Scoop – Mobile Payment

In diesem Artikel wird die elektronische Geldbörse Scoop vorgestellt, die im Rahmen eines KTI Projektes entwickelt worden ist. Im Gegensatz zu anderen Mobile Payment Lösungen muss bei Scoop der Point of Sale (POS) nicht mehr direkt an das Internet angeschlossen sein. Das Settlement der Zahlung wird direkt am POS vorgenommen und, falls das Mobiltelefon am POS zum Zeitpunkt der Zahlung nicht online ist, so werden die Transaktionsdaten über ein langsames Netzwerk an den Server ausgeliefert. Um «Double-Spend»-Attacken zu erkennen, werden alle Transaktionen in einer Kette (Chain) gespeichert und mit kryptographischen Hash-Codes gesichert. Im POS sind die Hash-Codes in einem mit JavaCard programmierten Secure-Element gespeichert. In diesem Artikel präsentieren wir die Idee von Scoop und erläutern Aspekte der Realisierung.

Dominik Gruntz, Markus Knecht, Stephan Wullschleger[1] | dominik.gruntz@fhnw.ch

Im Rahmen des Projektes *Supervised Chaining Offline/Online Purse* (Scoop) haben wir zusammen mit der Firma PBV Kaufmann Systeme GmbH eine Payment-Lösung entwickelt, mit der sichere Offline-Transaktionen abgewickelt werden können. Man kann sich zu Recht fragen, ob es neben *Apple Pay*, *Google Pay*, *Samsung Pay*, *Huawei Pay*, *Alipay*, *Twint*, *Boon*, *Seqr Go!*, *Postfinance*, *Visa Bonus Card App*, *MIGROS App* etc. wirklich noch eine weitere *Mobile Payment* Lösung braucht. Die existierenden Lösungen haben jedoch alle eines gemein: Der *Point of Sale* (POS) muss online mit dem Internet verbunden sein, damit bei der Zahlung mit dem Mobiltelefon das Zahlungsterminal die Kartengültigkeit, die Karten- und Tageslimite sowie eine ausreichende Kontodeckung überprüfen kann. Die Zahlung muss also vom Server freigegeben werden [Mau09].

Es macht jedoch nicht für jeden POS Sinn eine Internet-Connectivity sicherzustellen, auch wenn diese mit einem einfachen GSM-Modul realisiert werden könnte. Wir denken da insbesondere an Kaffeeautomaten oder Snackautomaten wie sie häufig auch in Firmen anzutreffen sind oder auch an Waschautomaten. Für solche Anwendungen wurden kartenbasierte elektronische Geldbörsen wie z.B. die *GeldKarte* in Deutschland, *CASH* in der Schweiz oder *Quick* in Österreich entwickelt. Sowohl CASH wie auch Quick sind inzwischen jedoch eingestellt worden. Die Einstellung von Quick per Mitte 2017 hat jedoch zu Problemen in Waschküchen sowie bei vielen Zigaretten-, Snack- und Parkautomaten geführt [Stau17]. Die Umstellung auf eine Online-Lösung ist gerade in Waschküchen wegen der fehlenden Internet-Verbindung nicht immer möglich.

Mit Scoop haben wir uns auf den Anwendungsbereich der bargeldlosen Offline-Zahlungen fokussiert. Offline-Zahlung heisst bei uns, dass sowohl das Payment-Terminal (also der eigentliche POS) wie auch das Mobiltelefon zum Zeitpunkt der Zahlung offline sein können.

