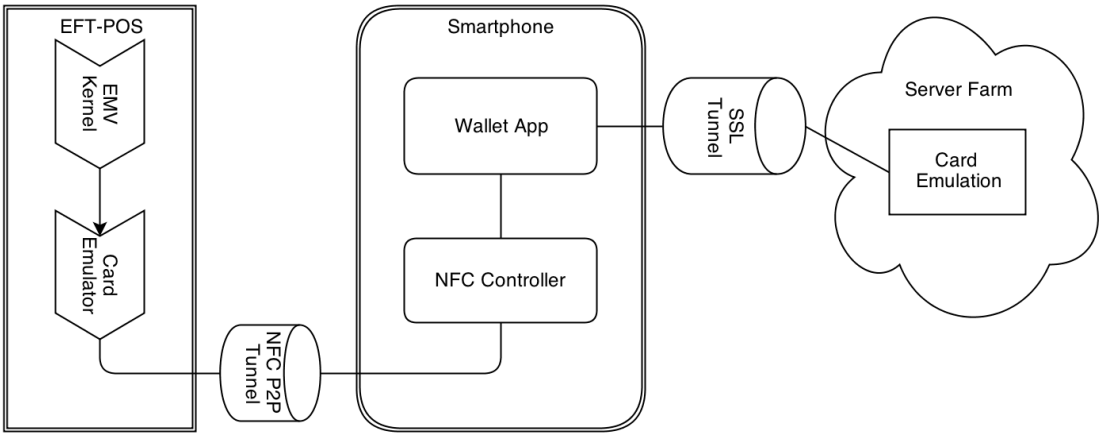

Abbildung 24: Situation, wenn als Übertragungsprotokoll NFC Peer-To-Peer eingesetzt wird und die Daten des SE auf einem sicheren Server vorgehalten werden.

Eine Variante der vorherigen Lösung wäre, die Kartendaten nicht auf dem Telefon, sondern in der *Cloud*, also auf einem Server, zu speichern.

Herausforderung Der sichere Transport dieser sensiblen Daten stellt die grösste Herausforderung dar.

Vorteile Die Daten sind vor Geräte-Verlust geschützt und es kann dank homogenem und kontrollierbarem Umfeld einfacher sichergestellt werden, dass die Daten sicher gespeichert sind.

Nachteile Es ist nicht mehr möglich, ohne aktive Internetverbindung zu bezahlen.

4.4 Lösungswahl

Als umzusetzende Lösung wurde die Tunneling-Lösung gewählt. Zur Auswahl wurde eine Matrix erstellt, in der die verschiedenen Aspekte bewertet wurden.

	Klassisch	SE Emulation	Shared Cardlet	Shared Cardlet (Backend)	Tunneling
MNO Abhängigkeit	-2	+1	-1	+2	+2
Aufwand	-2	-2	+1	+1	+2
Umsetzbarkeit	-2	-2	0	+1	0
Risiko	0	-2	0	-2	0
Nötiges Know-how	-2	-2	-2	-2	+1
Total	**-8**	**-7**	**-1**	**0**	**+5**

Tabelle 4: Bewertungsmatrix der einzelnen Varianten. Die beiden Tunneling-Varianten wurden als gleichwertig bewertet und sind deshalb unter dem Titel *Tunneling* zusammengefasst.

Die *Tunneling*-Lösung und die *Shared Cardlet (Backend)* Lösung können als Einzige auf die Beteiligung eines MNO verzichten. Da die Tunneling-Variante einfacher umgesetzt werden kann und bestimmt auch genug Know-how verfügbar ist, fiel der Entscheid zur Umsetzung auf diese Lösung.

Um die Anzahl der für einen Showcase benötigten Komponenten möglichst gering zu halten, wird die Tunneling-Lösung ohne Cloud-Anbindung umgesetzt. Die Erweiterung auf die Variante mit Cloud-Anbindung wäre aber ohne grösseren Aufwand möglich. Es muss lediglich die Kommunikation zum virtuellen Secure Element auf einen Server umgeleitet werden.

Die Lösung hat ausserdem den einmaligen Vorteil, Loyalty Systeme einbinden zu können, da grösstenteils auf die angestammten Schnittstellen verzichtet wird.

5 Umsetzungsbericht

5.1 Definition

Beim Prototyp soll gezeigt werden, dass eine Übertragung der EMV-Daten vom Terminal via NFC *Peer-To-Peer* (P2P) auf ein Handy und von dort weiter funktioniert. Dazu wird ein Terminal-Simulator eingesetzt, der die EMV-Kommunikation initialisiert und über ein Socket kommuniziert. An diesem Socket soll die terminalseitige Software die Kommunikation aufgreifen und über NFC P2P an die Smartphone Applikation übertragen.

Die Smartphone Applikation soll die empfangenen Daten an einen weiteren Service, beispielsweise an eine andere App oder an einen Webservice, weiterleiten.

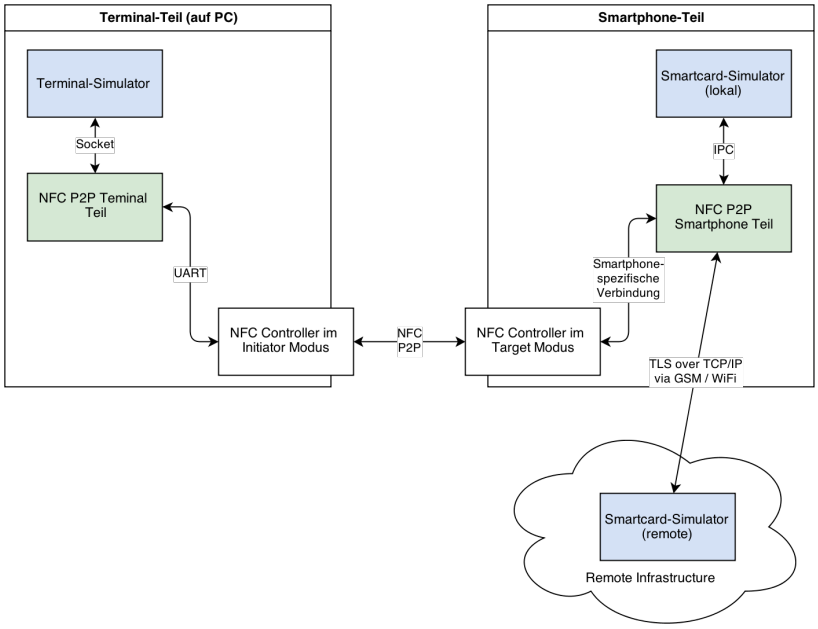

Abbildung 25: Grüne Kästchen zeigen Teile, die während dieser Arbeit umgesetzt werden. Blaue Kästchen symbolisieren Teile, die nicht umgesetzt werden (bzw. bereits existierende Komponenten vewendet werden).

5.2 Abgrenzung

Die Umsetzung umfasst keine Implementierung eines virtuellen Secure Element.

Die Lösung wird auf Commodity-Hardware implementiert. Eine Implementation auf echte Terminal-Hardware ist im Rahmen dieser Arbeit nicht vorgesehen.

Zum Testen werden Daten, welche einer EMV-Transaktion ähneln, über die Schnittstelle gesendet. Konkret wurden Null-Bytes in der Grösse und Anzahl, wie sei bei einer EMV-Transkation vorkommen eingesetzt. Da aus Sicht des Systems die transportierten Daten opak sind, ist dieser Ersatz als gleichwertig bezüglich des Tunnelings zu betrachten.

Weiter wird für die Validierung geprüft, ob die Lösung der EMV (Contactless) Spezifikation genügt. Auf Anforderungen der Card Schemes wird nicht eingegangen.

5.3 Systemüberblick

Die Hauptkomponenten der Lösung sind die Anwendung auf dem Smartphone, das Kommunikationsprotokoll sowie die Anwendung, die auf dem Terminal arbeitet.

Das Protokoll arbeitet im NFC P2P Modus und nutzt das NFC SNEP Protokoll zum Übertragen der Daten. Es sieht den Transport der EMV Kommandos vor und kann erweitert werden, um beispielsweise das Einlösen von Gutscheinen, Loyalty-Systeme oder das Übertragen von Kassen-Quittungen zu ermöglichen.

Über das Protokoll (siehe Use Case Zahlungsformalitäten) nimmt die Anwendung auf dem Smartphone die Kommandos des Terminals entgegen, extrahiert die EMV Befehle und leitet diese weiter ans virtuelle

Secure Element. Die Antworten des virtuellen Secure Elements werden wieder im Protokoll verpackt und ans Terminal zurück gesendet. Dies wird für jede vom Terminal empfangene Nachricht durchgeführt, bis entweder die Transaktion durchgeführt ist, oder die Kommunikation zum Terminal oder zum virtuellen Secure Element abbricht.

Die Anwendung auf dem Terminal erkennt herkömmliche kontaktlose Bezahlkarten und damit kompatible Geräte sowie die Smartphones, die auf den neuen P2P-Modus setzen. Sie meldet den bestehenden Komponenten im Terminal, dass eine neue Karte anwesend sei und die Zahlungssequenz ausgelöst werden könne. Alle so erhaltenen Befehle werden im Protokoll verpackt und an die Gegenstelle, typischerweise ein Smartphone, gesendet. Alle von der Gegenstelle empfangenen Daten werden aus dem Protokoll extrahiert und den bestehenden Komponenten weitergeleitet. Dies geschieht so lange, bis die Kommunikation beendet ist oder abbricht.

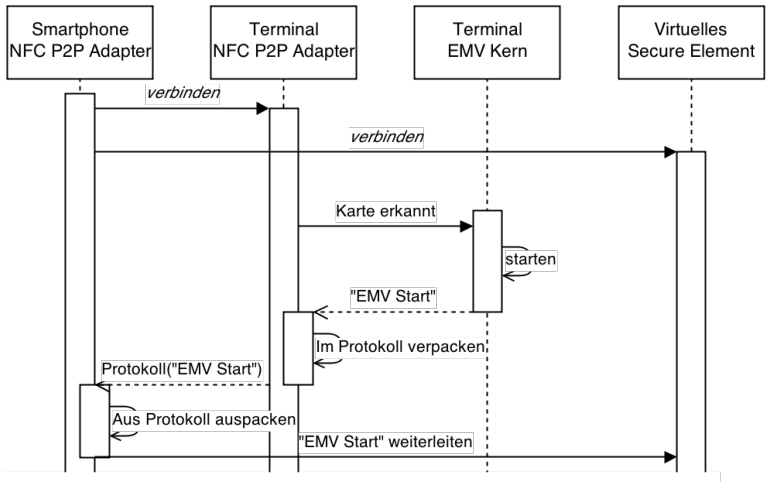

Abbildung 26: Das Sequenzdiagramm zeigt die initiale Sequenz, um eine Transaktion über NFC P2P aufzubauen.

Dieses Verhalten wurde in zwei Use Cases untersucht. Der Use Case *Bezahlen* zeigt dabei den Ablauf aus Consumer Sicht und der Use Case *Zahlungsformalitäten* beschreibt die technischen Feinheiten des Bezahlvorganges.

Use Cases im “fully dressed style” finden sich unter Use Cases.

5.3.1 Spezifikation der Protokollnachricht

Eine Protokollnachricht ist eine NDEF-Nachricht [66, p.8]. Die Nachricht hat einen NDEF-Record [66, p.8] mit dem MIME-Type `application/ch.hsr.peerpay.v1`. `v1` steht dabei für die Protokollversion und soll bei folgenden Versionen angepasst werden.

Der Payload des NDEF Record besteht aus einem ersten Byte für den Nachrichten-Typ und aus weiteren Bytes der eigentlichen Nachricht.

Es sind in der ersten Version zwei Nachrichten spezifiziert:

Typ (dec.)	Name

0	PeerPay Control Message
10	PeerPay EMV Message

Tabelle 5: Die zwei definierten Arten von Kontrollnachrichten.

Somit können in späteren Versionen weitere Nachrichten-Typen spezifiziert werden.

PeerPay Control Message Die Control Message wird hauptsächlich verwendet, um Status-Nachrichten und Fehlermeldungen auszutauschen und den Kontrollfluss zu regeln.

Beispielsweise wird mit einer Control Message der EMV Prozess eingeleitet und auch wieder beendet.

PeerPay EMV Message Im Payload, der *PeerPay EMV Message* wird, die ursprüngliche EMV-Nachricht übertragen. Es braucht dabei keine Unterscheidung, ob dies eine Anfrage- oder eine Antwort-Nachricht war, weil dies implizit klar ist: Nur das Terminal kann gemäss EMV-Anfragen stellen, und bis die Gegenstelle geantwortet hat, wird auch keine weitere Anfrage gestellt. Eine Nachricht des Smartphones ist deshalb immer als Antwort zu werten.

5.3.2 Zustand auf dem Smartphone

Zwischen Terminal und Smartphone werden konstant Nachrichten ausgetauscht. Da diese asynchron eintreffen können, müssen die Nachrichten ständig an die korrekten Kontrollinstanzen verteilt werden.

Bricht die Kommunikation ab, wird in einen Fehlerzustand übergegangen und eine Wiederaufnahme der Kommunikation ist (zum jetzigen Zeitpunkt) nicht möglich, beziehungsweise vorgesehen.

Die Zustandsmaschine auf dem Terminal ist analog aufgebaut.

Die beiden Zustände *Control State Machine* und *EMV State Machine* sind wiederum Zustandsmaschinen, die parallel zueinander laufen können. Sie funktionieren aber grundlegend anders.

Control State Machine Die *Control State Machine* nimmt eine Nachricht entgegen und verarbeitet diese. Sie ist auch dafür verantwortlich, dass die *EMV State Machine* initialisiert wird und nach Abschluss der EMV-Kommunikation beendet wird.

EMV State Machine Die *EMV State Machine* verbringt die meiste Zeit in den Zuständen *waiting on terminal* und *waiting on virtual SE*. Der EMV-Teil auf dem Smartphone ist also ein Dispatcher, der die EMV Nachrichten zwischen EFT/POS-Terminal und virtuellem SE weiterleitet.

Im Gegensatz zur *Control State Machine* kann diese Zustandsmaschine in einem Zustand nur eine bestimmte Nachricht verarbeiten. Dies widerspiegelt das von EMV vorgeschriebene Nachrichtenmodell.

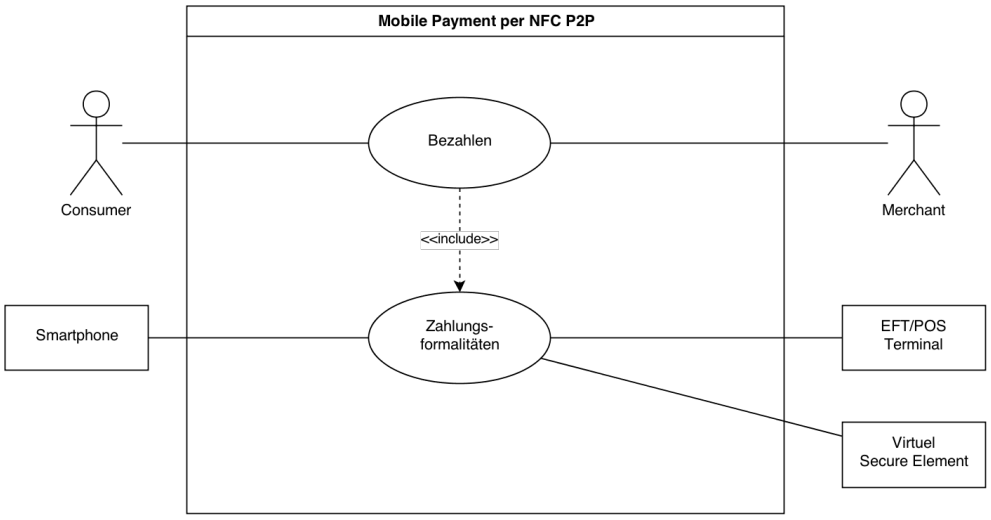

Abbildung 27: Dieses Use Case-Diagramm zeigt die Use Cases und damit das Zusammenspiel der für das neue System relevanten Aktoren.

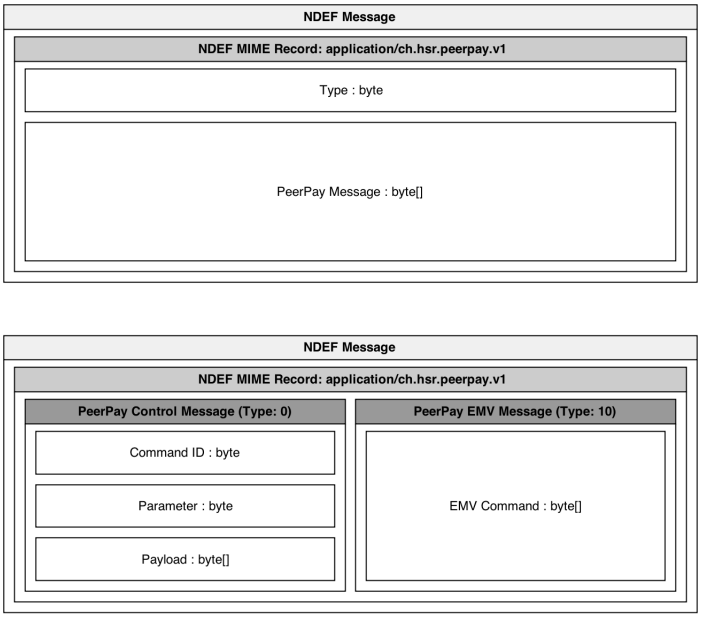

Abbildung 28: Die Grafik zeigt die Felder der Nachrichten des Protokolles sowie deren Verschachtelung. Wo im oberen Block die eigentliche Nachricht noch als Byte-Block *PeerPay Message* dargestellt ist, sind im unteren Block die beiden spezifizierten Nachrichten mit ihren jeweiligen Feldern abgebildet.

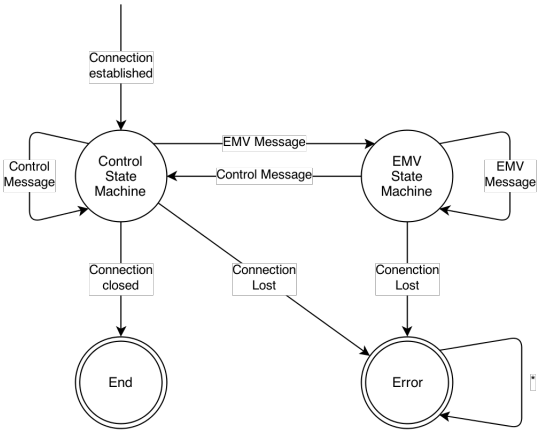

Abbildung 29: Das Zustandsdiagramm zeigt die ständigen Zustandsübergänge zwischen den Zustandsmaschinen *Control State Machine* und *EMV State Machine*, wenn Nachrichten für die jeweilige Zustandsmaschine eintreffen.

