Richtlinie zum „Software-Sprint“

Digital_Bargeld – Infrastruktur für bargeldlose Zahlungen ohne Überwachung

Schlussbericht

Zuwendungsempfänger:

Florian Dold

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS18S63 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Durch technischen Fortschritt verdrängen bargeldlose Bezahlsysteme immer mehr die Benutzung von Bargeld im Alltag vieler Bürger*innen. Während die Bequemlichkeit dieser Zahlungsmöglichkeiten willkommen ist, werden die Nachteile oft übersehen: Die derzeitige Umsetzung ermöglicht die Totalüberwachung der ökonomische Aktivität von Benutzer*innen.

Proprietäre Lösungen wie Apple Pay und Google Pay basieren auf geschlossenen Implementationen/Schnittstellen und werden von mächtigen US-Amerikanischen Oligopolen kontrolliert. Diese erlangen so Zugriff auf die Aktivitätsprofile von Benutzer*innen, welche dann für Werbezwecke ausgewertet und/oder verkauft werden.

GNU Taler ist ein freies Online-Bezahlsystem welches die Privatsphäre von Kund*innen schützt und gleichzeitig das Einkommen von Händler*innen gegenüber Buchprüfer*innen offenlegt. Damit werden illegale Aktivitäten wie Steuerhinterziehung oder der Handel mit illegalen Waren erschwert. Die bisherige Implementation von GNU Taler war jedoch stark auf das Bezahlen von Online-Inhalten im Browser fokussiert.

Ziel dieses Projekts war es, GNU Taler mit NFC-Zahlungen auf Hardware-Plattformen (primär Smartphones) zu erweitern, um somit auch bequeme bargeldlose Zahlungen in Präsenzsituationen zu ermöglichen. Dies umfasst Szenarien, in denen nur eine der beiden Parteien Internetzugang hat.

Es waren folgende Meilensteine geplant:

Meilenstein 1 (1. März – 31. März 2019): Design und Spezifikation des Taler NFC-Protokolls zwischen Käufer*innen und Bezahlterminal der Händler*innen.

Meilenstein 2 (1. April - 15. Mai 2019): Implementation und Testing einer Android-Bibliothek für das Taler NFC-Protokoll.

Meilenstein 3 (16. Mai - 30. Juni 2019): Implementation einer Bezahlterminal-App für die Android-Plattform, welche das NFC-Protokoll aus Meilenstein 1 und 2 unterstützt und mit dem existierenden GNU Taler Backend der Händler*innen kommuniziert.

Meilenstein 4 (1. Juli - 31. Juli 2019): Portierung des existierenden GNU Taler Wallets (= digitale Geldbörse) auf die Android-Plattform.

Meilenstein 5 (1. August - 31. August 2019): Integration der NFC-Zahlungen und der dazugehörigen Benutzeroberfläche in das GNU Taler Wallet auf Android, mit abschließendem Testing.

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Das Projekt richtet sich an Institutionen und Organisationen die ihren Mitgliedern oder Kund*innen ein bargeldloses Zahlungsmittel anbieten wollen, ohne dabei die Privatsphäre der Käufer*innen zu verletzen. Im Kleinen könnte das Mensa/Cafeteria einer Schule, Universität oder Firma sein.

In einem Größeren Umfang können Finanzdienstleister (wie z.B. Banken) Händler*innen und Kund*innen untereinander Zahlungen abwickeln lassen und von Transaktionsgebühren profitieren.

Kunden und Händler profitieren dabei von der Austauschbarkeit des Zahlungsdienstleisters und Wettbewerb unter den Dienstleistern, da das Bezahlsystem auf einem offenen Protokoll mit offener Implementation basiert.