Offline-Payment Systeme

Bei einer Geldkarte ist das Guthaben auf der Karte gespeichert, und wenn an einem POS mit der Karte bezahlt wird, dann wird der entsprechende Betrag vom Kartenguthaben abgezogen und auf dem POS gutgeschrieben. Falls das bezahlte Produkt nicht ausgegeben werden kann, so wird der Betrag auf die Karte zurückgebucht (falls die Karte noch zugreifbar ist) oder es wird eine Storno-Transaktion auf dem POS gespeichert, die vom Karteninhaber am POS abgeholt werden kann. Falls diese Transaktion jedoch nicht abgeholt und gelöscht wird, dann ist das Geld verloren. Geld geht auch dann verloren, falls ein Nutzer seine Karte verliert oder falls ein Betrag von der Karte abgezogen wird, der POS die Bestätigung dieser Transaktion aber nicht mehr erhält. Man spricht in diesem Zusammenhang auch von einem Schlupf, da so potentiell Geld aus dem System entweichen kann.

Online-Payment Systeme

Das geschilderte Schlupfproblem kann gelöst werden, indem die Guthaben auf einem Server gespeichert und die Transaktionen auf diesem Server nachgeführt werden, d.h. bei jedem Bezahlvorgang meldet der Sender oder der Empfänger den Geldübertrag an den Server, und dieser führt diese Transaktion in seiner Registratur nach. Solange der Server nicht informiert ist, ist das Geld nicht verschoben. Guthaben kann so nicht verschwinden und ist immer eindeutig einem Besitzer zugeordnet. Auf der Karte selber wird bei dieser Lösung kein Guthaben gespeichert, sondern nur die Identifikation des Nutzers, und der Bezahlvorgang wird nicht lokal am POS sondern auf dem Server ausgeführt. Die Karte für Zutritt und Bezahlung an der FHNW (FH-Card) verwendet beispielsweise diese Lösung und daher sind

1 PBV Kaufmann Systeme GmbH

die Kassenterminals, die Parking-Schranken und alle Kaffeeautomaten an der FHNW online mit dem Internet verbunden.

Anstelle einer Nutzeridentifikation könnte auf dem Mobiltelefon auch eine Bezahlungsberechtigung gespeichert werden (vergleichbar mit einem Verrechnungsscheck), die dann offline auf ein anderes Gerät oder an einen POS übertragen wird. Die Transaktion erfolgt jedoch erst, wenn der Sender oder der Empfänger die Verschiebung der Berechtigung an den Server meldet. Ein Schlupf wird so vermieden, denn auch wenn ein Check mehrfach verwendet wird, so kann er nur durch einen Empfänger eingelöst werden. Diese Variante ist 2015 von Visa patentiert worden [Sabba16].

Ein ebenfalls auf Bezahlungsberechtigungen basierendes Protokoll wurde bereits 2014 an unserem Institut im Rahmen des Projektes *iBeam* entwickelt [iBeam14]. Die Bezahlungsberechtigungen wurden damals mit einem Verfalldatum versehen. Wenn der Server bis zum Ablauf der Gültigkeit des Checks weder vom Sender noch vom Empfänger über eine Transaktion informiert wurde, so wurde der zurückgestellte Geldbetrag wieder freigegeben.

Scoop

Scoop vereinigt die Vorteile von Offline- und Online-Payment Systemen. Das Guthaben wird auf dem Mobiltelefon (bzw. auf der Karte) und auf dem POS gespeichert. Das Settlement (Austausch von Leistung gegen Geld) wird unmittelbar am POS (offline) ausgeführt und Guthaben kann nicht verloren gehen (d.h. kein Schlupf). Dies wird erreicht, indem Transaktionen mit idempotenten Operationen[2] zwischen verschiedenen Transaktionsketten verschoben werden. Zudem werden die am Scoop teilnehmenden Mobiltelefone genutzt, um Daten vom POS an den Server zu übertragen. Transaktionsdaten werden dabei über alle Mobiltelefone verschickt, die mit dem POS interagieren bis am POS eine Bestätigung eingetroffen ist (Schwarm-Netzwerk).