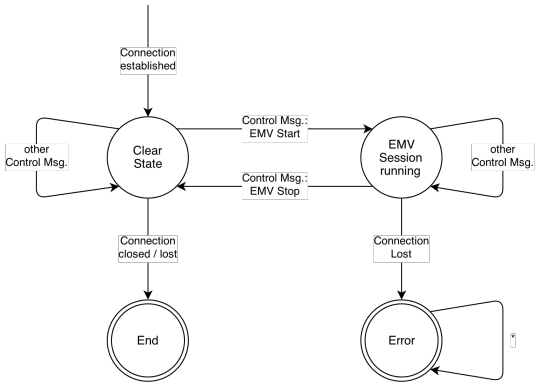

Abbildung 30: Das Zustandsdiagramm zeigt schematisch, dass die *Control State Machine* für die EMV Session verantwortlich ist. Bricht die Verbindung während der EMV-Transaktion ab, so wird in den Error-Zustand übergegangen.

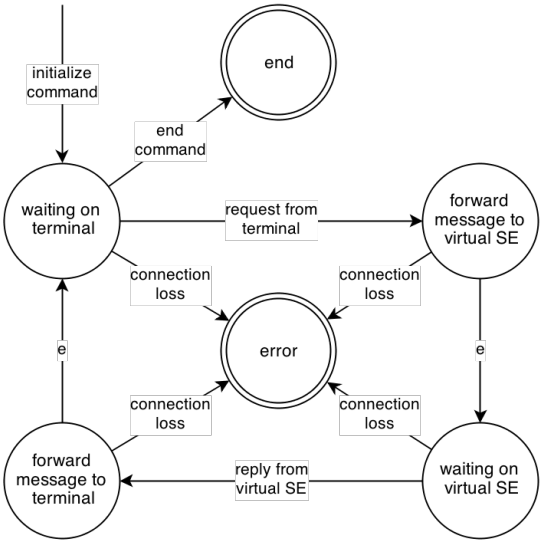

Abbildung 31: Das Zustandsdiagramm zur *EMV State Machine* zeigt schematisch, welche Zustände die Zustandsmaschine annehmen kann und welche Aktionen einen entsprechenden Zustandsübergang auslösen. Es ist klar ersichtlich, dass pro Zustand nur eine bestimmte Nachricht erwartet wird. Der *e*-Übergang steht für ein ε-Übergang, der sofort geschieht, wenn der entsprechende Ausgangs-Zustand des Übergangs erreicht wird.

5.4 Umsetzung

Dieses Kapitel erläutert die durchgeführten Experimente. Dabei wird auf die verwendete Hardware eingegangen, die benutzte Software (speziell Libraries) aufgezeigt und die Herausforderungen und Schwierigkeiten bei der Implementation verdeutlicht.

5.4.1 Probleme mit dem NFC-Reader ACR122U

Der *ACR122U* ist ein verbreiteter und günstiger NFC-Reader, der über *USB* mit einem Computer verbunden wird. Das Gerät stand schon zur Verfügung, weshalb erste Tests damit erfolgten. Das Gerät unterstützt grundsätzlich alle NFC-Modi. Jedoch wurde das Gerät primär für das Lesen und Schreiben von Tags und Contactless Smartcards entwickelt, weshalb dieses Gerät den NFC P2P-Modus in Zusammenarbeit mit LibNFC nicht vollständig beherrscht. Dieses Problem ist in der *LibNFC devices compatibility matrix* (siehe [67]) dokumentiert, weshalb es rechtzeitig erkannt wurde.

Es wurde daher auf ein anderes Gerät ausgewichen, welches gemäss der erwähnten *LibNFC devices compatibility matrix* vollständig unterstützt ist. Die Wahl fiel auf das Gerät *APPB2USOO*.

5.4.2 Umsetzung mit dem NFC-Reader APPB2USOO

Der Leser *APPB2USOO* des Herstellers Arygon, mittlerweile Identive, wurde gewählt, weil er sehr gut von LibNFC unterstützt wird. Er verwendet als Controller den PN532-Chip, welcher zu den verbreitetsten NFC-Controllern gehört und sehr gut dokumentiert ist. Wie der *ACR122U* wird er via USB an einen Computer angeschlossen.

Der Leser besitzt neben dem NFC-Controller auch über einen *PIC Microchip* und muss deshalb nicht ausschliesslich vom Host gesteuert werden. Damit konnten auch Ängste des Partners entgegengewirkt werden, wonach die ständige Kommunikation zurück auf den Host zu langsam sein könnte. Die Überlegung dabei war, dass EMV Timeouts spezifiziert sind, welche allenfalls nicht eingehalten würden.

Der Leser stellte sich als relativ problemlos in der Verwendung heraus. Es sind Treiber für zur Verwendung des Readers als PC/SC-Interface für Windows und Linux verfügbar. Im Übrigen registriert sich das Gerät als serielle Schnittstelle, über die direkt Kommandos gesendet werden können. So konnte das Gerät auch unter Mac OS erfolgreich angesprochen werden.

5.4.3 Probleme mit LibNFC

LibNFC[28] ist eine freie[29] und in *C* geschriebene Library für NFC. Sie stellt ein sehr primitives API für verschiedene NFC-Funktionen zur Verfügung. Da schon Erfahrung mit dieser Library vorhanden war, wurde sie als Ausgangspunkt für Experimente gewählt.

Ausser auf Windows konnte die LibNFC auf allen verwendeten Systemen (Mac OS und Linux) kompiliert und benutzt werden.

Nach anfänglich Erfolg versprechenden Versuchen, in denen eine Kommunikation zwischen dem Leser und dem Android-Smartphone zustande kam, erwies sich der Ansatz mit LibNFC als nicht zielführend.

Eine Kommunikation mit dem SNEP-Stack von Android konnte nicht aufgebaut werden. Wie sich herausstellte, ist dieser Protokollstack nicht vollständig implementiert und in der derzeit aktuellen Version *1.7.0-rc7* lediglich eine API für den ISO 18092 *DEP Modus* vorhanden. In Tests war es möglich, das Lesegerät als *DEP Initiator* und als *DEP Target* zu betreiben. Der DEP-Kommunikationsstack ist allerdings auf Android nicht zugänglich.

Bei genauerer Betrachtung des Codes der Library zeigte sich, dass die Unterstützung für höherer Protokolle noch nicht fertiggestellt ist. So unterstützt LibNFC in der aktuellen Version weder *LLCP* noch das darauf aufsetzende *SNEP*. Eine Implementation für *NDEF* ist vorhanden, da dies für den DEP-Modus notwendig ist.

Da es ausserhalb des Scopes dieser Thesis liegt, einen eigenen Protokollstack für die benötigten Kommunikationsprotokolle zu implementieren, wurde von einer Nutzung von LibNFC abgesehen.

Alternativ zur Kommunikation im SNEP-Modus wäre eine Verbindung auch über einen Trick möglich. Dabei wird der NFC *Reader/Writer*-Modus genutzt. Dieser Ansatz wurde unter dem Namen *Inverse Reader Mode*von Saminger et. al. in [65, pp.7–11] vorgestellt und auch erfolgreich getestet.

Es wurde untersucht, ob eine Implementation des Inverse Reader Modes mit LibNFC und dem *APPB2US00*-Leser möglich wäre. Die Datenübertragung konnte in Experimenten für beide Kommunikationsrichtungen erfolgreich getestet werden. Allerdings wurden die Tests (das heisst, Leser im Target-Modus und mit dem Smartphone beschreiben sowie Leser im Target-Modus und mit dem Smartphone lesen) separat durchgeführt. Ob eine fortlaufende Kommunikation zwischen den Geräten möglich ist (insbesondere, wie sich der Leser beim Wechsel zwischen den Modi verhält) wurde nicht getestet und müsste bei einer Implementation dieser Lösung noch genauer untersucht werden.

[28] Siehe http://nfc-tools.org/index.php?title=Libnfc.
[29] Lizensiert unter der GNU Lesser General Public License.

5.4.4 Probleme mit OPEN-SNEP

OPEN-SNEP[30] ist eine Library, die die PC/SC-Schnittstelle verwendet, um mit Geräten eine Verbindung herzustellen. Sie wurde auf dem *NFC Workshop 2013* in Zürich vorgestellt [65, pp.65–70]. Die Library fokussiert speziell auf die Kommunikation via *SNEP*, also über den *Peer-To-Peer*-Modus von NFC.

Eigentlich ist die Bibliothek für den ACR122U-Leser entwickelt worden. Der Code konnte aber auch mit dem APPB2US00-Leser verwendet werden.

Auf den Einsatz der Library wurde verzichtet, weil die Dokumentation als unzureichend bewertet wurde. Erschwerend kam noch hinzu, dass ausser zwei Testapplikationen keine weiteren Beispielcode zur Verfügung gestellt wird. Die Benutzung der Library würde dadurch weiter erschwert.

Vorteil dieser Bibliothek wäre, dass sie in Java geschrieben ist und dadurch aufgrund der Erfahrung der Autoren leichter einzusetzen wäre.

5.4.5 Probleme mit NFCTools

Eine weitere Library für die Programmierung mit NFC ist *NFCTools*[31].

Die Library beherrscht alle NFC-Modi. Sie ist in Java geschrieben und verfügt über eine vielversprechende Sammlung an Beispielcode.

Sie konnte jedoch in Tests nie erfolgreich eingesetzt werden. Deshalb wurde auf die Nutzung verzichtet.

5.4.6 Umsetzung mit NFCpy

NFCpy[32] ist ein Projekt, welches ähnliche Ziele wie die *LibNFC* verfolgt. Im Gegensatz zu jener verfügt sie aber über einen bereits sehr ausgereiften und funktionsfähigen SNEP-Stack und beherrscht somit den *Peer-To-Peer*-Modus von NFC. Die Library ist für und vollständig in *Python* entwickelt.

Die Library unterstützt den *APPB2US00* Reader vollständig. Sie bietet ausserdem eine stattliche Anzahl an Beispielcode und eine ausreichend gute Dokumentation.

Als gröbster Makel soll angemerkt werden, dass die Library unter Mac OS und Windows nicht lauffähig gemacht werden konnte. Mit einem *Raspberry Pi*[33]-Minicomputer, auf dem *Raspbian*, ein Debian-Derivat, installiert wurde, konnte aber überall mit der Library entwickelt werden.

5.4.7 Probleme mit Android

Als Implementationsplattform wurde erst *Android* gewählt, weil diese sonst sehr weitläufige Möglichkeiten für Entwickler bietet.

Wie sich bei Untersuchungen herausstellte, sind die APIs für NFC aber stark abstrahiert, sodass Entwickler sich nicht mit Low-Level Problemen befassen müssen. Auf der abstrahierten Schicht der API kann, wie aus unten stehendem Listing hervorgeht, eine NDEF Message zur Übermittlung hinterlegt werden. Diese starke Abstraktion behinderte eine Umsetzung der angedachten Lösung.

[30] Siehe https://code.google.com/p/ismb-snep-java/.
[31] Siehe https://github.com/grundid/nfctools und https://github.com/grundid/nfctools-examples.
[32] Siehe https://launchpad.net/nfcpy.
[33] Siehe http://www.raspberrypi.org/.

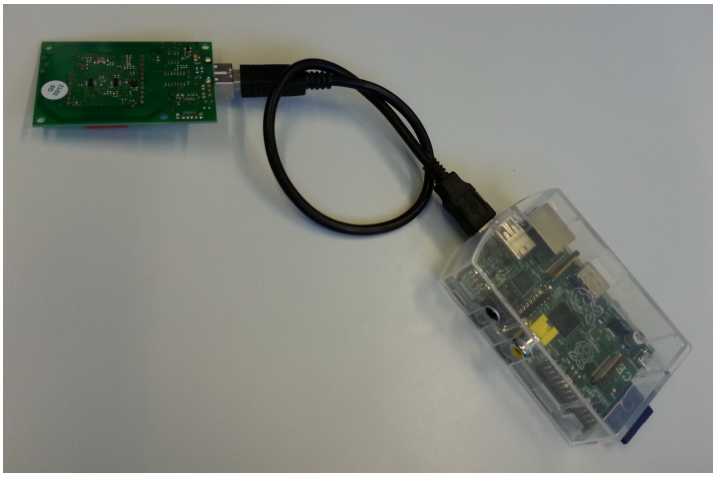

Abbildung 32: Das verwendete Raspberry Pi mit dem angeschlossenen APPB2US00 NFC Reader.

Das Android-SDK (bis und mit API Level 17) bietet durch die gewählte Implementierungsmethode (das heisst, indem genau eine NDEF-Nachricht hinterlegt werden kann) nur rudimentäre Unterstützung für NFC *SNEP*: So ist es lediglich möglich, die eine Nachricht pro hergestellte Verbindung per *PUT* Meldung zu übermitteln. Danach ist es nicht mehr möglich, weitere Nachrichten gleichen oder anderen Typs zu übermitteln. Das Gerät muss zuerst wieder vollständig aus dem Funkbereich der Gegenstelle entfernt werden, ehe eine neue Nachricht übermittelt werden kann.

Dabei liegt der Grund klar in der Abstraktion durch die API. Der unter der API verwendete Stack implementiert eindeutig und vollständig SNEP. Dies konnte verifiziert werden, weil Android grösstenteils Open Source ist (vgl. Listings).

Ein weiteres, aber nicht ganz so gravierendes Problem, ist die Art, wie Android die Nachrichten versendet. Dies geschieht ausschliesslich per *PUT*-Methode. Die Spezifikation [68, pp.8–15] definiert (analog zu HTTP) eine *GET*- und eine *PUT*-Methode. Der Unterschied liegt insbesondere bei der Response: Während bei einer GET-Anfrage die zugehörige Response einen Payload überträgt, fehlt diese Möglichkeit bei PUT. Responses auf PUT-Requeststst werden lediglich einer Statusmeldung quittiert. Dabei darf gemäss Spezifikation kein Payload mitgegeben werden [68, pp.8–9]. Die Kommunikation könnte aber durch beidseitiges Senden von *PUT*-Nachrichten trotzdem aufrechterhalten werden. Die Überprüfung über das Erhalten von Antworten auf Anfragen müsste dazu manuell implementiert werden, wie dies auch bei Umsetzung mit Windows Phone 8 gemacht wurde.

Der folgende Code zeigt die zentrale Klasse, die NFC P2P in Android steuert. Linien 12 bis 15 definieren ein Interface, welches *PUT* und *GET* für NFC P2P unterstützt. Zeilen 30 bis 38 zeigen, dass diese Funktionen auch tatsächlich implementiert sind.

```
1  /*
2   * Copyright (C) 2011 The Android Open Source Project
3   [...]
4   */
5  package com.android.nfc.snep;
6  [...]
7
```

```
public final class SnepServer {
    [...]

    [Anm: Hier ist *GET* und *PUT* implementiert]
    public interface Callback {
        public SnepMessage doPut(NdefMessage msg);
        public SnepMessage doGet(int acceptableLength, NdefMessage msg);
    }

    [...]

    static boolean handleRequest(SnepMessenger messenger, Callback callback) throws IOException {
        SnepMessage request;
        try {
            request = messenger.getMessage();
        } catch (SnepException e) {
            [...]
        }

        if (((request.getVersion() & 0xF0) >> 4) != SnepMessage.VERSION_MAJOR) {
            messenger.sendMessage(SnepMessage.getMessage(
                    SnepMessage.RESPONSE_UNSUPPORTED_VERSION));
        [Anm: Hier wird *GET* behandelt]
        } else if (request.getField() == SnepMessage.REQUEST_GET) {
            messenger.sendMessage(callback.doGet(request.getAcceptableLength(),
                    request.getNdefMessage()));
        [Anm: Hier wird *PUT* behandelt]
        } else if (request.getField() == SnepMessage.REQUEST_PUT) {
            if (DBG) Log.d(TAG, "putting message " + request.toString());
            messenger.sendMessage(callback.doPut(request.getNdefMessage()));
        } else {
            if (DBG) Log.d(TAG, "Unknown request (" + request.getField() +")");
            messenger.sendMessage(SnepMessage.getMessage(
                    SnepMessage.RESPONSE_BAD_REQUEST));
        }
        return true;
    }

    [...]
}
```

Der folgende Code zeigt die Schnittstelle, welche Android den Entwicklern zur Verfügung stellt. Die zwei gezeigten Methoden widerspiegeln dabei die einzigen Möglichkeiten, NDEF Nachrichten zu versenden, respektive versenden zu lassen.

