Richtlinie zum „Software-Sprint“

LibEuFin – Freie API und Sandbox für das europäische Finanzsystem

Schlussbericht

Zuwendungsempfänger:

Marcello Stanisci & Florian Dold, Fintech-Bibliotheksentwicklung GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS19S02 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Die europäischen Zahlungsdienstrichtlinie PSD2 soll unter anderem innovative Finanz-Anwendungen ermöglichen, indem Banken dazu verpflichtet werden, Programmierschnittstellen (APIs) für Kontoinformationen und Zahlungsauslösung anzubieten. Allerdings sind die APIs und Nachrichtenformate die von Banken bereitgestellt werden so vielfältig und komplex, dass kleinere Projekte und Privatpersonen diese kaum nutzen können.

Das Testen war bisher nur mit hohem Aufwand, echten Bankkonten bei diversen Anbietern und proprietärer Software möglich. Im Ergebnis werden Projekte für persönliche Finanzplanung und Banking für Bürger*innen praktisch nur von großen, profitorientierten Unternehmen entwickelt.

LibEuFin soll Entwickler*innen das Entwickeln und Testen von freien Anwendungen im Bereich Online-Banking erleichtern, beispielsweise für die persönliche Finanzplanung.

Zu diesem Zweck sollte im Rahmen dieses Projekts eine Bibliothek implementiert werden, die die verbreitetsten deutschen und europäischen Banking-Standardprotokolle (FinTS/EBICS/ ISO 20022) unter einer vereinfachten Schnittstelle zur Verfügung stellt. Zudem wurde eine Sandbox entwickelt, mit der Entwickler*innen ihre Banking-Anwendungen ausreichend automatisiert testen können, ohne Konten mit Testzugang bei mehreren Banken zu benötigen.

Das Projekt wurde ursprünglich in folgende Meilensteine aufgeteilt:

Meilenstein 1 (1. Sept. - 30. Sept. 2019): Herausarbeiten der wichtigsten Nachrichtenformate und Auftragsarten der Standards (FinTS/EBICS/ISO 20022)

Meilenstein 2 (1. Okt. - 31. Okt. 2019): Entwicklung einer Bibliothek für die Kryptographie und Nachrichtenformate

Meilenstein 3 (1. Nov. - 15. Nov. 2019): Entwicklung der Bibliothek für Kontoinformationen und Zahlungsauslösung

Meilenstein 4 (16. Nov. 2019 - 15. Jan 2020): Entwicklung der Banking-Sandbox

Meilenstein 5 (16. Jan - 31. Jan. 2020): Dokumentation und Lernmaterialien

Meilenstein 6 (1. Feb. - 29. Feb. 2020): Umsetzung einer Beispielanwendung

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

Die Zielgruppe des Projekts sind Entwickler*innen von Software, die Nutzern automatisierten Zugriff auf europäischen Bankkonten ermöglicht. Speziell kleine Unternehmen, Organisationen und Open-Source Entwickler*innen können von einer freien Implementation und Testumgebung profitieren.

Hierbei besteht Zusammenhang zu mehreren Themenfeldern und Zielen des Software Sprints:

1. *Softwareinfrastruktur.* Die Verfügbarkeit von einer Infrastruktursoftware wie LibEuFin, die vereinfachten programmatischen Zugriff auf Bankkonten bietet, ermöglicht die Automatisierung von Prozessen in Projekten und Organisationen. Existierende proprietäre Software für den elektronischen Zugriff auf Bankkonten bietet keine programmierbare Schnittstelle an, sondern nur vom Hersteller definierte feste Abläufe. Zudem muss Softwareinfrastruktur robust sein. Dies ist bei modernen Softwareprojekten grundsätzlich nur mit ausführlichen automatisiertem Testen möglich. Deshalb gibt LibEuFin der *Bank-Sandbox* einen besonders hohen Stellenwert.
2. *Data Literacy**.*** Der automatisierte Lesezugriff auf Bankkonten mit einer Open Source Softwarebibliothek wie LibEuFin ermöglicht die persönliche Finanzplanung und Auswertung der eigenen Ausgabegewohnheiten, ohne dabei diese Daten an Drittanbieter weiterzuleiten zu müssen.

Ausführliche Darstellung der Ergebnisse

Die folgenden Softwarekomponenten sind in diesem Projekt entwickelt worden:

- Die *LibEuFin Sandbox*, einer Serveranwendung welche einen Bankenserver simuliert der das EBICS-Protokoll (sowie zukünftig andere Protokolle wie FinTS) als Server anbietet. Dabei wird in sehr rudimentärer Weise die Benutzer- und Transaktionsverwaltung einer echten Bank nachgestellt.
- Der *LibEuFin Nexus*, einem Dienst der Anfragen in einer sehr leicht für Entwickler*innen zu benutzenden, auf HTTP+JSON basierten Schnittstelle entgegennimmt, und diese in verschiedene Transport- und Nachrichtenformate (derzeit EBICS und ISO 20022) übersetzt und an den Bankserver versendet. Dabei werden komplexe Prozesse wie Schlüsselverwaltung, Kryptographie und Protokolle zur signierten und segmentierten

Datenübertragung abstrahiert. Nutzer*innen der *LibEuFin Nexus* Programmierschnittstelle müssen sich darüber keine Gedanken machen.

Wie bereits erwähnt gibt es keine frei zugänglichen Testumgebungen für das EBICS-Protokoll oder ähnliche Bankprotokolle. Jedoch gibt es leicht für Privatkunden zugängliche, proprietäre Homebanking-Anwendungen, die gängig von deutschen Banken (GLS, Sparkasse, ...) angeboten werden.