Auf dem POS wird das Guthaben in einem *Secure Element* (SE) gespeichert (wir verwenden die MicroSD-Karte PS-100u VE mit einem SE von Swissbit). Ein SE ist ein sicherer Applikations- und Datenspeicher (*Trusted Execution Environment*), vergleichbar mit dem Chip auf einer Kreditkarte. Leider stehen entsprechende Elemente auf dem Mobiltelefon nicht zur Verfügung (bzw. können wie beim iPhone nur vom Hersteller genutzt werden). Daher könnte ein gewiefter Nutzer das auf dem Mobiltelefon gespeicherte Guthaben manipulieren. Das Protokoll ist jedoch so ausgelegt, dass solche Betrugsfälle entweder direkt am POS erkannt und zurückgewiesen oder spätestens auf dem Server erkannt und korrigiert werden können. Da wir neben dem Offline-Protokoll auch ein Online-Protokoll unterstützen, bei dem sichergestellt ist, dass das Guthaben nicht überzogen werden kann, wird empfohlen, dass die Offline-Variante nur vertrauenswürdigen Nutzern zur Verfügung gestellt wird (z.B. Nutzern, bei welchen man Zugriff auf eine Kreditkarte hat). Das Scoop-System erlaubt es auch, pro Benutzer eine Offline-Limite zu setzen und der POS kann zudem entscheiden, ob er überhaupt Offline-Transaktionen zulässt.

Die Scoop-Lösung ist als europäisches Patent angemeldet worden [AGKW16]. Im Folgenden werden die Kernelemente des Scoop-Protokolls dargestellt.

Protokoll

Das Scoop-Protokoll basiert auf Transaktionsketten, deren Elemente mit Hilfe von kryptographischen Hash-Funktionen untereinander verlinkt werden. Diese Ketten sind durch die Blockchain-Technologie von Bitcoin und anderen Kryptowährungen inspiriert, aber im Unterschied zu diesen Technologien wird bei Scoop kein dezentraler Konsens benötigt, da ein Server als zentrale Instanz diese Funktion übernehmen kann. Zudem verwenden wir in unserem Protokoll nicht nur eine Kette, sondern mehrere Ketten, die jedoch voneinander abhängen. Diese Ketten ermöglichen es, die Sicherheit im Offline-Fall effizient zu erhöhen, da am POS bestimmte Eigenschaften lokal geprüft werden können.

Jedes Element einer Transaktionskette enthält einen Hash-Wert, der aus den Transaktionsdaten und dem Hash-Wert des Vorgängerknotens mit Hilfe einer kryptografischen Hashfunktion berechnet wird. In Abbildung 1 ist ein einfaches Beispiel einer solchen Transaktionskette dargestellt.

In den Elementen wird neben den Daten ein Index abgelegt. Dies erlaubt es dem Server eine Kette einfach zu rekonstruieren, falls die einzelnen Elemente in einer beliebigen Reihenfolge eintreffen.

Der Vorteil dieser Transaktionsketten ist, dass die Integrität der Struktur sichergestellt ist. Hat man einen Hashwert auf das Ende der Kette (in Abb. 1 z.B. H_4) und jemand ändert die Daten eines Elementes oder einen Hashwert in der Kette, so kann dies festgestellt werden, indem die Hashwerte neu berechnet werden. Entweder ist einer der Hashwerte innerhalb der geänderten Kette falsch, oder man erhält einen anderen Wert auf das Ende der Kette[3].

Bei diesen Transaktionsketten ist es möglich, dass ein Element in mehreren Ketten enthalten

2 Idempotente Operationen führen mehrfach ausgeführt zum selben Ergebnis, wie wenn sie nur einmal ausgeführt werden. Dies garantiert Fehlertoleranz bei Verbindungsunterbrüchen.

3 Mit den aktuell verwendeten Algorithmen könnten mit einer vernachlässigbaren Wahrscheinlichkeit von $1/2^{256} = 8.6 \times 10^{-78}$ zwei unterschiedliche Ketten als gleich erkannt werden.