Es gibt dabei zwei mögliche Abläufe; beide sind im *JavaDoc* der entsprechenden Methoden beschrieben. Sie erlauben jedoch pro Verbindung (also pro *tap*) nur eine *PUT* Nachricht zu senden.

```
/*
 * Copyright (C) 2010 The Android Open Source Project
```

```
 [...]
 */
package android.nfc;
[...]

/**
 * Represents the local NFC adapter.
 * <p>
 * Use the helper {@link #getDefaultAdapter(Context)} to get the default NFC
 * adapter for this Android device.
 *
 [...]
 */
public final class NfcAdapter {
    [...]

    /**
     * Set a static {@link NdefMessage} to send using Android Beam (TM).
     *
     * <p>This method may be called at any time before {@link Activity#onDestroy},
     * but the NDEF message is only made available for NDEF push when the
     * specified activity(s) are in resumed (foreground) state. The recommended
     * approach is to call this method during your Activity's
     * {@link Activity#onCreate} - see sample
     * code below. This method does not immediately perform any I/O or blocking work,
     * so is safe to call on your main thread.
     *
     * <p>Only one NDEF message can be pushed by the currently resumed activity.
     *
       [...]
     *
     * <p class="note">Requires the {@link android.Manifest.permission#NFC} permission.
     *
     * @param message NDEF message to push over NFC, or null to disable
     * @param activity activity for which the NDEF message will be pushed
     * @param activities optional additional activities, however we strongly recommend
     *        to only register one at a time, and to do so in that activity's
     *        {@link Activity#onCreate}
     */
    public void setNdefPushMessage(NdefMessage message, Activity activity,
            Activity ... activities) {
        [...]
    }

    /**
     * Set a callback that dynamically generates NDEF messages to send using Android Beam (TM).
     *
     * <p>This method may be called at any time before {@link Activity#onDestroy},
     * but the NDEF message callback can only occur when the
```

```
52          * specified activity(s) are in resumed (foreground) state. The recommended
53          * approach is to call this method during your Activity's
54          * {@link Activity#onCreate} – see sample
55          * code below. This method does not immediately perform any I/O or blocking work,
56          * so is safe to call on your main thread.
57          *
58          * <p>Only one NDEF message can be pushed by the currently resumed activity.
59          * If both {@link #setNdefPushMessage} and
60          * {@link #setNdefPushMessageCallback} are set, then
61          * the callback will take priority.
62          *
63          * <p>If neither {@link #setNdefPushMessage} or
64          * {@link #setNdefPushMessageCallback} have been called for your activity, then
65          * the Android OS may choose to send a default NDEF message on your behalf,
66          * such as a URI for your application.
67          *
68            [...]
69          *
70          * <p class="note">Requires the {@link android.Manifest.permission#NFC} permission.
71          *
72          * @param callback callback, or null to disable
73          * @param activity activity for which the NDEF message will be pushed
74          * @param activities optional additional activities, however we strongly recommend
75          *        to only register one at a time, and to do so in that activity's
76          *        {@link Activity#onCreate}
77          */
78         public void setNdefPushMessageCallback(CreateNdefMessageCallback callback, Activity activity,
79                 Activity ... activities) {
80             [...]
81         }
82
83         [...]
84     }
```

5.4.8 Umsetzung mit Windows Phone 8

Als mögliche Lösung für das Problem bei der Umsetzung mit Android wurde die Plattform *Windows Phone 8* (WP8) evaluiert. Dies stellte die logische Wahl dar, weil es die nächst kleinere Smartphone-Platform mit NFC Untertützung ist, welcher einiges Potential zugemessen wird [29]. Dabei fiel eine erste Evaluation der API positiv aus.

Mit einem Testgerät konnte die erhoffte bessere Eignung bestätigt werden. Mit WP8 war es tatsächlich möglich, pro Verbindung mehrere NDEF-Nachrichten über das SNEP zu senden und zu empfangen.

Allerdings unterstützt auch WP8 lediglich die *PUT*-Methode des *SNEP*. Dieses Manko konnte durch wechselseitiges Senden von *PUT*-Nachrichten allerdings umgangen werden: Statt einer *GET*-Nachricht, die mit den entsprechenden Daten beantwortet werden muss, wird nun eine *PUT*-Nachricht gesendet, und das Smartphone muss wieder mit einer *PUT*-Nachricht antworten.

Die API von WP8 ist dabei sehr leicht verständlich und die Implementation scheint sehr stabil zu sein.

Ein Makel hat das System allerdings: Obwohl sich die App für den bestimmten Nachrichtentyp registriert hat und solche empfangenen Nachrichten auch verarbeitet, meldet das Betriebssystem dem Benutzer in einer nicht unterdrückbaren Mitteilung, dass eine Nachricht empfangen worden und ob er diese akzeptieren möchte. Der Benutzer muss erst diese Meldung bestätigen, bevor er die Applikation weiter benutzen kann. Im Hintergrund wurde die Nachricht aber bereits verarbeitet und die Kommunikation geht trotzdem weiter. Die Antwort des Benutzers hat keinen Einfluss auf das Verhalten der Applikation. Es konnte nicht abschliessend geklärt werden, weshalb Windows Phone eine derartige Dialogbox einblendet. In Anbetracht dessen, dass die Antwort des Benutzers ("Accept" bzw. "Ignore") keinerlei einfluss auf die Applikation hat, ist von einem Bug auszugehen.

Die Showcase-Applikation muss lediglich an das Terminal gehalten werden. Wenn eine Verbindung zustande kommt, wird sofort mit der Übertragung begonnen. Dabei zeigt eine Liste den detaillierten Fortschritt an, und die Hintergrund-Farbe ändert sich, um ein zusätzliches visuelles Feedback zu geben.

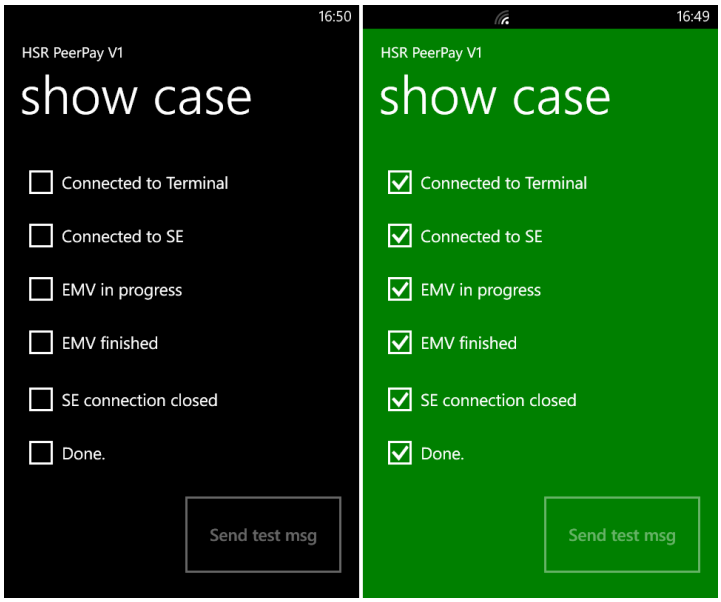

Abbildung 33: Die Abbildung zeigt die App, wie sie vor der Transaktion aussieht (links) und wie nach einer erfolgreichen Transaktion (rechts).

Eine App für Consumer müsste ein überarbeitetes Interface haben, welches die Schritte nicht so detailiert zeigt. Ausserdem müsste der Consumer sich registrieren können und allenfalls aus mehreren Karten auswählen können.

5.5 Beurteilung

Die gewählte Strategie, den Zahlvorgang mittels NFC Peer-To-Peer durchzuführen, hat das Potential, aktuelle Lösungen zu ersetzen.

In diesem Kapitel wird die entwickelte Lösung hinsichtlich ihrer Eignung für eine Implementierung in der Schweiz diskutiert und anhand von verschiedenen Kriterien mit der bestehenden Lösung, die auf dem *Card Emulation Mode* aufbaut, verglichen.

5.5.1 Technologisch

Die technologische Umsetzung des Showcases erfolgte fast wie geplant. Nachdem sich das Smartphone *Nokia Lumia 820* und der NFC Reader *APPB2US00* erkannt haben, werden die entsprechenden Kontroll-Nachrichten ausgetauscht.

Dazu konnten aber nicht wie geplant *GET*-Anfragen verwendet werden. Das Problem ist in der Umsetzung von *SNEP* in *Windows Phone 8* zu suchen. Dort kann kein eigener *SNEP*-Server oder -Client implementiert werden. Es wird lediglich der Default-Server vom Betriebssystem gestartet. Dieser akzeptiert aber standardkonform nur *PUT* Nachrichten. Diese werden dann durch das Betriebssystem zur entsprechenden App geroutet.

Die Umstellung auf *PUT*-Nachrichten bereitete aber keine Probleme, die Lösung ist lediglich nicht ganz so *elegant*.

Derzeit ist nur eine Umsetzung unter Windows Phone möglich. Wegen des geringen Marktanteils von Windows Phone wird eine Implementierung für den Produktiveinsatz wohl erst erfolgen, wenn auch die Android-API eine Umsetzung erlaubt.

Ebenso muss über eine Unterstützung für Apple iPhone nachgedacht werden. Da die Apple-Geräte derzeit nicht über NFC verfügen und die Alternativen (Jackets) nicht akzeptabel sind, sollte geprüft werden, ob eine Umsetzung ohne iPhone-Unterstützung möglich und sinnvoll ist.

Aufseiten des Terminals sollte eine Implementation gewählt werden, welche möglichst wenige Abhängigkeiten zum EMV-Kernel schafft. Ein möglicher Ansatz wäre allenfalls, die Lösung als NFC-Gerätetreiber zu implementieren.

Ein weiter Punkt ist die prinzipielle Unterstützung durch die Hardware. Es wurde nicht geprüft, ob und wie die Lösung auf den aktuellen Terminals eingesetzt werden kann. Allerdings soll eine kommende Generation von Terminals NFC von sich aus unterstützen. Es darf erwartet werden, dass die Implementation dort einfacher möglich wäre.

5.5.2 Sicherheit

Sichere Speicherung von Credentials Der implementierte Showcase setzt keinen eigentlichen Credential-Speicher ein, da nur Dummydaten übertragen werden.

Für eine tatsächliche Umsetzung muss aber der Einsatz eines Cloud-Storage empfohlen werden. Auch eine Hybrid-Lösung wäre denkbar.

Die Empfehlung rührt daher, da sich herausgestellt hat, dass der Zugriff auf ein hardwarebasiertes Secure Element praktisch nur durch Involvierung eines zusätzlichen Players möglich ist.

Die cloudbasierte Variante bietet den Vorteil, dass im Falle eines Verlustes des Smartphones die gespeicherten Credentials nicht verloren gehen. Weiter können damit in einer durch den Issuer kontrollierbaren Umgebung die Anforderungen der verschiedenen Parteien (speziell der Card Schemes) an den Credentials-Store eingehalten werden. Der Zugriff darauf wäre nur durch das Smartphone des Benutzers möglich. Genau wie bei einem Hardware Security Modul verlässt der Schlüssel das SE dabei nie: Das Smartphone übermittelt das zu signierende Kryptogramm, welches von der Cloud signiert zurückgesendet wird.

Die sichere lokale Speicherung der Credentials wäre aber bestimmt möglich. Beispielsweise könnte das unter Android verfügbare *Trusted Execution Environment* (TEE) genutzt werden. Dabei handelt es sich im Prinzip um ein Hardware Security Modul der CPU, welches zur Bootzeit vom Betriebssystem initialisiert wird, danach aber von der CPU vom restlichen System abgeschottet wird. Somit ist der vom TEE verwaltete

Speicherbereich nicht mehr direkt zugänglich. Ähnlich wie eine Smartcard verwendet das TEE Applets, welche im getrennten Speicherbereich ausgeführt werden. Eine Kommunikation mit diesen ist nur über spezielle CPU Interrupts und abgesicherte gemeinsame Speicherbereiche möglich.

Das TEE könnte auch für die Cloudlösung verwendet werden, indem die Credentials für den Zugang zur Cloud darin hinterlegt würden.

Allerdings ist TEE noch in der Entwicklung und eine abschliessende Beurteilung daher noch nicht möglich.

Vergleich zur SIM-Sicherheit Die wesentliche Herausforderung betreffend Sicherheit ist, die für die Zahlung (allgemein: zur Authentisierung der Consumer) notwendigen Credentials sicher zu speichern. Sicher bedeutet in dieser Beziehung, dass sie weder von einer anderen Applikation noch vom Betriebssystem des Smartphones gelesen werden können. Das Mindset des EMV-Referenzmodells für Mobile Payment geht davon aus, dass das OS des Smartphones kompromittiert werden könnte. Dass dies gar nicht so unwahrscheinlich ist, zeigt beispielsweise der kürzlich entdeckte Android-Trojaner *Obad.a* [69]. Hoch entwickelte Trojaner wie dieser versuchen gezielt das Betriebssystem zu infizieren und jede Art von wertvollen Daten zu kopieren. So existieren mehrere Trojaner, welche fähig sind, Credentials bei Mobile Banking mitzuschneiden (inklusive des per SMS gesendeten Sicherheitscodes).

Diese Entwicklung zeigt, dass das Smartphone in Zukunft vermehrt ein Ziel für Malware-Entwickler darstellen wird. Ob es die Hersteller von Betriebssystemen schaffen werden, ihr Produkt in den nächsten Jahren so sicher wie eine Smartcard zu gestalten, darf bezweifelt werden. In diesem Fall muss der gesamte durch das Betriebssystem verwaltete Speicher als potenziell kompromittiert betrachtet werden.

Die Verwendung einer Smartcard (SIM-Karte), auf welcher die Credentials gespeichert werden und die über einen separaten Kryptoprozessor verfügt, befriedigt auch höchste Sicherheitsansprüche. Wesentlich zu dieser Sicherheit trägt ebenfalls bei, dass zwischen der Karte und dem NFC-Controller eine direkte physikalische Verbindung besteht und dass der Card Emulation Modus ausschliesslich durch den NFC-Controller aktiviert werden kann. Damit hat das Betriebssystem des Smartphones keine Möglichkeit, auf die Kommunikation zuzugreifen. Somit kann auch im Falle einer Infektion des Betriebssystems die Sicherheit aufrechterhalten werden.

Die Sicherheit des *Card Emulation Modes* wird in Rahmen dieser Thesis nicht weiter untersucht, es soll aber darauf hingewiesen werden, dass die Technologie noch recht jung ist und das Fehlen (beziehungsweise das Nicht-publik-werden) eines Exploits keinesfalls die Sicherheit bestätigt. Es wären durchaus Angriffsvektoren auf den NFC-Controller denkbar. (Dieser verfügt über eine Schnittstelle, welche vom Betriebssystem aus angesprochen werden kann.) Ebenso könnte auch einen Angriff auf die SIM-Karte erfolgreich sein. Letzteres ist aber eher unwahrscheinlich, die SIM-Karten gelten als allgemein sehr gut gesichert.

Andererseits muss hinterfragt werden, ob diese Stufe von Sicherheit überhaupt notwendig für die Sicherheit des Systems ist. Solange Bezahlkarten immer noch mit Magnetstreifen ausgegeben werden, wird ein Angreifer versuchen, dessen habhaft zu werden. Dies ist wesentlich einfacher möglich als bei EMV-Systemen. Ebenso geben viele Banken Apps für Mobile Banking heraus, mit denen ebenfalls Geld ab dem eigenen Konto abgebucht werden kann. Wie weiter oben beschrieben, gibt es mehrere Schädlinge, die versuchen, über das Smartphone an die Credentials für den Online-Bank-Zugang zu kommen.

Verschlüsselung der Übertragung Der vorgeschlagene Wechsel auf ein anderes Kommunikationsprotokoll ist als unkritisch zu beurteilen. Dies daher, weil die EMV-Daten unverändert übertragen werden. Dadurch wird die Sicherheit von EMV nicht kompromittiert.

Wenn der Merchant eigene Daten (beispielsweise zu Loyalty-Zwecken) zwischen dem Terminal und dem Smartphone übertragen möchte, sollten diese jedoch verschlüsselt werden.

5.5.3 Organisatorische Umsetzung

Im Folgenden werden Hinweise zu den Komponenten gegeben, die bei einer Umsetzung beachtet werden sollten.

Implementation der Smartphone App Damit die Lösung von möglichst vielen Consumer verwendet werden kann, muss sie auf mehreren Smartphone-Betriebssystemen implementiert werden. Deshalb sollten bei der aktuellen Marktlage mindesten die Betriebssysteme Android und Windows Phone berücksichtigt werden. Auf eine Implementation für Apples iOS kann verzichtet werden, da zurzeit keine Version des iPhones über NFC verfügt. Sollte dies aber in Zukunft der Fall sein, so müsste diese Platform auf jeden Fall ebenfalls berücksichtigt werden.

Bevorzugt wird die App ebenfalls vom Acquirer entwickelt, der auch die Veränderungen am Terminal vornimmt. Dies vereinfacht den Testing-Prozess.

Die App sollte über die Stores der jeweiligen Betriebssysteme an die Consumer verteilt werden.

Implementation des virtuellen Secure Elements Es muss entschieden werden, wie die Credentials gespeichert werden sollen. Je nach Sicherheitsbedarf der Lösung sind dabei verschiedene Lösungen möglich.

Diese Thesis schlägt die Implementation mit einer Cloud-Lösung vor. In diesem Fall muss die dazu nötige Server-Infrastruktur nach den geforderten Kriterien aufgebaut werden (EMV, PCI-DSS, Spezifikationen des Card Schemes).

Es muss insbesondere die notwendige PKI implementiert werden, damit die vom Smartphone übermittelten Daten authentifiziert werden können.

Als alternative Lösung könnte das unter Android verfügbare *Trusted Execution Environment* (TEE) verwendet werden.

Update der Terminals Es muss geprüft werden, auf welchen eingesetzten Terminals die Lösung eingesetzt werden kann. Das heisst, es muss geprüft werden, ob auf den Terminals der NFC Peer-To-Peer-Modus unterstützt wird. Dabei ist es möglich, dass ein neuer Treiber für gewisse Geräte entwickelt werden muss oder nicht kompatiblen Terminals gar ersetzt werden müssten.

Durch die Änderungen der Terminalsoftware muss diese höchst wahrscheinlich zumindest teilweise neu zertifiziert werden.

Wenn die Lösung implementiert und gestestet ist, kann diese auf die Terminals verteilt werden. Für die Terminals existiert ein Prozess, mit dem regelmässig Updates auf die Terminals eingespielt werden. Dieser Prozess könnte vom Acquirer genutzt werden, um die Software auf die Terminals zu spielen.

Die Implementation auf dem Terminal muss auf Kompatibilität mit der Smartphone App geprüft werden, damit ein reibungsloser Zahlungsablauf gewährleistet werden kann.

5.5.4 Erfüllung der reglementarischen und rechtlichen Anforderungen

Anforderungen der EMV Es wurde von Anfang an nach einer Lösung gesucht, welche sich innerhalb der Regeln der EMV-Spezifikation bewegt. Die strengeren Regeln der Card Schemes wurden nicht betrachtet, weil diese derart spezifisch auf eine Contactless Smartcard ausgerichtet sind, dass ausser dem Card Emulation Mode keine andere Lösung denkbar ist.

EMV Contactless spezifiziert als physikalisches Kommunikationsprotokoll ISO 14443. Da der gewählte Lösungsansatz als Basistechnologie NFC verwendet, welches selbst wieder auf ISO 14443 aufbaut (vgl. Anhang II) ist NFC, und damit auch SNEP, per se EMV-kompatibel.

Durch die Lösung verhält sich die Terminal-Hardware leicht anders: Bisherige Terminals verfügen über einen RFID-Chip, welcher wie NFC auf 13.56 MHz sendet. Das Terminal erwartet dabei immer ein ISO 14443-2 Type A- oder Type B-Gerät. Da NFC verschiedene Kommunikationsmodi unterstützt, müssen diese erkannt werden, ehe die höheren Protokolllayer aufgebaut werden können. Dazu verwendet NFC einen Zyklus, mit dem das sich im Funkbereich befindliche Gerät erkannt werden kann. Diese Funktion ist im Anhang II beschrieben.