Unsere innovative Strategie war, zuerst die Bank-Seite des Protokolls in der *LibEuFin Sandbox* nachzubauen. Mit mehreren proprietären Homebanking-Anwendungen konnten wir dann leicht verifizieren, ob die Sandbox das jeweilige Protokoll und die Nachrichtenformate korrekt implementiert und wo Anpassungen unseres Programms nötig sind. Somit konnten wir uns indirekt eine validierte Testumgebung verschaffen, welche normalerweise von Banken nicht angeboten wird.

In der nächsten Phase haben wir dann unsere *LibEuFin Sandbox* verwendet, um unsere client-seitige Implementation einfach validieren und testen zu können.

Abschließend konnten wir mit einem echten Firmenkonto bei der GLS Bank verifizieren, dass die Implementation des *LibEuFin Nexus* der Protokollspezifikation entspricht.

Wir haben folgende Funktionalität entwickelt, deren Sandbox-Implementation mit mehreren Homebanking-Anwendungen verifiziert und mit einem echten Bank-Server getestet:

1. Teilnehmerverwaltung und Initialisierung auf Basis von kryptographischen Schlüsseln. Bei diesem (in EBICS und FinTS verwendeten) Verfahren erzeugt die Homebanking-Anwendung bzw. der *LibEuFin Nexus* kryptographische Schlüsselpaare und sendet die öffentlichen Schlüssel digital an die Bank. Zudem muss der/die Kund*in die öffentlichen Schlüssel auf Papier ausdrucken, unterzeichnen und an die Bank senden, welche nach Überprüfung der Unterschrift den Teilnehmer freischaltet.
2. Abrufen von maschinenlesbaren Kontoauszügen und Vormerkposten
3. Zahlungsauslösung auf Basis der SEPA-Überweisung

Andere Vorgänge (z.B. Verwaltung von Lastschriften) können in Zukunft mit relativ geringem Aufwand implementiert werden, da LibEuFin eine umfassende Hilfsbibliothek als Grundlage anbietet.

Alle Komponenten wurden in der Programmiersprache Kotlin entwickelt, welche (dank der darunterliegenden JVM Plattform) die sehr komplexen XML-Standards unterstützt, welche von dem EBICS-Protokoll benutzt werden. Zudem kann eine in Kotlin entwickelte Anwendung sehr einfach in mobile Anwendungen für Android-Smartphones eingebunden werden.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Wir wurden bereits von mehreren Community-Projekten mit Interesse an LibEuFin angesprochen. Als Beispiel darf "MyExpenses" (http://www.myexpenses.mobi/en/) genannt werden, eine Open-Source-Anwendung für persönliches Finanzmanagement auf Mobilgeräten. Ein weiteres Projekt ist daran interessiert, LibEuFin für das Ticket-Kaufsystem einer Eventmanagement-Plattform zu benutzen.

Zudem haben sich bereits mehrere Studenten bei uns gemeldet, die im Rahmen des "Google Summer of Code 2020" Projekts (https://summerofcode.withgoogle.com/) LibEuFin weiterentwickeln wollen.

Die Dachorganisation "GNU" wird auch im Jahr 2020 von Google als Mentor-Organisation gefördert und bietet in diesem Rahmen auch Projektideen für LibEuFin an. Eine Liste von weiterführenden Projektideen zu LibEuFin ist hier zu finden:
https://www.gnu.org/software/soc-projects/ideas-2020.html#taler

Das Taler Projekt (gefördert in Runde 5 des Prototype Funds) wird zudem LibEuFin einbinden, um den praktischen Einsatz der Software-Infrastruktur für ein datenschutzfreundliches Bezahlsystems für "digitales Bargeld" zu ermöglichen.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Wegen der immens hohen Komplexität des EBICS-Protokolls und des ISO 20022 Standards haben wir uns vorerst auf die Implementation dieses einen Übertragungsprotokolls beschränkt. Jedoch wäre die Integration von anderen Übertragungsstandards wie z.B. dem deutschen FinTS Standard mit erheblich weniger Aufwand verbunden, da dieser ebenso wie EBICS Nachrichten in dem auf XML basierenden ISO 20022 Standardnachrichtenformat für Finanzdienste austauscht.

Zudem wurde vorerst auf die Entwicklung einer Beispielanwendung mit graphischer Oberfläche verzichtet, und stattdessen eine an Entwickler*innen gerichtetes Kommandozeilenprogramm als Beispielanwendung entwickelt. Eine umfassende und an Endbenutzer*innen gerichtete grafische Oberfläche soll in dem bereits erwähnten Google Summer of Code Projekt von einem Studenten entwickelt werden.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Quellcode: https://git.libeufin.tech/
Dokumentation mit API-Dokumentation und ausführlichen Erläuterungen zu dem EBICS-Protokoll:
https://docs.libeufin.tech/

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Die Kostenplanung wurde weitgehend eingehalten. Jedoch musste wegen Mehraufwand bei den Meilensteinen 1-4 die für die beiden letzten Meilensteine zur Dokumentation und Entwicklung der Beispielanwendung gekürzt werden.

Zudem wurde die Entwicklung der Sandbox (Meilenstein 4) vorgezogen und parallel mit Meilensteinen 2-4 bearbeitet. Dies ermöglichte schnelles und zuverlässiges Testen mit der vorausgehend beschriebenen Methode der indirekt validierten Protokoll-Implementation.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Bei der Entwicklung der Anforderungen an die Architektur von LibEuFin wurde Rücksprache mit den Entwickler*innen des GNU Taler Projekts gehalten.