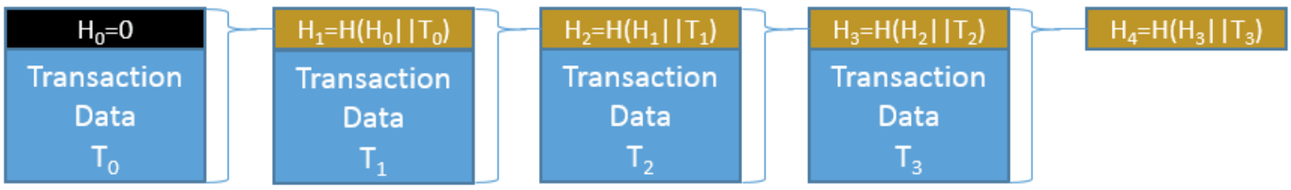

Abbildung 1: Einfache Transaktionskette. H ist eine kryptographische Hashfunktion und || die Konkatenation. T_x repräsentieren die Nutzdaten, H_y die Hashwerte. H_4 ist der Hash-Wert der gesamten Kette.

sein kann, was im Scoop-Protokoll oft verwendet wird. In Abbildung 2 ist ein Beispiel von zwei Ketten dargestellt. Die eine Kette (mit Hashwert A_4) enthält die Transaktionen T_0, T_1, T_2 und T_3, und die zweite Kette (mit Hashwert B_2) enthält nur die Transaktionen T_1 und T_3.

Eine validierende Autorität kann mit einer digitalen Signatur des Hashwerts einer Kette bestätigen, dass die gesamte Transaktionskette existiert und nur gültige Transaktionen enthält. Dies erlaubt es, grosse Transaktionsketten effizient auszutauschen (Hash + Signatur), falls der Empfänger nicht am Inhalt der Kette, sondern nur an deren Existenz und Validität interessiert ist.

Kennt jemand nur den Hashwert einer Transaktionskette, jedoch nicht deren Elemente, so kann er trotzdem prüfen, ob eine zweite Kette mit dieser identisch ist und er kann Elemente an diese Kette anfügen.

Nachfolgend werden die im Scoop-Protokoll verwendeten Transaktionsketten vorgestellt:

- *User-Chain:* Für jedes Mobiltelefon eines Nutzers existiert eine User-Chain, welche das Guthaben des Nutzers auf diesem Mobiletelefon repräsentiert und alle Transaktionen enthält, die das Guthaben erhöhen (Aufladung) oder reduzieren (Übertragung). Diese Kette wird vom Server überwacht und sowohl auf dem Server wie auch auf dem Mobiltelefon gespeichert.
- *POS-User-Chain:* Pro Nutzer und POS existiert eine POS-User-Chain. Diese Kette repräsentiert das von einem Nutzer an einem POS erhaltene (Übertragung) und ausgegebene (Settlement) Guthaben und wird nur auf dem POS gespeichert.
- *Transfer-Chain:* Die Transfer-Chain verbindet die POS-User-Chain mit der zugehörigen User-Chain und repräsentiert alle Transaktionen von Guthaben aus der User-Chain in die POS-User-Chain (Übertragung). Auf dem Mobiltelefon wird ein vom POS angeforderter Betrag von der User-Chain in die Transfer-Chain verschoben und damit für einen spezifischen POS freigegeben. Diese Kette wird danach mit jener auf dem POS synchronisiert, welcher die Einträge nutzt, um die POS-User-Chain zu aktualisieren.

Will ein Nutzer eine Bezahlung durchführen, so fügt er eine Übertragung in die Transfer- und User-Chain ein und synchronisiert dann die Transfer-Chain mit dem POS, wodurch die Übertragung in der POS-User-Chain landet. Schlägt dieser Schritt fehl (verlorene Nachricht, Verbindungsunterbruch etc.), so kann er wiederholt werden, bis die Ketten auf beiden Seiten identisch sind. Über ein Settlement kann nun der POS die Übertragung verwenden, um eine Leistung zu bezahlen. Falls jedoch eine gewünschte Leistung am POS nicht erbracht werden kann, so kann der Nutzer die Übertragung an diesem POS anderweitig verwenden. Nach einer gewissen Zeit wird dieses Guthaben jedoch zurückgesetzt und via Schwarm-Netzwerk und Server wieder in die User-Chain eingefügt.