Weil sich dadurch das elektromagnetische Verhalten des Terminals ändert (die Abwärtskompatibilität bleibt gewährleistet, kontaktlose Bezahlkarten werden durch das Feld als solche erkannt und die Kommunikation findet im *Reader/Writer*-Modus statt), musste geprüft werden, ob diese Änderung die EMV Contactless Spezifikation verletzt. Wie im EMV Contactless *Communication Protocol* [48, pp.164–167] beschrieben, ist es Terminals erlaubt, den Polling Cycle (in dem die im Funkbereich befindliche Hardware erkannt wird) um eigene Zyklen zu erweitern. Genau dies macht NFC, um zu erkennen, ob es sich um eine ISO 14443-2 Type A oder Type B-Karte handelt, oder ob es ein NFC-kompatibles Gerät ist.

Damit kann die vorgeschlagene Lösung die EMV-Spezifikation einhalten.

Weitere mögliche Kollisionen mit regulatorischen Bestimmungen Hinsichtlich der Speicherung der Credentials existieren eventuell noch weitergehende Anforderungen der Banken, um bestimmte regulatorische Bestimmungen einhalten zu können. Ob und welche solchen Anforderungen existieren und ob sie eingehalten werden können, ohne einen separaten Kryptoprozessor zu verwenden, wird im Rahmen dieser Studie nicht betrachtet.

Obwohl nicht geprüft, dürfte es eher unwahrscheinlich sein, dass durch die Verwendung von SNEP als Übertragungsprotokoll regulatorische Bestimmungen verletzt werden. Technisch gesehen wird durch die entworfene Lösung lediglich zusätzliche Kontrolldaten (Protokollheader) zu den übertragenen Daten hinzugefügt.

Wenn der Merchant das Protokoll erweitert und eigene Daten über die NFC-Schnittstelle überträgt, sollten diese verschlüsselt werden. Wird auf eine Verschlüsselung der zusätzlichen Daten verzichtet, könnten Regressansprüche auf den Merchant zurückfallen, sollte der Consumer einen Schaden erleiden, welcher durch die Verschlüsselung hätte vermieden werden können.

5.5.5 Wirtschaftliche Beurteilung

Zur Beurteilung der für die einzelnen Stakeholder entstehenden Kosten wurde die Methode der *Whole-Life-Cost*-Betrachtung gewählt. Dabei werden für jeden Stakeholder die anfallenden Kosten in Investitionskosten (*CAPEX*), Betriebskosten (*OPEX*) und Entsorgungs-/Ersetzungskosten (*Retirement*) aufgeteilt.

Zusätzlich wurden unter “Intention” die grundsätzliche Haltung und Interessen des Stakeholder festgehalten.

Diese Betrachtung hat nicht das Ziel, absolute Zahlen zu nennen, weil diese je nach Implementation variieren können. Vielmehr bieten sie Anhaltspunkte, welche Punkte bei der Kostenabschätzung für eine Implementation beachtet werden müssen.

Consumer

Intention Der Consumer bemerkt von der Veränderung grundsätzlich nichts. Allerdings wird damit die Entwicklung von Wallets deutlich vereinfacht.

Für den Conumser ist die Nutzung eines Wallets unabhängig von dessen Implementierung grundsätzlich vorteilhaft, weil er darauf verzichten kann, viele Karten in der Geldbörse mit sich zu tragen.

CAPEX Der Consumer muss für die Nutzung keine Investition tätigen, wenn davon ausgegangen wird, dass er nicht speziell dafür ein Smartphone anschafft und die Smartphone-App kostenlos zur Verfügung gestellt wird.

OPEX Für den Consumer fallen minimale Kosten an, weil er sich um Updates, eventuelle Passwörter und das Management der App kümmern muss. Die Vorteile sollten im Allgemeinen die Kosten deutlich übertreffen, anderenfalls besteht die Gefahr, dass der Kunde die Lösung nicht verwenden würde.

Retirement Es fallen für den Consumer die Kosten an, die Karten wieder physikalisch zu bestellen, sofern er das dann möchte. Wenn er das Smartphone wechselt, muss er die App neu konfigurieren, um wieder Zugriff auf die Credentials zu erlangen.

Merchant

Intention Der Merchant kann seine Kunden durch Mobile Payment einen Mehrwert bieten.

Das offene Protokoll, welches grundsätzlich alle übertragenen Daten als opak betrachtet, kann vom Merchant erweitert werden. Damit kann das Protokoll erweitert werden, damit der Merchant auch eigene Daten über die NFC-Schnittstelle in das Smartphone übertragen kann. Da die Systeme des Merchants dabei unabhängig vom Issuer bleiben, können praktisch alle Wünsche an Loyalty-Lösungen umgesetzt werden.

CAPEX Für die Nutzung der Zahlfunktion fällt dem Mechant lediglich Kosten für ein Upgrade des POS-Terminals an. Allenfalls handelt es sich dabei um ein reines Software-Update, welches er vom Acquirer kostenlos erhält. Anderenfalls muss er ein neues Terminal kaufen.

OPEX Die laufenden Kosten des Merchants verändern sich durch den Ansatz nicht.

Retirement Bei einem Downgrade auf die bisherige Lösung fallen für den Merchant keine Kosten an. Da alle Terminals rückwärts kompatibel sind, kann das Downgrade als Software eingespielt werden.

Issuer

Intention Das Hauptziel des Issuers ist, dass er keinen weiteren Player in der Wertschöpfungskette akzeptieren muss und das System somit unilateral ist. Das Ziel des Issuers ist es, die Kosten für den Einkauf der SE-Lösung (zum Beispiel SIM als SE) klein zu halten. Weil der Issuer die SE-Cloud selbst betreibt, benötigt er im Idealfall keine Schnittstelle mehr zum Card Manufacturer.

CAPEX Dem Issuer fallen Kosten für den Aufbau der SE-Cloud an. Diese muss den Bedingungen des jeweiligen Card-Scheme genügen.

OPEX Der Issuer muss die Kosten für die Wartung der Cloud-Infrastruktur übernehmen.

Retirement Um die Lösung ausser Betrieb zu nehmen, fallen dem Issuer Kosten an, um die Credentials auf eine neue Infrastruktur zu übertragen.

Acquirer

Intention Direkt entsteht für den Acquirer keinen Vorteil. Allenfalls kann die Investition durch erhöhtes Transaktionsvolumen finanziert werden. Anderenfalls könnte durch eine Absprache mit dem Issuer dessen finanzieller Vorteil mit dem Acquirer geteilt werden.

CAPEX Der Acquirer muss die Terminals aufrüsten, damit sie kompatibel sind. Dazu muss ev. neue Hardware eingesetzt werden; in diesem Fall kann der die Kosten für die neue Hardware dem Merchant verrechnen, wenn sich dieser ein neues Terminal anschafft.

Auf jeden Fall müssen die Kosten für die Entwicklung der Lösung (das heisst auf Smartphone- und Terminal-Seite), für das Testen und das Deployment berücksichtigt werden. Das Deployment kann über den üblichen Update-Mechanismus erfolgen. Die Mehrkosten für das Deployment sollten daher marginal ausfallen.

OPEX Es fallen die Kosten für die Wartung und Pflege der Software an. Weil die Software, welche auf dem Terminal läuft, komplexer wird, kann der Anstieg der Kosten überproportional sein.

Retirement Wenn die Lösung ausser Betrieb genommen wird, muss dies vorher angekündigt werden, damit die Änderung die Consumer und Merchants nicht überraschend trifft. Die Kosten für diese Massnahmen müssen berücksichtigt werden.

Card Manufacturer

Intention Der Card Manufacturer hat ein strategische Interesse, dass keine Mobile Payment-Lösungen auf den Markt kommen, weil er dadurch weniger Karten absetzten kann. Im (aus Sicht des Card Manufacturers) schlimmsten Fall bestellt der Issuer gar keine Karten mehr.

Eventuell kann sich der Card Manufacturer als TSM positionieren, indem er den Betrieb der Cloud für mehrere Issuer übernimmt und damit Skalenvorteile erreicht.

Kosten (CAPEX, OPEX, Retirement) Es fallen keine Kosten an.

Bank

Intention Die Bank hat ein strategisches Interesse an Mobile Payment, da damit das Transaktionsvolumen von bargeldlosen Zahlungen steigt, was zu einem höheren Umsatz bei der Bank führt.

Kosten (CAPEX, OPEX, Retirement) Es fallen keine Kosten an.

Card Schemes

Intention Die Card Schemes haben wie die Bank ein Interesse an erhöhtem Transaktionsvolumen. Vorausgesetzt, die Zahlungen werden tatsächlich über das Card Scheme abgewickelt und nicht etwa Person-to-Person oder Bank-to-Bank. Da die entwickelte Lösung für EMV-Transaktionen entwickelt wurde, ist dies immer der Fall.

Kosten (CAPEX, OPEX, Retirement) Es fallen keine Kosten an.

5.5.6 Zusammenfassung

Die entwickelte Lösung ist aus Sicht der Wertschöpfungskette nicht optimal, da insbesondere zwischen Issuer und Acquirer ein Ungleichgewicht zwischen Profiteur und Kostenträger entsteht. Da in der Schweiz aber die Issuer, wie auch die Acquirer, direkt oder indirekt den Banken (welche von der Lösung profitieren) angegliedert sind, dürften die Parteien geneigt sein, einen entsprechenden Zahlungsausgleich auszuhandeln. Auf jeden Fall wird ein Kostenausgleich zwischen den bestehenden Players eher akzeptiert, als wenn ein neuer Player bezahlt werden muss.

5.6 Schlussfolgerungen

Die Untersuchung konnte zeigen, dass eine Implementation von Mobile Payment auf Basis eines unilateralen Modells im Rahmen der bisherigen Marktteilnehmer möglich ist.

Weiter konnten mehrere Ursachen für die nur langsam verlaufende Markteinführung identifiziert werden.

Eine zentrale Rolle kommt dabei dem *Card Emulation Mode* zu, welcher notwendig ist, um mit dem Terminal kommunizieren zu können. Damit dieser aktiviert werden kann, muss zwingend ein *Secure Element* im Smartphone vorhanden sein, welches physikalisch direkt mit dem NFC-Controller verbunden ist. Die einzige von allen Herstellern implementierte Verbindung besteht zur SIM-Karte und zu einem allenfalls vorhandenen embedded Secure Element. Ob Lösungen mit SD-Karte möglich sind oder ob ein embedded Secure Element vorhanden ist, hängt vom konkreten Smartphone ab. Eine programmatische Aktivierung des Card Emulation Modes aus einer App heraus ist bei den meisten Smartphones nicht möglich. Daher bliebe als universelle Lösung lediglich die Kooperation mit den SIM-Karten Herausgeber, den Mobile Network Operator.

Eng mit diesem Punkt verbunden sind die Anforderungen an das Secure Element. Wie gezeigt werden konnte, ist das Secure Element keine Anforderung aus EMV. Da sich beim Secure Element die oben erwähnten Probleme ebenfalls stellen, verwendet die Lösung ein Credential Store, welcher in die Cloud ausgelagert ist. Damit können die sensiblen Daten auf Servern sicher gespeichert werden. Diese können nach den Anforderungen der Card Schemes gekauft und zertifiziert werden.

Um ein ähnliches Niveau an Sicherheit zu erreichen wie die Lösung mit SIM-Karte, muss auf zusätzliche Technologien zurückgegriffen werden. Als erfolgsversprechend könnte sich dabei die *Trusted Execution Environment*-Technologie herausstellen. Allerdings befindet sich diese Technologie noch in Entwicklung und ist nur unter Android nutzbar.

Für Newcomer stellt die starke Marktmacht der Banken und die enge Verflechtung mit Acquirer und Issuer eine deutliche Markteintrittsbarriere dar. Auch die Card Schemes sind traditionell stark mit dem Banksektor verbunden und bilden daher ebenfalls eine Hürde für Neueinsteiger, wenngleich sich die Card Schemes etwas offener für innovative Lösungen zeigen.

Die vorgeschlagene Lösung orientiert sich aus diesem Grund an dem bestehenden Geschäftsmodell und versucht, dieses sinnvoll zu erweitern.

Dabei wird auf den problematischen Card Emulation Mode verzichtet und stattdessen der *Peer-To-Peer*-Modus verwendet. Dieser kann über die normalen APIs genutzt werden und erleichtert damit die Implementation beträchtlich. Die einfachere Umsetzung kann sich bei einer Produktivversion auch finanziell niederschlagen.

Durch Verzicht auf den strikten Nachrichtenfluss gemäss EMV ergibt sich die Möglichkeit, weitere Daten zwischen Terminal und Smartphone auszutauschen. Das erarbeitete Protokoll kann leicht erweitert, um beispielsweise Loyalty-Lösungen zu realisieren. Damit entstehen auch für die Merchants positive Effekte.

Die Implementation ist unabhängig von der bestehenden Infrastruktur, insbesondere von den übertragenen Daten und der Implementation des EMV-Kernels im Terminal. Damit wird eine vereinfachte Wartung der Software ermöglicht und die Komplexität der bestehenden EMV-Kernel-Implementation nicht weiter erhöht.

Da der Lösungsvorschlag auf ein im Smartphone befindliches Secure Element (wie SIM-Karte oder embedded SE) verzichtet, wird eine Bindung an einen MNO oder Hardware-Hersteller verhindert. Diese beiden Faktoren ermöglichen es, die Lösung ohne die Kooperation mit neuen Playern zu implementieren.

Im Rahmen eines Showcases zeigt die Implementation die Machbarkeit der vorgeschlagenen Lösung.

Im Moment stellt die mangelhafte Unterstützung des Peer-To-Peer-Modus durch Android einen schwerwiegenden Nachteil dar. Dies weil davon auszugehen ist, dass sich der Marktanteil von Android in der Schweiz erhöhen wird.

Alternativ könnte eine Implementation mit der Inverse Reader Mode-Technik erfolgen. Der Nachteil dieser Lösung ist, dass sie vom Standard nicht vorgesehen ist. Insbesondere wird für die Kommunikation kein echtes Transportprotokoll eingesetzt, wie dies beim SNEP-Stack der Fall ist. Daher müsste hier eine proprietäre Lösung entwickelt werden.

Die fehlende Unterstützung von NFC durch das iPhone darf ebenfalls nicht unterschätzt werden. Dies betrifft aber alle Lösungen von NFC-basierten Mobile Payment-Systemen gleichermassen. Die existierenden Lösungsansätze (wie Jackets oder Sticker) sind ästhetisch oder funktional nicht geeignet. Bei einer Markteinführung muss diesem Punkt Aufmerksamkeit geschenkt werden und entschieden werden, ob auf eine Unterstützung des iPhones verzichtet werden kann.

Ein auf Basis dieser Studie zur Marktreife gebrachtes Produkt sollte möglichst rasch auf den Markt gebracht werden. Die Swisscom hat angekündigt, noch in diesem Herbst ein eigenes Produkt zu lancieren. Da der Markt in der Schweiz noch unbewirtschaftet ist, ist es wichtig, von Anfang an präsent zu sein. Nachdem bereits mehrere Produkte auf dem Markt sind, dürfte es bedeutend schwieriger sein, die notwendige Kooperation mit Acquirer und Issuer einzugehen.

Da die Terminal-Implementation vorzugsweise vom Acquirer vorgenommen wird, welcher wohl auch die Smartphone App implementieren müsste, ist das Deployment in der Schweiz relativ einfach, da hier nur

zwei grosse Acquirer existieren. Das Deployment kann dabei über die regelmässig stattfindenden Updates vonstattengehen.

Als eventuelle Schwierigkeit bei der Einführung könnte sich die ungleiche Verteilung der aus der Lösung entstehenden Vorteile herausstellen.

Der Issuer hat durch die Lösung den Vorteil, dass er keine Kooperation mit dem MNO eingehen muss. Wenn er die Cloud selbst implementiert, benötigt er für Mobile Payment auch keine Schnittstelle mehr zum Card Manufacturer, was die Kosten senken würde.

Auf der anderen Seite muss der Acquirer die Lösung implementieren und auch warten. Daher wird der Acquirer vom Issuer eventuell einen finanziellen Ausgleich verlangen. Da sowohl Issuer als auch Acquirer indirekt den Banken gehören, ist es durchaus wahrscheinlich, dass es hier zu einer Einigung kommen würde. Zudem dürfte diese Zahlung geringer ausfallen als die Kosten, welche ein MNO für die Benutzung der SIM-Karte verlangt.

6 Appendix I – Requirements Analyse und Design

6.1 Project Vision für PeerPay

6.1.1 Introduction

Wir stellen uns unter PeerPay eine Zahllösung vor, welche es dem Consumer ermöglicht, mit seinem Smartphone an einem POS-Terminal zu bezahlen. Dabei soll das System kompatibel zum EMV-Standard sein. Weiter soll dem Consumer ermöglicht werden, mehrere Karten auf seinem Mobiltelefon zu speichern und eine für den Bezahlvorgang auszuwählen.

Die Lösung soll, statt eine SIM als Secure Element zu verwenden, einer Cloudlösung den Vorzug geben. Damit kann verhindert werden, dass die Daten bei Verlust des Smartphones in fremde Hände gelangen.

Schliesslich soll PeerPay erweiterbar sein, damit Loyalty-Daten und weitere interessante Informationen wie Kassenbelege oder Abholnummern zwischen dem Smartphone und den Systemen des Merchants ausgetauscht werden können.

6.1.2 Positioning

Bisherige Mobile Payment-Lösungen verwenden den *Card Emulation Mode* und sind daher auf die Kommunikation, wie sie durch EMV vorgegeben wird, beschränkt. Diese limitiert die Erweiterbarkeit des Systems. Ausserdem ist es schwierig, das Smartphone in den Card Emulation Mode zu bringen. Alle bisherigen Lösungen *emulieren* lediglich eine Bezahlkarte und können daher das volle Potential der ins Smartphones eingebaute NFC-Technologie nicht ausschöpfen.

Die Lösung ist bewusst schlank geplant und betrachtet möglichst alle übertragenen Daten als opak. Damit entstehen keinerlei Abhängigkeiten von den übertragenen Daten und damit keine Abhängigkeiten von externen Systemen. Insbesondere ist es das Ziel, dass die Lösung unabhängig von den EMV-Daten bleibt und damit der Wartungsaufwand niedrig gehalten werden kann.