Ausführliche Darstellung der Ergebnisse

Folgende Ergebnisse wurden erzielt:

- Entwicklung und Dokumentation der Taler NFC Spezifikation (https://docs.taler.net/taler-nfc-guide.html) und der "taler://" URI-Schema-Spezifikation (https://docs.taler.net/core/taler-uri.html). Diese beiden Spezifikationen ermöglichen gemeinsam das Auslösen von Bezahlvorgängen (so wie Geldabhebevorgängen) in der Taler Wallet per NFC ("tap-to-pay") so wie durch das Scannen eines QR-Codes.
- Entwicklung von *node-android-v8*, einem Fork des Node.JS Projekts, der die nötigen Änderungen am Code und Buildsystem enthält, um den Node.JS Interpreter für Android-Geräte mit ARM Prozessor bauen und ausführen zu können.
- Entwicklung der *akono*-Bibliothek (**A**ndroid **Ko**tlin Bindings for **No**de.JS), welche es ermöglicht, beliebige Node.JS-Anwendungen von einer Kotlin-Anwendung auf Android zu starten und mit diesen Anwendungen per IPC (Interprozesskommunikation) zu interagieren.
- Erweiterung des existierenden Taler-Merchant-Backends. Das Taler-Merchant-Backend ist ein Dienstprozess, welcher eine einfache Schnittstelle für Händler*innen zur Zahlungsabwicklung zur Verfügung stellt. Im Rahmen dieses Vorhabens wurde das neu entwickelte "taler://" URI-Konzept in das Backend integriert.

- Entwicklung der *taler-merchant-terminal* Android-Anwendung. Diese Anwendung erlaubt es, eine Zahlungsaufforderung für eine Bestellung zu erzeugen und einen Zahlvorgang in der Wallet-Anwendung des Kunden anschließend per NFC oder QR-Code auszulösen. Bei erfolgreichem Abschluss der Zahlung wird dem Händler in der Anwendung eine Mitteilung angezeigt. Zudem kann die Historie der Zahlungsvorgänge betrachtet werden.
- Entwicklung der *android-wallet* Android-Anwendung. Diese Anwendung ermöglicht es Benutzer*innen, digitales Geld abzuheben und anonym auszugeben. Dabei wird die existierende Wallet mit Hilfe der *akono*-Bibliothek auf Android ausgeführt.
- Entwicklung von *idb-bridge*, einer Bibliothek welche die von der W3C standardisierte und in Browsern weit verbreitete IndexedDB Datenbankschnittstelle (https://www.w3.org/TR/IndexedDB/) für Anwendungen in der Node.JS-Umgebung zur Verfügung stellt. Die implementation basiert auf der existierenden fakeIDB Bibliothek, welche mit Persistenz und einem neuen Speicher-Backend basierent auf persistenten B+-Bäumen erweitert wurde.
- Integration des QR-Code Konzepts auf den Taler-Demo Websites. Es ist nun möglich, mit der Android-Wallet einen QR-Code auf einer Website im Browser eines andere Computers zu scannen, um z.B. für einen digitalen Zeitungsartikel anonym zu bezahlen.
- Überarbeitung der Projektseite (https://taler.net/en/) im Rahmen des UX-Coachings das durch die Open Knowledge Foundation organisiert wurde.

Im Rahmen der Arbeit an dem Projekt konnte die technische Herangehensweise der Portierung validiert und als erfolgreich eingestuft werden.

Der ursprünglich geplante Funktionsumfang konnte erreicht werden. Alle Meilensteine (mit den im Abschnitt "Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung" erläuterten Änderungen) wurden erreicht.

Im Rahmen des durch die Open Knowledge Foundation organisierte UX-Coaching wurde daran gearbeitet, die Kommunikation des Projekts mit der Öffentlichkeit zu verbessern. Es wurde gemeinsam die Informationsarchitektur der GNU Taler Website überarbeitet. Zudem wurden Werkzeuge erläutert, mit denen die Verständlichkeit der Anwendungen für Benutzer*innen verbessert werden kann. Ein hier besonders wertvolles Werkzeug war das Aufstellen von Wortlisten die in der öffentlichen Kommunikation benutzt (mit Begründung) bzw. nicht benutzt (mit Alternative) werden sollen.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Die Umsetzung dieses Projekts stellt einen wichtigen Meilenstein in der Entwicklung einer freien Infrastruktur für digitale Bezahlsysteme dar, welche die Privatsphäre der Benutzer*innen nicht verletzen, jedoch trotzdem das Vorgehen gegen Steuerhinterziehung oder illegale Geschäfte ermöglichen.

Die "Nebenprodukte" dieses Vorhabens sind als Open-Source auch generell einsetzbar: Die *Akono*-Laufzeitumgebung kann als Startpunkt verwenden werden, um andere JavaScript/Node.JS Projekte nach Android zu portieren. Die "idb-bridge" Bibliothek kann zum Portieren und Testen von Programmen verwenden werden, die ursprünglich in einer Browser-Umgebung laufen.