Sicherheit

Falls auf dem Mobiltelefon eine Manipulation vorgenommen worden ist, um ein Guthaben z.B. mehrfach an einem POS ausgeben zu können (Double-Spend-Angriff), so wird dieser Angriff am POS erkannt, da die Transfer-Chain, die auf dem POS gespeichert ist, Elemente enthält, die auf dem Mobiltelefon nicht vorhanden sind. Es genügt dabei, den auf dem POS gespeicherten Hash-Wert des letzten Elements der Transfer-Chain mit dem im neuen, vom Mobiltelefon gelieferten Kettenelement abgelegten Hash-Wert zu vergleichen.

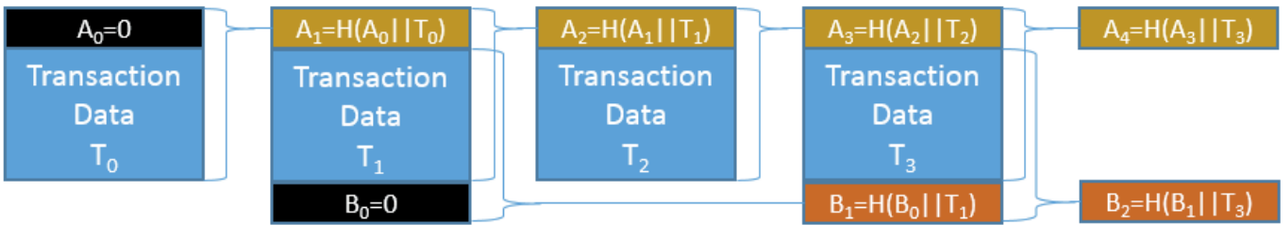

Abbildung 2: Zwei Transaktionsketten, welche die Elemente T_1 und T_3 teilen. T_x repräsentieren die Nutzdaten, A_y die Hashwerte von Kette A, B_y die Hashwerte von Kette B.

Falls nach einer Manipulation auf dem Mobiltelefon Guthaben an einem anderen POS ausgegeben wird, so wird dies nicht unmittelbar erkannt, sondern erst, wenn diese Transaktion über das Schwarm-Netzwerk an den Server übermittelt werden konnte. Jeder Nutzer besitzt daher ein Zugriffs-Token mit einer beschränken Gültigkeit. Ein POS lehnt einen Nutzer ohne gültiges Zugriffs-Token immer ab. Dies zwingt den Nutzer von Zeit zu Zeit online zu gehen und mit dem Server zu kommunizieren und seine Transaktionsketten mit jenen auf dem Server zu synchronisieren.

Scoop Schwarm-Netzwerk

Für die Realisierung des Schwarm-Netzwerkes wird davon ausgegangen, dass die Mobiltelefone und der POS während des Bezahlvorgangs offline sind, dass aber mindestens eines der Mobiltelefone, welches Zahlungen am POS ausführt, früher oder später eine Internetverbindung haben wird. Der POS nutzt dies nun aus und überliefert offene Nachrichten an jedes vorbeikommende Mobiltelefon. Sobald ein Mobiltelefon Internetzugriff hat, überliefert es die gespeicherten Nachrichten an den Server, welcher dann eine Empfangsbestätigung an alle Mobiltelefone ausliefert, sobald sich diese mit ihm verbinden. Mobiltelefone können nun diese Bestätigung an den entsprechenden POS ausliefern, sobald sie mit ihm interagieren. Sowohl die Mobiltelefone wie auch die POS liefern die Nachrichten solange wiederholt aus, bis sie eine entsprechende Bestätigung erhalten haben. Analog können Meldungen vom Server zum POS übertragen werden.