Zurzeit ist kein vergleichbares System auf dem Markt. Im Bereich von Loyalty-Integration gibt es Bestrebungen, diese auf der RF-Schnittstelle des Terminals verfügbar zu machen.

6.1.3 Stakeholder

Merchant Verkäufer von Waren oder Dienstleistungen.

High-Level Goal: Zahlsystem, an dem der Consumer problemlos mit seinem Smartphone zahlen kann.

Problems and Concerns:

- Das Zahlsystem muss mit den bisherigen Lösungen kompatibel sein, um die Einführung zu erleichtern.
- Es soll die Möglichkeit bieten, dass der Merchant eigene Systeme, beispielsweise zu Loyalty-Zwecken, einbinden kann.
- Es soll nur ein einziges Terminal nötig sein, an dem auch mit herkömmlichen kontaktlosen Kreditkarten bezahlt werden kann.

Consumer Konsument von Waren oder Dienstleistungen.

High-Level Goal: Bezahlkarten gemeinsam im Smartphone ablegen und für diese Dienstleistung nicht extra bezahlen zu müssen.

Problems and Concerns:

- Einfache Verwendung des Systems.

Issuer Herausgeber von Bezahlkarten.

High-Level Goal: Nicht gezwungen sein, Kooperationen mit weiteren Teilnehmern einzugehen, da solche den Gewinn schmälern könnten.

Problems and Concerns:

- Keine Kooperation mit MNO erwünscht.

Acquirer Betreiber von Kartenterminal-Lösungen.

High-Level Goal: Lösung, welche dem Consumer und dem Merchant einen Vorteil bietet und von diesen erweiterbar ist.

Problems and Concerns:

- System möglichst einfach in die bestehenden Terminals implementierbar.
- Möglichst keine Abhängigkeiten zum bestehenden Terminal-Code.

6.1.4 Product Overview

PeerPay bildet eine zusätzliche Protokollschicht auf der RF-Schnittstelle des Terminals. Darin werden die zwischen Terminal und Smartphone ausgetauschten Daten übermittelt. Die übertragenen Daten werden dabei nicht verändert und als opak betrachtet.

PeerPay besteht daher aus zwei Teilen: Eine Wrapper-Schicht auf der Terminalseite, welche die an die RF-Schnittstelle gesendeten Daten verpackt und via NFC *Peer-To-Peer*-Protokoll übermittelt. Auf der anderen Seite existiert eine Smartphone App, welche die Daten entpackt und an das Secure Element leitet, welche die für die EMV-kompatible Transaktion nötigen Schritte vornimmt. Anschliessend werden die Daten zurück an das Terminal übertragen und dort verarbeitet.

6.1.5 Summary of Benefits

PeerPay geht die bestehenden Probleme an, indem es den *Peer-To-Peer*-Modus verwendet. Damit werden auf der einen Seite die Limitationen des *Card Emulation Modes* elegant umgangen. Es wird ermöglicht, dass das Wallet als eine normale Smartphone-Applikation gebaut sein kann und keine spezielle Funktionen des Betriebssystems benötigt. Dies vereinfacht die Implementation und macht die Lösung flexibel für Erweiterungen.

Gleichzeitig werden die Daten EMV-kompatibel übertragen, was die Implementation auf dem Terminal einfach macht. Da die Lösung keine Abhängigkeit zum bisherigen Code aufweist, wird der notwendige Wartungsaufwand nur minimal vergrössert.

Ein weiterer Vorteil ist, dass die Credentials in einer Cloud-Lösung EMV-konform gespeichert werden können. Damit entfällt das Requirement für eine SIM-Karte, wodurch keine Kooperation des Issuers mit einem MNO notwendig ist. Die Wertkette des vier Parteien Modells wird dabei nicht verändert.

Als Erweiterung zum Protokoll ist es möglich, dass weitere Daten übertragen werden. Somit kann das System vom Merchant seinen Bedürfnissen entsprechend erweitert werden und beispielsweise für Loyalty-Funktionen genutzt werden.

6.2 Use Cases

6.2.1 Use Case UC1: Bezahlen (Fully dressed)

Name Bezahlen an einem P2P-EFT/POS-Terminal.

Scope Das gesamte PeerPay System.

Goal User-Goal

Primary Actor Consumer

Stakeholders and Interests

- Consumer: Will Produkte oder Dienstleistungen an einem EFT/POS-Terminal möglichst schnell und unkompliziert bezahlen.
- Merchant: Will möglichst schnell und sicher den Bezahlvorgang abwickeln und eine verbindliche Zahlbestätigung erhalten.
- Acquirer: Will vollständige Finanzdaten und eine sichere Cardholder-Verification.
- Issuer: Will dem Consumer ein möglichst einfaches, schnelles und sicheres Bezahlerlebnis bieten, welches günstig und zuverlässig ist.

Preconditions

- Das EFT/POS-Terminal kann NFC P2P Zahlungen verarbeiten.
- Das Smartphone des Consumers kann NFC P2P Zahlungen verarbeiten.
- Der Consumer hat einen entsprechenden Vertrag mit einem Issuer, welcher ihm den Zugang zu einem Zahlungsnetzwerk eines Card Schemes mit seinem Smartphone ermöglicht.
- Das EFT/POS-Terminal kennt den Transaktionsbetrag.

Postconditions

- Der Merchant hat eine Zahlungsbestätigung.
- Der Acquirer hat vollständige und gültige Transaktionsinformationen.

Basic Flow

1. Der Consumer hält sein Smartphone ans EFT/POS-Terminal.
2. Das Smartphone und das EFT/POS-Terminal handeln gemeinsam die Zahlungsformalitäten nach EMV über NFC SNEP aus, gemäss Use Case *Zahlungsformalitäten*.
3. Das Terminal verarbeitet die bestätigten Zahlungsinformationen gemäss EP2 und schliesst die Zahlung ab.
4. Das Handy kann aus dem Funkbereich des Terminals entfernt werden.

Alternative Flows

- **Jederzeit**: Das Mobiltelefon wird aus dem Funkbereich des Terminals entfernt, bevor die Zahlungsformalitäten (Schritt 2 des Basic Flow) ausgehandelt sind.
  1. Der Bezahlvorgang wird abgebrochen.
  2. Der Consumer wird auf seinem Smartphone und auf dem Terminal über die Ursache informiert.
- **Schritt 1**: Der Consumer möchte nicht mit der Standard-Karte bezahlen.
  1. Der Consumer wählt in der Wallet-App die Karte aus, mit der er bezahlen will.
  2. Der Consumer hält sein Smartphone ans EFT/POS-Terminal.
- **Schritt 2**: Die Höhe der Zahlung erfordert eine PIN-Authentifizierung (*high value transaction*):
  1. Dem Consumer wird über das Terminal-Display mitgeteilt, dass er sich mit der PIN authentifizieren muss.
  2. Das Terminal führt mit dem PIN eine Online-PIN-Verzifizierung gemäss EMV durch.[34]
  3. Wenn der PIN nicht verifiziert werden konnte, wird der Bezahlvorgang abgebrochen.
  4. Sonnst wird der Bezahlvorgang bestätigt.
- **Schritt 4**: Die Zahlung konnte nicht bestätigt werden.
  1. Der Bezahlvorgang wird abgebrochen.
  2. Der Consumer wird auf dem Terminal über die Ursache informiert.

Special Requirements

- Das Terminal benötigt eine aktive Verbindung zum Acquirer.

Frequency of Occurrence Bei jeder Zahlung.

Miscellaneous Der Use Case könnte um Pre- und Post-Payment Aktionen erweitert werden, um beispielsweise Gutscheine, Loyalty-Systeme, Quittungen oder sonstiges Feedback zu ermöglichen.

[34] Offline PIN-Verifizierung wäre grundsätzlich auch denkbar. Dann müsste der Consumer aber sein Smartphone während der PIN-Eingabe im Funkbereich des Terminals halten, was Usability-Überlegungen widerspricht. Eine (evtl. vorgängige) Authentifizierung des Consumers auf dem Smartphone wäre aber beispielsweise denkbar. Dies ist gemäss Swisscom (siehe [32]) möglich und durch die Card Schemes gestattet.

6.2.2 Use Case UC2: Zahlungsformalitäten (Fully dressed)

Name Durchführen der Zahlungsformalitäten

Scope Übertragen der EMV Transaktionsinformationen

Goal Sub-Function

Primary Actor EFT/POS-Terminal

Stakeholders and Interests

- EFT/POS-Terminal: Durchführen der EMV-Transaktion
- Consumer: Sichere, schnelle und automatische Transaktionsabwicklung
- Acquirer: Korrekte Transaktion und durchgeführte Cardholder-Verifikation
- Merchant: Sichere, schnelle und automatische Transaktionsabwicklung
- Smartphone: Abwicklung der Transaktion über NFC P2P

Preconditions

- Das Smartphone hat mit einem EFT/POS-Terminal eine Verbindung über NFC P2P / SNEP hergestellt.
- Auf dem Smartphone ist eine entsprechende Wallet-Applikation installiert, die auch mit mindestens einer virtuellen Bezahlkarte konfiguriert ist.

Postconditions

- Die EMV-Transaktion ist korrekt abgelaufen, das Kryptogramm ist korrekt signiert beim Terminal angekommen.
- Das Smartphone kann aus dem Funkbereich des Terminals entfernt werden.

Basic Flow

1. Das Terminal teilt mit einer SNEP *GET* Nachricht dem Smartphone mit, dass es jetzt mit der EMV-Transaktion beginnen möchte.
2. Das Smartphone stellt die Verbindung zum virtuellen Secure Element her. Sobald die Verbindung steht, beantwortet es die *GET*-Anfrage mit einer entsprechenden “Bereit”-Nachricht.
3. Das Terminal sendet die Bits, die jetzt gemäss EMV (Contactless) Protokoll zu senden sind, per *GET* Anfrage ans Smartphone.
4. Das Smartphone leitet diese Bits an das virtuelle Secure Element weiter.
5. Das Smartphone empfängt die Antwort des virtuellen Secure Elements. Es beantwortet mit dieser Information die *GET*-Anfrage des Terminals aus Schritt 3. *Die Schritte drei bis fünf werden nun durchgeführt, bis die EMV-Transaktion gemäss Spezifikation abgeschlossen ist.*

6. Das Terminal teilt dem Smartphone per *PUT* Nachricht mit, dass die EMV-Transaktion nun abgeschlossen ist.
7. Das Smartphone beendet die Verbindung zum virtuellen Secure Element.

Alternative Flows

- **Jederzeit**: Das Smartphone wird aus dem Funkbereich des Terminals entfernt.
  1. Die Transaktion wird abgebrochen.
  2. Der Consumer wird auf seinem Smartphone und auf dem Terminal über die Ursache informiert.
- **Schritt 2**: Es kann keine Verbindung zum virtuellen Secure Element hergestellt werden.
  1. Die Transaktion wird abgebrochen.
  2. Der Consumer wird auf seinem Smartphone über die Ursache informiert.
- **Schritte 3 bis 5**: Die Verbindung zum virtuellen Secure Element bricht ab.
  1. Die Transaktion wird abgebrochen.
  2. Der Consumer wird auf seinem Smartphone über die Ursache informiert.

Special Requirements

- Das Smartphone benötigt eine aktive Verbindung zum virtuellen Secure Element. Dies könnte eine mobile Datenverbindung sein, kann aber auch lokal sein.
- Das Terminal braucht normalerweise auch eine Online-Verbindung um die PIN-Verifikation durchzuführen.

Frequency of Occurrence Bei jeder Zahlung.

Miscellaneous

- Das Übertragen der EMV Transaktionsdaten könnte verkürzt werden, in dem nur sich effektiv ändernde Daten übertragen werden. Beispielsweise sieht EMV zu Beginn den Reset und das Aufstarten der Zahlungskarte vor. Dies ist aber im gegebenen Fall unnötig.

6.3 Interviews

In den nachfolgenden Unterkapiteln findet sich eine Zusammenfassung der Kernaussagen der geführten Interviews.

6.3.1 Interview mit UBS CardCenter

Das Interview wurde am 21. März 2013 mit Herrn M. Bosshard und Herrn J-P. Koelbl durchgeführt [8].

- Das UBS CardCenter (UBSCC) stelle für die UBS die Kreditkarten aus und handhabe auch das weitere Processing. Dazu zählen zum Beispiel Zahlungen zu verifizieren oder Rechnungen auszustellen

- Das UBSCC braucht dafür eine Lizenz von Visa und von MasterCard
- Die Anforderungen an das SE sei implizit gegeben. FIPS 140-2 L2 oder L3 sei massgebend, demnach sei lediglich ein separater Crypto-Prozessor notwendig.
- Tokenisation sei lediglich ein psychologisches Mittel.
- USA setze noch fast vollständig auf Magstripe, und nicht auf EMV.
- Bei Karten des UBSCC könne der Embosser Name nicht über NFC ausgelesen werden. Es existierten Pläne, Magstripe über NFC nicht zuzulassen, oder dies nur auf expliziten Wunsch des Kunden zu aktivieren.
- Eine Bezahlkarte OTA zu aktualisieren sei theoretisch möglich, erfordert aber, dass der Kunde ein zweites Mal die Karte ans Terminal halte.
- Das UBSCC sehe Mobile Payment vor allem aus Kostengründen negativ entgegen. Die Prozesse für die Kartenbestellung seien heute hochoptimiert. Ein neuer Partner würde zu beginn somit viele neue Kosten im Personalisierungsprozess verursachen.
- Wenn die Zusammenarbeit mit einem MNO nicht mehr Kosten verursache, als eine Karte zu produzieren, sei eine solche Zusammenarbeit denkbar.
- Bei den embedded SE sei das Problem, dass es viele Hersteller gäbe, mit denen man Partnerschaften eingehen müsse. Ausserdem sei die Schweiz ein kleiner Markt und man habe somit keinen Einfluss auf die zukünftigen Produktentwicklungen bei den Partnern.
- Es beständen noch keine verbindlichen Standards um Loyalty vom EFT/POS aus zu betreiben.
- Issuer wollten Wallet-Applikationen nicht selbst entwickeln / betreiben; dies sei nicht ihre Kernkompetenz und sei teuer und komplex (Wartung, verschiedene Betriebssysteme, etc.).

6.3.2 Interview mit Aduno

Das Interview wurde am 22. März 2013 mit Herrn R. Fäh durchgeführt [17].

- Seit Sommer 2012 sollten alle Terminals NFC beherrschen.
- Einige grosse wie Coop / Migros würden erst 2013 nachziehen.
- Kartenerneuerung brauchten aber noch einige Zeit.
- Vorläufig gäbe es keine Debitkarten mit NFC, obwohl dies technisch machbar wäre. Dies, weil die Banken an den Kreditkarten mehr verdienen würden.
- Schweiz sei aber grundsätzlich ein “Debit-Land”.
- Debitkarten sei aber für Issuer / Banken ein Verlustgeschäft.
- Im Vending-Bereich (Kleinzahlungen an Automaten) sei in Zukunft neben Kleingeld “Contactless only” zu erwarten. Dies, weil es besser geschützt sei gegen Vandalismus.
- Prepaid Kreditkarten seien sehr erfolgreich und würden an Personen ab 14 Jahren abgegeben, besässen aber kein Embosser Name.
- Es gäbe momentan kein Loyalty- oder Quittungs-System für Wallets oder Wallet-ähnliche Dienstleistungen.
  - Es brauche somit einen separaten “Touch” für Loyalty.
- Wallet-Anwendungen sollen in der Domäne der Issuer sein, und nicht bei 3rd Parties wie Swisscom / SBB.
  - Dieses müsse offen für andere Teilnehmer sein, auch aus anderen Branchen.
  - Issuer würden sich auf gemeinsames Wallet einigen können.
- Bei Aduno sei das SIM-System der Favorit.

- Abhängigkeiten zu Mobile Device Manufacturer sei zu vermeiden, weil auf diese keinen Einfluss ausgeübt werden könne, somit eine einseitige Abhängigkeit bestehen würde.
- Sunrise und Swisscom seien beide “ready”, aber Swisscom sei der Leader.
- Dass man nicht von einem Mobile Device Manufacturer abhängig sei und auf die nationalen MNO auch Einfluss nehmen könne, dürfe auch etwas kosten.
- Contactless Payment soll bei Kleinbeträgen ohne PIN möglich sein, bei Grossbeträgen jedoch nur mit PIN.
- Die Terminals würden mindestens einmal im Jahr, normalerweise aber häufiger, ein Update erhalten.
  - Die Terminals meldeten sich dazu jede Nacht beim Service Center.
- Eine Neu-Zertifizierung sei nur bei Kernel-Änderungen nötig.
- Schweizer Merchants kauften gerne neue und aktuelle Terminal-Hardware.

6.3.3 Interview mit SIX Payment Services

Das Interview wurde am 21. März 2013 mit Herrn S. Breite durchgeführt [70].

- Die SIX sei interessiert, mehr Informationen zur Zahlungstransaktion dazu zu transportieren, wie zum Beispiel Line-Items, Loyalty, etc.
- SIX setze sich dafür ein, Services und Server für Wallet-Anwendungen anzubieten, respektive zu betreiben.
- Die Acquirer hätten die terminalseitige Umstellung auf NFC bereits weitestgehend abgeschlossen.
- SIX werde aber weiterhin im B2B-Bereich tätig sein, und keine eigene Mobile Wallet Services anbieten.
- Banken würden entscheiden, welche Features ihre Karten haben. Weil aber Debit nur Margen im Rappen-Bereich brächten, würden Kreditkarten forciert.
- Bei der Deutschen T-Mobile beanspruche das Applet der Bezahlkarte rund 50kB vom Speicher der SIM-Karte.

6.3.4 Präsentation des Swisscom Wallet

Die Präsentation fand am 3. April 2013 bei der Abrantix statt. Das Produkt wurde von Herrn S. Mittal vorgestellt [32].

- Swisscom Wallet stehe allen Anbietern offen, auch anderen MNO.
- Swisscom selbst wolle aber keine eigenen Karten anbieten.
- Die Personalisierung der Bezahlkarten solle via die bestehenden Personalisierer vonstatten gehen. Namentlich erwähnt wurden Trüb und Oberthur.
- SIM-Karten müssten alle ausgetauscht werden. Dies geschehe entweder auf Wunsch des Consumer oder durch die reguläre Halbwertszeit der Karten; auf jeden Fall aber kostenlos für den Consumer.
- Die modernen SIM-Karten würden sich neben dem integrierten SE durch Speicherplatz im Umfang von rund 700 kB bis 1 MB auszeichnen. Rund 250 kB davon würden aber die GSM Applikationen bereits für sich beanspruchen.
- Swisscom wolle alle neuen SIM-Karten von Haus aus bereits mit den nötigen MasterCard und Visa Kerneln ausrüsten und später nur noch die entsprechenden Personalisierungs-Information OTA auf die Karten laden.