Durch die Arbeit an dem Projekt war es mir möglich, mich tief in die Node.JS+V8 Laufzeitumgebung einzuarbeiten und die Entwicklung von Android-Anwendungen mit Kotlin zu erlernen. Zudem lernte ich bei dem UX Coaching hilfreiche Werkzeuge, die ich auch in weiteren Projekten einsetzen kann.

Noch dieses Jahr wird voraussichtlich eine Gruppe von Studenten der Berner Fachhochschule an einem Projekt arbeiten, in dem das GNU Taler NFC-Protokoll in einen Warenverkaufsautomat integriert werden soll. Dieser Arbeit liegt die im Rahmen dieses Vorhabens entwickelte NFC-Spezifikation zu Grunde, so wie die Android Wallet-Application.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Der anfängliche Arbeitsplan enthielt einen Meilenstein zur Implementation einer Hilfsbibliothek für das NFC-Protokoll. Die Architektur des Bezahlterminals wurde in der Planungsphase jedoch sehr stark vereinfacht. Anstatt selbst Anfragen des Wallets zu bearbeiten, leitet das Bezahlterminal diese Anfragen an das existierende Merchant-Backend weiter. Dort werden die Anfragen des Wallets entweder direkt bearbeitet, oder an die Exchange (d.h. den Zahldienstleister) weitergeleitet. Die per NFC gesendeten Anfragen werden als in JSON (JavaScript Object Notation) gekapselte HTTP-Requests dargestellt. Diese vereinfachte Architektur und das vereinfachte Format von Anfragen macht die Implementation einer gesonderten NFC-Bibliothek für das Bezahlterminal unnötig. Stattdessen musste nur eine einfache Weiterreichung von Anfragen an das Merchant-Backend implementiert werden.

Zudem wurde ursprünglich geplant, die graphische Oberfläche der Android-Komponenten in einer plattformunabhängigen Programmierumgebung (z.B. Flutter oder React Native) zu implementieren. In der Designphase der grafischen Oberfläche stellte sich jedoch heraus, dass dieser Ansatz nicht zielführend war, da viele Interaktionsmuster der grafischen Oberfläche auf verschiedenen Plattformen zur Verbesserung der Benutzbarkeit anders gestaltet werden müssen.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Der Quellcode des GNU Taler Projekts kann auf der folgenden Website abgerufen werden und auch in das Versionskontrollprogramm Git importiert werden: https://git.taler.net/

Speziell im Rahmen des Vorhabens "Digital_Bargeld" wurde primär an den Repositories "akono.git", "wallet-core.git", "android-node-v8.git", "wallet-android.git", "merchant.git", "merchant-terminal-android.git", "docs.git" und "exchange.git" gearbeitet.

Generelle Informationen über das gesamte Projekt so wie Dokumentation können unter https://taler.net/ abgerufen werden.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Die Kostenplanung wurde weitgehend Eingehalten. Die Komplexität der Portierung der Wallet (Meilenstein 4) erforderte einen Mehraufwand. Zudem wurde dieser Meilenstein in der Projektplanung an den Anfang verlegt.

Die Implementation der NFC-Bibliothek (Meilenstein 2) wurde aus der Projektplanung gestrichen, da in dem Design des NFC-Protokolls (Meilenstein 1) eine vereinfachte Architektur herausgearbeitet

wurde, die eine Taler-spezifische NFC-Bibliothek unnötig macht. Mit dieser Änderung konnte der anfänglich geplante Funktionsumfang gänzlich erreicht werden.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Während der Förderung bestand regelmäßiger Austausch mit anderen Mitgliedern des GNU Taler Projekts. Dies diente Hauptsächlich der Absprache von Protokolländerungen, die im Rahmen des Vorhabens nötig waren.

Zudem bestand kurzer Kontakt mit dem V8-Projektteam von Google, um gemeinsam einen Fehler (siehe https://bugs.chromium.org/p/v8/issues/detail?id=9171) in dem V8 JavaScript-Interpreter zu beheben, da dieser Fehler ein Hindernis bei der Portierung des GNU Taler Wallets ein Hindernis war.