Die Struktur dieses Schwarm-Netzwerkes ist in Abbildung 3 dargestellt. Der Server (links) kommuniziert mit den Mobiltelefonen (Mitte), welche Nachrichten an die POS (rechts) weiterleiten bzw. Meldungen der POS ausliefern können. Der in Abbildung 3 dargestellte Graph ist bipartit und besteht aus den beiden Teilmengen der Mobiltelefone und der POS. Der Server kann dabei als spezieller POS angesehen werden. Das Schwarm-Netzwerk erlaubt, dass neben Mobiltelefonen auch Karten am System partizipieren können.

Bei einer naiven Implementierung kann dies zu einer grossen Flut an Nachrichten führen. Durch Einbezug der Position, der Internetverfügbarkeit der Mobiltelefone und des Kaufverhaltens (an welchen POS ein Mobiltelefon in der Vergangenheit Transaktionen ausgeführt hat) kann die Auslieferung von Nachrichten auf wenige Mobiltelefone beschränkt werden.

Scoop Simulation

Um ein Gefühl zu bekommen, wie schnell Meldungen beim Server ankommen, wenn sie über das Schwarm-Netzwerk verschickt werden, haben wir einen Simulator entwickelt. Mit Hilfe einer domänen-spezifische Sprache (DSL) kann die Anzahl POS und Kunden sowie deren Kaufverhalten definiert werden. Zudem kann definiert werden, wie viele POS in einer Offline-Zone stehen, in der Kunden keinen Internetzugriff haben, sowie wann und wie oft ein Mobiltelefon online ist. Basierend auf diesen Parametern wird dann eine diskrete Ereignissimulation über einen bestimmten Zeitraum durchgeführt und die Resultate gesammelt und aggregiert.

Eine Simulation unter eher pessimistischen Annahmen (25% der POS in einer Offline-Zone, sowie 33% der Mobiltelefone immer offline) mit insgesamt 100 POS und 3750 Kunden hat ergeben, dass die durchschnittliche Nachricht vom POS in-

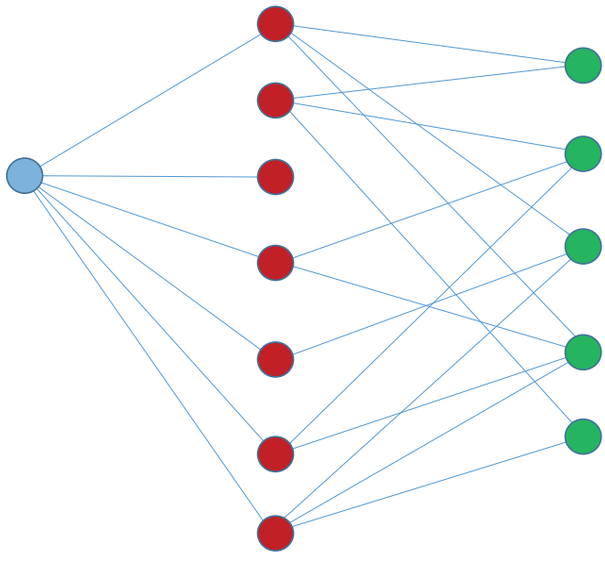

Abbildung 3: Struktur des Schwarm-Netzwerkes: Server (links), Mobiltelefone (Mitte), POS (rechts)