- Alle installierten Karten sollen über eine kostenlose und Swisscom eigene Wallet Applikation verwaltet werden können.
- Der Speicher für die Applets solle in periodischen Abständen den Karten-Issuern verrechnet werden. Die Kosten seien im zweistelligen Bereich pro Monat.
- Issuern benötigten keine weiteren Investitionen, da sie alle Interfaces mit ihren Partnern weiter benutzen könnten.
- Loyalty sei zwar mit der Swisscom Lösung möglich, allerdings nur mit einem Tap für Loyalty und dann mit einem weiteren für die eigentliche Zahlung.

6.3.5 Interview mit Swisscom

Das Interview wurde am 5. April 2013 mit Herrn H. Staumann durchgeführt [30].

- NFC sei vor allem Convenience, ein neues Erlebnis. Payment mache nur ein kleiner Teil dieses Erlebnisses aus.
- Denkbar seien neben Bezahlkarten auch Tickets, Zutrittskarten (“Badge”), Transport-Ausweise.
- NFC ersetze aber nicht nur Karten. So könnten beispielsweise intelligente Verpackungen Auskunft über Inhalte für Allergiker geben. Wichtig sei dabei aber, dass die Usability bedacht wird. So könnte im Beispiel eine Ampel oder ein “Thermometer” aufgrund der individuellen Verträglichkeit die Gefahr für den Konsumenten visuell zeigen.
- Quintessenz sei, dass “alles” mit einem Tap funktioniere. Ob dies technologisch nun Smart Tags, Peer-To-Peer Modi oder sonst was ist, sei eigentlich egal.
- Der MNO wolle sich nicht in das bestehende vier Parteien Modell drängen. Er werde lediglich ein Dienstleister “am Rande”, wie dies beispielsweise die Kartenhersteller seien. Jedoch vermittle der MNO einen konstanten Service und erhebe deshalb eine regelmässige Gebühr.
- Diese Gebühren würden dabei dem Angebot angepasst erhoben. Jährlich, monatlich, wöchentlich, täglich, dies sei nur Verhandlungssache.
- In Japan sei der Markt durch die Einführung von NFC insgesamt gewachsen, und alle Aktoren hätten dabei gewonnen.
- Schliesslich seien die Banken aber die grössten Kunden der MNO. Sie kauften dort die Telecom Services ein, aber auch Hosting Dienstleistungen und Weiteres.
- Der Vorteil der SIM sei, dass sie im Gegensatz zu den anderen Möglichkeiten nicht an ein Gerät gebunden sei.
- Alles, was im Handy sei, sei potenziell unsicher. Ein Handy könne verseucht werden, die SIM-Karte aber nicht.
- Swisscom sei daran interessiert, ihr Produkt auch anderen MNO zur Verfügung zu stellen. Diese müssten aber ihre eigenen Prozesse zur Personalisierung bereitstellen. Es sei aber das Ziel, mit den anderen MNO ein einvernehmliches Verhältnis bez. Mobile Payment zu pflegen, ähnlich der Rufnummernportierung.
- Die SIM-Karte solle direkt im Shop ersetzt werden können, und die Neu-Personalisierung von dort direkt ausgelöst werden.
- Swisscom habe auch die Integration des Callcenters vorangetrieben. Ein Anruf dort, und die Partner würden über die Sperrung der Karte(n) informiert.
- Ein Anbieter könne auch jederzeit von sich aus nur sein Dienst sperren lassen.
- Werde die SIM gesperrt, zum Beispiel wenn das Abo ablaufe, verfielen auch die darauf aufgeschalteten Karten.
- Bei einem Providerwechsel müssten die virtuellen Karten wieder neu angefordert werden.

- Grosse Ketten, wie Migros, würden schnellere Prozesse an den Kassen anstreben, und NFC sei ein mögliches Hilfsmittel hierfür.
- Relevant für den Durchbruch im Markt sei die Zahl der Akzeptanzstellen. Bei den Bezahlterminals schnelle diese Zahl zurzeit rasant nach oben.
- Auch die Zahl der NFC fähigen Konsumentengeräte (Smartphones, Tablets, etc.) sei wichtig. Swisscom fördere dies, in dem, sofern verfügbar, jeweils nur die NFC fähige Version eines Smartphones eingekauft und angeboten werde.
- Das "Apple Problem" werde sich, sobald der Markt NFC akzeptiert habe, lösen. Entweder kauften sich die Kunden keine iPhones mehr, oder Apple ziehe nach und rüste seine Geräte mit NFC aus.
- Um Karten auf die SIM zu laden, seien neue SIM-Karten nötig. Dies sei aber kein Problem und falle in den normalen Zyklus. (Denn für LTE brauche es sowieso neue SIM-Karten.)
- Bei den Bezahlkarten würden die "Standard-Applets" von Visa und von MasterCard bereits bei der SIM-Herstellung auf die Karte geladen, um weniger Speicher zu verbrauchen. Nur die Personalisierungsinformationen würden per OTA auf die SIM geladen.

6.3.6 Interview mit Sunrise

Das Interview wurde am 26. April 2013 mit Herrn T. Graf durchgeführt [55].

- Es seien schon Tests mit der UBS gemacht worden.
- Die Technik sei keine grosse Hürde im Ganzen.
- Obwohl schon lange prophezeit, könne, dank dem Rollout der neuen Terminals, in Kürze (dieses oder nächstes Jahr) wirklich der Rollout für Mobile Payment gelingen.
- Payment sei aber nur ein kleiner Bereich.
- Man sehe sich als Enabler, der vor allem die Infrastruktur zur Verfügung stelle.
- Wenn Swisscom eine gute Technologie bei ihren Kunden durchsetzten könne, müsse Sunrise mitziehen, um konkurrenzfähig zu bleiben. Die gleiche Technologie, oder zumindest die gleichen Grundlagen, zu verwenden sei dabei nicht ausgeschlossen.
- Für einige Anforderungen sei das Secure Element überhaupt nicht nötig. Aber auch solche Anwendungen sollen berücksichtigt werden.
- Zurzeit halte man aber noch zurück, was die Förderung von NFC betreffe. Strategisch habe dies noch keine Priorität.
- Der Markt für Wallets werde sich zuerst zersplittern. Jeder würde erstmal sein eigenes Wallet machen wollen (beispielsweise die Banken, der Detailhandel, die SBB [71]). Die MNOs könnten hier den Markt einen, in dem sie ein gemeinsames Framework bereitstellten.
- Der Endkunde soll die Kosten für das System nicht direkt tragen müssen. Diese sollen die Service Provider tragen. Nämlich pro aktivierte Karte pro Zeitperiode.
- Ziel einiger Issuer sei es, eine Verschiebung hin zu den lukrativeren Kreditkarten Transaktionen zu erreichen.
- Um die Technologien verwenden zu können, müssten neue SIM-Karten gekauft werden. Diese seien aktuell aber etwa um den Faktor fünf teurer als herkömmliche SIM-Karten.
- Es werde rund 512 kB an Speicherplatz für Dritt-Applets auf den Karten haben.
- SIX Payment Services arbeite mit der österreichischen Firma Nexperts an einer Loyalty Lösung zusammen.
- Es sei zu erwarten, dass, wenn der Consumer den Anbieter wechsle, sich für die Service-Übergabe ein ähnliches Verfahren entwickle, wie bei der Rufnummernportierung.
- Das grösste Problem sei zurzeit, dass man sich nicht auf Tarife einigen konnte.

7 Appendix II – NFC: Technik und Standards

Es ist nicht im Scope dieser Arbeit, die Funktionsweise von NFC, RFID und EMV Contactless im Detail zu erklären. Dazu sei auf die bestehende Literatur (siehe Literaturverzeichnis) verwiesen.

Da aber in dieser Thesis mehrmals auf Spezifika der zugrunde liegenden Normen eingegangen wird, werden hier zum besseren Verständnis kurz die wichtigsten Zusammenhänge erläutert. Denn in der Literatur sind die Zusammenhänge zwischen den verschiedenen Normen oft nicht oder nicht richtig wiedergegeben.

7.1 Internationale Standards

Die technischen Spezifikationen im Bereich von NFC werden von verschiedenen Gremien geschaffen. In diesem Bereich relevante internationale Normierungsgremien sind die ISO/IEC, die JIS und ECMA International. Gewisse Normen der ECMA wurden in eigene ISO-Standards überführt, andere wurden nicht übernommen und wieder andere Themen wurden durch die ISO neu standardisiert.

Die zentralen Normen für den NFC-Bereich sind neben ECMA-340 (NFCIP-1) beziehungsweise ISO 18092 die ECMA-352 (NFCIP-2) beziehungsweise ISO 21481. Es ist anzumerken, dass dies lediglich die Grundlegenden internationalen Normen im Bereich von NFC sin. Daneben existiert noch eine Vielzahl weitere Normen, Nebenbüchern, Technical Specifications, etc. Auf diese wird hier nicht weiter eingegangen. Die unten stehenden Tabellen geben einen Überblick über die für diese Thesis relevanten Normen.

Norm	Bezeichnung
ECMA-340	Near Field Communication Interface and Protocol (NFCIP-1)
ECMA-352	Near Field Communication Interface and Protocol-2 (NFCIP-2)
ECMA-356	NFCIP-1 RF Interface Test methods
ECMA-362	NFCIP-1 Protocol Test Methods
ECMA-373	Near Field Communication Wired Interface (NFC-WI)
ECMA-385	NFC-SEC: NFCIP-1 Security Services and Protocol
ECMA-386	NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES
ECMA-390	Front-End Configuration Command for NFC-WI

Tabelle 6: Übersicht über die ECMA-Normen zu NFC (Auswahl)

Norm	Bezeichnung
ISO 7816	Integrated Circuit Card
ISO 14443	Proximity cards
ISO 15693	Vicinity cards
ISO 18092	Near Field Communication Interface and Protocol (NFCIP-1)
ISO 21481	Near Field Communication Interface and Protocol-2 (NFCIP-2)
ISO 23917	NFCIP-2 Protocol Test Methods

Tabelle 7: Übersicht über die ISO Normen zu NFC und Proximity Cards (Auswahl). Die ersten drei Normen wurden hier der Vollständigkeit halber aufgenommen, da sie zwar nicht direkt mit NFC zusammenhängen, aber für die Kommunikation mit Chipkarten relevant sind.

7.2 NFC Forum

Das NFC Forum ist ein unabhängiges Gremium, welches aus Herstellern, Entwicklern, sowie weiteren an der Weiterentwicklung von NFC interessierten Unternehmen und Organisationen besteht. Das NFC Forum ist ein rein normatives Gremium, welches Standards unabhängig von nationalen oder internationalen Gremien verabschiedet.

Im Gegensatz zu den nationalen und internationalen Normierungsinstituten (wie beispielsweise der ISO/IEC) verabschiedet das NFC Forum Spezifikation in aller Regel deutlich rasche. Daher enthalten die NFC Forum Spezifikationen typischerweise keine Querverweise zu internationalen Normen. Tatsächlich ist es bisweilen so, dass die ISO oder die ECMA die Spezifikationen des NFC Forums in ihre Normenreihen übernehmen. Dabei werden die Inhalte in aller Regel neu formuliert und spezifiziert. Aus diesem Grund ist es relativ schwierig und entsprechend aufwendig einander entsprechende Normen zu identifizieren.

Norm	Bezeichnung
ANALOG	NFC Analog Specification
DIGITAL	NFC Digital Protocol
ACTIVITY	NFC Activity Specification
LLCP	Logical Link Control Protocol
NDEF	NFC Data Exchange Format
RTD	NFC Record Type Definition
RTD-Text	Text Record Type Definition
RTC-URI	URI Record Type Definition
SNEP	Simple NDEF Exchange Protocol
T4TOP	Type 4 Tag Operation Specification

Tabelle 8: Übersicht über die Spezifikationen des NFC Forums (Auswahl)

Da die Spezifikationen des NFC Forums deutlich rascher publiziert werden und dadurch näher am Marktgeschehen sind, hat das NFC Forum auch Spezifikationen für höher liegende Protokollschichten definiert. Die internationalen Standardisierungsgremien haben bisher darauf verzichtet; wohl aus dem Grund, weil die Technologie relativ neu ist und die höheren Schichten naturgemäss häufiger Änderungen durchlaufen.

Die von ISO und ECMA spezifizierten Teile der Kommunikation beziehen sich vor allem auf die Übertragungstechnik (Physical Layer, Low-Level Protocol) sowie auf die darauf aufsetzende Bitcodierung und Encapsulation (Frame Format). Gerade komplexere Kommunikationsmodi wie SNEP, welche die Vorteile von NFC als bidirektionales Kommunikationsprotokoll ausspielen können, sind ausschliesslich vom NFC Forum spezifiziert.

7.3 NFC Protokollaufbau und Funktionsweise

NFC baut auf der RFID-Technologie auf, definiert aber die Trägerfrequenz fix bei 13.56 MHz. Diese relativ hohe Frequenz schränkt den Aktionsradius der Technologie auf wenige Zentimeter ein. Theoretisch ist der Empfangsbereich von NFC nur gerade 5mm (sic!) hoch [72, pp.17–18, 51]. Aufgrund technischer Limitationen beim Antennenbau ist es nicht möglich, den minimal spezifizierten Empfangskörper zu erreichen. In der Realität zeigt sich, dass die Kommunikation innerhalb von ca. zwei bis sechs Centimeter möglich ist (abhängig von Leser und Karten). RFID lässt im Gegensatz dazu mehrere verschiedene Frequenzen zu, mit denen Empfangsbereiche von mehreren Metern möglich sind.

Der Verzicht auf eine grosse Übertragungsdistanz erfolgte bewusst, um das Mithören der Kommunikation zu erschweren. Allerdings zeigte sich relativ rasch, dass zumindest Abhören der Kommunikation (“Eavesdropping”) auch “ausserhalb von Laborbedingungen mit billigen und portablen Geräten” möglich ist [73, pp.12–13][35].

[35] Übersetzung der Autoren.

NFC unterscheidet nicht prinzipiell zwischen dem Gerät, welches den Funkbereich aufbaut und demjenigen, welches es absorbiert, wie dies RFID Geräte tun. Das Gerät, welches das Feld aufbaut, wird als *Initiator* bezeichnet, dasjenige, welches es absorbiert, als *Target*. Im Falle von NFC wird der Modus (Initiator oder Target), in welchen jedes der beiden Geräte geht, dynamisch ausgehandelt. Das Protokoll zur Wahl des Modus' wird als *Activity Selection* bezeichnet und ist in [74] beschrieben. Dabei wird unter anderem das Kommunikationsprotokoll (NFC-A, NFC-B oder NFC-F) ausgehandelt und die Geräte verständigen sich darauf, ob die Kommunikation im aktiven oder passiven Betrieb stattfinden soll. Im Fall des passiven Modus wird vom Initiator das Feld während der gesamten Kommunikation aufrechterhalten; der Initiator übermittelt die Daten durch *amplitude shift keying* (NFC-A und NFC-B) [72, pp.32–39], während das Target durch Lastmodulation (*load modulation*) antwortet [72, p.44].

Im aktiven Modus besteht keine Notwendigkeit, dass der Initiator das Target mit Strom versorgen muss; daher erzeugt jedes Gerät sein eigenes HF-Feld, während es Daten übertragen möchte [54, pp.93–95].

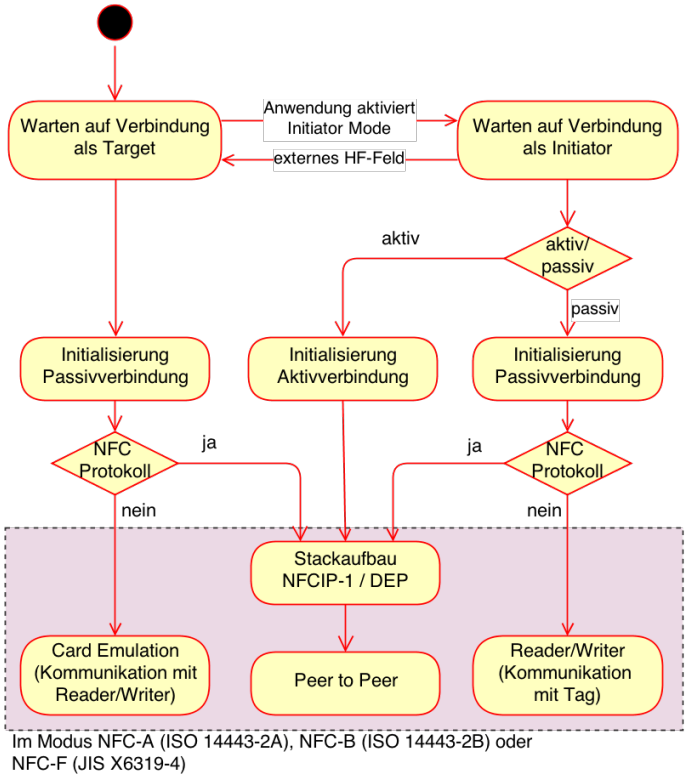

Abbildung 34: Aufbau der Kommunikation für die drei NFC Modi (Activity Selection) [75, pp.12–68, 128–145], [76], [77], [54, pp.91–105]

Die Basis für alle NFC-Betriebsarten stellt ISO 18092 dar, was ISO 14443 Typ A umfasst [54, pp.89–91]. Weiter kann in jeder der drei Arten auf Basis von NFC-A (ISO 14443-2A) oder NFC-B (ISO 14443-2B) kommuniziert werden. Ausserdem sind die Modi in ISO 15693 auch für *Vicinity Cards*, also Karten, welche auf grössere Distanz funktionieren, spezifiziert.

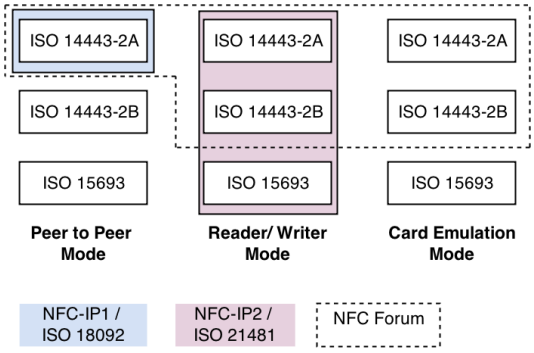

Abbildung 35: Überlappung der Standards nach ISO, ECMA und NFC Forum für die drei Betriebsmodi im passiven Betrieb [78], [72], [75], [66], [68]

Peer-To-Peer Mode Der Peer-To-Peer Mode (abgekürzt P2P-Mode) erlaubt es, eine bidirektionale Kommunikation aufzubauen. Weder der Card Emulation- noch Reader/Writer-Modus gestatten dies sonst noch. Ein weiterer Unterschied ist, dass das NFC Forum für den Peer-To-Peer Modus einen kompletten Stack spezifiziert, was bei den anderen beiden Protokollen nicht der Fall ist.

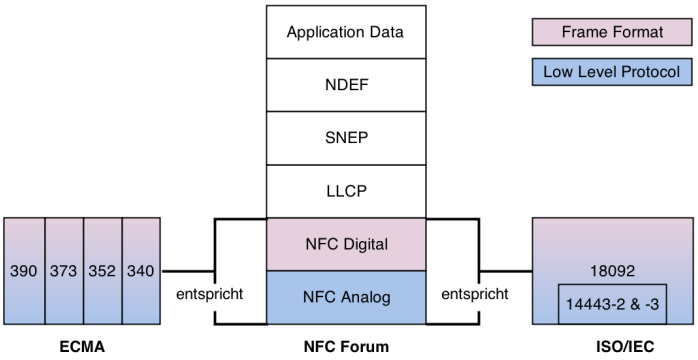

Abbildung 36: Aufbau des Protokoll-Stacks im Peer-To-Peer Mode (SNEP), spezifizierte Teilbereiche nach ECMA, NFC Forum, ISO/IEC [72, pp.43–69], [75], [66], [68]

Card Emulation Mode Wie bereits beschrieben, dient der Card Emulation Mode dazu, mit einem NFC-fähigen Gerät eine ISO 14443-konforme Proximity Card simulieren zu können. Das NFC-Gerät muss sich dabei immer im Target-Modus befinden, darf also selbst kein Feld aufbauen.

Die Kommunikation findet in diesem Fall nach ISO 7816 mittels APDUs statt. Dabei sendet der Initiator Anfragen an das Target, welches darauf antwortet. Im Gegensatz zum Peer-To-Peer Modus darf das Target von sich aus keine Anfragen an den Initiator stellen, das heisst, keine Kommunikation beginnen. Es darf ausschliesslich auf Anfragen antworten.

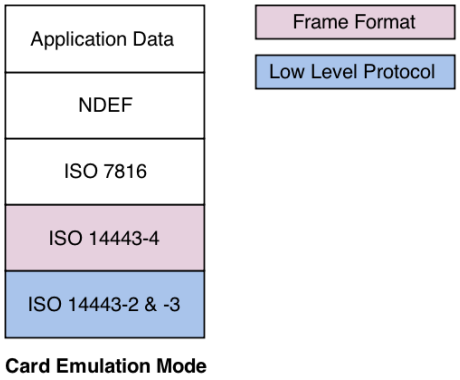

Abbildung 37: Aufbau des Protokoll-Stacks im Card Emulation Mode [78]

8 Appendix III – Ablauf einer EMV-Transaktion

Die Kommunikation zwischen Karte und Terminal findet bei EMV nach ISO 7816 statt (vgl. Card Emulation Mode). Dabei werden sogenannte APDUs verwendet. Diese Datenpakete sind hoch strukturiert und transportieren die Kommandos sowie die Antwort. Jede Request-APDU besteht aus einem Header uns je nach Kommandotyp aus einem Body. Die Response beinhaltet mindesten zwei Statusworte und je nach gesendetem Kommando den Body.

Die APDUs können theoretisch eine Länge von 65546 Bytes erreichen; die im EMV-Umfeld verwendeten APDU sind aber typischerweise nur wenige Bytes lang.

Auch der Ablauf, den ein EMV-kompatibles Terminal durchführen muss, ist genau festgelegt. Dabei finden direkt nach dem Aufbau der Verbindung mehrere Kommunikationsphasen zwischen dem Terminal und der Karte statt. Nachdem die *Card Action Analysis* abgeschlossen worden ist, ist keine weitere Kommunikation zwischen Karte und Terminal mehr nötig. Insbesondere verfügt das Terminal an dieser Stelle bereits über alle nötigen Daten, dass eine *Cardholder Verfification* durchgeführt werden kann, wenn dies notwendig sein sollte.

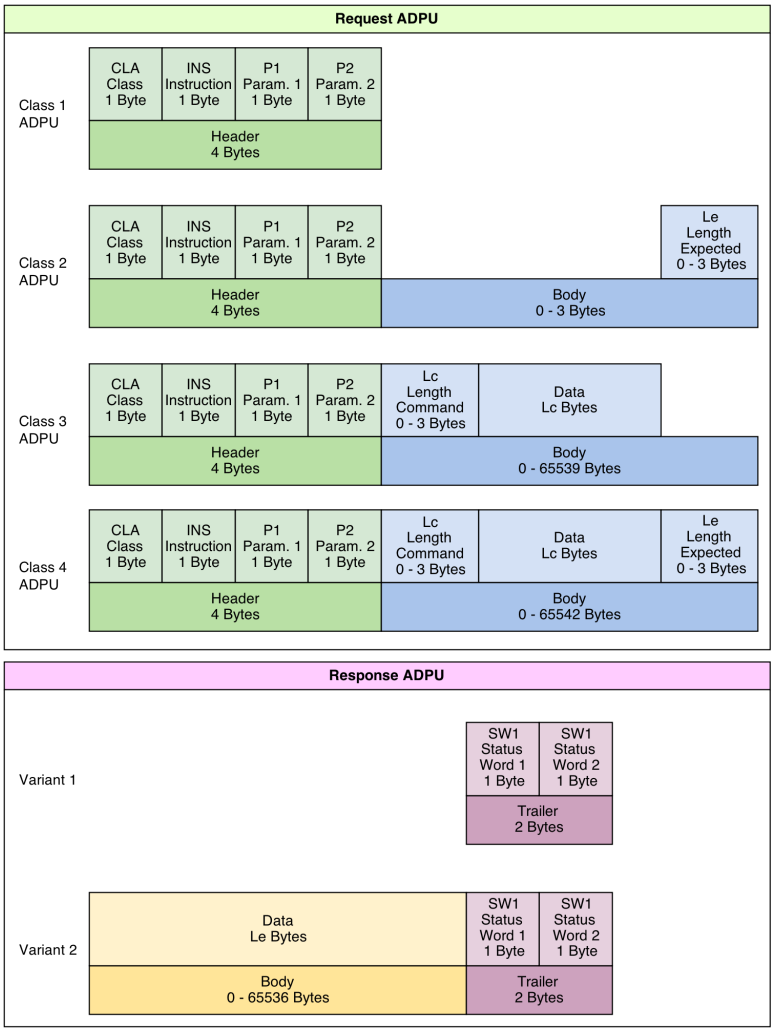

Abbildung 38: In der Spezifikation *ISO 7816-4* [79] gibt vier definierte Klassen von ADPU-Request Nachrichten, und zwei Arten von ADPU-Response Nachrichten, die sich aus dem Text ableiten. Die sechs Nachrichten-Container sind im Diagramm schematisch dargestellt. Der grüne Teil (teilweise *Header* genannt) ist allen Request-Klassen gemein, der blaue Teil (teilweise *Body* genant) ist unter den Request-Klassen verschieden. Bei den Response-Nachrichten ist der zwei Byte grosse Trailer (rot) obligatorisch. Der Daten-Teil (gelb) ist genau so gross, wie im *Le* Feld der Anfrage angegeben und wird nur gesendet, wenn keine Fehler bei der Verarbeitung aufgetreten sind.

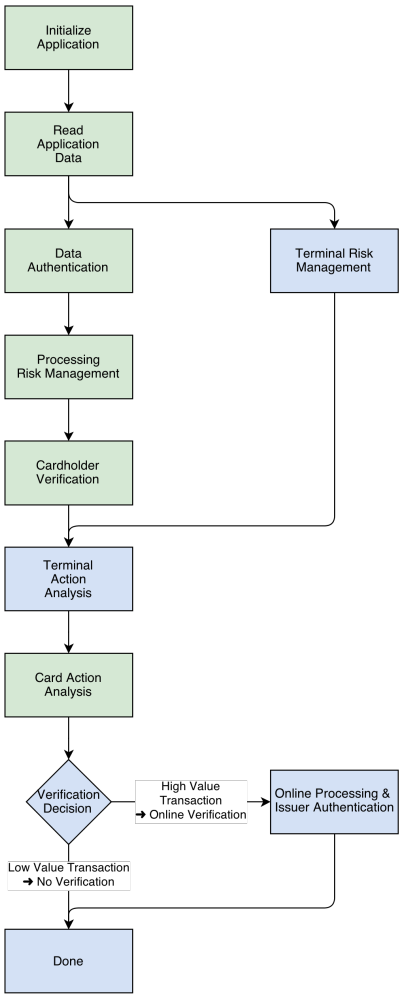

Abbildung 39: Das Diagramm zeigt eine typische EMV Transaktion. Alle grünen Aktionen bedingen ein Befehl ans (virtuelle) Secure Element. Bei den blauen Aktionen ist nur das EFT/POS-Terminal und gegebenenfalls dessen Backend involviert. Es ist ersichtlich, dass ab der *Verification Decision* keine Kommunikation mit dem SE mehr durchgeführt wird. Die Verbindung kann dann geschlossen werden und der Consumer kann sein Smartphone aus dem Funkbereich des EFT/POS-Terminal entfernen.

9 Glossar

Acquirer Der *Acquirer* stellt die Infrastruktur zur Abwicklung von elektronischen EMV Zahlungen gegen eine Gebühr Merchants zur Verfügung.

APDU Die *Application Protocol Data Unit* stellt die Kommunikationseinheit zwischen Chipkarten (sowohl für kontaktbehaftete Karten als auch für kontaktlose Proximity Cards) dar. Der Aufbau von APDUs ist in ISO 7816 spezifiziert.

B2B *B2B* steht für *Business to Business* und bezeichnet Geschäftsbeziehungen zwischen Unternehmen.

Bezahlkarte Eine *Bezahlkarte* ist eine Karte im Format *ID-1* gemäss *ISO/IEC 7810*. Bezahlkarten gemäss EMV sind mit einem Sicherheitschip bestückt. Siehe Chipkarte.

Card emulation Mode Modus von NFC, in welchem sich ein NFC-Gerät (zum Beispiel ein Smartphone) wie eine herkömmliche *contactless Smartcard* verhält. Dieser Modus wird von Smartphones verwendet, um gegenüber POS-Terminals wie eine Bezahlkarte zu wirken.

Card OS (Card Operating System) Ein *Card OS* oder *Card Operating System* ist ein Betriebssystem für Chipkarten. Jede Chipkarte braucht ein solches Programm. Es gibt verschiedene Standards, die beschreiben, wie sich das Card OS gegenüber einem Kartenleser und gegenüber unter dem OS ausgeführten Applets zu verhalten hat. Der wichtigste Standard dafür heisst *GlobalPlatform* und wurde ursprünglich von Visa entwickelt.

Card Scheme Unter *Card Schemes* versteht man die Unternehmen hinter den Bezahlkarten-Marken (wie beispielsweise MasterCard, Visa oder American Express). Card Schemes geben den Acquirern und den Issuern über die in EMV festgelegten Vorgaben hinaus weitere Anweisungen, wie genau Karten und Terminals zu funktionieren haben und wie Zahlungen zu verarbeiten sind.

Chipkarte *Chipkarten* sind Plastikträger im Format *ID-1* (gemäss *ISO/IEC 7810*) mit genormten Kontaktflächen (gemäss *ISO/IEC 7816*), welche ein Chip enthalten. Dieser hat neben einem Speicherbereich einen eigenen Prozessor und ist daher in der Lage, Befehle auszuführen, den Speicherinhalt zu abstrahieren und Zugriffe einzuschränken.

Chipkarten werden manchmal auch als *Smartcards* bezeichnet.

Consumer Der *Consumer* bezieht Waren oder Dienstleistungen vom Merchant und möchte dies mit seiner Karte bezahlen. Er besitzt dazu eine Bezahlkarte von einem Issuer.

Contactless Smartcard Chipkarte, welche Kontaktlos ausgelesen werden kann. Contactless Smartcards können gleichzeitig auch Kontaktflächen einer herkömmlichen Chipkarte aufweisen. Als Funkstandard kommt typischerweise *ISO/IEC 14443* zum Einsatz.

EFT/POS *EFT/POS* (manchmal auch EFTPOS geschrieben) steht für *Electronic Funds Transfer at Point Of Sale* und beschreibt somit das Terminal-Gerät, an dem ein Consumer mit seiner Bezahlkarte oder seinem Smartphone mit Mobile Payment Fähigkeit bezahlt.

embedded Secure Element, embeddded SE Auf die Hauptplatine des Smartphones aufgelöteter oder im NFC Controller eingebauter Chip, welcher funktional mit demjenigen eines Secure Elements identisch ist.

Embosser Name Der *Embosser Name* ist der Name des Inhabers einer Bezahlkarte. Er ist auf der Karte aufgedruckt oder meist auch eingeprägt. Der Prägedruck ist nur noch bei Kreditkarten üblich und wurde herkömmlich mit Imprinter-Geräten auf ein Belegformular übertragen. Im europäischen Raum ist diese Methode kaum noch anzutreffen.

Es gibt auch Bezahlkarten ohne Embosser Name, meist sind dies anonyme Prepaid Kreditkarten oder Firmenkarten.

EMV Weltweit gültige Spezifikation für den Zahlungsverkehr mittels Chipkarte. Bei den Karten bietet EMV im Gegensatz zum Magstripe-Verfahren den Vorteil, dass ein Chip auf der Bezahlkarte eingesetzt wird, der nicht ausgelesen werden kann und der Berechnungen durchführen kann. So kann beispielsweise mit Public- / Privat-Key Verfahren die bei Magstripe häufige durchgeführte Replay-Attacke verhindert werden. Als Chips kommen sogenannte Secure Elements zum Einsatz.

EMV regelt aber auch das Zusammenspiel der Stakeholder im Zahlungsprozess. Siehe dazu das vier Parteien Modell.

EMVCo Die EMVCo ist eine von den grossen Kreditkarten-Unternehmen gegründete Organisation, welche über die EMV-Standards wacht und diese weiter entwickelt.

GlobalPlatform GlobalPlatform ist eine Industrievereinigung, welche das Ziel hat Spezifikationen für sichere Datenspeicherung und Kommunikation zu entwickeln. Insbesondere spezifiziert GlobalPlatform Anforderungen an ein Secure Element.

GSMA Die *GSM Association* ist eine Industrievereinigung, welche die Interessen der *MNOs* repräsentiert. Derzeit gehören der GSMA fast 800 Mobilfunkbetreiber aus über 220 Ländern an.

Hardware Security Module Bezeichnung für ein *Secure Element*. Hardware Secure Element streicht das lokale Vorhandensein des Secure Elemnts heraus, also dass es sich nicht um eine Cloud-Lösung handel.

IPC Unter *Inter Process Communication* werden alle Arten verstanden, mit denen zwei Computer-Prozesse miteinander kommunizieren können. Am häufigsten werden dazu Shared Memory oder TCP/IP-Sockets eingesetzt, unter Linux/Unix sind auch Named Pipes sehr verbreitet.

Issuer Der *Issuer* ist für die Herausgabe der Bezahlkarten verantwortlich und steht meist einer Bank sehr nahe oder gehört sogar einer solchen.

NDEF Das *NFC Data Exchange Format* ist der Standard Nachrichten Container beim Datenaustausch via NFC. Bei Tags wird dabei eine NDEF-Nachricht auf dem Tag gespeichert und bei jeder Verbindung vom Tag gelesen. Beim P2P Modus werden zwischen den Geräten die Daten im NDEF-Format ausgetauscht.

Magstripe Als *Magstripe* (auch: MagStripe) wird das Bezahlen per Magnetstreifen oder zumindest aufgrund der darauf enthaltenen Daten bezeichnet. Beispielsweise ist es gemäss EMV Contactless möglich, die entsprechenden Magstripe-Daten aus dem Chip zu erhalten, falls dies das Terminal wünscht.

Merchant Der *Merchant* Anbieter von Waren oder Dienstleistungen, zu derer Bezahlung er dem Consumer Infrastruktur bereit stellt, damit dieser mit seiner Karte bezahlen kann.

MNO Abkürzung für *Mobile Network Operator*, Mobilfunkanbieter.

MNO TSM Der *Mobile Network Operator TSM* ist der TSM, der im Auftrag eines MNO die Kartendaten des SP TSM entgegennimmt und über das Mobilfunknetzwerk des MNO auf die SIM-Karte eines Consumers lädt.

Mobile Payment In dieser Arbeit wird unter *Mobile Payment* die Zahlungen mittels NFC fähigem Smartphone an einem EFT/POS Terminal verstanden.

Explizit nicht gemeint sind damit Zahlungssysteme, bei denen über die Mobilfunkrechnung abgerechnet wird oder bei denen Geld zwischen zwei Smartphones ausgetauscht werden kann.

NFC *Near Field Communication*. Ein Standard für drahtlose Datenübertragung, mit dem kleine Datenmengen übertragen werden können. NFC basiert und ist kompatibel mit den älteren Standards *RFID* und *ISO 14443*.

OTA *Over the Air*. Bezeichnet das Nachladen von Daten auf die SIM-Karte oder das Smartphone über das Netz des Mobilfunkproviders.

P2P Alternative Schreibweise für Peer to Peer.

PCSC International standardisierte Schnittstelle für die Kommunikation mit Chipkarten.

Personalisierung Die *Personalisierung* ist der Prozess, bei dem die individuellen Kartendaten auf eine Bezahlkarte, respektive auf ein SE, geladen werden.

PayPass Als *PayPass* bewirbt MasterCard die Technologie, mit welcher über eine Funkschnittstelle Zahlungen an Terminals durchgeführt werden können. Technisch handelt es sich um contactless Smartcards, die nach EMV funktionieren. Der Begriff wird zunehmend auch im Mobile Payment Bereich verwendet.