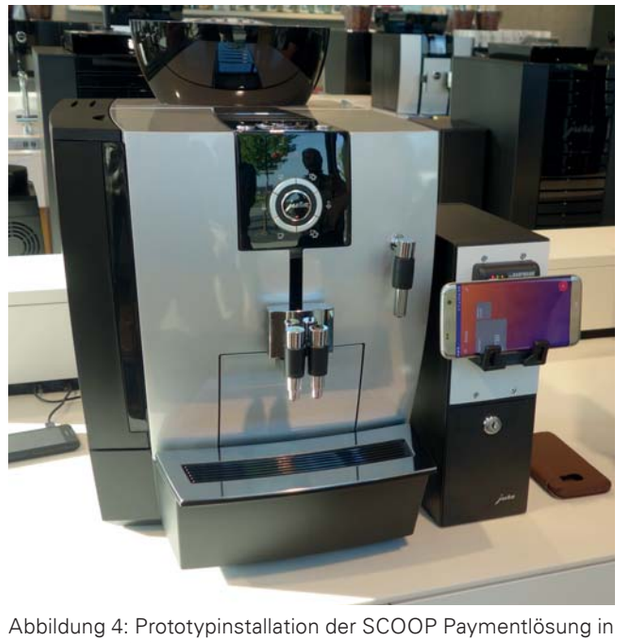

Abbildung 4: Prototypinstallation der SCOOP Paymentlösung in einem Jura Kaffeeautomaten

nerhalb von 35 Sekunden beim Server ankommt und dass die Mobiltelefone maximal 45 Nachrichten gespeichert haben, die auf eine Auslieferung warten. Beim POS waren es sogar nur maximal 8 Nachrichten, die unbestätigt auf eine Auslieferung warteten. Da die Nachrichten klein sind, ist diese Last kaum bemerkbar.

Resultat

Im Rahmen unseres Projektes haben wir das Scoop-Protokoll umgesetzt. Dazu gehört die SE-Applikation, welche die Ketten auf dem POS verwaltet und welche für die Sicherheit verantwortlich ist. Dieses SE wird vom Controller aus angesprochen, der sich im POS befindet. Dieser Controller ist auch für die Kommunikation mit den Mobiltelefonen über NFC sowie für die Implementierung des Schwarm-Netzwerkes zuständig. Auf den Mobiltelefonen ist neben der eigentlichen Scoop-Purse-Applikation auch ein *Host Card Emulation* (HCE)-Service aktiv, mit dem eine NFC-Karte emuliert wird. Das Mobiltelefon kommuniziert schlussendlich via Internet mit dem Server.

Als Resultat existiert ein erster Prototyp, der das Bezahlen von Kaffees aus einem *Jura* Kaffeeautomaten unterstützt (vgl. Abb. 4). In einer nächsten Phase werden im Rahmen einer Pilot-Installation in einer Firma sämtliche POS (Kaffee- und Snack-Automaten sowie Mensa) mit Scoop ausgerüstet.

Ein Nachteil unserer Lösung ist, dass diese aktuell nur mit Mobiltelefonen funktioniert, welche eine NFC-Schnittstelle besitzen, d.h. es funktioniert nur mit Android-Geräten. Es ist geplant, diese Einschränkung in einem weiteren Projekt anzugehen, denn wir rechnen nicht damit, dass Apple den Zugriff auf die NFC-Schnittstelle in absehbarer Zeit vollständig freigeben wird.

Referenzen

[Mau09] David Maurer; Einblicke in die Ökonomie der Zahlungskartensysteme, SNB 2009: https://www.snb.ch/de/mmr/reference/Zahlungskarten/source/Zahlungskarten.de.pdf

[Stau17] Anita Staudacher; Aus für „Quick“ sorgt für Probleme: https://kurier.at/wirtschaft/aus-fuer-quick-sorgt-fuer-probleme/278.600.942

[Sabba16] Yaasha Sabba and Jordan Scheinfield; Token check offline, US Patent 20160224977: https://patents.google.com/patent/US20160224977

[iBeam14] iBeam: Datenaustausch via NFC, Projekt 20130331-05_iBeam, gefördert durch den Forschungsfonds Aargau.

[AGKW16] C. Arnosti, D. Gruntz, M. Knecht, S. Wullschleger, System zum offline-Bezahlen mit E-Geld mit mobilem Gerät mit kurzer Transaktionszeit und abschliessendem Settlement, EP-Patentanmeldung Nr. 16205267.4-1958, 2016

Links

https://de.wikipedia.org/wiki/Cash_(Geldkarte)

https://de.wikipedia.org/wiki/Quick_(Geldkarte)

https://de.wikipedia.org/wiki/GeldKarte

https://swissbit.com/de/products/security-products/micro-sd-memory-cards/ps-100u-ve