Peer to Peer (P2P) *Peer to Peer* bezeichnet im Allgemeinen die Kommunikation zwischen zwei gleichberechtigten Partnern (also keine Server-Client-Architektur).

Im Umfeld von NFC bezeichnet Peer to Peer einen bestimmten Kommunikationsmodus, welcher den bidirektionalen Datentausch zwischen zwei aktiven Geräten bezichnet.

Alternativ wird die Schreibweise P2P verwendet.

POS-Terminal Siehe *EFT/POS*.

Proximity Card Alternative Bezeichnung für *Contactless Smartcard*; siehe dort.

Die Bezeichnung wird unter anderem von der ISO verwendet.

SE Siehe *Secure Element*.

Secure Element Art eines Chips, dessen Speicherbereich besonders gegen unbefugten Zugriff geschützt ist. Auf einem solchen Chip können beispielsweise Credentials für den Zahlungsprozess gespeichert werden, ohne dass diese von Unbefugten wieder ausgelesen werden können. Dieser Speicherinhalt ist logisch und physikalisch geschützt. So kann der Chip auch mechanischen Angriffen (micro probing, optisches Auslesen, etc.) standhalten.

Ein Secure Element muss dabei nicht phyisch vor Ort sein, sondern kann sich auch in einer Cloud befinden. Dabei greift das benutzende Gerät via Internet auf das Secure Module zu.

SIM-Karte Die *SIM-Karte*, auch *UICC* oder *USIM-Karte* bezeichnet, ist eine *Chipkarte*, welche Credentials für die Kommunikation mit dem Mobilfunknetz enthält. Sie wird in einen speziell dafür vorgesehen Slot in einem Mobilgerät eingelegt. Die Chips der SIM-Karten sind Secure Elemente. Es existieren verschiedene Generation von Karten. Sie unterscheiden sich in technischen Fähigkeiten und Speichergrössen. Es bestehen auch verschiedene Form-Faktoren für SIM-Karten, die in verschiedenen Standards[36] geregelt sind.

Smartcard Alternative Bezeichung für Chipkarten.

SNEP Das *Simple NDEF Exchange Protocol* ist das Standard-Protokoll bei NFC P2P. Es beschreibt zwei Basis-Kommunikations-Arten, nämlich den *PUT* und den *GET* Request. Beim PUT-Request wird dabei eine NDEF-Nachricht an die Gegenpartei gesendet. Beim GET-Request wird von der Gegenpartei eine NDEF-Nachricht angefordert.

SP TSM Der *Service Provider TSM* ist der TSM, der im Auftrag eines Issuers Kartendaten verarbeitet. Dies umfasst meist entweder das Aufbrennen der Daten auf einen Chip für eine Bezahlkarte (siehe Chipkarte) oder das Signieren und Weiterreichen der Daten an einen MNO TSM.

SWP Unter dem *Single Wire Protokoll* wird die direkte physikalische Verbindung zwischen NFC Controller und Secure Element sowie das dazu verwendete Kommunikationsprotokoll verstanden.

[36] Namentlich sind dies die Standards *ISO/IEC 7810* und *ETSI TS 102 221*, sowie der *JEDEC Design Guide 4.8* für fest eingebaute SIM-Karten (auch *Embedded SIM* genannt).

TSM Ein *Trusted Service Manager* ist ein Vertrauenspartner des Issuers, der Karten-Informationen über einen Consumer verarbeitet. Es wird zwischen dem SP TSM und dem MNO TSM unterschieden. Ersterer steht dem Issuer nahe, letzterer dem MNO.

UART Der *Universal Asynchronous Receiver Transmitter* ist eine elektronische Schaltung, mit der serielle Schnittstellen realisiert werden können.

UART USB Bridge Mittels einer *UART USB Bridge* kann eine Schaltung, die sonst nur über eine serielle (UART-) Schnittstelle verfügt, über an mit einem PC verbunden werden. Auf diesem steht dann eine virtuelle serielle Schnittstelle zur Verfügung, deren Ein- und Ausgaben via USB von, rsp. zur, Schaltung übertragen werden.

UBSCC Das *UBS Card Center* ist ein Tochterunternehmen der UBS AG, welches die Bezahlkarten für jene herausgibt. Somit ist das UBS Card Center ein Issuer.

UICC *Universal integrated circuit card* ist eine alternative Bezeichnung für Chipkarte und steht kontextabhängig auch für die SIM-Karte.

Vier Parteien Modell Das *vier Parteien Modell* (auch: *Four Player Model*) beschreibt die Beziehungen zwischen den Stakeholder im Zahlungsprozess gemäss EMV. Die vier Parteien sind: Consumer, Merchant, Acquirer und Issuer. Weitere Informationen dazu finden sich im Kapitel Kartengeschäft.

Wallet *Wallet* (englisch für Geldbörse) bezeichnet eine Smartphone-App, welche eine oder mehrere virtuelle Bezahlkarten enthält und Mobile Payment ermöglicht.

Wallet (manchmal auch *Google Wallet*) ist auch ein Produkt von *Google*, welches entsprechende Wallet-Funktionen auf Android bietet.

WP8 *WP8* ist eine Abkürzung für das Smartphone-Betriebssystem *Windows Phone 8* von Microsoft.

10 Literaturverzeichnis

[1]ISO, “ISO/IEC 14443-1:2000 - Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics.” 2000.

[2]Google, “Official Blog: Coming soon: make your phone your wallet.” 2011 [Online]. Available: http://googleblog.blogspot.ch/2011/05/coming-soon-make-your-phone-your-wallet.html. [Accessed: 03–May-2013]

[3]Gartner Inc., “Gartner’s 2012 Hype Cycle for Emerging Technologies,” 2012 [Online]. Available: http://www.gartner.com/newsroom/id/2124315. [Accessed: 03–May-2013]

[4]Kaba AG, “Sicherer Zutritt mit Mobiltelefon.” 2012 [Online]. Available: http://www.kaba.com/workforce-management/de/News-Medien/Mitteilungen-Berichte/484462/security-2012-nfc.html. [Accessed: 03–May-2013]

[5]GSMA, “White Paper□: Mobile NFC in Transport.” 2012.

[6]C. Maeder and S. Vogler, “NFC in Plakatkampagnen.” dec-2012 [Online]. Available: http://eprints.hsr.ch/253/1/NFC in Plakatkampagnen.pdf. [Accessed: 03–May-2013]

[7]NFC Forum, “NFC Forum□: The NFC Ecosystem.” 2013 [Online]. Available: http://www.nfc-forum.org/aboutnfc/ecosystem/. [Accessed: 03–May-2013]

[8]J.-P. Koelbl and M. Bosshard, “Interview mit UBS Card Center AG,” 2013.

[9]MobilePaymentsToday.com, “Does Spanish FI Bankinter have a solution for the SE conundrum?” 2013 [Online]. Available: http://www.mobilepaymentstoday.com/article/209157/Does-Spanish-FI-Bankinter-have-a-solution-for-th [Accessed: 11AD–Mar-2013]

[10]A. Baumert and S. Reich, *Interviews in der Recherche*. .

[11]European Payments Council and GSM Association, “EPC – GSMA Mobile Contactless Payments Service Management Roles Requirements and Specifications.” European Payments Council and GSM Association, 2010.

[12]Aduno, “Geschäftsbericht der Aduno Gruppe 2012,” 2012.

[13]MasterCard, “The SEPA 4-party business model□: Bringing increased merchant and consumer choice and fostering convenience and competition in the Single Euro Payments Area.”

[14]Visa, “Fees and interchange.” 2013 [Online]. Available: http://www.visaeurope.com/en/about\char”005C\relax{}_us/our\char”005C\relax{}_business/fees\char”005C\relax{}_and\char”005C\relax{}_interchange.aspx. [Accessed: 03–May-2013]

[15]Schweizerische Nationalbank SNB, “C2 Zahlungsverkehr mit Karten und Checks / Trafic des paiements par cartes et chèques,” *Statistisches Monatsheft*, no. 2013, pp. 34–37, 2013 [Online]. Available: http://www.snb.ch/de/iabout/stat/statpub/statmon/stats/statmon/statmon\char”005C\relax{}_C2. [Accessed: 03–May-2013]

[16]Comparis, “Schweizer kaufen nicht gerne auf Pump,” 2008.

[17]R. Fäh, “Interview mit Aduno Gruppe,” 2013.

[18]Bundesamt für Statistik, “Bevölkerungsstand und -struktur – Indikatoren,” 2013 [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/01/02/blank/key/raeumliche\char”005C\relax{}_verteilung/kantone\char”005C\relax{}_\char”005C\relax{}_gemeinden.html. [Accessed: 03–May-2013]

[19]Bank for international Settlements, “Statistics on payment, clearing and settlement systemsn in the CPSS countries,” 2013.

[20]ECB, “Payment card accepting devices - ECB Statistical Data Warehouse.” [Online]. Available: http://sdw.ecb.europa.eu/browse.do?node=3447412. [Accessed: 03–May-2013]

[21]Insee, “Population - Évolution de la population jusqu’en 2013.” 2013 [Online]. Available: http://www.insee.fr/fr/themes/tableau.asp?reg\char”005C\relax{}_id=0\char”005C\relax{}&ref\char”005C\relax{}_id=NATnon02145. [Accessed: 03–May-2013]

[22]ISTAT, “Bilancio demografico anno 2010 e popolazione residente al 31 Dicembre Italia.” 2013 [Online]. Available: http://demo.istat.it/bil2010/index.html. [Accessed: 03–May-2013]

[23]P. Mooslechner, H. Stix, and K. Wagner, “Zahlungsmittelnutzung in Österreich eine analyse auf Basis von Erhebungsdaten von 1996 bis 2011,” 2012.

[24]W. Rankl and W. Effing, “Handbuch der Chipkarten,” 5 ed., Hanser, 2008.

[25]Technical Cooperation ep2, *System Specification*, 5 ed. Zürich: Technical Cooperation ep2, 2011.

[26]T. Lerner, *Mobile Payment*. Springer, 2013.

[27]J. Henkel, *Mobile Commerce*. Silberer, 2001.

[28]Comparis, “Verbreitung von Smartphones,” 2012 [Online]. Available: http://www.comparis.ch/~/media/files/mediencorner/medienmitteilungen/2012/telecom/verbreitung-smartphone.pdf. [Accessed: 03–May-2013]

[29]Gartner Inc., “Gartner Says Asia/Pacific Led Worldwide Mobile Phone Sales to Growth in First Quarter of 2013.” 2013 [Online]. Available: https://www.gartner.com/newsroom/id/2482816. [Accessed: 03–May-2013]

[30]H. Straumann, “Interview mit Swisscom AG,” 2013.

[31]Bundesamt für Kommunikation BAKOM and B. Michel, “Amtliche Fernmeldestatistik 2011,” no. November, 2012 [Online]. Available: http://www.bakom.admin.ch/dokumentation/zahlen/00744/00746/index.html?lang=de. [Accessed: 03–May-2013]

[32]S. Mittal, “Präsentation der Swisscom AG bez. Mobile Payment bei Abrantix AG,” 2013.

[33]B. Narter, “Mobile Banking- Opportunity for entrants,” *Communiqué*, 2012 [Online]. Available: http://microsite.hcltech.com/communique/article23.html. [Accessed: 03–May-2013]

[34]Ixaris and Anthemis Group, “The PaymenTs Innovation Jury Report,” 2013.

[35]WesternUnion, “Mobile Money Transfer Fact Sheet.” 2013 [Online]. Available: http://corporate.westernunion.com/Mobile\char”005C\relax{}_Money\char”005C\relax{}_Transfer\char”005C\relax{}_Fact\char”005C\relax{}_Sheet.html. [Accessed: 03–May-2013]

[36]K. Fehrenbacher, “Square COO: There’s no value in NFC.” 2011 [Online]. Available: http://gigaom.com/2011/09/26/square-mobilize-2011/. [Accessed: 03–May-2013]

[37]EMV, “Book 1: Application Independent ICC to Terminal Interface Requirements,” in *EMV Integrated Circuit Card Specifications for Payment Systems*, no. November, 2011 [Online]. Available: http://www.emvco.com/specifications.aspx?id=223. [Accessed: 03–May-2013]

[38]EMV, “Book 2: Security and Key Management,” in *EMV Integrated Circuit Card Specifications for Payment Systems*, 43rd ed., no. November, EMVCo, LLC, 2011 [Online]. Available: http://www.emvco.com/specifications.aspx?id=223. [Accessed: 03–May-2013]

[39]EMV, “Book 3: Application Specification,” in *EMV Integrated Circuit Card Specifications for Payment Systems*, 43rd ed., no. November, EMVCo, LLC, 2011 [Online]. Available: http://www.emvco.com/specifications.aspx?id=223. [Accessed: 03–May-2013]

[40]EMV, “Book 4: Cardholder, Attendant, and Acquirer Interface Requirements,” in *EMV Integrated Circuit Card Specifications for Payment Systems*, no. November, 2011 [Online]. Available: http://www.emvco.com/specifications.aspx?id=223. [Accessed: 03–May-2013]

[41]EMV, “Book A: Architecture and General Requirements,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[42]EMV, “Book B: Entry Point Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[43]EMV, “Book C-1: Kernel 1 Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[44]EMV, “Book C-2: Kernel 2 Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[45]EMV, “Book C-3: Kernel 3 Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[46]EMV, “Book C-5: Kernel 5 Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[47]EMV, “Book C-4: Kernel 4 Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013 [Online]. Available: http://www.emvco.com/specifications.aspx?id=21. [Accessed: 03–May-2013]

[48]EMV, “Book D: EMV Contactless Communication Protocol Specification,” in *Contactless Specifications for Payment Systems*, 23rd ed., no. February, 2013.

[49]MasterCard, “Mobile MasterCard PayPass User Interface Application Design Guide,” 2011.

[50]GlobalPlatform Inc., “Secure Element Access Control.” 2012.

[51]National Institute of Standards and Technology, “Security Requirements For Cryptographic Modules.” National Institute of Standards and Technology, Gaithersburg, MD, USA, 2002 [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. [Accessed: 03–May-2013]

[52]N. Elenkov, “Emulating a PKI smart card with CyanogenMod 9.1.” 2012 [Online]. Available: http://nelenkov.blogspot.ch/2012/10/emulating-pki-smart-card-with-cm91.html. [Accessed: 06AD–May-13AD]

[53]A. Jakl and M. Roland, “Developer Comparison Peer-to-peer Software card emulation,” 2012.

[54]J. Langer and M. Roland, *Anwendungen und Technik von Near Field Communication (NFC)*. 2010.

[55]T. Graf, “Interview mit Sunrise AG,” 2013.

[56]Sunrise Communications AG, “Medienmitteilung Sunrise startet erstes Pilotprojekt für Mobile Payment Medienmitteilung.” 2012 [Online]. Available: http://www1.sunrise.ch/Mobile-Payment-cbJprAqFI.yaUAAAE1isc.6zdo-Sunrise-Info-Site-WFS-de\char”005C\relax{}_CH-CHF.html. [Accessed: 03–May-2013]

[57]MasterCard, “MasterCard Approved Mobile Devices,” 2013.

[58]SD Association, “ASSD.” 2013 [Online]. Available: https://www.sdcard.org/developers/overview/ASSD/. [Accessed: 03–May-2013]

[59]SD Group, “Advanced Security SD Extension Simplified Specification Version 2.00.” 2010.

[60]MasterCard, “Mobile PayPass.” 2013 [Online]. Available: http://www.mastercard.com/corporate/mobile-paypass.html. [Accessed: 03–May-2013]

[61]MasterCard, “Getting Started.” 2013 [Online]. Available: http://www.mastercard.com/us/paypass/phonetrial/gettingstarted.html. [Accessed: 03–May-2013]

[62]Visa, “Visa payWave for Mobile.” 2013 [Online]. Available: https://developer.visa.com/paywavemobile. [Accessed: 03–May-2013]

[63]Google, “How it Works - Wallet Help.” 2013 [Online]. Available: https://support.google.com/wallet/bin/answer.py?hl=en\char”005C\relax{}&answer=2463711\char”005C\relax{}&topic=3157452\char”005C\relax{}&ctx=topic. [Accessed: 03–May-2013]

[64]M. Reardon, “Is NFC killing Google Wallet? | Mobile - CNET News.” 2012 [Online]. Available: http://news.cnet.com/8301-1035\char”005C\relax{}_3-57441842-94/is-nfc-killing-google-wallet/. [Accessed: 11AD–Mar-13AD]

[65]F. Michahelles and J. Langer, “5th International Workshop on Near Field Communication (NFC2013),” in *5th International Workshop on Near Field Communication (NFC2013)*, 2013 [Online]. Available: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6478871 http://nfc-workshop.org/2013/. [Accessed: 03–May-2013]

[66]NFC Forum, “NFC Data Exchange Format.” 2006.

[67]Libnfc, “libnfc devices compatibility matrix.” 2013 [Online]. Available: http://nfc-tools.org/index.php?title=Devices\char”005C\relax{}_compatibility\char”005C\relax{}_matrix. [Accessed: 30.5.13]

[68]NFC Forum, “Simple NDEF Exchange Protocol.” 2011.

[69]H. online, “Hochentwickelte Android-Trojaner ins Netz gegangen.” 2013 [Online]. Available: http://www.heise.de/newsticker/meldung/Hochentwickelte-Android-Trojaner-ins-Netz-gegangen-1885163.html. [Accessed: 12AD–Jun-13AD]

[70]S. Breite, “Interview mit SIX Payment Services,” 2013.

[71]R. Regenass, “SBB planen im Alleingang ein Handy-Portemonnaie.” 2012 [Online]. Available: http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/SBB-planen-im-Alleingang-ein-HandyPortemonnaie/story/19246885. [Accessed: 03.05.2013]

[72]NFC Forum, “NFC Analog Specification.” 2012.

[73]G.P. Hancke, “Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens,” *Journal of Computer Security*, vol. 19, no. 2, pp. 259–288, 2011.

[74]NFC Forum, “NFC Activity Specification Technical Specification NFC Forum TM.” 2010.

[75]NFC Forum, “NFC Digital Protocol Technical Specification NFC Forum TM.” 2010.

[76]ECMA, “Ecma-340.” 2004.

[77]ECMA, “Ecma-352.” 2010.

[78]InsideSecure, “Debunking NFC Peer-2-Peer Myths,” 2012.

[79]International Electrotechnical Commission and International Organization for Standardization, “Interindustry commands for interchange,” in *ISO 7816*, 2005 ed., International Organization for Standardization, 2005.